FortiAuthenticator - Cookbook

Version 6.1.0

December 16, 2020
FortiAuthenticator 6.1.0 Cookbook
23-610-616361-20201216

TABLE OF CONTENTS

Change Log

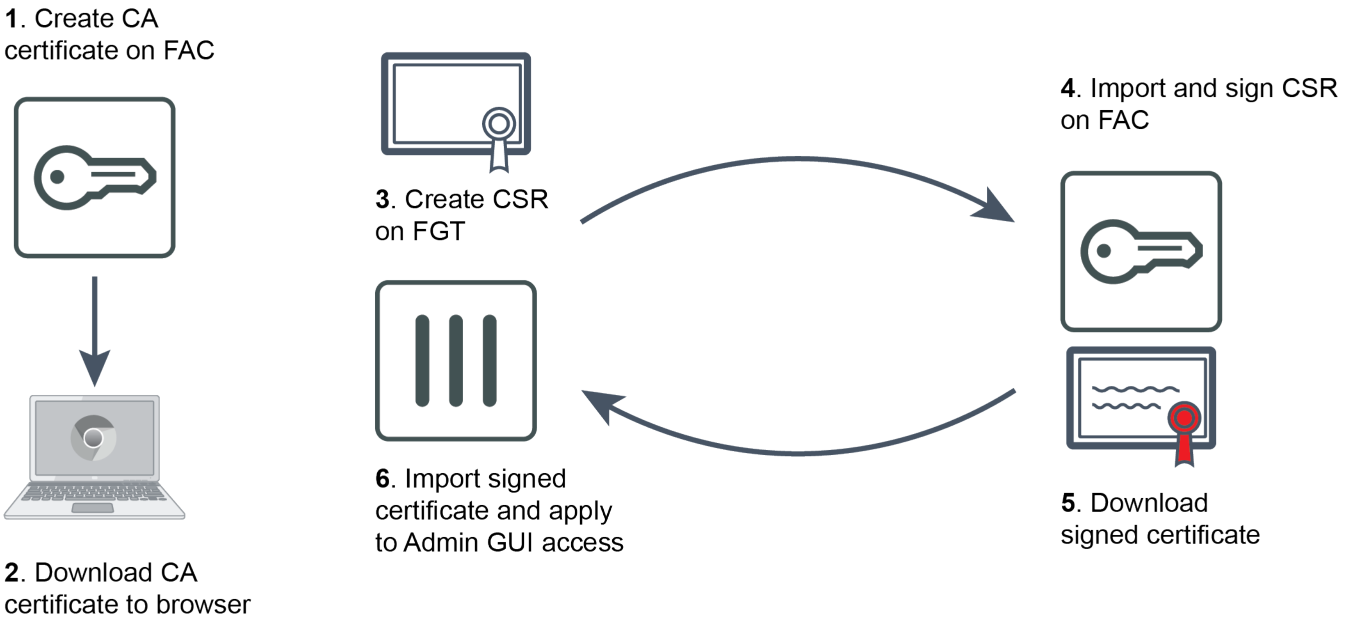
Date	Change Description
2020-03-28	Initial release.
2020-04-06	Added additional configuration information to FortiToken Mobile Push for SSL VPN on page 34.
2020-05-25	Added new configuration examples: • FortiAuthenticator as Guest Portal for FortiWLC on page 49 • MAC authentication bypass with dynamic VLAN assignment on page 59
2020-06-17	Added SAML FSSO with FortiAuthenticator and Okta on page 160.
2020-08-27	Added Office 365 SAML authentication using FortiAuthenticator with 2FA on page 175.
2020-12-16	Updated Configuring the remote SAML server on page 157 in SAML IdP Proxy for G Suite.

Certificate management

This section describes managing certificates with the FortiAuthenticator device.

FortiAuthenticator can act as a certificate authority (CA) for the creation and signing of X.509 certificates, such as server certificates for HTTPS and SSH, and client certificates for HTTPS, SSL, and IPsec VPN.

FortiAuthenticator as a Certificate Authority


1. Create CA certificate on FAC
2. Download CA certificate to browser
3. Create CSR on FGT
4. Import and sign CSR on FAC
5. Download signed certificate
6. Import signed certificate and apply to Admin GUI access

For this recipe, you will configure the FortiAuthenticator as a Certificate Authority (CA). This will allow the FortiAuthenticator to sign certificates that the FortiGate will use to secure administrator GUI access.

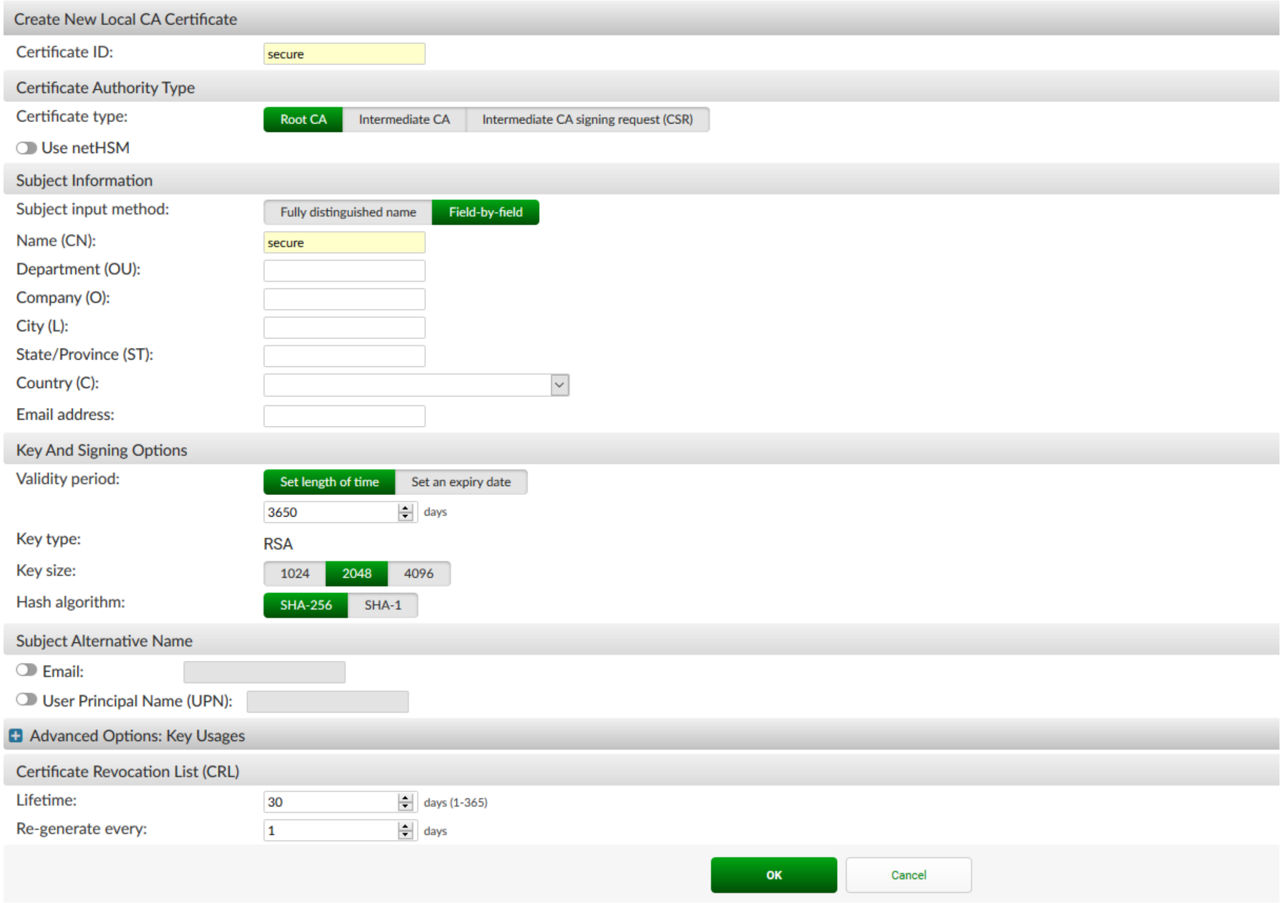
This scenario includes creating a certificate request on the FortiGate, downloading the certificate to the network's computers, and then importing it to the FortiAuthenticator. You will sign the certificate with the FortiAuthenticator's own certificate, then download and import the signed certificate back to the FortiGate.

The process of downloading the certificate to the network's computers will depend on which web browser you use. Internet Explorer and Chrome use one certificate store, while Firefox uses another. This configuration includes both methods.

Creating a new CA on the FortiAuthenticator

To create a new CA:

1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and create a new CA. Enter a *Certificate ID*, select *Root CA certificate*, and configure the key options as shown in the example.



Create New Local CA Certificate

Certificate ID:	secure

Certificate Authority Type

Certificate type:	[✓ Root CA] Intermediate CA Intermediate CA signing request (CSR)
○ Use netHSM	

Subject Information

Subject input method:	Fully distinguished name [✓ Field-by-field]
Name (CN):	secure
Department (OU):	
Company (O):	
City (L):	
State/Province (ST):	
Country (C):	
Email address:	

Key And Signing Options

Validity period:	[✓ Set length of time] Set an expiry date
	3650 days
Key type:	RSA
Key size:	1024 [✓ 2048] 4096
Hash algorithm:	[✓ SHA-256] SHA-1

Subject Alternative Name

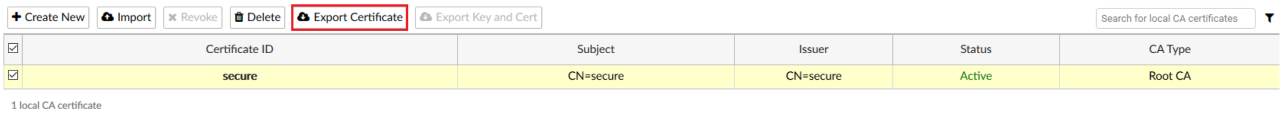
○ Email:	
○ User Principal Name (UPN):	

⊞ Advanced Options: Key Usages

Certificate Revocation List (CRL)

Lifetime:	30 days (1-365)
Re-generate every:	1 days

2. Once created, highlight the certificate and select *Export Certificate*.



☑	Certificate ID	Subject	Issuer	Status	CA Type
☑	secure	CN=secure	CN=secure	Active	Root CA

1 local CA certificate

This will save a *.crt* file to your local drive.

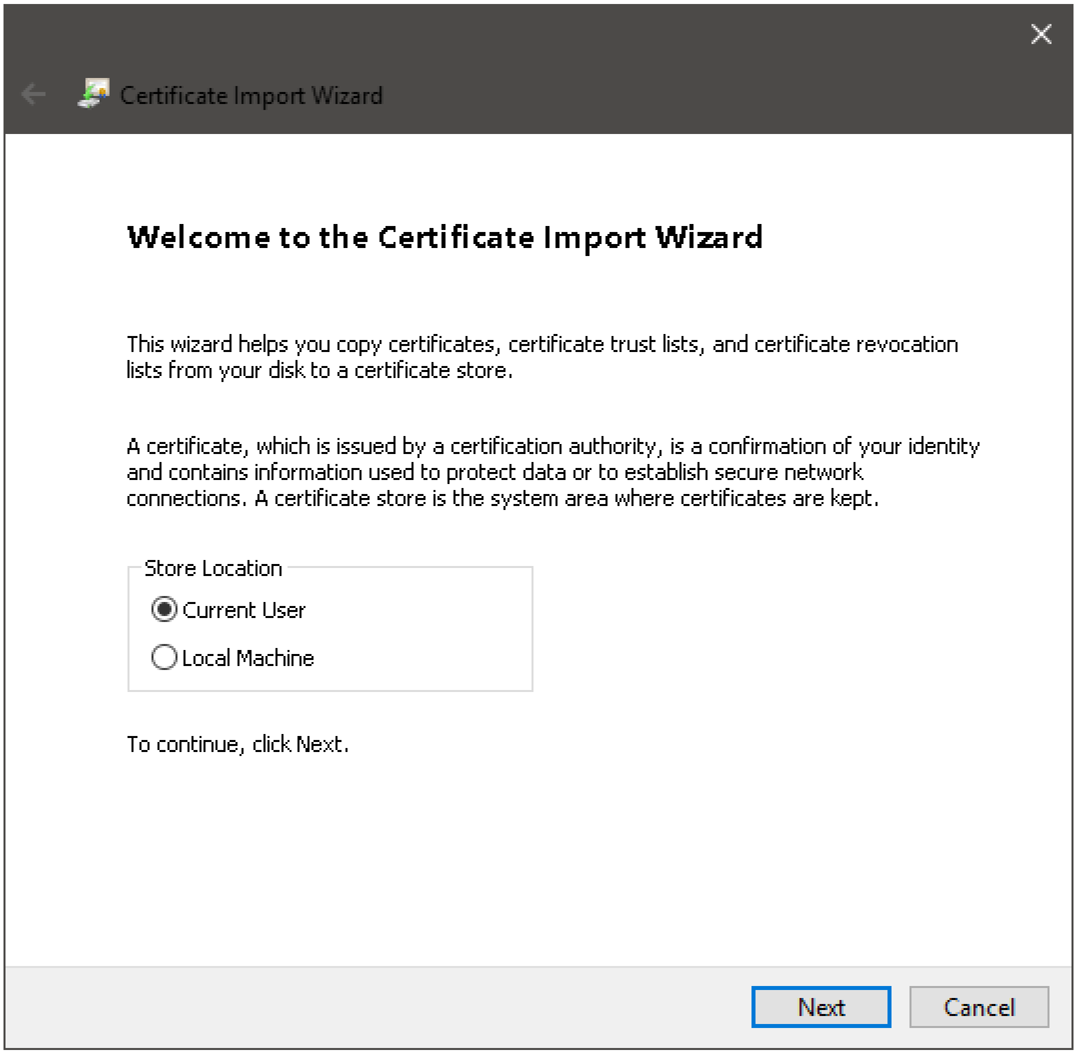
secure.crt

Installing the CA on the network

The certificate must now be installed on the computers in your network as a trusted root CA. The steps below show different methods of installing the certificate, depending on your browser.

Internet Explorer and Chrome

1. In Windows Explorer, right-click on the certificate and select *Install Certificate*. Open the certificate and follow the *Certificate Import Wizard*.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

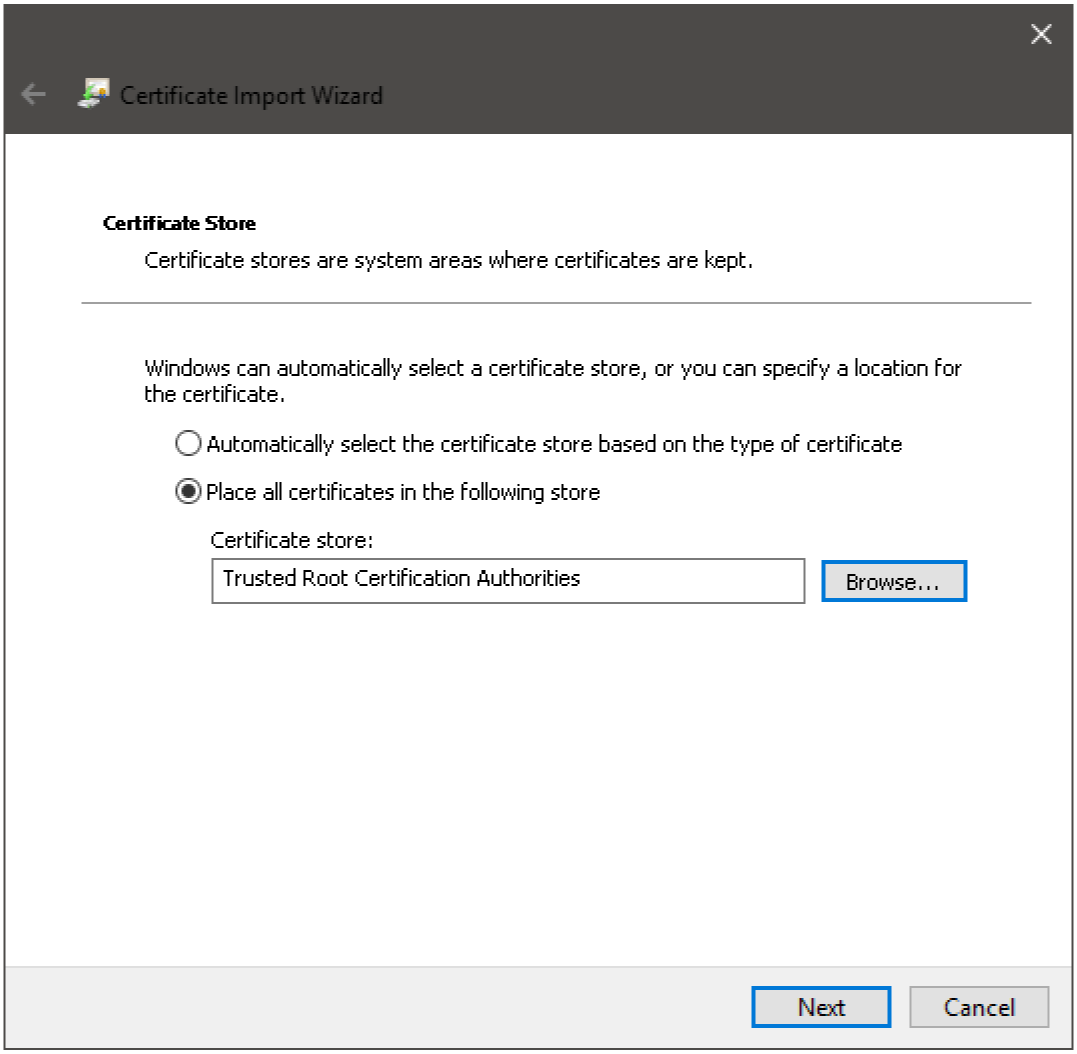
Store Location

● Current User

○ Local Machine

To continue, click Next.

2. Make sure to place the certificate in the *Trusted Root Certification Authorities* store.



Certificate Store

Certificate stores are system areas where certificates are kept.

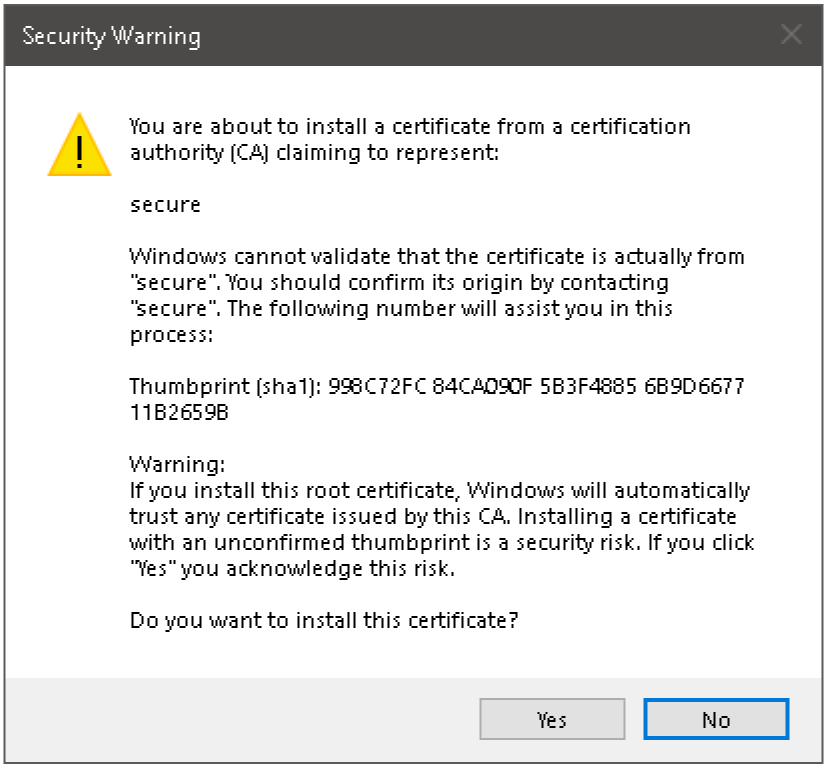
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

3. Finish the Wizard and select *Yes* to confirm and install the certificate.



You are about to install a certificate from a certification authority (CA) claiming to represent:

secure

Windows cannot validate that the certificate is actually from "secure". You should confirm its origin by contacting "secure". The following number will assist you in this process:

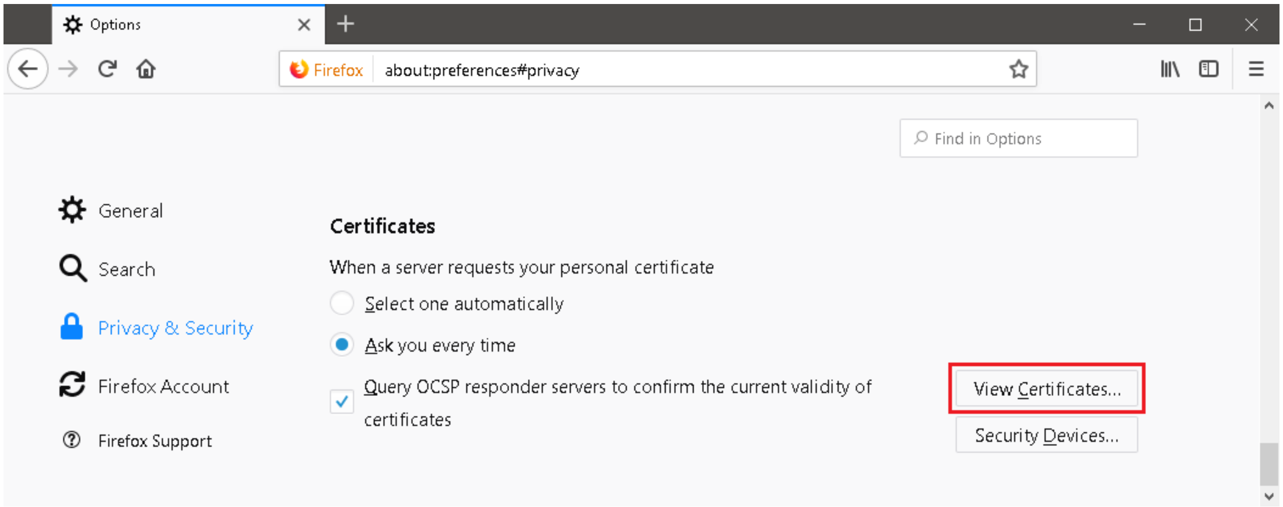
Thumbprint (sha1): 998C72FC 84CA090F 5B3F4885 6B9D6677 11B2659B

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Firefox

1. In the web browser, go to *Options* > *Privacy & Security* > *Certificates*, and select *View Certificates*.



Certificates

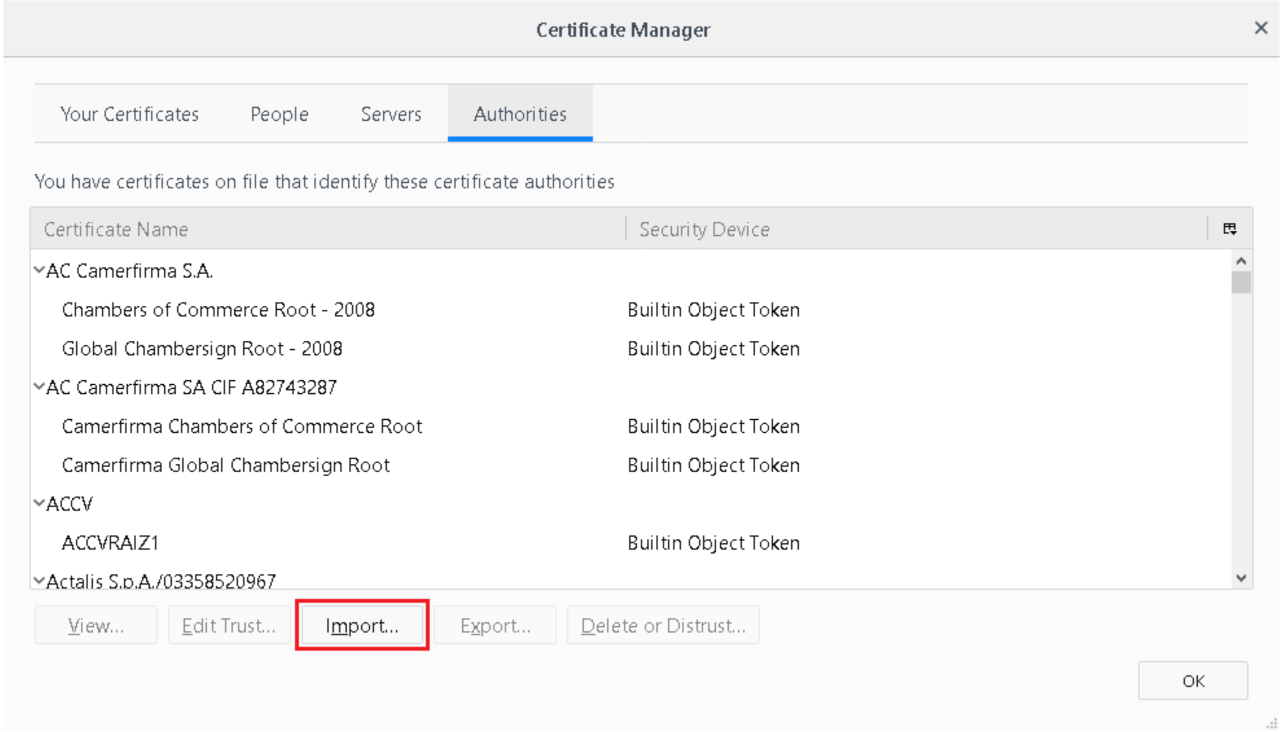
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

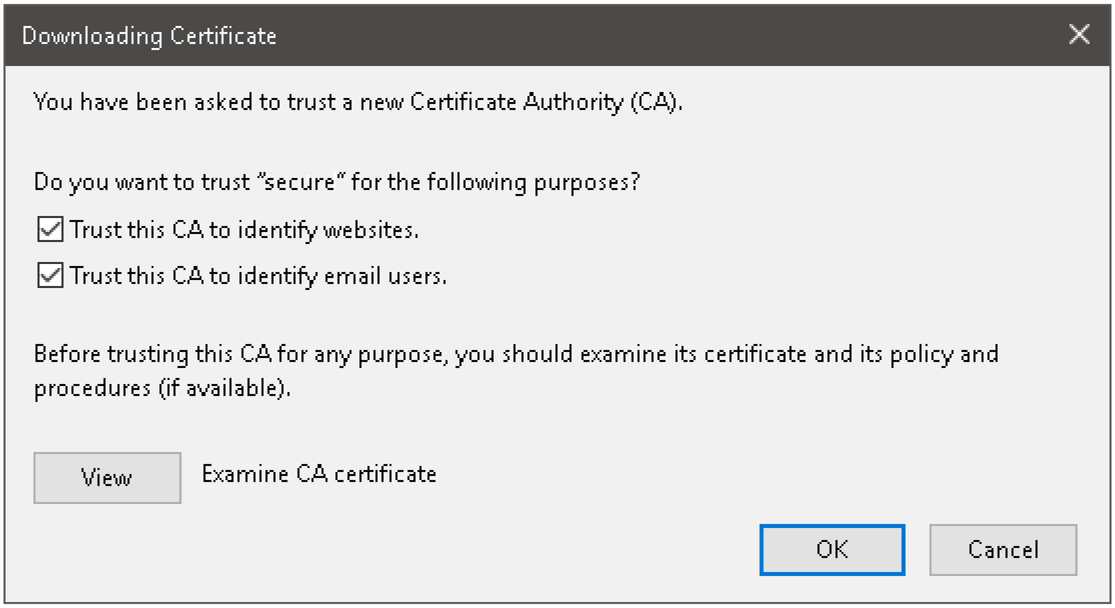
2. In the *Authorities* tab, select *Import*.



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

3. Find and open the root certificate.
   You will be asked what purposes the certificate will be trusted to identify. Select all options and select *OK*.



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "secure" for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

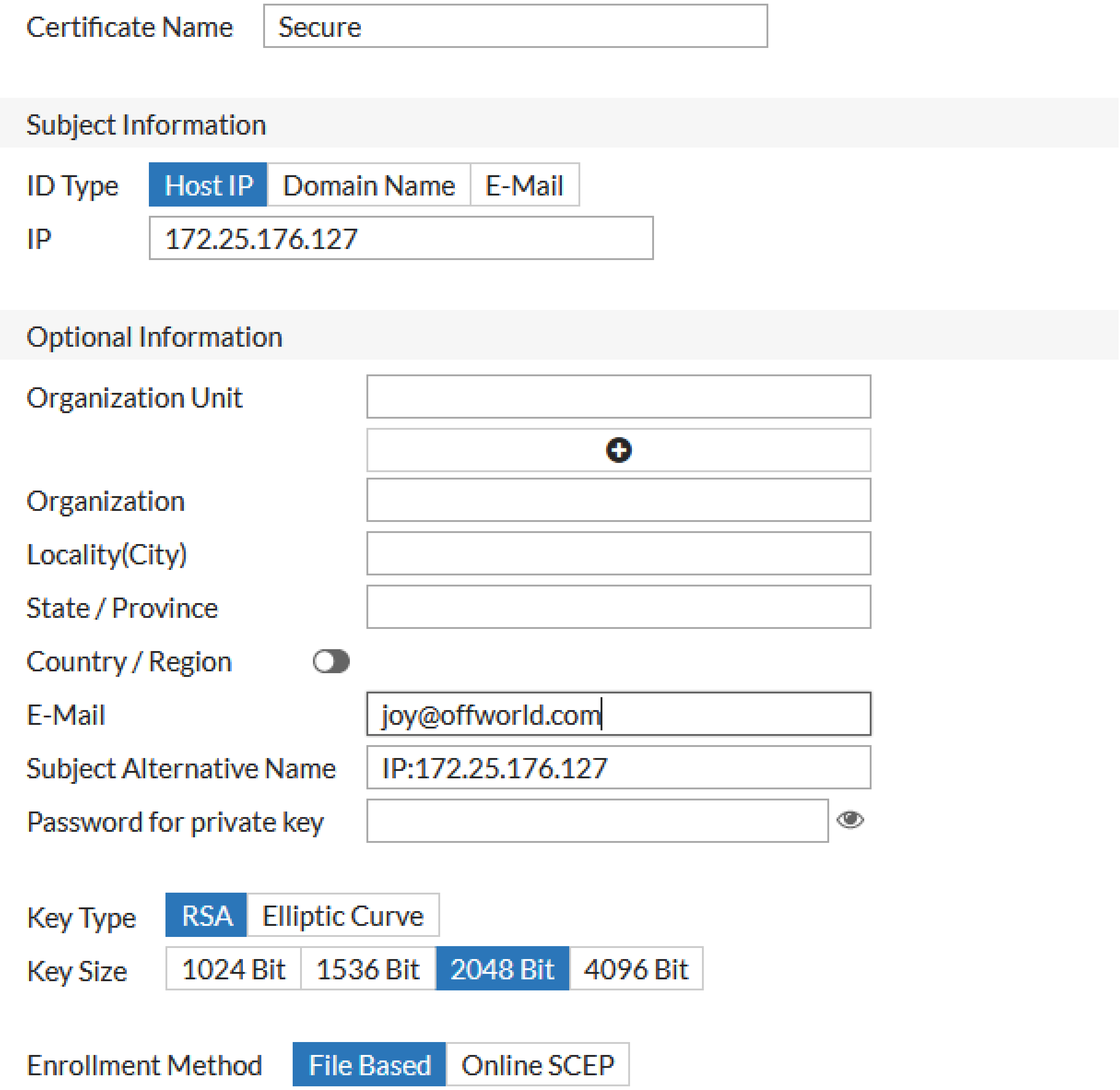
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

Creating a CSR on the FortiGate

To create a CSR:

1. On the FortiGate, go to *System* > *Certificates* and select *Generate* to create a new certificate signing request (CSR). Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.
   The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



Certificate Name: Secure

Subject Information

ID Type: [✓ Host IP] Domain Name E-Mail

IP: 172.25.176.127

Optional Information

Organization Unit:

Organization:

Locality(City):

State / Province:

Country / Region: ○

E-Mail: joy@offworld.com

Subject Alternative Name: IP:172.25.176.127

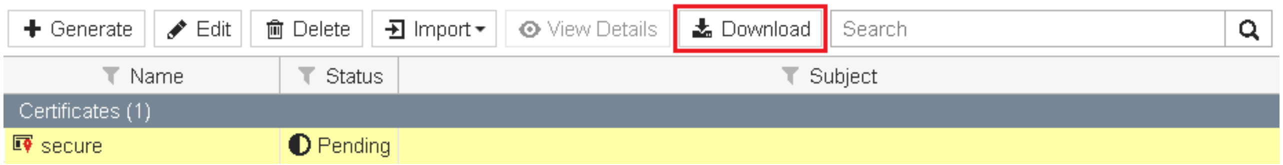
Password for private key:

Key Type: [✓ RSA] Elliptic Curve

Key Size: 1024 Bit 1536 Bit [✓ 2048 Bit] 4096 Bit

Enrollment Method: [✓ File Based] Online SCEP

2. Once created, the certificate will show a *Status* of *Pending*. Highlight the certificate and select *Download*.



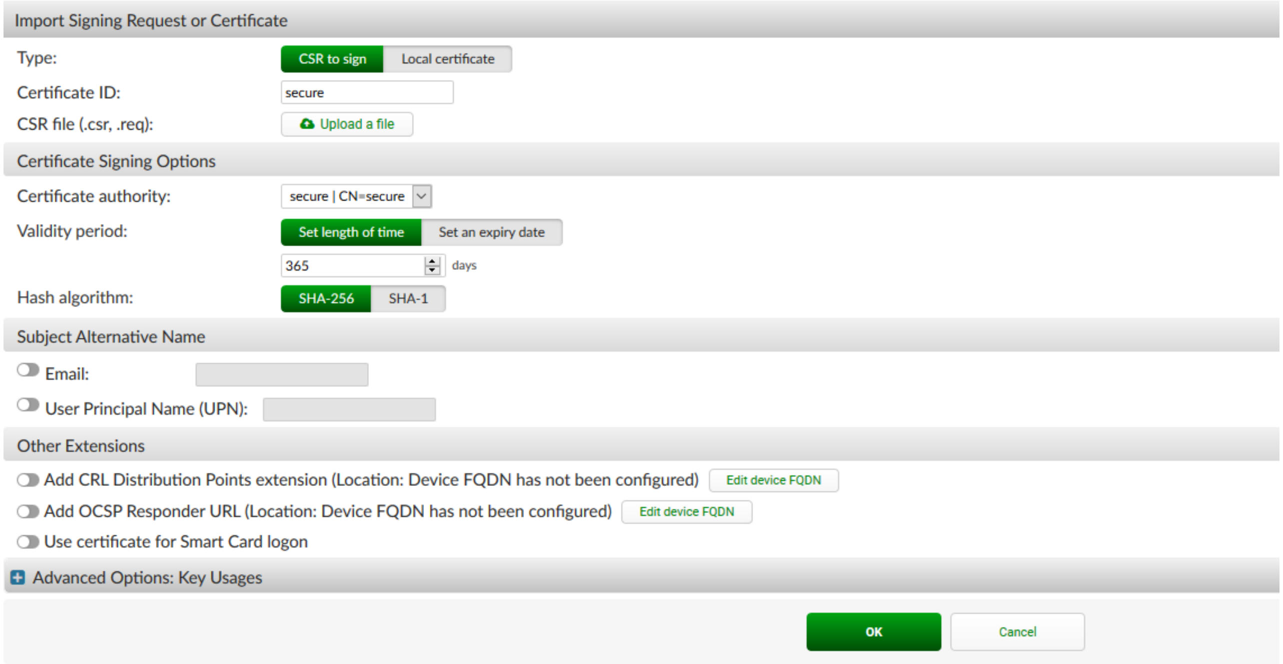
Name	Status	Subject
Certificates (1)		
secure	Pending	

This will save a **.csr** file to your local drive.

Importing and signing the CSR on the FortiAuthenticator

To import and sign the CSR:

1. Back on the FortiAuthenticator, go to *Certificate Management* > *End Entities* > *Users* and import the *.csr* certificate created earlier.
   Make sure to select the *Certificate authority* from the dropdown menu, and set the *Hash algorithm* to *SHA-256*, as configured earlier.



Import Signing Request or Certificate

Type:	CSR to sign / Local certificate
Certificate ID:	secure
CSR file (.csr, .req):	Upload a file

Certificate Signing Options

Certificate authority:	secure | CN=secure
Validity period:	Set length of time / Set an expiry date
	365 days
Hash algorithm:	SHA-256 / SHA-1

Subject Alternative Name

○ Email:

○ User Principal Name (UPN):

Other Extensions

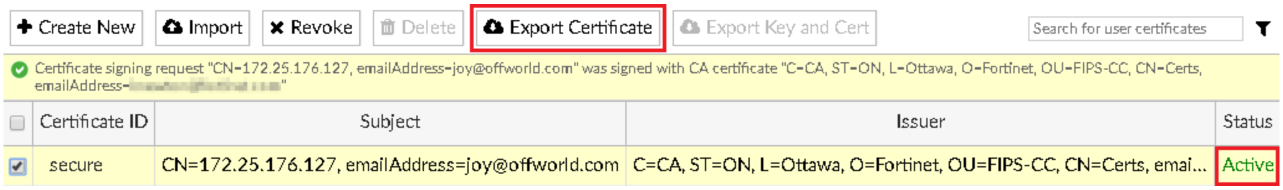
○ Add CRL Distribution Points extension (Location: Device FQDN has not been configured) Edit device FQDN

○ Add OCSP Responder URL (Location: Device FQDN has not been configured) Edit device FQDN

○ Use certificate for Smart Card logon

Advanced Options: Key Usages

2. Once imported, you should see that the certificate has been signed by the FortiAuthenticator, with a *Status* of *Active*. Highlight the certificate and select *Export Certificate*.



Certificate signing request "CN=172.25.176.127, emailAddress=joy@offworld.com" was signed with CA certificate "C=CA, ST=ON, L=Ottawa, O=Fortinet, OU=FIPS-CC, CN=Certs, emailAddress=[redacted]"

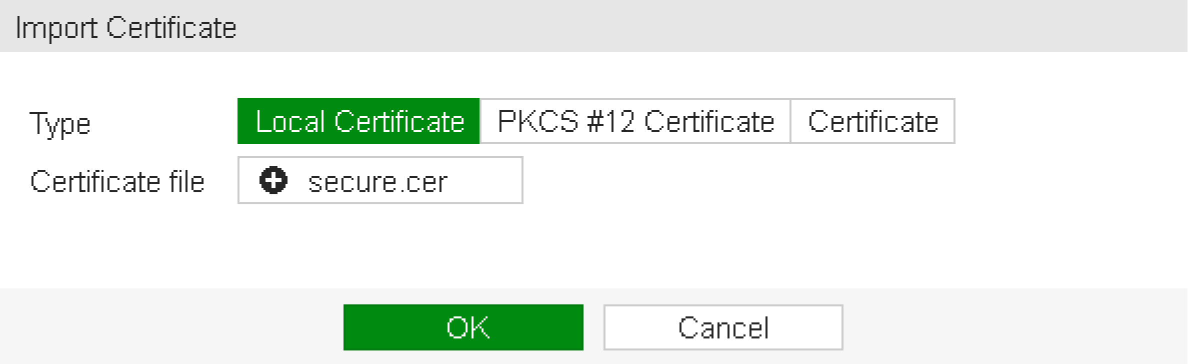
☐	Certificate ID	Subject	Issuer	Status
☑	secure	CN=172.25.176.127, emailAddress=joy@offworld.com	C=CA, ST=ON, L=Ottawa, O=Fortinet, OU=FIPS-CC, CN=Certs, emai...	Active

This will save a **.cer** file to your local drive.

Importing the local certificate to the FortiGate

To import the local certificate:

1. Back on the FortiGate, go to *System* > *Certificates*, and select *Local Certificate* from the *Import* dropdown menu. Browse to the *.cer* certificate, and select *OK*.

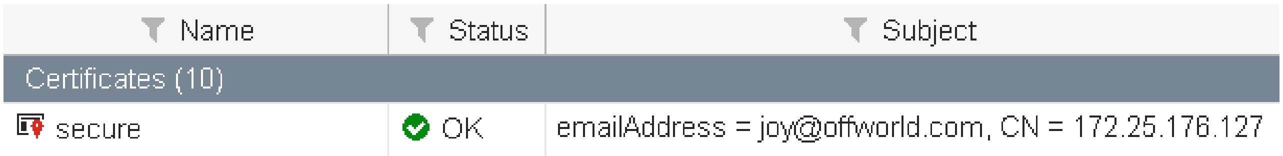


Import Certificate

Type: Local Certificate | PKCS #12 Certificate | Certificate

Certificate file: secure.cer

You should now see that the certificate's *Status* has changed from *Pending* to *OK*. You may have to refresh your page to see the status change.



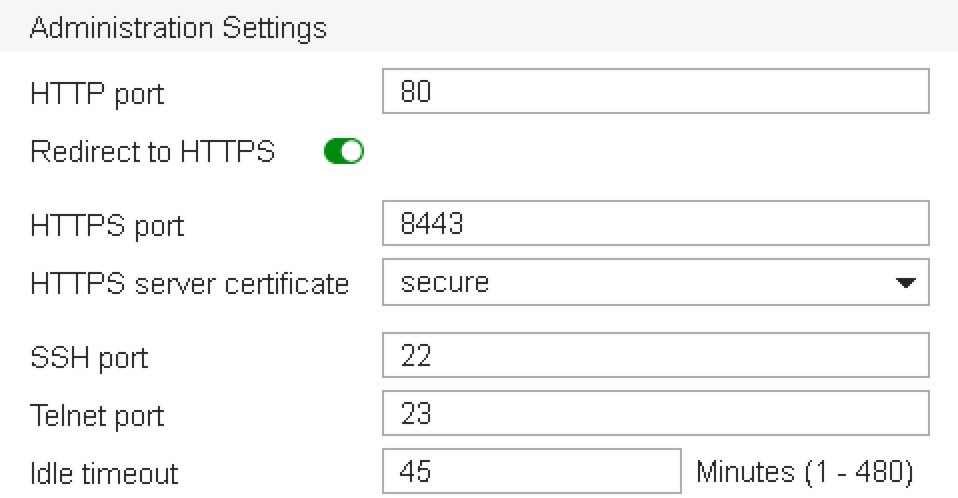
Name	Status	Subject
Certificates (10)		
secure	✓ OK	emailAddress = joy@offworld.com, CN = 172.25.176.127

Configuring the certificate for the GUI

To configure the certificate:

1. On the FortiGate, go to *System* > *Settings*.
Under *Administration Settings*, set *HTTPS server certificate* to the certificate created/signed earlier, then select

Apply.

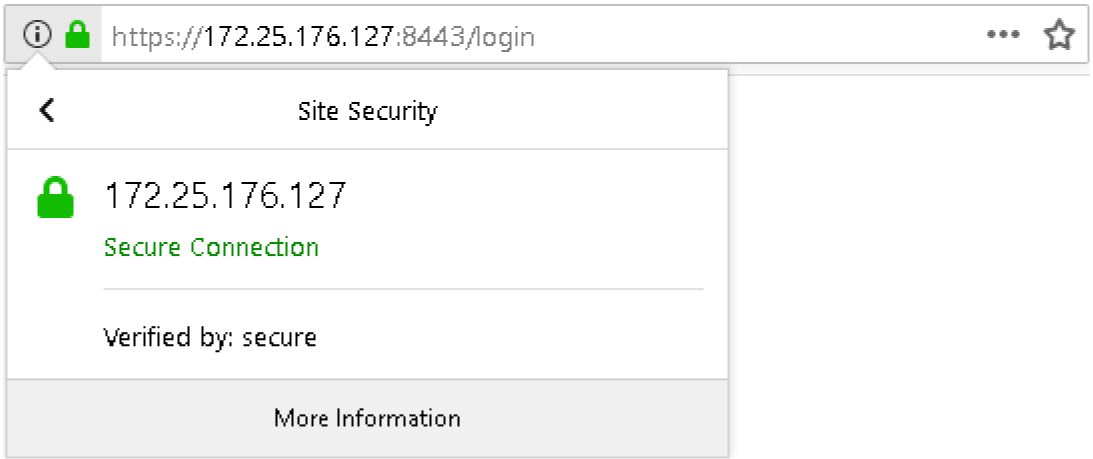


Administration Settings

HTTP port	80
Redirect to HTTPS	●
HTTPS port	8443
HTTPS server certificate	secure
SSH port	22
Telnet port	23
Idle timeout	45 Minutes (1 - 480)

Results

Close and reopen your browser, and go to the FortiGate admin login page. If you click on the lock icon next to the address bar, you should see that the certificate has been signed and verified by the FortiAuthenticator. As a result, no certificate errors will appear.



https://172.25.176.127:8443/login

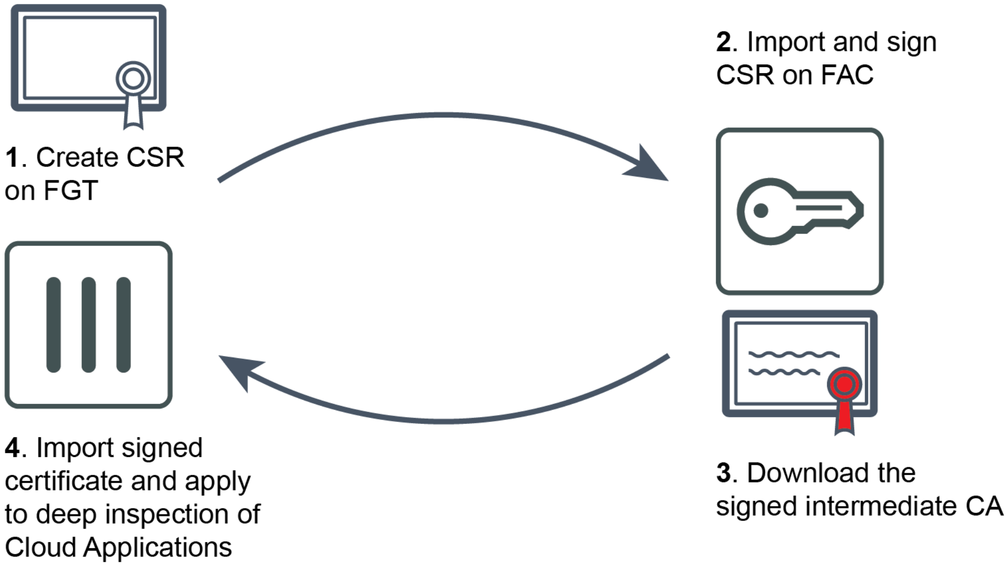
Site Security

172.25.176.127

Secure Connection

Verified by: secure

FortiAuthenticator certificate with SSL inspection


1. Create CSR on FGT
2. Import and sign CSR on FAC
3. Download the signed intermediate CA
4. Import signed certificate and apply to deep inspection of Cloud Applications

For this recipe, you will create a certificate on the FortiGate, have it signed on the FortiAuthenticator, and configure the FortiGate so that the certificate can be used for SSL deep inspection of HTTPS traffic.

Note that, for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this recipe will not be trusted. For more information on how to do this, see FortiAuthenticator as a Certificate Authority.

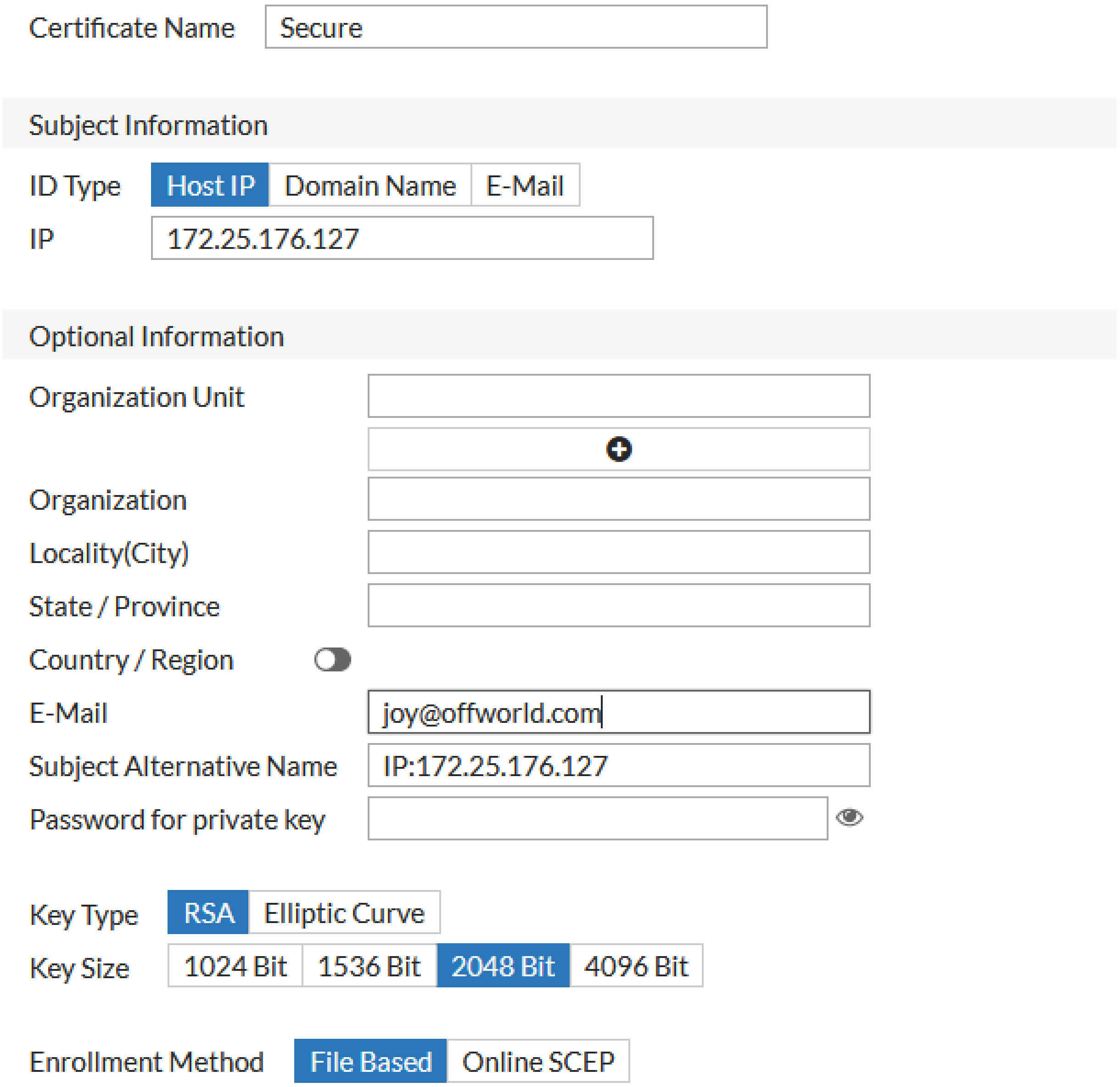
This scenario includes creating a certificate signing request (CSR), signing the certificate on the FortiAuthenticator, and downloading the signed certificate back to the FortiGate. You will then create an *SSL/SSH Inspection* profile for full SSL inspection, add the certificate created to the profile, and apply the profile to the policy allowing Internet access.

As an example, you will also have *Application Control* with *Deep Inspection of Cloud Applications* enabled. This will apply inspection to HTTPS traffic. Note that you may use another security profile instead of *Application Control*.

Creating a CSR on the FortiGate

To create a CSR:

1. On the FortiGate, go to *System* > *Certificates* and select *Generate* to create a new certificate signing request (CSR). Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.
   The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



Certificate Name	Secure

Subject Information

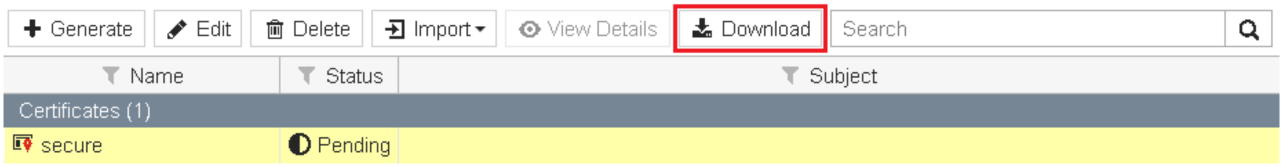
ID Type	[✓ Host IP] Domain Name E-Mail
IP	172.25.176.127

Optional Information

Organization Unit	
Organization	
Locality(City)	
State / Province	
Country / Region	○
E-Mail	joy@offworld.com
Subject Alternative Name	IP:172.25.176.127
Password for private key	

Key Type	[✓ RSA] Elliptic Curve
Key Size	1024 Bit 1536 Bit [✓ 2048 Bit] 4096 Bit
Enrollment Method	[✓ File Based] Online SCEP

2. Once created, the certificate will show a *Status* of *Pending*. Highlight the certificate and select *Download*.



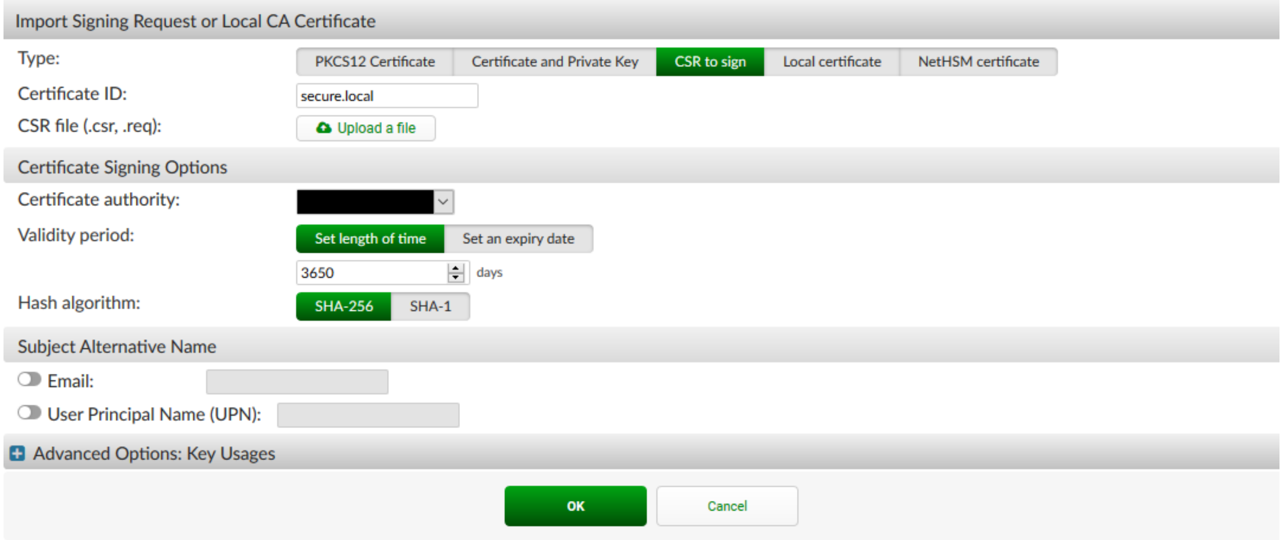
Name	Status	Subject
Certificates (1)		
secure	Pending	

This will save a **.csr** file to your local drive.

Creating an Intermediate CA on the FortiAuthenticator

To create an Intermediate CA:

1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Import*. Set *Type* to *CSR to sign*, enter a *Certificate ID*, and import the CSR file. Make sure to select the *Certificate authority* from the dropdown menu, and set the *Hash algorithm* to *SHA-256*.



Import Signing Request or Local CA Certificate

Type: PKCS12 Certificate | Certificate and Private Key | **CSR to sign** | Local certificate | NetHSM certificate

Certificate ID: secure.local

CSR file (.csr, .req): Upload a file

Certificate Signing Options

Certificate authority: [redacted]

Validity period: **Set length of time** | Set an expiry date

3650 days

Hash algorithm: **SHA-256** | SHA-1

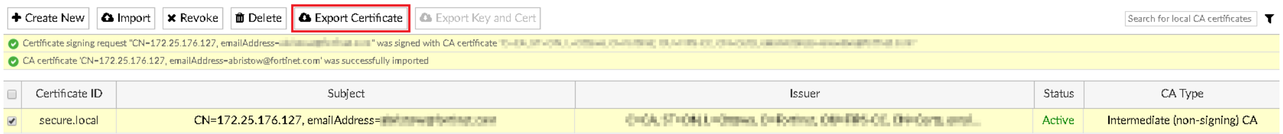
Subject Alternative Name

○ Email:

○ User Principal Name (UPN):

Advanced Options: Key Usages

2. Once imported, you should see that the certificate has been signed by the FortiAuthenticator, showing a *Status* of *Active*, and with the *CA Type* of *Intermediate (non-signing) CA*. Highlight the certificate and select *Export Certificate*.



Certificate signing request "CN=172.25.176.127, emailAddress=[redacted]" was signed with CA certificate [redacted]

CA certificate 'CN=172.25.176.127, emailAddress=abristow@fortinet.com' was successfully imported

☐	Certificate ID	Subject	Issuer	Status	CA Type
☑	secure.local	CN=172.25.176.127, emailAddress=[redacted]	[redacted]	Active	Intermediate (non-signing) CA

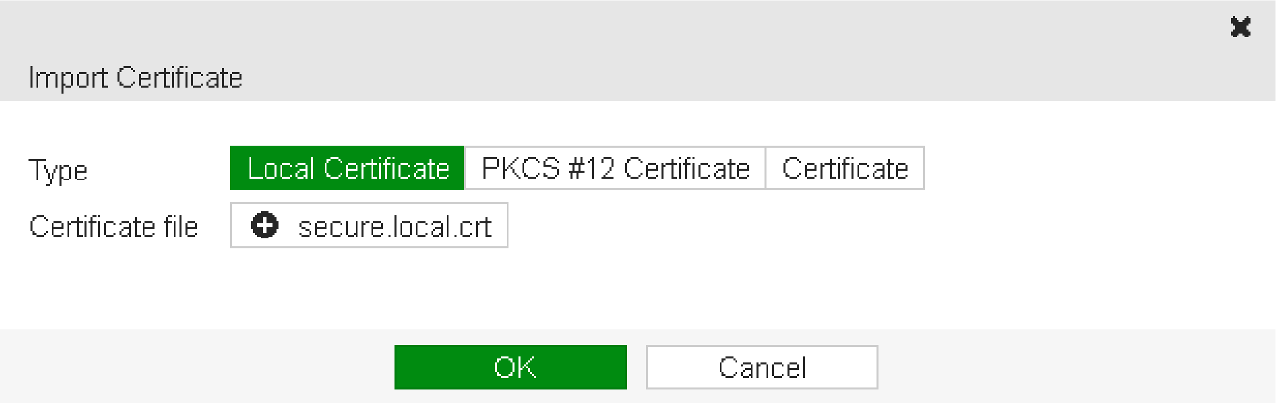
This will save a *.crt* file to your local drive.

secure.local.crt

Importing the signed certificate on the FortiGate

To import the signed certificate:

1. Back on the FortiGate, go to *System* > *Certificates*, and select *Import* > *Local Certificate*. Browse to the CRT file and select *OK*.

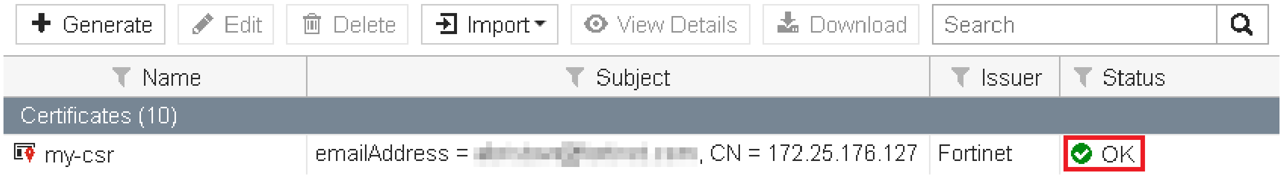


Import Certificate

Type: Local Certificate | PKCS #12 Certificate | Certificate

Certificate file: secure.local.crt

2. You should now see that the certificate has a *Status* of *OK*.

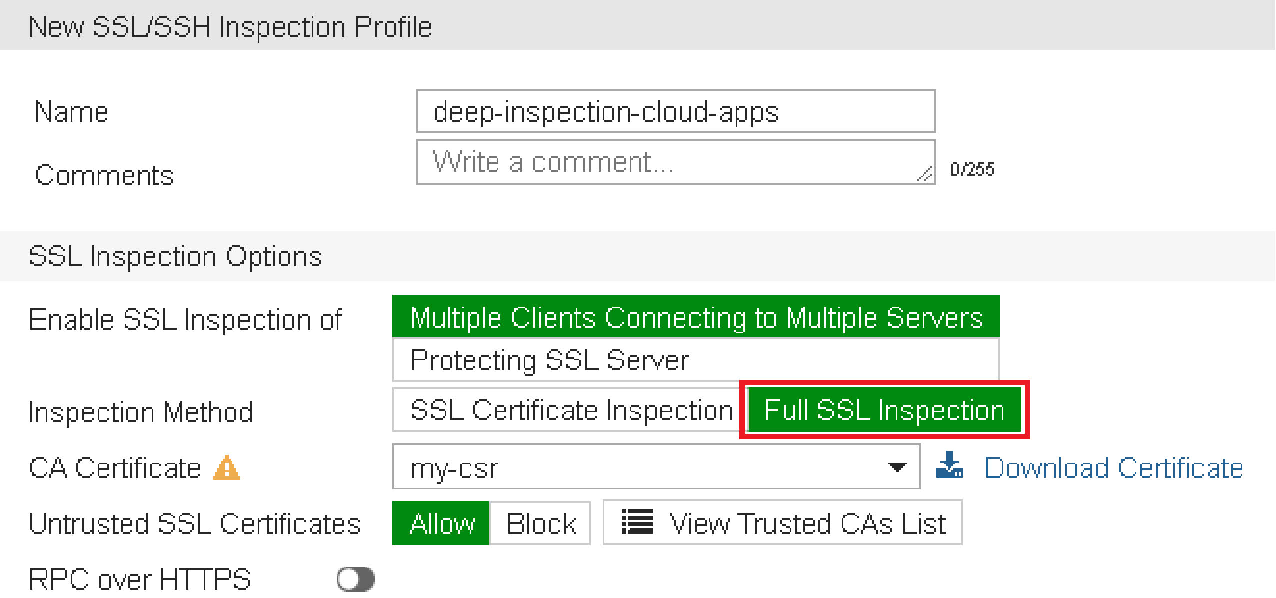


Name	Subject	Issuer	Status
Certificates (10)			
my-csr	emailAddress = [redacted], CN = 172.25.176.127	Fortinet	✓ OK

Configuring full SSL inspection

To configure full SSL inspection:

1. Go to *Security Profiles > SSL/SSH Inspection*, and create a new profile.
Enter a *Name*, select the certificate from the *CA Certificate* dropdown menu, and make sure *Inspection Method* is set to *Full SSL Inspection*.



New SSL/SSH Inspection Profile

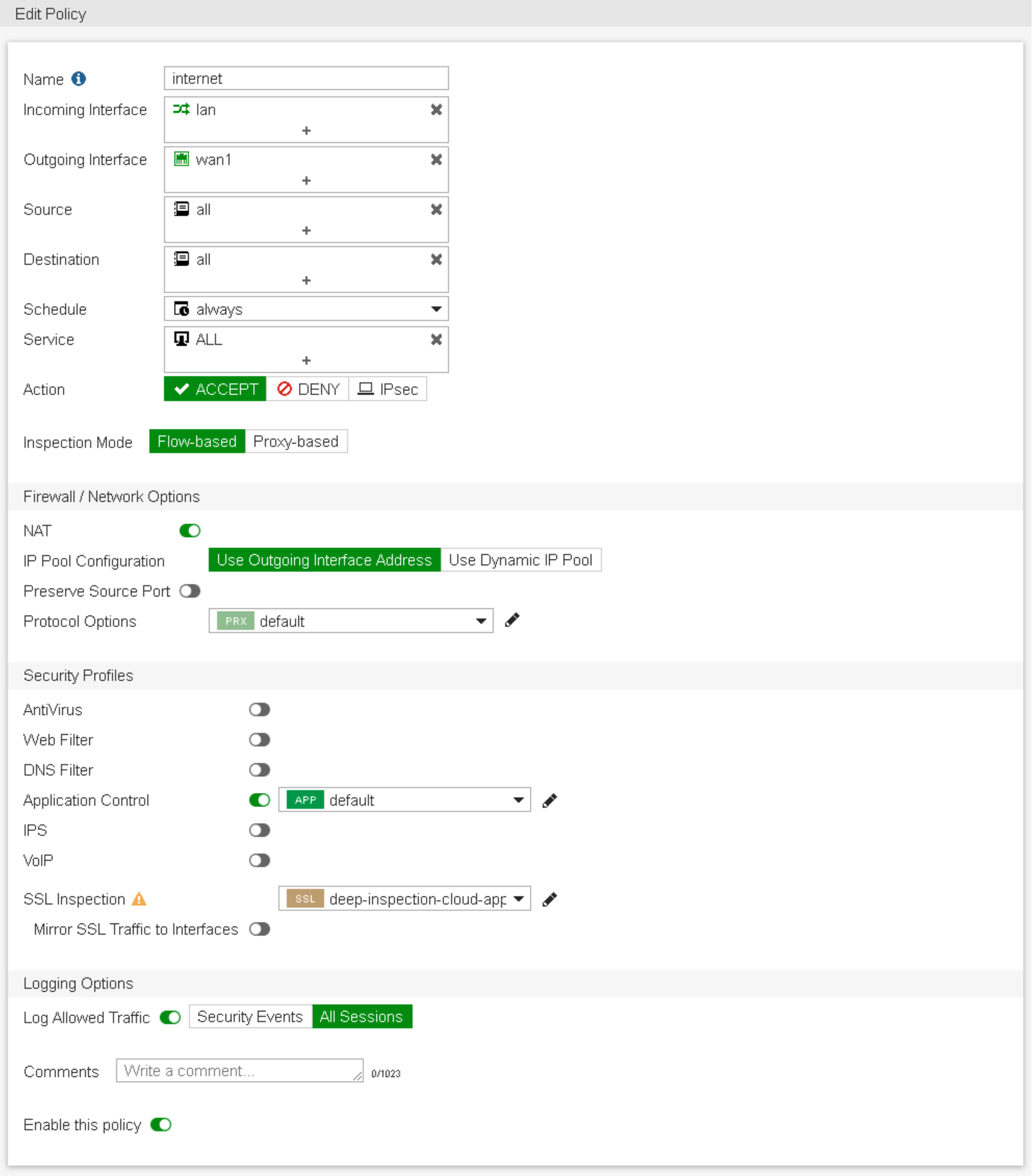
Name	deep-inspection-cloud-apps
Comments	Write a comment... 0/255

SSL Inspection Options

Enable SSL Inspection of	[✓ Multiple Clients Connecting to Multiple Servers] Protecting SSL Server
Inspection Method	SSL Certificate Inspection [✓ Full SSL Inspection]
CA Certificate ⚠	my-csr
Untrusted SSL Certificates	[✓ Allow] Block
RPC over HTTPS	○

2. Add the certificate to your web browser's list of trusted certificates. End users will likely see certificate warnings unless the certificate is installed in their browser.

3. Next go to *Policy & Objects > IPv4 Policy* and edit the policy that allows Internet access.
   Under *Security Profiles*, enable *SSL/SSH Inspection* and select the custom profile created earlier.
   Enable *Application Control* and set it to *default*.



Edit Policy

Name: internet
Incoming Interface: lan
Outgoing Interface: wan1
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY | IPsec
Inspection Mode: Flow-based | Proxy-based

Firewall / Network Options

NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PRX default

Security Profiles

AntiVirus: ○
Web Filter: ○
DNS Filter: ○
Application Control: ● APP default
IPS: ○
VoIP: ○
SSL Inspection ⚠: SSL deep-inspection-cloud-apr
Mirror SSL Traffic to Interfaces: ○

Logging Options

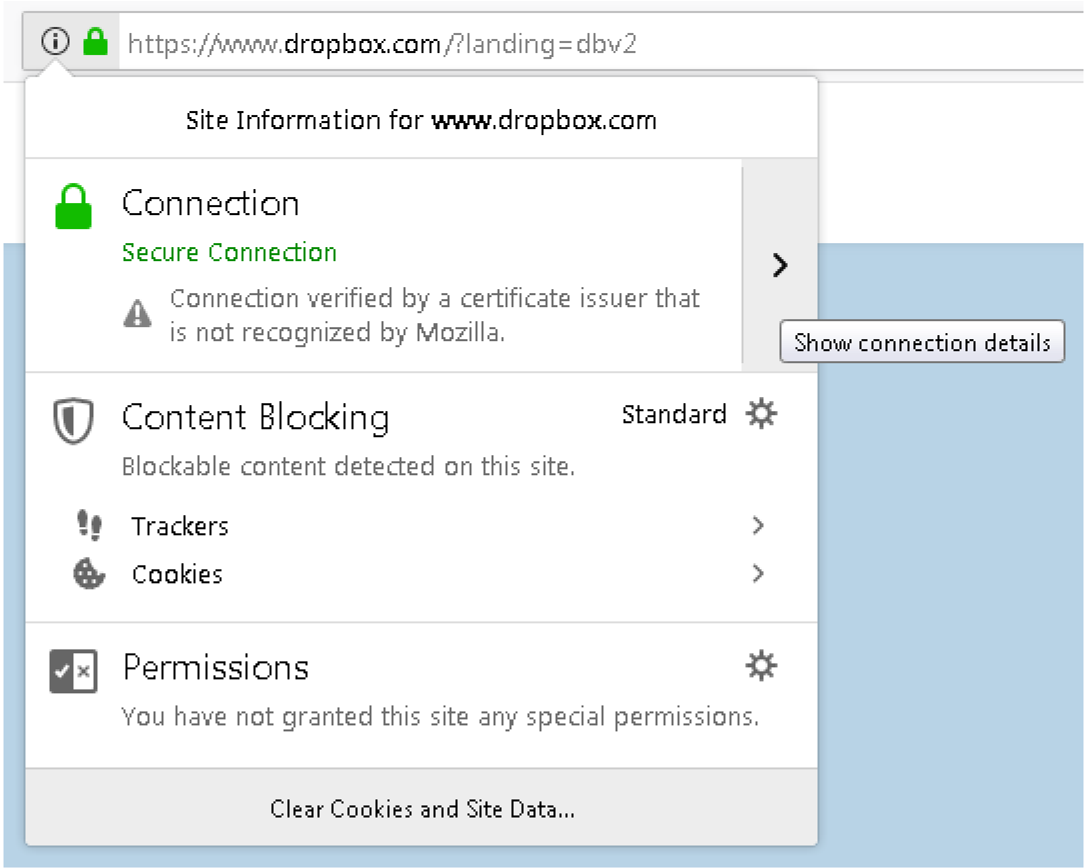
Log Allowed Traffic: ● Security Events | All Sessions

Comments: Write a comment... 0/1023

Enable this policy: ●

Results

1. To test the certificate, open your web browser and attempt to navigate to an HTTPS website (in the example, `https://www.dropbox.com`).
   Click on the lock icon next to the address bar and click *Show connection details*.



https://www.dropbox.com/?landing=dbv2

Site Information for www.dropbox.com

Connection

Secure Connection

Connection verified by a certificate issuer that is not recognized by Mozilla.

Show connection details

Content Blocking — Standard

Blockable content detected on this site.

Trackers

Cookies

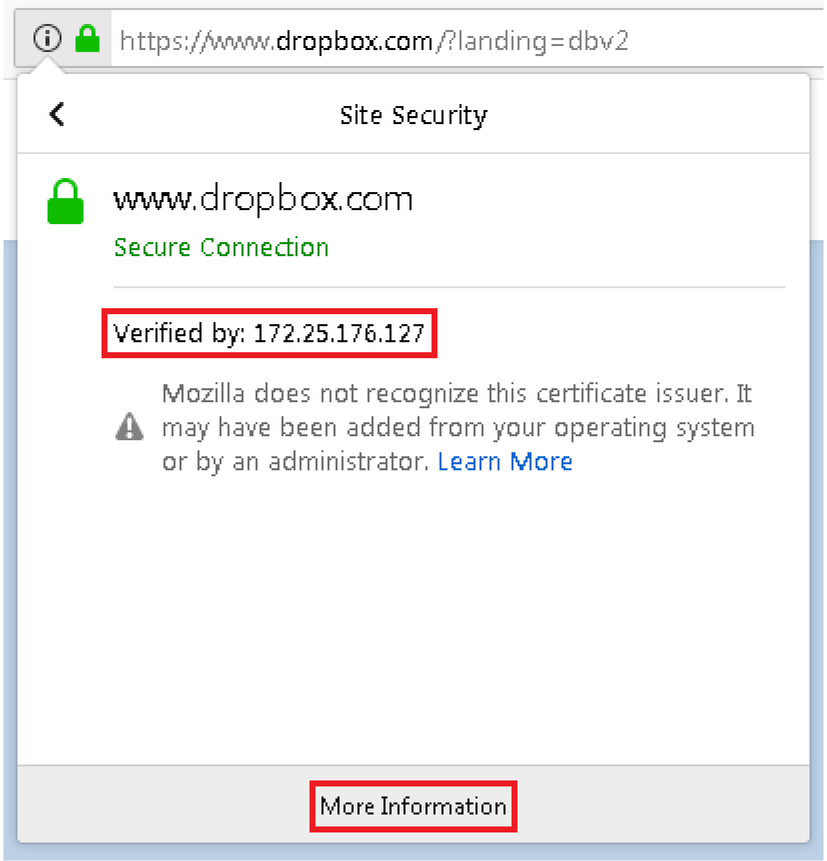
Permissions

You have not granted this site any special permissions.

Clear Cookies and Site Data...

2. You should now see that the certificate from the FortiGate (`172.25.176.127`) has signed and verified access to the site. As a result, no certificate errors will appear.

Optionally select *More Information*.



https://www.dropbox.com/?landing=dbv2

Site Security

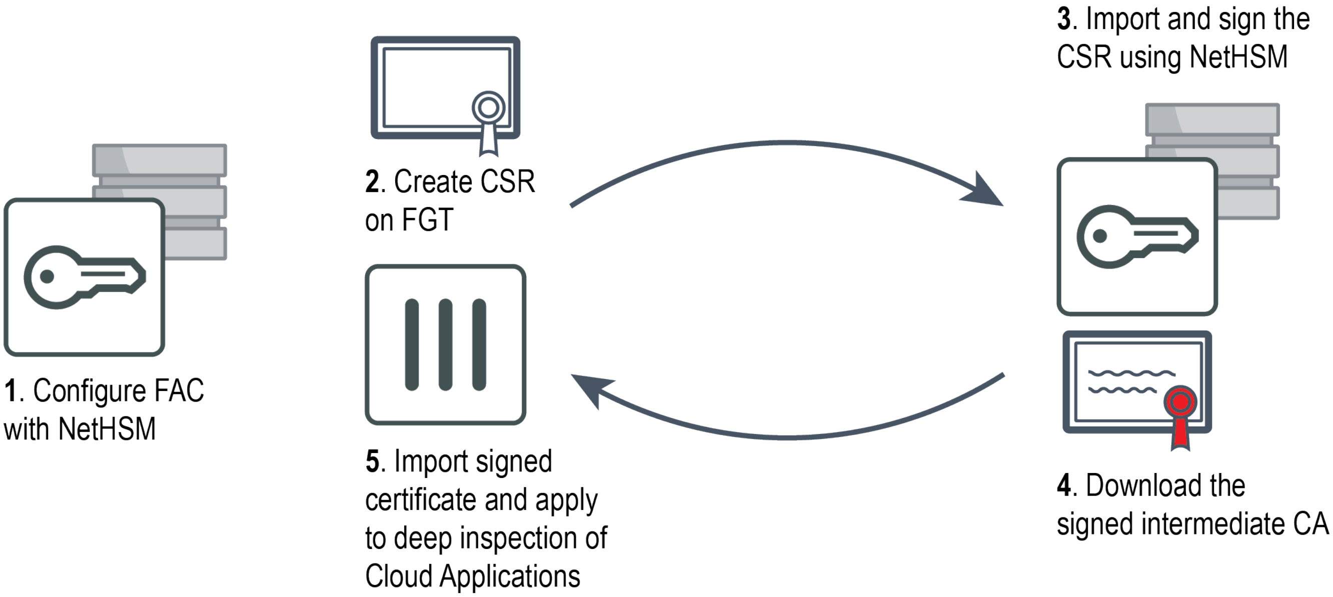
www.dropbox.com

Secure Connection

Verified by: 172.25.176.127

Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

FortiAuthenticator certificate with SSL inspection using an HSM


1. Configure FAC with NetHSM
2. Create CSR on FGT
3. Import and sign the CSR using NetHSM
4. Download the signed intermediate CA
5. Import signed certificate and apply to deep inspection of Cloud Applications

For this recipe, you will create a certificate on the FortiGate, have it signed on a FortiAuthenticator with a configured HSM server, and configure the FortiGate so that the certificate can be used for SSL deep inspection of HTTPS traffic. This example uses the Safenet Luna V7 HSM.

To set up the certificate with SSL inspection using an HSM:

1. Configuring the NetHSM profile on FortiAuthenticator on page 25
2. Creating a local CA certificate using an HSM server on page 26
3. Creating a CSR on the FortiGate on page 27
4. Creating an Intermediate CA on the FortiAuthenticator on page 28
5. Importing the signed certificate on the FortiGate on page 29
6. Configuring full SSL inspection on page 29
7. Results on page 32

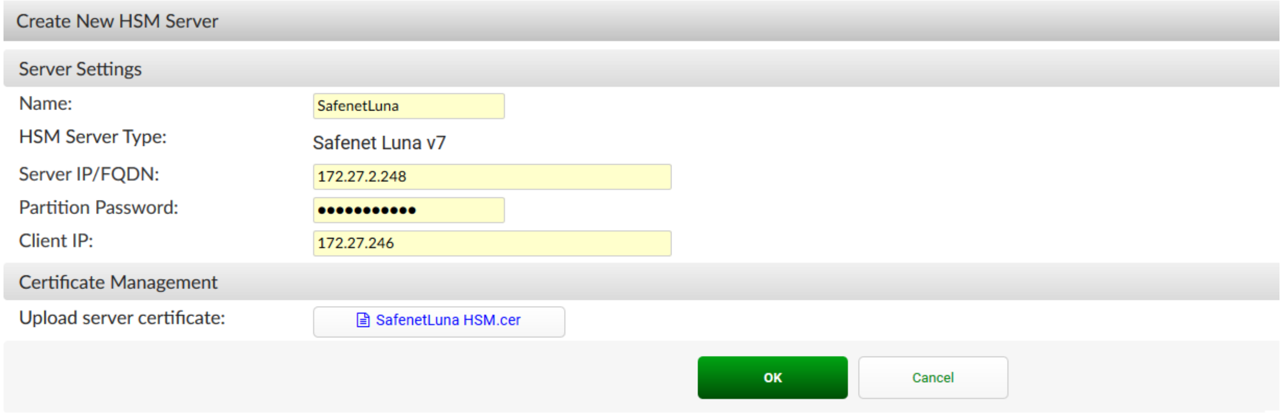
In order for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this recipe will not be trusted. For more information on how to do this, see Creating a local CA certificate using an HSM server on page 26 and FortiAuthenticator as a Certificate Authority.

As an example, you will also have *Application Control* with *Deep Inspection of Cloud Applications* enabled. This will apply inspection to HTTPS traffic. Note that you may use another security profile instead of *Application Control*.

Configuring the NetHSM profile on FortiAuthenticator

To configure a new the Safenet Luna HSM server:

1. In FortiAuthenticator, go to *System* > *Administration* > *NetHSMs*, and click *Create New*.
2. In the *Create New HSM Server* window, configure the following:



Create New HSM Server

Server Settings

Name: SafenetLuna

HSM Server Type: Safenet Luna v7

Server IP/FQDN: 172.27.2.248

Partition Password: ●●●●●●●●●●●

Client IP: 172.27.246

Certificate Management

Upload server certificate: SafenetLuna HSM.cer

Name	Enter a name for the HSM server.
Server IP/FQDN	Enter the IP address or FQDN of the HSM server to which the FortiAuthenticator will connect.
Partition Password	Enter the key partition password from the HSM server.
Client IP	Enter the address of the FortiAuthenticator interface that the HSM will see.
Upload server certificate	Click *Upload server certificate* to select the certificate from your HSM.

3. Click *OK* to complete the setup.

To authorize FortiAuthenticator as a Safenet Luna HSM client:

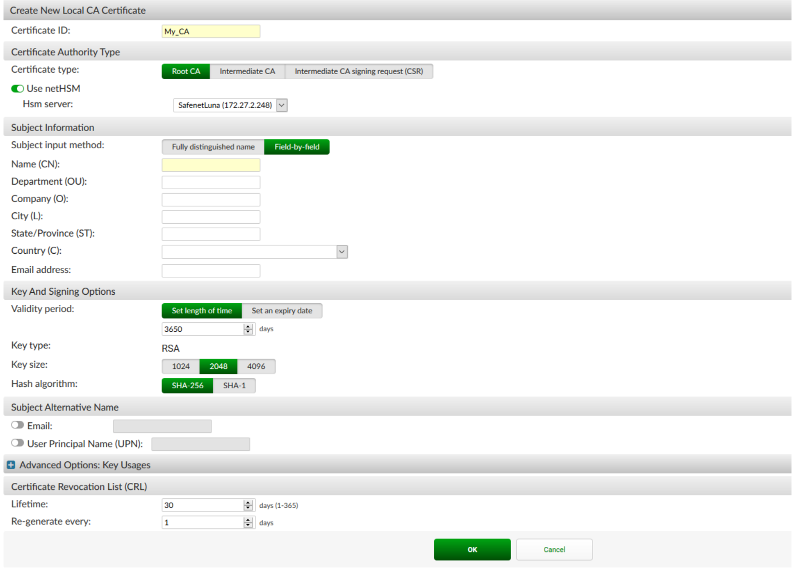
1. Make sure the FortiAuthenticator client certificate uses the `<FAC IP>.pem` naming convention. For example: `172.16.68.47.pem`
2. Upload the FortiAuthenticator client certificate to Safenet Luna HSM using SCP transfer.
   ```
   scp [certificate filename] admin@[HSM address]:
   ```
3. Use SSH to connect to the HSM, then register your FortiAuthenticator, and associate it with a partition.
   ```
   ssh -1 admin [HSM address]
   client register -c [client name] -ip [client address]
   client assignpartition -c [client name] -p [partition name]
   ```
4. Confirm the status of the NetHSM client. For example:
   ```
   client show -c my_fac
      ClientID: my_fac
      IPAddress: 172.16.68.47
      Partitions: my_partition
   ```

Creating a local CA certificate using an HSM server

Once you have configured the HSM server on FortiAuthenticator, you can create a local CA certificate using the HSM server to sign requests. For more information on setting up a certificate authority, see FortiAuthenticator as a Certificate Authority on page 8.

To create a new local CA certificate using HSM:

1. On FortiAuthenticator, go to *Certificate Management > Certificate Authorities > Local CAs*, and click *Create New*.



Create New Local CA Certificate

Certificate ID: My_CA

Certificate Authority Type

Certificate type: [✓ Root CA] Intermediate CA | Intermediate CA signing request (CSR)

● Use netHSM

Hsm server: SafenetLuna (172.27.2.248)

Subject Information

Subject input method: Fully distinguished name | [✓ Field-by-field]

Name (CN):

Department (OU):

Company (O):

City (L):

State/Province (ST):

Country (C):

Email address:

Key And Signing Options

Validity period: [✓ Set length of time] Set an expiry date

3650 days

Key type: RSA

Key size: 1024 | [✓ 2048] | 4096

Hash algorithm: [✓ SHA-256] SHA-1

Subject Alternative Name

○ Email:

○ User Principal Name (UPN):

Advanced Options: Key Usages

Certificate Revocation List (CRL)

Lifetime: 30 days (1-365)

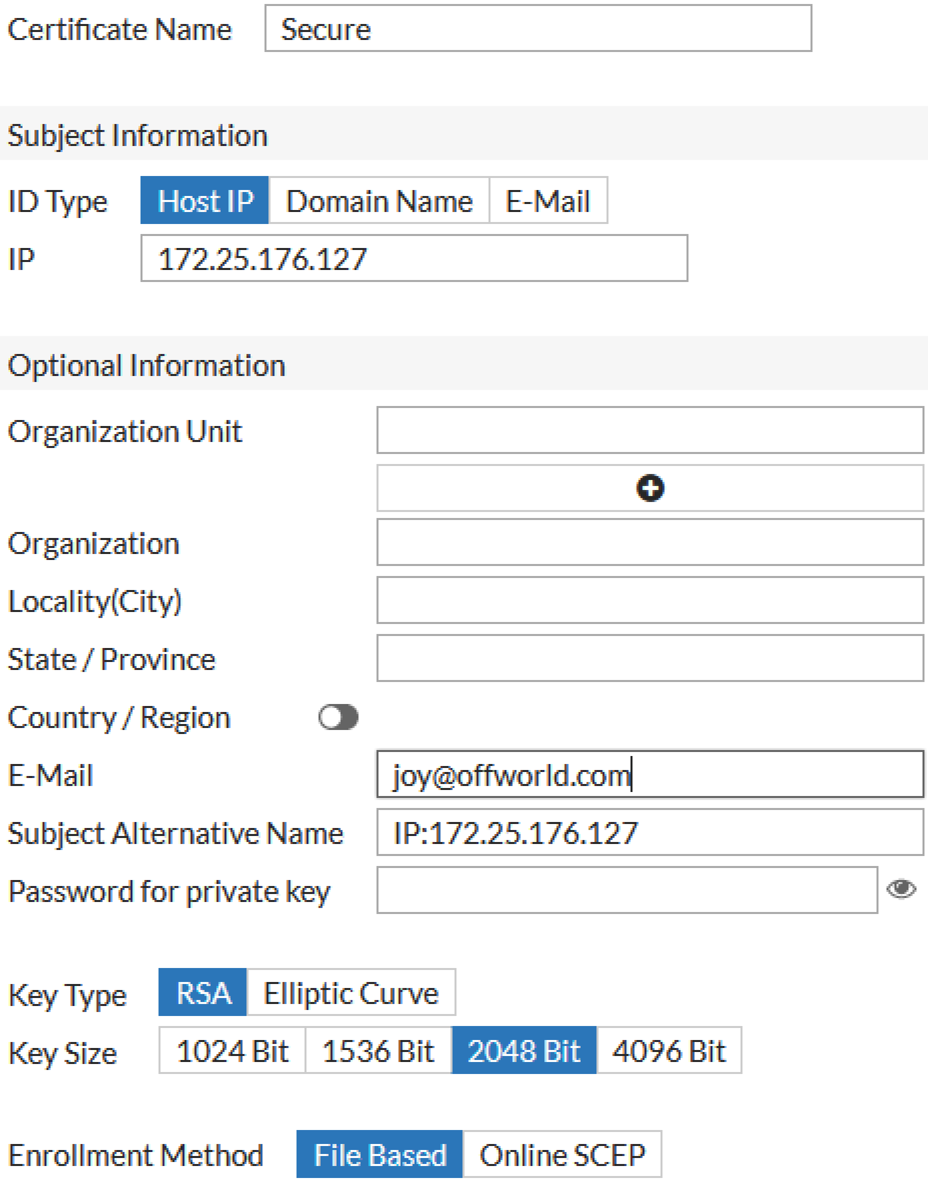
Re-generate every: 1 days

2. Enter a name for the CA certificate, for example *My_CA*.
3. Select *Root CA* as the *Certificate type*.
4. Enable *Use NetHSM*, and choose an HSM server from the dropdown menu.
5. Configure the remaining settings as desired, and click *OK* to save your changes.
   Once your CA certificate has been created, it can be exported and installed on your network. For more information on setting up a certificate authority, see FortiAuthenticator as a Certificate Authority on page 8.

Creating a CSR on the FortiGate

To create a CSR:

1. On the FortiGate, go to *System* > *Certificates* and select *Generate* to create a new certificate signing request (CSR). Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.
   The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



Certificate Name: Secure

Subject Information

ID Type: [✓ Host IP] Domain Name E-Mail

IP: 172.25.176.127

Optional Information

Organization Unit:

Organization:

Locality(City):

State / Province:

Country / Region: ○

E-Mail: joy@offworld.com

Subject Alternative Name: IP:172.25.176.127

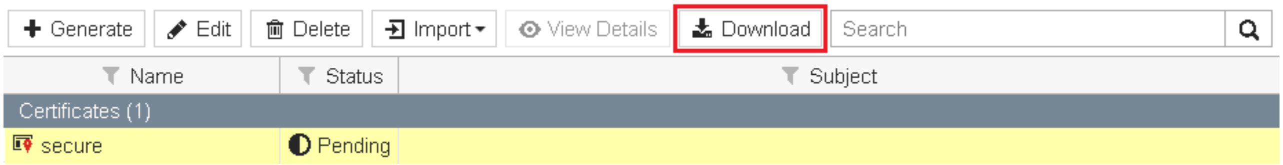
Password for private key:

Key Type: [✓ RSA] Elliptic Curve

Key Size: 1024 Bit 1536 Bit [✓ 2048 Bit] 4096 Bit

Enrollment Method: [✓ File Based] Online SCEP

2. Once created, the certificate will show a *Status* of *Pending*. Highlight the certificate and select *Download*.



Name	Status	Subject
Certificates (1)		
secure	Pending	

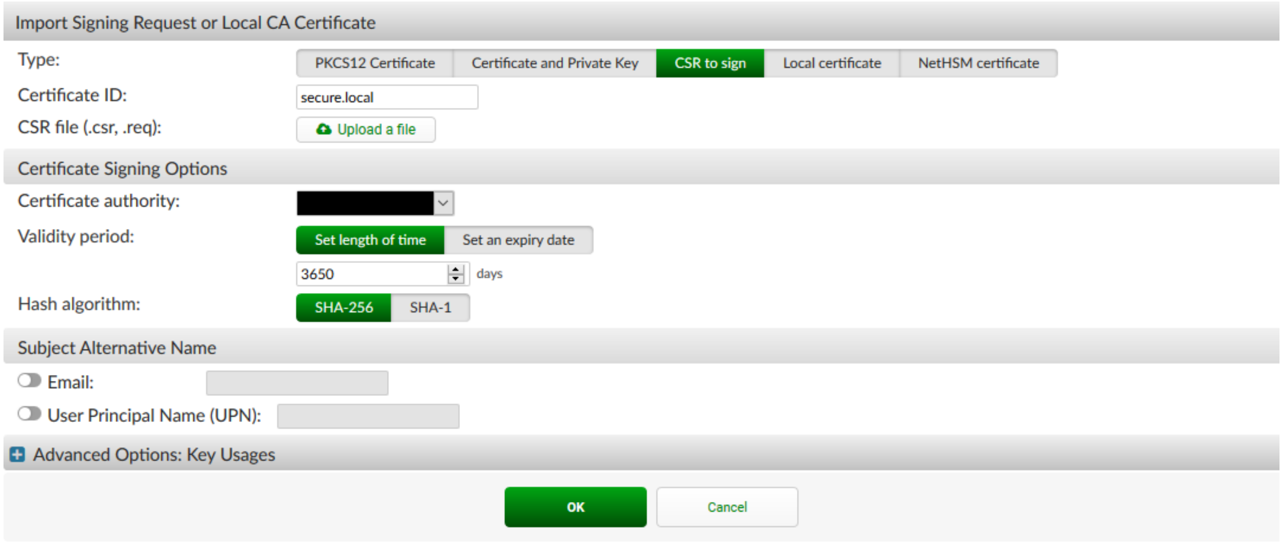
This will save a **.csr** file to your local drive.

secure.csr

Creating an Intermediate CA on the FortiAuthenticator

To create an Intermediate CA:

1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Import*. Set *Type* to *CSR to sign*, enter a *Certificate ID*, and import the CSR file.
2. Select the *Certificate authority* configured with the HSM from the dropdown menu, and set the *Hash algorithm* to *SHA-256*. Click *OK*.


Import Signing Request or Local CA Certificate

Type: PKCS12 Certificate | Certificate and Private Key | [✓ CSR to sign] | Local certificate | NetHSM certificate

Certificate ID: secure.local

CSR file (.csr, .req): Upload a file

Certificate Signing Options

Certificate authority: [redacted]

Validity period: [✓ Set length of time] | Set an expiry date

3650 days

Hash algorithm: [✓ SHA-256] | SHA-1

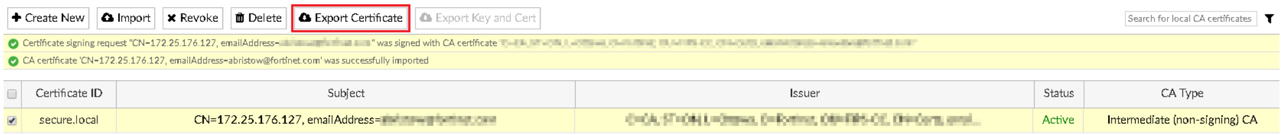
Subject Alternative Name

○ Email:

○ User Principal Name (UPN):

Advanced Options: Key Usages

3. Once imported, you should see that the certificate has been signed by the FortiAuthenticator, showing a *Status* of *Active*, and with the *CA Type* of *Intermediate (non-signing) CA*.
4. Highlight the certificate and select *Export Certificate*.



Certificate signing request "CN=172.25.176.127, emailAddress=[redacted]" was signed with CA certificate '[redacted]'

CA certificate 'CN=172.25.176.127, emailAddress=abristow@fortinet.com' was successfully imported

☐	Certificate ID	Subject	Issuer	Status	CA Type
☑	secure.local	CN=172.25.176.127, emailAddress=[redacted]	[redacted]	Active	Intermediate (non-signing) CA

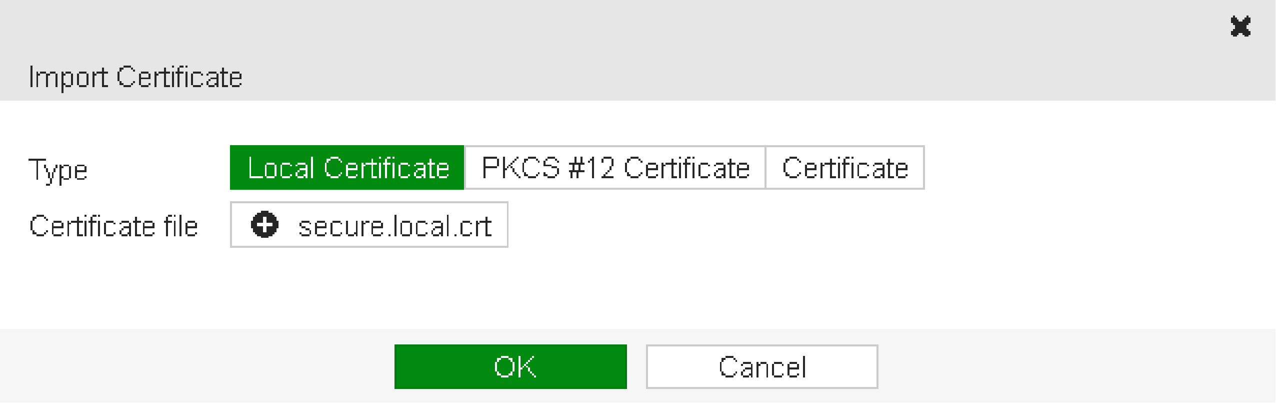
This will save a *.crt* file to your local drive.

secure.local.crt

Importing the signed certificate on the FortiGate

To import the signed certificate:

1. Back on the FortiGate, go to *System* > *Certificates* and select *Import* > *Local Certificate*.
   Browse to the *.crt* file, and select *OK*.

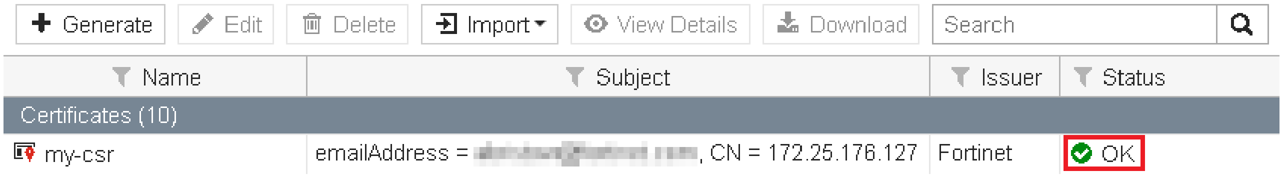


Import Certificate

Type: Local Certificate | PKCS #12 Certificate | Certificate

Certificate file: secure.local.crt

2. You should now see that the certificate has a *Status* of *OK*.

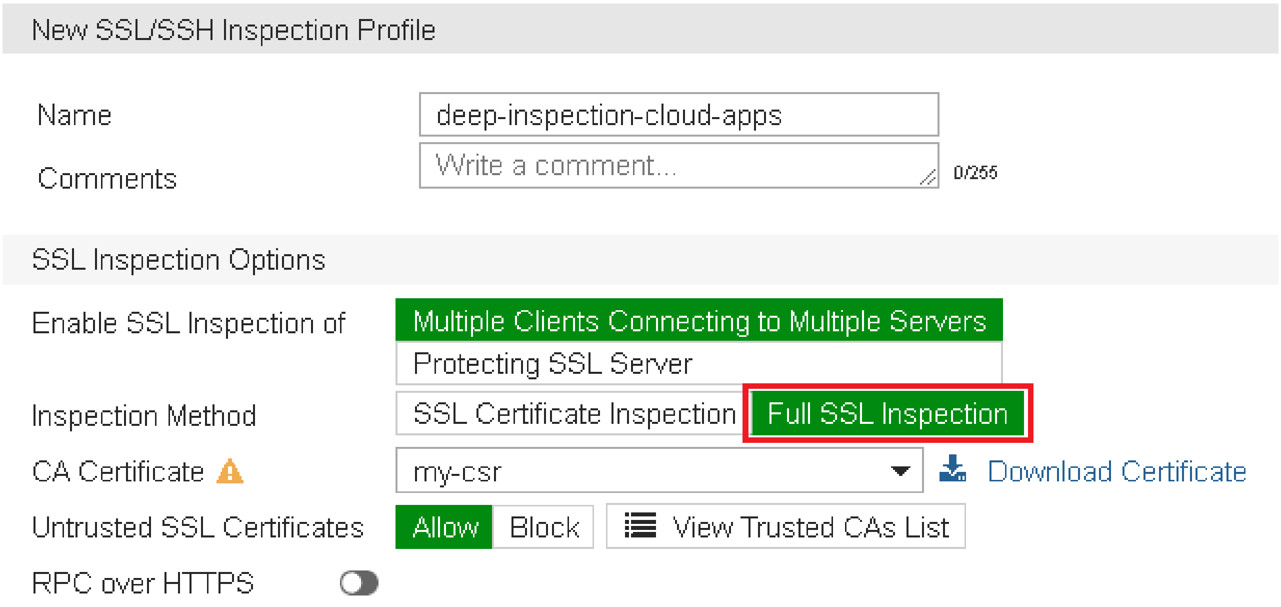


Name	Subject	Issuer	Status
Certificates (10)			
my-csr	emailAddress = [redacted], CN = 172.25.176.127	Fortinet	✓ OK

Configuring full SSL inspection

To configure full SSL inspection:

1. On the FortiGate, go to *Security Profiles* > *SSL/SSH Inspection*, and create a new profile.
   Enter a *Name*, select the certificate from the *CA Certificate* dropdown menu, and make sure *Inspection Method* is set to *Full SSL Inspection*.



New SSL/SSH Inspection Profile

Name: deep-inspection-cloud-apps

Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL Inspection of: [✓ Multiple Clients Connecting to Multiple Servers] Protecting SSL Server

Inspection Method: SSL Certificate Inspection [✓ Full SSL Inspection]

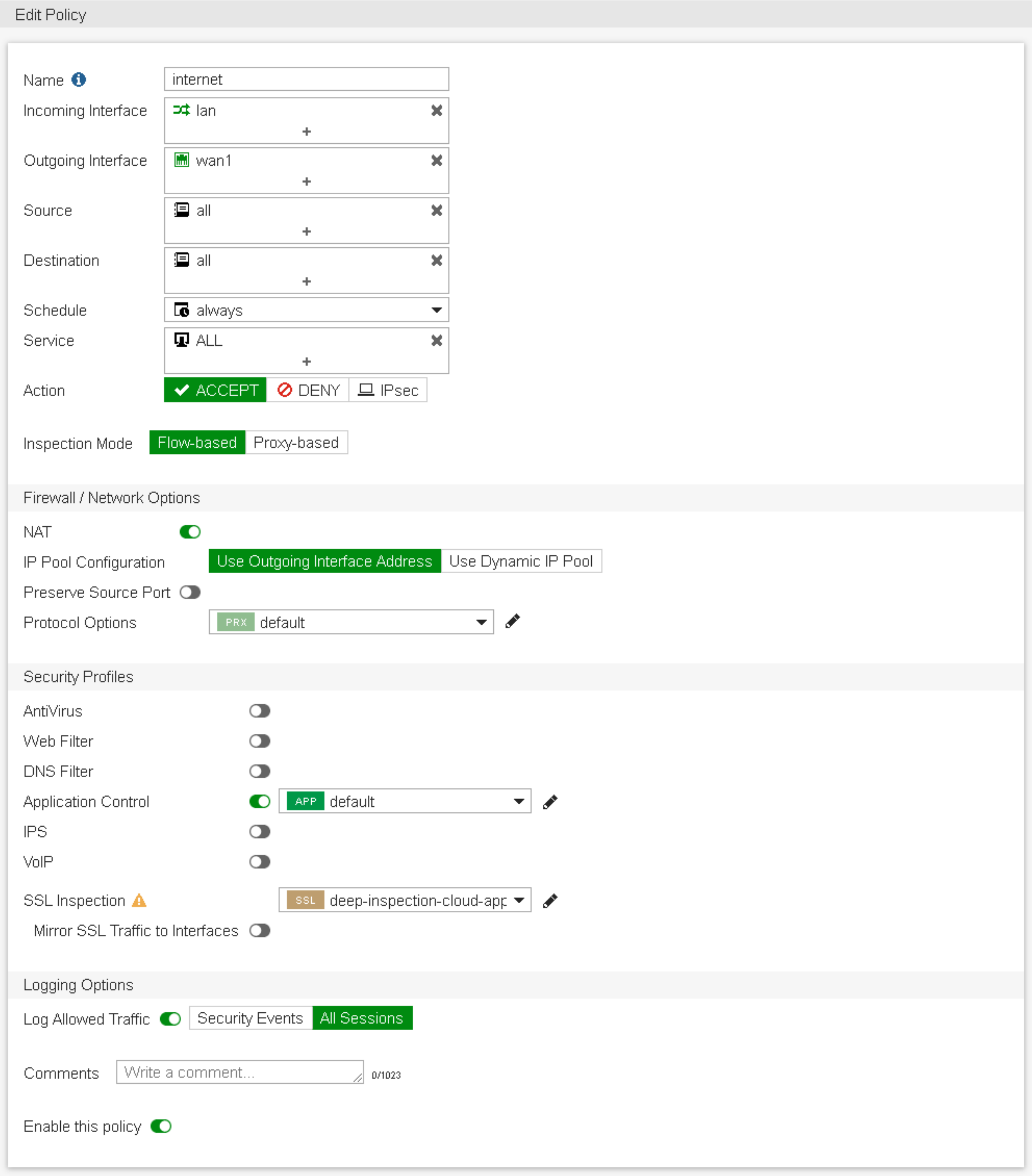
CA Certificate ⚠: my-csr Download Certificate

Untrusted SSL Certificates: [✓ Allow] Block View Trusted CAs List

RPC over HTTPS ○

2. Add the certificate to your web browser's list of trusted certificates. End users will likely see certificate warnings unless the certificate is installed in their browser.

3. Next go to *Policy & Objects* > *IPv4 Policy* and edit the policy that allows Internet access.



Edit Policy

Name	internet
Incoming Interface	lan
Outgoing Interface	wan1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY IPsec
Inspection Mode	[✓ Flow-based] Proxy-based

Firewall / Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PRX default

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	● APP default
IPS	○
VoIP	○
SSL Inspection ⚠	SSL deep-inspection-cloud-apr
Mirror SSL Traffic to Interfaces	○

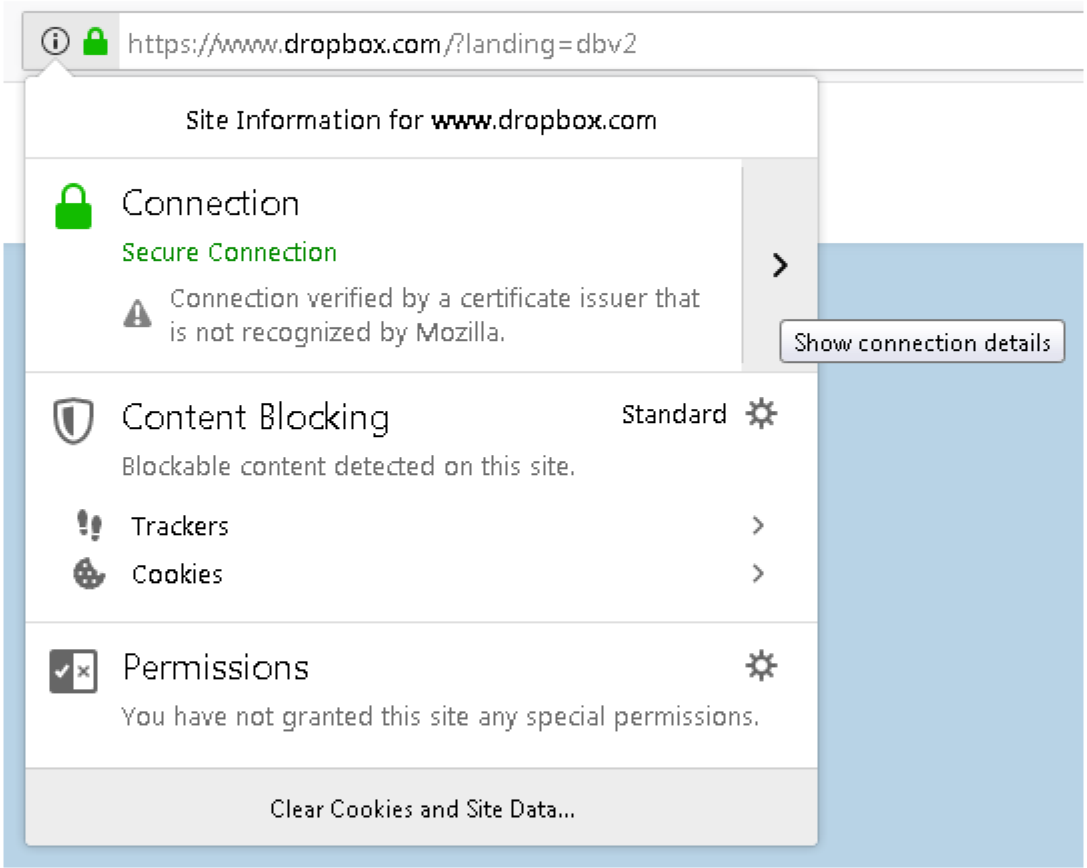
Logging Options

Log Allowed Traffic	● Security Events [✓ All Sessions]
Comments	Write a comment... 0/1023
Enable this policy	●

4. Under *Security Profiles*, enable *SSL/SSH Inspection* and select the custom profile created earlier.
5. Enable *Application Control* and set it to *default*.

Results

1. To test the certificate, open your web browser and attempt to navigate to an HTTPS website (in the example, `https://www.dropbox.com`).
   Click on the lock icon next to the address bar, and click *Show connection details*.



https://www.dropbox.com/?landing=dbv2

Site Information for www.dropbox.com

Connection

Secure Connection

Connection verified by a certificate issuer that is not recognized by Mozilla.

Content Blocking

Standard

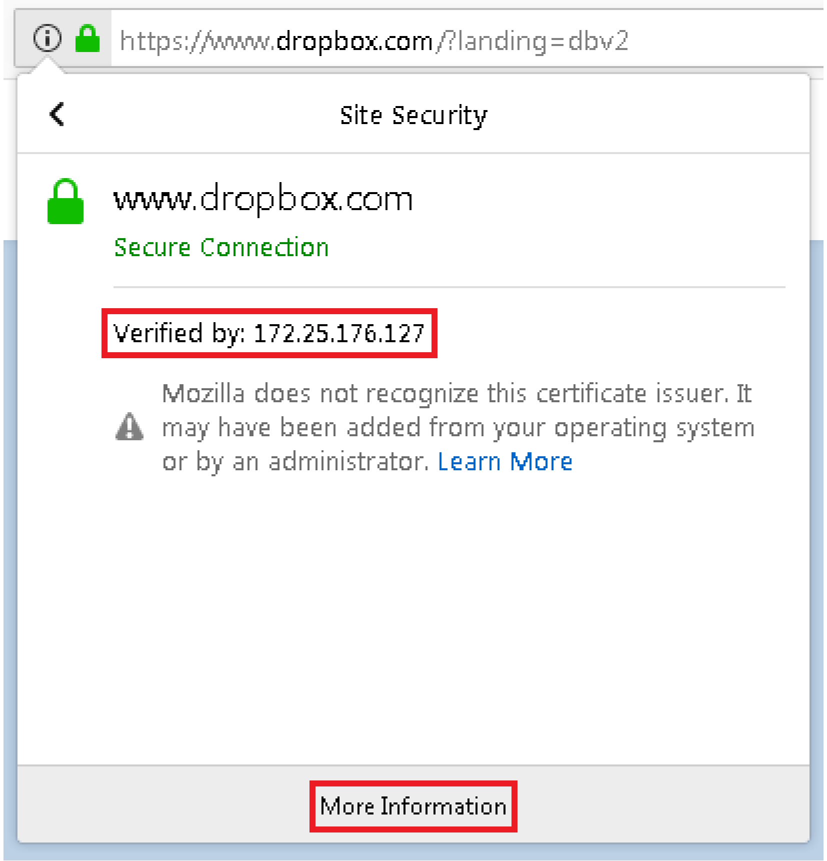
Blockable content detected on this site.

Permissions

You have not granted this site any special permissions.

2. You should now see that the certificate from the FortiGate has signed and verified access to the site. As a result, no certificate errors will appear.

Optionally select *More Information*.



https://www.dropbox.com/?landing=dbv2

Site Security

www.dropbox.com

Secure Connection

Verified by: 172.25.176.127

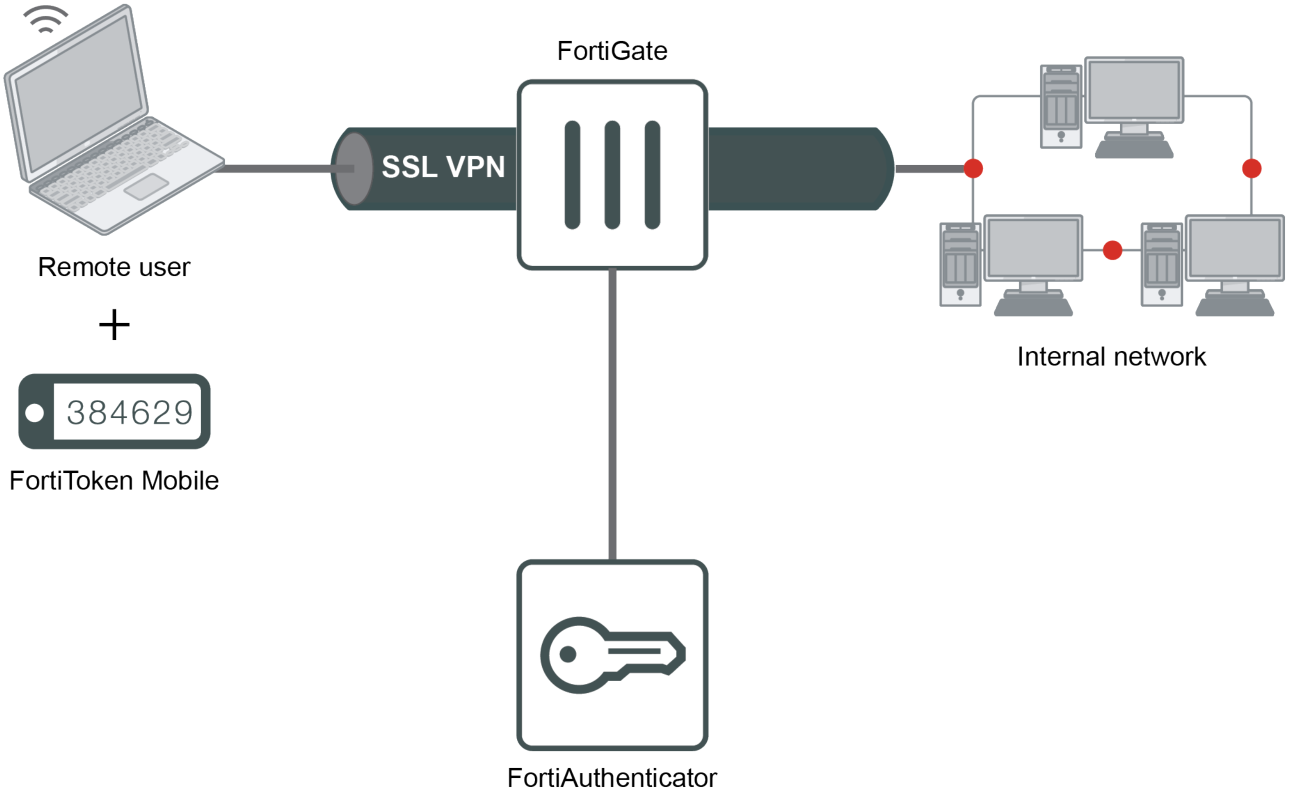
Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

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

Before push notifications can be enabled, a *Public IP/FQDN for FortiToken Mobile* must be configured in *System > Administration > System Access*.

If the FortiAuthenticator is behind a firewall, the public IP/FQDN will be an IP/port forwarding rule directed to one of the FortiAuthenticator interfaces.

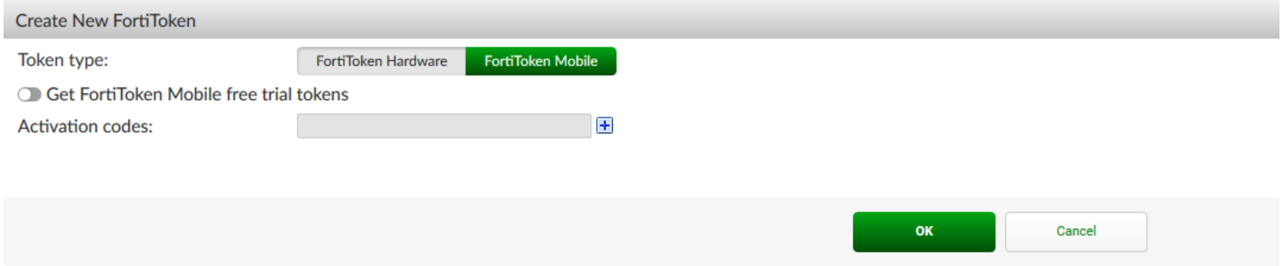
The interface that receives the approve/deny FTM push responses must have the *FortiToken Mobile API* service enabled.

If FortiAuthenticator is not accessible to the Internet, you must create a VIP and policy on FortiGate in order for mobile push to work. The VIP must point from an external port to FortiAuthenticator at port 443.

Once configured, you can add your FortiToken.

To add a FortiToken:

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

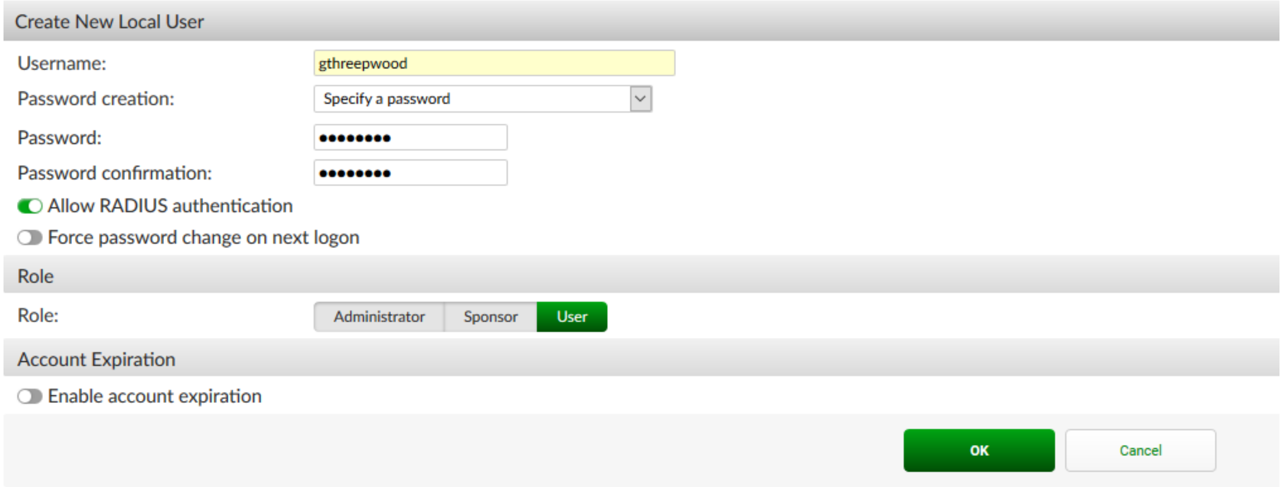
Activation codes:

Adding the user to the FortiAuthenticator

To add a user to 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

Username:	gthreepwood
Password creation:	Specify a password
Password:	••••••••
Password confirmation:	••••••••

● Allow RADIUS authentication

○ Force password change on next logon

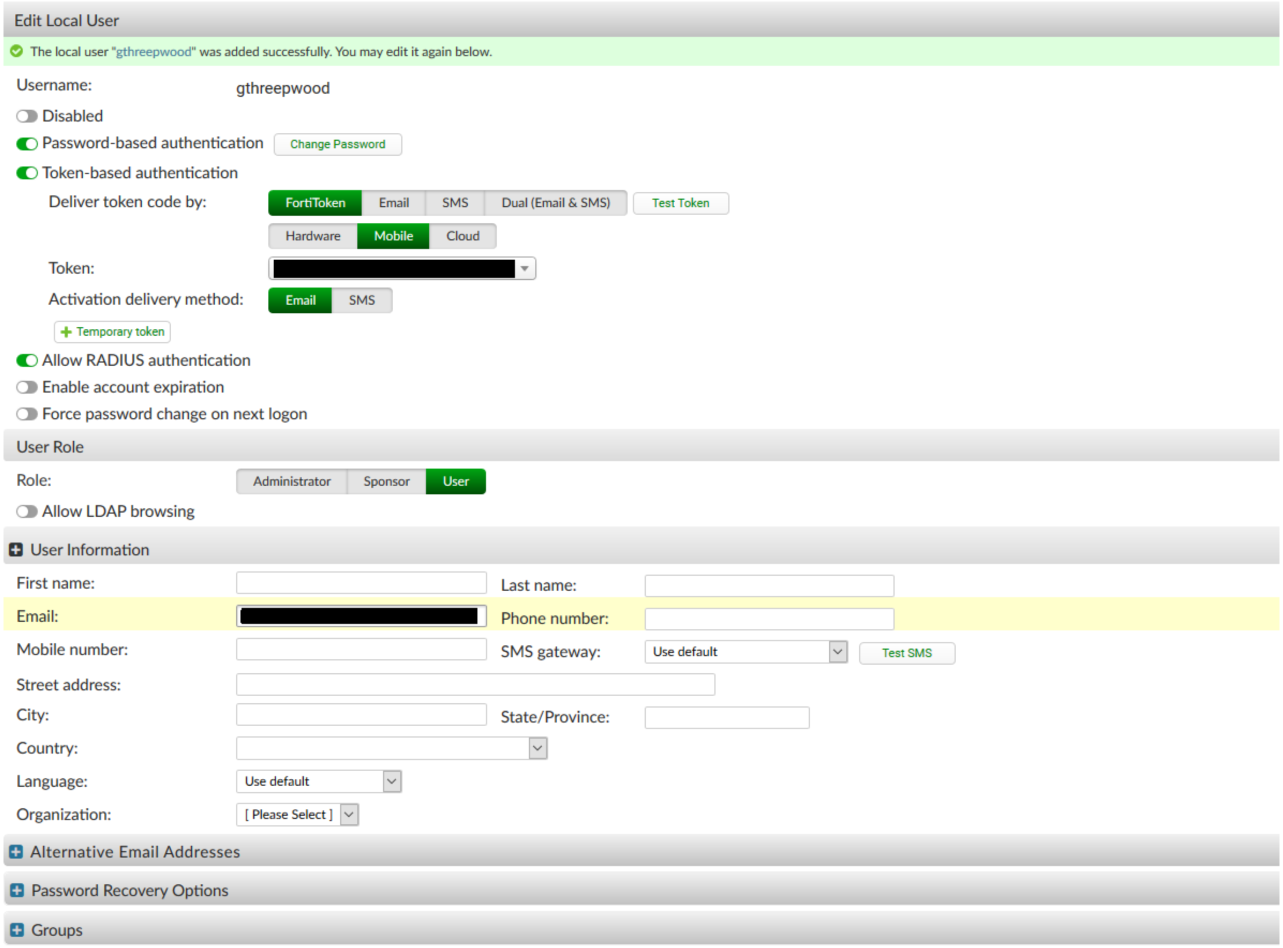
Role

Role: Administrator | Sponsor | [✓ User]

Account Expiration

○ 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.



Edit Local User

The local user "gthreepwood" was added successfully. You may edit it again below.

Username: gthreepwood

○ Disabled

● Password-based authentication

● Token-based authentication

Deliver token code by: [✓ FortiToken] Email SMS Dual (Email & SMS)

[✓ Mobile] (Hardware, Mobile, Cloud)

Token: [redacted]

Activation delivery method: [✓ Email] SMS

● Allow RADIUS authentication

○ Enable account expiration

○ Force password change on next logon

User Role

Role: Administrator Sponsor [✓ User]

○ Allow LDAP browsing

User Information

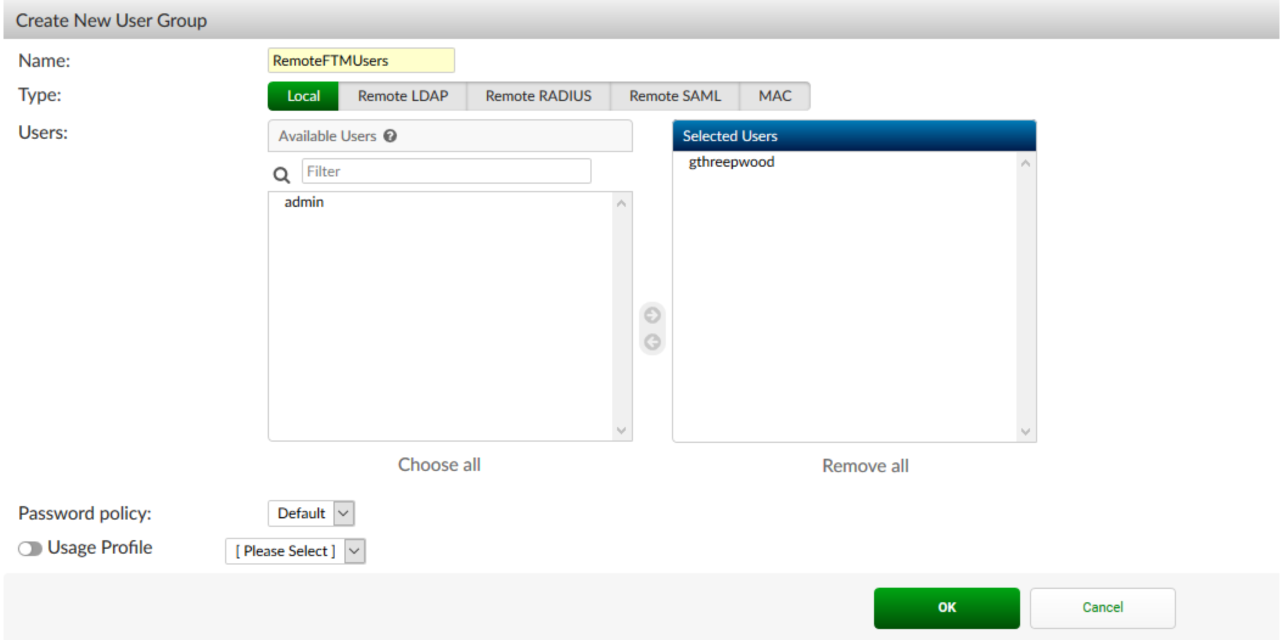
Email: [redacted]

SMS gateway: Use default

Language: Use default

Organization: [Please Select]

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 Remote SAML MAC

Users:

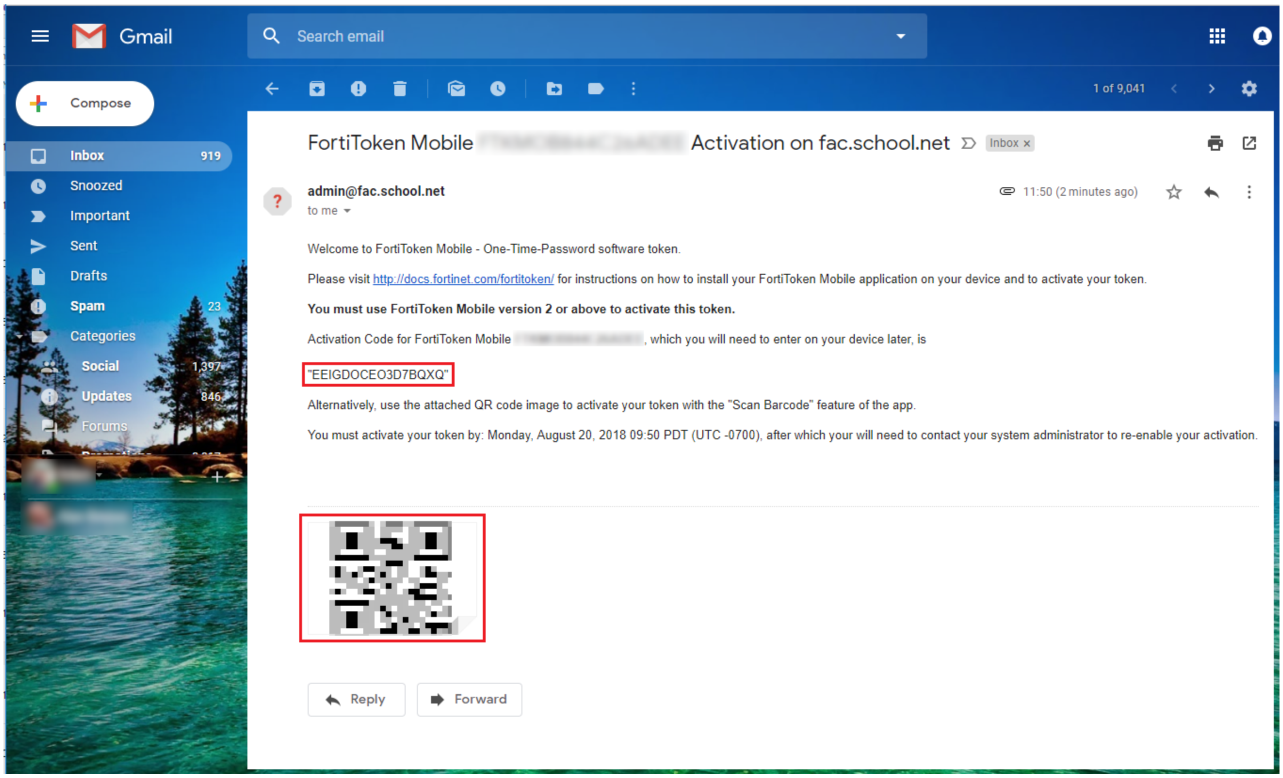
Available Users: admin

Selected Users: gthreepwood

Password policy: Default

○ Usage Profile [Please Select]

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



FortiToken Mobile [redacted] Activation on fac.school.net

admin@fac.school.net
to me

11:50 (2 minutes ago)

Welcome to FortiToken Mobile - One-Time-Password software token.

Please visit http://docs.fortinet.com/fortitoken/ for instructions on how to install your FortiToken Mobile application on your device and to activate your token.

You must use FortiToken Mobile version 2 or above to activate this token.

Activation Code for FortiToken Mobile [redacted], which you will need to enter on your device later, is

"EEIGDOCEO3D7BQXQ"

Alternatively, use the attached QR code image to activate your token with the "Scan Barcode" feature of the app.

You must activate your token by: Monday, August 20, 2018 09:50 PDT (UTC -0700), after which your will need to contact your system administrator to re-enable your activation.

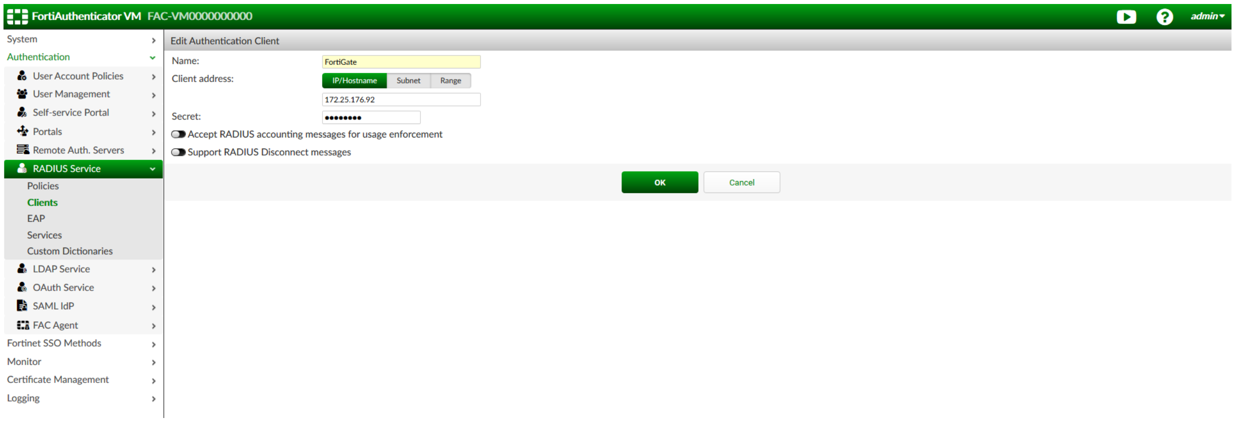
For more information, see the FortiToken Mobile user instructions.

Creating the RADIUS client and policy on the FortiAuthenticator

To create the RADIUS client:

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. Click *OK*.



Edit Authentication Client

Name: FortiGate

Client address: IP/Hostname | Subnet | Range

172.25.176.92

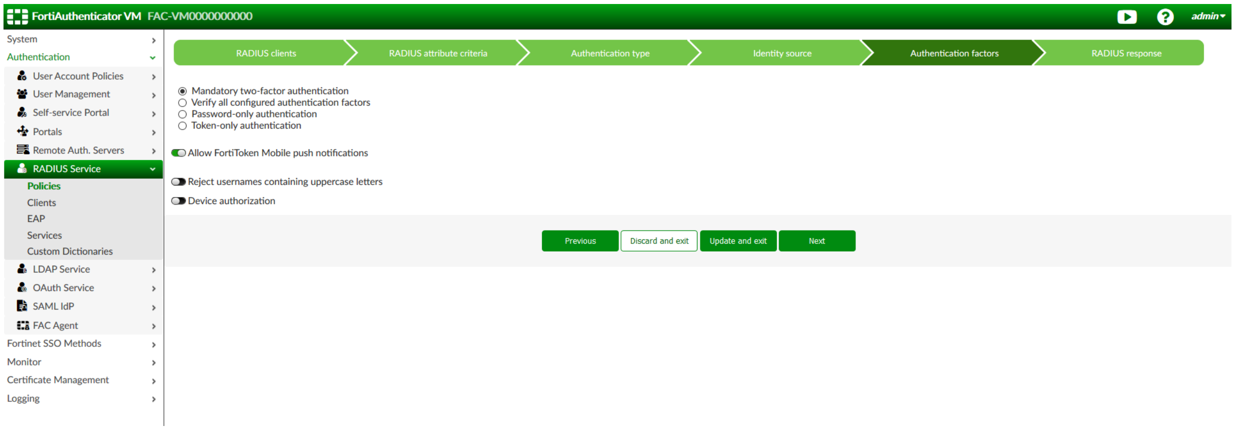
Secret: ••••••••

Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Optionally, configure RADIUS attribute criteria.
4. Choose *Password/OTP* authentication as the authentication type.
5. Choose a username format (in this example: `username@realm`), and select the *Local* realm.
6. Set the authentication method to *Mandatory two-factor authentication*, and enable the *Allow FortiToken Mobile push notifications* option.
7. Click *Save and Exit*.



● Mandatory two-factor authentication
○ Verify all configured authentication factors
○ Password-only authentication
○ Token-only authentication

Allow FortiToken Mobile push notifications

Reject usernames containing uppercase letters

Device authorization

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

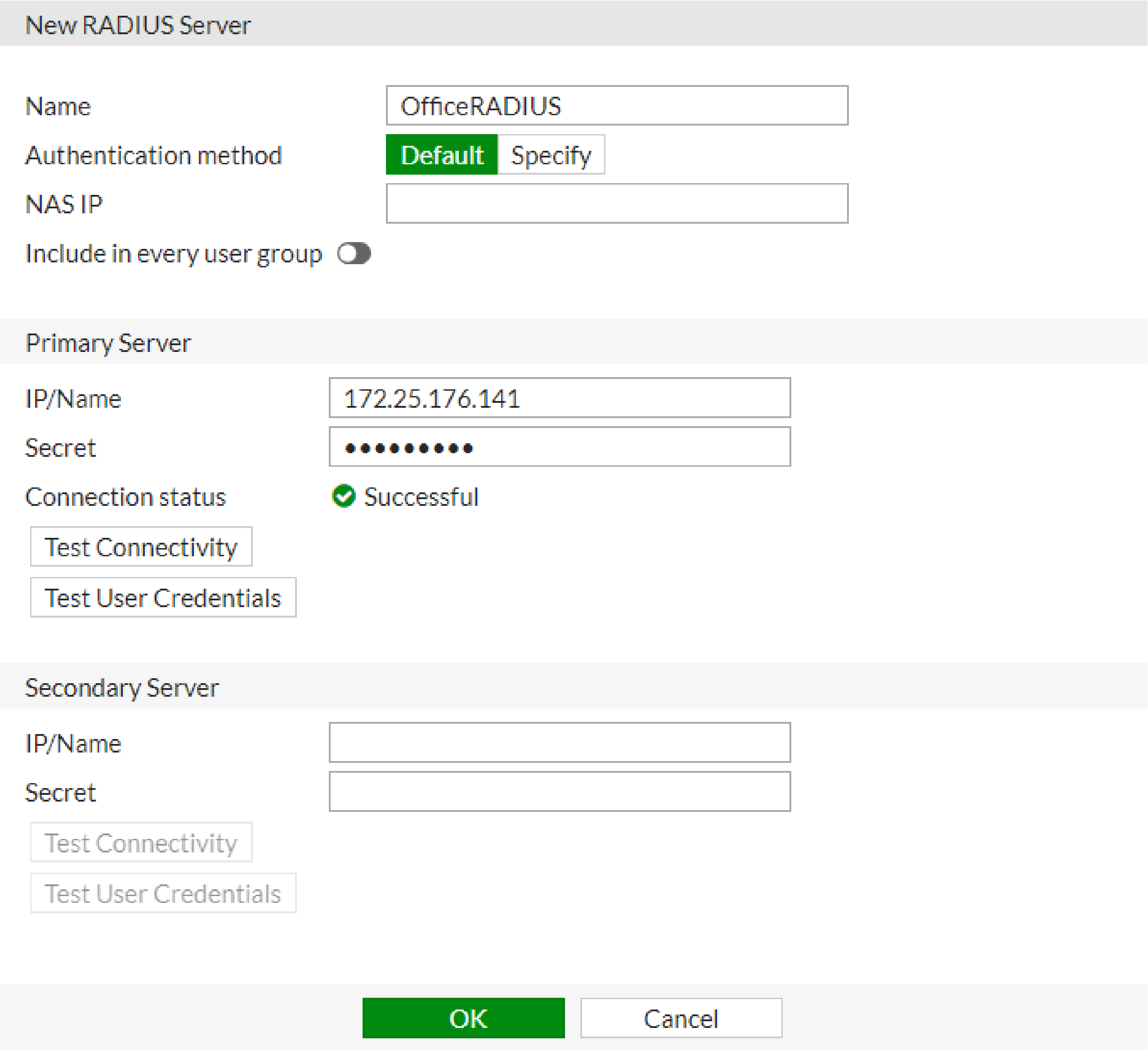
Connecting the FortiGate to the RADIUS server

To connect 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	○

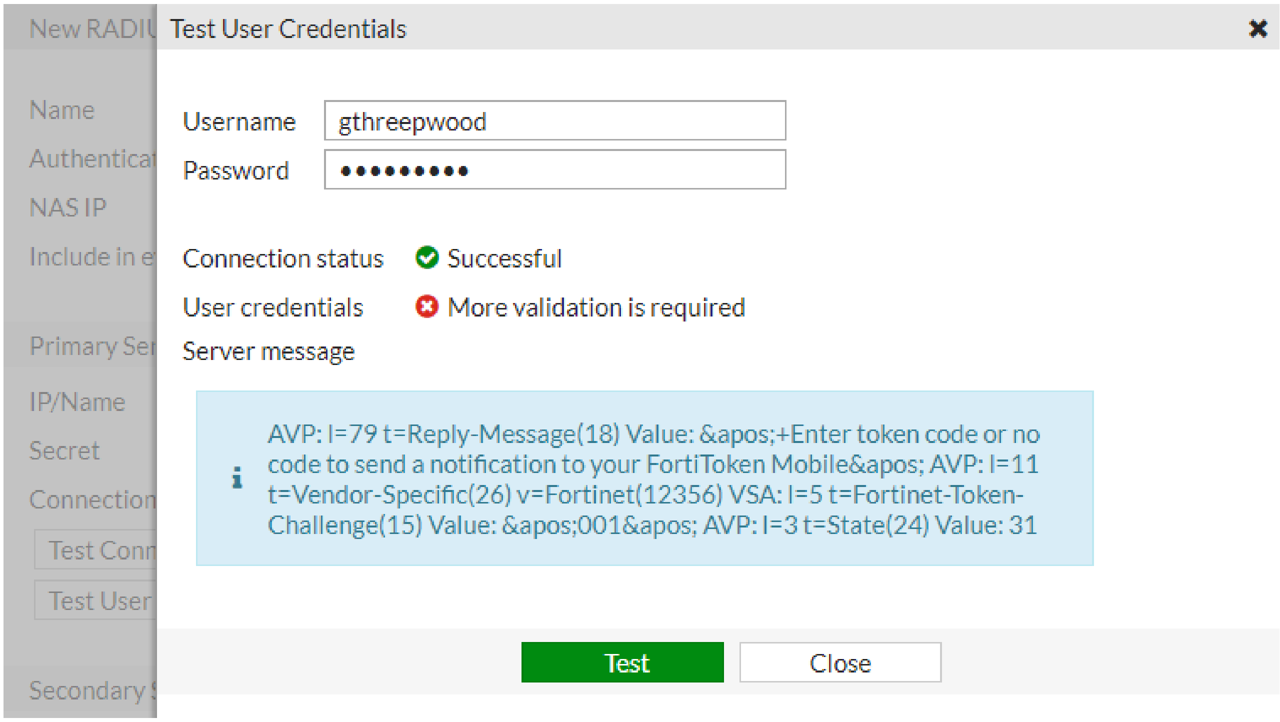
Primary Server

IP/Name	172.25.176.141
Secret	••••••••••
Connection status	✓ Successful

Secondary Server

IP/Name	
Secret	

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



Username: gthreepwood

Password: •••••••••

Connection status: ✓ Successful

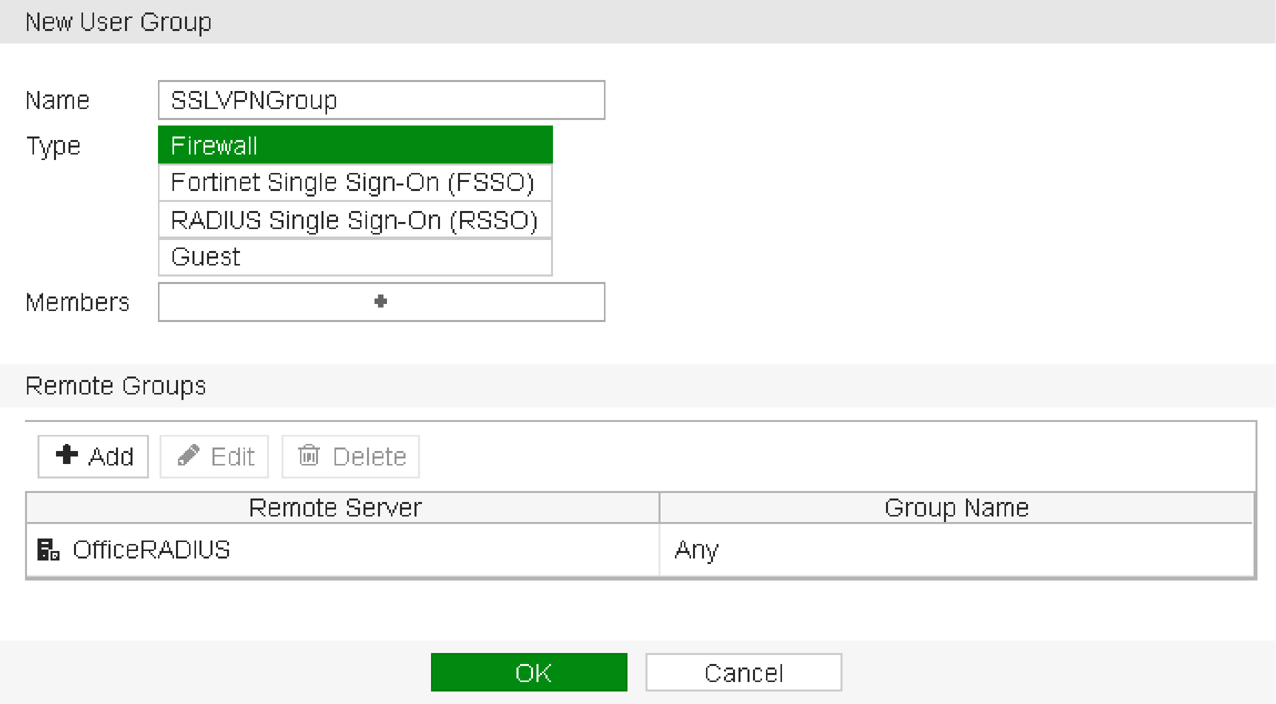
User credentials: ✖ More validation is required

Server message

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

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.



Name: SSLVPNGroup

Type: Firewall

Remote Server	Group Name
OfficeRADIUS	Any

3. In the FortiGate CLI, increase the remote authentication timeout to 60 seconds.

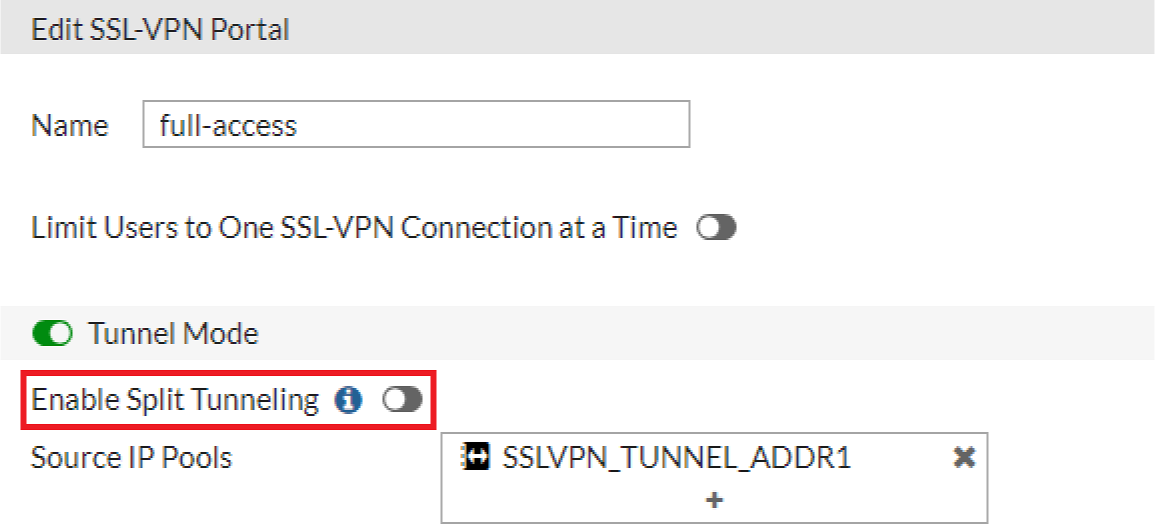
```
#config system global
```

```
    #set remoteauthtimeout 60
#end
```

Configuring the SSL-VPN

To configure 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.



Edit SSL-VPN Portal

Name: full-access

Limit Users to One SSL-VPN Connection at a Time ○

● Tunnel Mode

Enable Split Tunneling ○

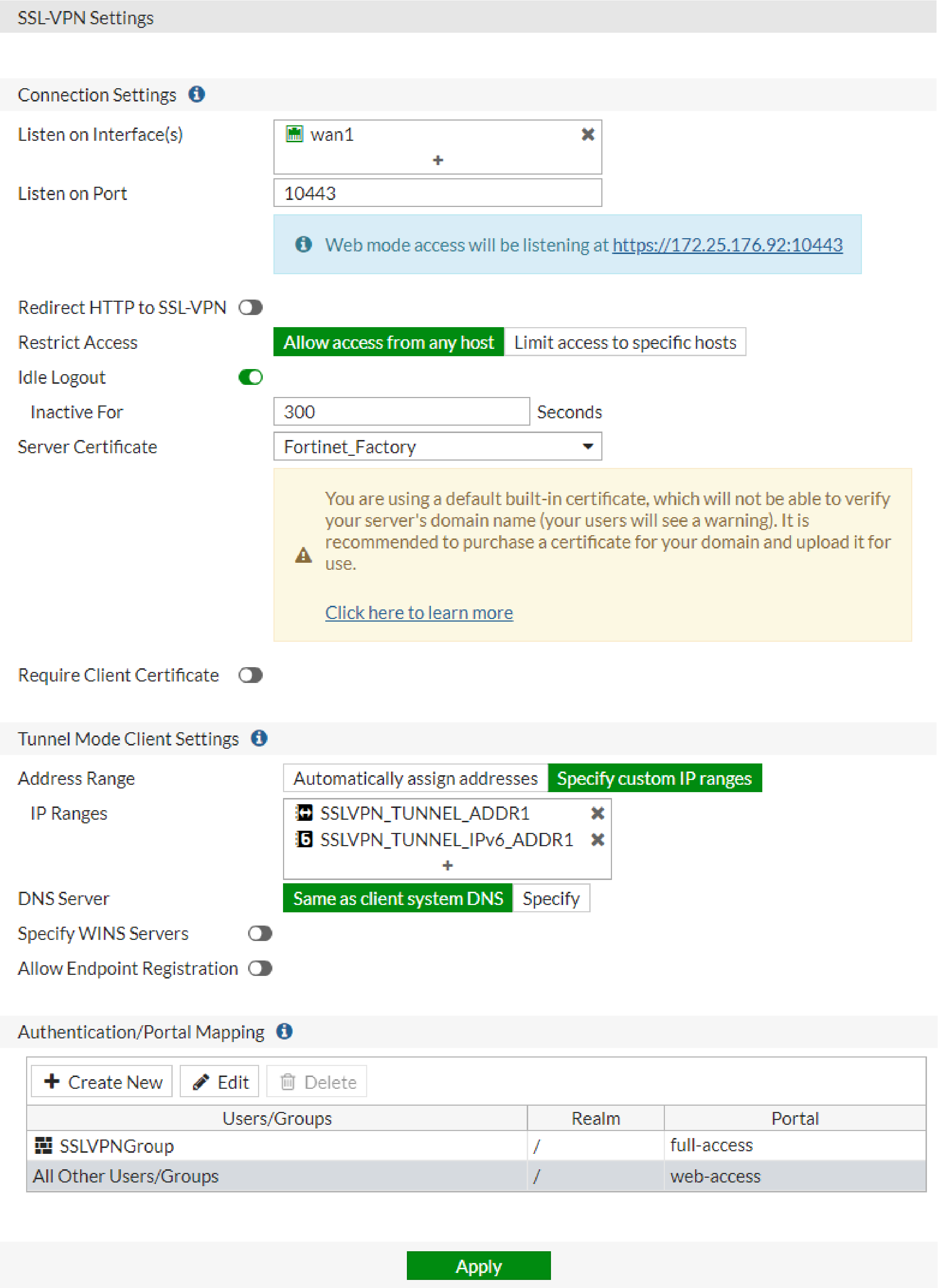
Source IP Pools: SSLVPN_TUNNEL_ADDR1

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: ○

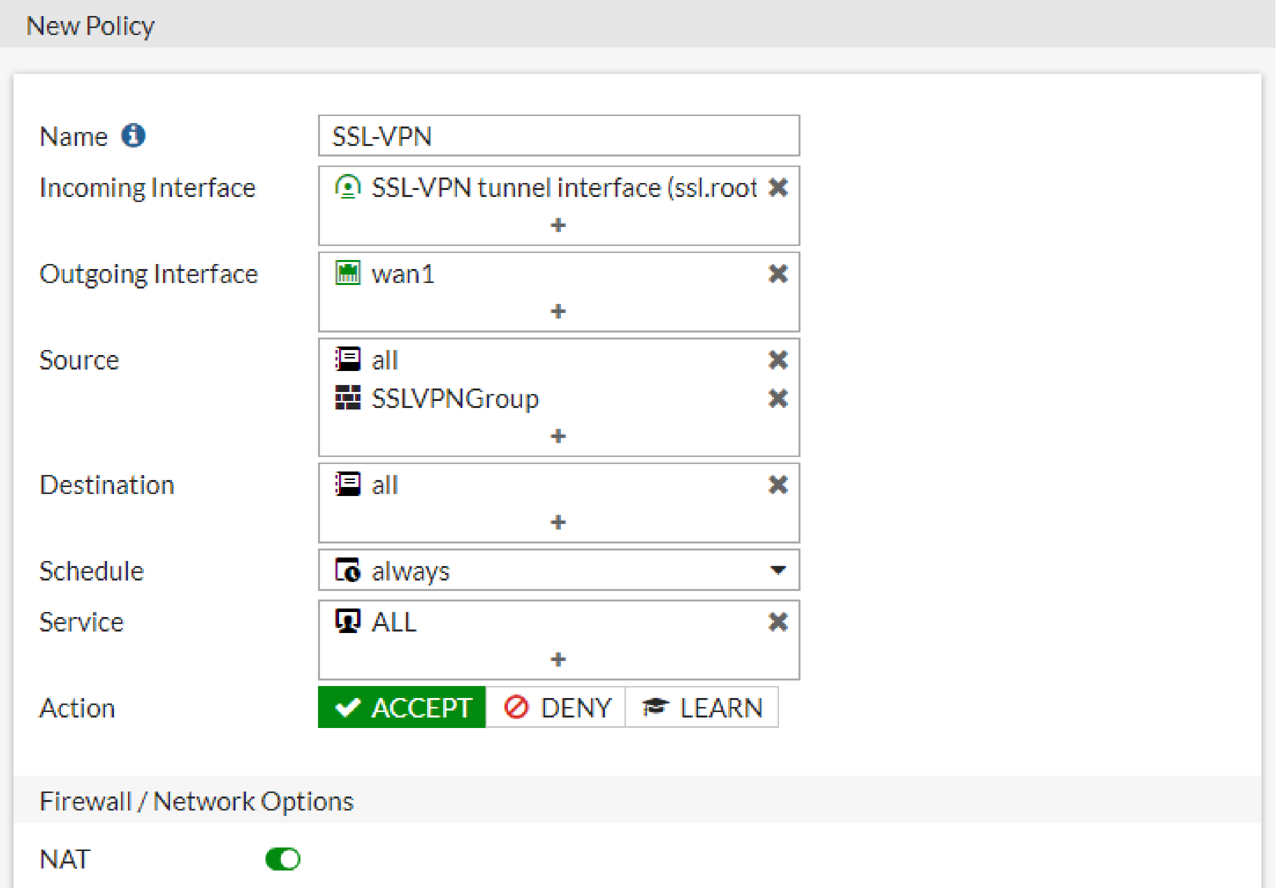
Authentication/Portal Mapping

Users/Groups	Realm	Portal
SSLVPNGroup	/	full-access
All Other Users/Groups	/	web-access

3. Then go to *Policy & Objects* > *IPv4 Policy* and create a new SSL VPN policy.
   Set *Incoming Interface* to the *SSL-VPN tunnel interface* and set *Outgoing Interface* to the Internet-facing interface (in this case, *wan1*).

   Set *Source* to the *SSLVPNGroup* user group and the *all* address.

   Set *Destination* to *all*, *Schedule* to *always*, *Service* to *ALL*, and enable *NAT*.



New Policy

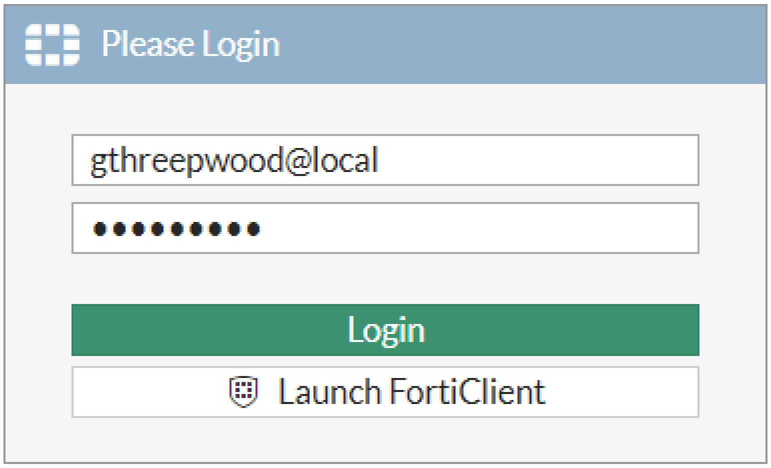
Name	SSL-VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.root
Outgoing Interface	wan1
Source	all SSLVPNGroup
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY LEARN

Firewall / Network Options

NAT	●

Results

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

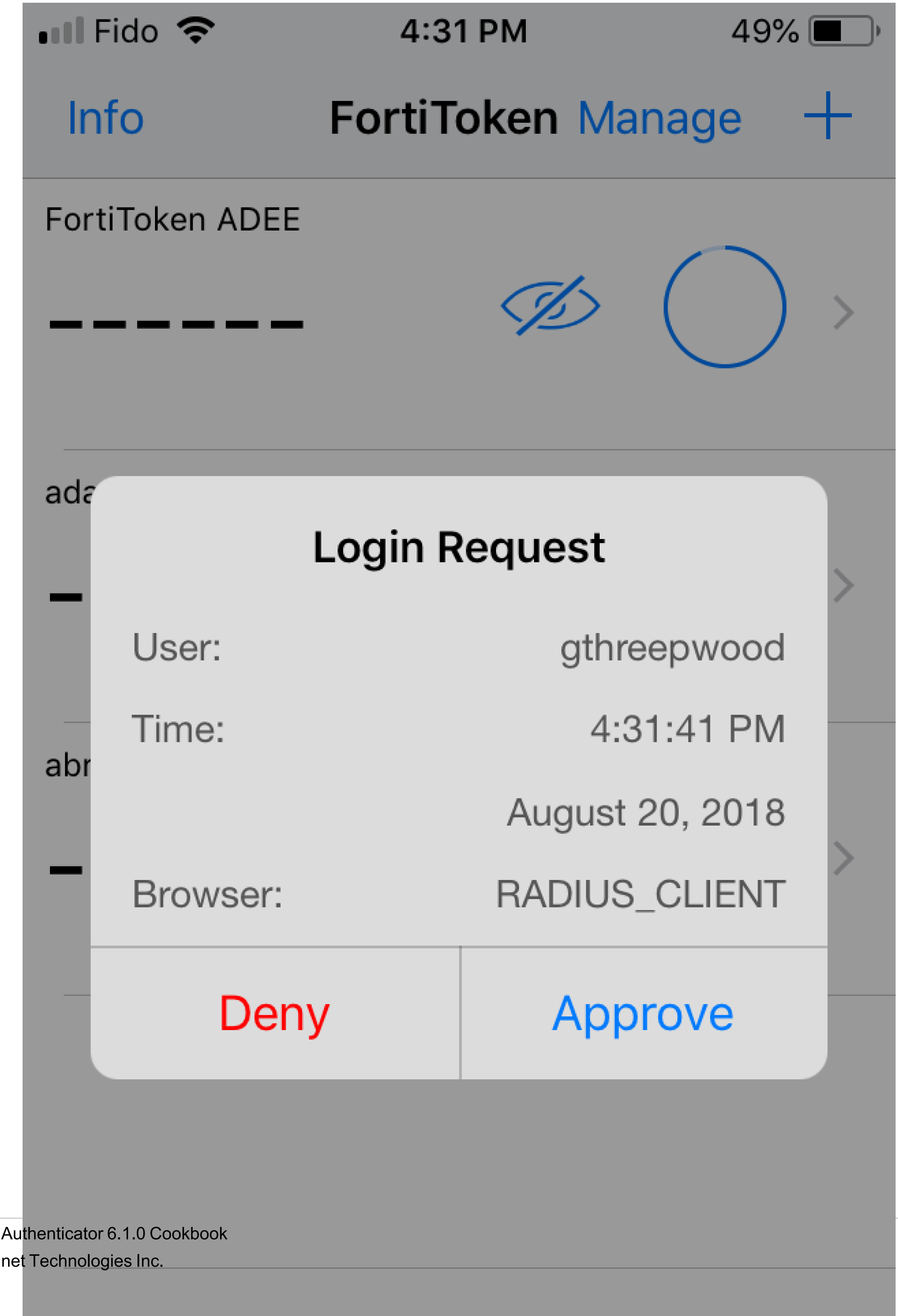


Please Login

gthreepwood@local

••••••••••

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



Login Request

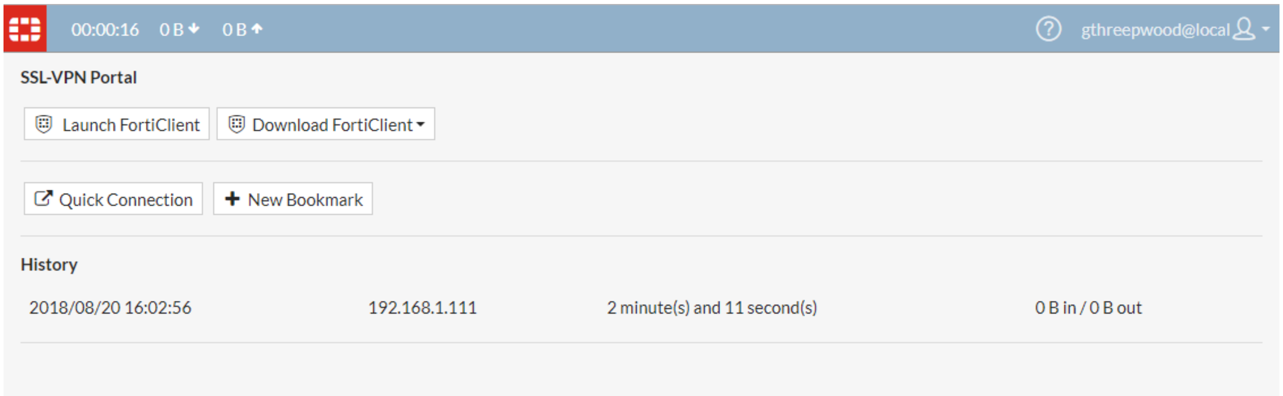
User: gthreepwood

Time: 4:31:41 PM

August 20, 2018

Browser: RADIUS_CLIENT

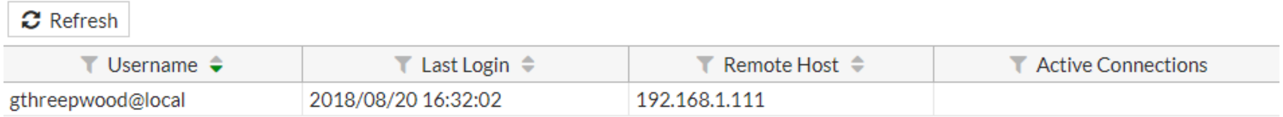
Upon approving the authentication, *gthreepwood* is successfully logged into the SSL VPN portal.



History

2018/08/20 16:02:56	192.168.1.111	2 minute(s) and 11 second(s)	0 B in / 0 B out

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

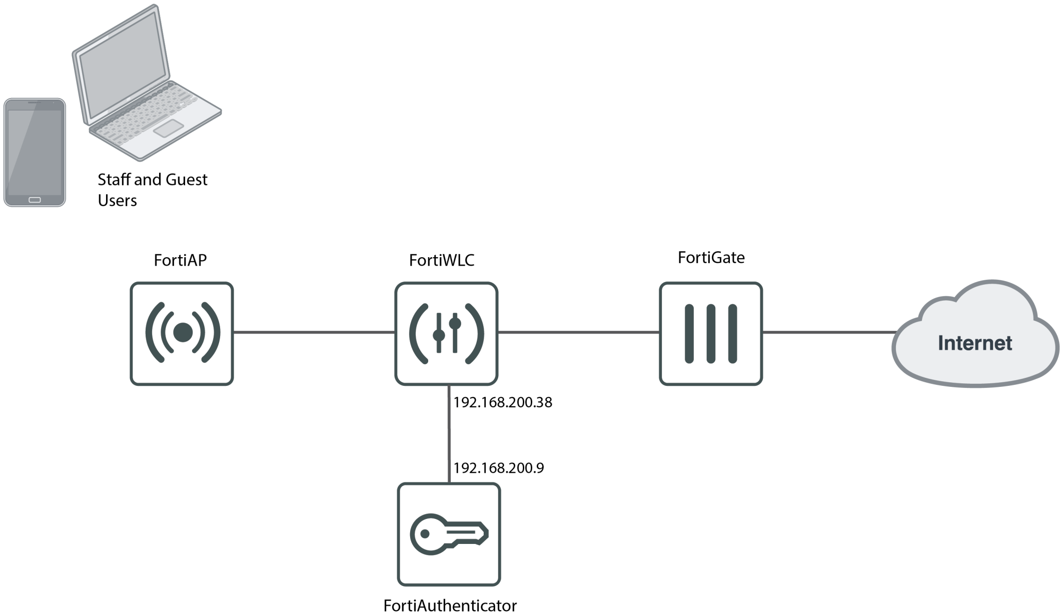


Username	Last Login	Remote Host	Active Connections
gthreepwood@local	2018/08/20 16:32:02	192.168.1.111	

Guest Portals

This section contains information about creating and using guest portals.

FortiAuthenticator as Guest Portal for FortiWLC

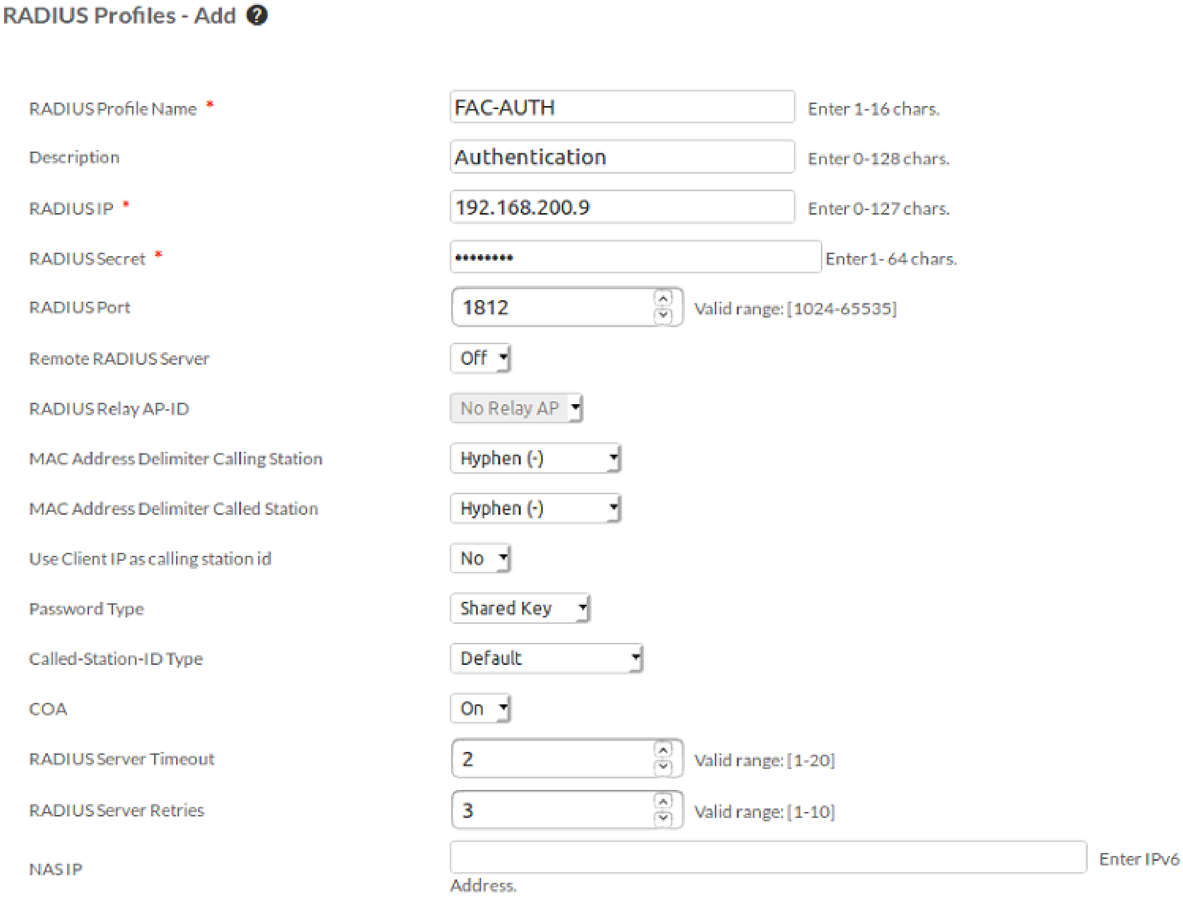


In this recipe we will use FortiAuthenticator as Guest Portal for users getting wireless connection provided by FortiWLC.

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.



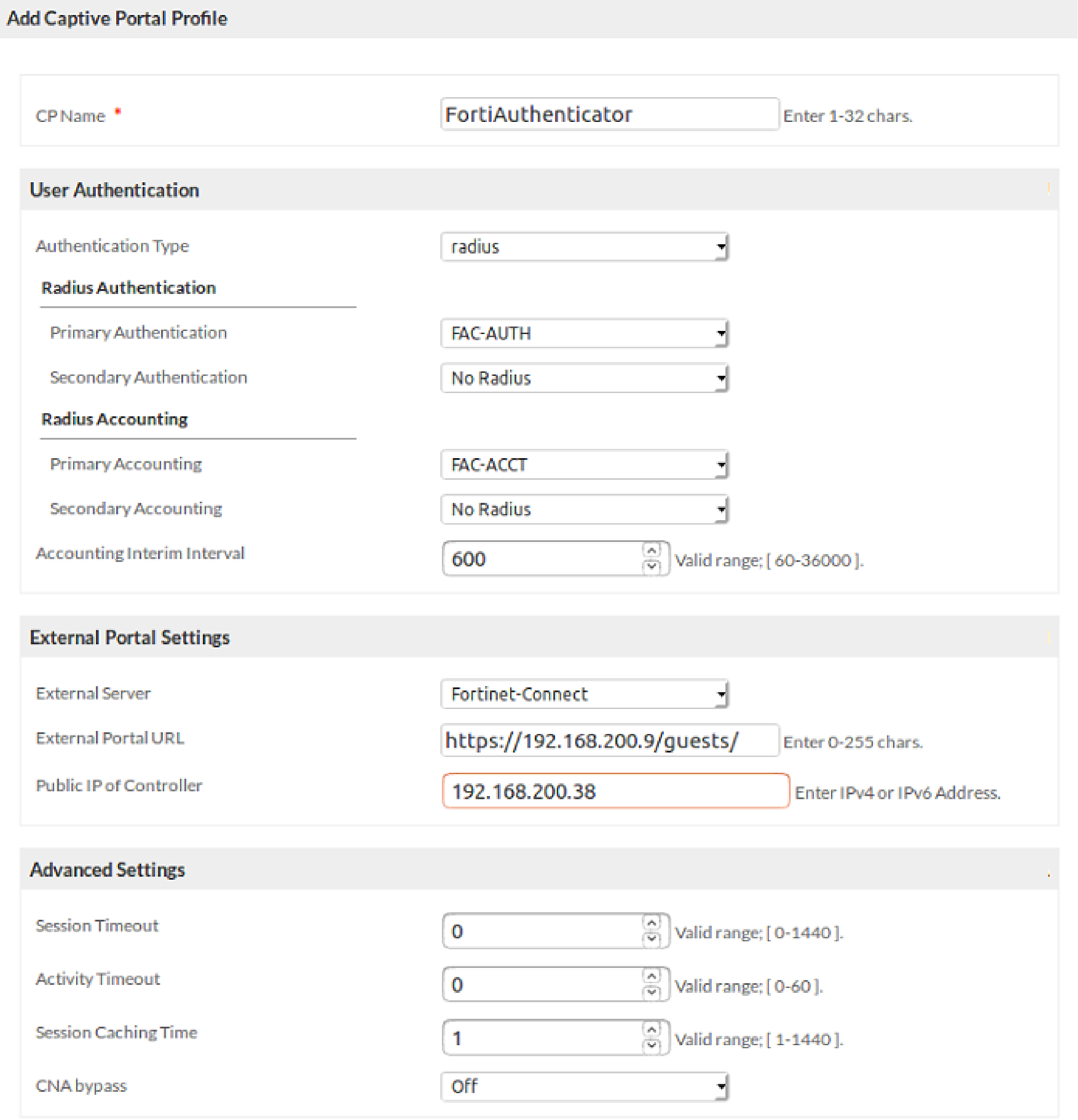
RADIUS Profiles - Add

RADIUS Profile Name *	FAC-AUTH	Enter 1-16 chars.
Description	Authentication	Enter 0-128 chars.
RADIUS IP *	192.168.200.9	Enter 0-127 chars.
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 Calling Station	Hyphen (-)	
MAC Address Delimiter Called Station	Hyphen (-)	
Use Client IP as calling station id	No	
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]
NAS IP		Enter IPv6 Address.

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 that the FortiAuthenticator can use to communicate with 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-ACCT	
Secondary Accounting	No Radius	
Accounting Interim Interval	600	Valid range: [60-36000].

External Portal Settings

External Server	Fortinet-Connect	
External Portal URL	https://192.168.200.9/guests/	Enter 0-255 chars.
Public IP of Controller	192.168.200.38	Enter IPv4 or IPv6 Address.

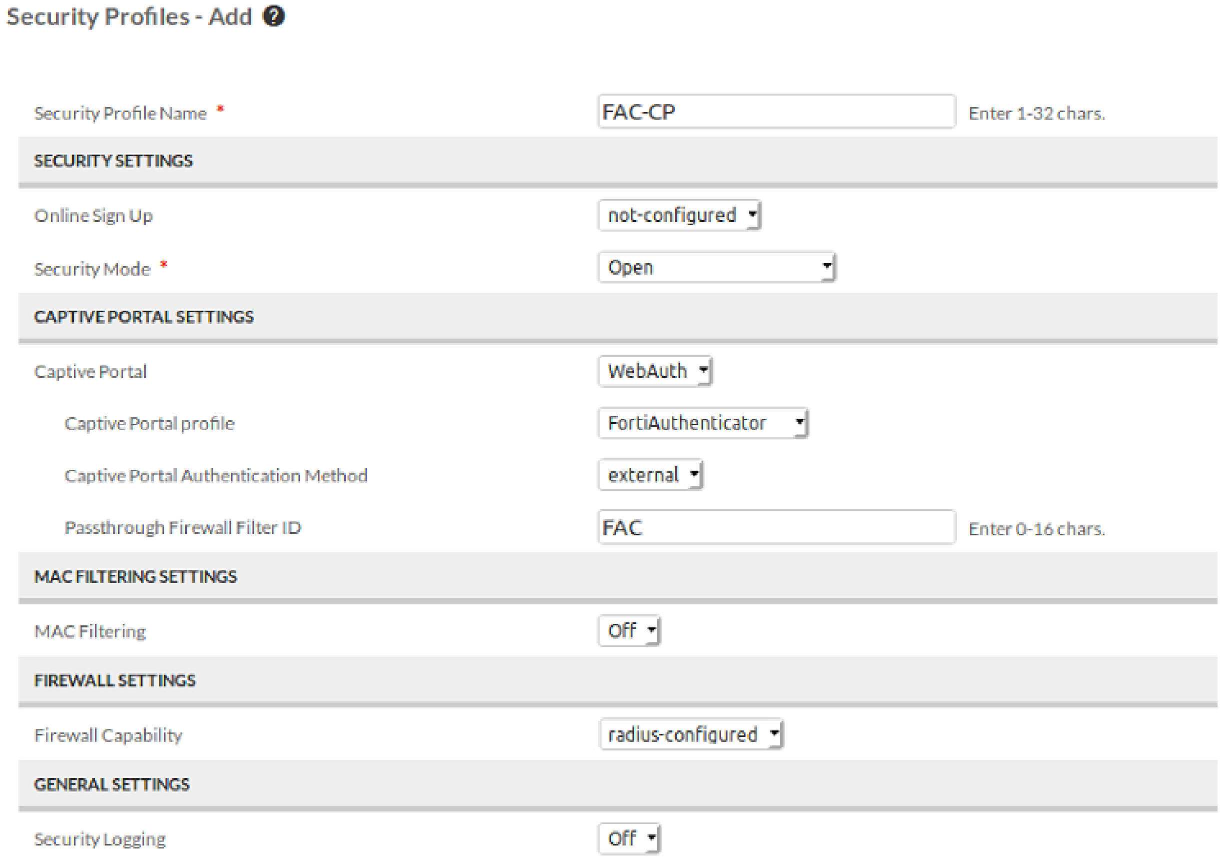
Advanced Settings

Session Timeout	0	Valid range: [0-1440].
Activity Timeout	0	Valid range: [0-60].
Session Caching Time	1	Valid range: [1-1440].
CNA bypass	Off	

Creating the security profile on the FortiWLC

1. On the FortiWLC, go to *Configuration* > *Security* > *Profile* and *ADD* a new profile.
   - *Profile Name*: Enter a name for the profile.
   - *Security Mode*: *Open*
   - *Captive Portal*: *WebAuth*
   - *Captive Portal Profile*: Select the profile created earlier.
   - *Captive Portal Authentication Method*: *external*

- *Passthrough Firewall Filter ID*: An ID used to allow access to the portal before authentication using QoS rules.



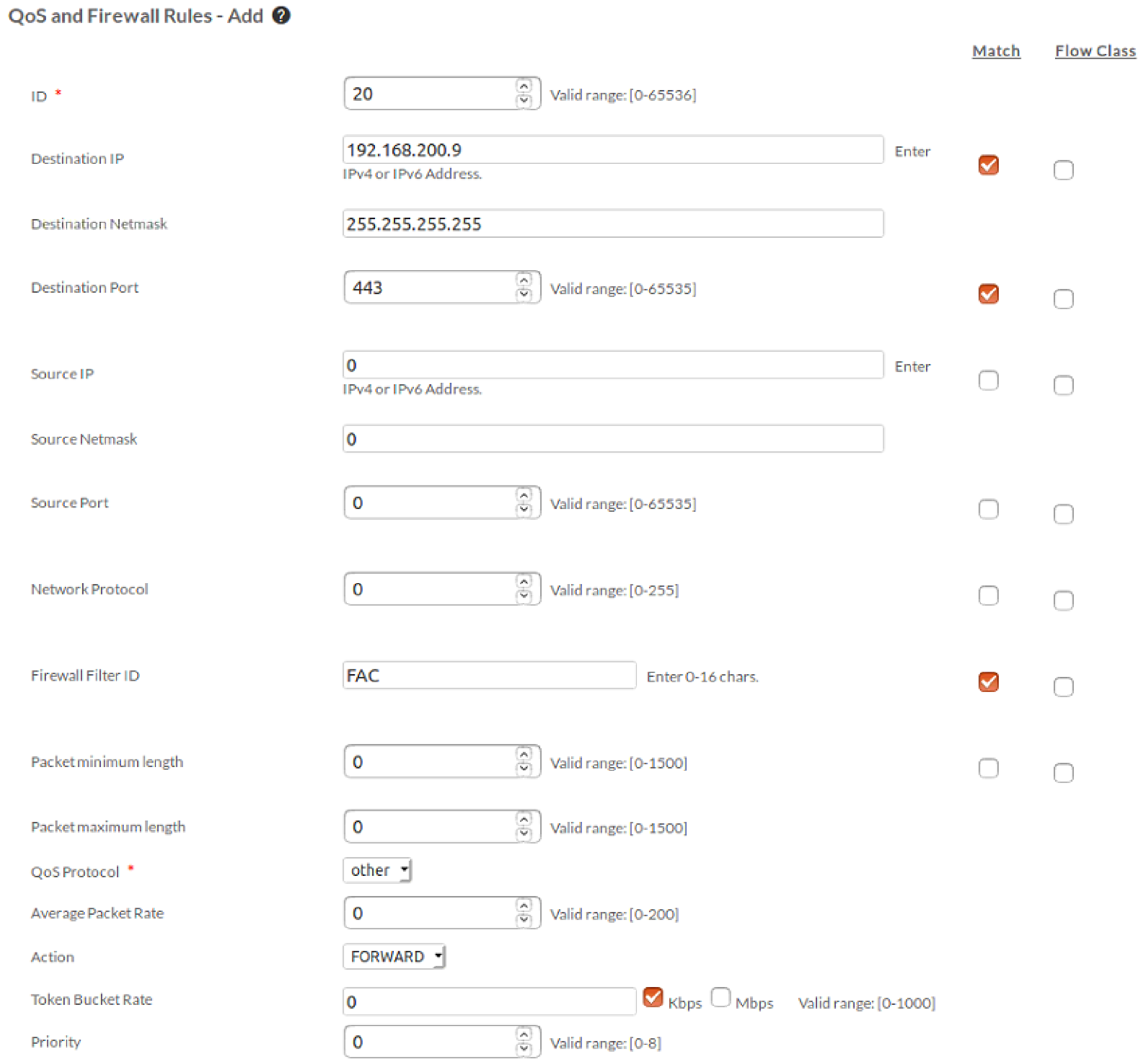
Security Profiles - Add

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 0-16 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

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

- *QoS Protocol*: Other.

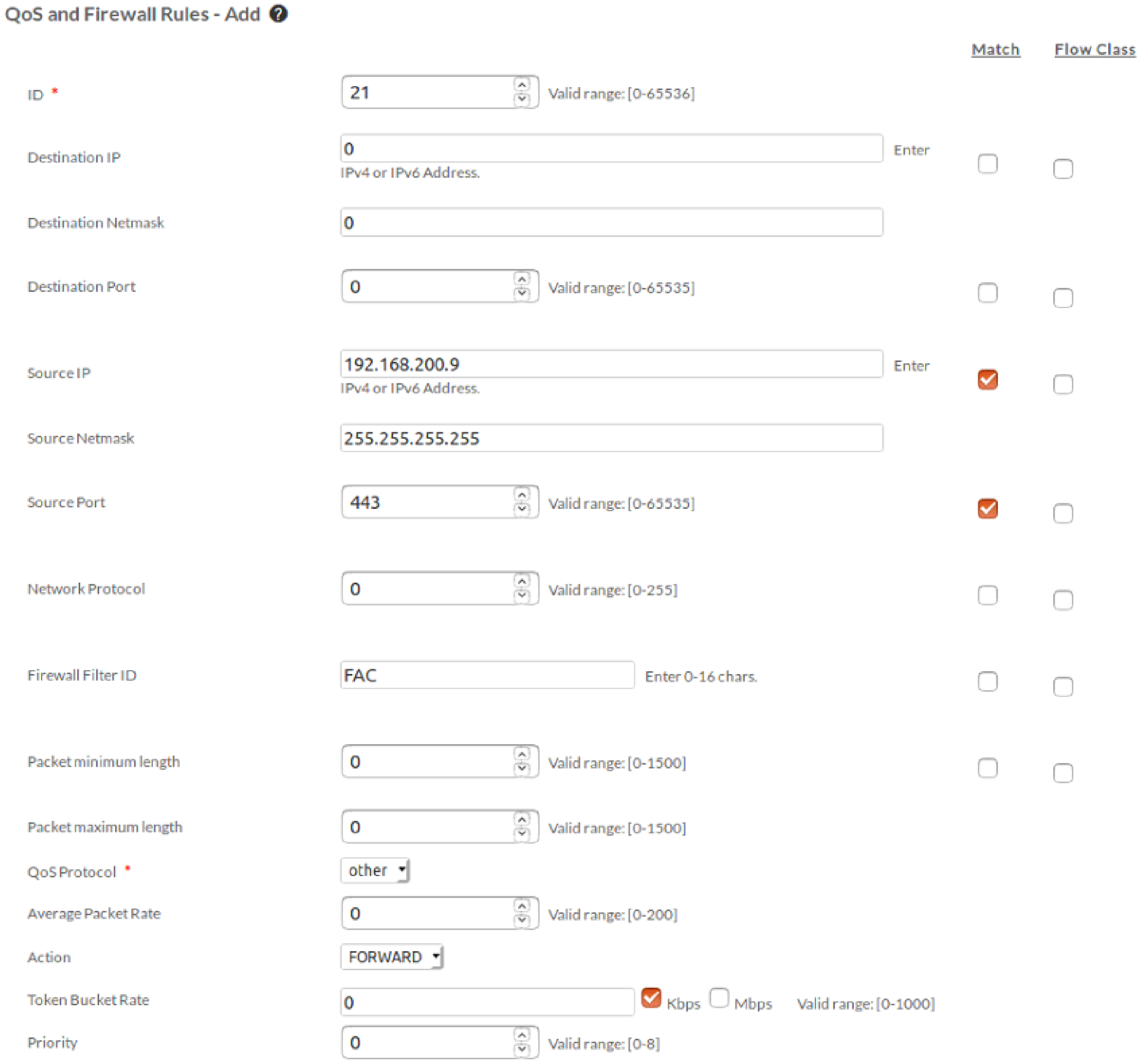


QoS and Firewall Rules - Add

			Match	Flow Class
ID *	20	Valid range: [0-65536]		
Destination IP	192.168.200.9 IPv4 or IPv6 Address.	Enter	☑	□
Destination Netmask	255.255.255.255			
Destination Port	443	Valid range: [0-65535]	☑	□
Source IP	0 IPv4 or IPv6 Address.	Enter	□	□
Source Netmask	0			
Source Port	0	Valid range: [0-65535]	□	□
Network Protocol	0	Valid range: [0-255]	□	□
Firewall Filter ID	FAC	Enter 0-16 chars.	☑	□
Packet minimum length	0	Valid range: [0-1500]	□	□
Packet maximum length	0	Valid range: [0-1500]		
QoS Protocol *	other			
Average Packet Rate	0	Valid range: [0-200]		
Action	FORWARD			
Token Bucket Rate	0	☑ Kbps □ Mbps Valid range: [0-1000]		
Priority	0	Valid range: [0-8]		

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.



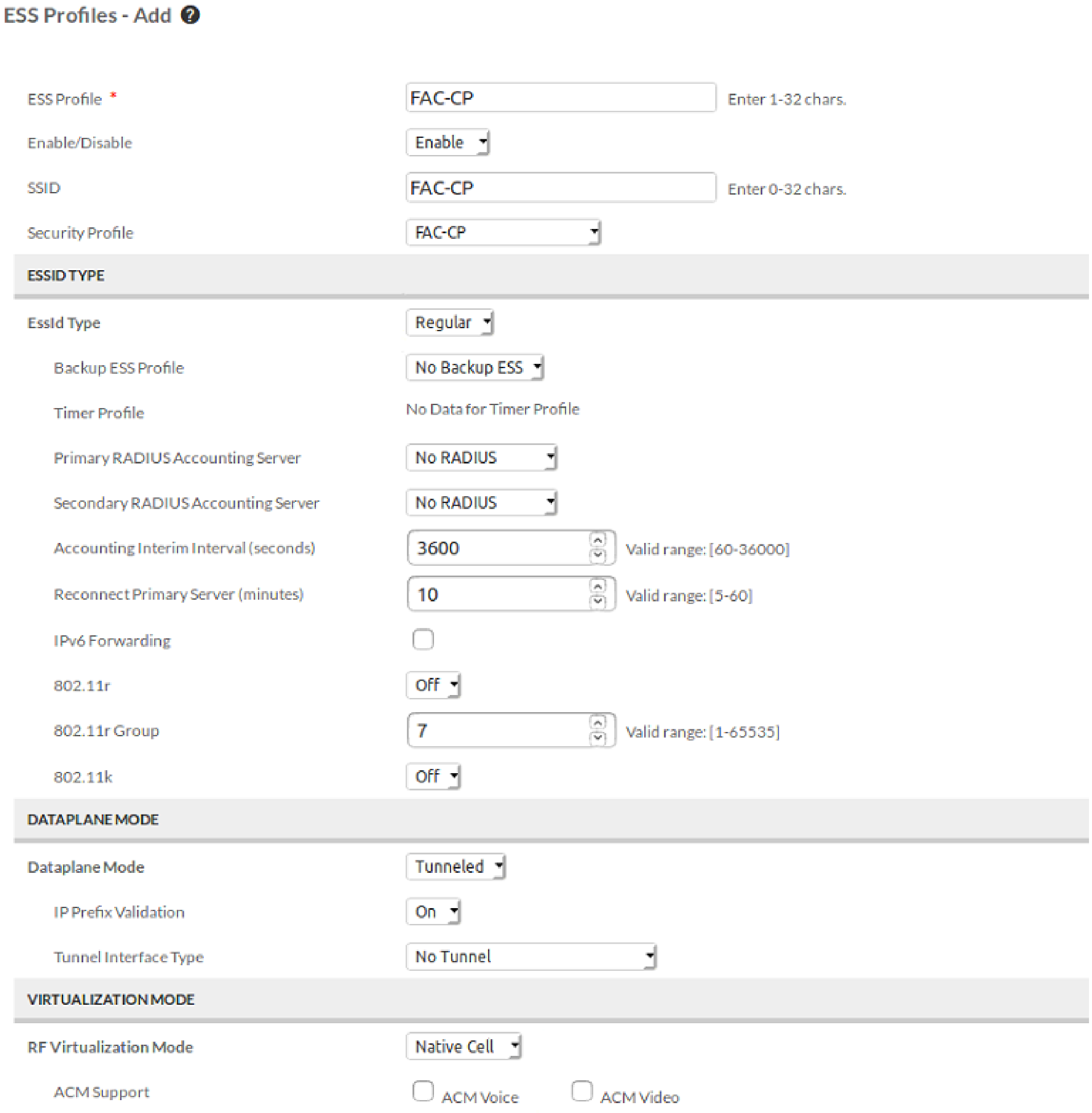
QoS and Firewall Rules - Add

			Match	Flow Class
ID *	21	Valid range: [0-65536]		
Destination IP	0 IPv4 or IPv6 Address.	Enter	☐	☐
Destination Netmask	0			
Destination Port	0	Valid range: [0-65535]	☐	☐
Source IP	192.168.200.9 IPv4 or IPv6 Address.	Enter	☑	☐
Source Netmask	255.255.255.255			
Source Port	443	Valid range: [0-65535]	☑	☐
Network Protocol	0	Valid range: [0-255]	☐	☐
Firewall Filter ID	FAC	Enter 0-16 chars.	☐	☐
Packet minimum length	0	Valid range: [0-1500]	☐	☐
Packet maximum length	0	Valid range: [0-1500]		
QoS Protocol *	other			
Average Packet Rate	0	Valid range: [0-200]		
Action	FORWARD			
Token Bucket Rate	0	☑ Kbps ☐ Mbps Valid range: [0-1000]		
Priority	0	Valid range: [0-8]		

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

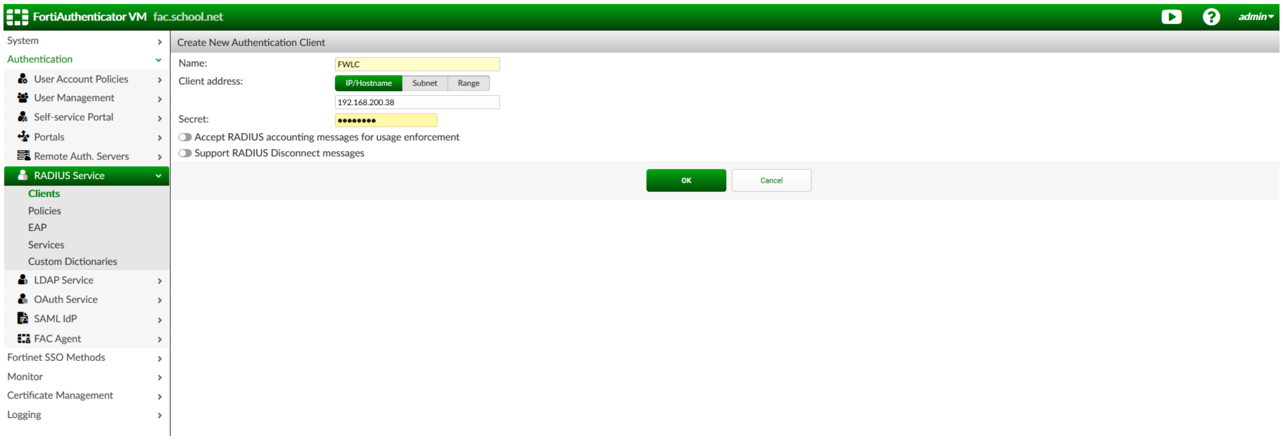
ESS Profile *	FAC-CP	Enter 1-32 chars.
Enable/Disable	Enable	
SSID	FAC-CP	Enter 0-32 chars.
Security Profile	FAC-CP	
ESSID TYPE		
EssId Type	Regular	
Backup ESS Profile	No Backup ESS	
Timer Profile	No Data for Timer Profile	
Primary RADIUS Accounting Server	No RADIUS	
Secondary RADIUS Accounting Server	No RADIUS	
Accounting Interim Interval (seconds)	3600	Valid range: [60-36000]
Reconnect Primary Server (minutes)	10	Valid range: [5-60]
IPv6 Forwarding	□	
802.11r	Off	
802.11r Group	7	Valid range: [1-65535]
802.11k	Off	
DATAPLANE MODE		
Dataplane Mode	Tunneled	
IP Prefix Validation	On	
Tunnel Interface Type	No Tunnel	
VIRTUALIZATION MODE		
RF Virtualization Mode	Native Cell	
ACM Support	□ ACM Voice	□ ACM Video

Creating FortiWLC as RADIUS client on the FortiAuthenticator

To create a RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients* and create a new client.
   Set *Client address* to *IP/Hostname* and enter the IP address the FortiWLC will send its RADIUS requests from.

Set the same *Secret* that was entered during the RADIUS configuration on the FortiWLC.



Create New Authentication Client

Name: FWLC

Client address: IP/Hostname | Subnet | Range

192.168.200.38

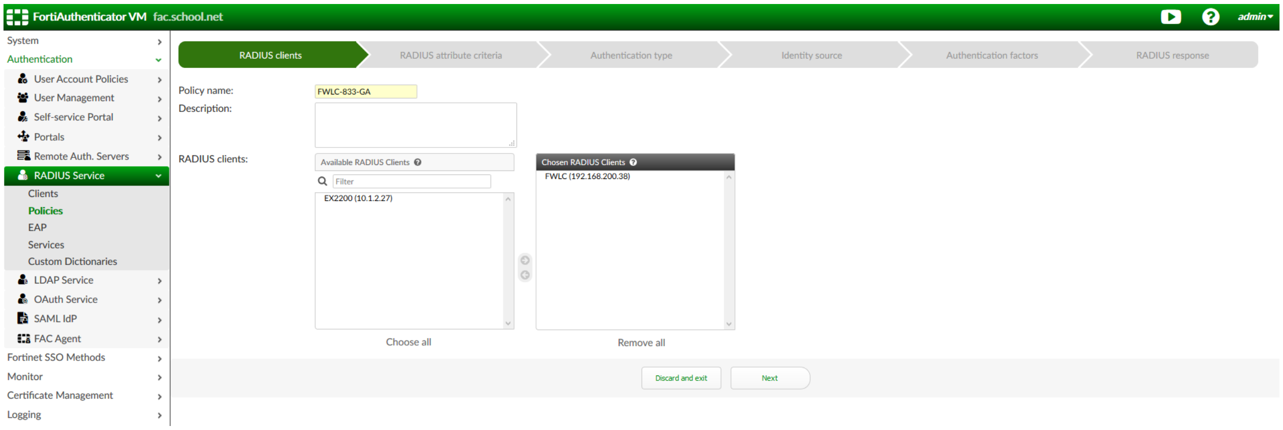
Secret: ••••••••

○ Accept RADIUS accounting messages for usage enforcement

○ Support RADIUS Disconnect messages

To create the RADIUS policy:

1. Go to *Authentication > RADIUS Service > Policies*, and create a new policy.



Policy name: FWLC-833-GA

Description:

RADIUS clients:

Available RADIUS Clients: EX2200 (10.1.2.27)

Chosen RADIUS Clients: FWLC (192.168.200.38)

2. In *RADIUS clients*, select the FWLC client previously created.
3. In *RADIUS attribute criteria*, click *Next*. No RADIUS attribute criteria need to be specified in this configuration.
4. In *Authentication type*, select *Password/OTP authentication*. If EAP is being used for wireless authentication, enable *Accept EAP*, along with the desired EAP types.
5. In *Identity source*, select the realm for which user authentication is needed.
6. In *Authentication factors*, select *Verify all configured authentication factors*.
7. Review the *RADIUS response*, and save the policy.

Creating the portal and access point on FortiAuthenticator

To create a portal:

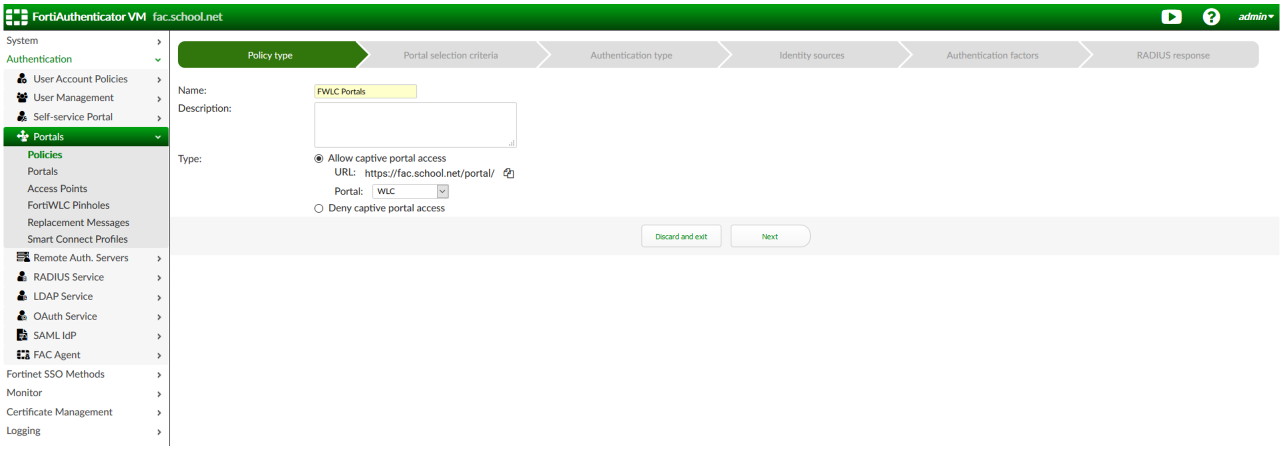
1. On the FortiAuthenticator, go to *Authentication > Portals > Portals*, and create a new portal.
2. Enter a name for the portal, and click *OK*.

To create an access point:

1. On FortiAuthenticator, go to *Authentication* > *Portals* > *Access Points*, and create a new access point.
2. Enter a name for the access point, and provide the client IP/Hostname from the FortiAP, and click *OK*.

Creating the portal policy on FortiAuthenticator

1. On the FortiAuthenticator, go to *Authentication* > *Portals* > *Policies*, and create a new policy.
   Enter a name for the policy, select *Allow captive portal access*, and choose the previously configured FortiWLC Portal.



Name: FWLC Portals

Description:

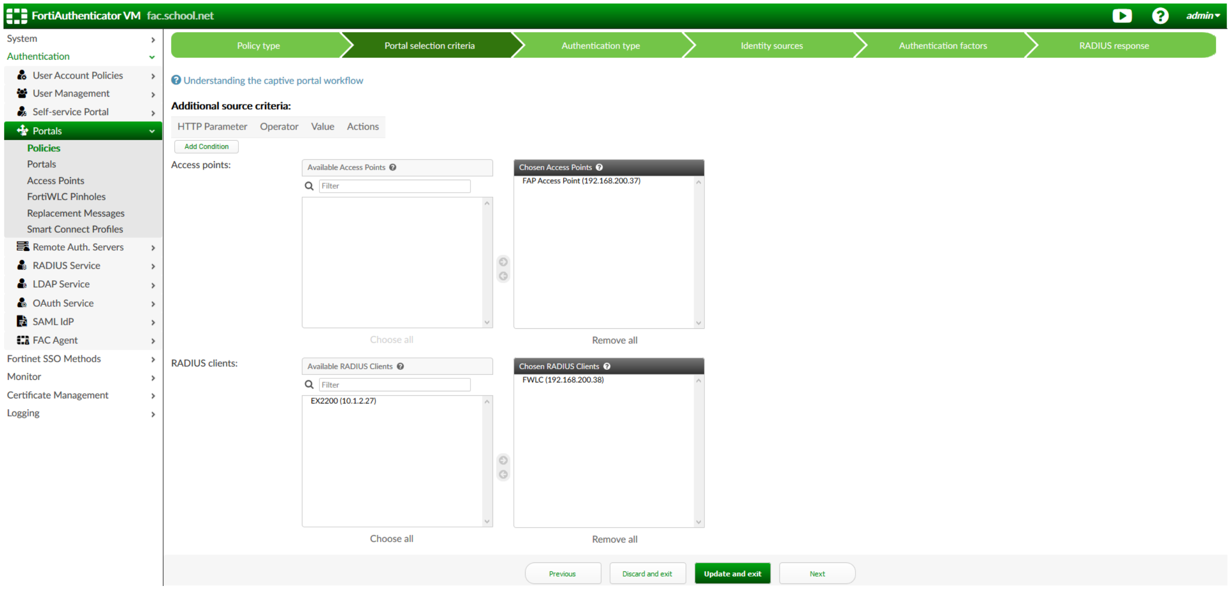
Type: ● Allow captive portal access

URL: https://fac.school.net/portal/

Portal: WLC

○ Deny captive portal access

2. In Portal selection criteria, configure the following:
   a. *Access points*: Select the previously configured FortiAP access point.
   b. *RADIUS clients*: Select the previously configured FortiWLC RADIUS client.



Additional source criteria:

HTTP Parameter	Operator	Value	Actions

Access points:

Available Access Points	Chosen Access Points
	FAP Access Point (192.168.200.37)

RADIUS clients:

Available RADIUS Clients	Chosen RADIUS Clients
EX2200 (10.1.2.27)	FWLC (192.168.200.38)

3. In *Authentication type*, select *Password/OTP authentication* and *Local/remote user*.
4. In *Identity sources*, select the realm for which the user authentication is needed.
5. In *Authentication factors*, select *Verify all configured authentication factors*.
6. Review the RADIUS response and save your changes.

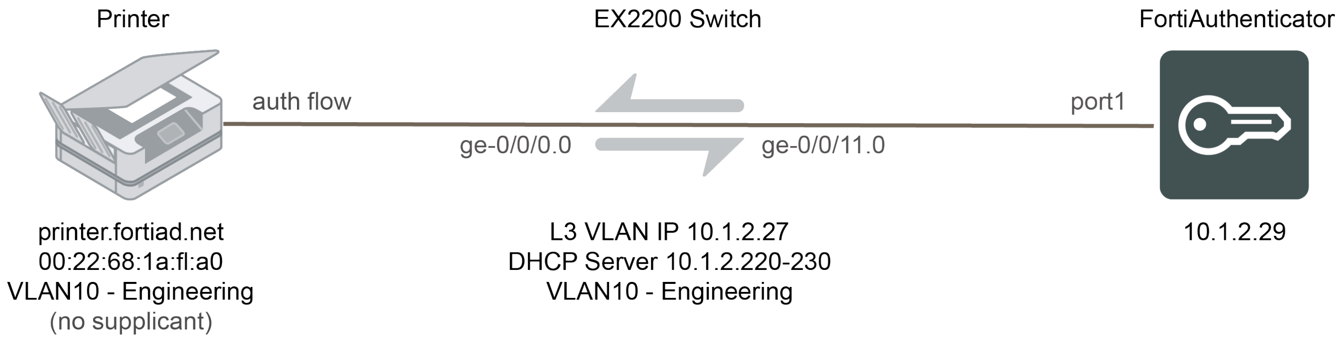
Results

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

MAC authentication bypass

This section describes configuring MAC address bypass with FortiAuthenticator.

MAC authentication bypass with dynamic VLAN assignment

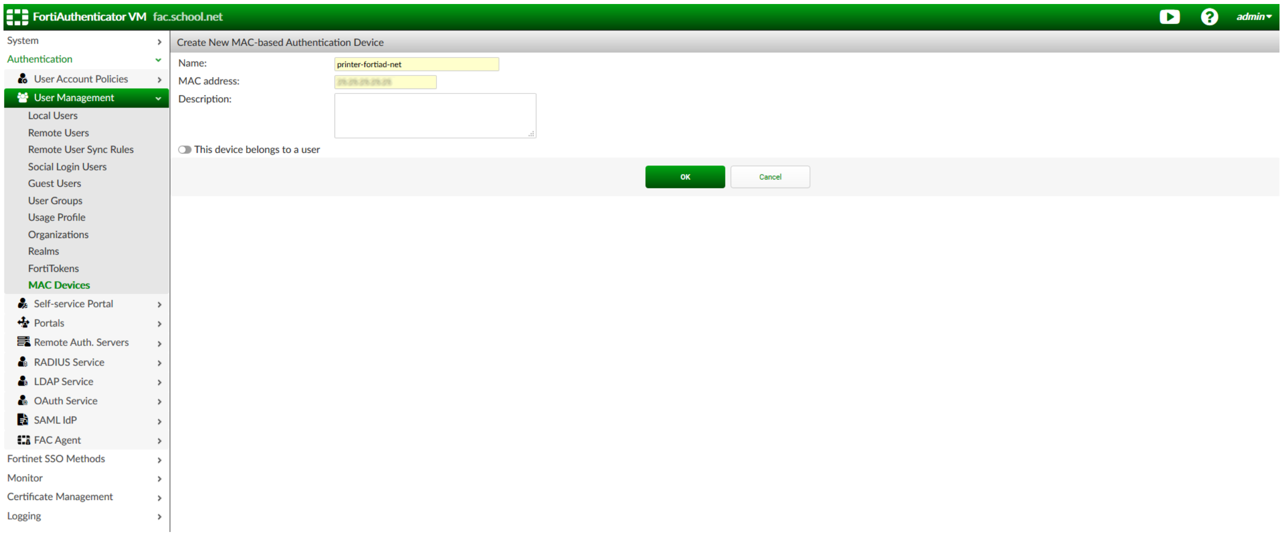


In this recipe, you will configure MAC authentication bypass (MAB) in a wired network with dynamic VLAN assignment.

The purpose of this recipe is to configure and demonstrate MAB 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.
   Enter a name for the device along with the device's MAC address.
   Alternatively, you can use the *Import* option to import this information from a CSV file.



Create New MAC-based Authentication Device

Name: printer-fortiad-net

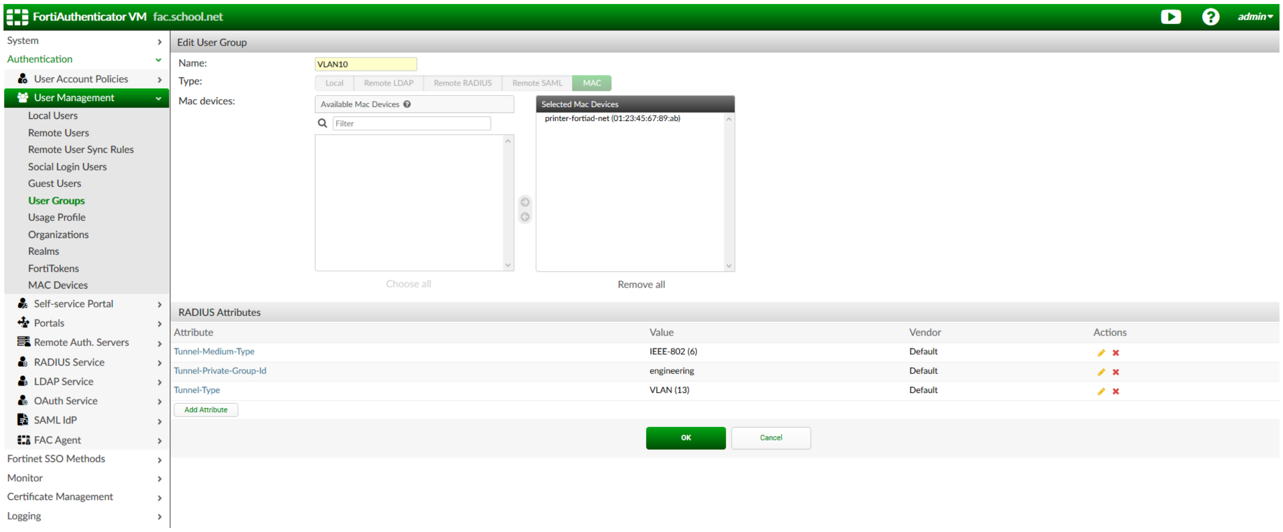
MAC address: [redacted]

Description:

○ This device belongs to a user

Configuring the user group

1. Go to *Authentication* > *User Management* > *User Groups* and create a new user group. Select *MAC* as the type, and add the newly created MAC device. Click *OK*.
2. Enter the *RADIUS Attributes* as shown in the image below.



Edit User Group

Name: VLAN10

Type: Local | Remote LDAP | Remote RADIUS | Remote SAML | MAC

Mac devices:

Selected Mac Devices: printer-fortiad-net (01:23:45:67:89:ab)

RADIUS Attributes

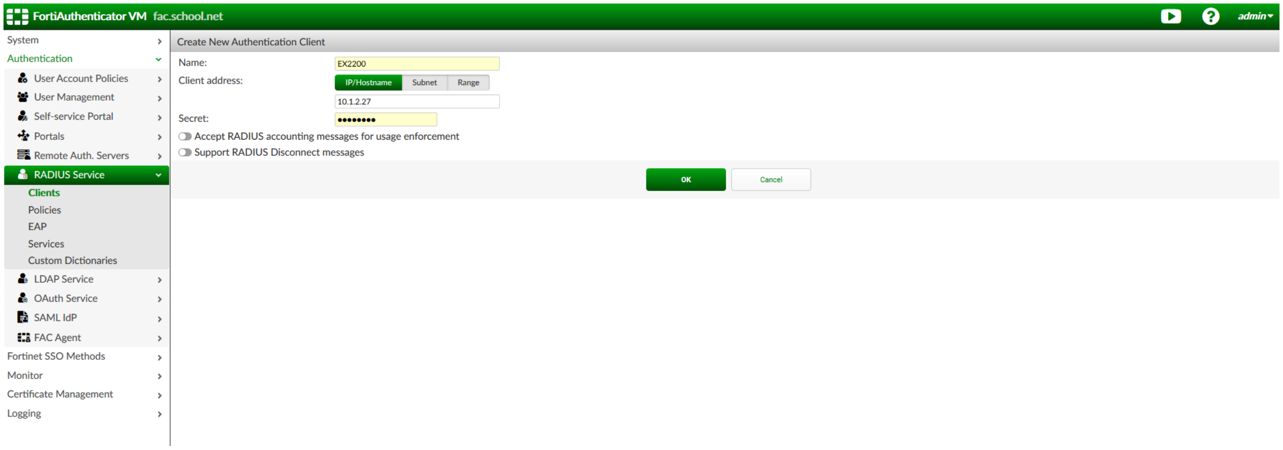
Attribute	Value	Vendor	Actions
Tunnel-Medium-Type	IEEE-802 (6)	Default	✎ ✖
Tunnel-Private-Group-Id	engineering	Default	✎ ✖
Tunnel-Type	VLAN (13)	Default	✎ ✖

RADIUS attributes can only be added after the group has been created.

Configuring RADIUS settings on FortiAuthenticator

To create the RADIUS client:

1. Go to *Authentication* > *RADIUS Service* > *Clients* and create a new RADIUS client. Configure the IP and shared secret from your switch, and click *OK*.



Create New Authentication Client

Name: EX2200

Client address: [✓ IP/Hostname] Subnet Range

10.1.2.27

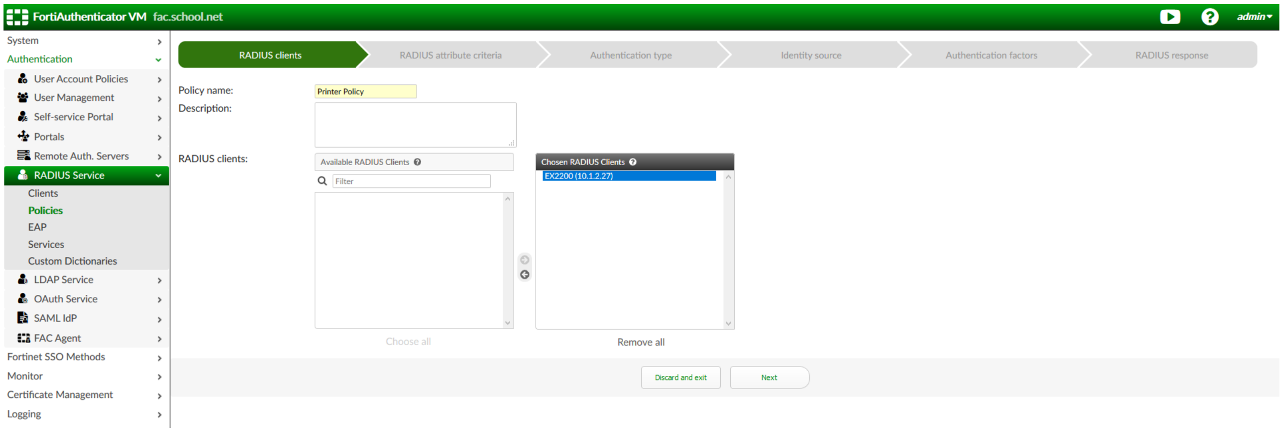
Secret: •••••••••

○ Accept RADIUS accounting messages for usage enforcement

○ Support RADIUS Disconnect messages

To create the RADIUS policy:

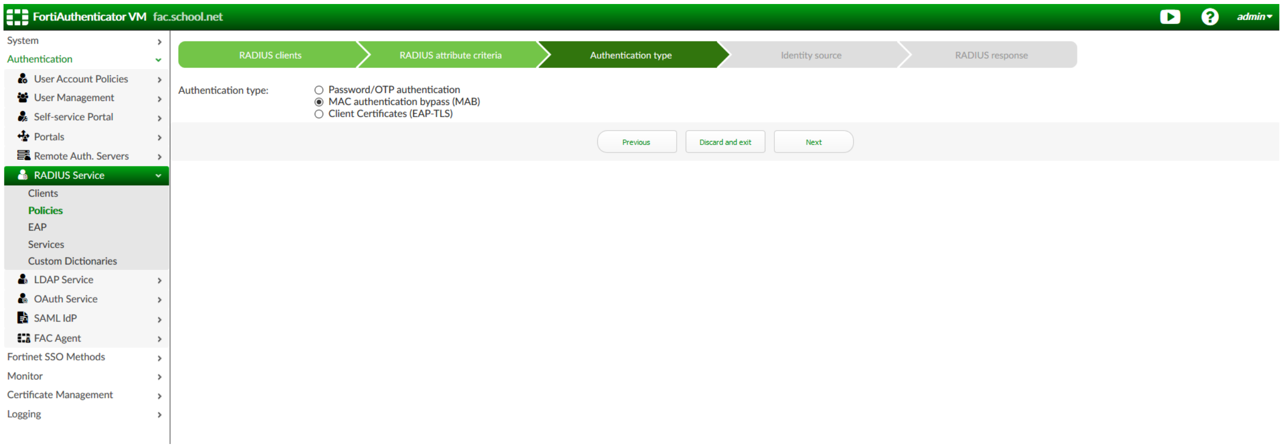
1. Go to *Authentication* > *RADIUS Service* > *Policies* and create a new RADIUS policy.
   In *RADIUS clients*, enter a policy name, and add the previously configured RADIUS client.



Policy name: Printer Policy
Description:
RADIUS clients: EX2200 (10.1.2.27)

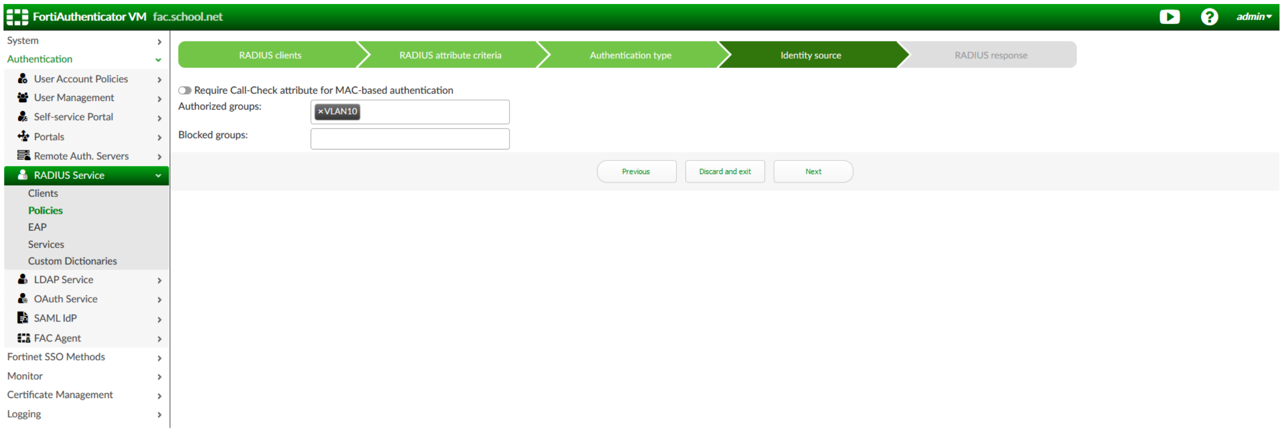
   RADIUS attribute criteria can be left blank.

2. In *Authentication type*, select *MAC authentication bypass (MAB)*.



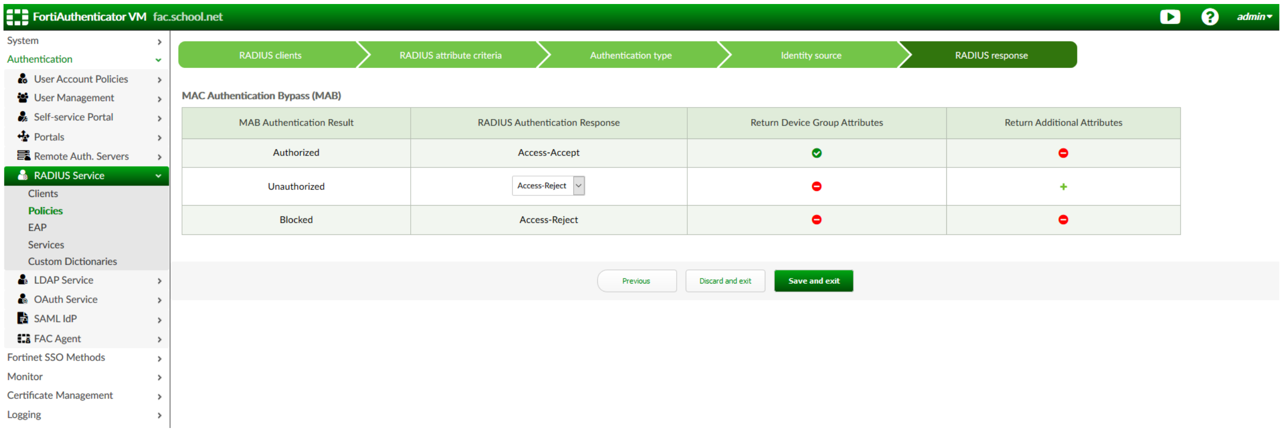
Authentication type:
○ Password/OTP authentication
● MAC authentication bypass (MAB)
○ Client Certificates (EAP-TLS)

3. In *Identity source*, add the previously configured MAC group to *Authorized groups*.



Require Call-Check attribute for MAC-based authentication
Authorized groups: ×VLAN10
Blocked groups:

4. Configure the RADIUS response to reject unauthorized requests, and click *Save and exit*.



MAC Authentication Bypass (MAB)

MAB Authentication Result	RADIUS Authentication Response	Return Device Group Attributes	Return Additional Attributes
Authorized	Access-Accept	✓	⊖
Unauthorized	Access-Reject	⊖	+
Blocked	Access-Reject	⊖	⊖

Configuring the 3rd-party switch

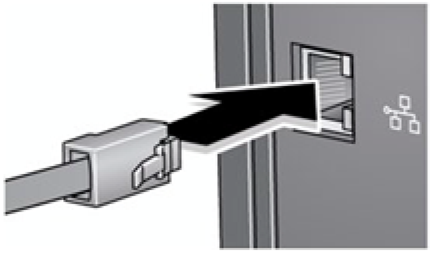
The switch configuration provided below is intended for demonstration only. Your switch configuration is likely to differ significantly.

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

No configuration is required on the endpoint.

Results

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



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

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

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

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

```
17:36:19.115264 IP (tos Ox0, ttl 64, id 49111, offset 0, flags [none], proto UDP (17),
     length 73)
  10.1.2.29.1812 > 10.1.2.27.60114: (bad udp cksum 0x1880 -> 0x5ccel] RADIUS, length: 45
     Access-Accept (2), id: 0x08, Authenticator: b5c7b1bb5a316fb483a622eaae58ccc2
        Tunnel-Type Attribute (64), length: 6, Value: Tag[Unused] #13
           0x0000: 0000 000d
        Tunnel-Medium-Type Attribute (65), length: 6, Value: Tag[Unused] 802
           0x0000: 0000 0006
        Tunnel-Private-Group-ID Attribute (81), length: 13, Value: engineering
```

```
          0x0000: 656e 6769 6e65 6572 696e 67
     0x0000: 4500 0049 bfd7 0000 4011 a293 0a01 021d E..I....@ .......
     0x0010: 0a01 021b 0714 ead2 0035 1880 0208 002d 5
     0x0020: b5c7 blbb 5a31 6fb4 83a6 22ea ae58 ccc2 ....21o..."..X..
     0x0030: 4006 0000 0000 4106 0000 0006 510d 656e @ A Q en
     0x0040: 6769 6e65 6572 696e 67 gineering
```

5. **Post-authentication DHCP transaction is picked up by FortiAuthenticator**

   The Switch CLI shows a successful dot1x session:

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

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

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

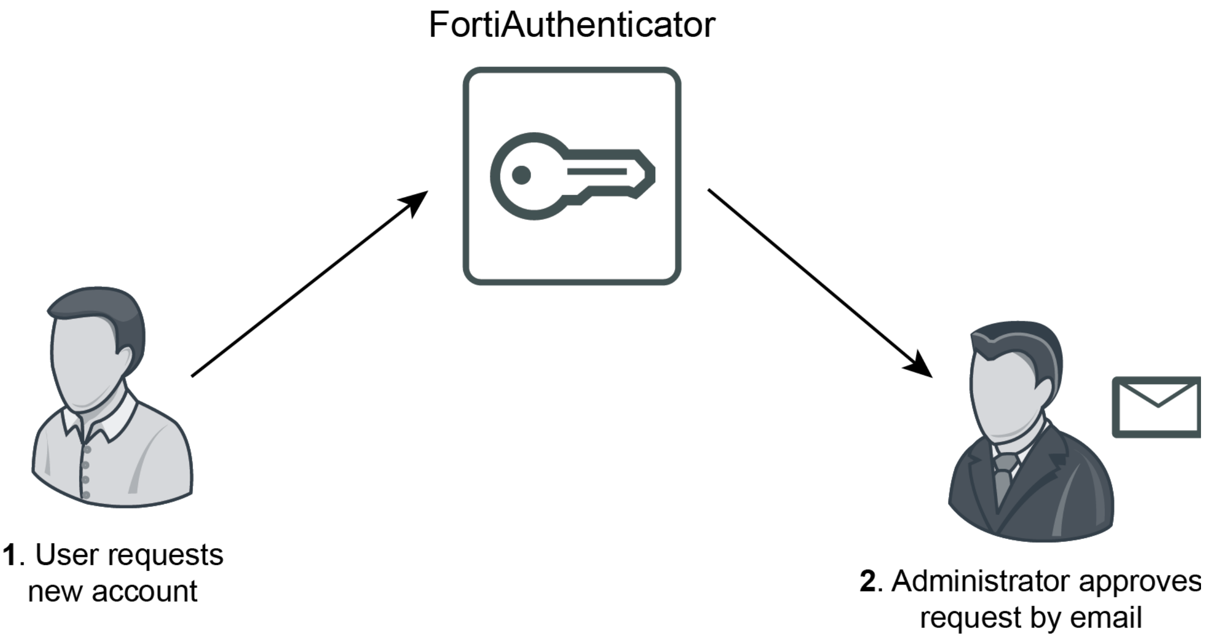
   Additionally, the printer shows as available on the network:

   ```
   root# run show arp interface vlan.10
   MAC Address Address Name Interface Flags
   00:0c:29:5b:90:68 10.1.2.29 10.1.2.29 vlan.10 none
   6c:70:9f:d6:ae:al 10.1.2.220 10.1.2.220 vlan.10 none
   b8:53:ac:4a:d5:f5 10.1.2.221 10.1.2.221 vlan.10 none
   00:22:68:1a: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 tt1=128 time=2.068 ms
   64 bytes from 10.1.2.224: icmp_seq=1 tt1=128 time=2.236 ms
   64 bytes from 10.1.2.224: icmp_seq=2 tt1=128 time=2.699 ms

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

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


FortiAuthenticator
1. User requests new account
2. Administrator approves request by email

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

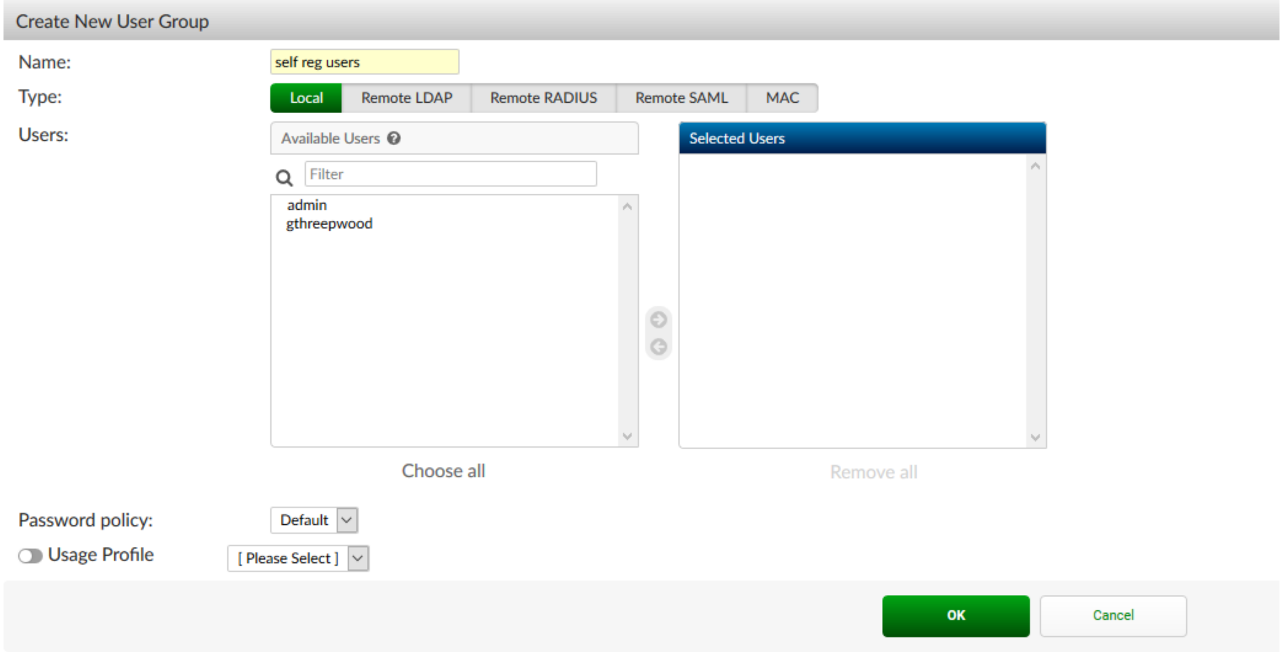
Note that enabling and using administrator approval requires the use of an email server, or SMTP server. Since administrators will approve requests by email, this recipe describes how to add an email server to your FortiAuthenticator. You will create and use a new server instead of the unit’s default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

Creating a self-registration user group

To create 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.



Create New User Group

Name: self reg users

Type: Local

Users:

Available Users

admin
gthreepwood

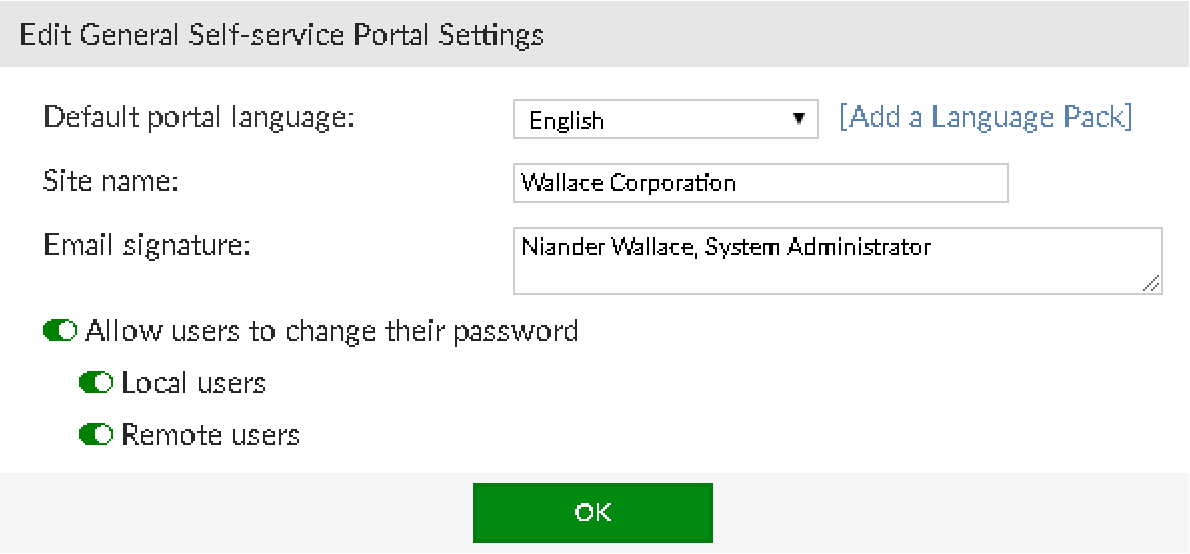
Password policy: Default

Usage Profile [Please Select]

Enabling self-registration

To enable 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*.

   Edit General Self-service Portal Settings

   Default portal language: English

   Site name: Wallace Corporation

   Email signature: Niander Wallace, System Administrator

   Allow users to change their password

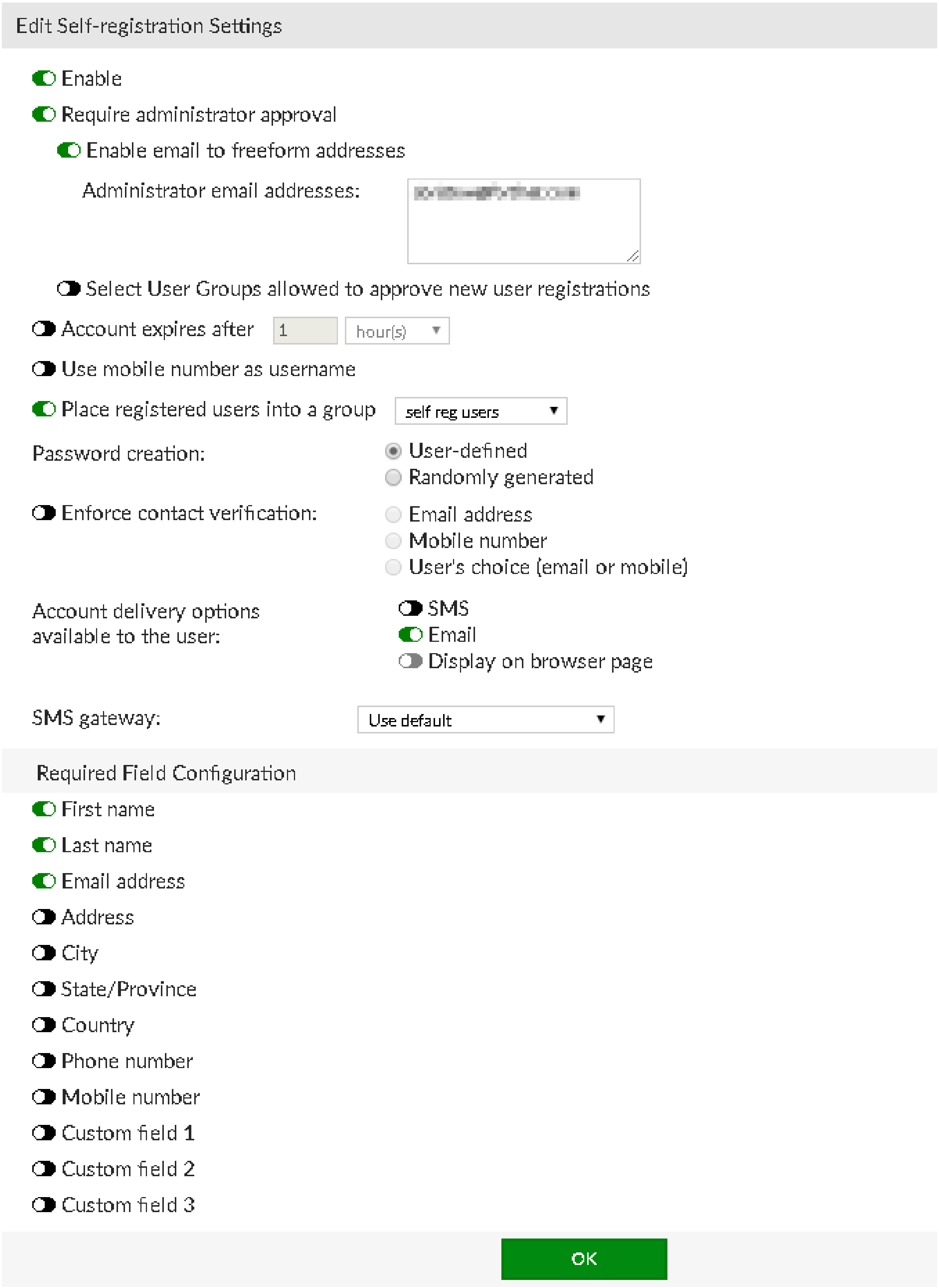
   Local users

   Remote users

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* dropdown 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: [redacted]

☐ Select User Groups allowed to approve new user registrations

☐ Account expires after 1 hour(s)

☐ Use mobile number as username

☑ Place registered users into a group: self reg users

Password creation: ● User-defined ○ Randomly generated

☐ Enforce contact verification: ○ Email address ○ Mobile number ○ User's choice (email or mobile)

Account delivery options available to the user: ☐ SMS ☑ Email ☐ Display on browser page

SMS gateway: Use default

Required Field Configuration

☑ First name

☑ Last name

☑ Email address

☐ Address

☐ City

☐ State/Province

☐ Country

☐ Phone number

☐ Mobile number

☐ Custom field 1

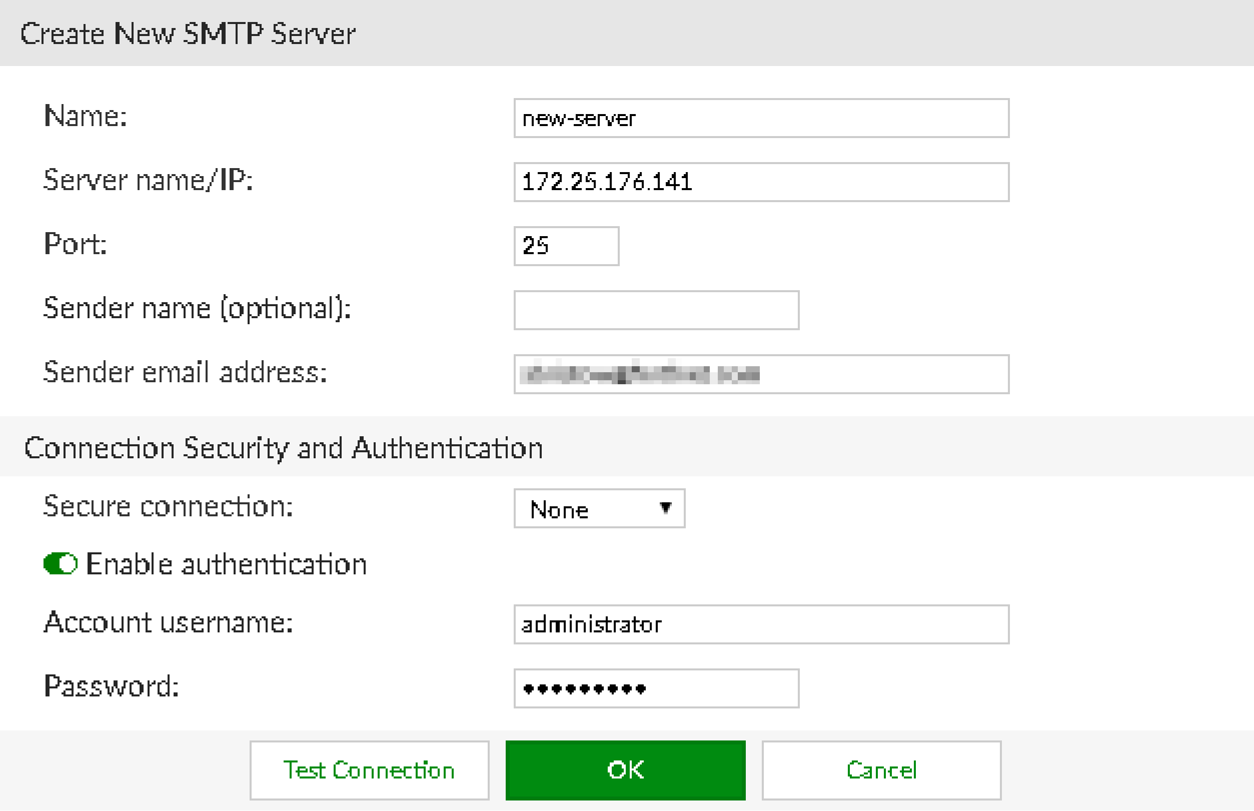
☐ Custom field 2

☐ Custom field 3

Creating a new SMTP server

To create 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.



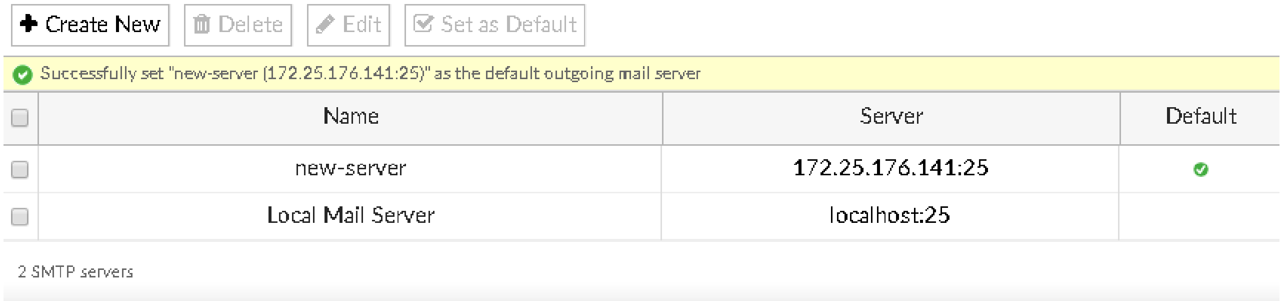
Create New SMTP Server

Name:	new-server
Server name/IP:	172.25.176.141
Port:	25
Sender name (optional):	
Sender email address:	[redacted]

Connection Security and Authentication

Secure connection:	None ▾
● Enable authentication	
Account username:	administrator
Password:	••••••••••

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



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

□	Name	Server	Default
□	new-server	172.25.176.141:25	✓
□	Local Mail Server	localhost:25	

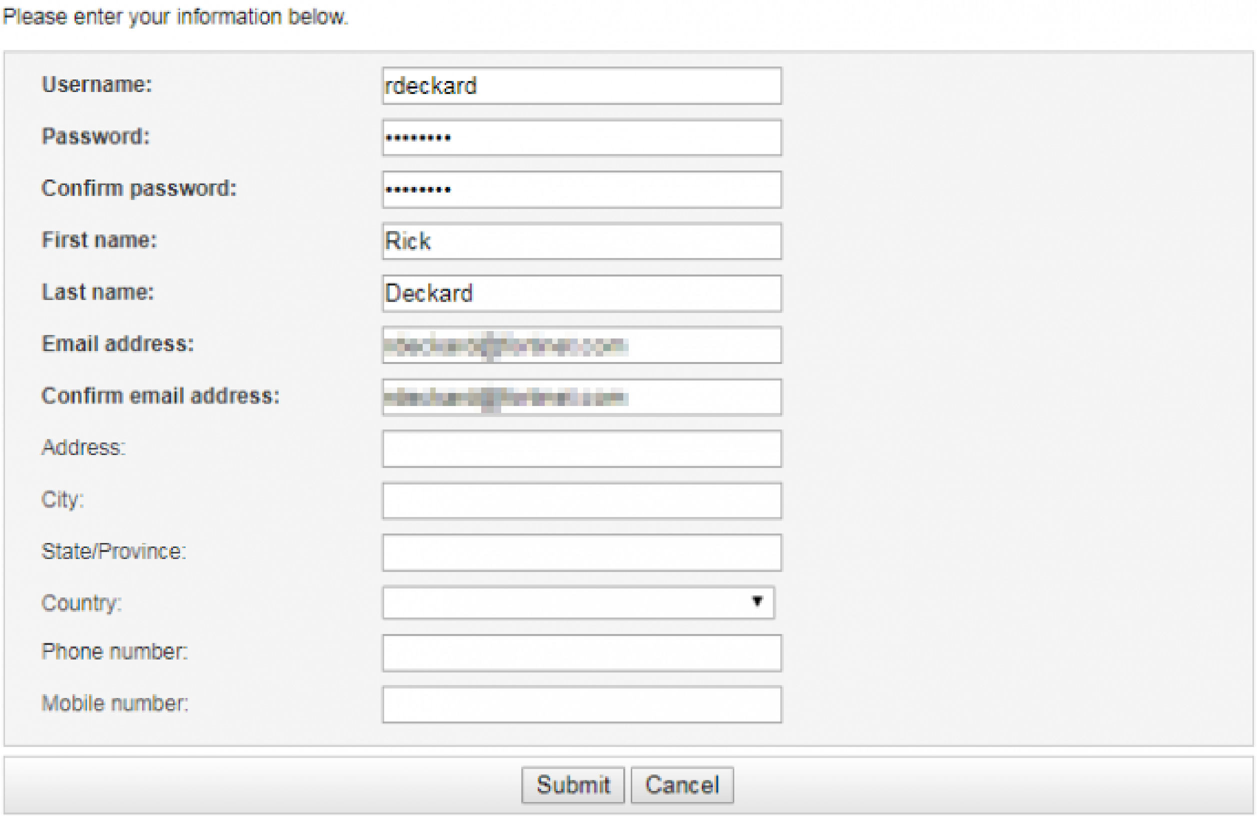
2 SMTP servers

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.

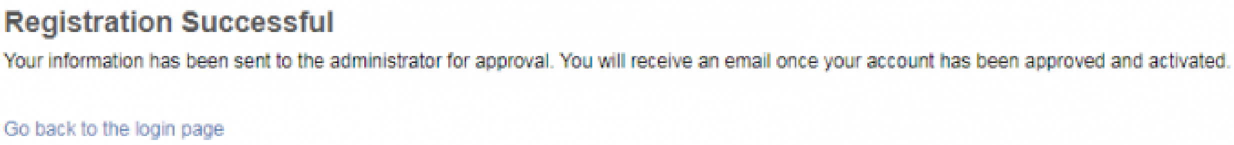
   Select *Submit*.



Please enter your information below.

Username:	rdeckard
Password:	••••••••
Confirm password:	••••••••
First name:	Rick
Last name:	Deckard
Email address:	[redacted]
Confirm email address:	[redacted]
Address:	
City:	
State/Province:	
Country:	▾
Phone number:	
Mobile number:	

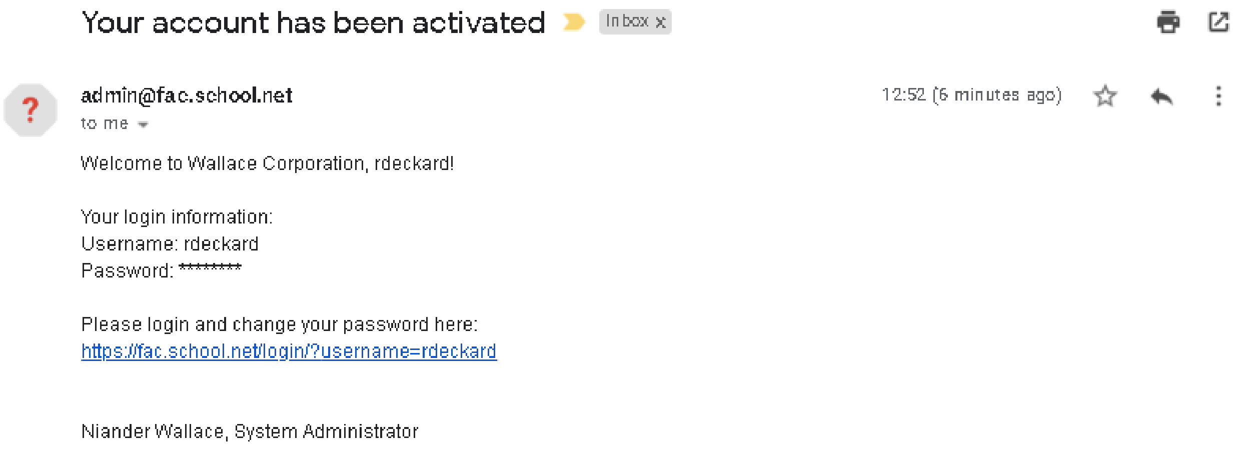
2. The user's registration is successful, and their information has been sent to the administrator for approval.



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.

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



Your account has been activated

admin@fac.school.net

to me

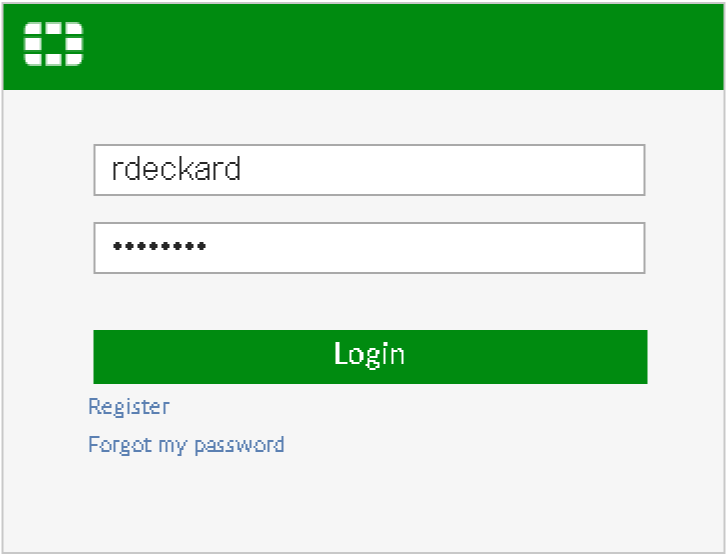
Welcome to Wallace Corporation, rdeckard!

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

Please login and change your password here:
https://fac.school.net/login/?username=rdeckard

Niander Wallace, System Administrator

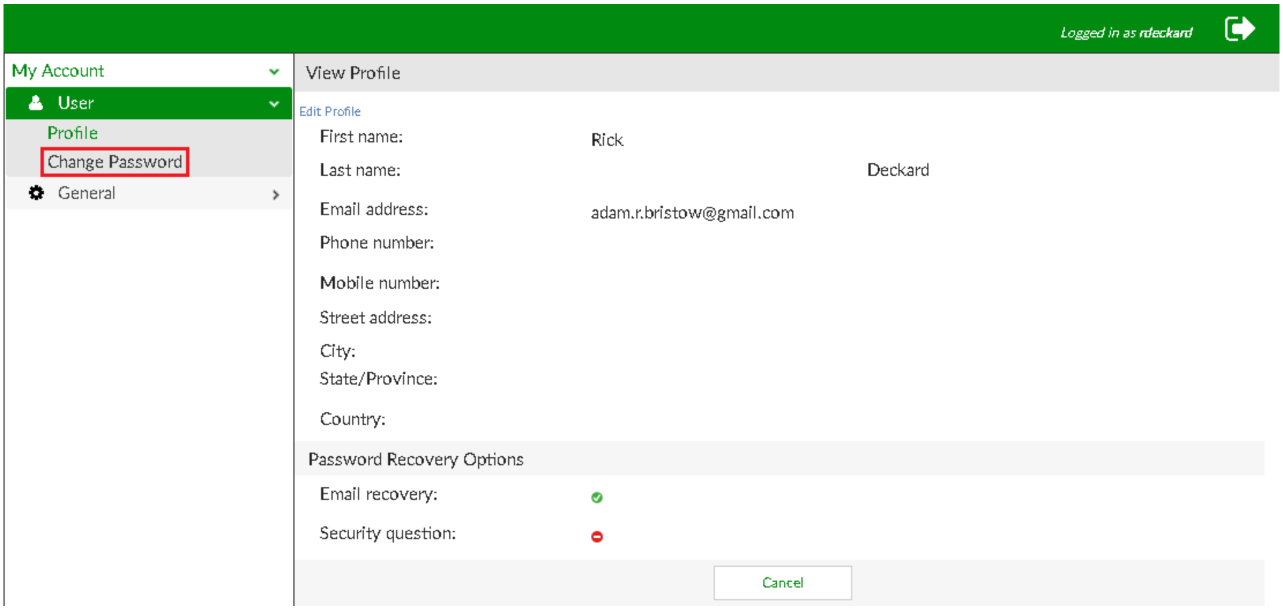
4. Select the link and log in to the user's portal.



rdeckard

•••••••••

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.



First name: Rick

Last name: Deckard

Email address: adam.r.bristow@gmail.com

Phone number:

Mobile number:

Street address:

City:

State/Province:

Country:

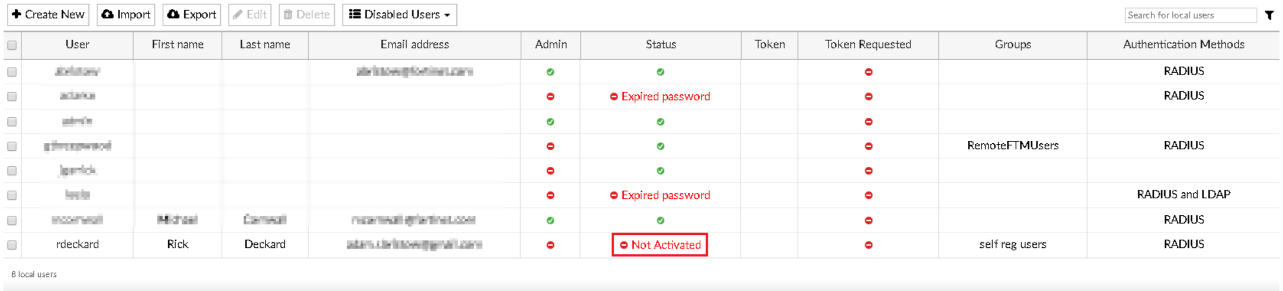
Password Recovery Options

Email recovery: ✓

Security question: ⊖

Results - Administrator approval

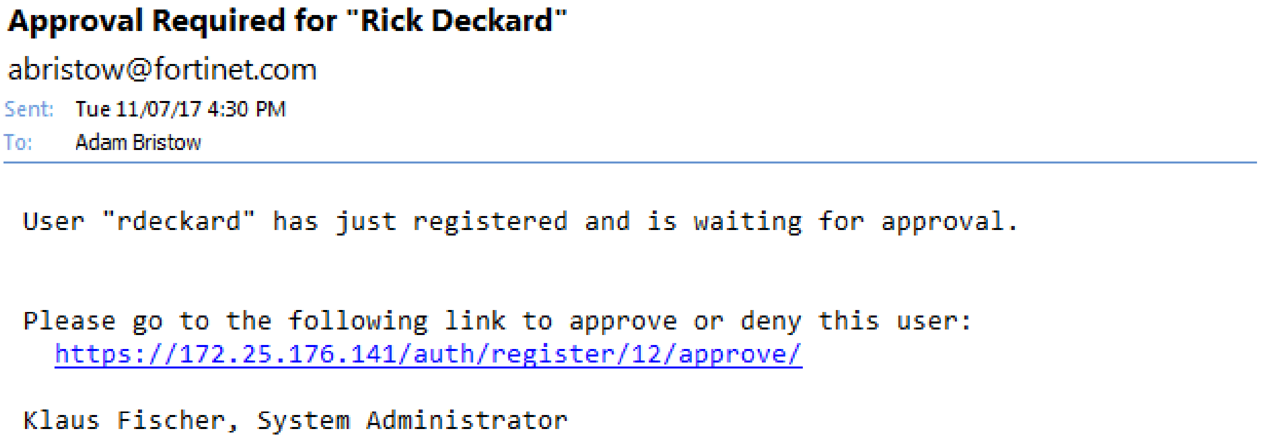
1. After receiving the user's registration request, in the FortiAuthenticator as the administrator, go to *Authentication > User Management > Local Users*. The user has been added, but their *Status* is listed as *Not Activated*.



□	User	First name	Last name	Email address	Admin	Status	Token	Token Requested	Groups	Authentication Methods
□	[redacted]			[redacted]	✓	✓		⊖		RADIUS
□	[redacted]				⊖	⊖ Expired password		⊖		RADIUS
□	[redacted]				✓	✓		⊖		
□	[redacted]				⊖	✓		⊖	RemoteFTMUsers	RADIUS
□	[redacted]				⊖	✓		⊖		
□	[redacted]				⊖	⊖ Expired password		⊖		RADIUS and LDAP
□	[redacted]	[redacted]	[redacted]	[redacted]	✓	✓		⊖		RADIUS
□	rdeckard	Rick	Deckard	[redacted]	⊖	⊖ Not Activated		⊖	self reg users	RADIUS

8 local users

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



Approval Required for "Rick Deckard"

abristow@fortinet.com

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

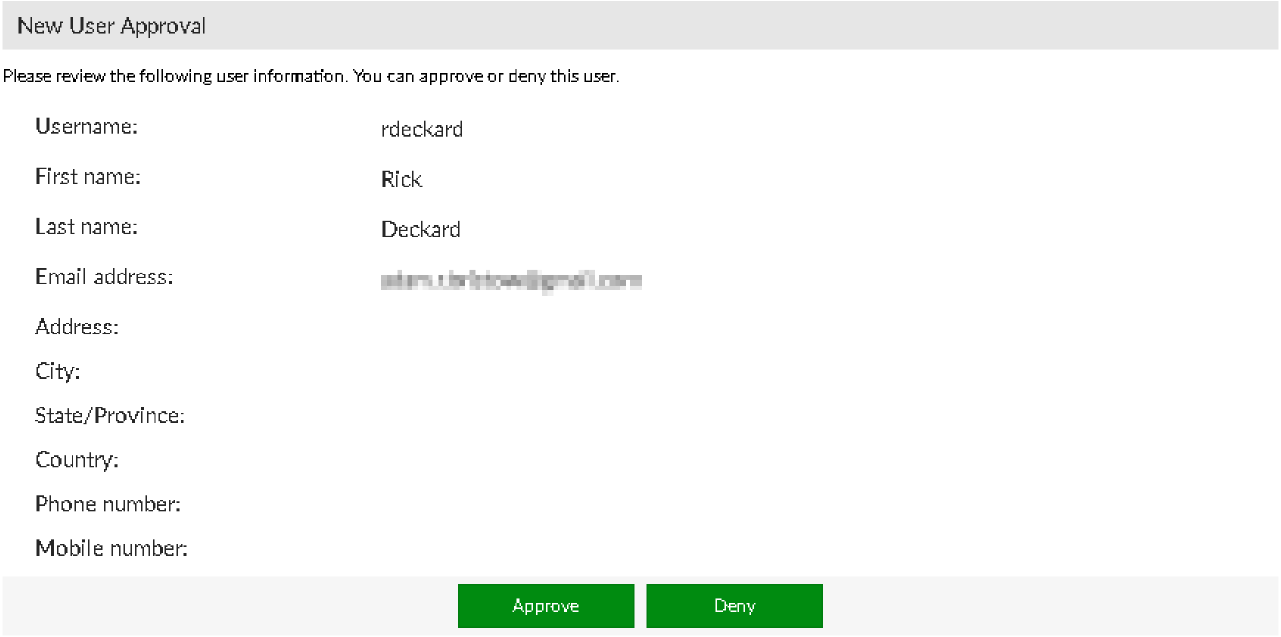
To: Adam Bristow

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

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

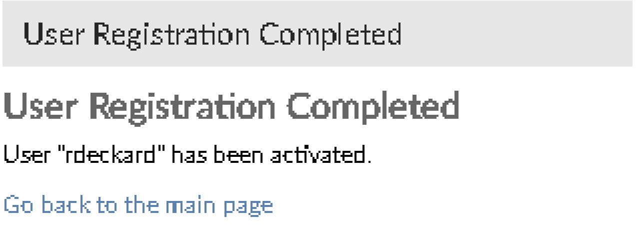


New User Approval

Please review the following user information. You can approve or deny this user.

Username:	rdeckard
First name:	Rick
Last name:	Deckard
Email address:	[redacted]
Address:	
City:	
State/Province:	
Country:	
Phone number:	
Mobile number:	

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



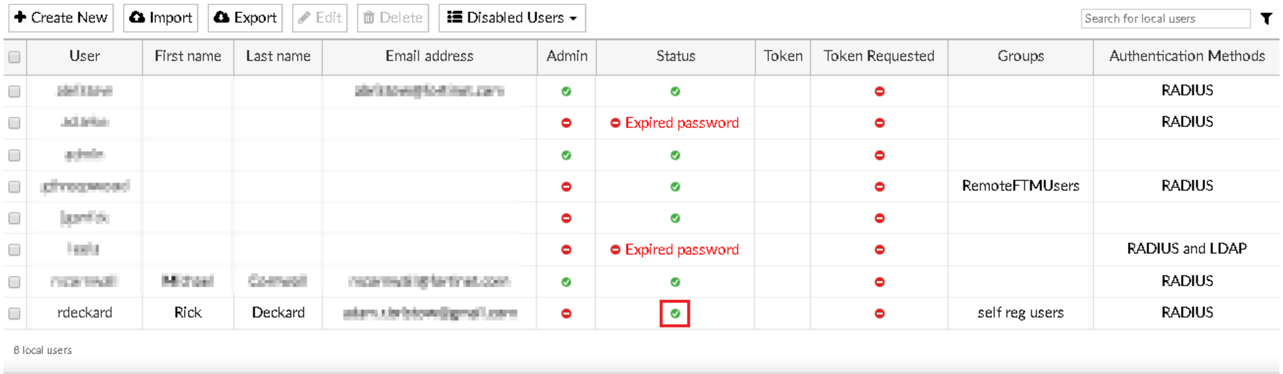
User Registration Completed

User Registration Completed

User "rdeckard" has been activated.

Go back to the main page

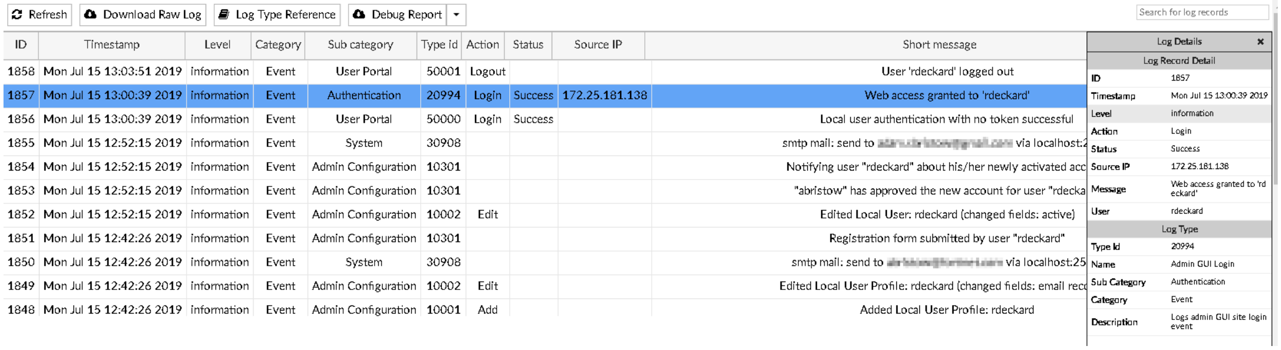
This can be confirmed by going back to *Authentication* > *User Management* > *Local Users*. The user's **Status** has changed to **Enabled**.



□	User	First name	Last name	Email address	Admin	Status	Token	Token Requested	Groups	Authentication Methods
□	[redacted]			[redacted]	✓	✓		⊖		RADIUS
□	[redacted]				⊖	⊖ Expired password		⊖		RADIUS
□	[redacted]				✓	✓		⊖		
□	[redacted]				⊖	✓		⊖	RemoteFTMUsers	RADIUS
□	[redacted]				⊖	✓		⊖		
□	[redacted]				⊖	⊖ Expired password		⊖		RADIUS and LDAP
□	[redacted]	[redacted]	[redacted]	[redacted]	✓	✓		⊖		RADIUS
□	rdeckard	Rick	Deckard	[redacted]	⊖	✓		⊖	self reg users	RADIUS

8 local users

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



ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message
1858	Mon Jul 15 13:03:51 2019	information	Event	User Portal	50001	Logout			User 'rdeckard' logged out
1857	Mon Jul 15 13:00:39 2019	information	Event	Authentication	20994	Login	Success	172.25.181.138	Web access granted to 'rdeckard'
1856	Mon Jul 15 13:00:39 2019	information	Event	User Portal	50000	Login	Success		Local user authentication with no token successful
1855	Mon Jul 15 12:52:15 2019	information	Event	System	30908				smtp mail: send to [redacted] via localhost:2
1854	Mon Jul 15 12:52:15 2019	information	Event	Admin Configuration	10301				Notifying user "rdeckard" about his/her newly activated acc
1853	Mon Jul 15 12:52:15 2019	information	Event	Admin Configuration	10301				"abristow" has approved the new account for user "rdecka
1852	Mon Jul 15 12:52:15 2019	information	Event	Admin Configuration	10002	Edit			Edited Local User: rdeckard (changed fields: active)
1851	Mon Jul 15 12:42:26 2019	information	Event	Admin Configuration	10301				Registration form submitted by user "rdeckard"
1850	Mon Jul 15 12:42:26 2019	information	Event	System	30908				smtp mail: send to [redacted] via localhost:25
1849	Mon Jul 15 12:42:26 2019	information	Event	Admin Configuration	10002	Edit			Edited Local User Profile: rdeckard (changed fields: email recı
1848	Mon Jul 15 12:42:26 2019	information	Event	Admin Configuration	10001	Add			Added Local User Profile: rdeckard

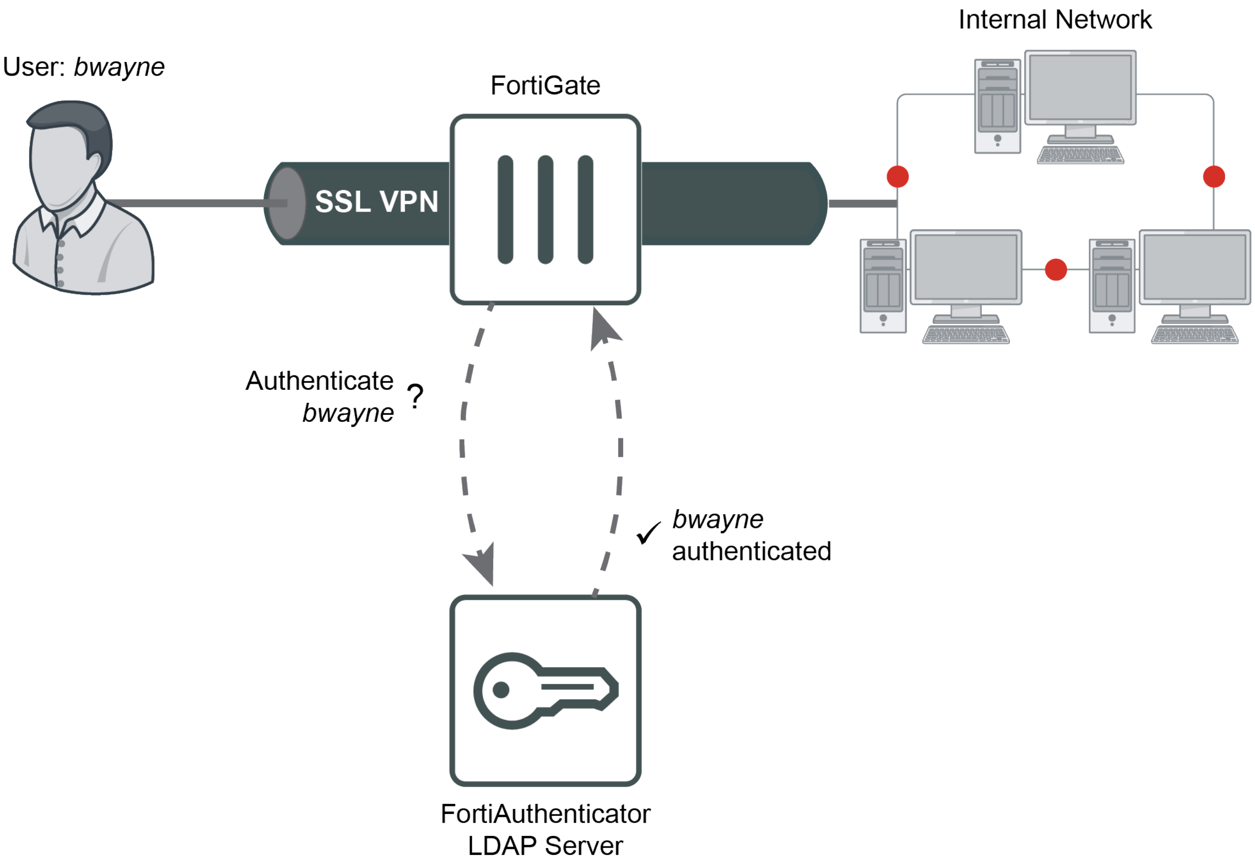
Log Details

Log Record Detail	
ID	1857
Timestamp	Mon Jul 15 13:00:39 2019
Level	information
Action	Login
Status	Success
Source IP	172.25.181.138
Message	Web access granted to 'rdeckard'
User	rdeckard
Log Type	
Type Id	20994
Name	Admin GUI Login
Sub Category	Authentication
Category	Event
Description	Logs admin GUI site login event

VPNs

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

LDAP authentication for SSL VPN with FortiAuthenticator



This recipe describes how to set up FortiAuthenticator to function as an LDAP server for FortiGate SSL VPN authentication. It involves adding users to FortiAuthenticator, setting up the LDAP server on the FortiAuthenticator, and then configuring the FortiGate to use the FortiAuthenticator as an LDAP server.

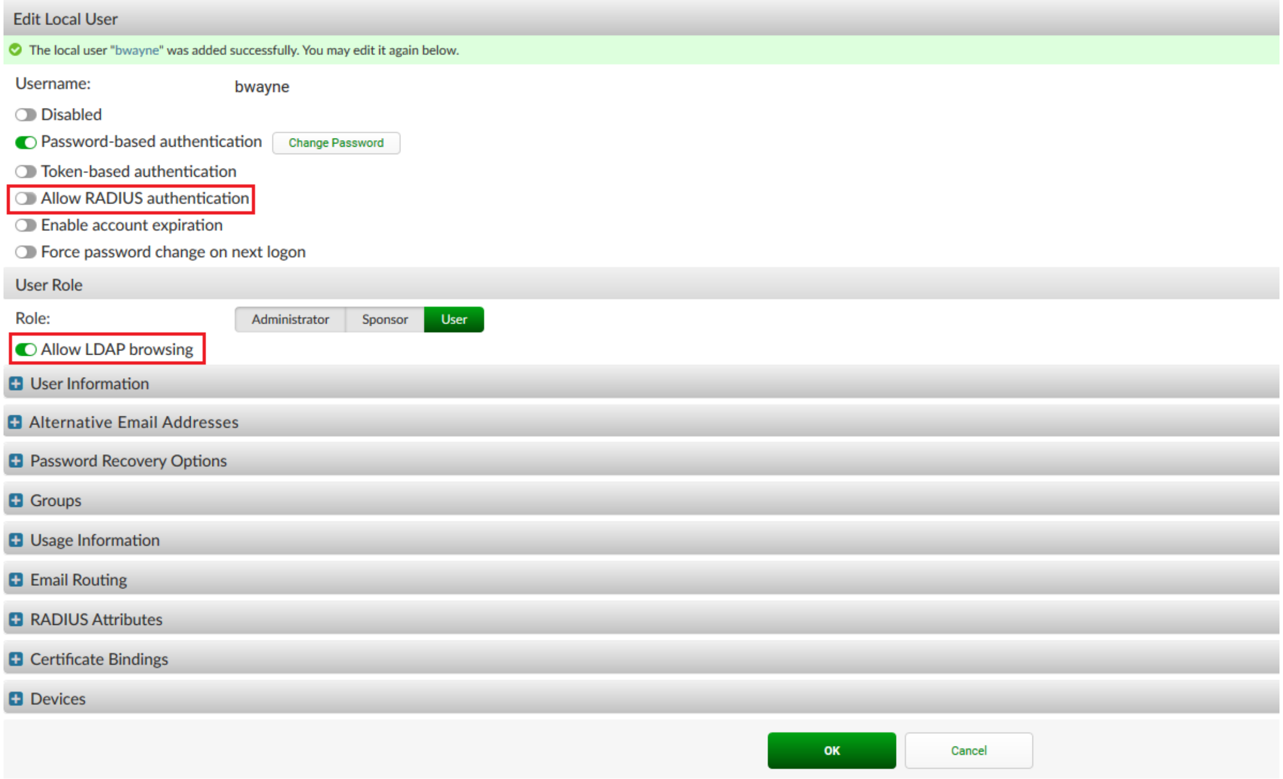
Creating the user and user group on the FortiAuthenticator

To create the user and user group:

1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users* and select *Create New*.
   Enter a name for the user, enter and confirm a password, and be sure to disable *Allow RADIUS authentication* — RADIUS authentication is not required for this recipe.

   Set *Role* as *User*, and select *OK*. New options will appear.

Make sure to enable *Allow LDAP browsing* — the user will not be able to connect to the FortiGate otherwise.



Edit Local User

The local user "bwayne" was added successfully. You may edit it again below.

Username: bwayne

○ Disabled

● Password-based authentication [Change Password]

○ Token-based authentication

○ Allow RADIUS authentication

○ Enable account expiration

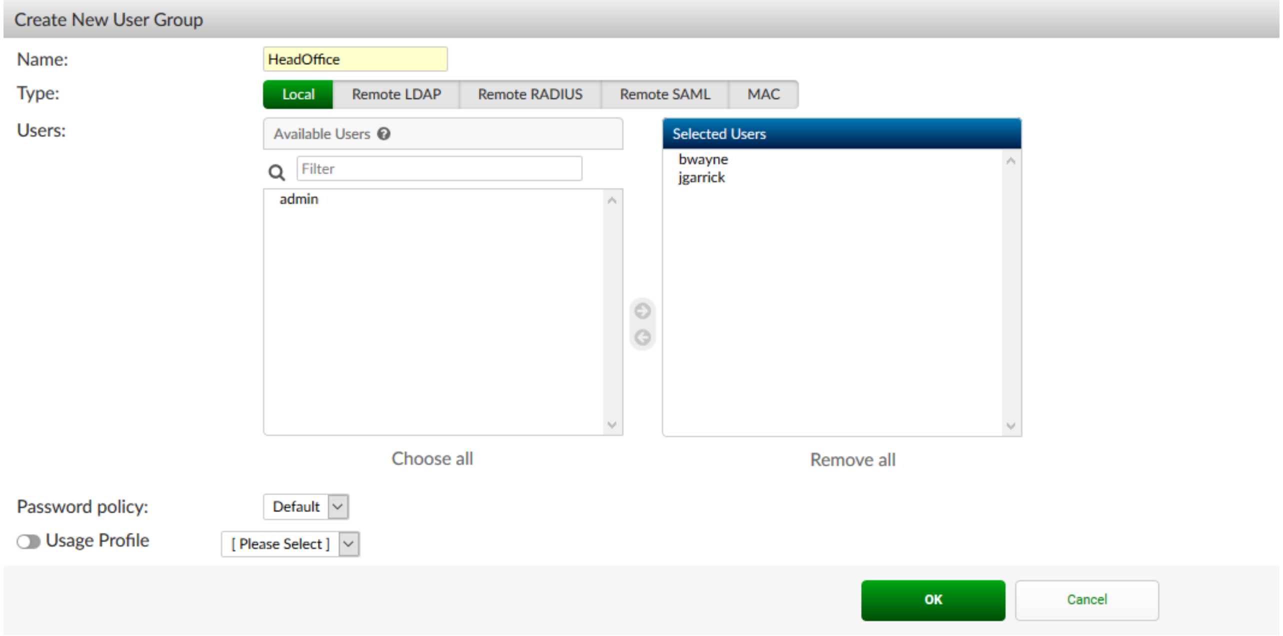
○ Force password change on next logon

User Role

Role: Administrator | Sponsor | [✓ User]

● Allow LDAP browsing

2. Create another user with the same settings. Later, you will use `jgarrick` on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use `bwayne` credentials to connect to the VPN tunnel.
3. Next go to *Authentication* > *User Management* > *User Groups*, and create a user group for the FortiGate users. Add the desired users to the group.



Create New User Group

Name: HeadOffice

Type: [✓ Local] | Remote LDAP | Remote RADIUS | Remote SAML | MAC

Users:

Available Users: admin

Selected Users: bwayne, jgarrick

Password policy: Default

○ Usage Profile [Please Select]

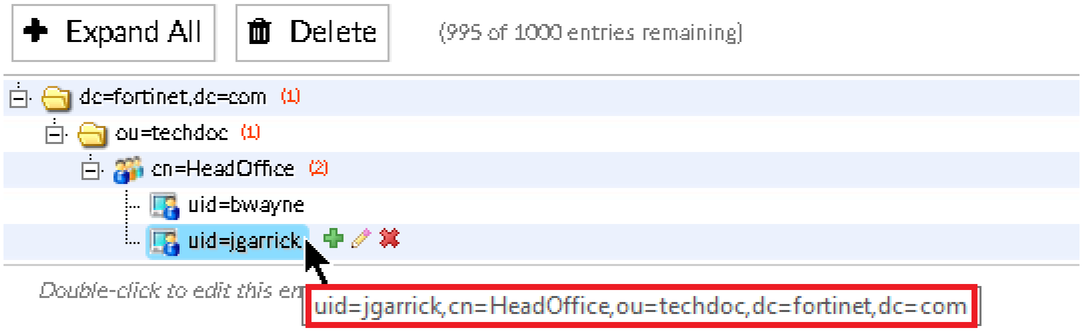
Creating the LDAP directory tree on the FortiAuthenticator

To create the LDAP directory tree:

1. Go to *Authentication* > *LDAP Service* > *Directory Tree*, and create a Distinguished Name (DN). A DN is made up of Domain Components (DC).
   Both the users and user group created earlier are the User ID (UID) and the Common Name (CN) in the LDAP Directory Tree.

   Create an Organizational Unit (OU), and a Common Name (CN). Under the *cn=HeadOffice* entry, add UIDs for the users.

   If you mouse over a user, you will see the full DN of the LDAP server.


Expand All
Delete
(995 of 1000 entries remaining)
dc=fortinet,dc=com (1)
ou=techdoc (1)
cn=HeadOffice (2)
uid=bwayne
uid=jgarrick
Double-click to edit this en
uid=jgarrick,cn=HeadOffice,ou=techdoc,dc=fortinet,dc=com

Later, you will use `jgarrick` on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use `bwayne` credentials to connect to the VPN tunnel.

Connecting the FortiGate to the LDAP server

To connect the FortiGate to the LDAP server:

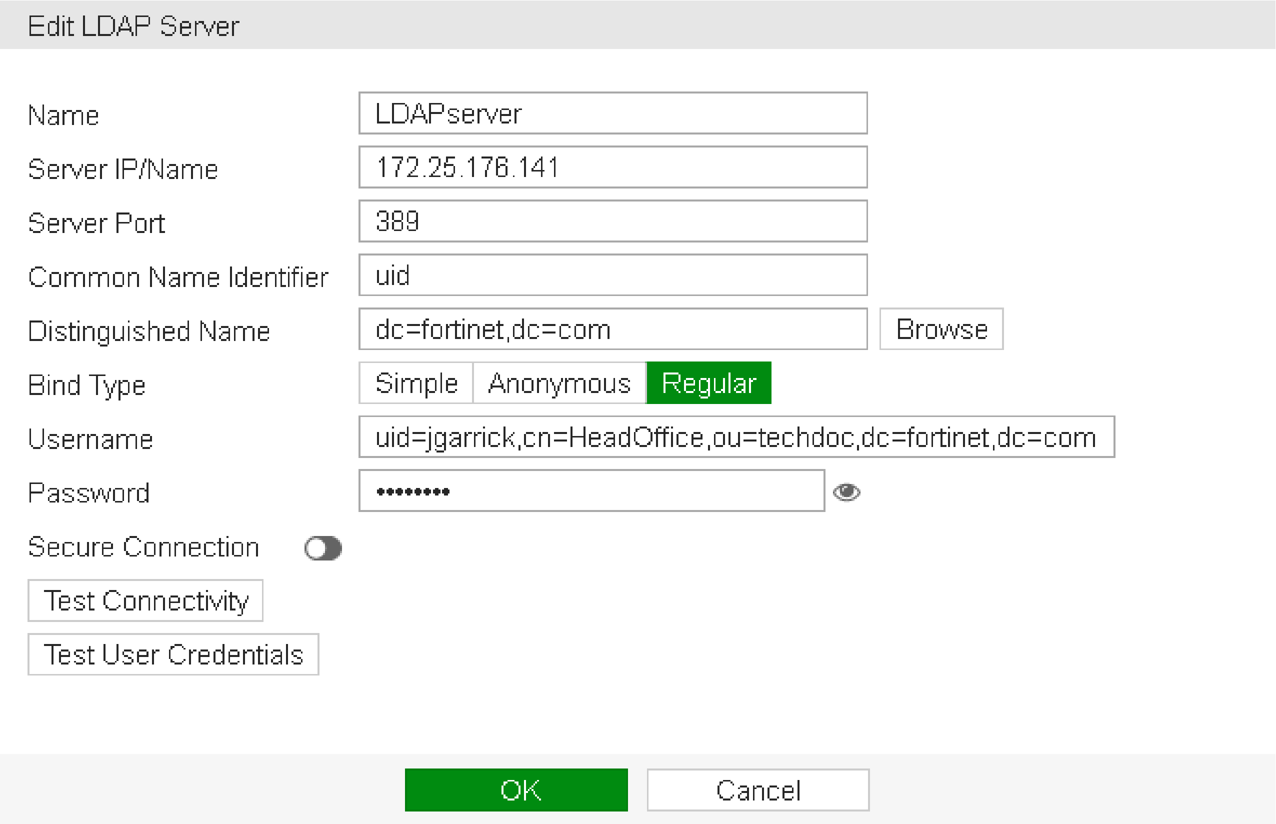
1. On the FortiGate, go to *User & Device* > *LDAP Servers*, and select *Create New*.
   Enter a name for the LDAP server connection.

   Set *Server IP/Name* to the IP of the FortiAuthenticator, and set the *Common Name Identifier* to *uid*.

   Set *Distinguished Name* to `dc=fortinet,dc=com`, and set the *Bind Type* to *Regular*.

   Enter the user DN for jgarrick of the LDAP server, and enter the user's *Password*.

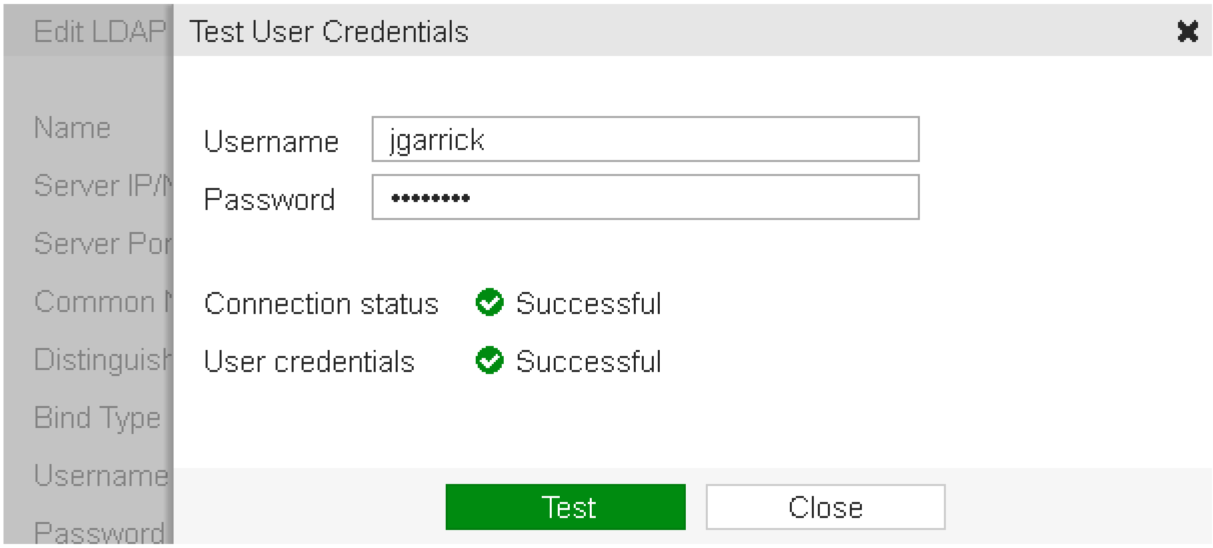
   The DN is an account that the FortiGate uses to query the LDAP server.



Edit LDAP Server

Name	LDAPserver
Server IP/Name	172.25.176.141
Server Port	389
Common Name Identifier	uid
Distinguished Name	dc=fortinet,dc=com
Bind Type	Simple Anonymous [✓ Regular]
Username	uid=jgarrick,cn=HeadOffice,ou=techdoc,dc=fortinet,dc=com
Password	•••••••••
Secure Connection	○

2. Select *Test Connectivity* to determine a successful connection.
Then select *Test User Credentials* to query the LDAP directory using jgarrick's credentials. The query is successful.



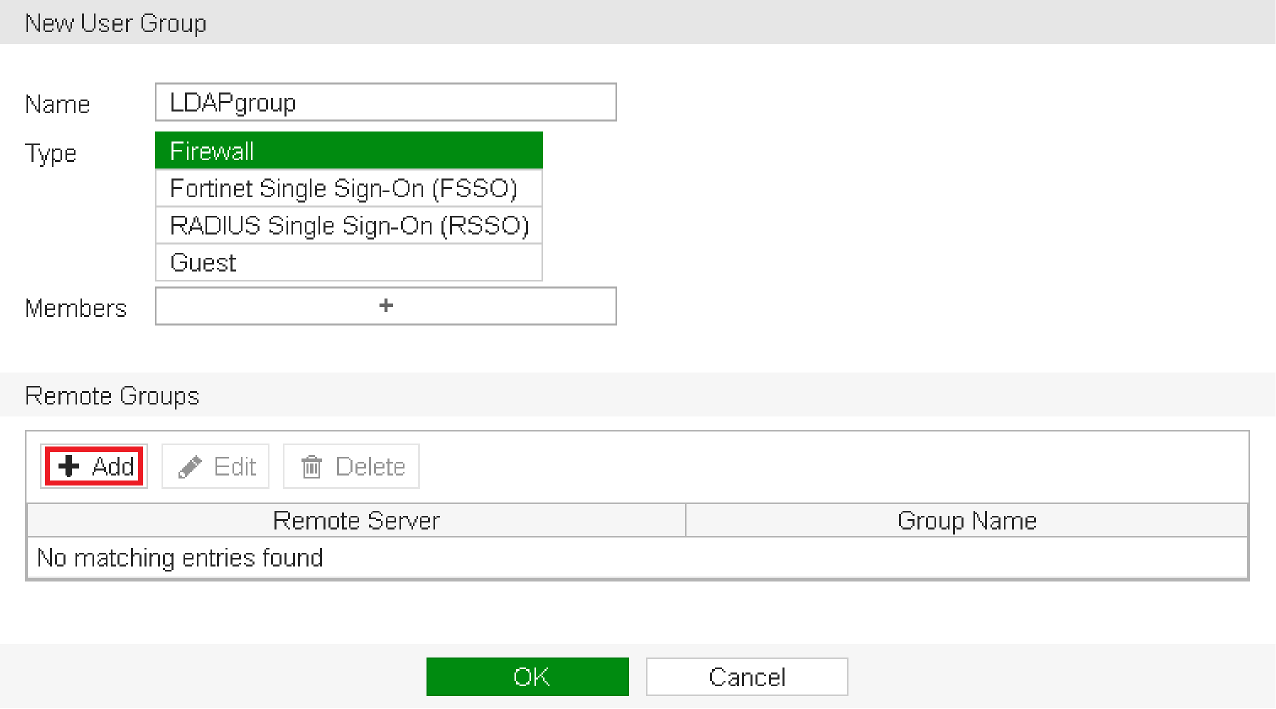
Test User Credentials

Username	jgarrick
Password	•••••••••
Connection status	✓ Successful
User credentials	✓ Successful

Creating the LDAP user group on the FortiGate

To create the LDAP user group:

1. Go to *User & Device > User Groups*, and select *Create New*.
Enter a name for the user group. Under *Remote Groups* select *Add*.



New User Group

Name: LDAPgroup

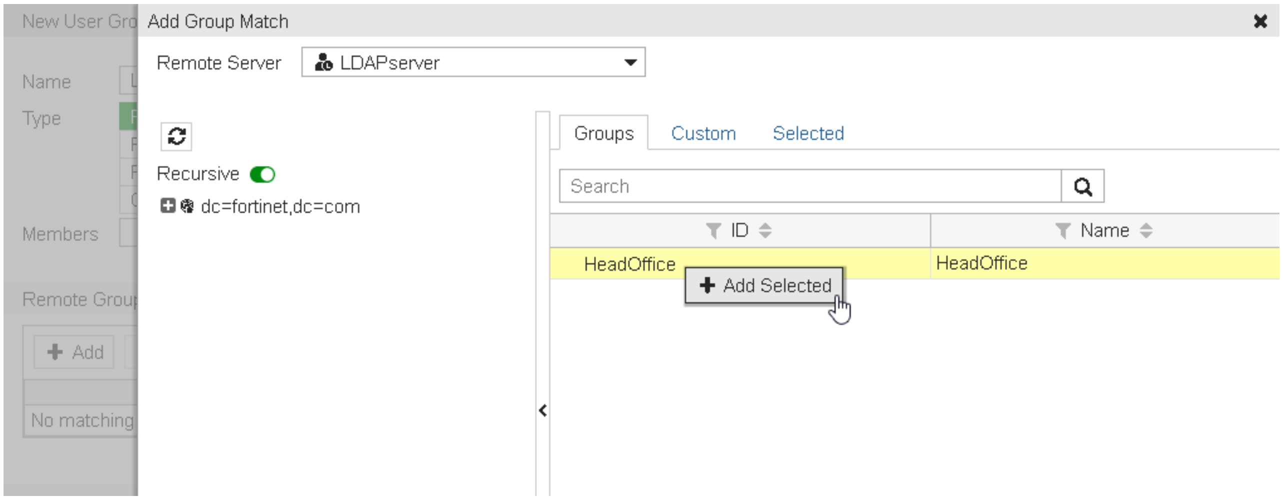
Type: Firewall | Fortinet Single Sign-On (FSSO) | RADIUS Single Sign-On (RSSO) | Guest

Members: +

Remote Groups

Remote Server	Group Name
No matching entries found	

2. Select *LDAPserver* under the *Remote Server* dropdown.
In the new *Add Group Match* window, right-click *HeadOffice* under the *Groups* tab, and select *Add Selected*. The group will be added to the *Selected* tab. Select *OK*.



Add Group Match

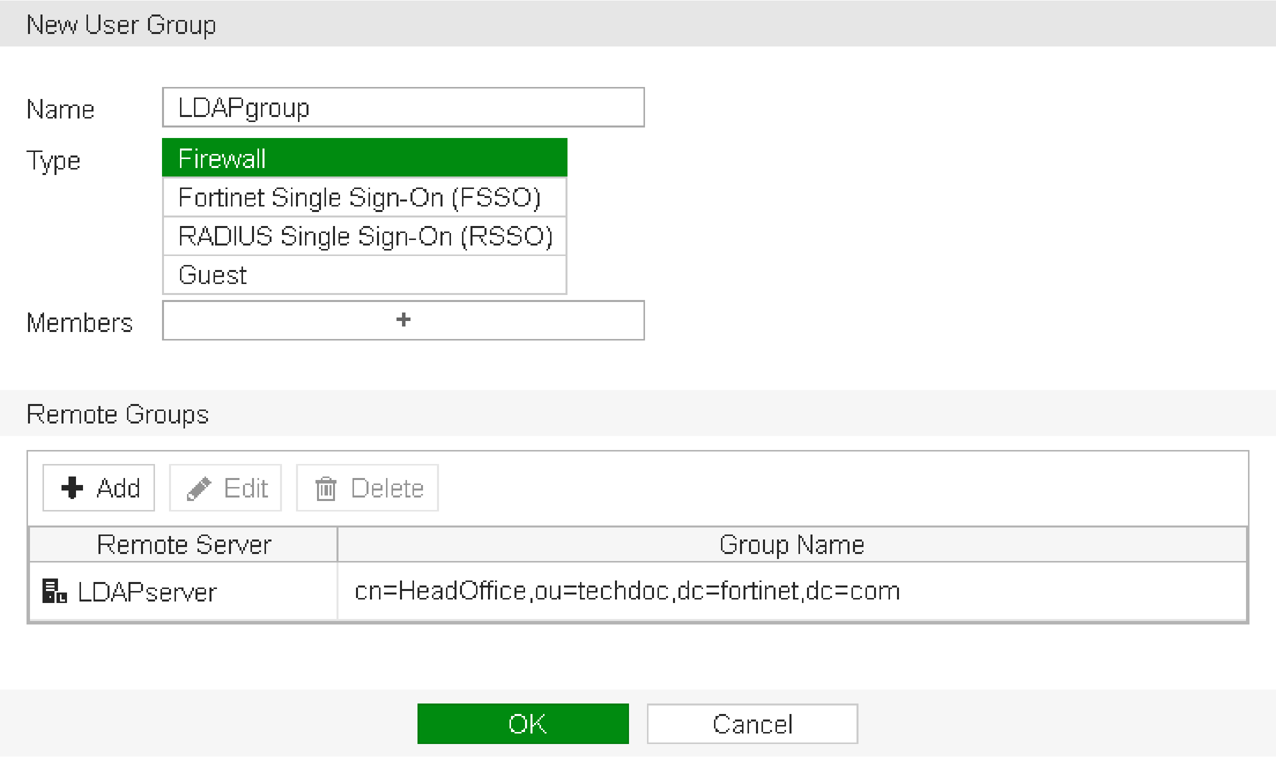
Remote Server: LDAPserver

Recursive

dc=fortinet,dc=com

ID	Name
HeadOffice	HeadOffice

3. *LDAPserver* has been added to the LDAP group. Select *OK*.



New User Group

Name: LDAPgroup

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

Members: +

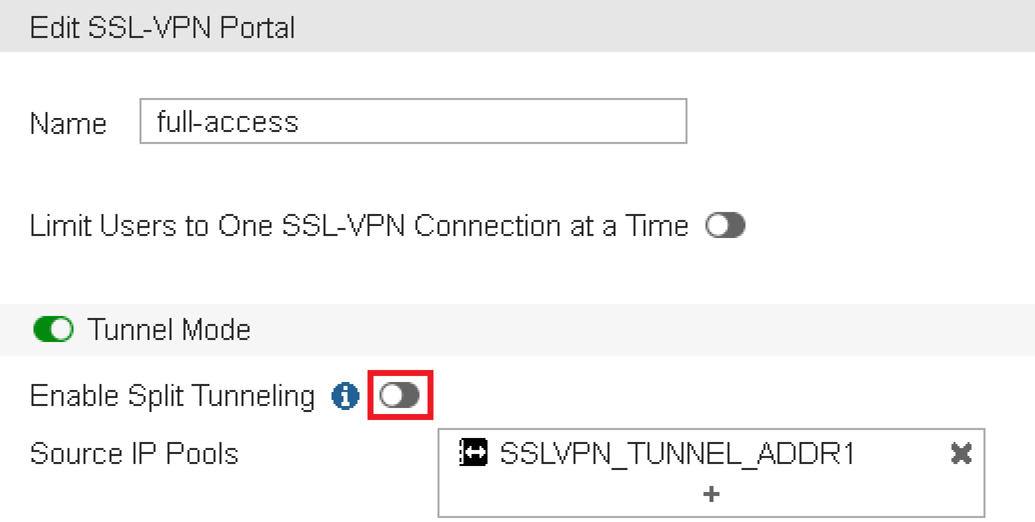
Remote Groups

Remote Server	Group Name
LDAPserver	cn=HeadOffice,ou=techdoc,dc=fortinet,dc=com

Configuring the SSL-VPN

To configure the SSL-VPN:

1. On the FortiGate, go to *VPN > SSL-VPN Portals*, and edit the full-access portal. Disable *Split Tunneling*.



Edit SSL-VPN Portal

Name: full-access

Limit Users to One SSL-VPN Connection at a Time ○

● Tunnel Mode

Enable Split Tunneling ○

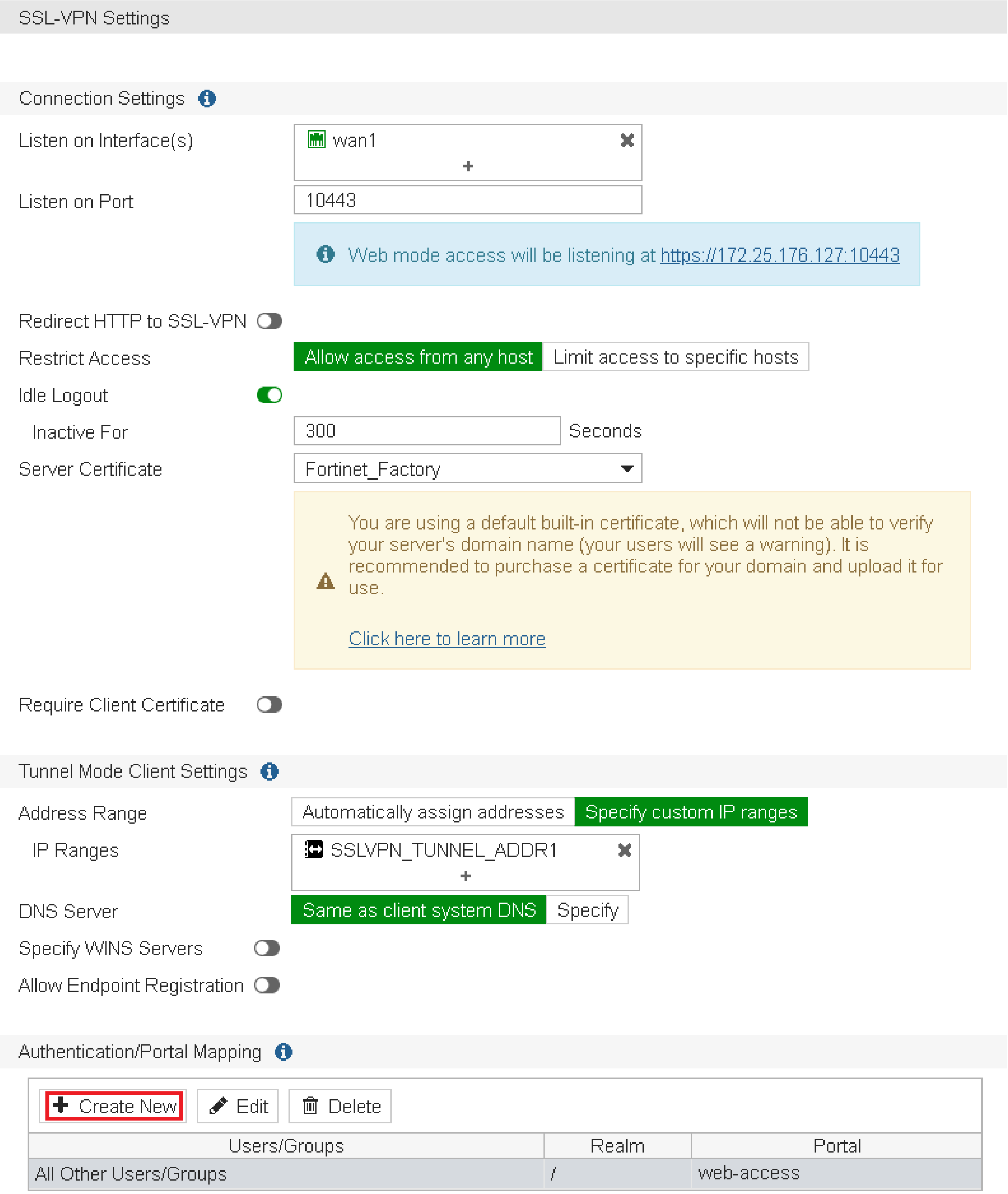
Source IP Pools: SSLVPN_TUNNEL_ADDR1 ✖ +

2. Go to *VPN > SSL-VPN Settings*.

Under *Connection Settings* set *Listen on Port* to `10443`.

Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set it to *SSLVPN_TUNNEL_ADDR1*.

Under *Authentication/Portal Mapping*, select *Create New*.



SSL-VPN Settings

Connection Settings

Listen on Interface(s): wan1

Listen on Port: 10443

Web mode access will be listening at https://172.25.176.127:10443

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

DNS Server: [✓ Same as client system DNS] Specify

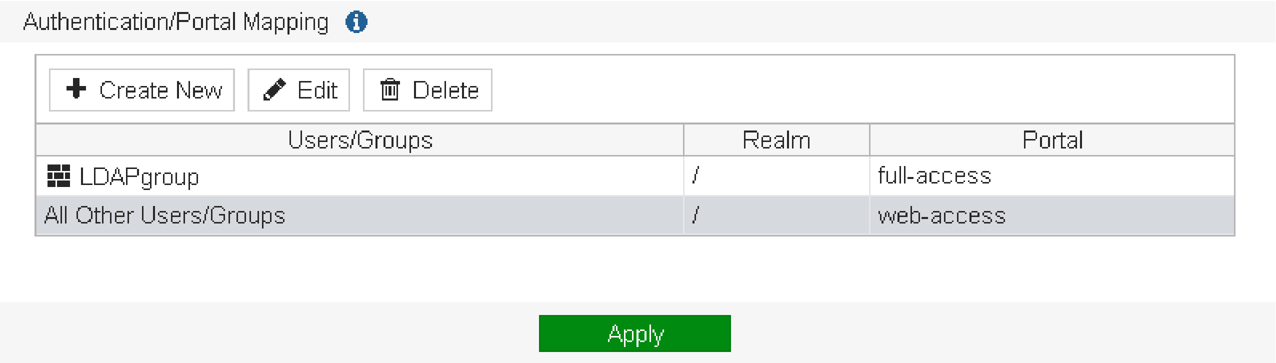
Specify WINS Servers: ○

Allow Endpoint Registration: ○

Authentication/Portal Mapping

Users/Groups	Realm	Portal
All Other Users/Groups	/	web-access

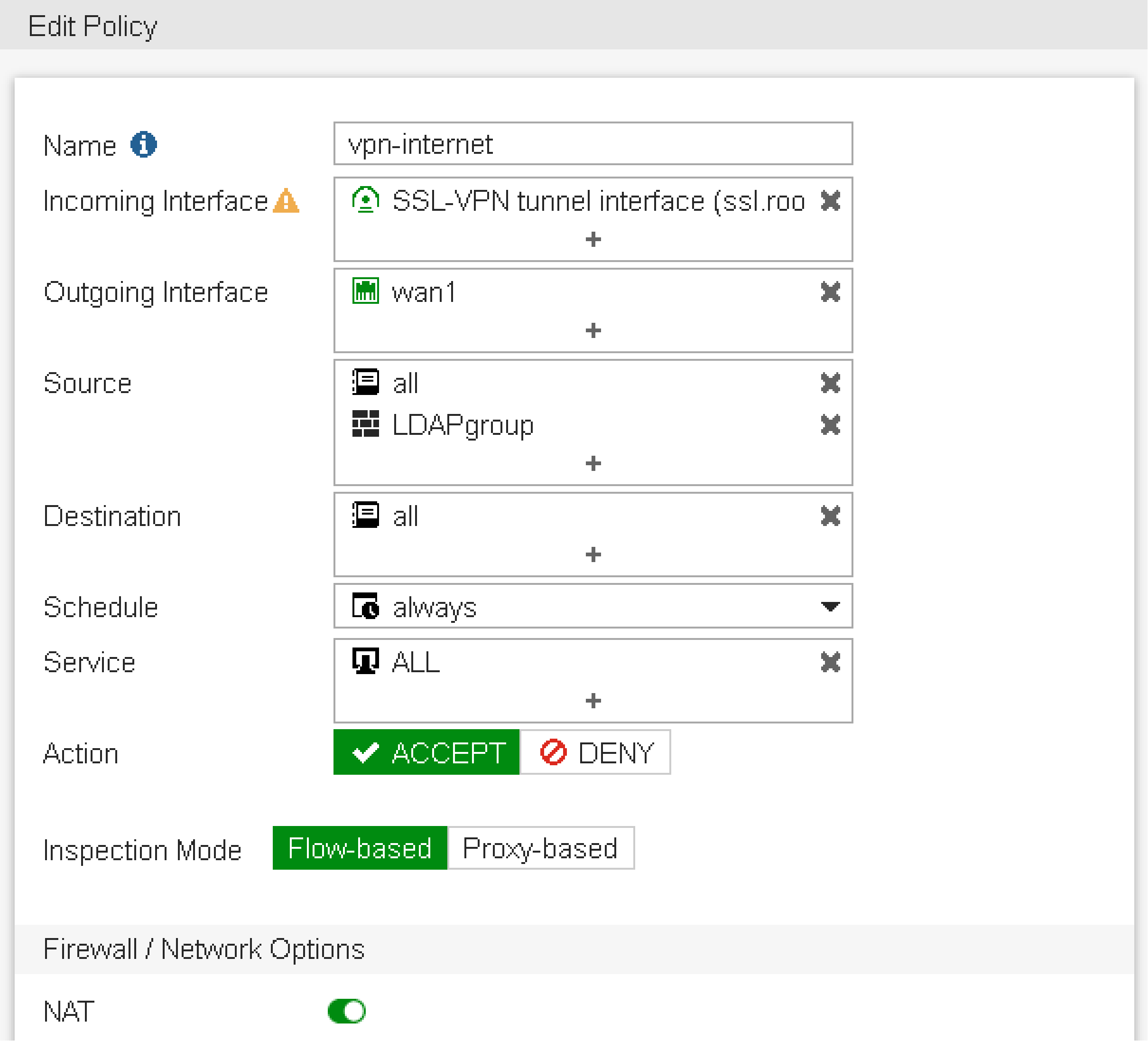
3. Assign the *LDAPgroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to the desired portal. Select *Apply*.



Authentication/Portal Mapping

Users/Groups	Realm	Portal
LDAPgroup	/	full-access
All Other Users/Groups	/	web-access

4. Select the prompt at the top of the screen to create a new SSL-VPN policy, including the *LDAPgroup*, as shown.



Edit Policy

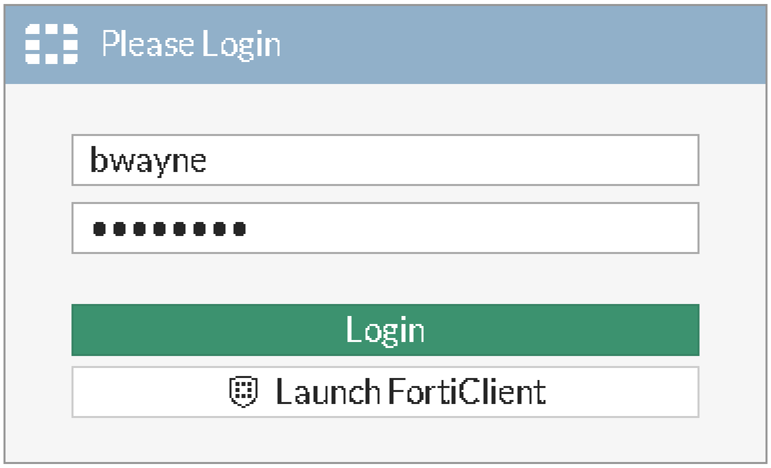
Name	vpn-internet
Incoming Interface	SSL-VPN tunnel interface (ssl.roo
Outgoing Interface	wan1
Source	all LDAPgroup
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT (selected) / DENY
Inspection Mode	Flow-based (selected) / Proxy-based

Firewall / Network Options

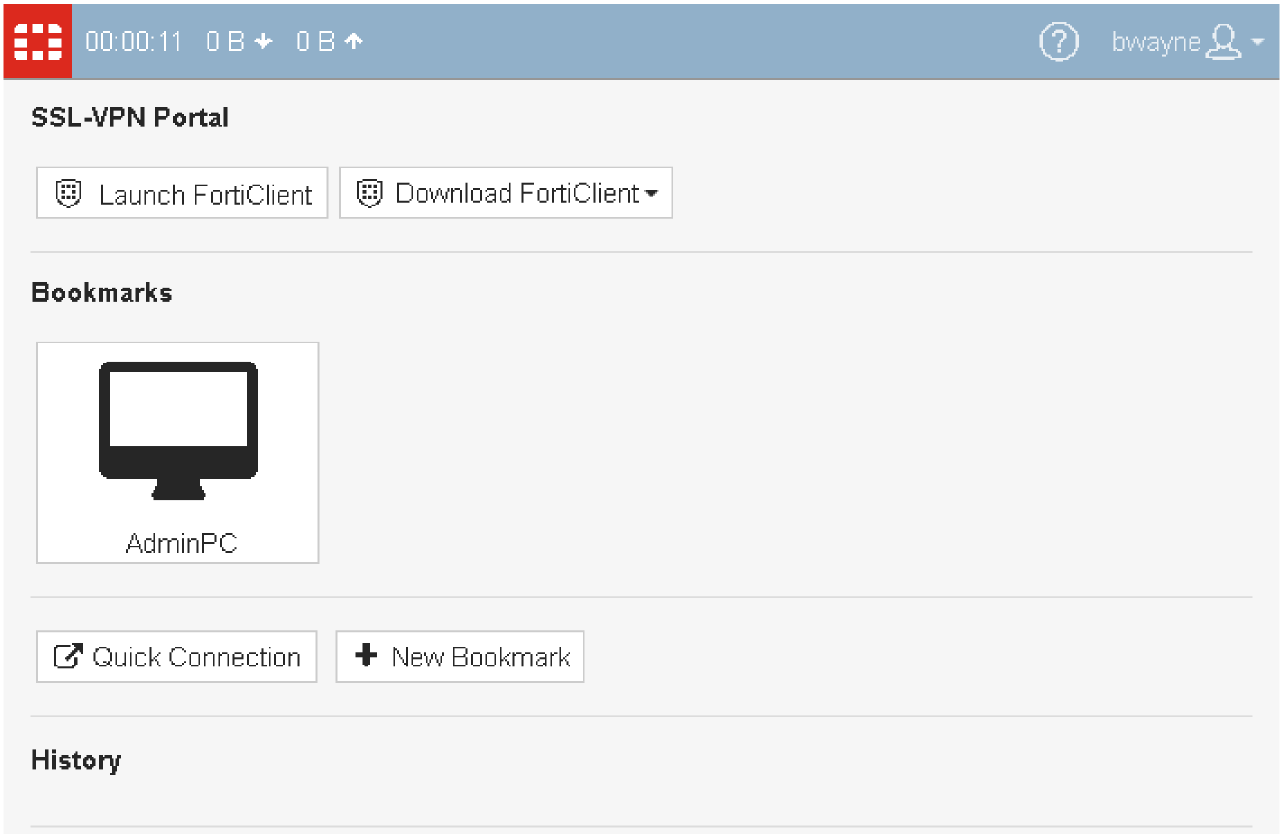
NAT ●

Results

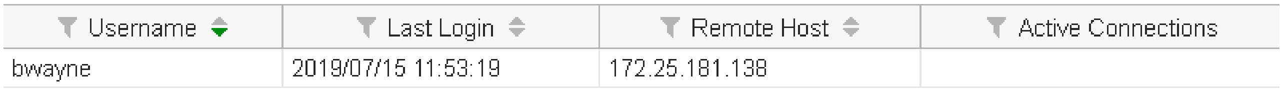
1. From a remote device, access the SSL VPN Web Portal.
   Enter valid LDAP credentials (in the example, bwayne).



2. The user is now successfully logged into the SSL VPN Portal.

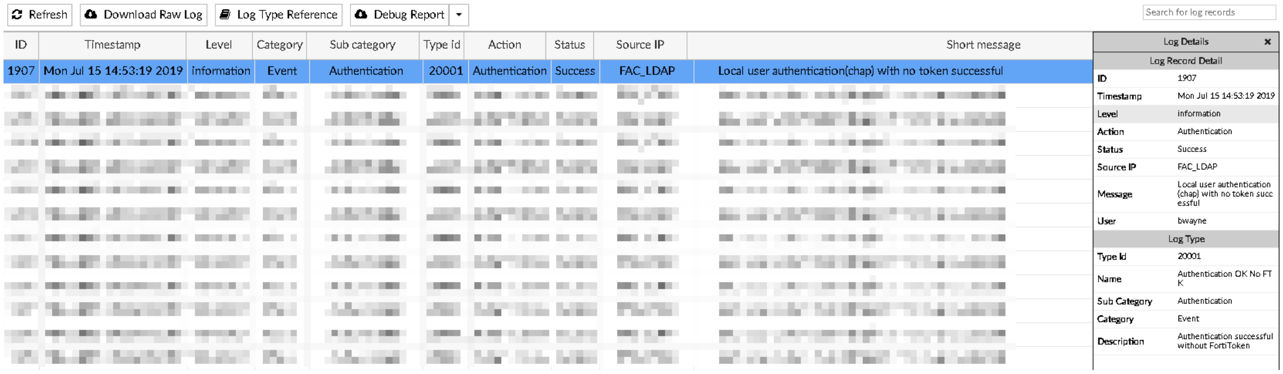


3. On the FortiGate, go to *Monitor* > *SSL-VPN Monitor* to confirm the connection.



Username	Last Login	Remote Host	Active Connections
bwayne	2019/07/15 11:53:19	172.25.181.138	

4. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* and confirm the connection.

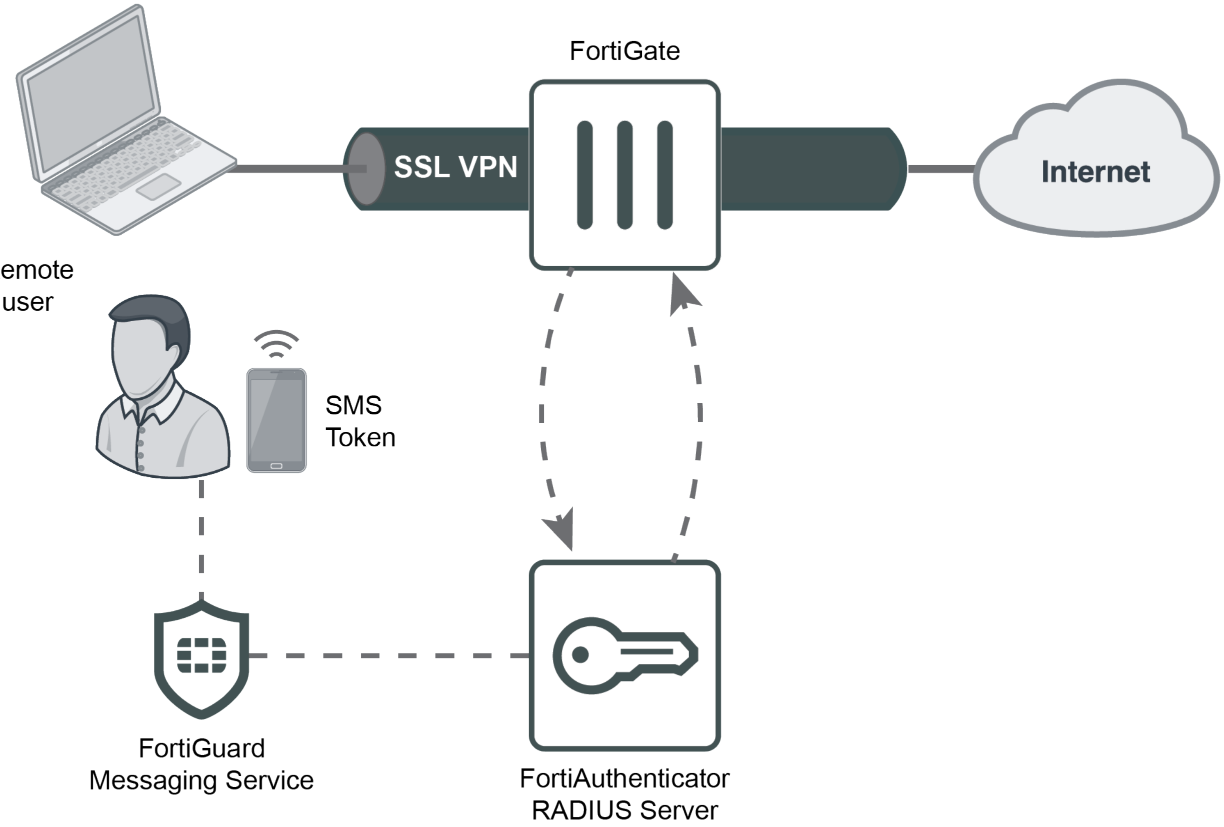


ID	Timestamp	Level	Category	Sub category	Type Id	Action	Status	Source IP	Short message
1907	Mon Jul 15 14:53:19 2019	information	Event	Authentication	20001	Authentication	Success	FAC_LDAP	Local user authentication(chap) with no token successful

Log Details

Log Record Detail	
ID	1907
Timestamp	Mon Jul 15 14:53:19 2019
Level	information
Action	Authentication
Status	Success
Source IP	FAC_LDAP
Message	Local user authentication (chap) with no token succ essful
User	bwayne
Log Type	
Type Id	20001
Name	Authentication OK No FT K
Sub Category	Authentication
Category	Event
Description	Authentication successful without FortiToken

SMS two-factor authentication for SSL VPN


FortiGate
SSL VPN
Internet
Remote user
SMS Token
FortiGuard Messaging Service
FortiAuthenticator RADIUS Server

In this recipe, you will create an SSL VPN with two-factor authentication consisting of a username, password, and an SMS token.

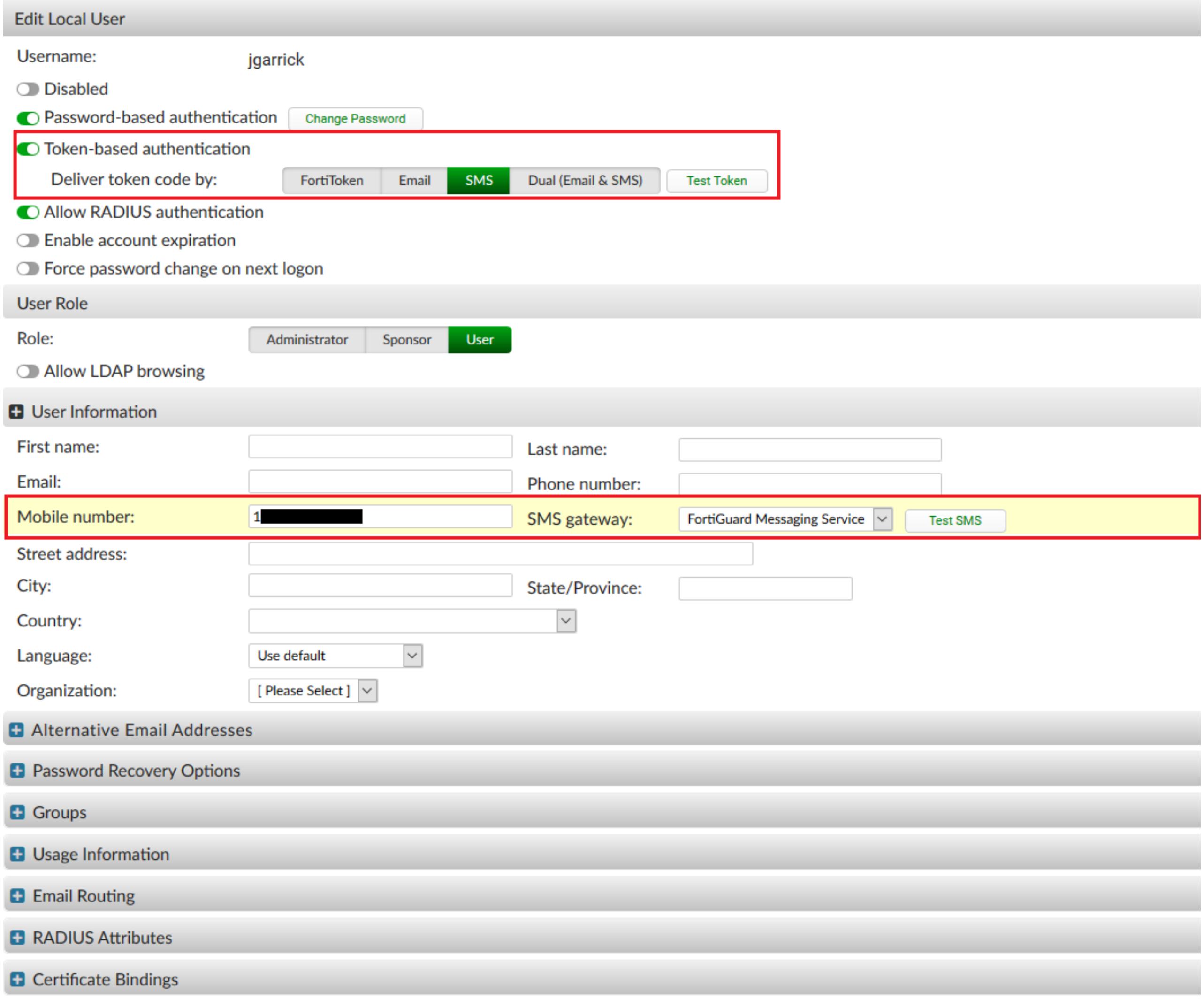
When a user attempts to connect to this SSL VPN, they are prompted to enter their username and password. After successfully entering their credentials, they receive an SMS message on their mobile phone containing a 6-digit number (called the FortiToken code). They must also enter this number to get access to the internal network and the Internet.

Although this recipe uses the FortiGuard Messaging Service, it will also work with any compatible SMS service you configure as an SMS Gateway.

Creating an SMS user and user group on the FortiAuthenticator

To create an SMS user and user group:

1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users* and add/modify a user to include *SMS Token-based authentication* and a *Mobile number* using the preferred *SMS gateway* as shown.
   The *Mobile number* must be in the following format:
   `+[international-number]`
   Enable *Allow RADIUS authentication*.



Edit Local User

Username: jgarrick

○ Disabled

● Password-based authentication

● Token-based authentication

Deliver token code by: FortiToken | Email | [✓ SMS] | Dual (Email & SMS)

● Allow RADIUS authentication

○ Enable account expiration

○ Force password change on next logon

User Role

Role: Administrator | Sponsor | [✓ User]

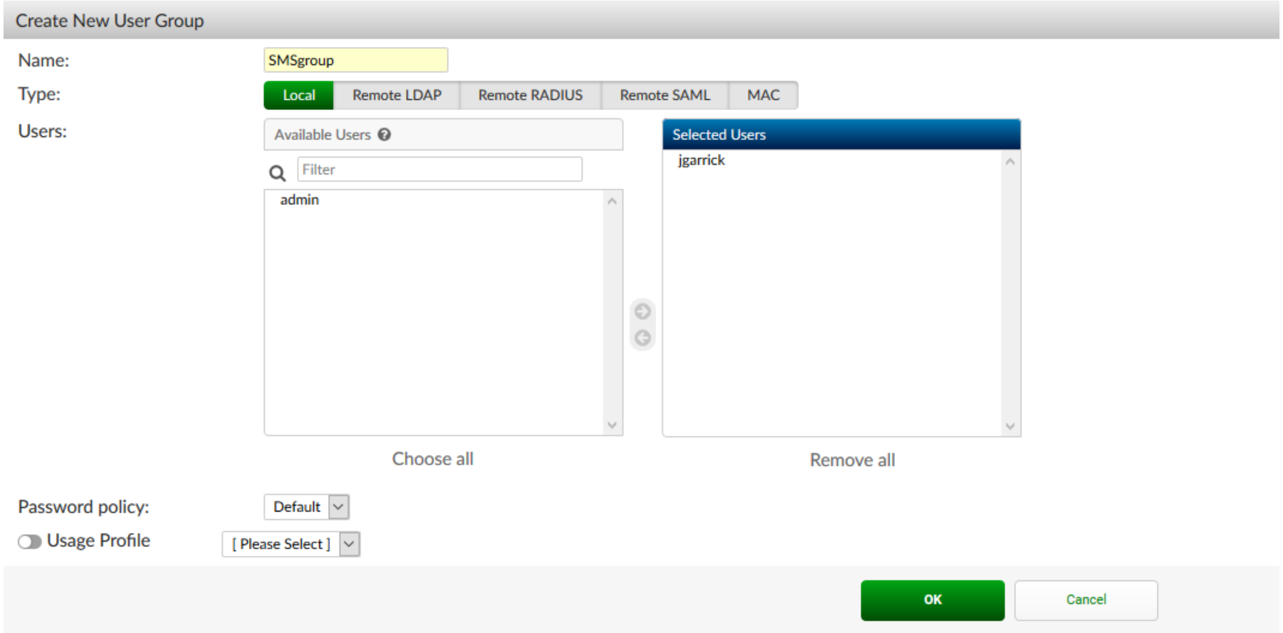
○ Allow LDAP browsing

User Information

First name:		Last name:	
Email:		Phone number:	
Mobile number:	1[redacted]	SMS gateway:	FortiGuard Messaging Service
Street address:			
City:		State/Province:	
Country:			
Language:	Use default		
Organization:	[Please Select]		

2. Go to *Authentication* > *User Management* > *User Groups* and add the above user to a new SMS user group (in the

example, *SMSgroup*).



Create New User Group

Name: SMSgroup

Type: Local

Users:

Selected Users: jgarrick

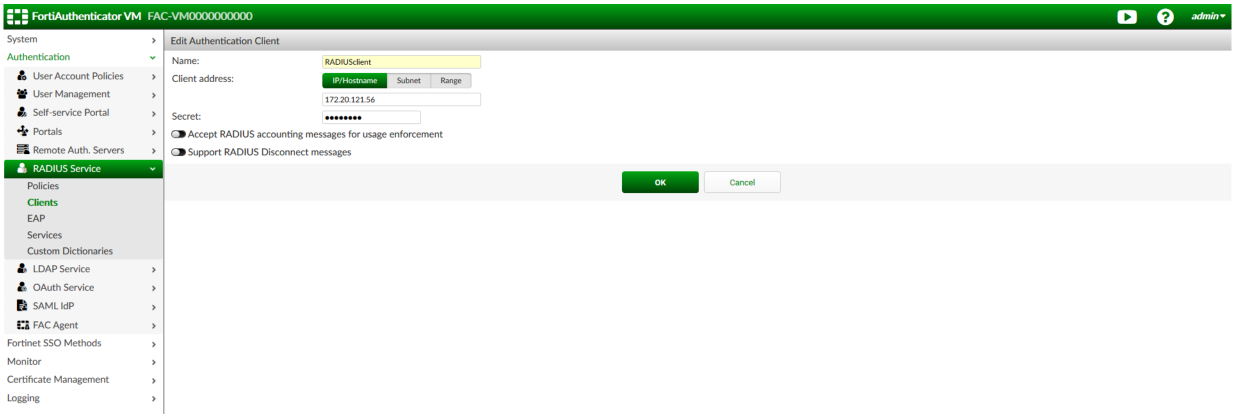
Password policy: Default

Usage Profile: [Please Select]

Configuring the FortiAuthenticator RADIUS client

To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, 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. Click *OK*.



Edit Authentication Client

Name: RADIUSclient

Client address: IP/Hostname

172.20.121.56

Secret: ●●●●●●●●●

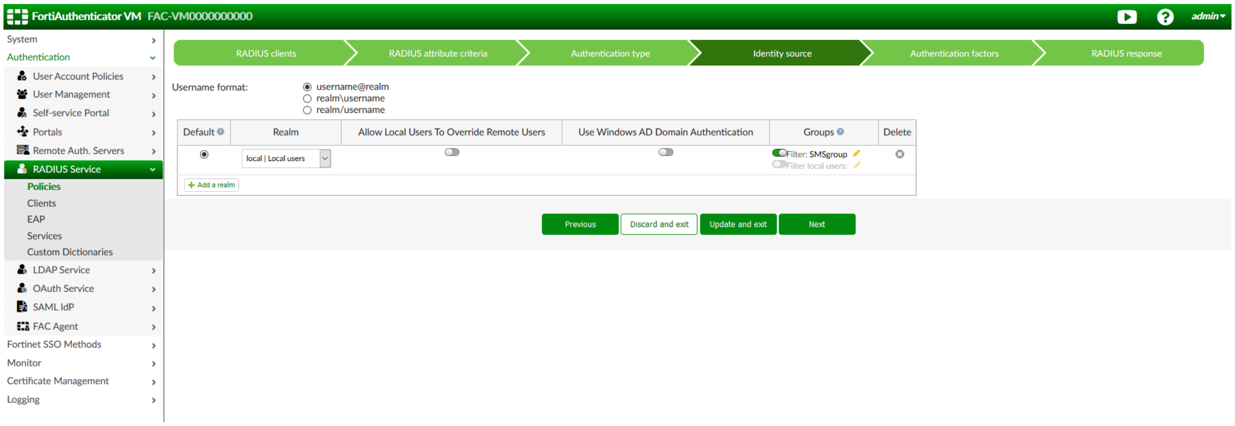
Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Optionally, configure RADIUS attribute criteria.
4. Choose *Password/OTP* authentication as the authentication type.

5. Choose a username format (in this example: *username@realm*), select the *Local* realm, and add the *SMSgroup* as a filter.



Username format:
● username@realm
○ realm\username
○ realm/username

Default	Realm	Allow Local Users To Override Remote Users	Use Windows AD Domain Authentication	Groups	Delete
●	local | Local users			Filter: SMSgroup Filter local users:	

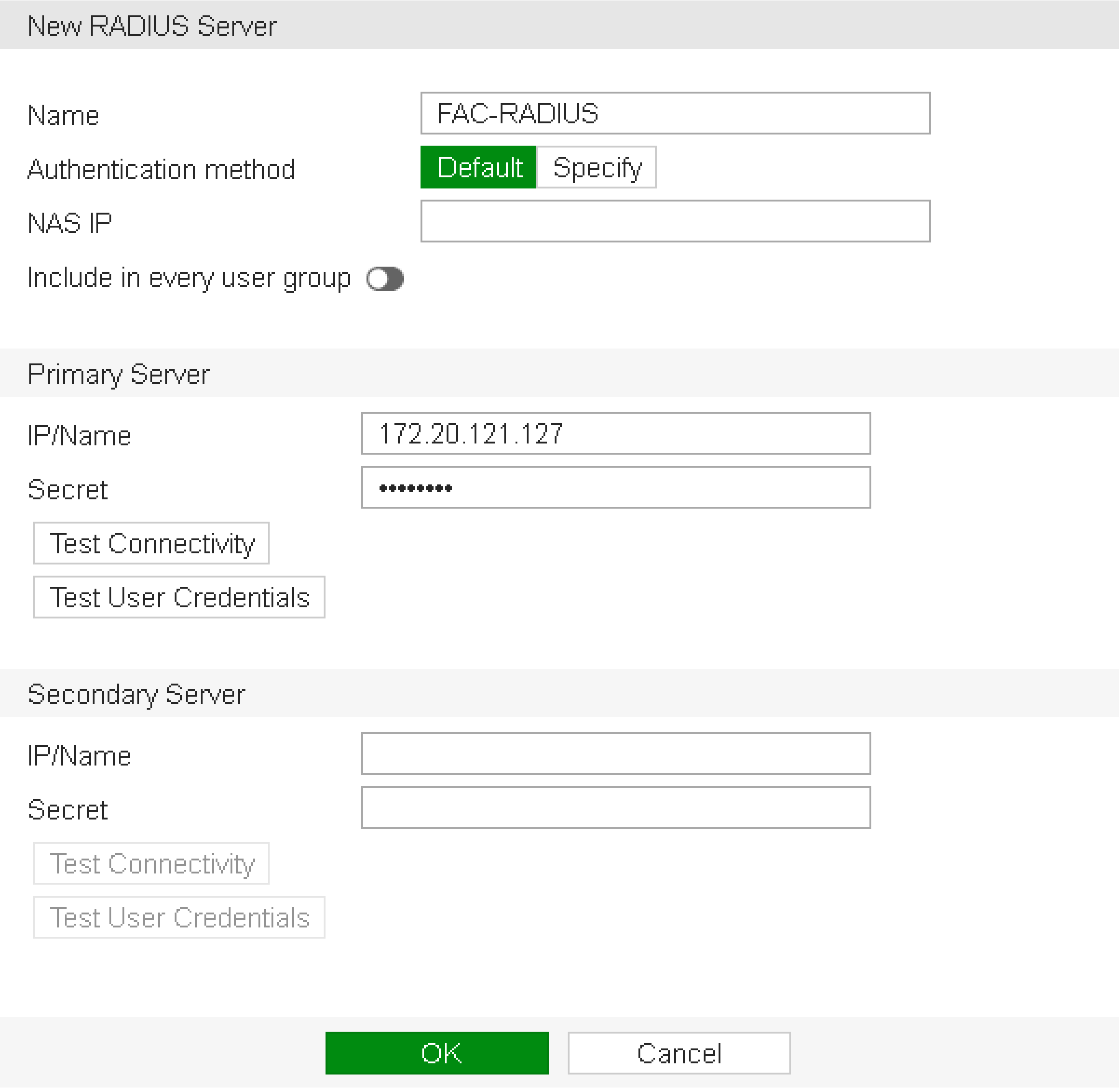
+ Add a realm

6. Set the authentication method to *Mandatory two-factor authentication*.
7. Click *Save and Exit*.

Configuring the FortiGate authentication settings

To configure 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 address and pre-shared secret.
   Use *Test Connectivity* to make sure that the FortiGate can communicate with the FortiAuthenticator.



New RADIUS Server

Name	FAC-RADIUS
Authentication method	Default Specify
NAS IP	
Include in every user group	

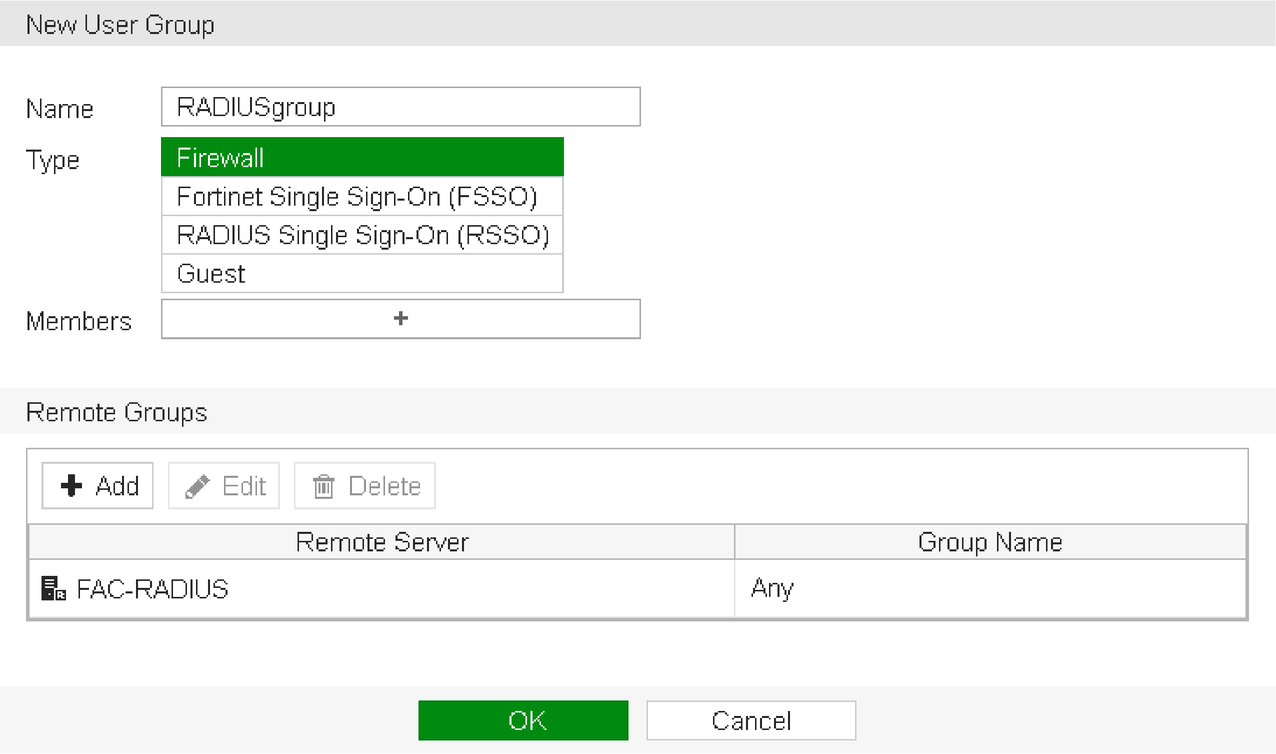
Primary Server

IP/Name	172.20.121.127
Secret	•••••••••

Secondary Server

IP/Name	
Secret	

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



New User Group

Name	RADIUSgroup
Type	Firewall Fortinet Single Sign-On (FSSO) RADIUS Single Sign-On (RSSO) Guest
Members	+

Remote Groups

Remote Server	Group Name
FAC-RADIUS	Any

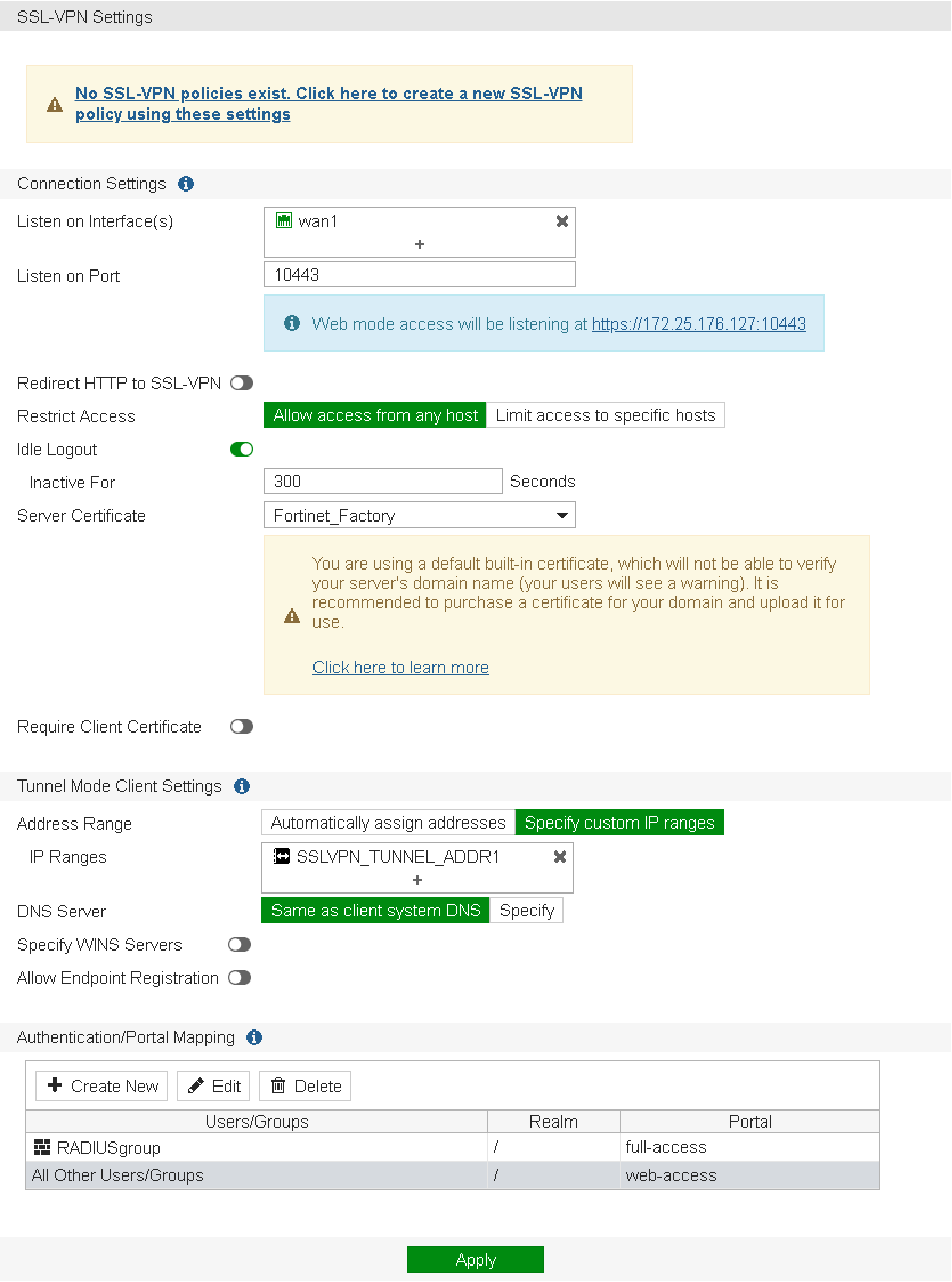
Configuring the SSL-VPN

Configure the SSL-VPN settings:

1. Go to *VPN > SSL-VPN Settings*.
   Under *Connection Settings*, set *Listen on Port* to `10443`. Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set *IP Ranges* to the SSL VPN tunnel address range.

   Under *Authentication/Portal Mapping*, select *Create New*.

   Assign the *RADIUSgroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to the desired portal.



SSL-VPN Settings

⚠ No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings

Connection Settings ℹ

Listen on Interface(s): wan1 ✖ +

Listen on Port: 10443

ℹ Web mode access will be listening at https://172.25.176.127:10443

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 ℹ

Address Range: Automatically assign addresses [✓ Specify custom IP ranges]

IP Ranges: SSLVPN_TUNNEL_ADDR1 ✖ +

DNS Server: [✓ Same as client system DNS] Specify

Specify WINS Servers: ○

Allow Endpoint Registration: ○

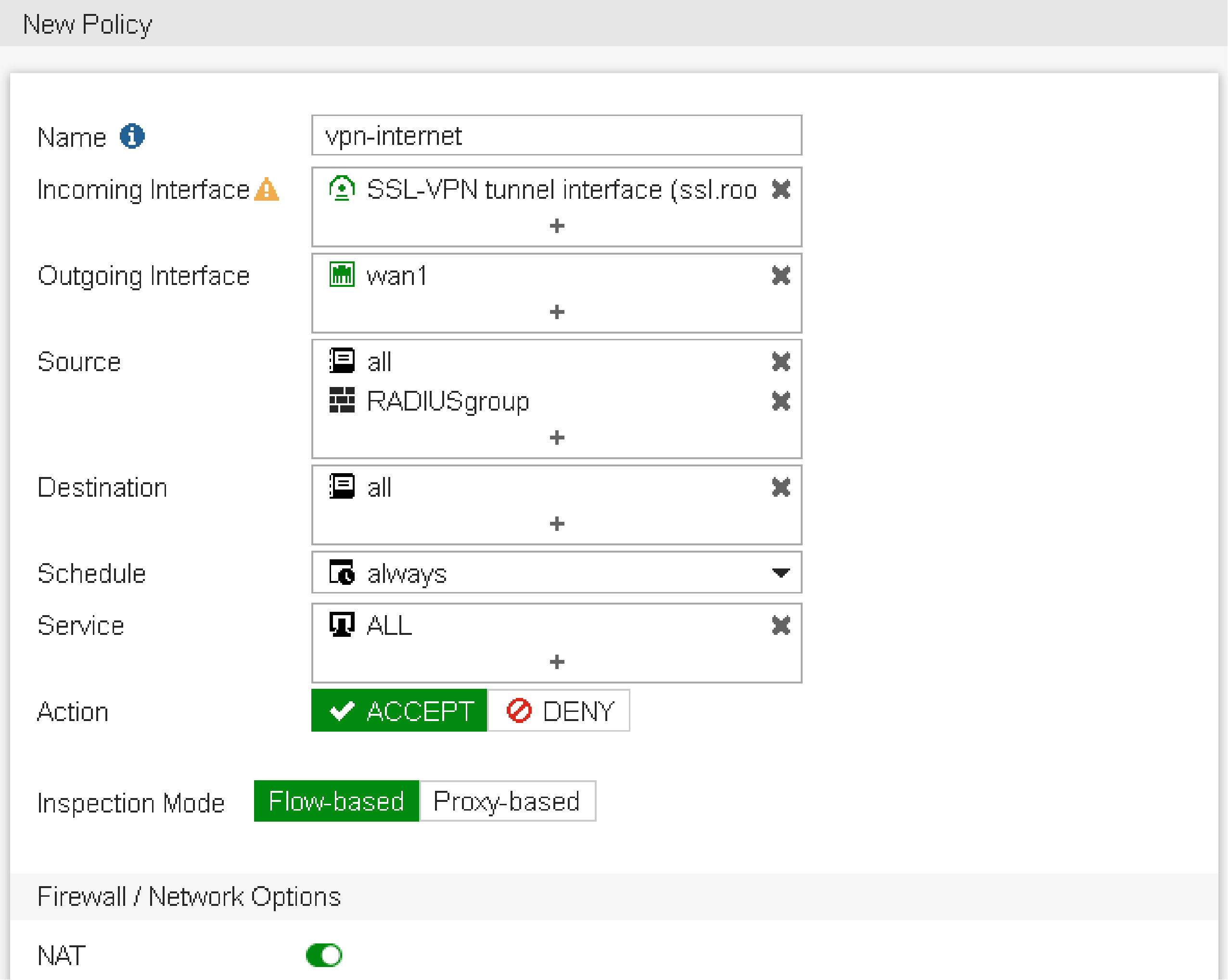
Authentication/Portal Mapping ℹ

Users/Groups	Realm	Portal
RADIUSgroup	/	full-access
All Other Users/Groups	/	web-access

Creating the security policy for VPN access to the Internet

To create the security profile:

1. Go to *Policy & Objects > IPv4 Policy* and create a new SSL-VPN policy, including the *RADIUSgroup*, as shown.



New Policy

Name: vpn-internet

Incoming Interface: SSL-VPN tunnel interface (ssl.roo

Outgoing Interface: wan1

Source: all
RADIUSgroup

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT | DENY

Inspection Mode: Flow-based | Proxy-based

Firewall / Network Options

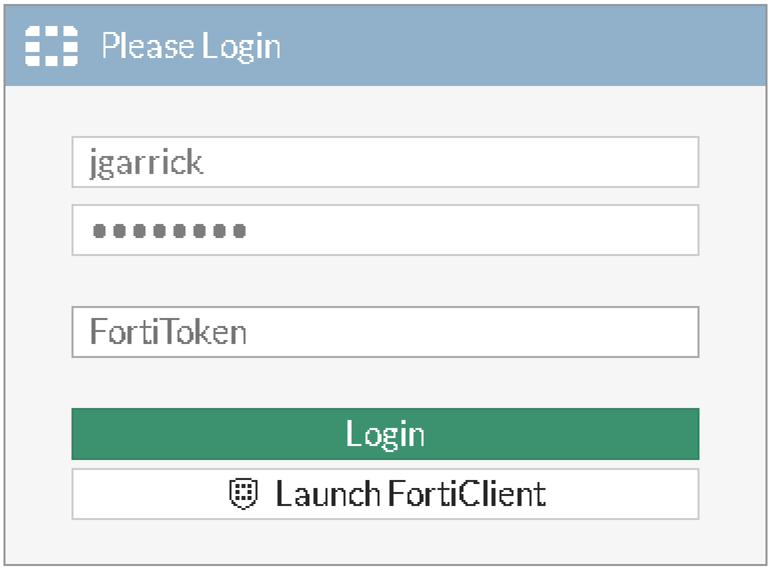
NAT: ●

Results

In this example, we will use the web portal to access the SSL VPN and test the two-factor authentication.

To test two-factor authentication:

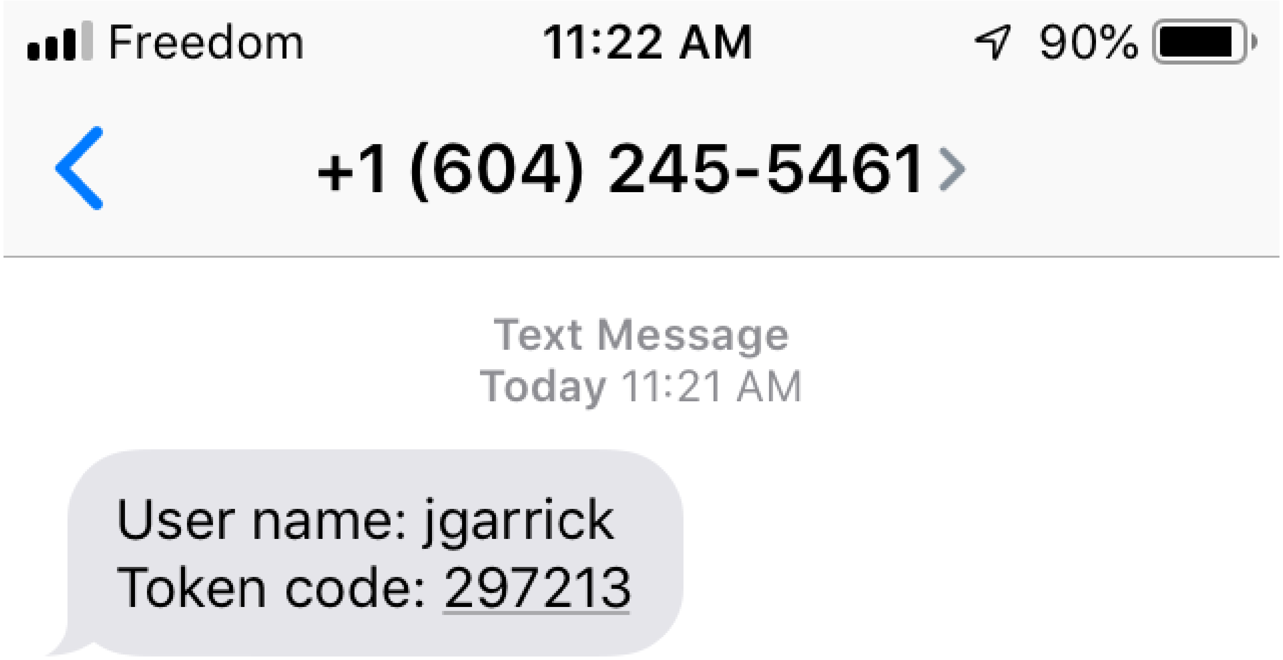
1. Open a browser and navigate to the SSL VPN web portal, in this case *https://172.25.176.127:10443*.
   Enter a valid username and password and select *Login*. You should be prompted to enter a *FortiToken Code*.



jgarrick

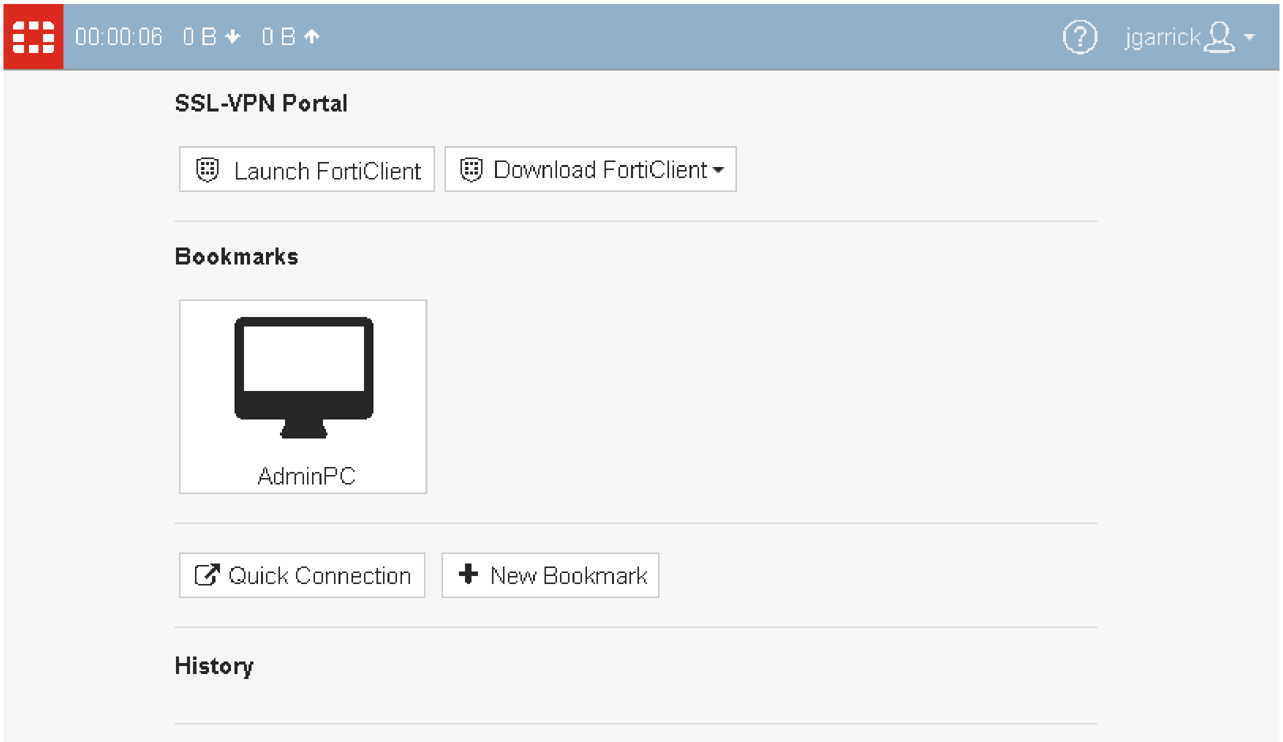
••••••••

2. The *FortiToken Code* should have been sent to your mobile phone as a text message containing a 6-digit number. Enter the number into the SSL VPN login portal and select *Login*.

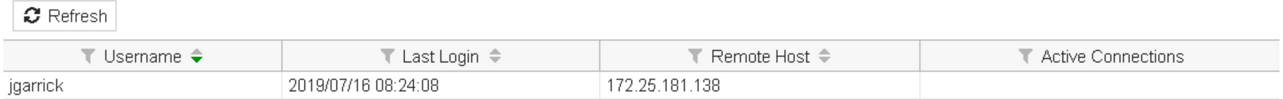


User name: jgarrick
Token code: 297213

3. You should now have access to the SSL VPN tunnel.



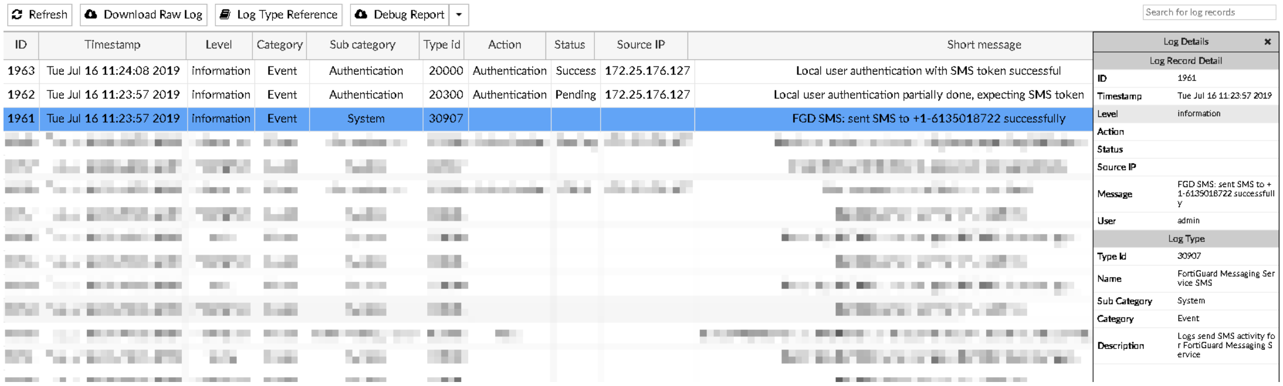
4. To verify that the user has connected to the tunnel, on the FortiGate, go to *Monitor* > *SSL-VPN Monitor*.



Refresh

Username	Last Login	Remote Host	Active Connections
jgarrick	2019/07/16 08:24:08	172.25.181.138	

5. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* to confirm the user's connection.



Refresh | Download Raw Log | Log Type Reference | Debug Report

Search for log records

ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message
1963	Tue Jul 16 11:24:08 2019	information	Event	Authentication	20000	Authentication	Success	172.25.176.127	Local user authentication with SMS token successful
1962	Tue Jul 16 11:23:57 2019	information	Event	Authentication	20300	Authentication	Pending	172.25.176.127	Local user authentication partially done, expecting SMS token
1961	Tue Jul 16 11:23:57 2019	information	Event	System	30907				FGD SMS: sent SMS to +1-6135018722 successfully

[redacted]

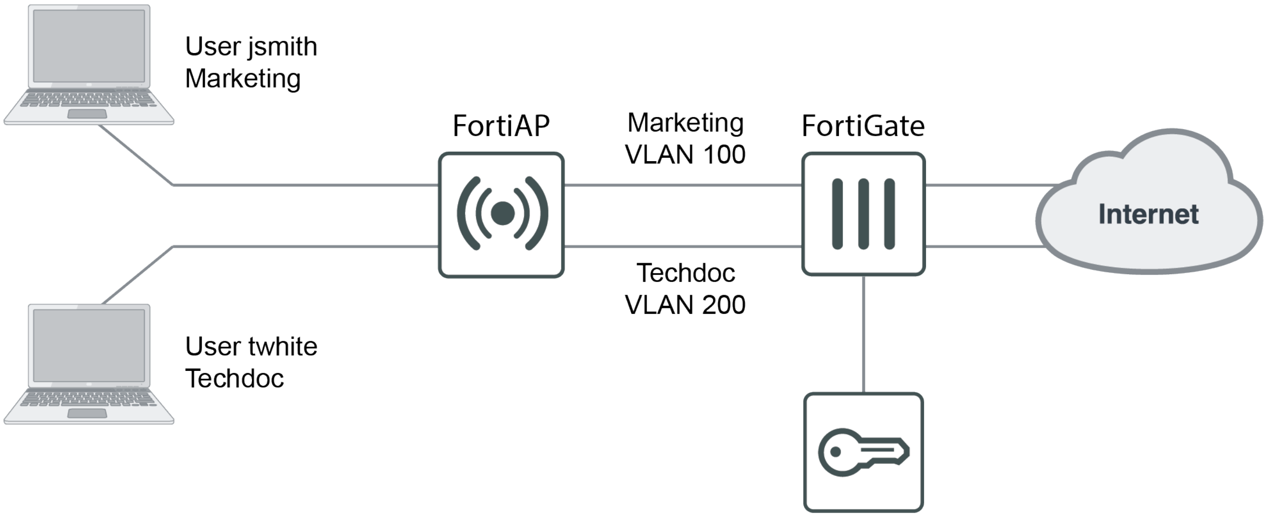
Log Details

Log Record Detail	
ID	1961
Timestamp	Tue Jul 16 11:23:57 2019
Level	information
Action	
Status	
Source IP	
Message	FGD SMS: sent SMS to +1-6135018722 successfully
User	admin
Log Type	
Type Id	30907
Name	FortiGuard Messaging Service SMS
Sub Category	System
Category	Event
Description	Logs send SMS activity for FortiGuard Messaging Service

WiFi authentication

This section describes configuring WiFi authentication with FortiAuthenticator.

Assigning WiFi users to VLANs dynamically



Virtual LANs (VLANs) are used to assign wireless users to different networks without requiring the use of multiple SSIDs. Each user's VLAN assignment is stored in the user database of the RADIUS server that authenticates the users.

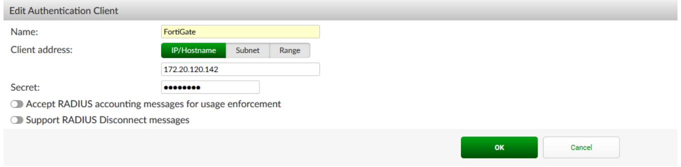
This example creates dynamic VLANs for the Techdoc and Marketing departments. The RADIUS server is a FortiAuthenticator. It is assumed a user group on the FortiAuthenticator has already been created (in this example, *employees*).

```
config certificate ca
    edit {name}
    # CA certificate.
        set name {string}   Name. size[79]
        set ca {string}   CA certificate as a PEM file.
        set range {global | vdom}   Either global or VDOM IP address range for the CA
certificate.
                global  Global range.
                vdom    VDOM IP address range.
        set source {factory | user | bundle}   CA certificate source type.
                factory  Factory installed certificate.
                user     User generated certificate.
                bundle   Bundle file certificate.
        set trusted {enable | disable}   Enable/disable as a trusted CA.
        set scep-url {string}   URL of the SCEP server. size[255]
        set auto-update-days {integer}   Number of days to wait before requesting an updated
CA certificate (0 - 4294967295, 0 = disabled). range[0-4294967295]
```

Configuring the FortiAuthenticator

To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, 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.



Edit Authentication Client

Name: FortiGate

Client address: IP/Hostname | Subnet | Range

172.20.120.142

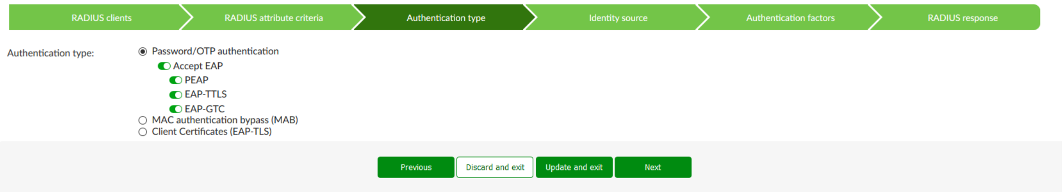
Secret: ●●●●●●●●

Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Choose *Password/OTP* authentication as the authentication type and enable all *EAP* types.

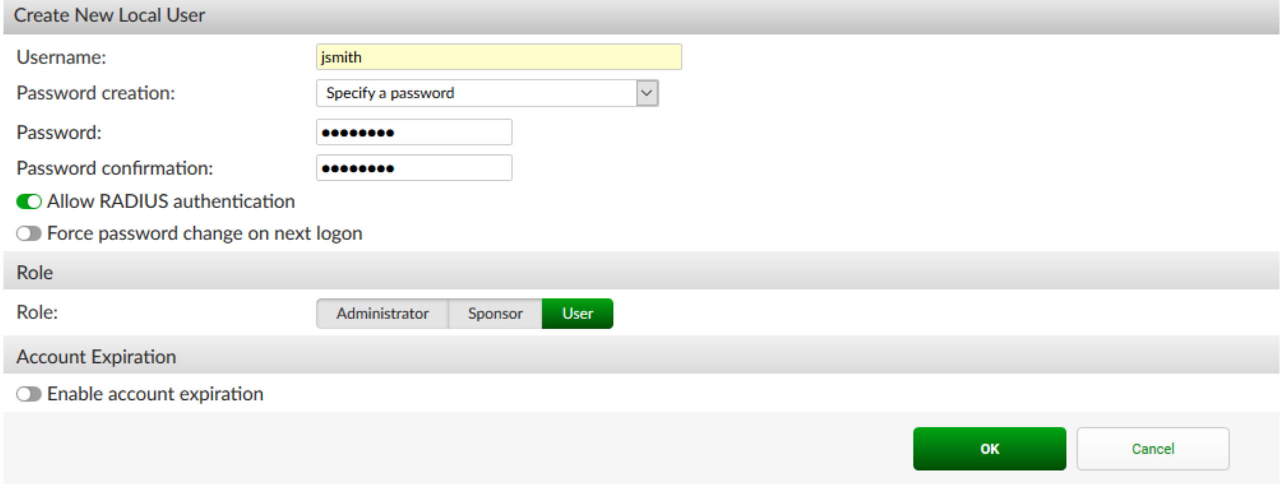


Authentication type:
● Password/OTP authentication
Accept EAP
PEAP
EAP-TTLS
EAP-GTC
○ MAC authentication bypass (MAB)
○ Client Certificates (EAP-TLS)

5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
   Add the *employees* user group as a filter.
6. Set the authentication method to *Password only authentication*.
7. Review the RADIUS response, and click *Save and Exit*.

To create the local user accounts:

1. Next go to *Authentication* > *User Management* > *Local Users* and create local user accounts as needed.



Create New Local User

Username: jsmith

Password creation: Specify a password

Password: ●●●●●●●●

Password confirmation: ●●●●●●●●

Allow RADIUS authentication

Force password change on next logon

Role

Role: Administrator | Sponsor | User

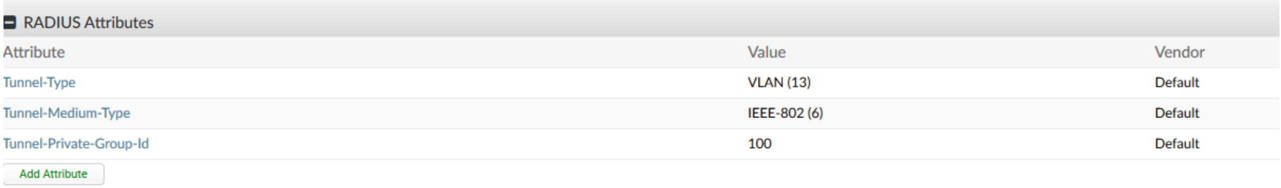
Account Expiration

Enable account expiration

2. For each user, add the following RADIUS attributes which specify the VLAN information to be sent to the FortiGate.

The *Tunnel-Private-Group-Id* attribute specifies the VLAN ID.

In this example, jsmith is assigned VLAN *100* and twhite is assigned VLAN *200*.



RADIUS Attributes

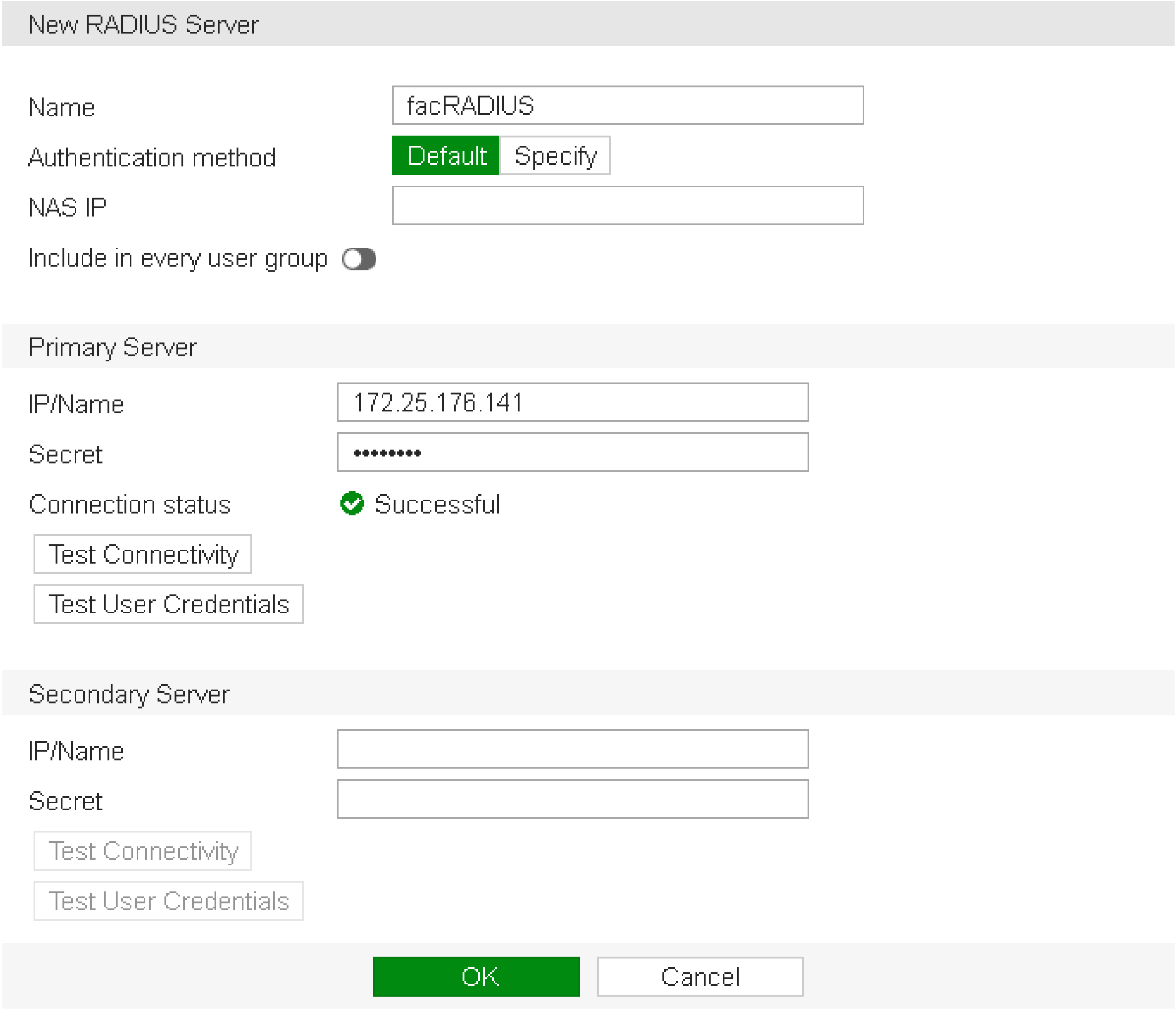
Attribute	Value	Vendor
Tunnel-Type	VLAN (13)	Default
Tunnel-Medium-Type	IEEE-802 (6)	Default
Tunnel-Private-Group-Id	100	Default

Add Attribute

Adding the RADIUS server to the FortiGate

To add the RADIUS server to the FortiGate:

1. On the FortiGate, go to *User & Device* > *RADIUS Servers* and select *Create New*.
   Enter the FortiAuthenticator IP address and the server *Secret* entered on the FortiAuthenticator earlier.
   Select *Test Connectivity* to confirm the successful connection.



New RADIUS Server

Name	facRADIUS
Authentication method	[✓ Default] Specify
NAS IP	
Include in every user group	○

Primary Server

IP/Name	172.25.176.141
Secret	•••••••••
Connection status	✓ Successful

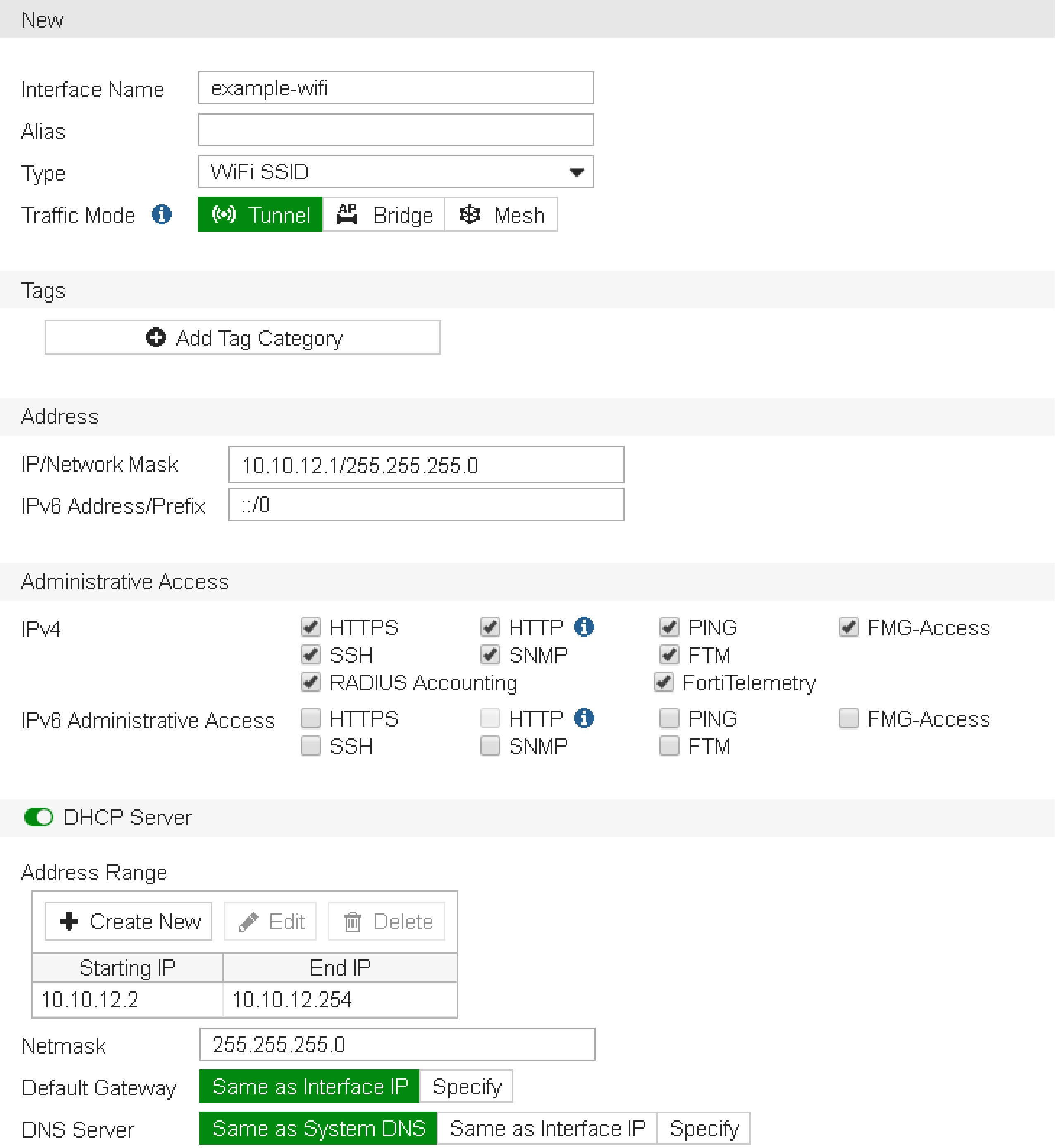
Secondary Server

IP/Name	
Secret	

Creating an SSID with dynamic VLAN assignment

To create an SSID with dynamic VLAN assignment:

1. On the FortiGate, go to *WiFi & Switch Controller > SSID* and create a new SSID.
   Set up DHCP service.



New

Interface Name: example-wifi

Alias:

Type: WiFi SSID

Traffic Mode: [✓ Tunnel] Bridge Mesh

Tags

Add Tag Category

Address

IP/Network Mask: 10.10.12.1/255.255.255.0

IPv6 Address/Prefix: ::/0

Administrative Access

IPv4: ☑ HTTPS ☑ HTTP ☑ PING ☑ FMG-Access ☑ SSH ☑ SNMP ☑ FTM ☑ RADIUS Accounting ☑ FortiTelemetry

IPv6 Administrative Access: □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM

● DHCP Server

Address Range

Create New Edit Delete

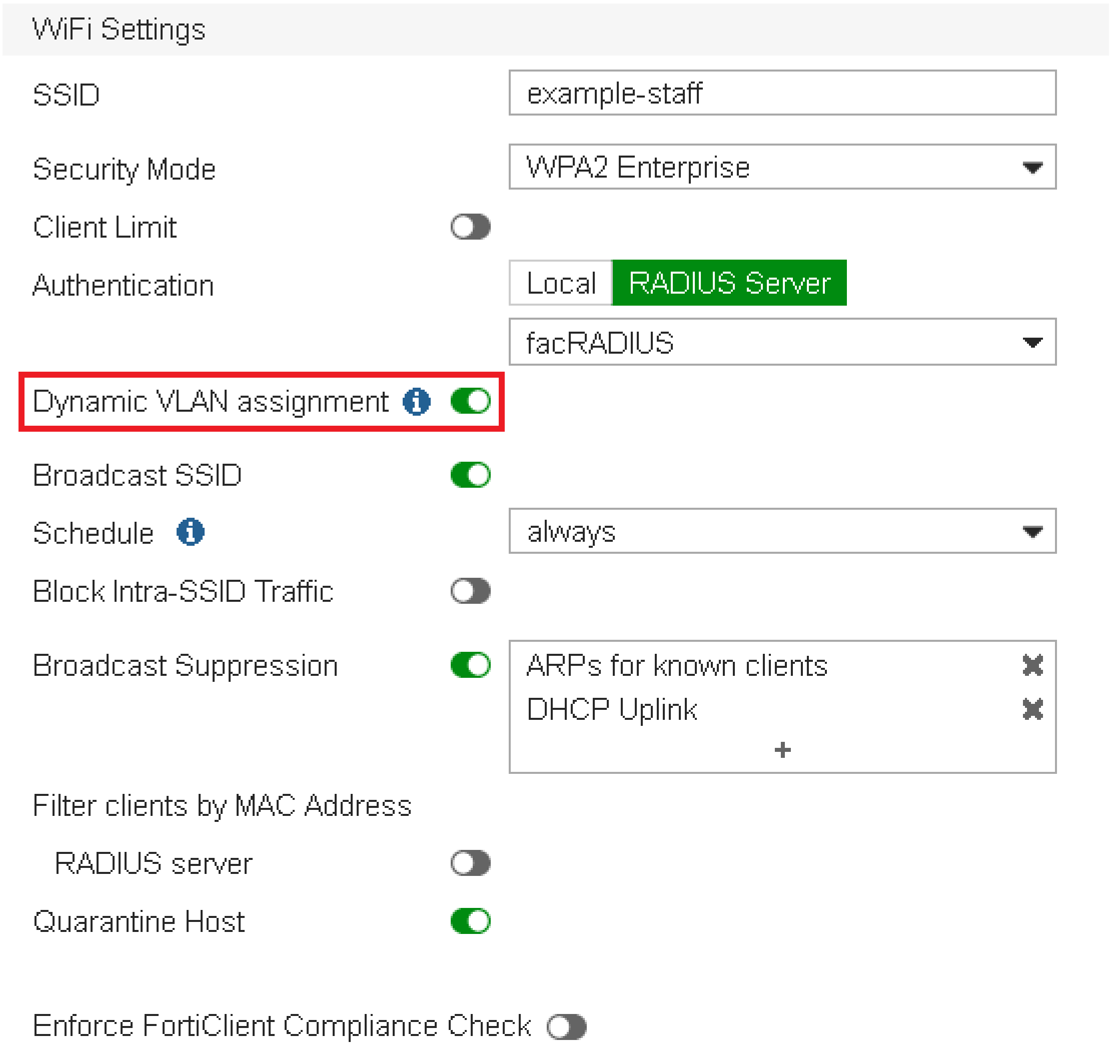
Starting IP	End IP
10.10.12.2	10.10.12.254

Netmask: 255.255.255.0

Default Gateway: [✓ Same as Interface IP] Specify

DNS Server: [✓ Same as System DNS] Same as Interface IP Specify

2. Select *WPA2 Enterprise* security and select your RADIUS server for authentication.
   Enable *Dynamic VLAN Assignment*.



WiFi Settings

SSID: example-staff

Security Mode: WPA2 Enterprise

Client Limit: ○

Authentication: Local [✓ RADIUS Server]

facRADIUS

Dynamic VLAN assignment: ●

Broadcast SSID: ●

Schedule: always

Block Intra-SSID Traffic: ○

Broadcast Suppression: ●

ARPs for known clients ✖
DHCP Uplink ✖
+

Filter clients by MAC Address

RADIUS server: ○

Quarantine Host: ●

Enforce FortiClient Compliance Check: ○

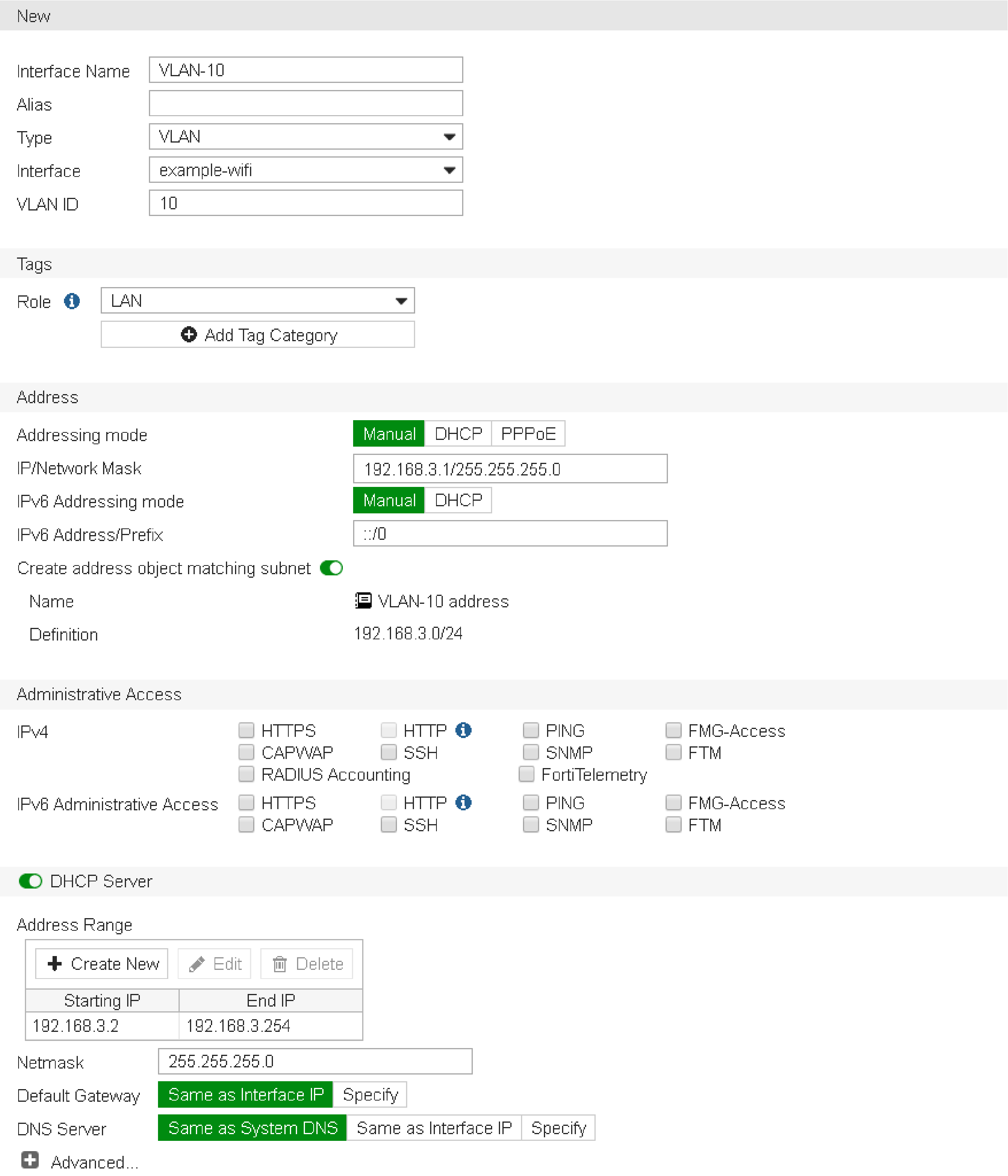
3. Then open the *CLI Console* and enter the following command to assignment and set the VLAN ID to `10`. This VLAN is used when RADIUS does not assign a VLAN:

```
config wireless-controller vap
   edit example-wifi
      set vlanid 10
   next
end
```

Creating the VLAN interfaces

To create the VLAN interfaces:

1. Go to *Network* > *Interfaces*.
   Create the VLAN interface for default *VLAN-10* and set up DHCP service.



New

Interface Name	VLAN-10
Alias	
Type	VLAN
Interface	example-wifi
VLAN ID	10

Tags

Role	LAN
	Add Tag Category

Address

Addressing mode	[✓ Manual] DHCP PPPoE
IP/Network Mask	192.168.3.1/255.255.255.0
IPv6 Addressing mode	[✓ Manual] DHCP
IPv6 Address/Prefix	::/0
Create address object matching subnet	●
Name	VLAN-10 address
Definition	192.168.3.0/24

Administrative Access

IPv4	□ HTTPS	□ HTTP	□ PING	□ FMG-Access
	□ CAPWAP	□ SSH	□ SNMP	□ FTM
	□ RADIUS Accounting		□ FortiTelemetry	
IPv6 Administrative Access	□ HTTPS	□ HTTP	□ PING	□ FMG-Access
	□ CAPWAP	□ SSH	□ SNMP	□ FTM

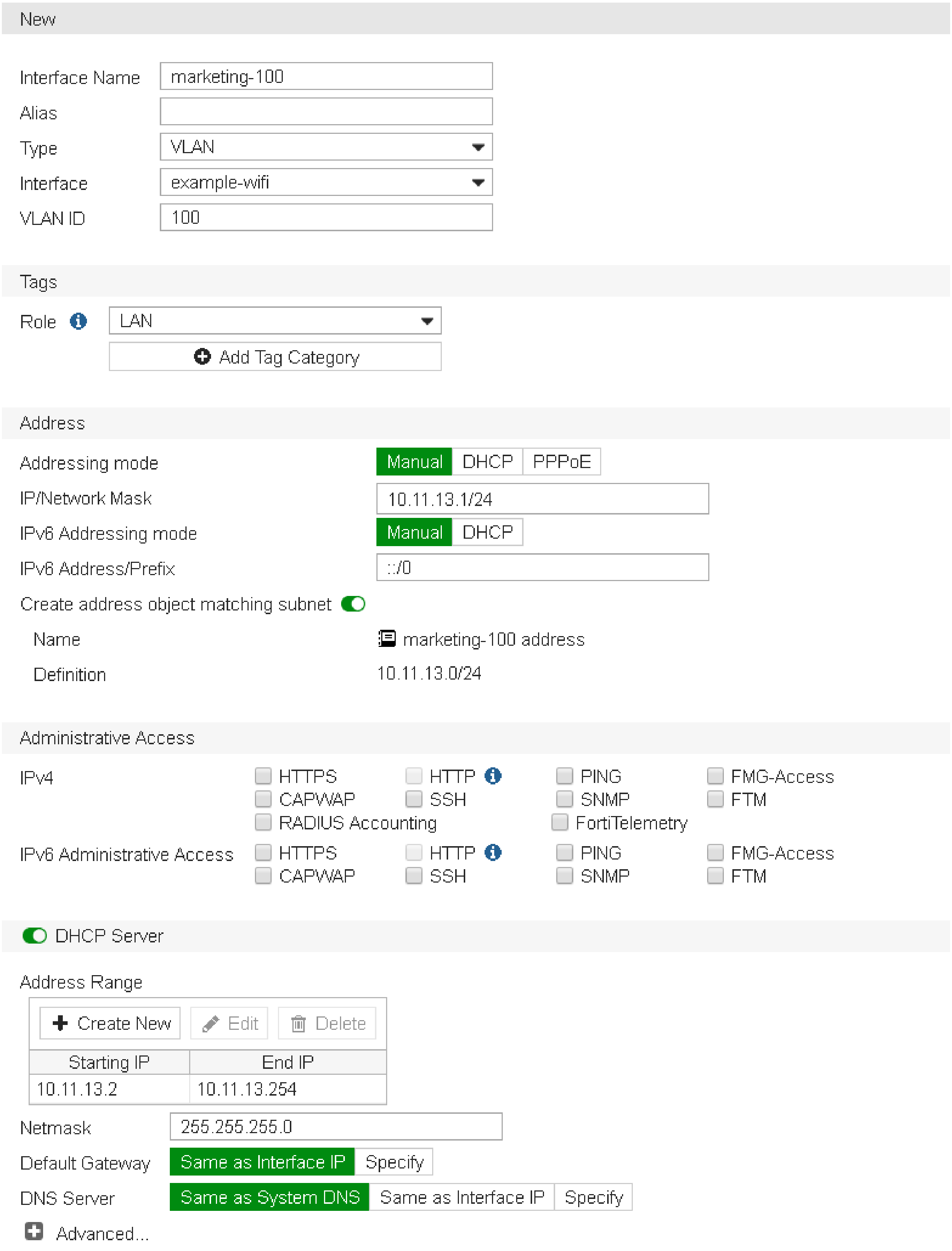
● DHCP Server

Address Range

Starting IP	End IP
192.168.3.2	192.168.3.254

Netmask	255.255.255.0
Default Gateway	[✓ Same as Interface IP] Specify
DNS Server	[✓ Same as System DNS] Same as Interface IP Specify

2. Then create two more VLAN interfaces: one for *marketing-100* and another for *techdoc-200*, both with DHCP service.



New

Interface Name	marketing-100
Alias	
Type	VLAN
Interface	example-wifi
VLAN ID	100

Tags

Role: LAN

Add Tag Category

Address

Addressing mode	[✓ Manual] DHCP PPPoE
IP/Network Mask	10.11.13.1/24
IPv6 Addressing mode	[✓ Manual] DHCP
IPv6 Address/Prefix	::/0
Create address object matching subnet	●
Name	marketing-100 address
Definition	10.11.13.0/24

Administrative Access

IPv4: □ HTTPS □ HTTP □ PING □ FMG-Access □ CAPWAP □ SSH □ SNMP □ FTM □ RADIUS Accounting □ FortiTelemetry

IPv6 Administrative Access: □ HTTPS □ HTTP □ PING □ FMG-Access □ CAPWAP □ SSH □ SNMP □ FTM

● DHCP Server

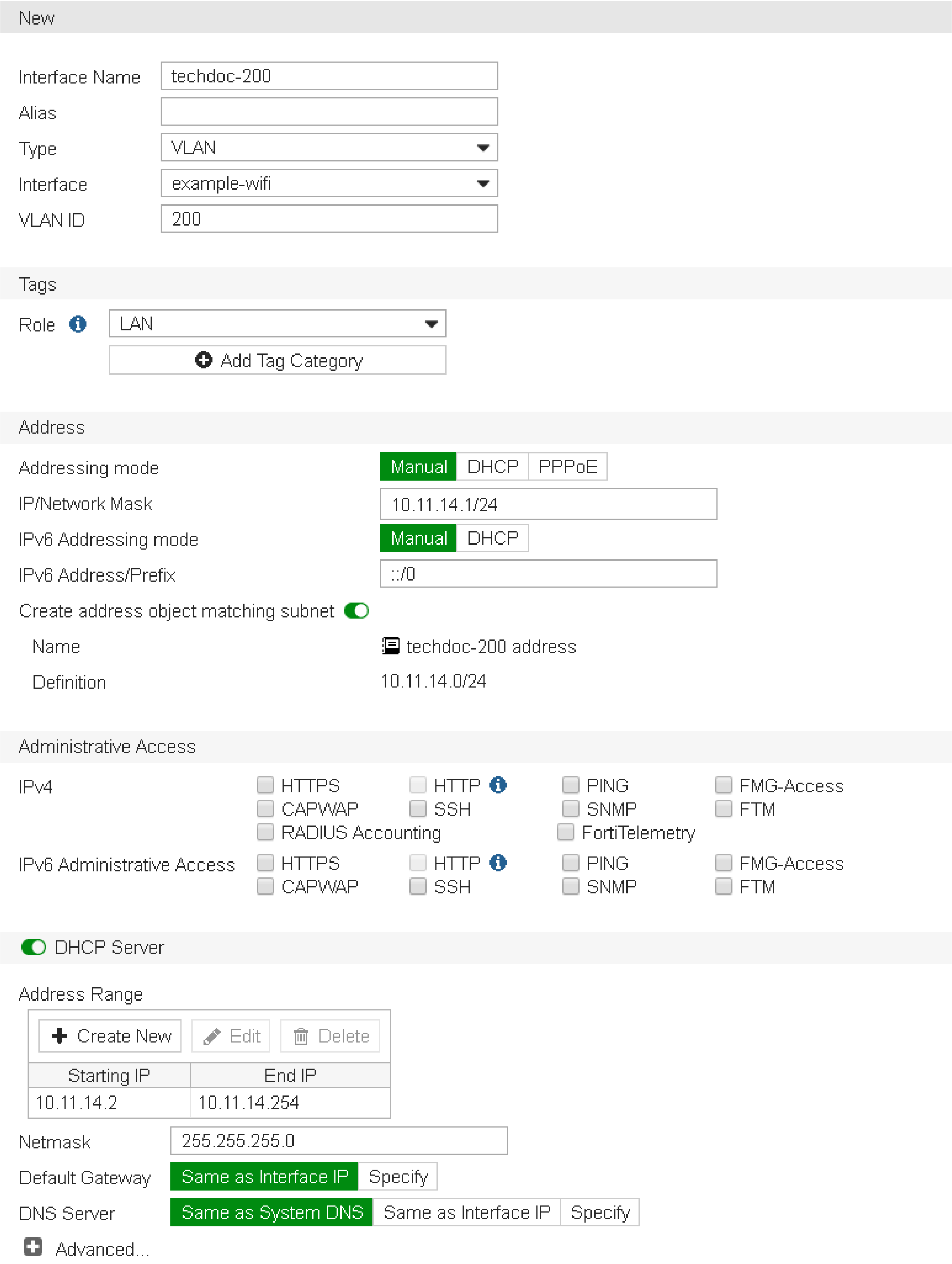
Address Range

Create New | Edit | Delete

Starting IP	End IP
10.11.13.2	10.11.13.254

Netmask	255.255.255.0
Default Gateway	[✓ Same as Interface IP] Specify
DNS Server	[✓ Same as System DNS] Same as Interface IP Specify

Advanced...



New

Interface Name	techdoc-200
Alias	
Type	VLAN
Interface	example-wifi
VLAN ID	200

Tags

Role	LAN
	Add Tag Category

Address

Addressing mode	[✓ Manual] DHCP PPPoE
IP/Network Mask	10.11.14.1/24
IPv6 Addressing mode	[✓ Manual] DHCP
IPv6 Address/Prefix	::/0
Create address object matching subnet	●
Name	techdoc-200 address
Definition	10.11.14.0/24

Administrative Access

IPv4	□ HTTPS	□ HTTP	□ PING	□ FMG-Access
	□ CAPWAP	□ SSH	□ SNMP	□ FTM
	□ RADIUS Accounting		□ FortiTelemetry	
IPv6 Administrative Access	□ HTTPS	□ HTTP	□ PING	□ FMG-Access
	□ CAPWAP	□ SSH	□ SNMP	□ FTM

● DHCP Server

Address Range

Starting IP	End IP
10.11.14.2	10.11.14.254

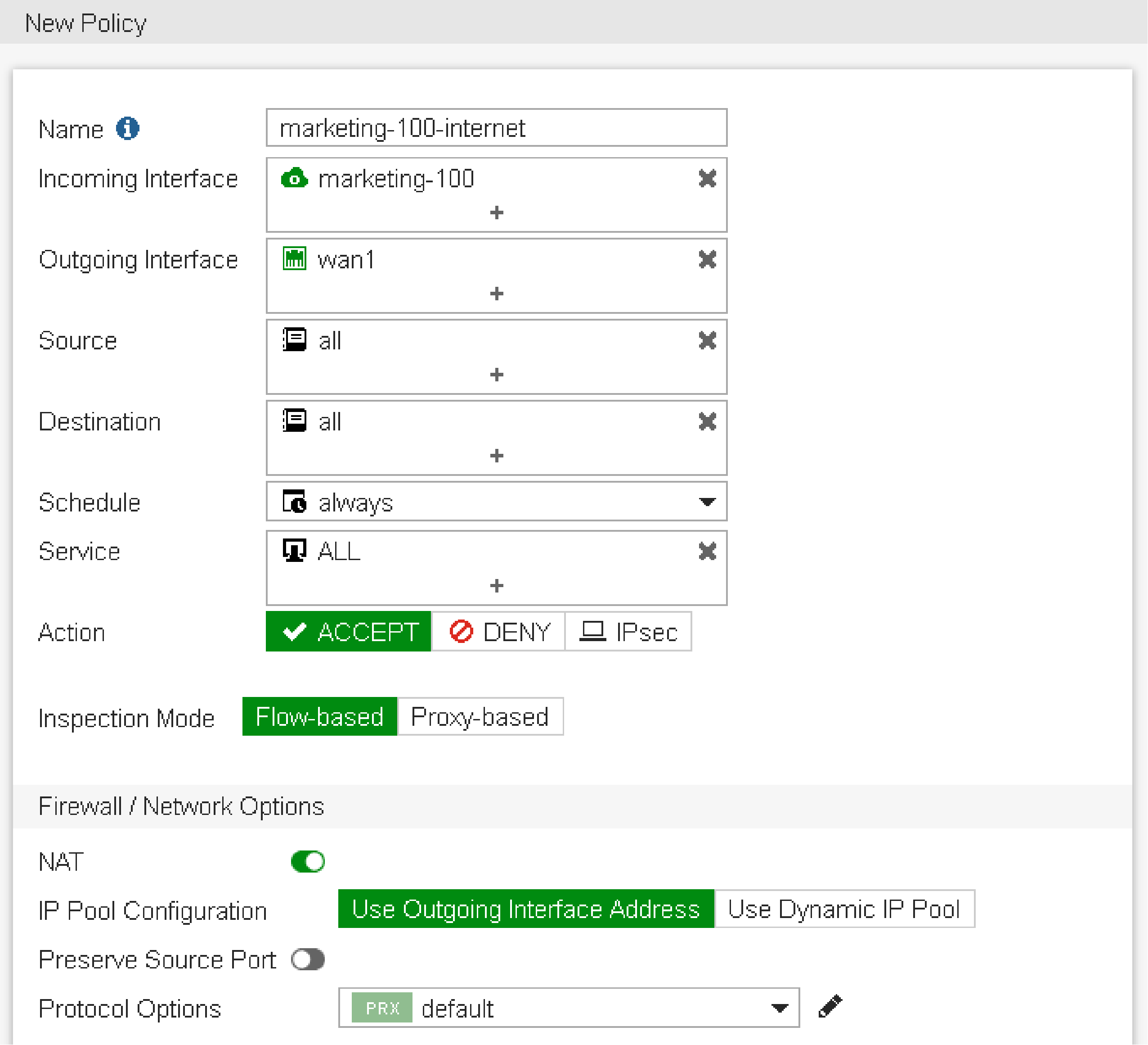
Netmask	255.255.255.0
Default Gateway	[✓ Same as Interface IP] Specify
DNS Server	[✓ Same as System DNS] Same as Interface IP Specify

Advanced...

Creating security policies

To create the security policies:

1. Go to *Policy & Objects > IPv4 Policy*.
   Create a policy that allows outbound traffic from *marketing-100* to the Internet.



New Policy

Name: marketing-100-internet

Incoming Interface: marketing-100

Outgoing Interface: wan1

Source: all

Destination: all

Schedule: always

Service: ALL

Action: [✓ ACCEPT] DENY IPsec

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

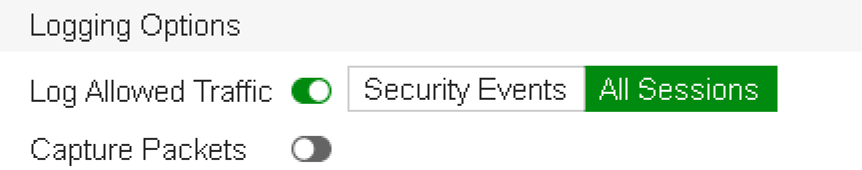
NAT: ●

IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve Source Port: ○

Protocol Options: PRX default

2. Under *Logging Options*, enable logging for *All Sessions*.



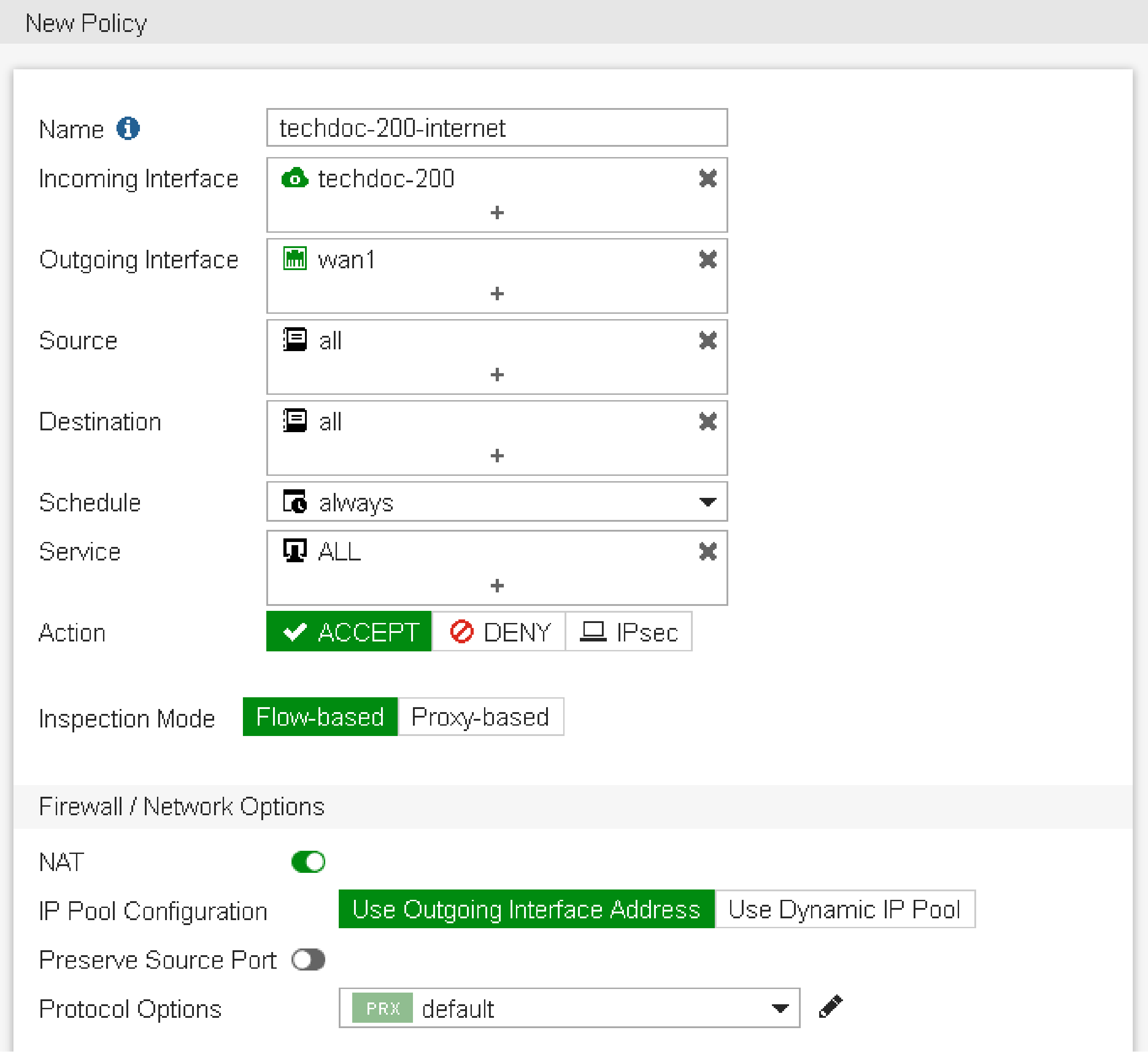
Logging Options

Log Allowed Traffic: ● Security Events [✓ All Sessions]

Capture Packets: ○

3. Create another policy that allows outbound traffic from *techdoc-200* to the Internet.

For this policy too, under *Logging Options*, enable logging for *All Sessions*.



New Policy

Name	techdoc-200-internet
Incoming Interface	techdoc-200
Outgoing Interface	wan1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY IPsec
Inspection Mode	[✓ Flow-based] Proxy-based

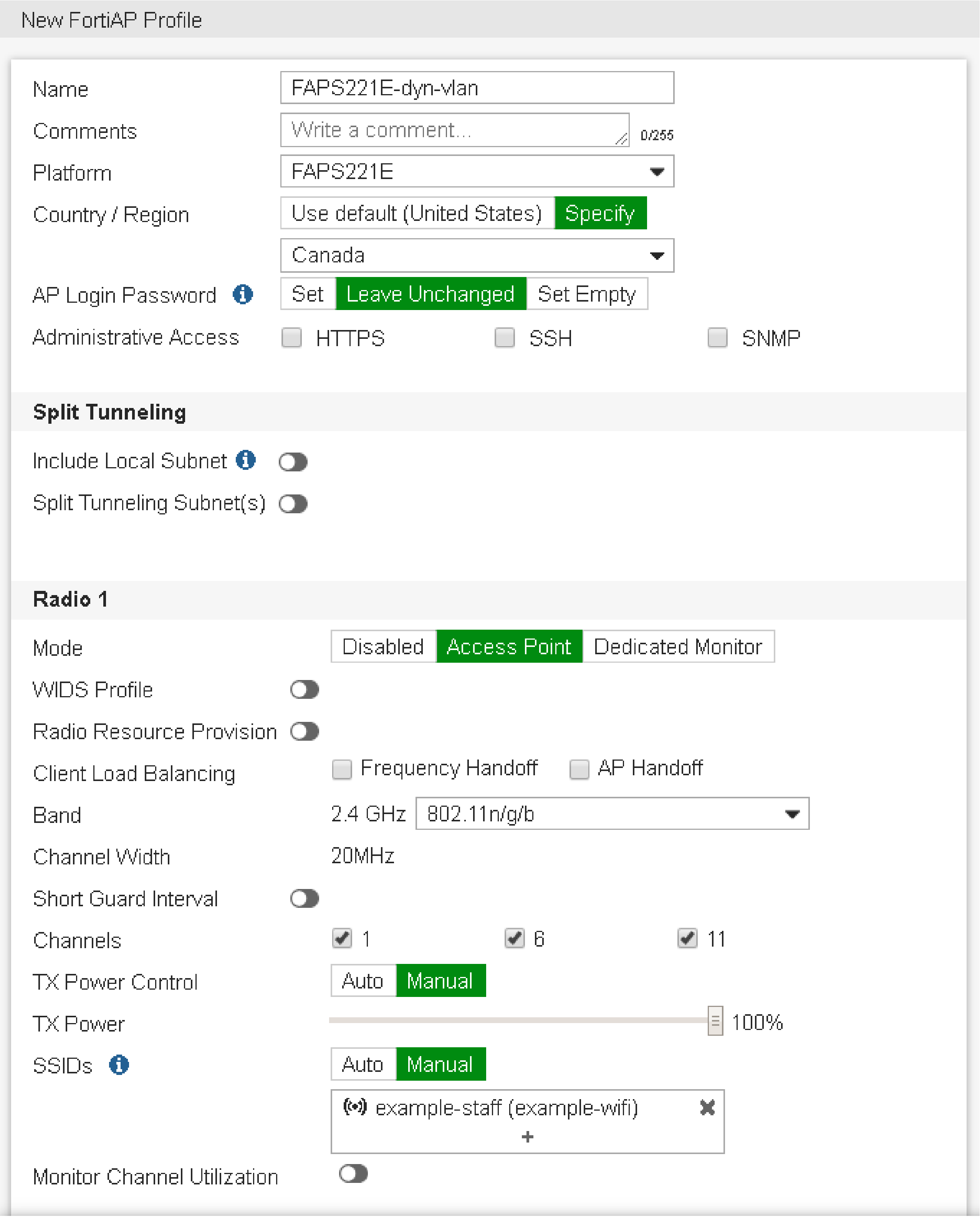
Firewall / Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PRX default

Creating the FortiAP profile

To create the FortiAP profile:

1. Go to *WiFi & Switch Controller > FortiAP Profiles*.
   Create a new profile for your FortiAP model and select the new SSID for both *Radio 1* and *Radio 2*.



New FortiAP Profile

Name	FAPS221E-dyn-vlan
Comments	Write a comment... 0/255
Platform	FAPS221E
Country / Region	Use default (United States) [✓ Specify] Canada
AP Login Password	Set [✓ Leave Unchanged] Set Empty
Administrative Access	□ HTTPS □ SSH □ SNMP

Split Tunneling

Include Local Subnet	○
Split Tunneling Subnet(s)	○

Radio 1

Mode	Disabled [✓ Access Point] Dedicated Monitor
WIDS Profile	○
Radio Resource Provision	○
Client Load Balancing	□ Frequency Handoff □ AP Handoff
Band	2.4 GHz 802.11n/g/b
Channel Width	20MHz
Short Guard Interval	○
Channels	☑ 1 ☑ 6 ☑ 11
TX Power Control	Auto [✓ Manual]
TX Power	100%
SSIDs	Auto [✓ Manual] example-staff (example-wifi) ✖ +
Monitor Channel Utilization	○

Connecting and authorizing the FortiAP

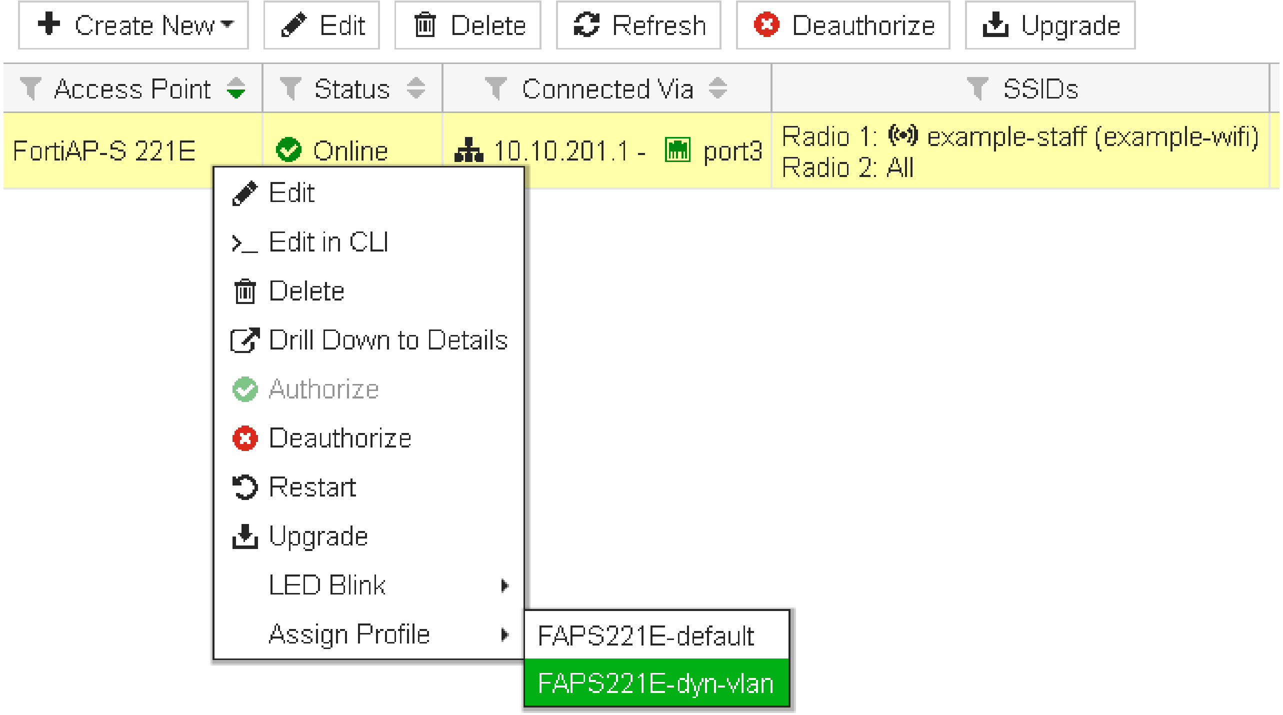
To connect and authorize the FortiAP:

1. Go to *Network* > *Interfaces* and edit an unused interface.
   Set an *IP/Network Mask* and enable *CAPWAP* under *Administrative Access* > *IPv4*.

   Enable *DHCP Server*.

   Now connect the FortiAP unit to the this interface and apply power.
2. Go to *WiFi & Switch Controller* > *Managed FortiAPs*.
   Right-click on the FortiAP unit and select *Authorize*.

   Once authorized, right-click on the FortiAP unit again and select *Assign Profile* and select the FortiAP profile created earlier.



Access Point	Status	Connected Via	SSIDs
FortiAP-S 221E	✓ Online	10.10.201.1 - port3	Radio 1: example-staff (example-wifi) Radio 2: All

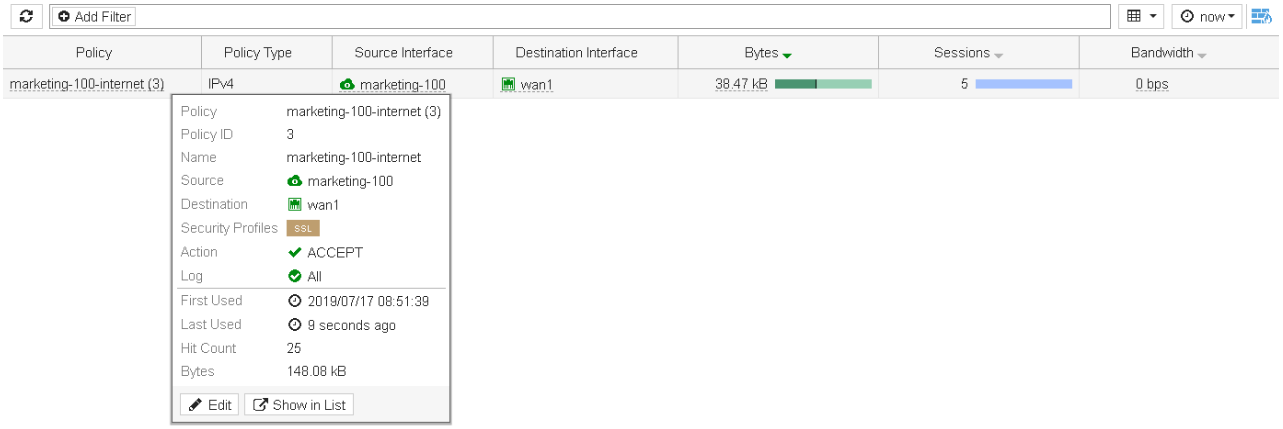
Results

The SSID will appear in the list of available wireless networks on the users’ devices.

Both twhite and jsmith can connect to the SSID with their credentials and access the Internet.

If a certificate warning message appears, accept the certificate.

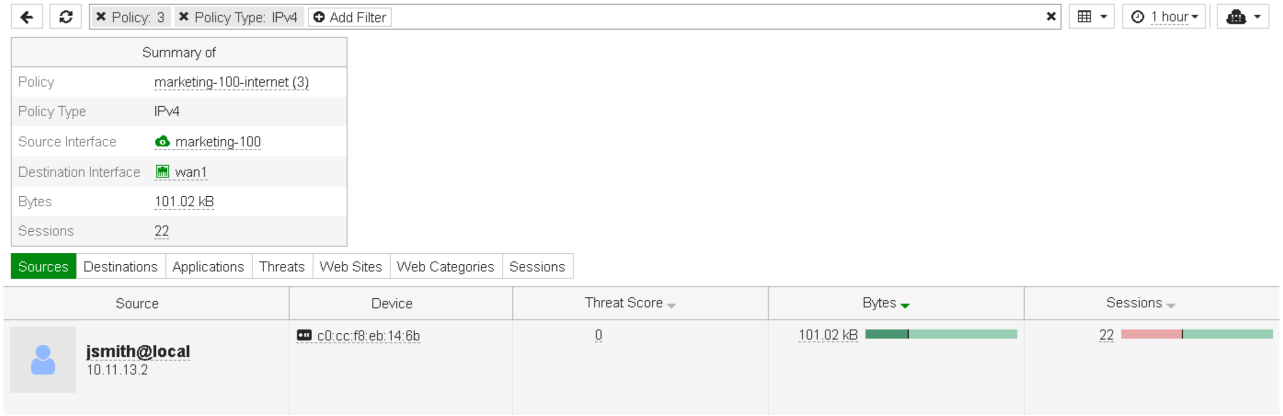
1. Go to *FortiView* > *Policies*.
   Note that traffic for jsmith and twhite will pass through different policies. In this example, the *marketing-100-internet* policy is displayed, indicating that jsmith has connected to the WiFi.



Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	Bandwidth
marketing-100-internet (3)	IPv4	marketing-100	wan1	38.47 kB	5	0 bps

Policy	marketing-100-internet (3)
Policy ID	3
Name	marketing-100-internet
Source	marketing-100
Destination	wan1
Security Profiles	SSL
Action	✓ ACCEPT
Log	✓ All
First Used	2019/07/17 08:51:39
Last Used	9 seconds ago
Hit Count	25
Bytes	148.08 kB

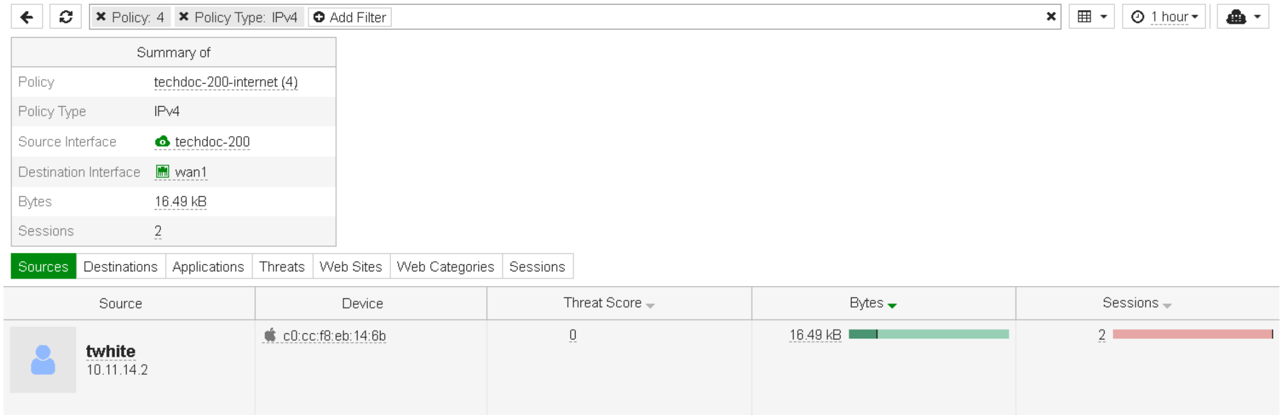
2. Double-click to drill-down, where the user's identity (including username, source IP, and device address) is confirmed.



Summary of	
Policy	marketing-100-internet (3)
Policy Type	IPv4
Source Interface	marketing-100
Destination Interface	wan1
Bytes	101.02 kB
Sessions	22

Source	Device	Threat Score	Bytes	Sessions
jsmith@local 10.11.13.2	c0:cc:f8:eb:14:6b	0	101.02 kB	22

3. When twhite has connected to the WiFi network, go to *FortiView > Policies* and drill-down. The user, and *techdoc-200-internet* policy, is confirmed.



Summary of	
Policy	techdoc-200-internet (4)
Policy Type	IPv4
Source Interface	techdoc-200
Destination Interface	wan1
Bytes	16.49 kB
Sessions	2

Source	Device	Threat Score	Bytes	Sessions
twhite 10.11.14.2	c0:cc:f8:eb:14:6b	0	16.49 kB	2

WiFi using FortiAuthenticator RADIUS with certificates

This recipe will walk you through the configuration of FortiAuthenticator as the RADIUS server for a FortiGate wireless controller. WPA2-Enterprise with 802.1X authentication can be used to authenticate wireless users with FortiAuthenticator. 802.1X utilizes the Extensible Authentication Protocol (EAP) to establish a secure tunnel between participants involved in an authentication exchange.

EAP-TLS is the most secure form of wireless authentication because it replaces the client username/password with a client certificate. Every end user, including the authentication server, that participates in EAP-TLS must possess at least two certificates:

1. A client certificate signed by the certificate authority (CA)
2. A copy of the CA root certificate.

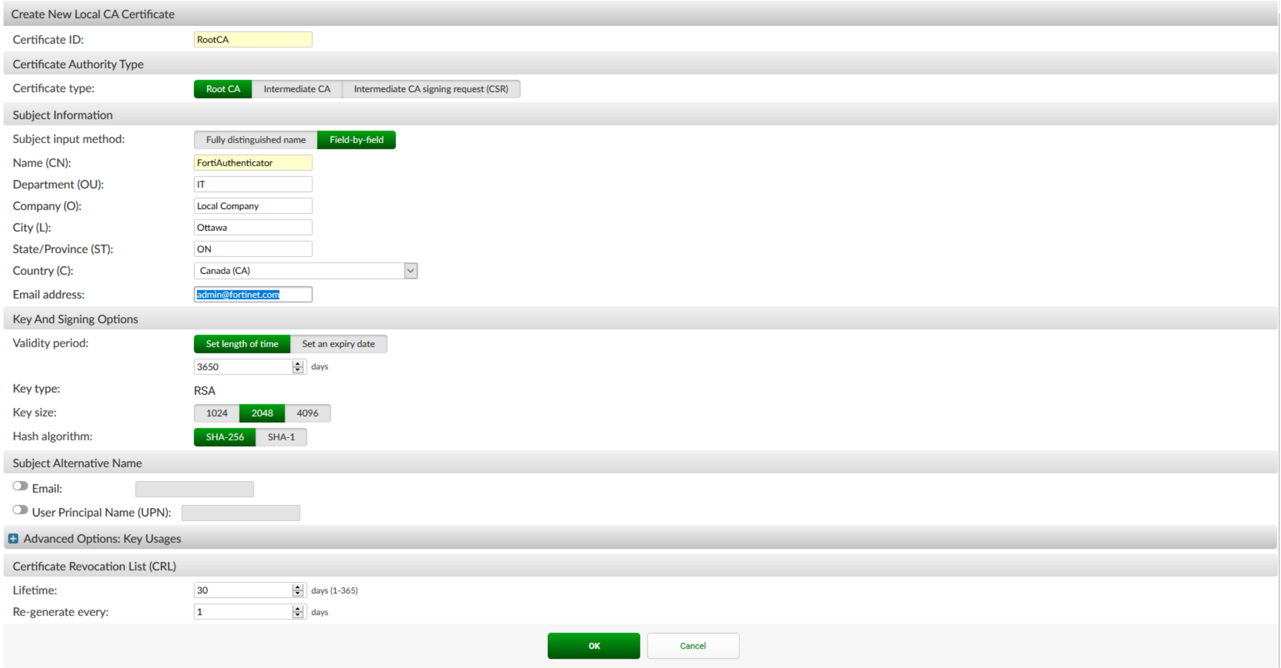
This recipe specifically focuses on the configuration of the FortiAuthenticator, FortiGate, and Windows 10 computer.

Creating a local CA on FortiAuthenticator

The FortiAuthenticator will act as the certificate authority for all certificates authenticated for client access. To enable this functionality, a self-signed root CA certificate must be generated.

To create the local CA:

1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Create New*.
   Configure the fields as required.



Create New Local CA Certificate

Certificate ID: RootCA

Certificate Authority Type

Certificate type: Root CA

Subject Information

Subject input method: Field-by-field

Name (CN): FortiAuthenticator

Department (OU): IT

Company (O): Local Company

City (L): Ottawa

State/Province (ST): ON

Country (C): Canada (CA)

Email address: admin@fortinet.com

Key And Signing Options

Validity period: Set length of time

3650 days

Key type: RSA

Key size: 2048

Hash algorithm: SHA-256

Subject Alternative Name

Email:

User Principal Name (UPN):

Advanced Options: Key Usages

Certificate Revocation List (CRL)

Lifetime: 30 days (1-365)

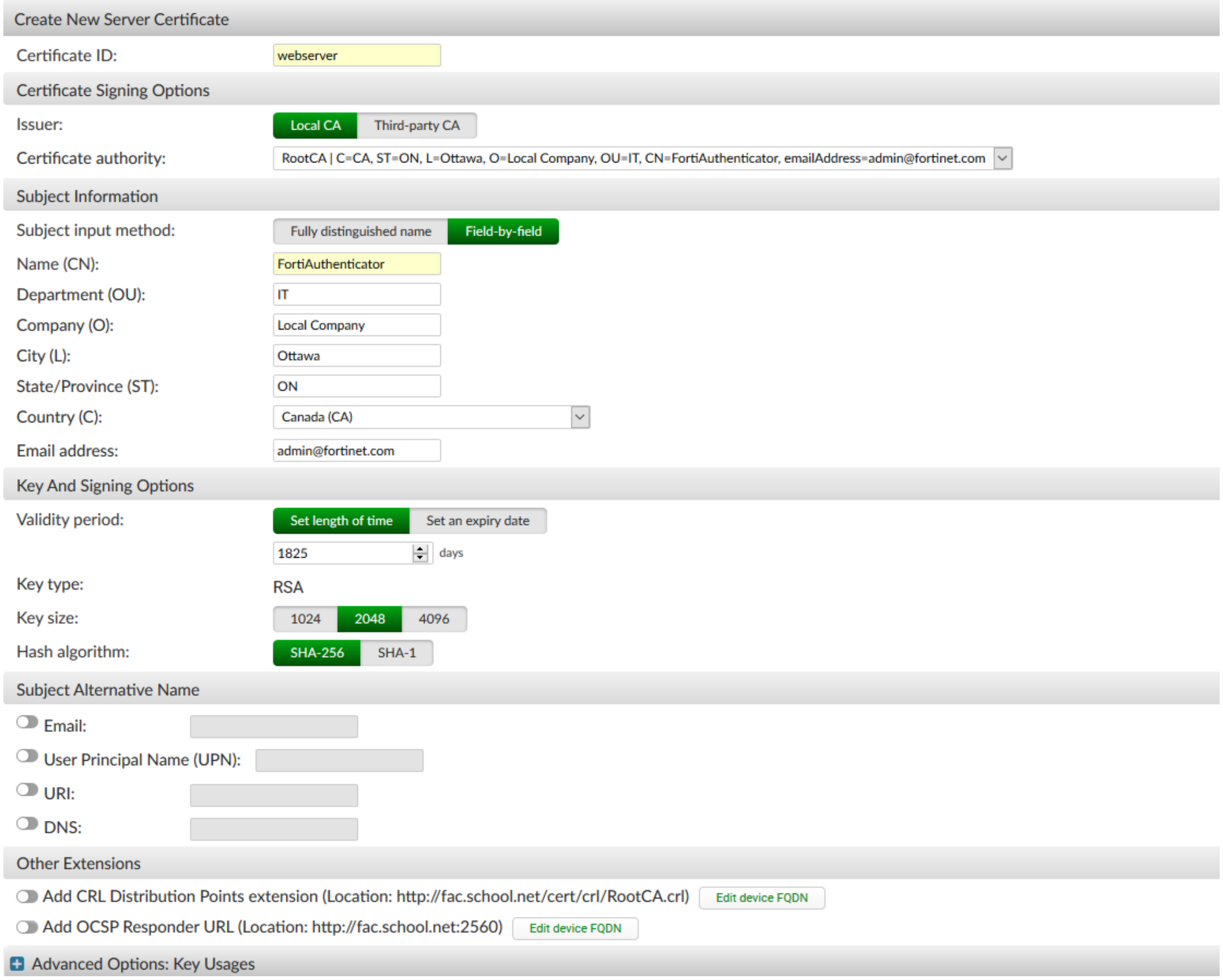
Re-generate every: 1 days

Creating a local service certificate on FortiAuthenticator

In order for the FortiAuthenticator to use a certificate in mutual authentication (supported by EAP-TLS), a local services certificate has to be created on behalf of the FortiAuthenticator.

To create the local service certificate:

1. Go to *Certificate Management* > *End Entities* > *Local Services* and select *Create New*. Complete the information in the fields pertaining to your organization.



Create New Server Certificate

Certificate ID:	webserver

Certificate Signing Options

Issuer:	Local CA (selected) / Third-party CA
Certificate authority:	RootCA | C=CA, ST=ON, L=Ottawa, O=Local Company, OU=IT, CN=FortiAuthenticator, emailAddress=admin@fortinet.com

Subject Information

Subject input method:	Fully distinguished name / Field-by-field (selected)
Name (CN):	FortiAuthenticator
Department (OU):	IT
Company (O):	Local Company
City (L):	Ottawa
State/Province (ST):	ON
Country (C):	Canada (CA)
Email address:	admin@fortinet.com

Key And Signing Options

Validity period:	Set length of time (selected) / Set an expiry date 1825 days
Key type:	RSA
Key size:	1024 / 2048 (selected) / 4096
Hash algorithm:	SHA-256 (selected) / SHA-1

Subject Alternative Name

○ Email:

○ User Principal Name (UPN):

○ URI:

○ DNS:

Other Extensions

○ Add CRL Distribution Points extension (Location: http://fac.school.net/cert/crl/RootCA.crl) Edit device FQDN

○ Add OCSP Responder URL (Location: http://fac.school.net:2560) Edit device FQDN

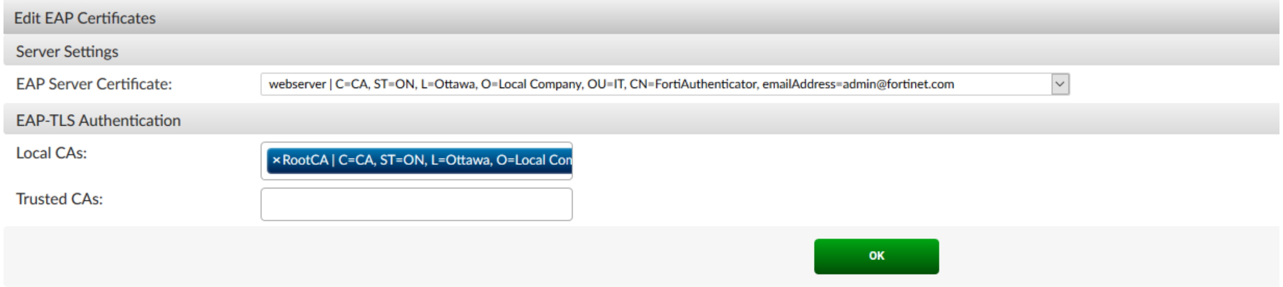
⊞ Advanced Options: Key Usages

Configuring RADIUS EAP on FortiAuthenticator

In order for the FortiAuthenticator to present the newly created Local Services certificate as its authentication to the WiFi client, the RADIUS-EAP must be configured to use this certificate.

To configure RADIUS EAP on FortiAuthenticator:

1. Go to *Authentication* > *RADIUS Service* > *EAP,* and select *Create New*.
2. Select the corresponding Local Services certificate in the EAP Server Certificate section.
3. Choose the Local CA certificate previous configured in the Local CAs section.



Edit EAP Certificates

Server Settings

EAP Server Certificate: webserver | C=CA, ST=ON, L=Ottawa, O=Local Company, OU=IT, CN=FortiAuthenticator, emailAddress=admin@fortinet.com

EAP-TLS Authentication

Local CAs: ×RootCA | C=CA, ST=ON, L=Ottawa, O=Local Con

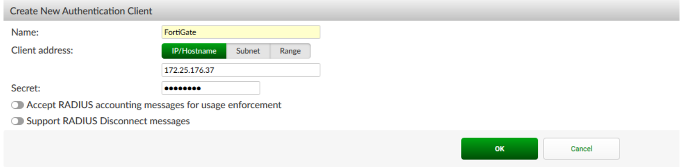
Trusted CAs:

Configuring RADIUS client on FortiAuthenticator

The FortiAuthenticator has to be configured to allow RADIUS clients to make authorization requests to it.

To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, 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.



Create New Authentication Client

Name: FortiGate

Client address: IP/Hostname | Subnet | Range

172.25.176.37

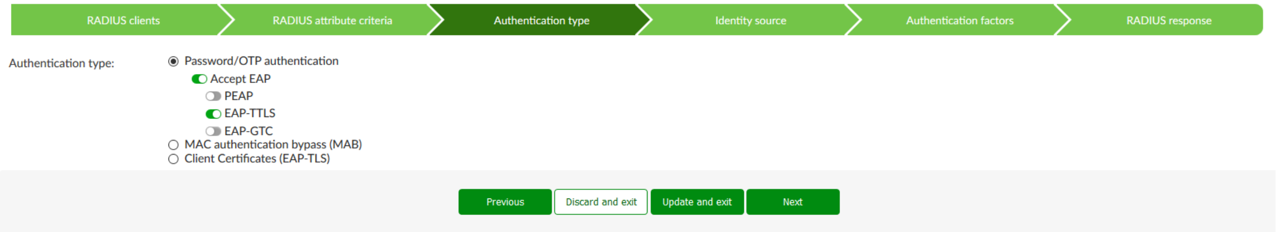
Secret: ••••••••

Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Set the authentication type as *Password/OTP authentication*, and enable *Accept EAP* with only *EAP-TTLS* selected.
   EAP-TLS should be the only EAP type selected to prevent fallback to a less secure version of authentication if a certificate is not presented by the WiFi client.



Authentication type:

● Password/OTP authentication
  Accept EAP
    PEAP
    EAP-TTLS
    EAP-GTC
○ MAC authentication bypass (MAB)
○ Client Certificates (EAP-TLS)

5. Choose a username format (in this example: *username@realm*), select the *Local* realm.

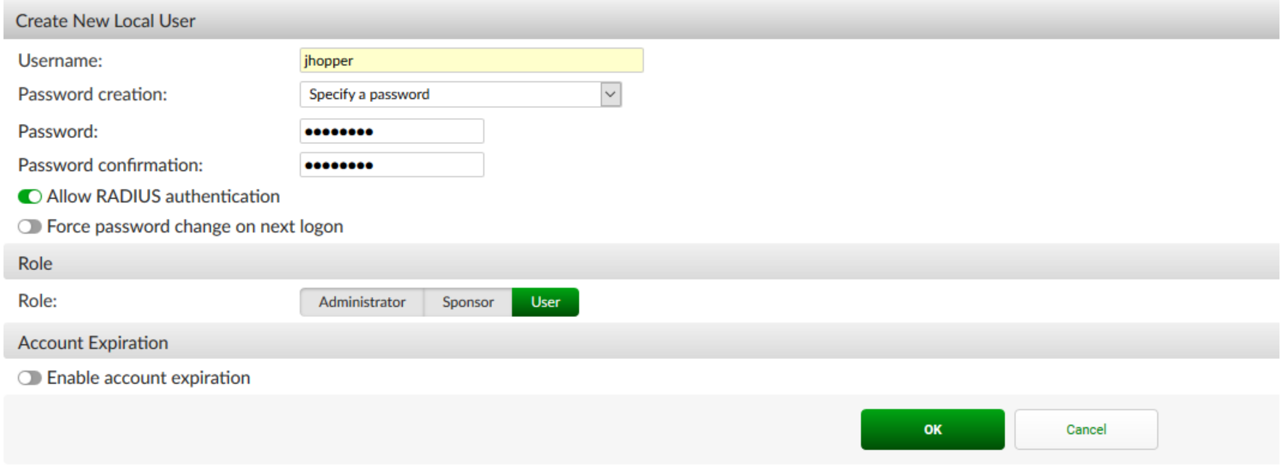
6. Set the authentication method to *Password only authentication*.
7. Review the RADIUS response, and click *Save and Exit*.

Configuring local user on FortiAuthenticator

The authentication of the WiFi client will be tied to a user account on the FortiAuthenticator. In this scenario, a local user will be configured but remote users associated with LDAP can be configured as well.

To configure a local user:

1. Go to *Authentication* > *User Management* > *Local Users* and select *Create New*.
   Fill out applicable user information.



Create New Local User

Username:	jhopper
Password creation:	Specify a password
Password:	••••••••
Password confirmation:	••••••••

☑ Allow RADIUS authentication

□ Force password change on next logon

Role

Role: Administrator | Sponsor | [✓ User]

Account Expiration

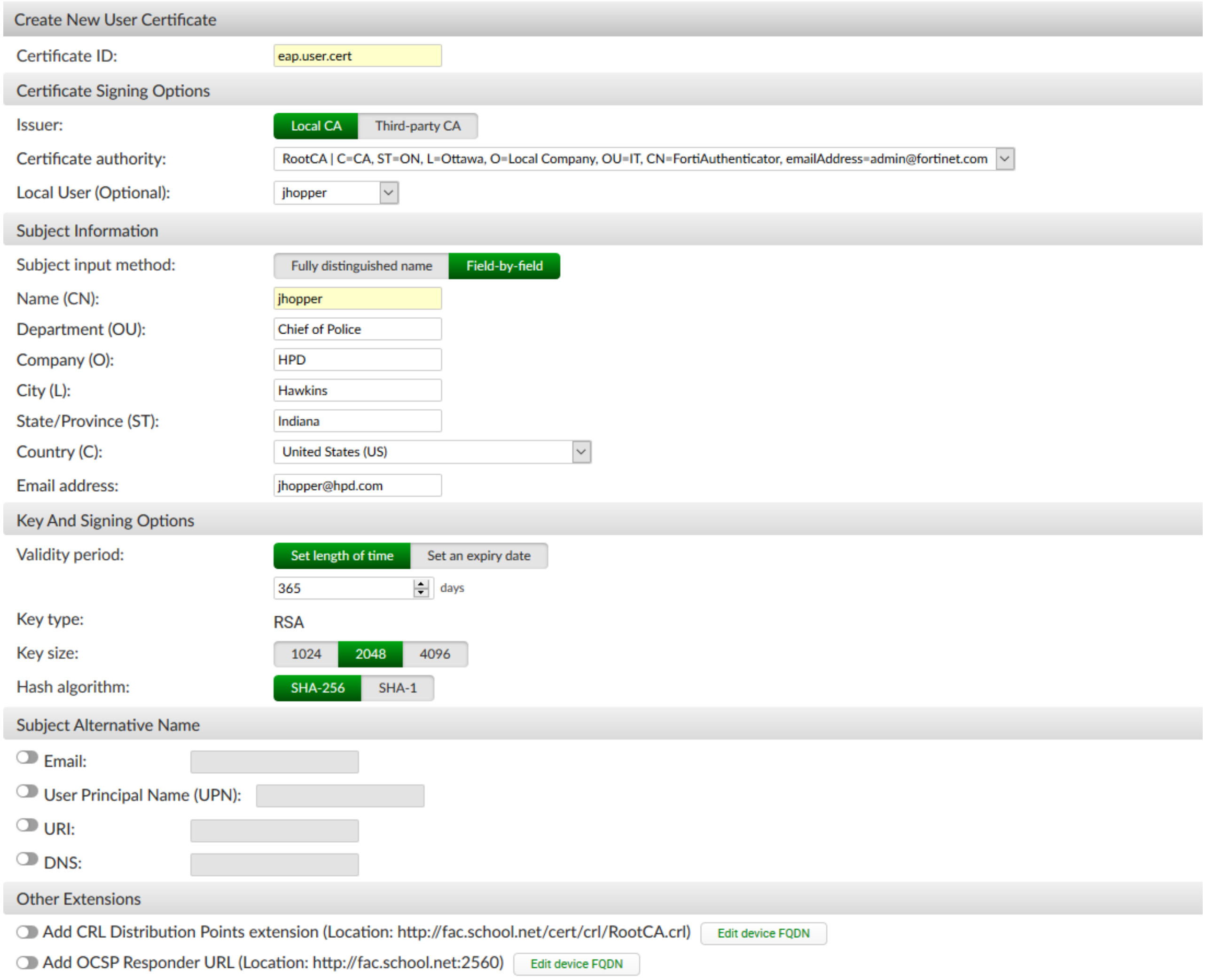
□ Enable account expiration

Configuring local user certificate on FortiAuthenticator

The certificate created locally on the FortiAuthenticator will be associated with the local user. It is important to note that the *Name (CN)* must match the username exactly of the user that is registered in the FortiAuthenticator (in the example, *eap-user*).

To configure the local user certificate:

1. Go to *Certificate Management* > *End Entities* > *Users* and select *Create New*.
   Fill out applicable user information to map the certificate to the correct user.



Create New User Certificate

Certificate ID:	eap.user.cert

Certificate Signing Options

Issuer:	[✓ Local CA] Third-party CA
Certificate authority:	RootCA | C=CA, ST=ON, L=Ottawa, O=Local Company, OU=IT, CN=FortiAuthenticator, emailAddress=admin@fortinet.com
Local User (Optional):	jhopper

Subject Information

Subject input method:	Fully distinguished name [✓ Field-by-field]
Name (CN):	jhopper
Department (OU):	Chief of Police
Company (O):	HPD
City (L):	Hawkins
State/Province (ST):	Indiana
Country (C):	United States (US)
Email address:	jhopper@hpd.com

Key And Signing Options

Validity period:	[✓ Set length of time] Set an expiry date
	365 days
Key type:	RSA
Key size:	1024 [✓ 2048] 4096
Hash algorithm:	[✓ SHA-256] SHA-1

Subject Alternative Name

○ Email:

○ User Principal Name (UPN):

○ URI:

○ DNS:

Other Extensions

○ Add CRL Distribution Points extension (Location: http://fac.school.net/cert/crl/RootCA.crl) Edit device FQDN

○ Add OCSP Responder URL (Location: http://fac.school.net:2560) Edit device FQDN

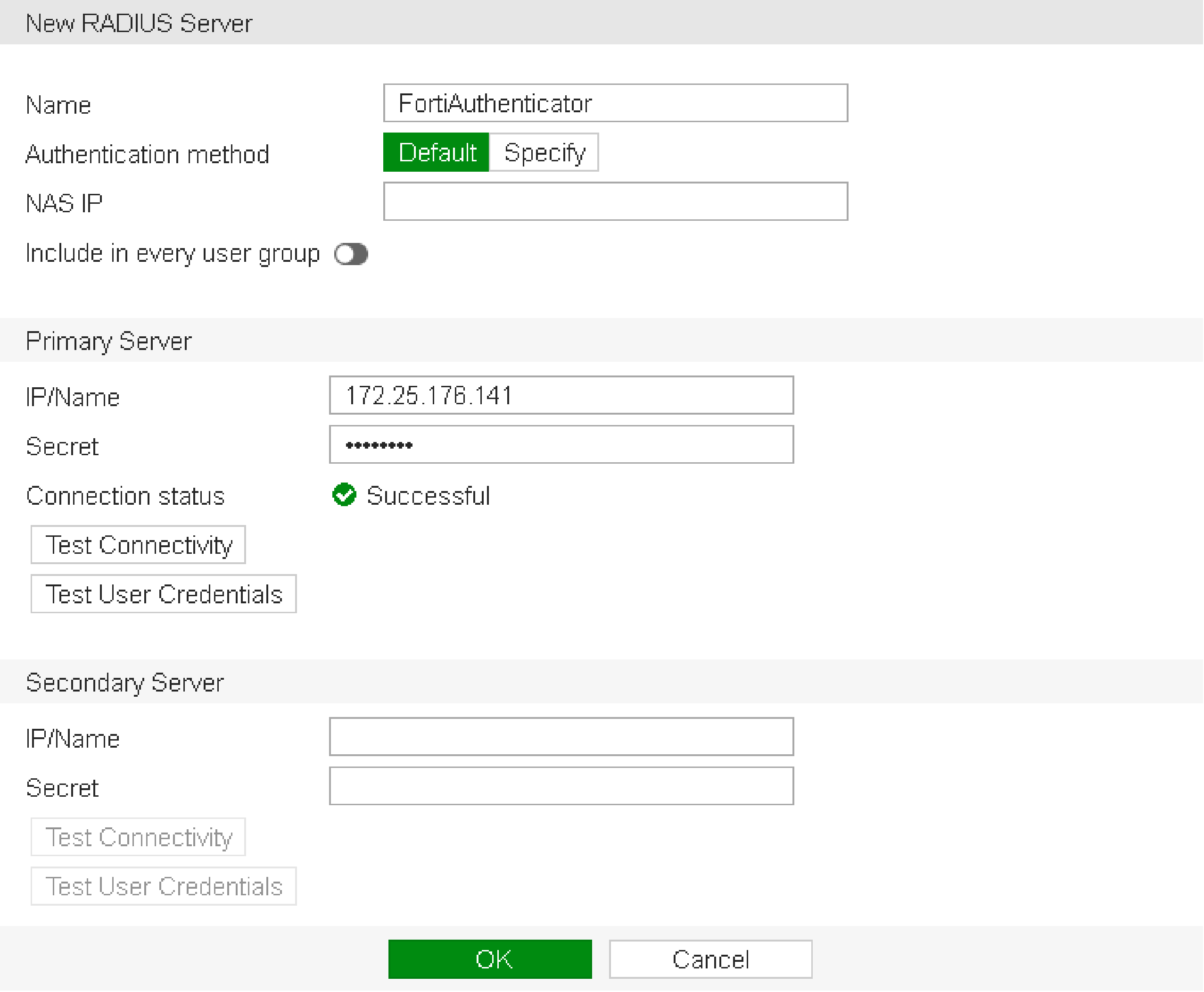
Creating RADIUS server on FortiGate

In order to proxy the authentication request from the wireless client, the FortiGate will need to have a RADIUS server to submit the authentication request to.

To create the RADIUS server on FortiGate:

1. On the FortiGate, go to *User & Device* > *RADIUS Servers* and select *Create New*. Enter a *Name*, the FortiAuthenticator's IP address, and the same *Secret* set on the FortiAuthenticator.

Select *Test Connectivity* to confirm the successful connection.



New RADIUS Server

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

Primary Server

IP/Name	172.25.176.141
Secret	•••••••••
Connection status	✓ Successful

Secondary Server

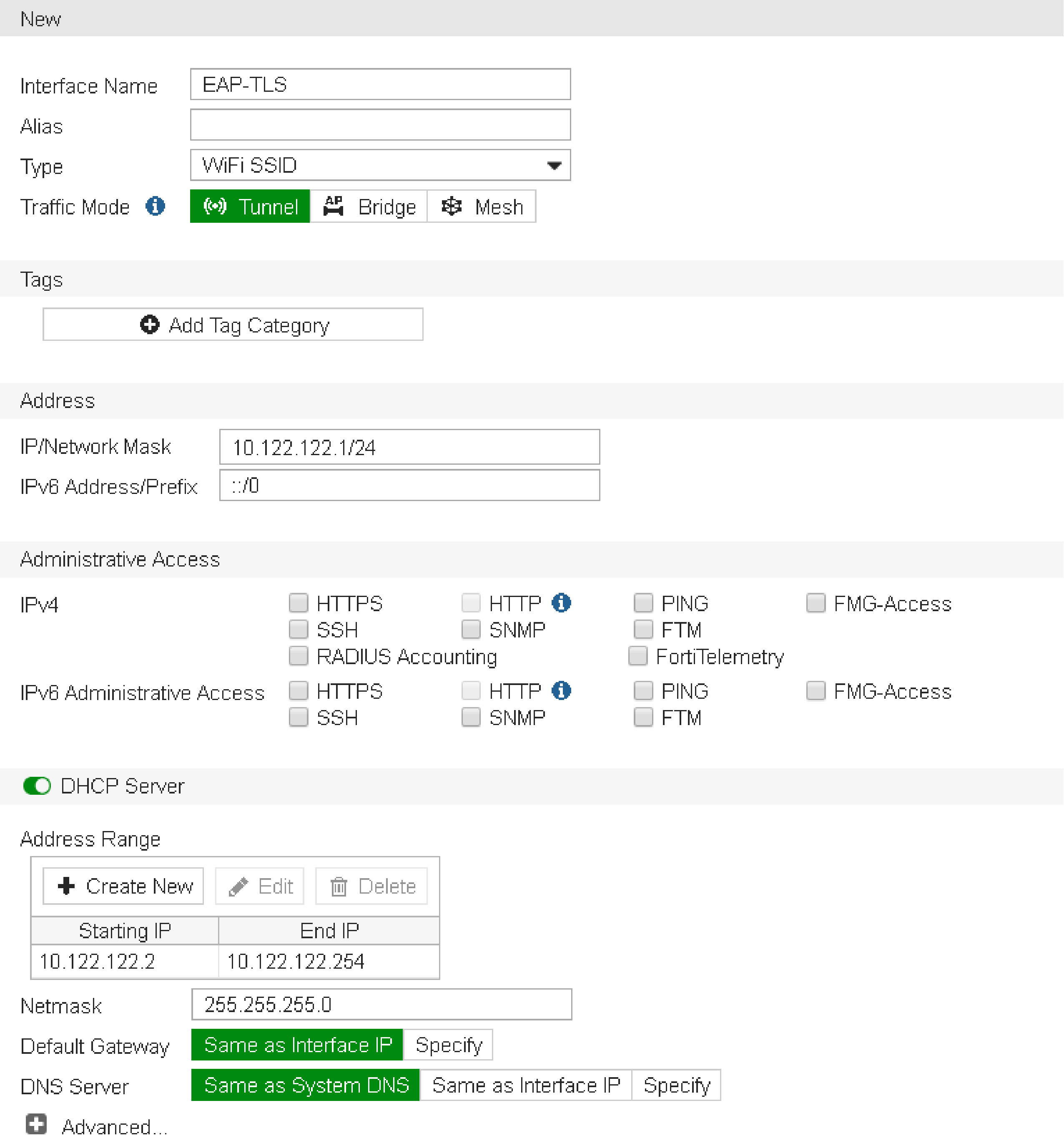
IP/Name	
Secret	

Creating WiFi SSID on FortiGate

In order for the WiFi client to connect using its certificate a SSID has to be configured on the FortiGate to accept this type of authentication.

To create the WiFi SSID:

1. Go to *WiFi & Switch Controller > SSID* and create an SSID with DHCP for clients.



New

Interface Name	EAP-TLS
Alias	
Type	WiFi SSID
Traffic Mode	[✓ Tunnel] Bridge Mesh

Tags

Add Tag Category

Address

IP/Network Mask	10.122.122.1/24
IPv6 Address/Prefix	::/0

Administrative Access

IPv4: □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ FortiTelemetry

IPv6 Administrative Access: □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM

● DHCP Server

Address Range

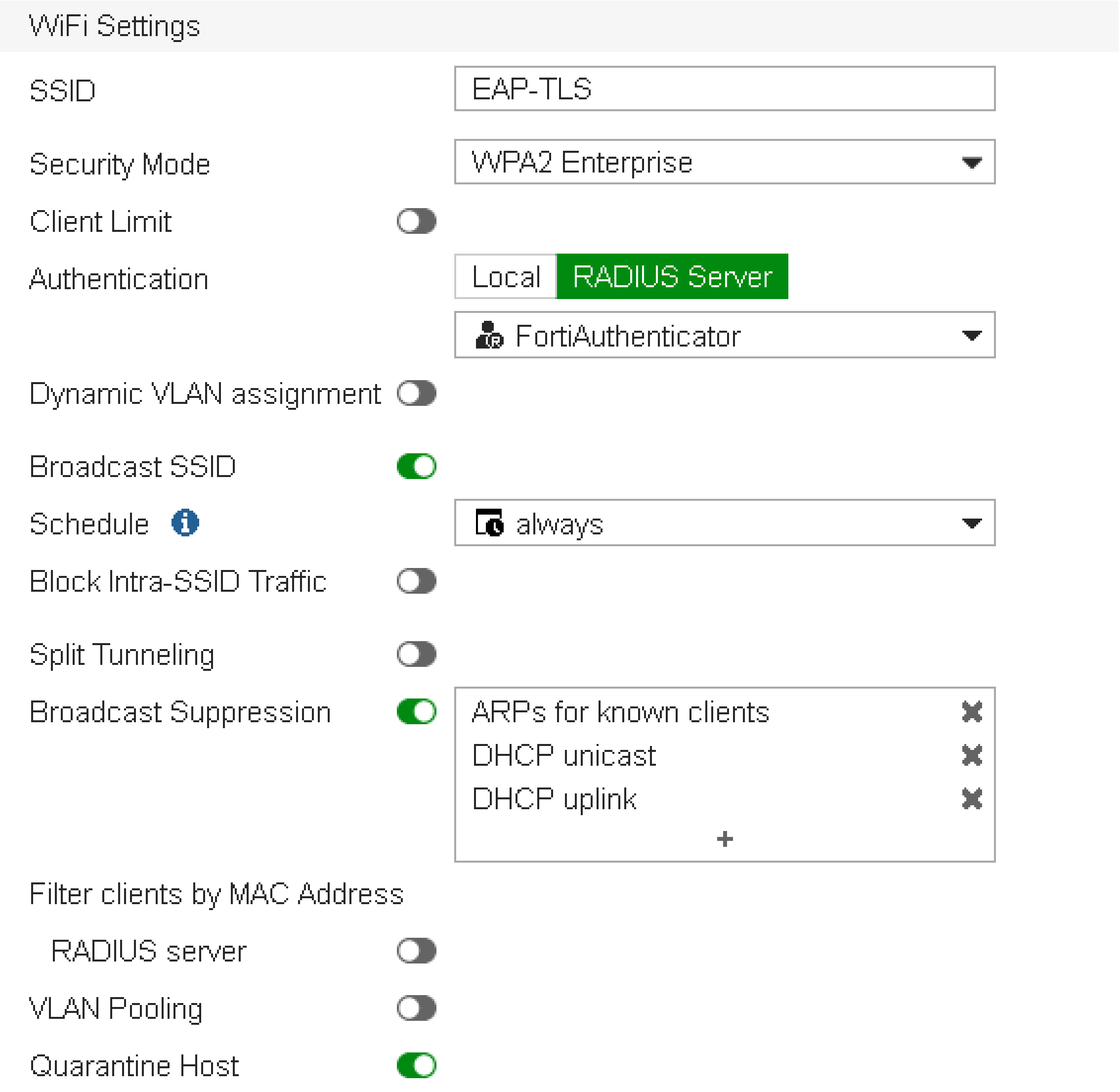
Create New Edit Delete

Starting IP	End IP
10.122.122.2	10.122.122.254

Netmask	255.255.255.0
Default Gateway	[✓ Same as Interface IP] Specify
DNS Server	[✓ Same as System DNS] Same as Interface IP Specify

Advanced...

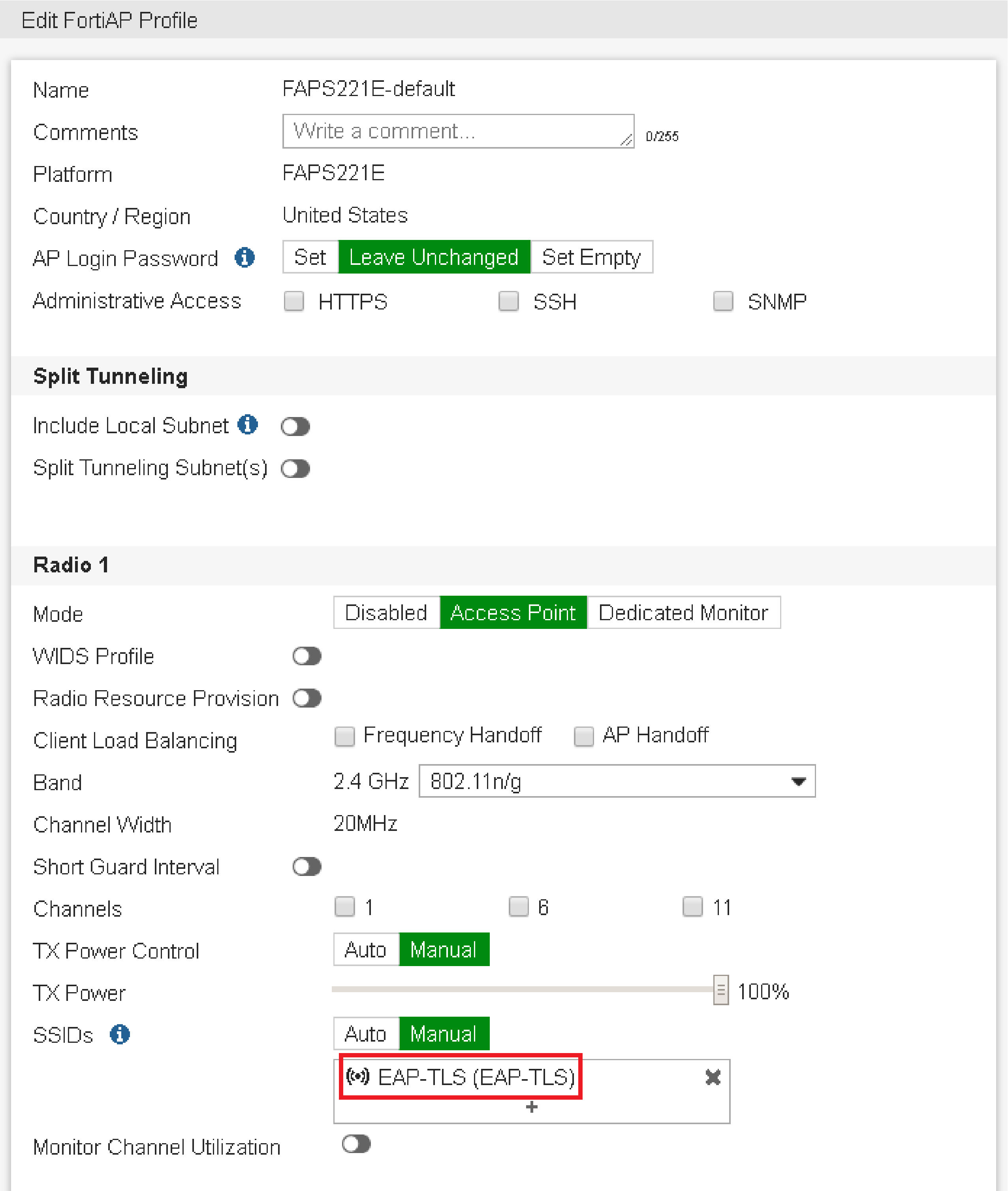
2. Set the following *WiFi Settings*, assigning the *RADIUS Server* configured earlier.



WiFi Settings

SSID	EAP-TLS
Security Mode	WPA2 Enterprise
Client Limit	○
Authentication	Local [✓ RADIUS Server] FortiAuthenticator
Dynamic VLAN assignment	○
Broadcast SSID	●
Schedule	always
Block Intra-SSID Traffic	○
Split Tunneling	○
Broadcast Suppression	● ARPs for known clients DHCP unicast DHCP uplink
Filter clients by MAC Address	
RADIUS server	○
VLAN Pooling	○
Quarantine Host	●

3. Then go to *WiFi & Switch Controller* > *FortiAP Profiles* and edit your FortiAP default profile. Select the new SSID for both *Radio 1* and *Radio 2*.



Edit FortiAP Profile

Name	FAPS221E-default
Comments	Write a comment... 0/255
Platform	FAPS221E
Country / Region	United States
AP Login Password	Set [✓ Leave Unchanged] Set Empty
Administrative Access	□ HTTPS □ SSH □ SNMP

Split Tunneling

Include Local Subnet	○
Split Tunneling Subnet(s)	○

Radio 1

Mode	Disabled [✓ Access Point] Dedicated Monitor
WIDS Profile	○
Radio Resource Provision	○
Client Load Balancing	□ Frequency Handoff □ AP Handoff
Band	2.4 GHz 802.11n/g
Channel Width	20MHz
Short Guard Interval	○
Channels	□ 1 □ 6 □ 11
TX Power Control	Auto [✓ Manual]
TX Power	100%
SSIDs	Auto [✓ Manual] EAP-TLS (EAP-TLS)
Monitor Channel Utilization	○

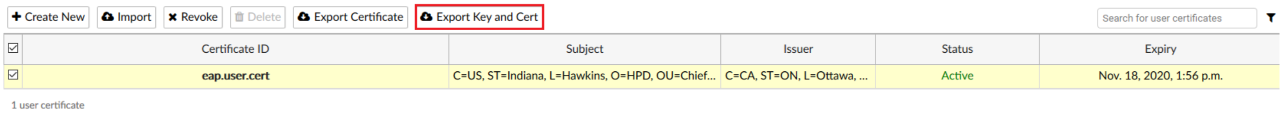
4. Then go to *Policy & Objects* > *IPv4 Policy* and create a policy that allows outbound traffic from the *EAP-TLS* wireless interface to the Internet.

Exporting user certificate from FortiAuthenticator

In order for the WiFi client to authenticate with the RADIUS server, the user certificate created in the FortiAuthenticator must first be exported.

To export the FortiAuthenticator user certificate:

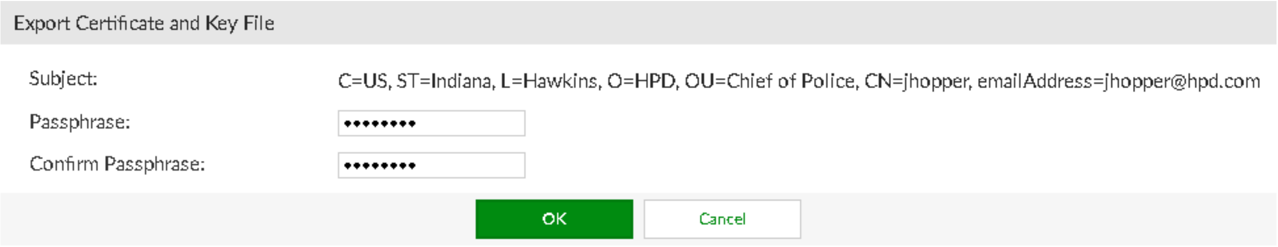
1. On the FortiAuthenticator, go to *Certificate Management* > *End Entities* > *Users*. Select the certificate and select *Export Key and Cert*.



☑	Certificate ID	Subject	Issuer	Status	Expiry
☑	eap.user.cert	C=US, ST=Indiana, L=Hawkins, O=HPD, OU=Chief...	C=CA, ST=ON, L=Ottawa, ...	Active	Nov. 18, 2020, 1:56 p.m.

1 user certificate

2. In the *Export User Certificate and Key File* dialog, enter and confirm a *Passphrase*. This password will be used when importing the certificate into a Windows 10 computer. Select *OK*.


Export Certificate and Key File

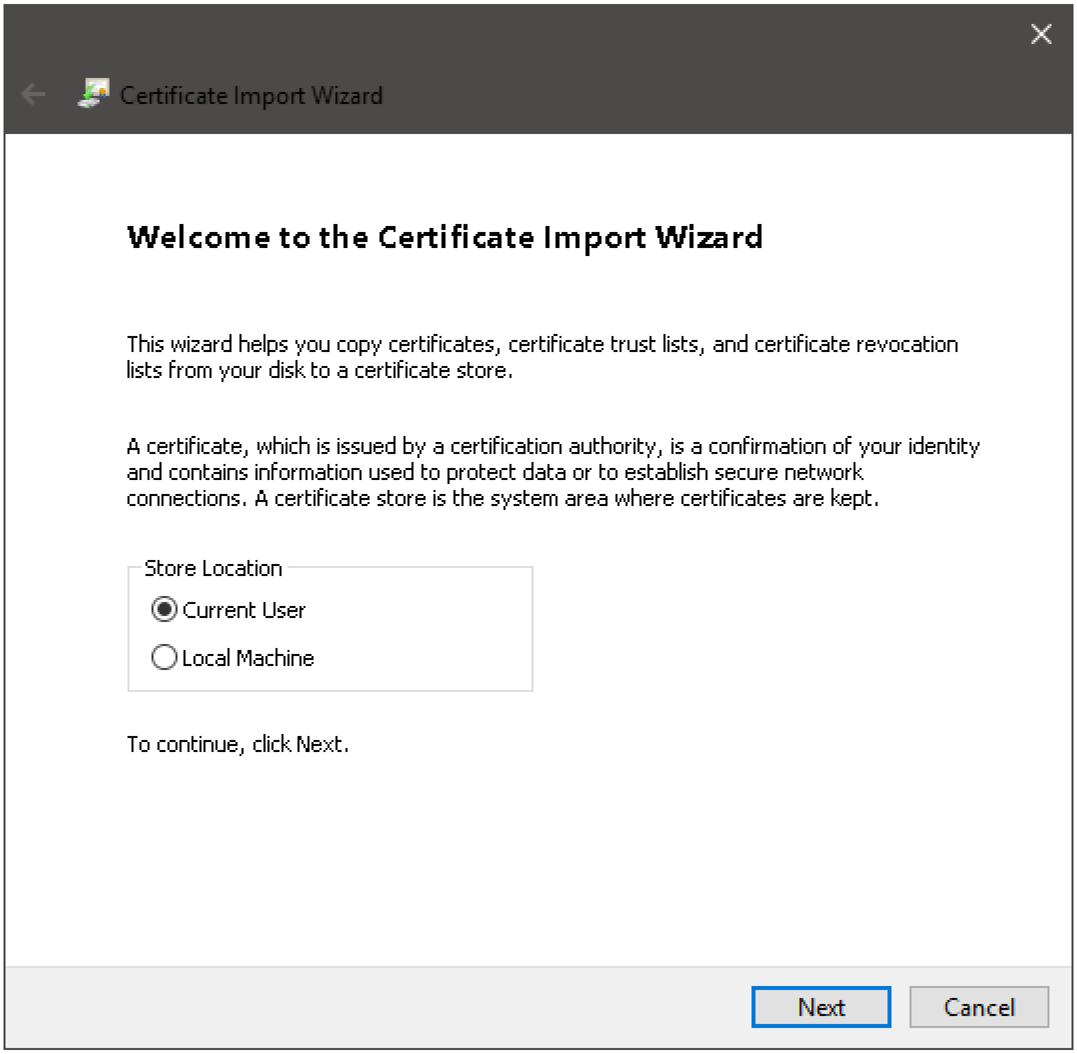
Subject:	C=US, ST=Indiana, L=Hawkins, O=HPD, OU=Chief of Police, CN=jhopper, emailAddress=jhopper@hpd.com
Passphrase:	••••••••
Confirm Passphrase:	••••••••

3. Select *Download PKCS#12 file* to pull this certificate to the Widows 10 computer. Select *Finish*.

Importing user certificate into Windows 10

To import the user certificate:

1. On the Windows 10 computer, double-click the downloaded certificate file from the FortiAuthenticator. This will launch the *Certificate Import Wizard*. Select *Next*.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

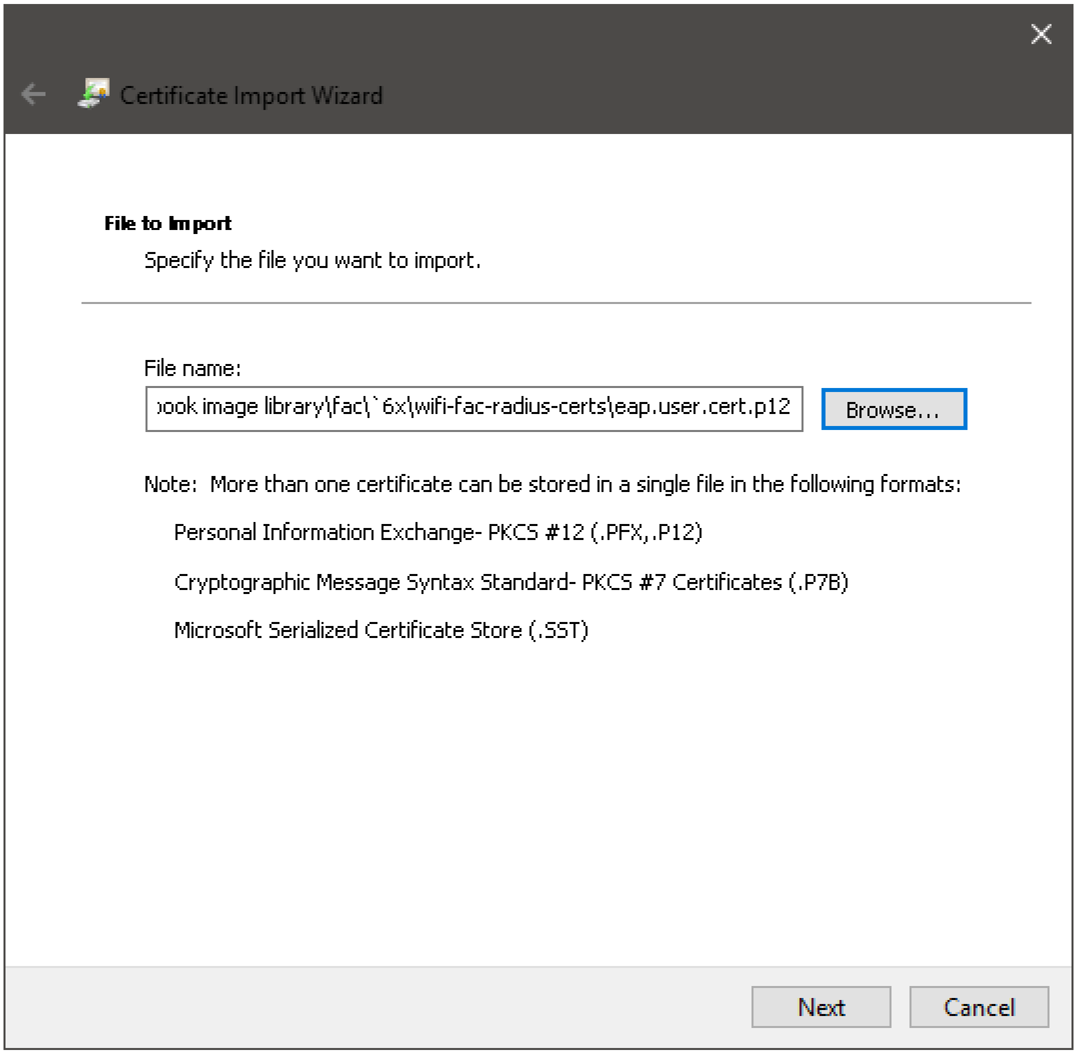
Store Location

● Current User

○ Local Machine

To continue, click Next.

2. Make sure the correct certificate is shown in the *File name* section in the *File to Import* window. Select *Next*.



File to Import

Specify the file you want to import.

File name:

ook image library\fac\`6x\wifi-fac-radius-certs\eap.user.cert.p12

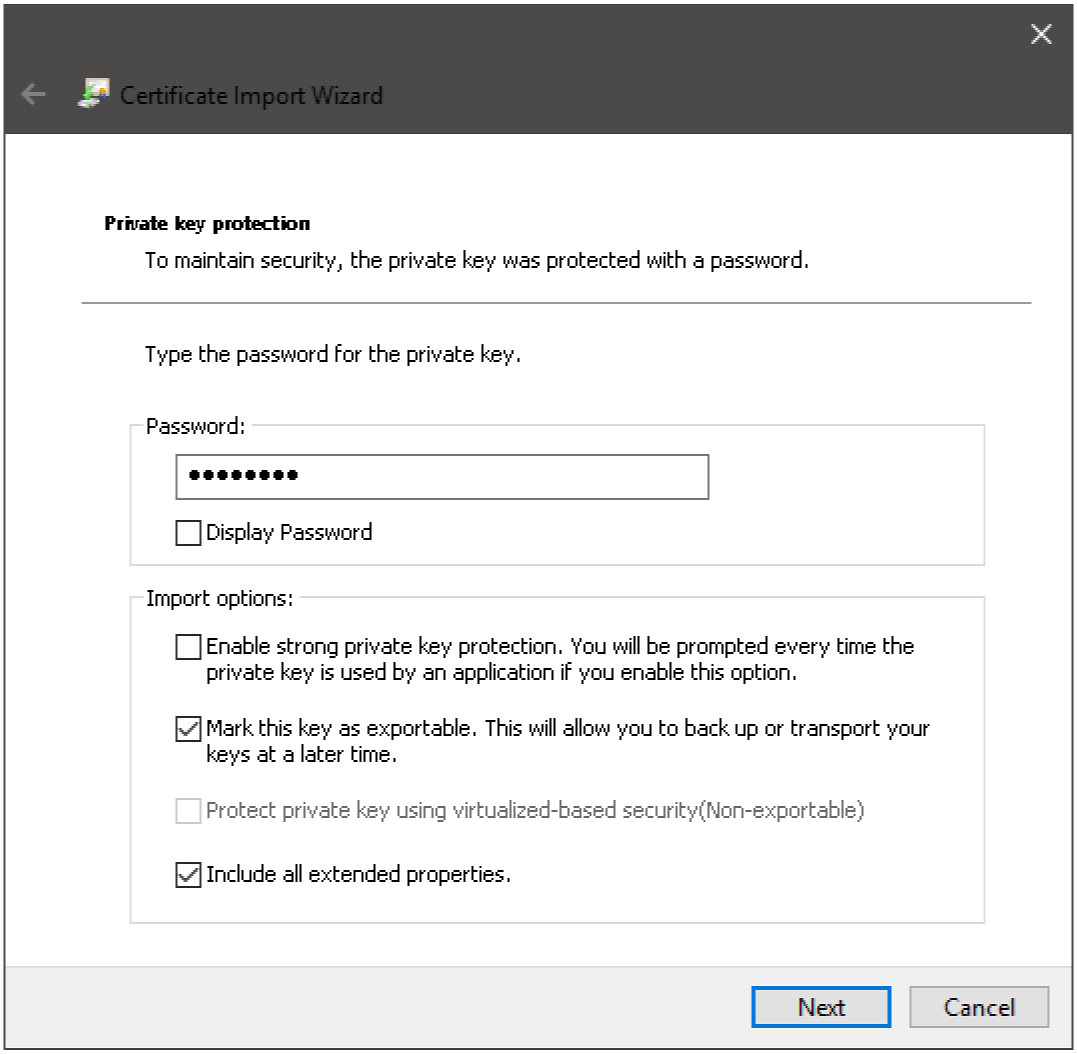
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3. Enter the *Password* created on the FortiAuthenticator during the export of the certificate. Select *Mark this key as exportable* and leave the remaining options to default. Select *Next*.



Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●●●●●●●

□ Display Password

Import options:

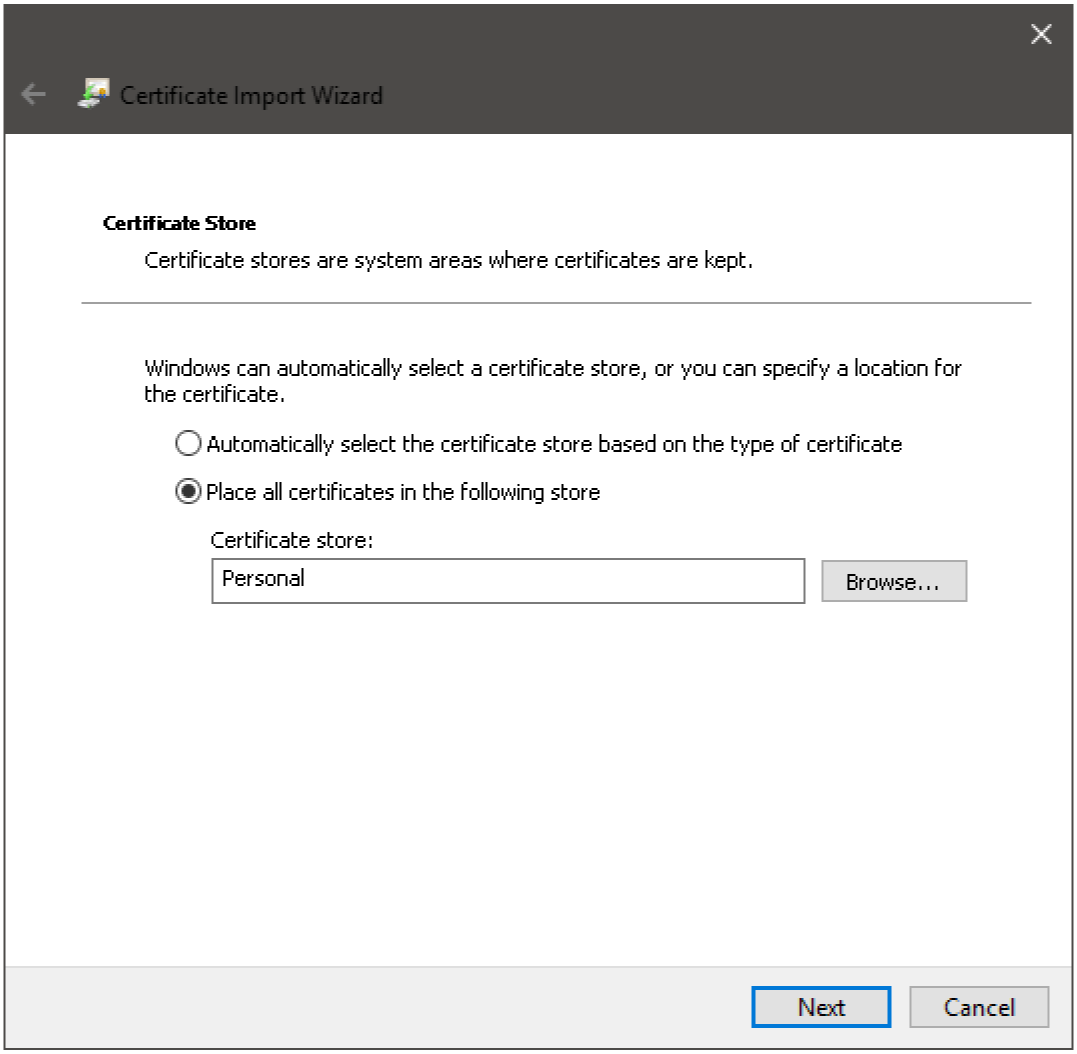
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

4. In the *Certificate Store*, choose the *Place all certificates in the following store*.
   Select *Browse* and choose *Personal*. Select *Next*, and then *Finish*.
   A dialog box will show up confirming the certificate was imported successfully.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

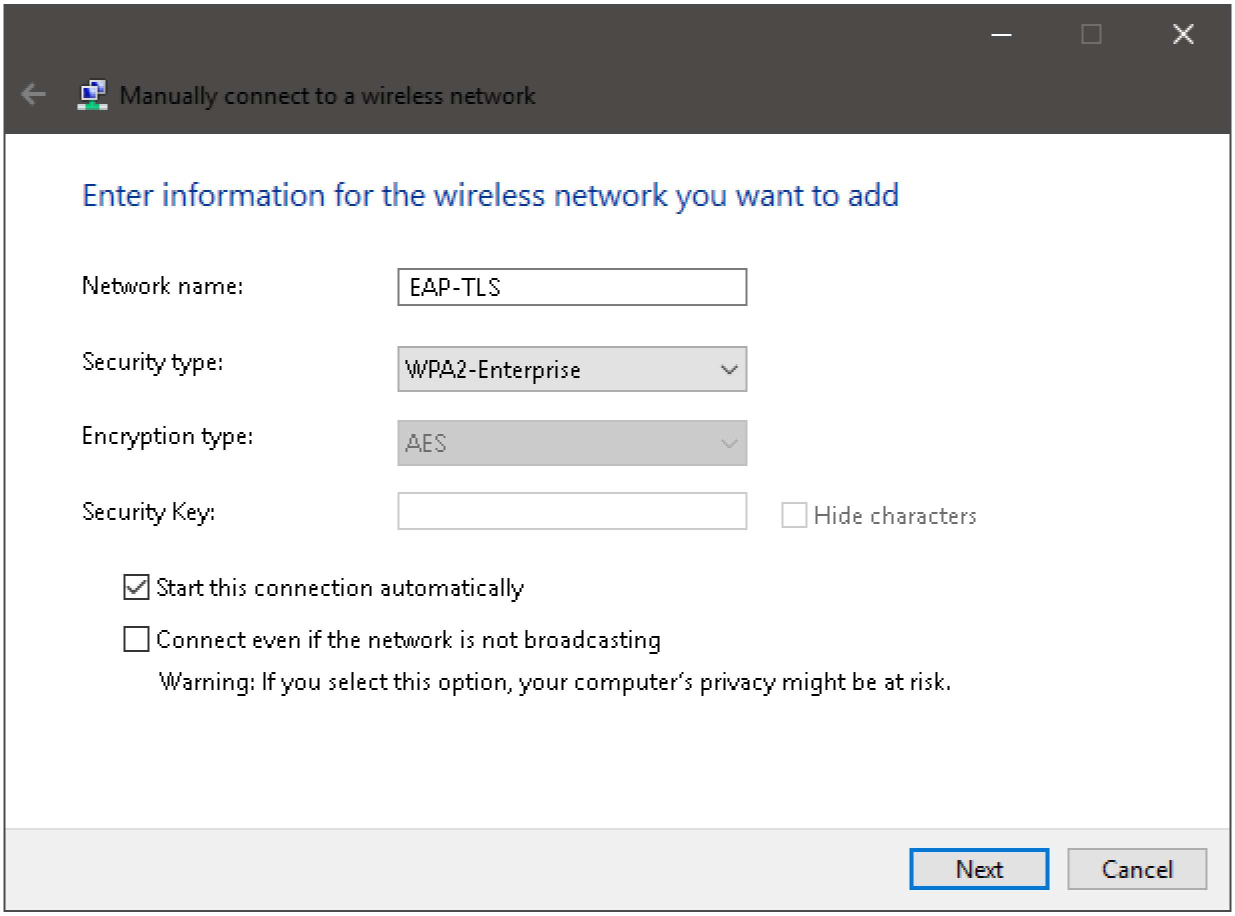
Certificate store: Personal

Configuring Windows 10 wireless profile to use certificate

Create a new wireless SSID for this secure connection, in this case EAP-TLS.

To create a wireless SSID:

1. On Windows 10, got to *Control Panel* > *Network and Sharing Center* > *Set up a new connection or network* > *Manually connect to a wireless network*. Enter a *Network name* and set *Security type* to *WPA2-Enterprise*. The *Encryption type* is set to *AES*.



Enter information for the wireless network you want to add

Network name: EAP-TLS

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

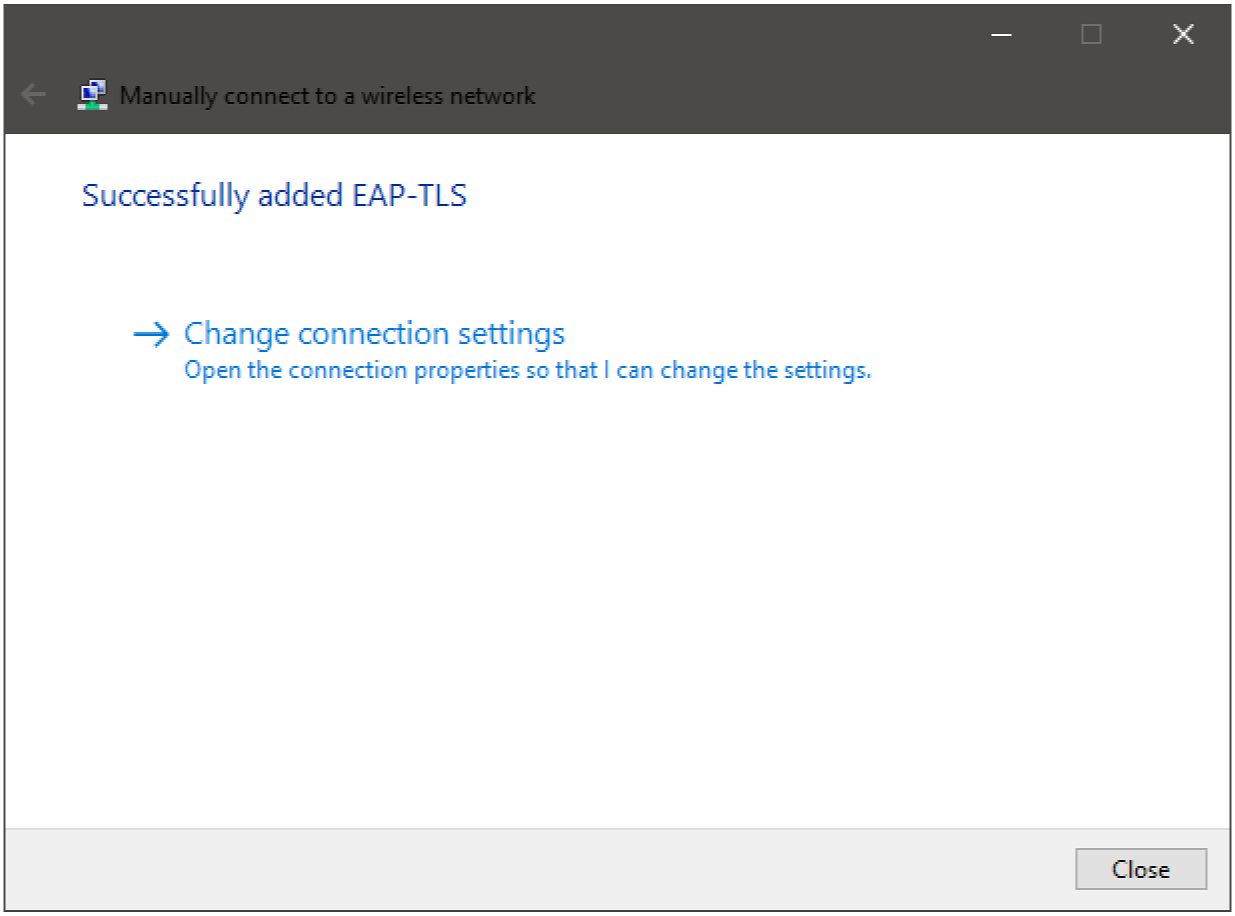
□ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

2. Once created, you have the option to modify the wireless connection. Select *Change connection settings*.

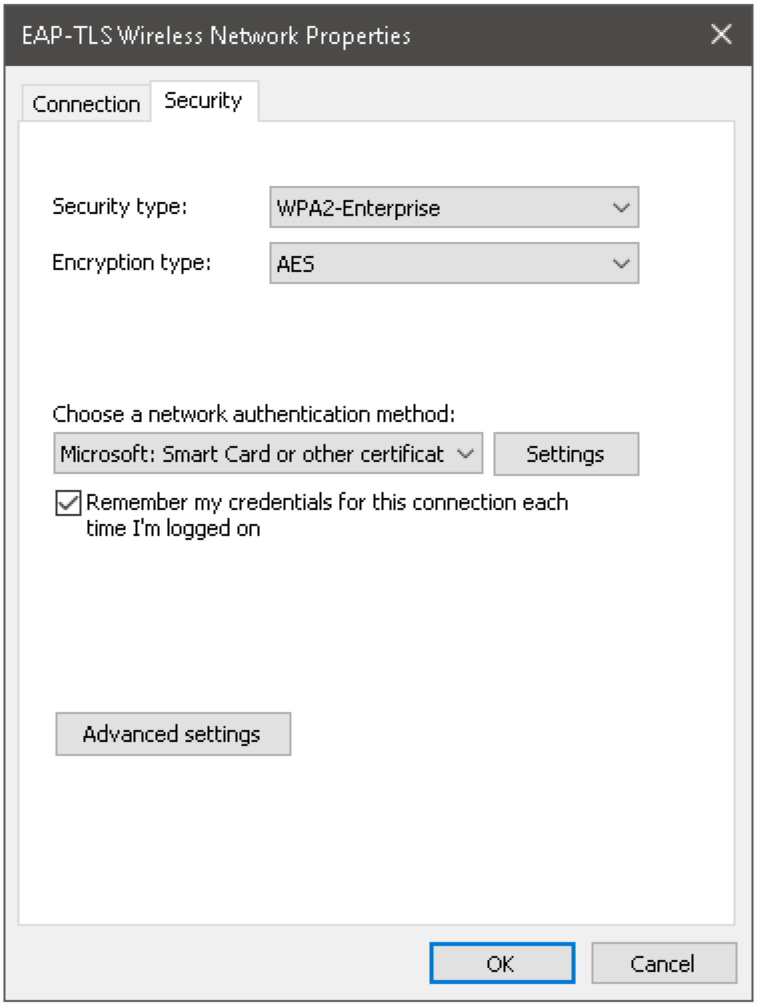


Manually connect to a wireless network

Successfully added EAP-TLS

→ Change connection settings
Open the connection properties so that I can change the settings.

3. In the *Security* tab, set *Choose a network authentication method* to *Microsoft: Smart card or other certificates*, and select *Settings*.



EAP-TLS Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

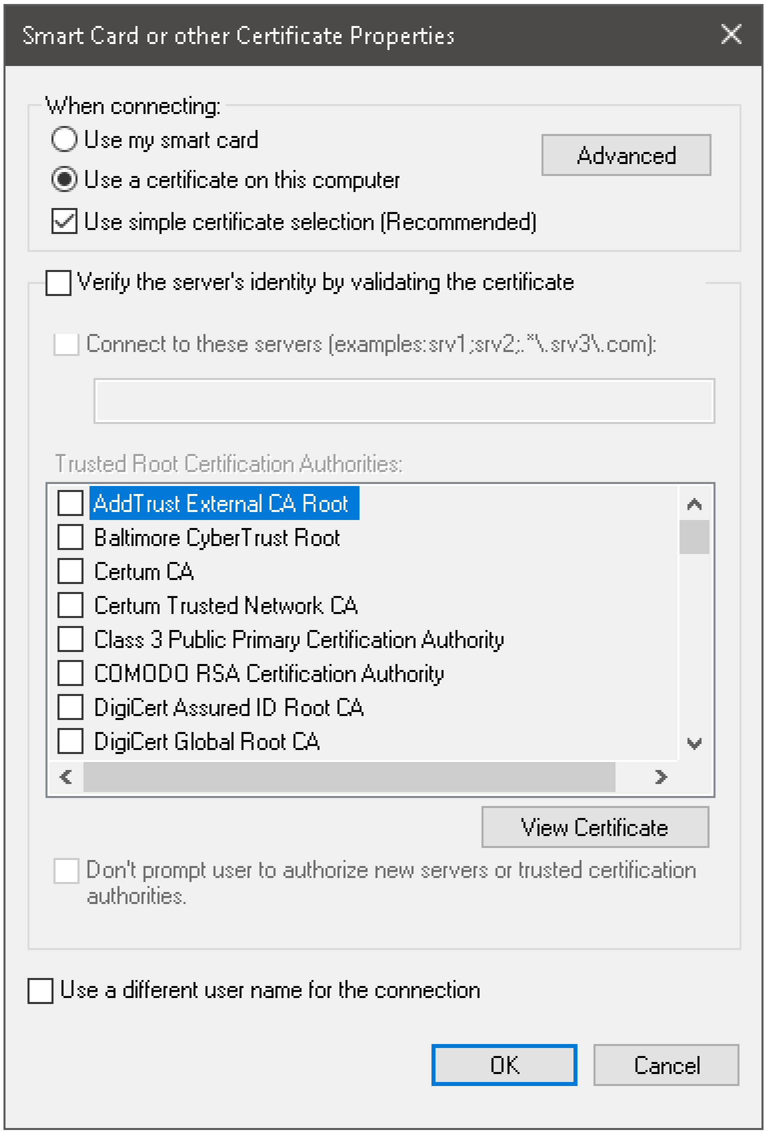
Choose a network authentication method:

Microsoft: Smart Card or other certificat

☑ Remember my credentials for this connection each time I'm logged on

4. Enable both *Use a certificate on this computer* and *Use simple certificate selection*.
   Note that, for simplification purposes, *Verify the server's identity by validating the certificate* has been disabled. However EAP--TLS allows the client to validate the server as well as the server validate the client. To enable this, you will need to import the CA from the FortiAuthenticator to the Windows 10 computer and make sure that it is enabled as a Trusted Root Certification Authority.

   Select *OK* for all dialog windows to confirm all settings. The configuration for the Windows 10 computer has been completed and the user should be able to authenticate to WiFi via the certificate without using their username and password.



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

□ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

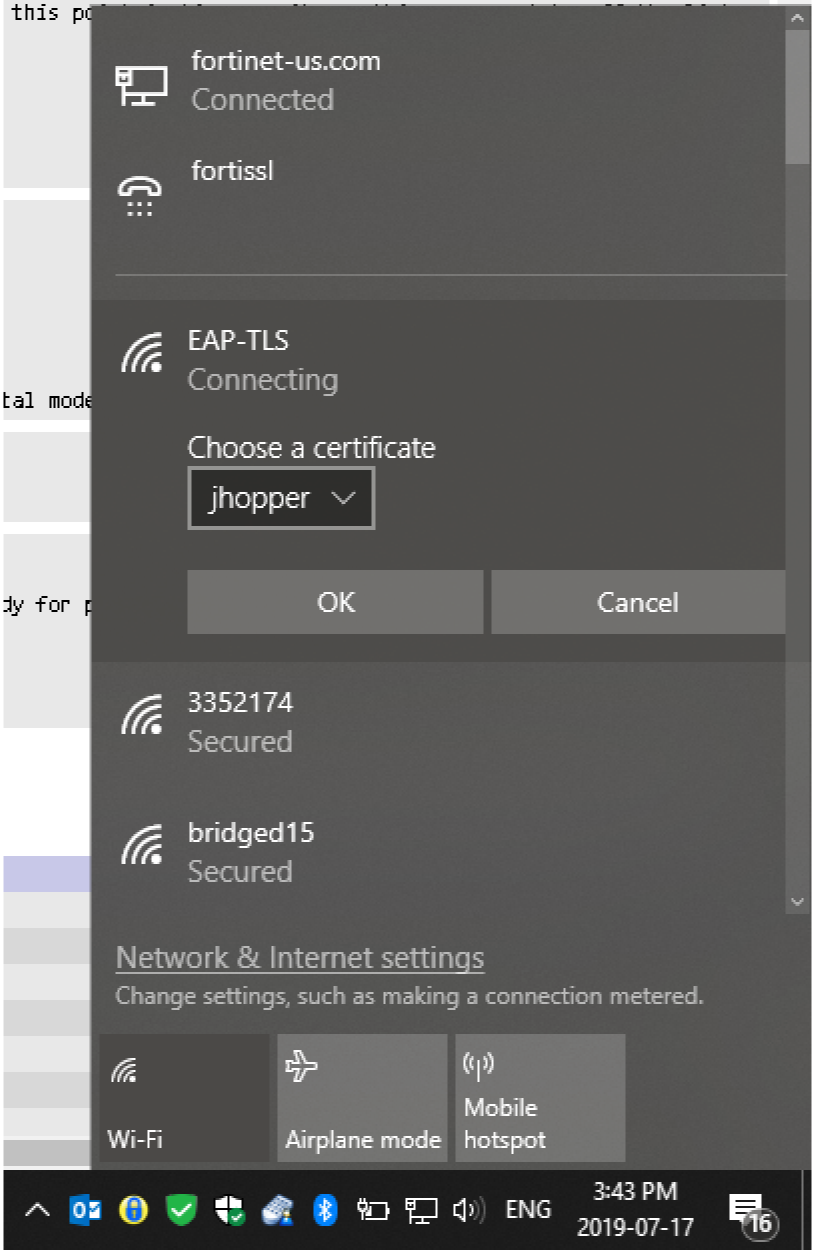
- □ AddTrust External CA Root
- □ Baltimore CyberTrust Root
- □ Certum CA
- □ Certum Trusted Network CA
- □ Class 3 Public Primary Certification Authority
- □ COMODO RSA Certification Authority
- □ DigiCert Assured ID Root CA
- □ DigiCert Global Root CA

□ Don't prompt user to authorize new servers or trusted certification authorities.

□ Use a different user name for the connection

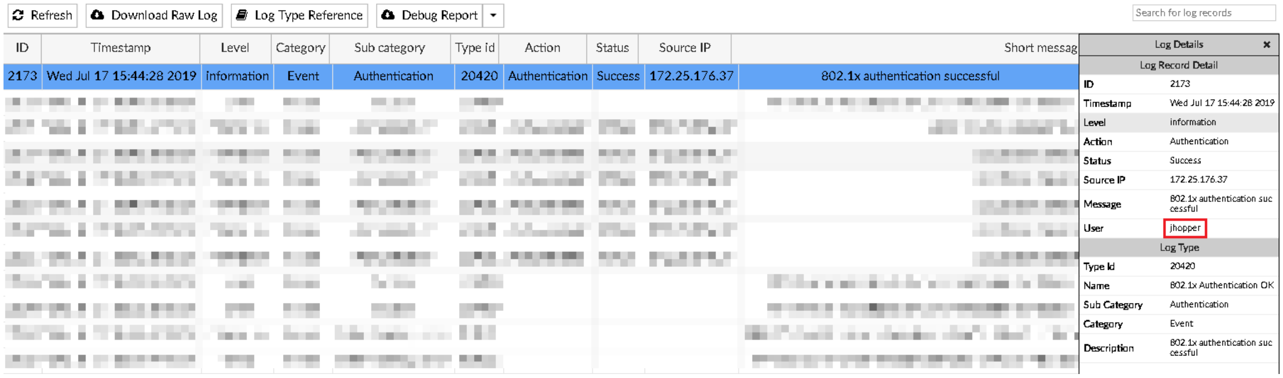
Results

1. On the user's device, attempt to connect to the WiFi. Select the user's certificate and select *OK*.



Choose a certificate
jhopper

2. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* to confirm the successful authentication.



ID	Timestamp	Level	Category	Sub category	Type Id	Action	Status	Source IP	Short messag
2173	Wed Jul 17 15:44:28 2019	Information	Event	Authentication	20420	Authentication	Success	172.25.176.37	802.1x authentication successful

[redacted]

Log Details

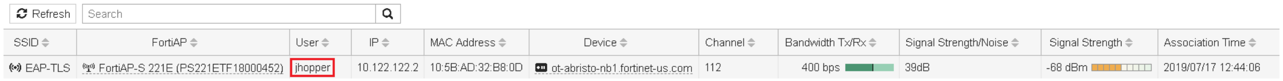
Log Record Detail

ID	2173
Timestamp	Wed Jul 17 15:44:28 2019
Level	information
Action	Authentication
Status	Success
Source IP	172.25.176.37
Message	802.1x authentication successful
User	jhopper

Log Type

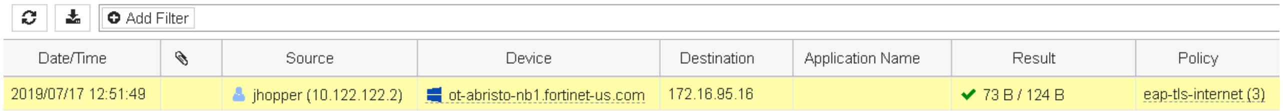
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

3. On the FortiGate, go to **Monitor > WiFi Client Monitor** to view various information about the client.

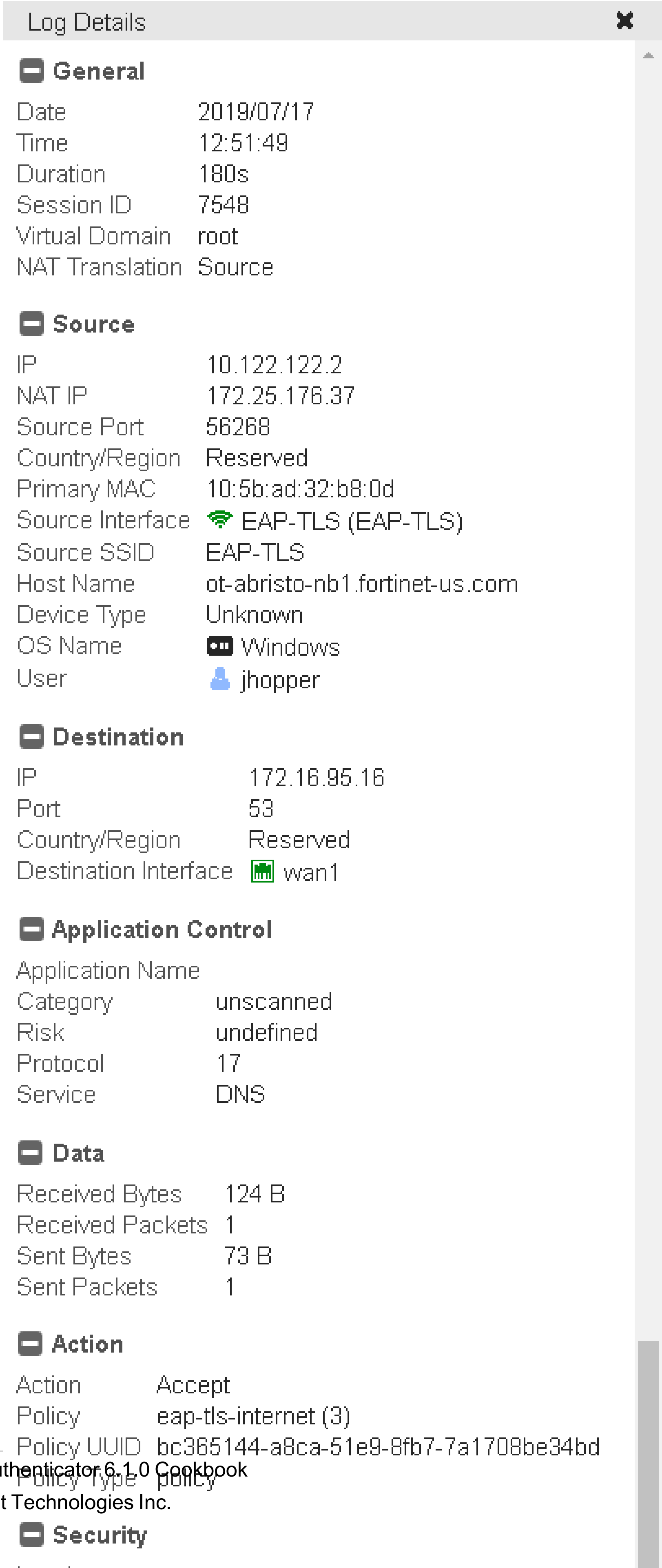


SSID	FortiAP	User	IP	MAC Address	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal Strength	Association Time
EAP-TLS	FortiAP-S 221E (PS221ETF18000452)	jhopper	10.122.122.2	10:5B:AD:32:B8:0D	ot-abristo-nb1.fortinet-us.com	112	400 bps	39dB	-68 dBm	2019/07/17 12:44:06

You can also go to *Log & Report > Forward Traffic* to view more log details.



Date/Time		Source	Device	Destination	Application Name	Result	Policy
2019/07/17 12:51:49		jhopper (10.122.122.2)	ot-abristo-nb1.fortinet-us.com	172.16.95.16		✓ 73 B / 124 B	eap-tls-internet (3)



Log Details

General

Date	2019/07/17
Time	12:51:49
Duration	180s
Session ID	7548
Virtual Domain	root
NAT Translation	Source

Source

IP	10.122.122.2
NAT IP	172.25.176.37
Source Port	56268
Country/Region	Reserved
Primary MAC	10:5b:ad:32:b8:0d
Source Interface	EAP-TLS (EAP-TLS)
Source SSID	EAP-TLS
Host Name	ot-abristo-nb1.fortinet-us.com
Device Type	Unknown
OS Name	Windows
User	jhopper

Destination

IP	172.16.95.16
Port	53
Country/Region	Reserved
Destination Interface	wan1

Application Control

Application Name	
Category	unscanned
Risk	undefined
Protocol	17
Service	DNS

Data

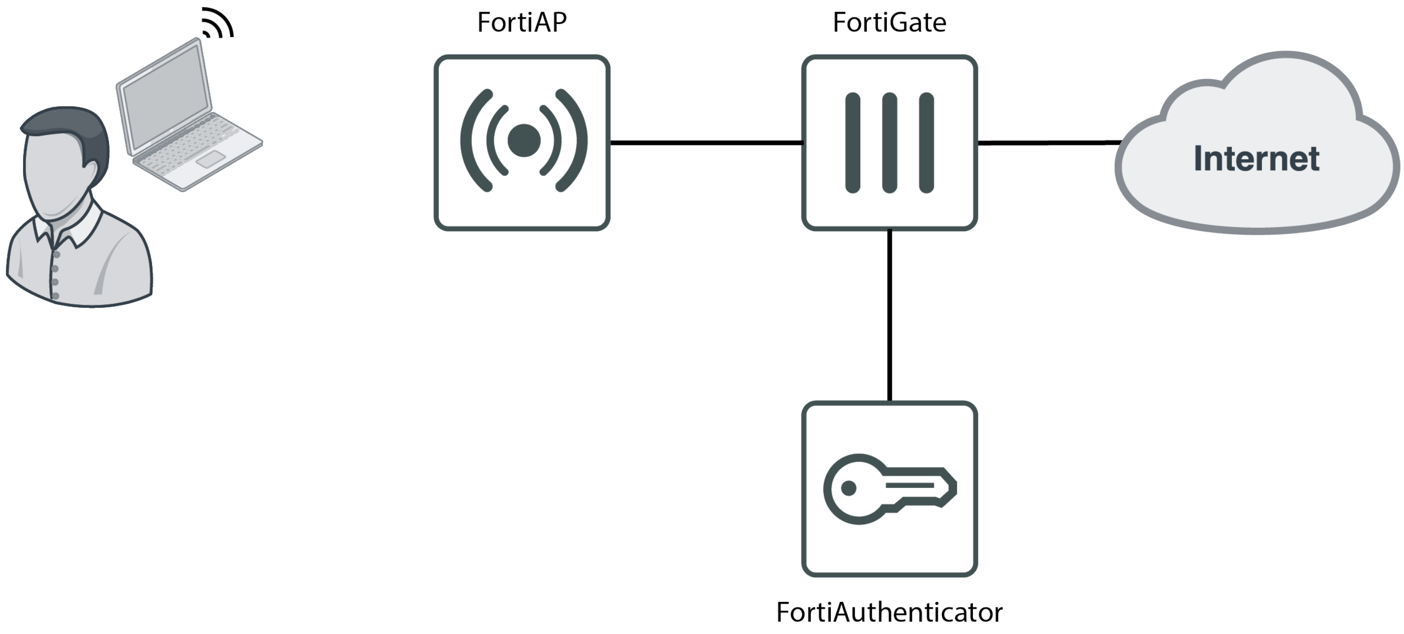
Received Bytes	124 B
Received Packets	1
Sent Bytes	73 B
Sent Packets	1

Action

Action	Accept
Policy	eap-tls-internet (3)
Policy UUID	bc365144-a8ca-51e9-8fb7-7a1708be34bd
Policy Type	policy

Security

WiFi RADIUS authentication with FortiAuthenticator



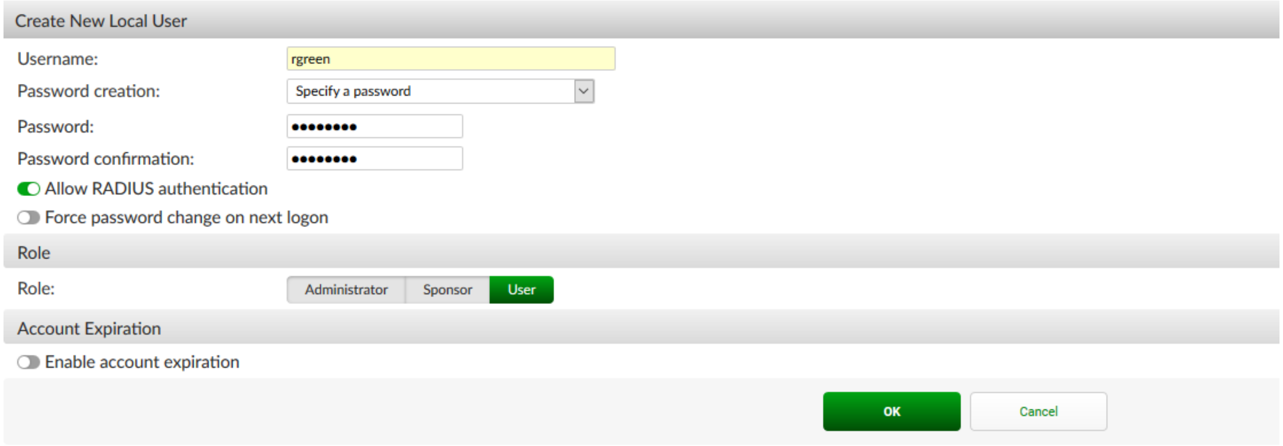
In this example, you use a RADIUS server to authenticate your WiFi clients.

The RADIUS server is a FortiAuthenticator that is used authenticate users who belong to the employees user group.

Creating users and user groups on the FortiAuthenticator

To create users and user groups:

1. Go to *Authentication* > *User Management* > *Local Users* and create a user account.



Create New Local User

Username:	rgreen
Password creation:	Specify a password
Password:	••••••••
Password confirmation:	••••••••

● Allow RADIUS authentication

○ Force password change on next logon

Role

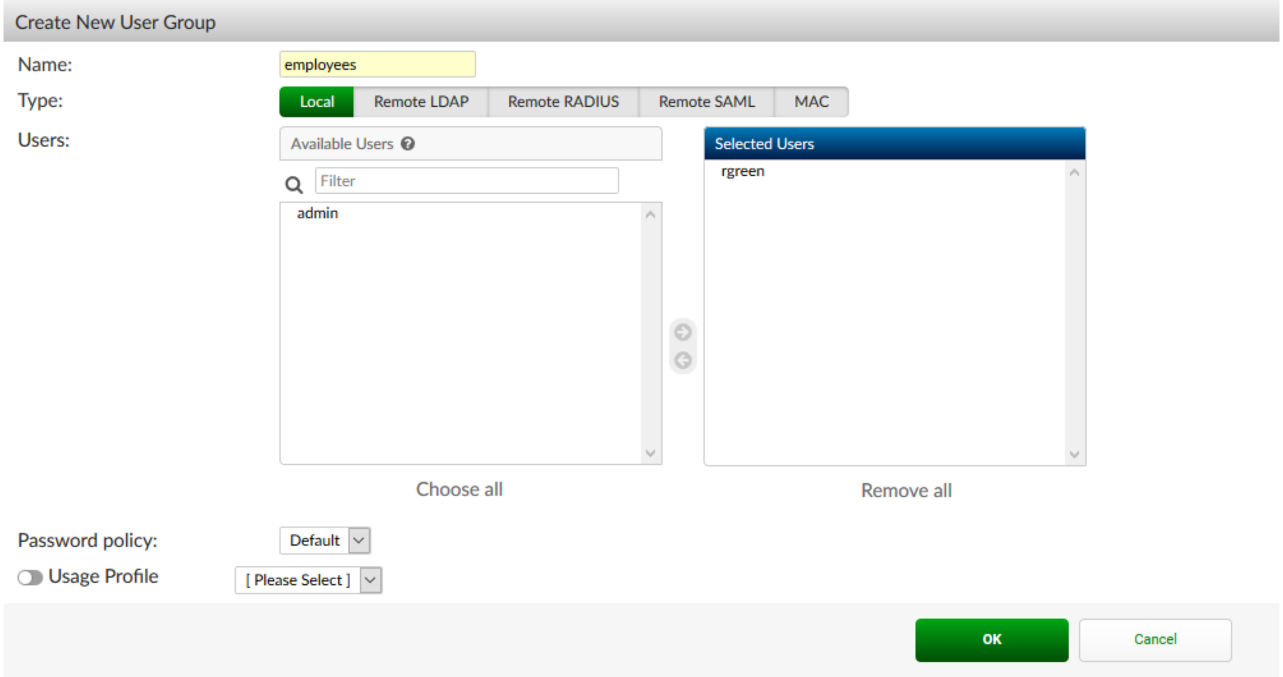
Role: Administrator | Sponsor | [✓ User]

Account Expiration

○ Enable account expiration

2. Then go to *Authentication* > *User Management* > *User Groups* and create a local user group (employees), adding

the newly created user.



Create New User Group

Name: employees

Type: Local

Users:

Available Users: admin

Selected Users: rgreen

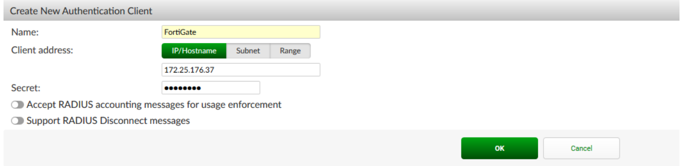
Password policy: Default

Usage Profile: [Please Select]

Registering the FortiGate as a RADIUS client on the FortiAuthenticator

To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New*.
2. Enter a *Name*, 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.



Create New Authentication Client

Name: FortiGate

Client address: IP/Hostname

172.25.176.37

Secret: •••••••••

Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

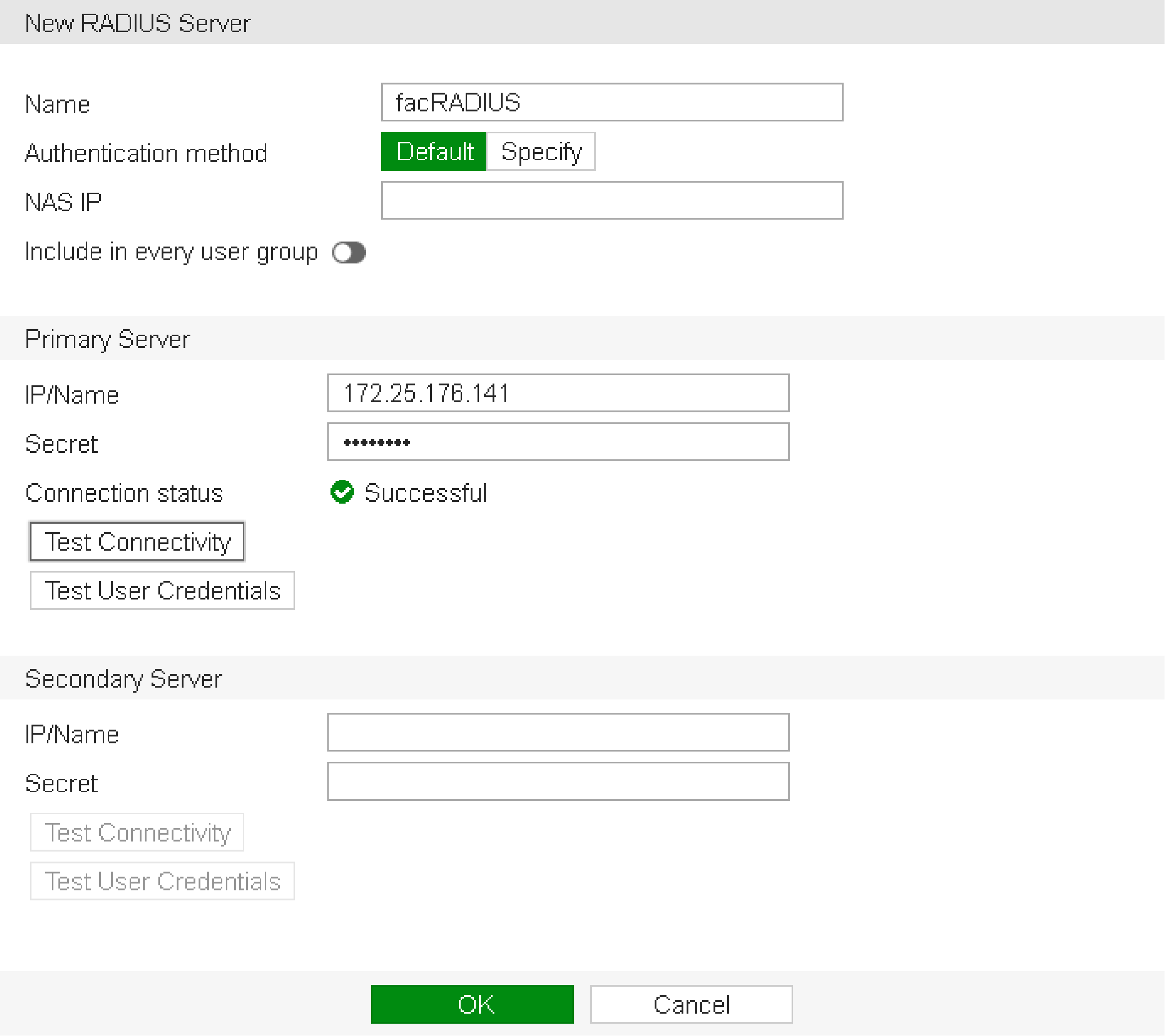
To create the RADIUS policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Set the authentication type as *Password/OTP authentication*, and enable all *EAP* types.
5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
   Add the user group *employees* as a filter.
6. Review the remaining configurations, and click *Save and Exit*.

Configuring FortiGate to use the RADIUS server

To configure FortiGate to use the RADIUS server:

1. Go to *User & Device > RADIUS Servers* and add the FortiAuthenticator as a RADIUS server.
   Select *Test Connectivity* to confirm the successful connection.



New RADIUS Server

Name: facRADIUS

Authentication method: [✓ Default] Specify

NAS IP:

Include in every user group: ○

Primary Server

IP/Name: 172.25.176.141

Secret: •••••••••

Connection status: ✓ Successful

Secondary Server

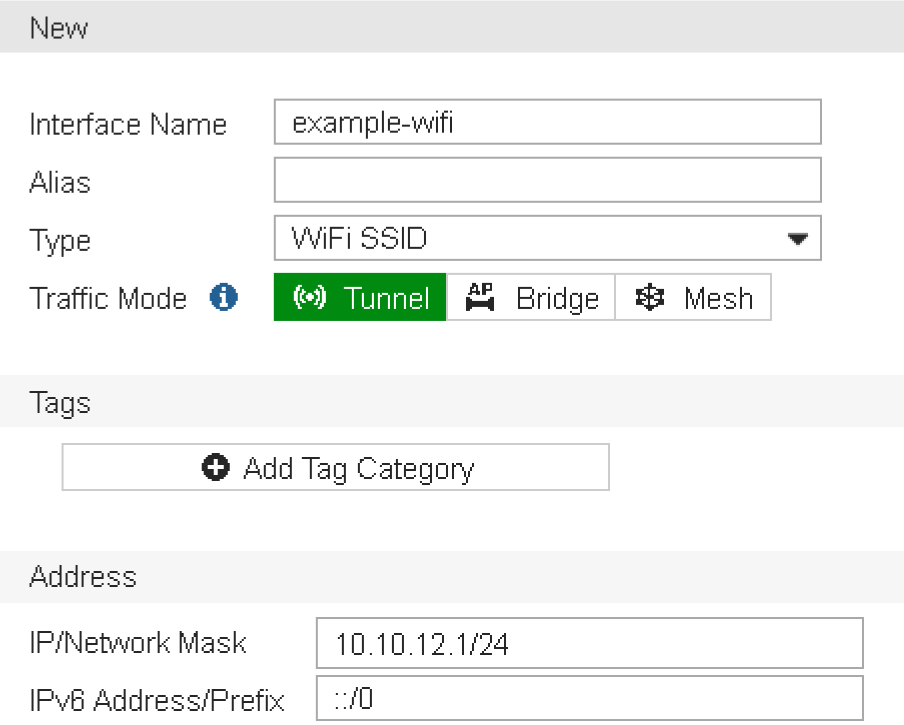
IP/Name:

Secret:

Creating SSID and set up authentication

To create an SSID and set up authentication:

1. Go to *WiFi & Switch Controller* > *SSID* and define your wireless network.



New

Interface Name: example-wifi

Alias:

Type: WiFi SSID

Traffic Mode: Tunnel | Bridge | Mesh (Tunnel selected)

Tags

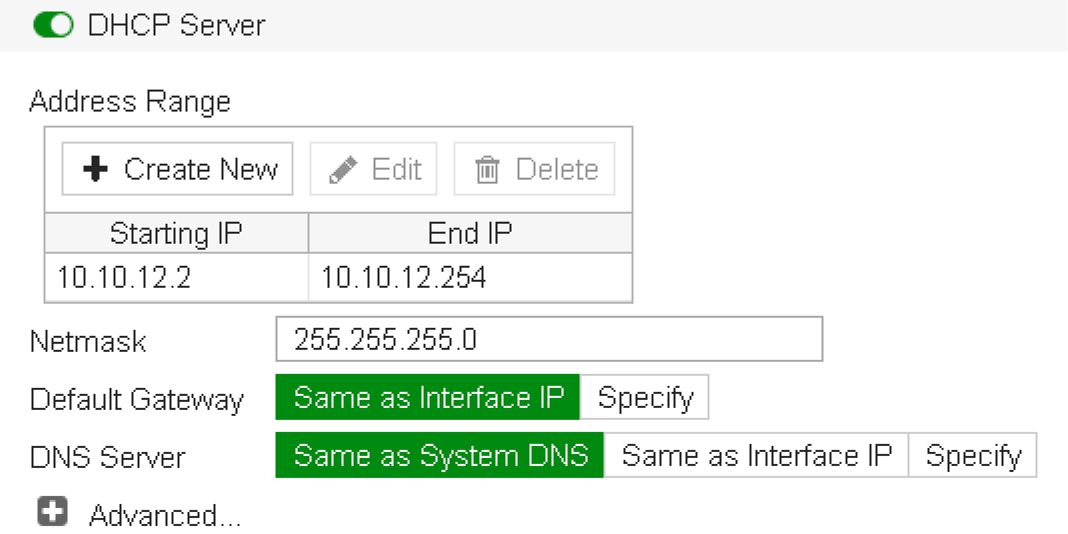
Add Tag Category

Address

IP/Network Mask: 10.10.12.1/24

IPv6 Address/Prefix: ::/0

2. Set up DHCP for your clients.



DHCP Server (enabled)

Address Range

Create New | Edit | Delete

Starting IP	End IP
10.10.12.2	10.10.12.254

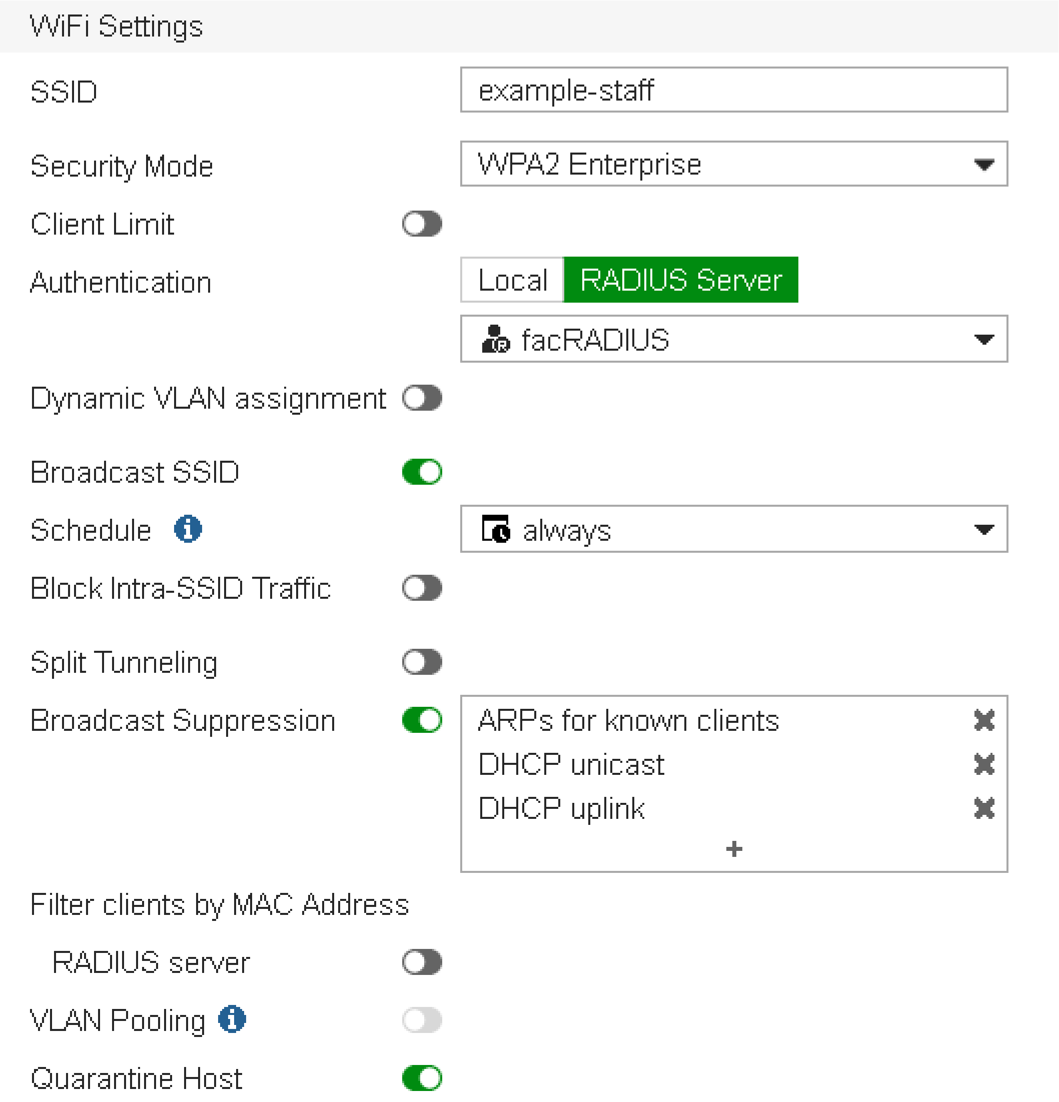
Netmask: 255.255.255.0

Default Gateway: Same as Interface IP | Specify (Same as Interface IP selected)

DNS Server: Same as System DNS | Same as Interface IP | Specify (Same as System DNS selected)

Advanced...

3. Configure WPA2 Enterprise security that uses the RADIUS server.



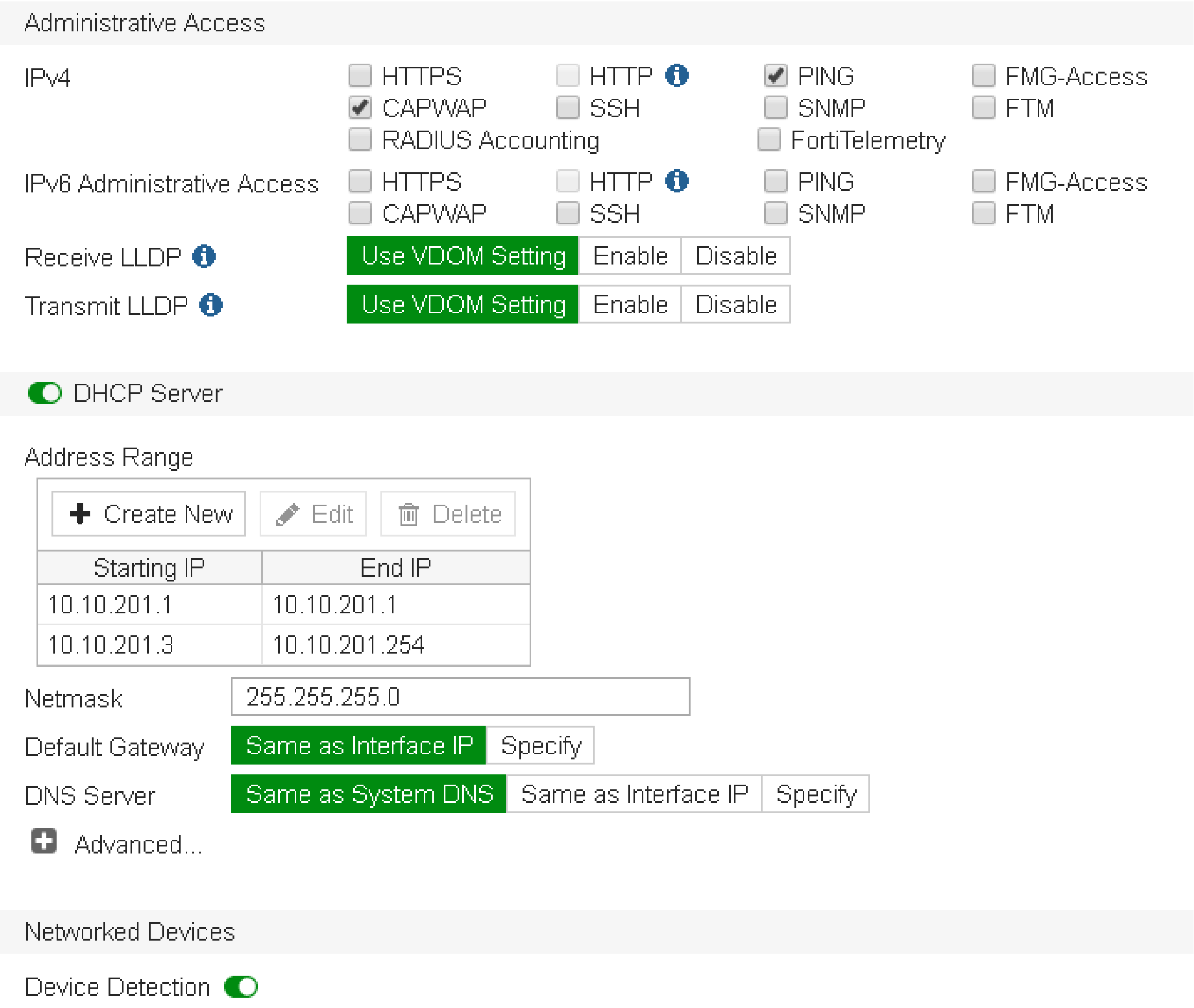
WiFi Settings

SSID		example-staff
Security Mode		WPA2 Enterprise ▾
Client Limit	○	
Authentication		Local [✓ RADIUS Server]
		facRADIUS ▾
Dynamic VLAN assignment	○	
Broadcast SSID	●	
Schedule ℹ		always ▾
Block Intra-SSID Traffic	○	
Split Tunneling	○	
Broadcast Suppression	●	ARPs for known clients ✖ DHCP unicast ✖ DHCP uplink ✖ +
Filter clients by MAC Address		
RADIUS server	○	
VLAN Pooling ℹ	○	
Quarantine Host	●	

Connecting and authorizing the FortiAP

To connect and authorize the FortiAP:

1. Go to *Network* > *Interfaces* and configure a dedicated interface for the FortiAP.
   Under *Administrative Access*, enable *PING* and *CAPWAP*, and enable *DHCP Server*.
   Under *Networked Devices*, enable *Device Detection*.



Administrative Access

IPv4: □ HTTPS □ HTTP ☑ PING □ FMG-Access ☑ CAPWAP □ SSH □ SNMP □ FTM □ RADIUS Accounting □ FortiTelemetry

IPv6 Administrative Access: □ HTTPS □ HTTP □ PING □ FMG-Access □ CAPWAP □ SSH □ SNMP □ FTM

Receive LLDP: [✓ Use VDOM Setting] Enable Disable

Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

DHCP Server (enabled)

Address Range

Starting IP	End IP
10.10.201.1	10.10.201.1
10.10.201.3	10.10.201.254

Netmask: 255.255.255.0

Default Gateway: [✓ Same as Interface IP] Specify

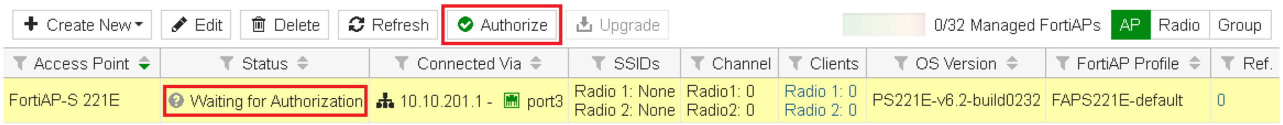
DNS Server: [✓ Same as System DNS] Same as Interface IP Specify

Advanced...

Networked Devices

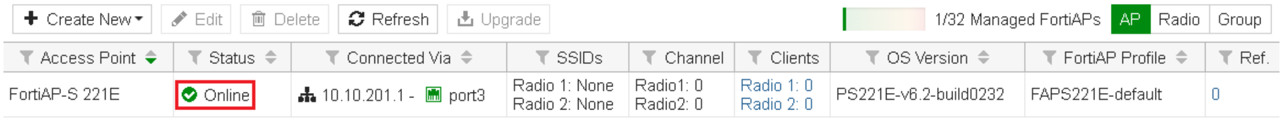
Device Detection (enabled)

2. Connect the FortiAP unit to the interface. Then go to *WiFi & Switch Controller > Managed FortiAPs*. Notice the *Status* is showing *Waiting for Authorization*.
   When the FortiAP is listed, select and *Authorize* it.



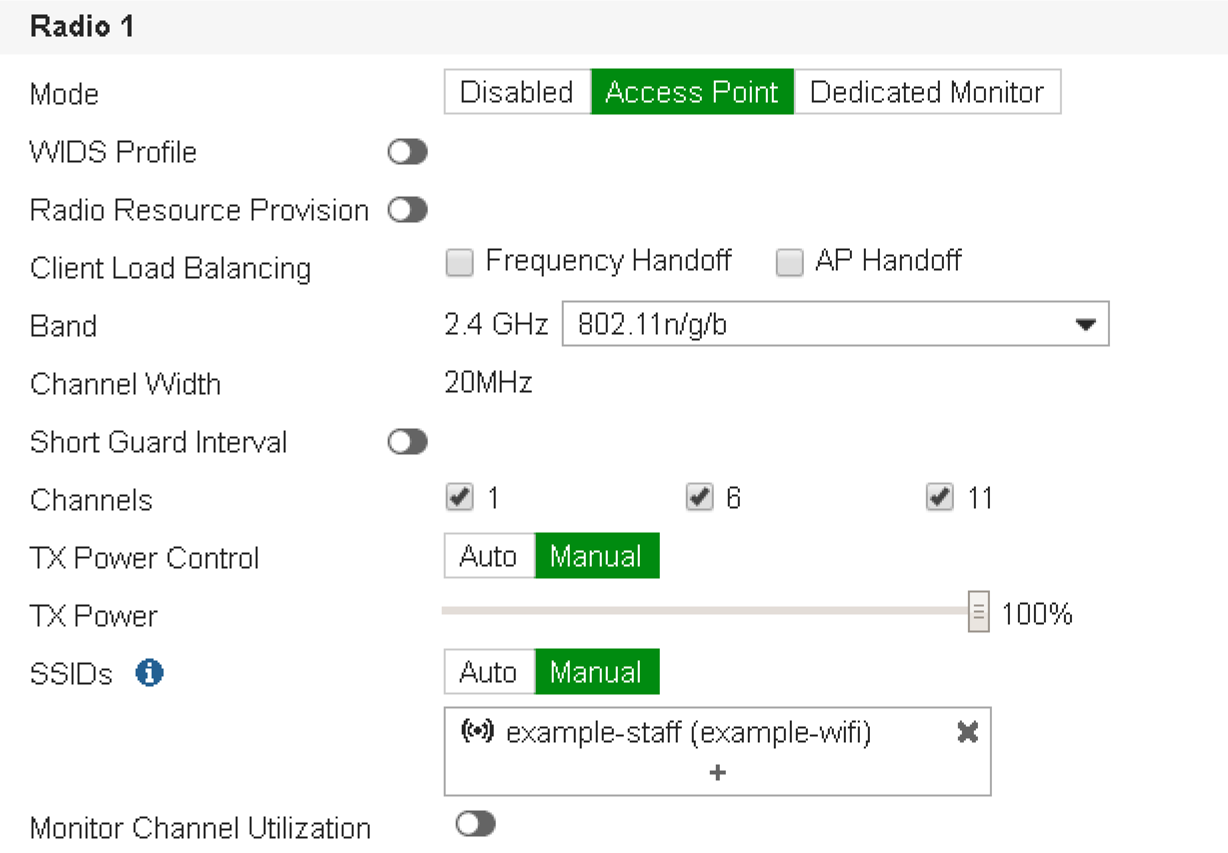
Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Ref.
FortiAP-S 221E	Waiting for Authorization	10.10.201.1 - port3	Radio 1: None Radio 2: None	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	PS221E-v6.2-build0232	FAPS221E-default	0

3. The FortiAP is now *Online*. The *Status* may take a few minutes to update.



Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Ref.
FortiAP-S 221E	Online	10.10.201.1 - port3	Radio 1: None Radio 2: None	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	PS221E-v6.2-build0232	FAPS221E-default	0

4. Go to *WiFi & Switch Controller > FortiAP Profiles* and edit the profile.
   This example uses a FortiAP-S 221E, so the *FAPS221E-default* profile applies.
   For each radio, make sure to select your *SSID*.



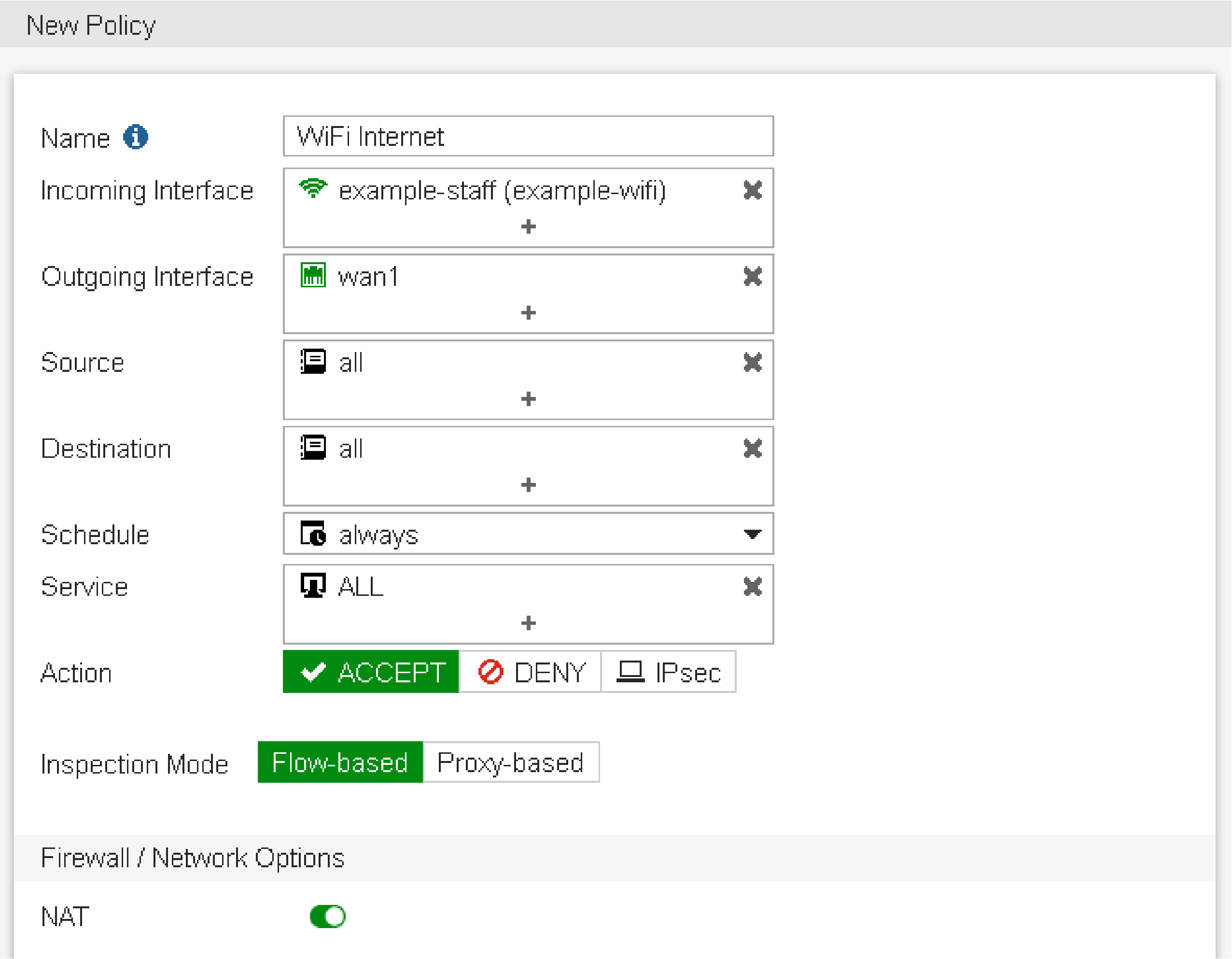
Radio 1

Mode	Disabled [✓ Access Point] Dedicated Monitor
WIDS Profile	○
Radio Resource Provision	○
Client Load Balancing	□ Frequency Handoff □ AP Handoff
Band	2.4 GHz 802.11n/g/b ▾
Channel Width	20MHz
Short Guard Interval	○
Channels	☑ 1 ☑ 6 ☑ 11
TX Power Control	Auto [✓ Manual]
TX Power	100%
SSIDs ℹ	Auto [✓ Manual] example-staff (example-wifi) ✖ +
Monitor Channel Utilization	○

Creating the security policy

To create the security policy:

1. Go to *Policy & Objects > IPv4 Policy* and add a policy that allows WiFi users to access the Internet.



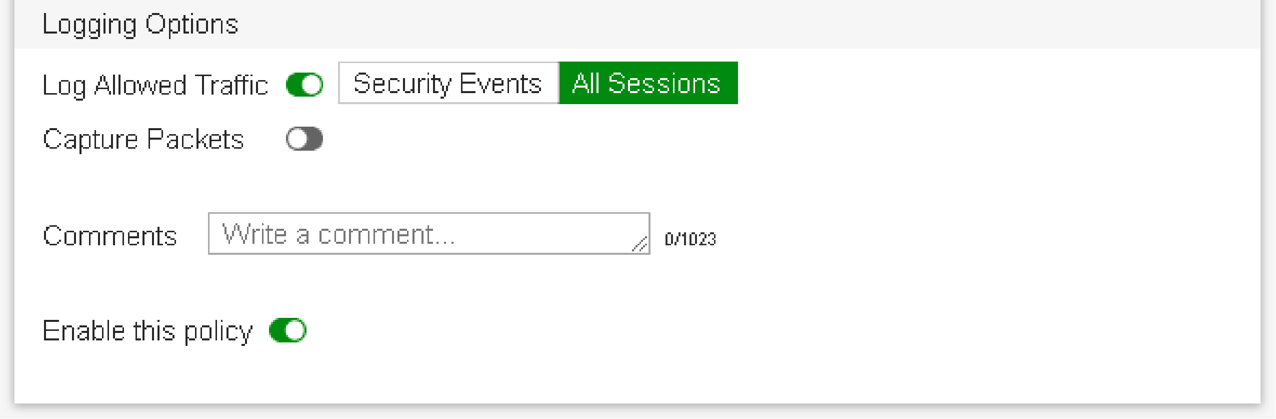
New Policy

Name	WiFi Internet
Incoming Interface	example-staff (example-wifi)
Outgoing Interface	wan1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY IPsec
Inspection Mode	[✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●

2. Under *Logging Options*, enable *Log Allowed Traffic* and *All Sessions*.



Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

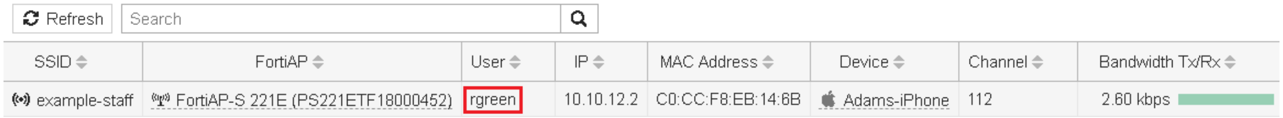
Capture Packets ○

Comments Write a comment... 0/1023

Enable this policy ●

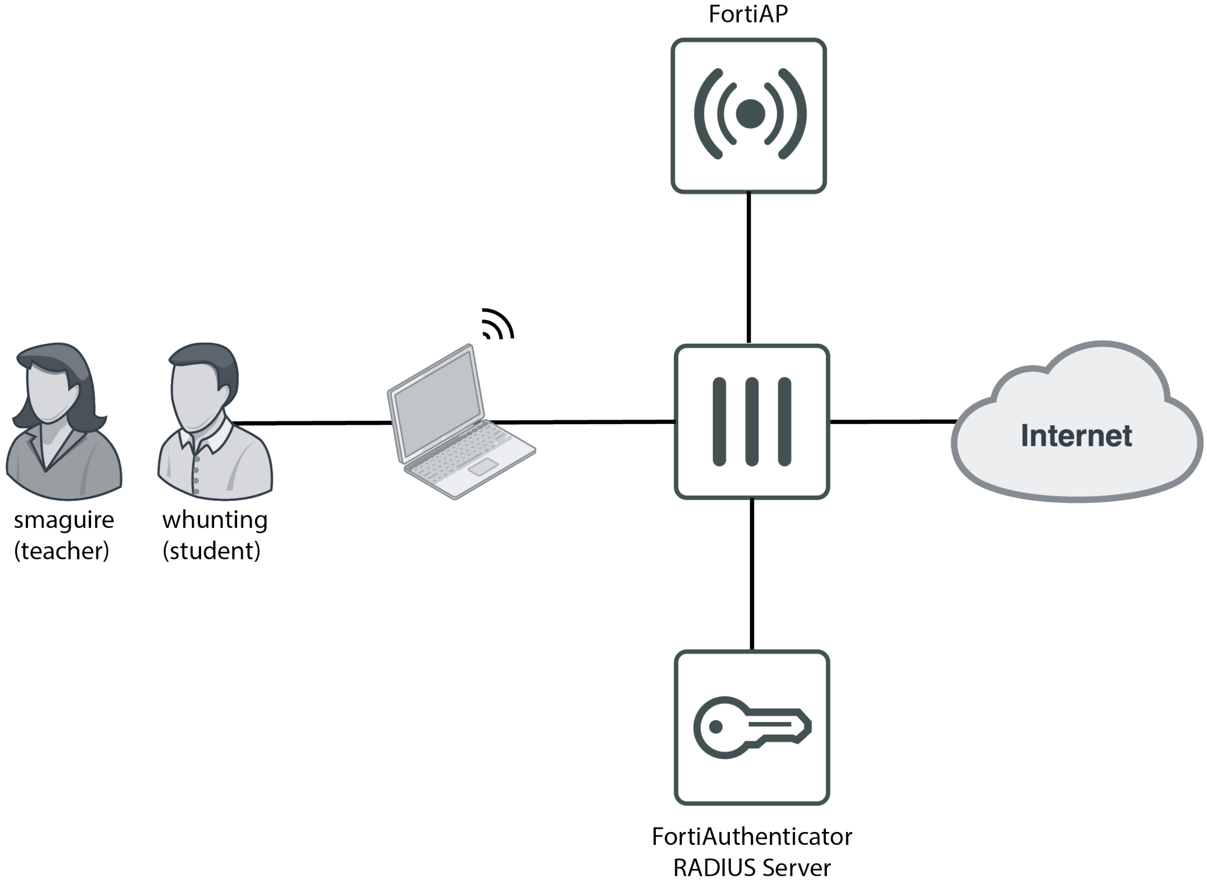
Results

1. Connect to the *example-staff* network and browse Internet sites.
   On the FortiGate, go to *Monitor* > *WiFi Client Monitor* to see that clients connect and authenticate.



SSID	FortiAP	User	IP	MAC Address	Device	Channel	Bandwidth Tx/Rx
example-staff	FortiAP-S 221E (PS221ETF18000452)	rgreen	10.10.12.2	C0:CC:F8:EB:14:6B	Adams-iPhone	112	2.60 kbps

WiFi with WSSO using FortiAuthenticator RADIUS and Attributes



This is an example of wireless single sign-on (WSSO) with a FortiGate and FortiAuthenticator. The WiFi users are teachers and students at a school. These users each belong to a user group, either *teachers* (*smaguire*) or *students* (*whunting*). The FortiAuthenticator performs user authentication and passes the user group name to the FortiGate so that the appropriate security policy is applied.

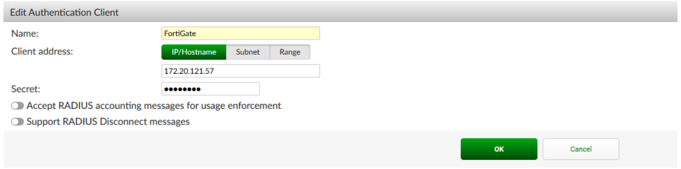
This recipe assumes that an SSID and a FortiAP are configured on the FortiGate unit. In this configuration, you will be changing the existing SSID's WiFi settings so authentication is provided by the RADIUS server.

For this example, the student security policy applies a more restrictive web filter.

Registering the FortiGate as a RADIUS client on the FortiAuthenticator

To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication > RADIUS Service > Clients*, and select *Create New*.
2. Enter a *Name*, 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.



Edit Authentication Client

Name: FortiGate

Client address: IP/Hostname | Subnet | Range

172.20.121.57

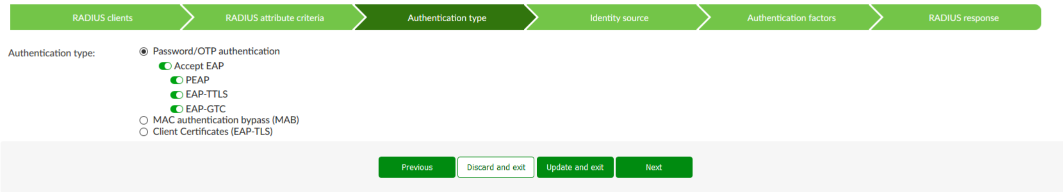
Secret: ●●●●●●●●●

Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

To create the RADIUS policy:

1. Go to *Authentication > RADIUS Service > Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Set the authentication type as *Password/OTP authentication*, and enable all *EAP* types.



Authentication type:

● Password/OTP authentication

Accept EAP

PEAP

EAP-TTLS

EAP-GTC

○ MAC authentication bypass (MAB)

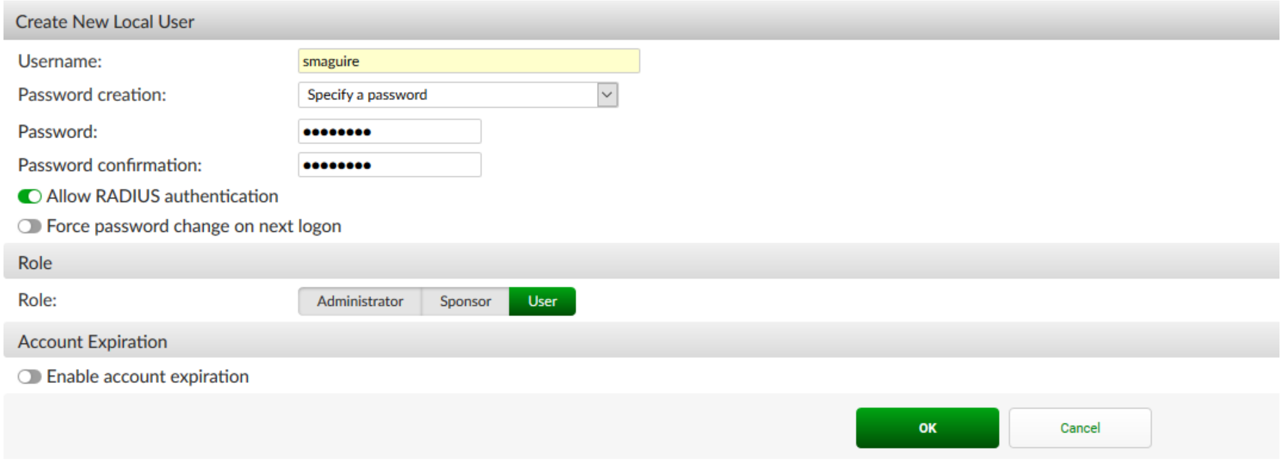
○ Client Certificates (EAP-TLS)

5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
6. Review the remaining configurations, and click *Save and Exit*.

Creating users on the FortiAuthenticator

To create users:

1. Go to *Authentication > User Management > Local Users* and select *Create New*.
   Create one teacher user (*smaguire*) and another student user (*whunting*).



Create New Local User

Username: smaguire

Password creation: Specify a password

Password: ●●●●●●●●

Password confirmation: ●●●●●●●●

Allow RADIUS authentication

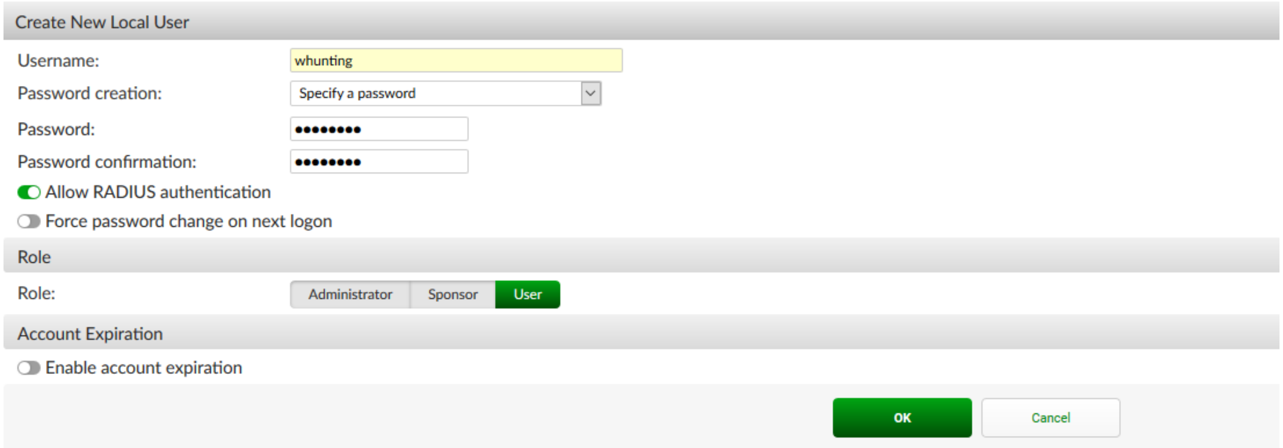
Force password change on next logon

Role

Role: Administrator | Sponsor | User

Account Expiration

Enable account expiration



Create New Local User

Username: whunting

Password creation: Specify a password

Password: ••••••••

Password confirmation: ••••••••

☑ Allow RADIUS authentication

□ Force password change on next logon

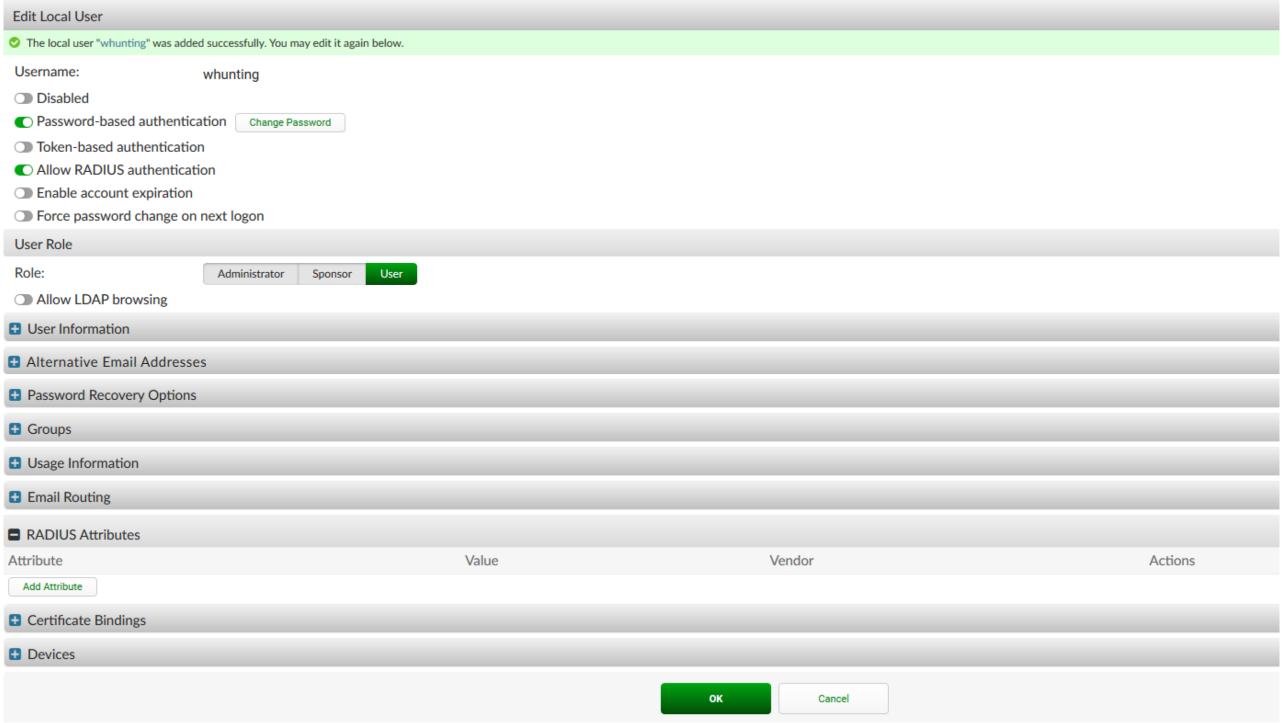
Role

Role: Administrator | Sponsor | [✓ User]

Account Expiration

□ Enable account expiration

2. Note that, after you create the users, *RADIUS Attributes* appears as an option.
   If your configuration involves multiple users, it is more efficient to add RADIUS attributes in their respective user groups, in the next step.



Edit Local User

The local user "whunting" was added successfully. You may edit it again below.

Username: whunting

□ Disabled

☑ Password-based authentication

□ Token-based authentication

☑ Allow RADIUS authentication

□ Enable account expiration

□ Force password change on next logon

User Role

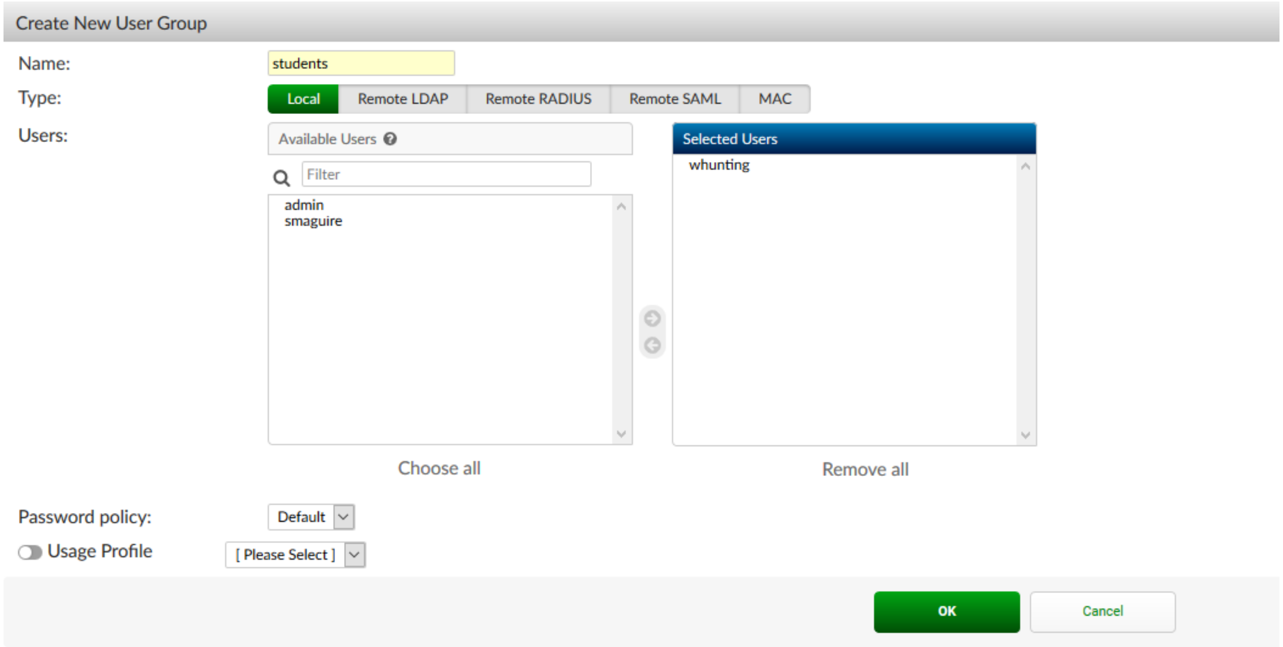
Role: Administrator | Sponsor | [✓ User]

□ Allow LDAP browsing

Creating user groups on the FortiAuthenticator

To create user groups:

1. Go to *Authentication* > *User Management* > *User Groups* and create two user groups: *teachers* and *students*.
   Add the users to their respective groups.



Create New User Group

Name: students

Type: Local

Users:

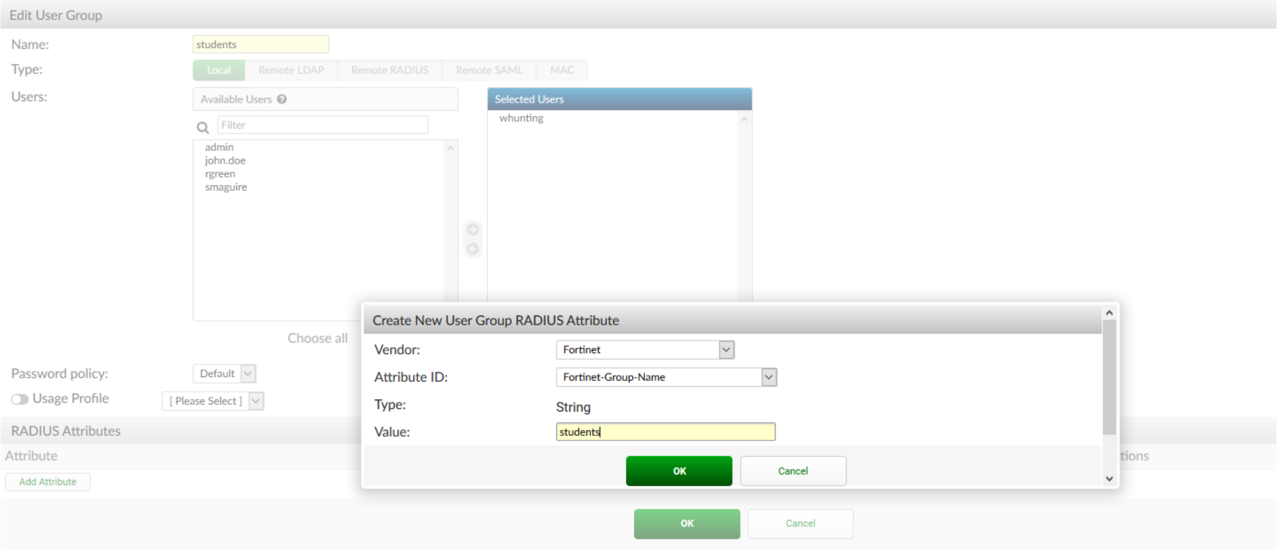
Available Users: admin, smaguire

Selected Users: whunting

Password policy: Default

Usage Profile: [Please Select]

2. Once created, edit both user groups and select *Add Attribute*.
3. Add the *Fortinet-Group-Name* RADIUS attribute to each group, which specifies the user group name to be sent to the FortiGate.



Edit User Group

Name: students

Type: Local

Users:

Available Users: admin, john.doe, rgreen, smaguire

Selected Users: whunting

Password policy: Default

Usage Profile: [Please Select]

RADIUS Attributes

Create New User Group RADIUS Attribute

Vendor: Fortinet

Attribute ID: Fortinet-Group-Name

Type: String

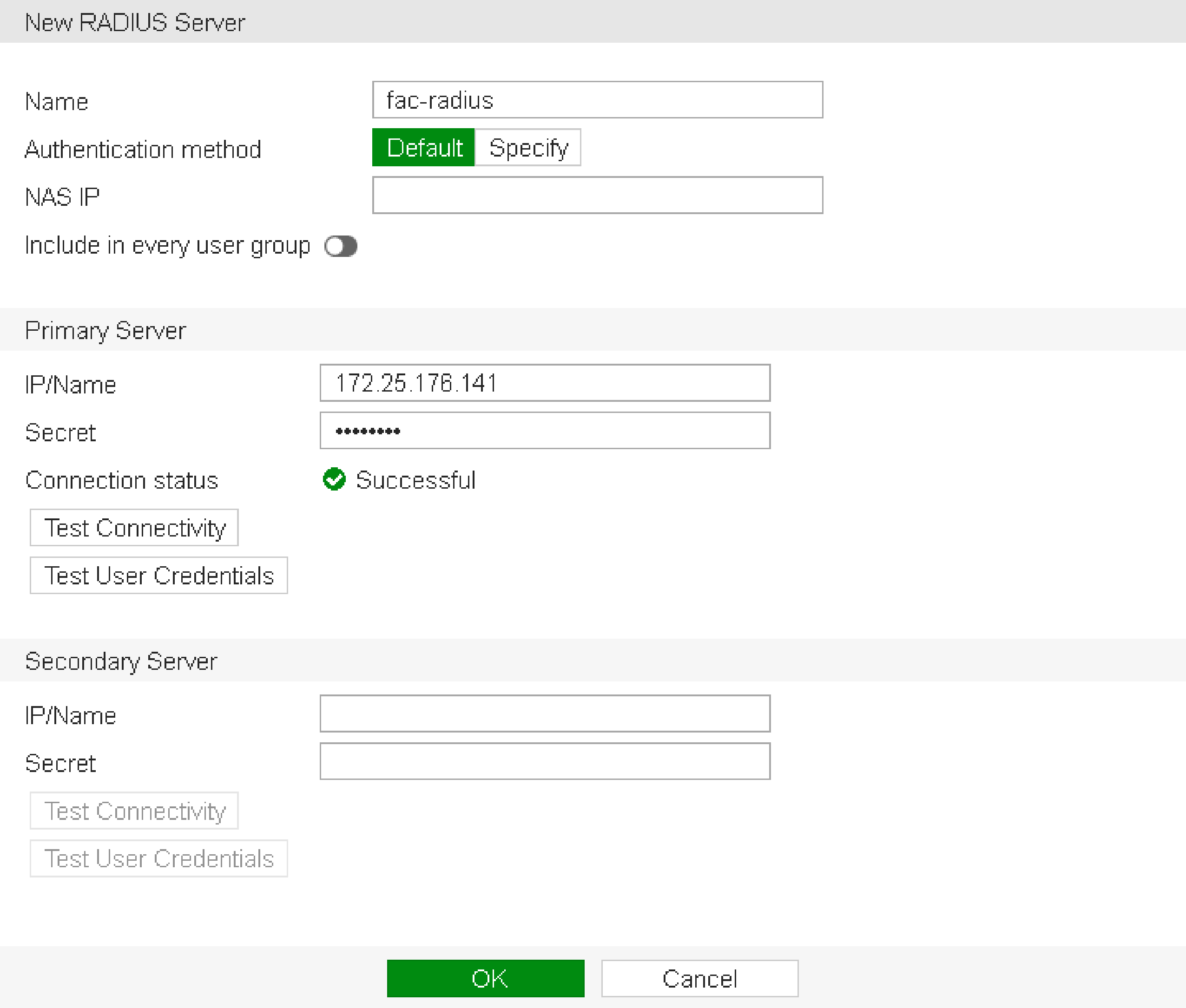
Value: students

Configuring the FortiGate to use the FortiAuthenticator as the RADIUS server

To configure the FortiGate to use the FortiAuthenticator RADIUS server:

1. On the FortiGate, go to *User & Device* > *RADIUS Servers* and select *Create New*.
   Enter a *Name*, the Internet-facing IP address of the FortiAuthenticator, and enter the same *Primary Server Secret* entered on the FortiAuthenticator.

Select *Test Connectivity* to confirm the successful connection.



New RADIUS Server

Name	fac-radius
Authentication method	[✓ Default] Specify
NAS IP	
Include in every user group	○

Primary Server

IP/Name	172.25.176.141
Secret	•••••••••
Connection status	✓ Successful

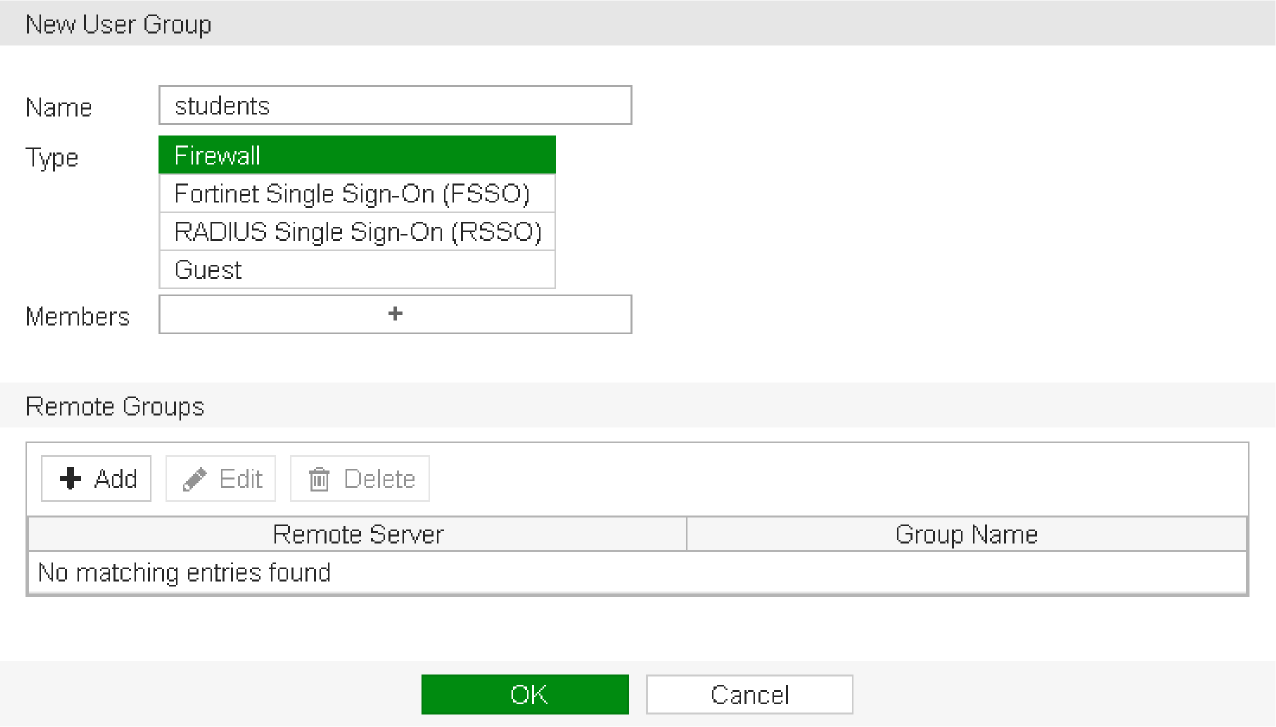
Secondary Server

IP/Name	
Secret	

Configuring user groups on the FortiGate

To configure user groups on the FortiGate:

1. Go to *User & Device* > *User Groups* and create two groups named the same as the ones created on the FortiAuthenticator.



New User Group

Name: students

Type: Firewall

Remote Server	Group Name
No matching entries found	

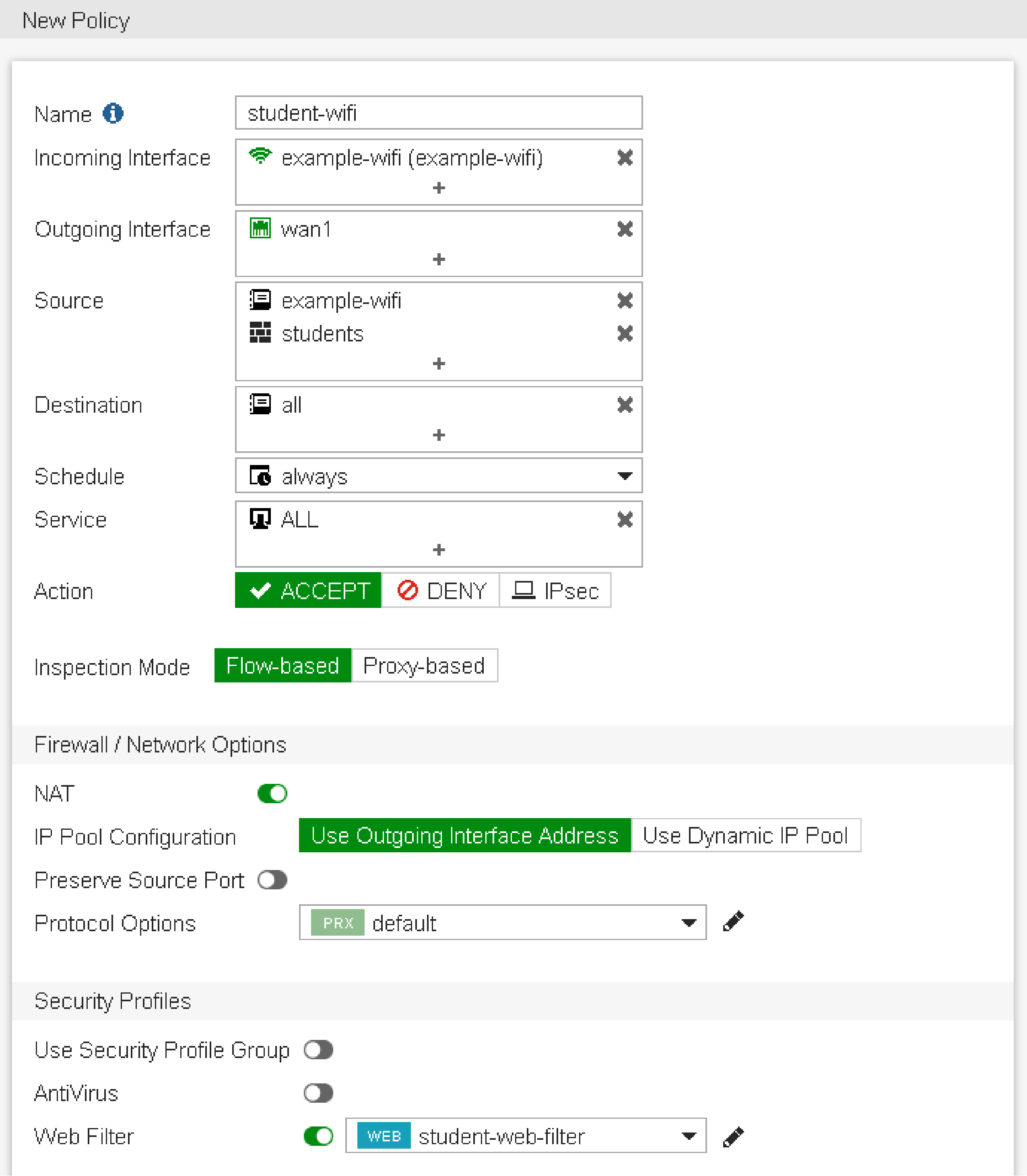
Do not add any members to either group.

Creating security policies

To create a security policy:

1. Go to *Policy & Objects* > *IPv4 Policy* and select *Create New*.
   Create two policies (*student-wifi* and *teacher-wifi*) with WiFi-to-Internet access: one policy with *Source* set to the *students* user group, and the other set to *teachers*. Make sure to add the SSID address (*example-wifi*) to both policies also.

The student policy has a more restrictive *Web Filter* profile enabled.



New Policy

Name	student-wifi
Incoming Interface	example-wifi (example-wifi)
Outgoing Interface	wan1
Source	example-wifi students
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT (selected) DENY IPsec
Inspection Mode	Flow-based (selected) Proxy-based

Firewall / Network Options

NAT	●
IP Pool Configuration	Use Outgoing Interface Address (selected) Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PRX default

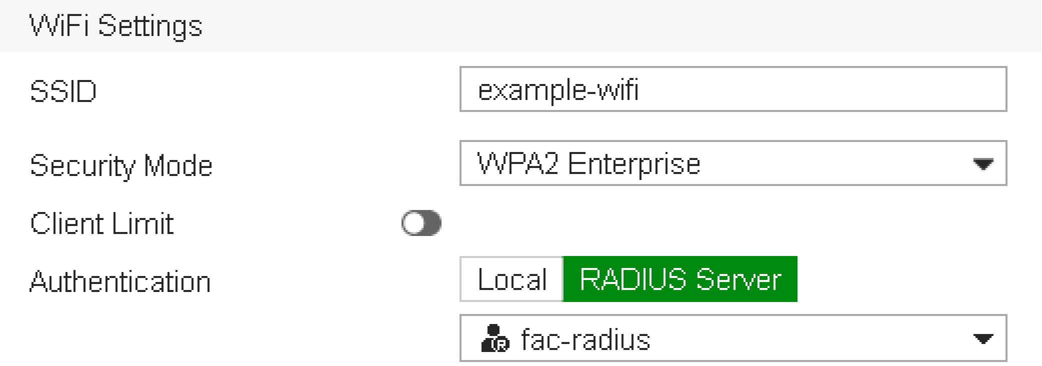
Security Profiles

Use Security Profile Group	○
AntiVirus	○
Web Filter	● WEB student-web-filter

Configuring the SSID to RADIUS authentication

To configure the SSID to RADIUS authentication:

1. Go to *WiFi & Switch Controller > SSID* and edit your pre-existing SSID interface.
   Under *WiFi Settings*, set *Security Mode* to *WPA2 Enterprise*, set *Authentication* to *RADIUS Server*, and add the RADIUS server configured on the FortiGate earlier from the dropdown menu.



WiFi Settings

SSID: example-wifi

Security Mode: WPA2 Enterprise

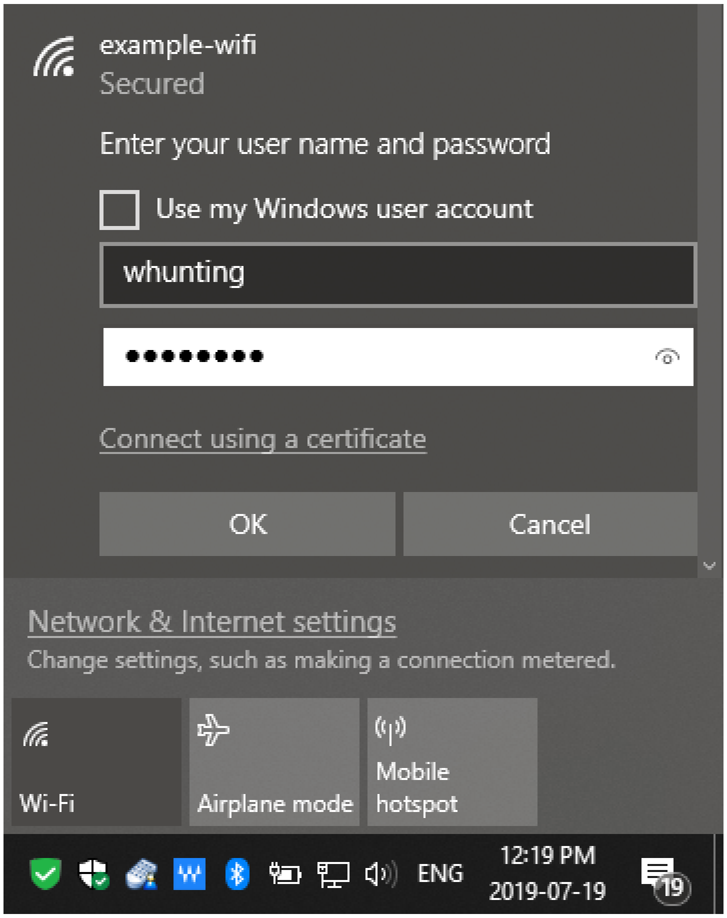
Client Limit: ○

Authentication: Local [✓ RADIUS Server]

fac-radius

Results

1. Connect to the WiFi network as a student.



example-wifi
Secured

Enter your user name and password

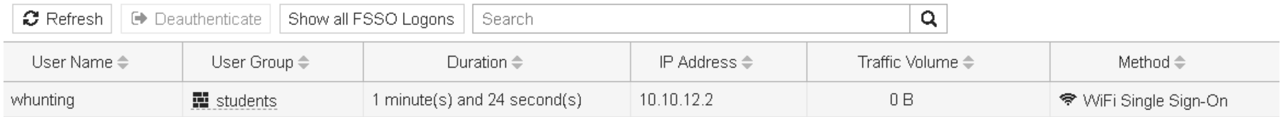
□ Use my Windows user account

whunting

●●●●●●●●●

Connect using a certificate
OK
Cancel
Network & Internet settings
Change settings, such as making a connection metered.
Wi-Fi
Airplane mode
Mobile hotspot
ENG
12:19 PM
2019-07-19
19

2. Then on the FortiGate go to *Monitor > Firewall User Monitor*. From here you can verify the user, the user group, and that the WSSO authentication method was used.



User Name	User Group	Duration	IP Address	Traffic Volume	Method
whunting	students	1 minute(s) and 24 second(s)	10.10.12.2	0 B	WiFi Single Sign-On

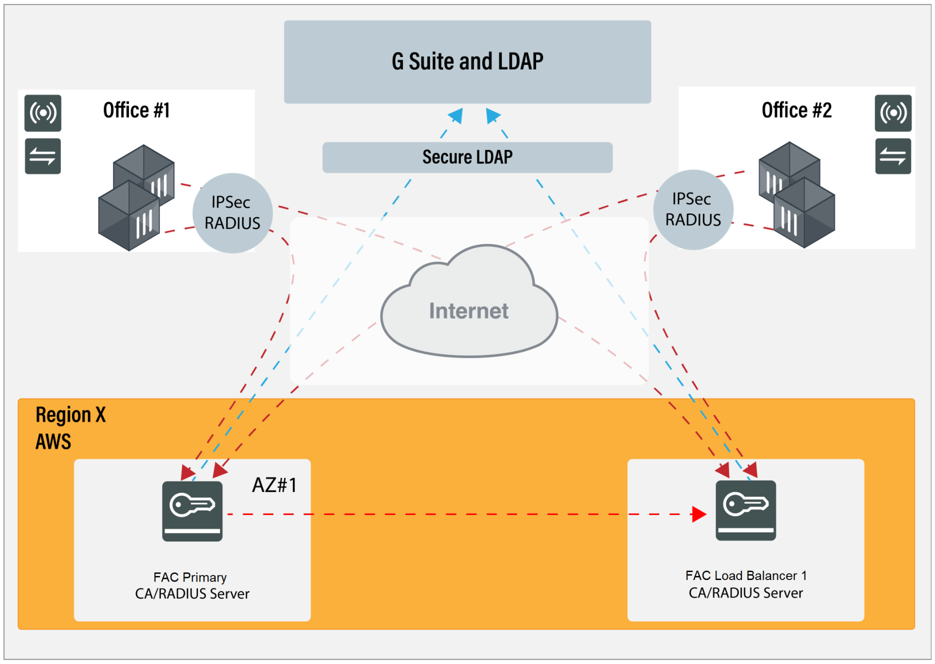
LDAP Authentication

This section describes configuring LDAP authentication.

G Suite integration using LDAP

This article explains how to integrate the FortiAuthenticator with G Suite Secure LDAP using client authentication through a certificate. You will use the LDAP in Google DB to authenticate end users for 802.1X and VPN.

1. Generating the G Suite certificate on page 146
2. Importing the certificate to FortiAuthenticator on page 148
3. Configuring LDAP on the FortiAuthenticator on page 148
4. Troubleshooting on page 150



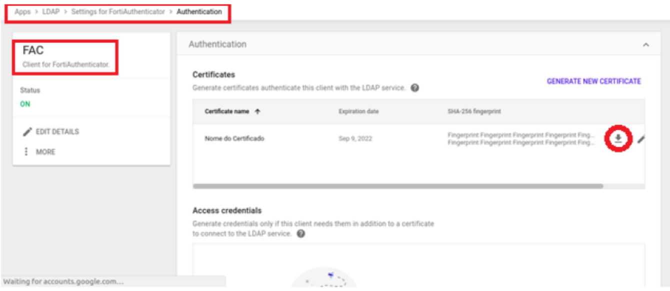
Generating the G Suite certificate

You must first generate certificates to authenticate the LDAP client with Secure LDAP service.

To generate certificate authentication:

1. From the Google Admin console, go to *Apps* > *LDAP*.
2. Select one of the clients in the list.
3. Click the *Authentication* card.
4. Click *GENERATE NEW CERTIFICATE*, then click the download icon to download the certificate.

5. Upload the certificate to your client, and configure the application.
   Depending on the type of LDAP client, configuration may require LDAP access credentials. See Generate access credentials.



Apps > LDAP > Settings for FortiAuthenticator > Authentication

FAC
Client for FortiAuthenticator

Status
ON

Certificates

Generate certificates authenticate this client with the LDAP service.

Certificate name	Expiration date	SHA-256 fingerprint
Nome do Certificado	Sep 9, 2022	Fingerprint Fingerprint Fingerprint Fingerprint Fing... Fingerprint Fingerprint Fingerprint Fingerprint Fing...

Access credentials

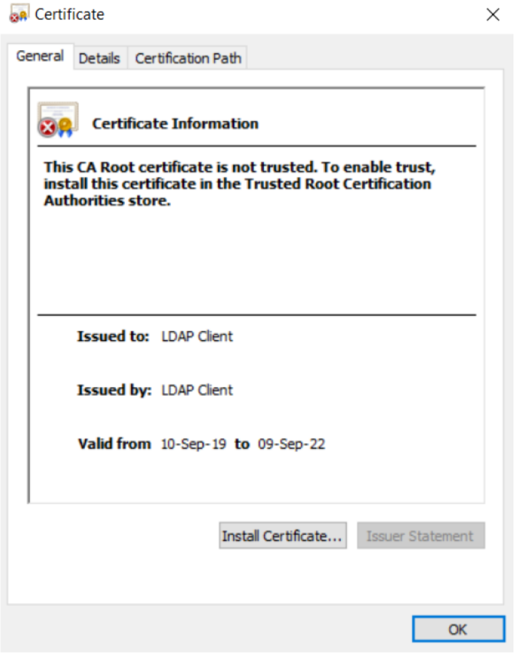
Generate credentials only if this client needs them in addition to a certificate to connect to the LDAP service.

Waiting for accounts.google.com...

Once you have uploaded the certificate to your client, G Suite will generate a client certificate and key.

Example:

- Cert: `Google_2022_09_09_72372.crt`
- Key: `Google_2022_09_09_72372.key`



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: LDAP Client

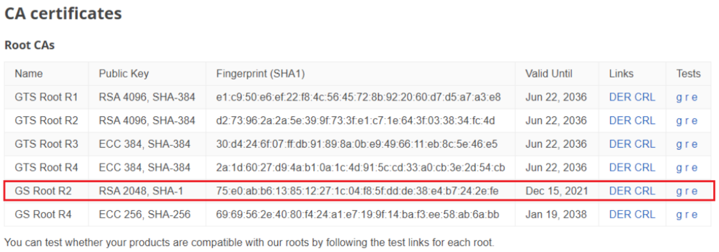
Issued by: LDAP Client

Valid from 10-Sep-19 to 09-Sep-22

Store the certificate and key in a safe place.

By default, FortiAuthenticator will not trust the certificate issued by Google. You must install a Google Trusted CA to match the chain group, which can be downloaded at https://pki.goog/.

- `GS Root R2`



CA certificates

Root CAs

Name	Public Key	Fingerprint (SHA1)	Valid Until	Links	Tests
GTS Root R1	RSA 4096, SHA-384	e1:c9:50:e6:ef:22:f8:4c:56:45:72:8b:92:20:60:d7:d5:a7:a3:e8	Jun 22, 2036	DER CRL	g r e
GTS Root R2	RSA 4096, SHA-384	d2:73:96:2a:2a:5e:39:9f:73:3f:e1:c7:1e:64:3f:03:38:34:fc:4d	Jun 22, 2036	DER CRL	g r e
GTS Root R3	ECC 384, SHA-384	30:d4:24:6f:07:ff:db:91:89:8a:0b:e9:49:66:11:eb:8c:5e:46:e5	Jun 22, 2036	DER CRL	g r e
GTS Root R4	ECC 384, SHA-384	2a:1d:60:27:d9:4a:b1:0a:1c:4d:91:5c:cd:33:a0:cb:3e:2d:54:cb	Jun 22, 2036	DER CRL	g r e
GS Root R2	RSA 2048, SHA-1	75:e0:ab:b6:13:85:12:27:1c:04:f8:5f:dd:de:38:e4:b7:24:2e:fe	Dec 15, 2021	DER CRL	g r e
GS Root R4	ECC 256, SHA-256	69:69:56:2e:40:80:f4:24:a1:e7:19:9f:14:ba:f3:ee:58:ab:6a:bb	Jan 19, 2038	DER CRL	g r e

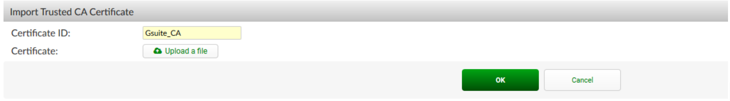
You can test whether your products are compatible with our roots by following the test links for each root.

Importing the certificate to FortiAuthenticator

This series of steps can be performed on the primary FortiAuthenticator.

To import the trusted CA certificate:

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs* > *Import*.
2. Enter a Certificate ID, upload a file, and click *OK*.

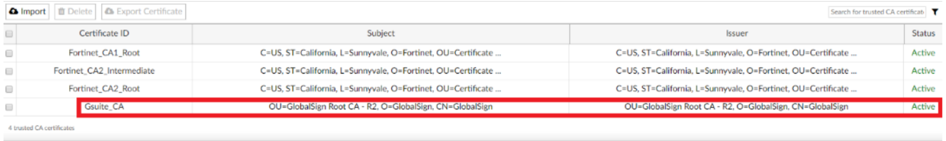


Import Trusted CA Certificate

Certificate ID: Gsuite_CA

Certificate:

Results:



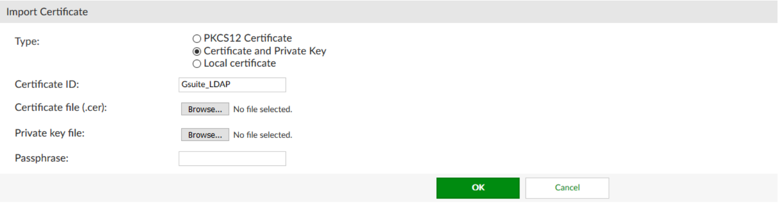
□	Certificate ID	Subject	Issuer	Status
□	Fortinet_CA1_Root	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	Active
□	Fortinet_CA2_Intermediate	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	Active
□	Fortinet_CA2_Root	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	Active
□	Gsuite_CA	OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign	OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign	Active

4 trusted CA certificates

You can now import the LDAP certificate generated by G Suite.

To import the client authentication certificate:

1. Go to *Certificate Management* > *End Entities* > *Local Services* > *Import*.
2. Select *Certificate and Private Key* as the *Type*.
3. Enter the Certificate ID, choose the files for the previously saved certificate and private key files, and select *OK*.



Import Certificate

Type: ○ PKCS12 Certificate
● Certificate and Private Key
○ Local certificate

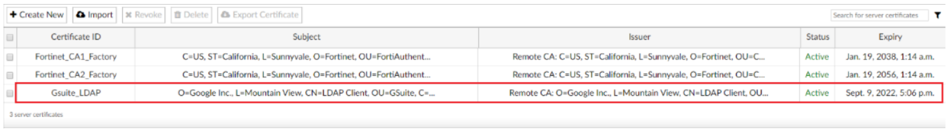
Certificate ID: Gsuite_LDAP

Certificate file (.cer): Browse... No file selected.

Private key file: Browse... No file selected.

Passphrase:

4. Results:



□	Certificate ID	Subject	Issuer	Status	Expiry
□	Fortinet_CA1_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthent...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active	Jan. 19, 2038, 1:14 a.m.
□	Fortinet_CA2_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthent...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active	Jan. 19, 2056, 1:14 a.m.
□	Gsuite_LDAP	O=Google Inc., L=Mountain View, CN=LDAP Client, OU=GSuite, C=...	Remote CA: O=Google Inc., L=Mountain View, CN=LDAP Client, OU...	Active	Sept. 9, 2022, 5:06 p.m.

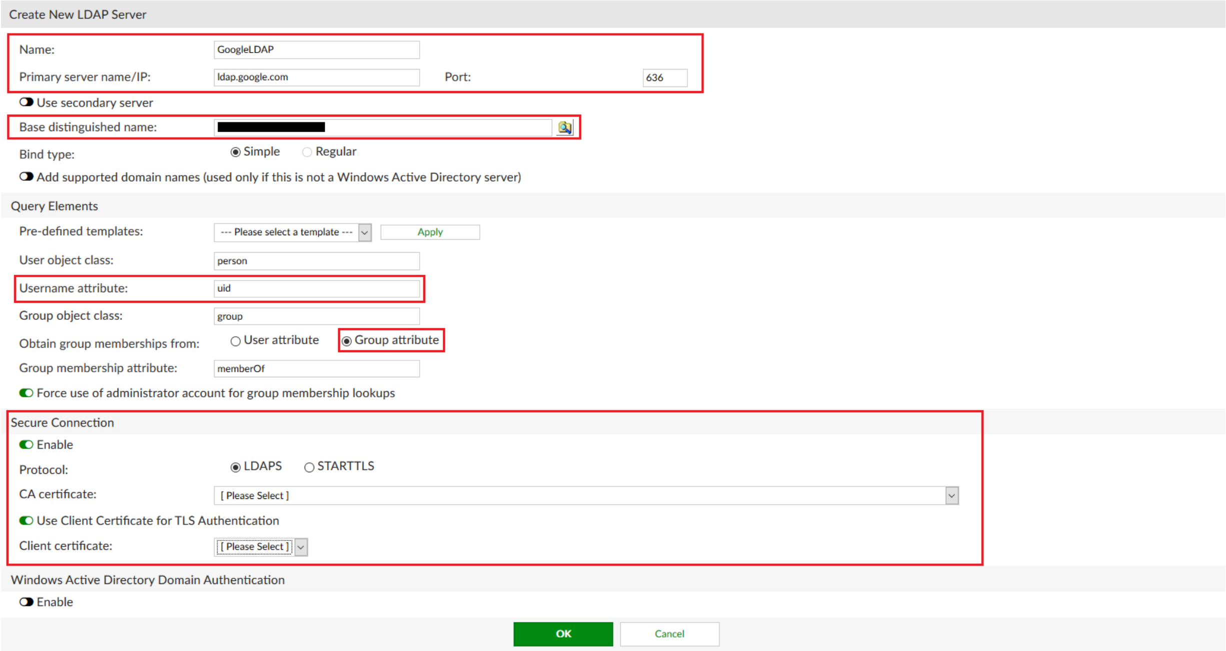
3 server certificates

Configuring LDAP on the FortiAuthenticator

Now you can finish the LDAPS configuration using client authentication through certificate.

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* > *Create New*, and enter the following information:
   a. Enter a name.
   b. For *Primary server name/IP* enter `ldap.google.com`, and set the port to `636`.
   c. Enter the base distinguished name.
   d. For the Username attribute, enter `uid`.
   e. Select the option to obtain group memberships from *Group attribute*.
   f. Enable *Secure Connection* and select either *LDAPS* or *STARTTLS* as the Protocol, and select the Google CA certificate.

g. Enable *Use Client Certificate for TLS Authentication,* and select the LDAP certificate.



Create New LDAP Server

Name: GoogleLDAP

Primary server name/IP: ldap.google.com Port: 636

○ Use secondary server

Base distinguished name: [redacted]

Bind type: ● Simple ○ Regular

○ Add supported domain names (used only if this is not a Windows Active Directory server)

Query Elements

Pre-defined templates: --- Please select a template --- Apply

User object class: person

Username attribute: uid

Group object class: group

Obtain group memberships from: ○ User attribute ● Group attribute

Group membership attribute: memberOf

● Force use of administrator account for group membership lookups

Secure Connection

● Enable

Protocol: ● LDAPS ○ STARTTLS

CA certificate: [Please Select]

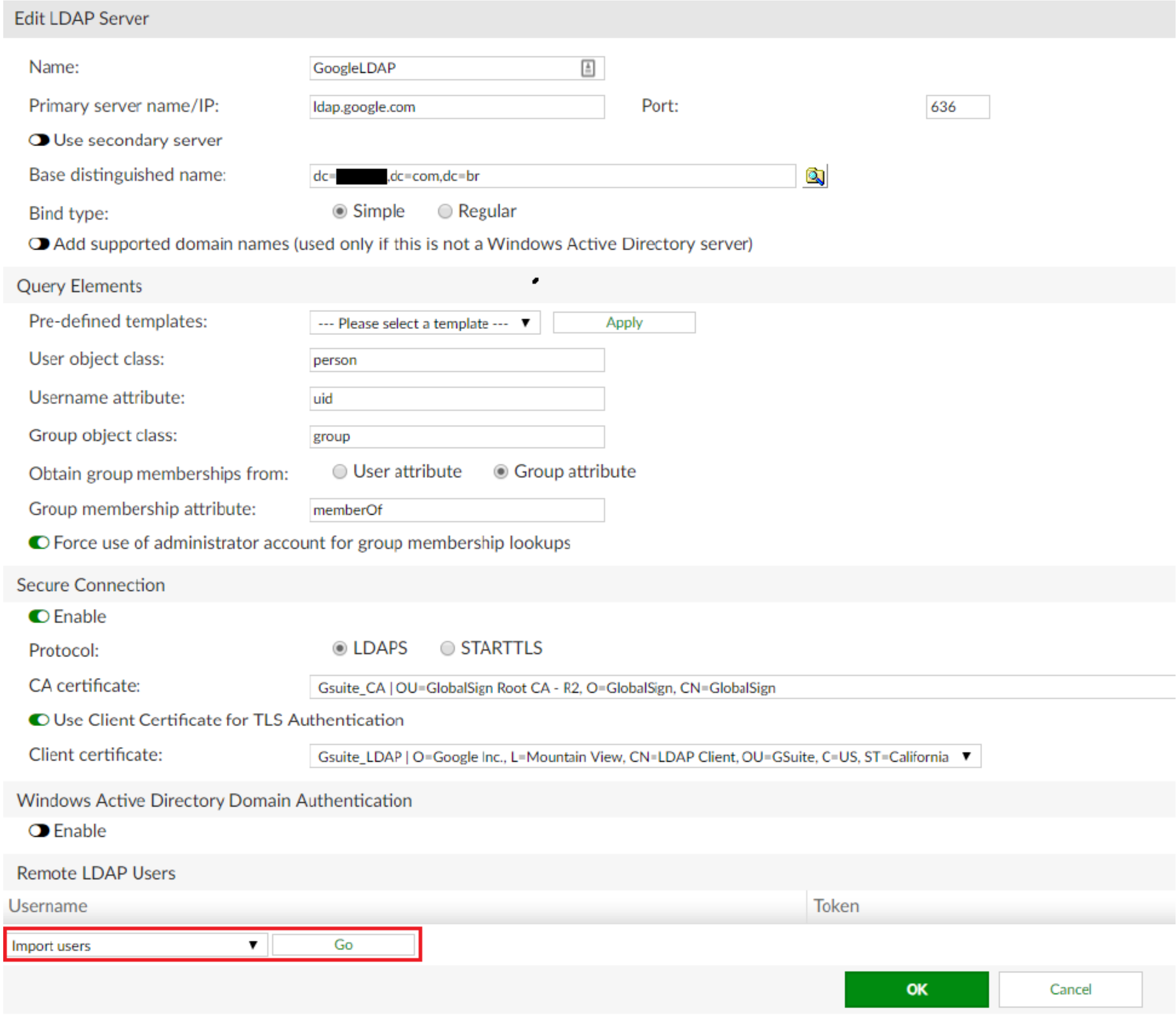
● Use Client Certificate for TLS Authentication

Client certificate: [Please Select]

Windows Active Directory Domain Authentication

○ Enable

2. Select *OK*.
If required, you can now import users by clicking the *Go* button next to the *Import users* dropdown. This is not a required step, but can be done in cases where you want to include additional information to their accounts or assign FortiTokens.



Edit LDAP Server

Name: GoogleLDAP

Primary server name/IP: ldap.google.com Port: 636

○ Use secondary server

Base distinguished name: dc=[redacted],dc=com,dc=br

Bind type: ● Simple ○ Regular

○ Add supported domain names (used only if this is not a Windows Active Directory server)

Query Elements

Pre-defined templates: --- Please select a template --- ▼ Apply

User object class: person

Username attribute: uid

Group object class: group

Obtain group memberships from: ○ User attribute ● Group attribute

Group membership attribute: memberOf

● Force use of administrator account for group membership lookups

Secure Connection

● Enable

Protocol: ● LDAPS ○ STARTTLS

CA certificate: Gsuite_CA | OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign

● Use Client Certificate for TLS Authentication

Client certificate: Gsuite_LDAP | O=Google Inc., L=Mountain View, CN=LDAP Client, OU=GSuite, C=US, ST=California ▼

Windows Active Directory Domain Authentication

○ Enable

Remote LDAP Users

Username	Token

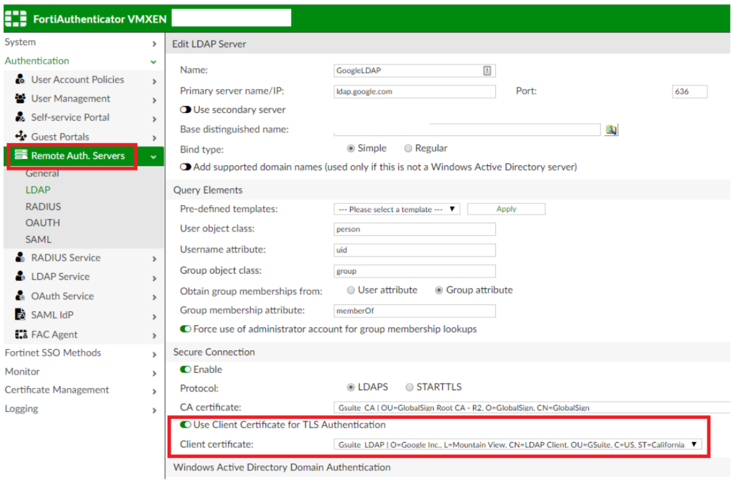
Import users ▼ Go

OK Cancel

Troubleshooting

Missing option to use client certificate for TLS authentication

Use Client Certificate for TLS Authentication is only supported in FortiAuthenticator 6.0.1 and higher.



Edit LDAP Server

Name: GoogleLDAP

Primary server name/IP: ldap.google.com Port: 636

Use secondary server

Base distinguished name:

Bind type: ● Simple ○ Regular

Add supported domain names (used only if this is not a Windows Active Directory server)

Query Elements

Pre-defined templates: --- Please select a template --- ▼ Apply

User object class: person

Username attribute: uid

Group object class: group

Obtain group memberships from: ○ User attribute ● Group attribute

Group membership attribute: memberOf

Force use of administrator account for group membership lookups

Secure Connection

Enable

Protocol: ● LDAPS ○ STARTTLS

CA certificate: Gsuite_CA | OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign

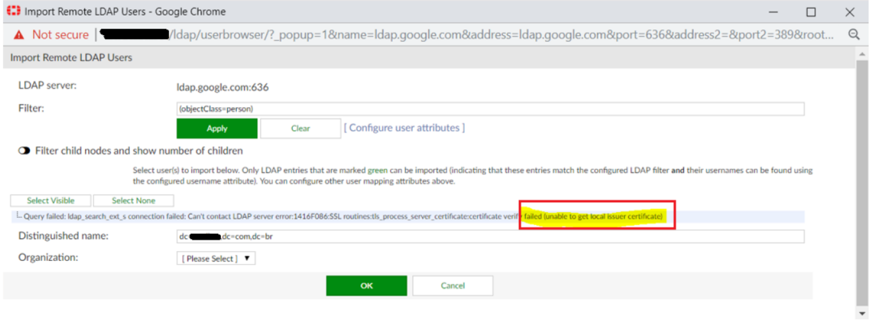
Use Client Certificate for TLS Authentication

Client certificate: Gsuite_LDAP | O=Google Inc., L=Mountain View, CN=LDAP Client, OU=GSuite, C=US, ST=California ▼

Windows Active Directory Domain Authentication

Certificate error messages

The following is an example of an incorrect Trusted CA certificate entry. Please verify that you have followed the steps included in Generating the G Suite certificate on page 146.



Import Remote LDAP Users - Google Chrome

Not secure | [redacted]/ldap/userbrowser/?_popup=1&name=ldap.google.com&address=ldap.google.com&port=636&address2=&port2=389&root...

Import Remote LDAP Users

LDAP server: ldap.google.com:636

Filter: (objectClass=person)

Apply Clear [Configure user attributes]

Filter child nodes and show number of children

Select user(s) to import below. Only LDAP entries that are marked green can be imported (indicating that these entries match the configured LDAP filter **and** their usernames can be found using the configured username attribute). You can configure other user mapping attributes above.

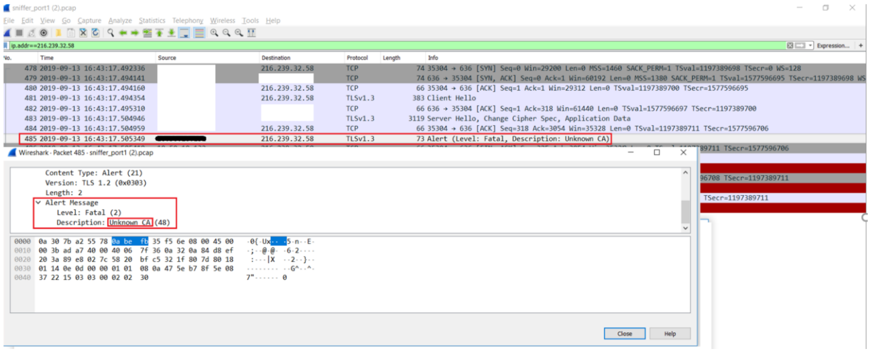
Select Visible Select None

```
└ Query failed: ldap_search_ext_s connection failed: Can't contact LDAP server error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed (unable to get local issuer certificate)
```

Distinguished name: dc[redacted],dc=com,dc=br

Organization: [Please Select] ▼

OK Cancel



sniffer_port1 (2).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

ip.addr==216.239.32.58

```
No.  Time                          Source        Destination     Protocol  Length  Info
 478 2019-09-13 16:43:17.492336                 216.239.32.58   TCP         74 35304 → 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1197389698 TSecr=0 WS=128
 479 2019-09-13 16:43:17.494141                                 TCP         74 636 → 35304 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=1577596695 TSecr=1197389698 WS
 480 2019-09-13 16:43:17.494160                 216.239.32.58   TCP         66 35304 → 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1197389700 TSecr=1577596695
 481 2019-09-13 16:43:17.494354                 216.239.32.58   TLSv1.3    383 Client Hello
 482 2019-09-13 16:43:17.495310                                 TCP         66 636 → 35304 [ACK] Seq=1 Ack=318 Win=61440 Len=0 TSval=1577596697 TSecr=1197389700
 483 2019-09-13 16:43:17.504946                                 TLSv1.3   3119 Server Hello, Change Cipher Spec, Application Data
 484 2019-09-13 16:43:17.504959                 216.239.32.58   TCP         66 35304 → 636 [ACK] Seq=318 Ack=3054 Win=35328 Len=0 TSval=1197389711 TSecr=1577596706
 485 2019-09-13 16:43:17.505349  [redacted]     216.239.32.58   TLSv1.3     73 Alert (Level: Fatal, Description: Unknown CA)
```

Wireshark · Packet 485 · sniffer_port1 (2).pcap

```
    Content Type: Alert (21)
    Version: TLS 1.2 (0x0303)
    Length: 2
  ∨ Alert Message
      Level: Fatal (2)
      Description: Unknown CA (48)
```

```
0000  0a 30 7b a2 55 78 0a be  fb 35 f5 6e 08 00 45 00   ·0{·Ux·· ·5·n··E·
0010  00 3b ad a7 40 00 40 06  7f 36 0a 32 0a 84 d8 ef   ·;··@·@· ·6·2····
0020  20 3a 89 e8 02 7c 58 20  bf c5 32 1f 80 7d 80 18    :···|X  ··2··}··
0030  01 14 0e 0d 00 00 01 01  08 0a 47 5e b7 8f 5e 08   ········ ··G^··^·
0040  37 22 15 03 03 00 02 02  30                        7"······ 0
```

SAML Authentication

This section describes configuring SAML authentication.

SAML IdP proxy for Azure

This recipe describes how to set up FortiAuthenticator as a SAML IdP proxy for Microsoft Azure.

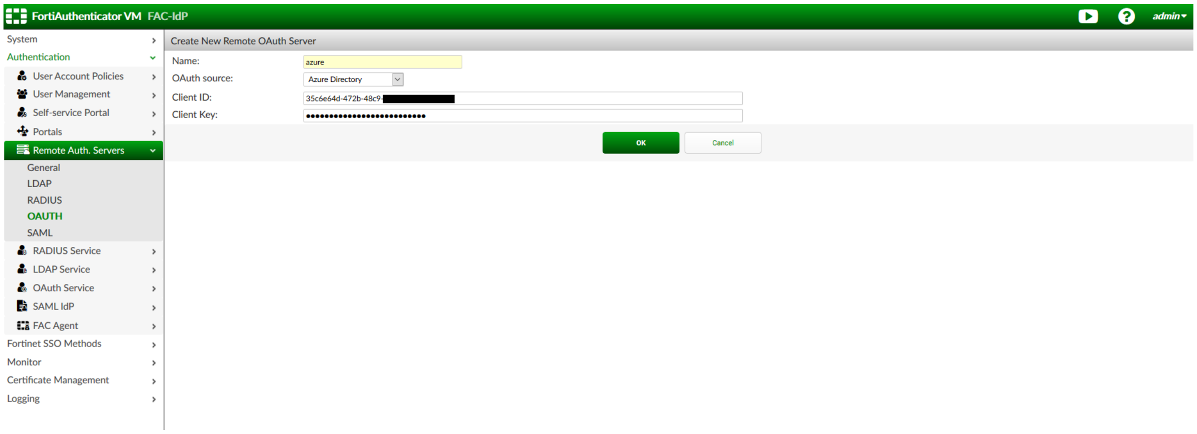
To configure FortiAuthenticator as a SAML IdP proxy for Azure:

1. Configuring OAuth settings on page 152
2. Configuring the remote SAML server on page 153
3. Enabling the SAML SP FSSO Portal on page 153
4. Configuring an Azure realm on page 154
5. Configuring SAML IdP settings on page 154
6. Configuring the login page replacement message on page 155
7. Results on page 156

Configuring OAuth settings

To configure remote OAuth settings:

1. On FortiAuthenticator, go to *Remote Auth. Servers* > *OAUTH*, and click *Create New*.
2. Provide a name for the server and select *Azure Directory* as the OAuth source.
3. Enter the client ID and client key from the SAML application on your Azure account.



Create New Remote OAuth Server

Name: azure

OAuth source: Azure Directory

Client ID: 35c6e64d-472b-48c9-[redacted]

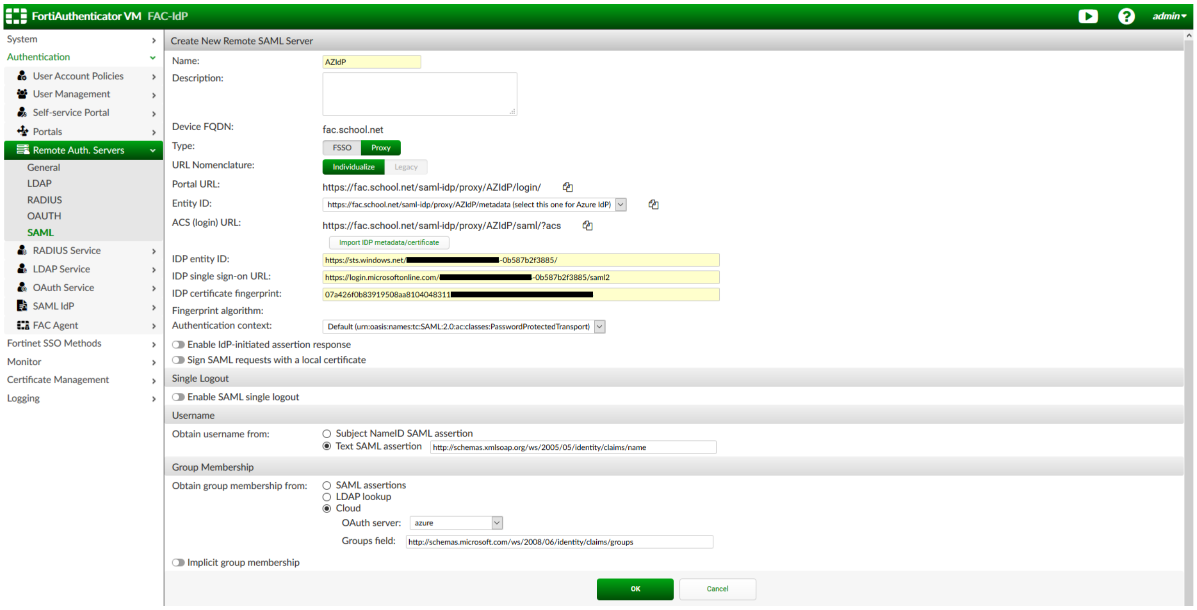
Client Key: ••••••••••••••••••••••••••

4. Click *OK* to save your changes.

Configuring the remote SAML server

To configure the remote SAML server:

1. Go to *Remote Auth. Servers* > *SAML*, and click *Create New*.
   The server name must match the one created in https://portal.azure.com/. For example, if the name in Azure is set as AZIdP, the SAML server should also use AZIdP (case sensitive).
2. For the *Entity ID*, click the dropdown menu and select the Azure IdP option.
3. Import the IdP metadata from Azure. To download and import the Azure federation metadata:
   a. In Azure, go to *Azure Active Directory* > *App Registrations* and select the application being used for SAML authentications for your FortiAuthenticator.
   b. In *Endpoints*, select the federation metadata document, enter the URL into the browser, and save it as an XML file.
   c. Click *Import IDP metadata/certificate*, and upload the federation metadata file.
4. In Group Membership, select *Cloud* and choose the previously created Azure OAuth server.
5. At the top of the page, select *Proxy* as the Type, and copy the *Portal URL* to be used later when customizing the replacement message.



Create New Remote SAML Server

Name: AZIdP
Description:
Device FQDN: fac.school.net
Type: FSSO [✓ Proxy]
URL Nomenclature: [✓ Individualize] Legacy
Portal URL: https://fac.school.net/saml-idp/proxy/AZIdP/login/
Entity ID: https://fac.school.net/saml-idp/proxy/AZIdP/metadata (select this one for Azure IdP)
ACS (login) URL: https://fac.school.net/saml-idp/proxy/AZIdP/saml/?acs
Import IDP metadata/certificate
IDP entity ID: https://sts.windows.net/[redacted]-0b587b2f3885/
IDP single sign-on URL: https://login.microsoftonline.com/[redacted]-0b587b2f3885/saml2
IDP certificate fingerprint: 07a426f0b83919508aa8104048311[redacted]
Fingerprint algorithm:
Authentication context: Default (urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport)
Enable IdP-initiated assertion response
Sign SAML requests with a local certificate

Single Logout

Enable SAML single logout

Username

Obtain username from:
○ Subject NameID SAML assertion
● Text SAML assertion http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Group Membership

Obtain group membership from:
○ SAML assertions
○ LDAP lookup
● Cloud
OAuth server: azure
Groups field: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

Implicit group membership

OK Cancel

6. Click *OK* to save your changes.

Enabling the SAML SP FSSO Portal

To enable the SAML SP FSSO Portal:

1. Go to *Fortinet FSSO Methods* > *SSO* > *Portal Services* and enable the SAML portal.
2. Go to *Fortinet FSSO Methods* > *SSO* > *SAML Authentication* and create a new SAML server.
   Select the previously created remote SAML server and click *OK*.

Configuring an Azure realm

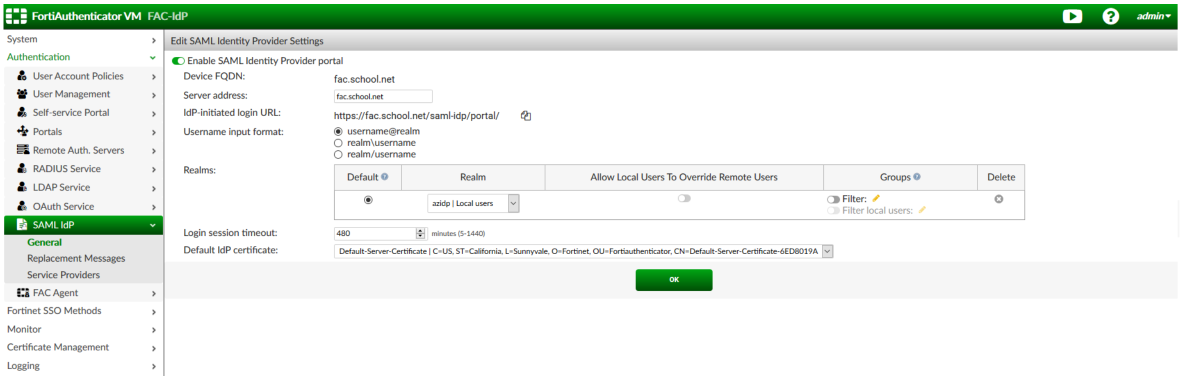
To create an Azure realm and add it to the IdP:

1. Go to *Authentication* > *User Management* > *Realms*
2. Click *Create New*.
3. Add the details of the Azure realm, and click *OK*.

Configuring SAML IdP settings

To configure general settings:

1. Go to *Authentication* > *SAML IdP* > *General.*
2. Enable the SAML identity provider portal and enter the following:
   a. **Server address**: Enter the FortiAuthenticator FQDN.
   b. **Realms**: Add the realm associated with the remote server for Azure IdP.
   c. **Default IdP certificate**: Select a default certificate to use.



Edit SAML Identity Provider Settings

Enable SAML Identity Provider portal

Device FQDN: fac.school.net

Server address: fac.school.net

IdP-initiated login URL: https://fac.school.net/saml-idp/portal/

Username input format: ● username@realm ○ realm\username ○ realm/username

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	azidp | Local users		Filter: Filter local users:	

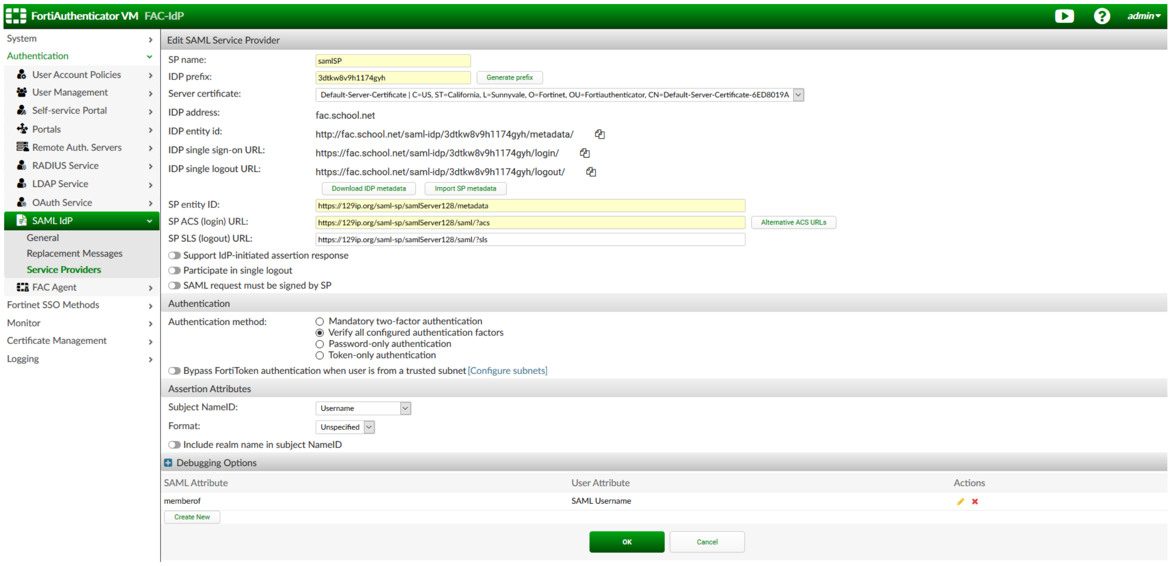
Login session timeout: 480 minutes (5-1440)

Default IdP certificate: Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-6ED8019A

3. Click *OK* to save your changes.

To configure service provider settings:

1. Go to *Authentication* > *SAML IdP* > *Service Providers* and create a new reference for the service provider that you will be using as your SAML client.
   The name can be anything you want.
2. Enter the SP information from the client you will be using as the SAML service provider.
3. Download the IdP metadata.
   This can be used to set up the SAML IdP configuration in your SAML SP client (if allowed by your client).
4. Under *SAML Attribute* click *Create New*, and enter a *SAML Attribute* name that your SAML SP is expecting to identify the user. Select a *User Attribute* for this selection. If you're unsure of which attribute to pick, select *SAML Username*.



Edit SAML Service Provider

SP name: samlSP
IDP prefix: 3dtkw8v9h1174gyh
Server certificate: Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-6ED8019A
IDP address: fac.school.net
IDP entity id: http://fac.school.net/saml-idp/3dtkw8v9h1174gyh/metadata/
IDP single sign-on URL: https://fac.school.net/saml-idp/3dtkw8v9h1174gyh/login/
IDP single logout URL: https://fac.school.net/saml-idp/3dtkw8v9h1174gyh/logout/
SP entity ID: https://129ip.org/saml-sp/samlServer128/metadata
SP ACS (login) URL: https://129ip.org/saml-sp/samlServer128/saml/?acs
SP SLS (logout) URL: https://129ip.org/saml-sp/samlServer128/saml/?sls

Support IdP-initiated assertion response
Participate in single logout
SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory two-factor authentication
● Verify all configured authentication factors
○ Password-only authentication
○ Token-only authentication

Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets]

Assertion Attributes

Subject NameID: Username
Format: Unspecified
Include realm name in subject NameID

Debugging Options

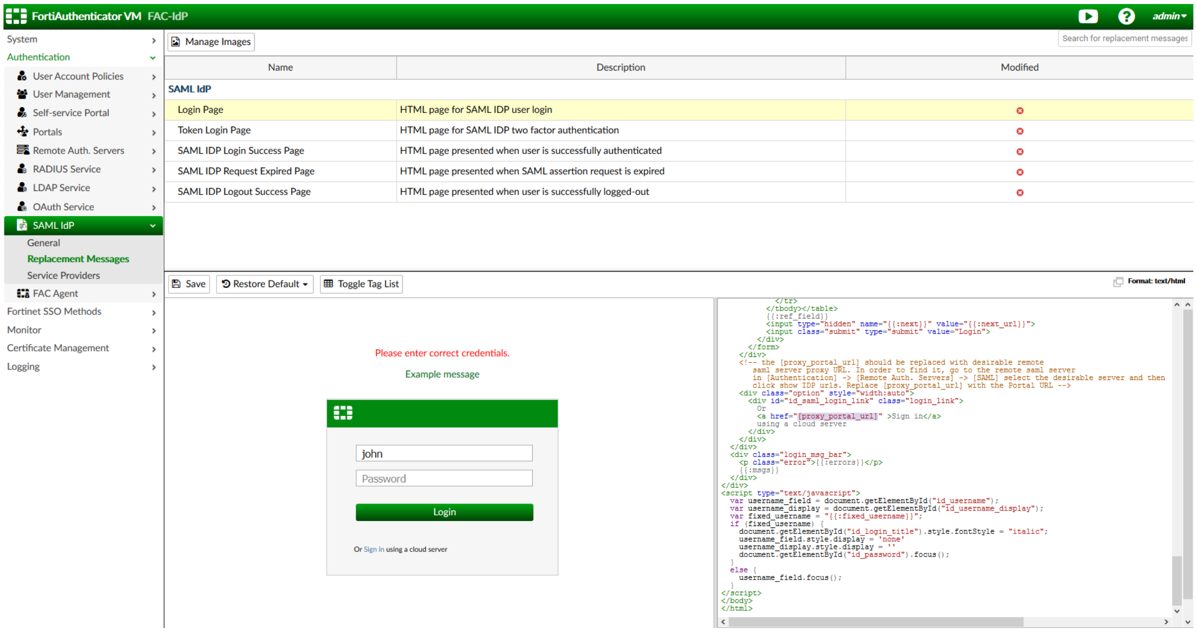
SAML Attribute	User Attribute	Actions
memberof	SAML Username	✎ ✖

5. Click *OK* to save your changes.

Configuring the login page replacement message

To configure the login page replacement message:

1. Go to *Authentication > SAML IdP > Replacement Messages*.
2. On the *Login Page* replacement message, click the *Restore Defaults* dropdown and choose *idp-server-and-proxy*.
3. In the text/html editor, scroll down until you see the `[proxy_portal_url]` placeholder and replace it with the previously saved proxy portal URL.



Name	Description	Modified
SAML IdP		
Login Page	HTML page for SAML IDP user login	✖
Token Login Page	HTML page for SAML IDP two factor authentication	✖
SAML IDP Login Success Page	HTML page presented when user is successfully authenticated	✖
SAML IDP Request Expired Page	HTML page presented when SAML assertion request is expired	✖
SAML IDP Logout Success Page	HTML page presented when user is successfully logged-out	✖

Please enter correct credentials.

Example message

john
Password

Or Sign in using a cloud server

```
          </tr>
        </tbody></table>
        {{:ref_field}}
        <input type="hidden" name="{{:next}}" value="{{:next_url}}">
        <input class="submit" type="submit" value="Login">
      </div>
    </form>
  </div>
  <!-- the [proxy_portal_url] should be replaced with desirable remote
     saml server proxy URL. In order to find it, go to the remote saml server
     in [Authentication] -> [Remote Auth. Servers] -> [SAML] select the desirable server and then
     click show IDP urls. Replace [proxy_portal_url] with the Portal URL -->
  <div class="option" style="width:auto">
    <div id="id_saml_login_link" class="login_link">
      Or
      <a href="[proxy_portal_url]" >Sign in</a>
      using a cloud server
    </div>
  </div>
</div>
<div class="login_msg_bar">
  <p class="error">{{:errors}}</p>
  {{:msgs}}
</div>
</div>
<script type="text/javascript">
  var username_field = document.getElementById("id_username");
  var username_display = document.getElementById("id_username_display");
  var fixed_username = "{{:fixed_username}}";
  if (fixed_username) {
    document.getElementById("id_login_title").style.fontStyle = "italic";
    username_field.style.display = 'none'
    username_display.style.display = ''
    document.getElementById("id_password").focus();
  }
  else {
    username_field.focus();
  }
</script>
</body>
</html>
```

4. Click *Save*.

Results

To test Azure login through the SP:

1. Enter in the portal login URL from the service provider in a new browser.
   You are redirect you to the FAC's IdP-server and proxy page.
2. Click on the link below the login options to be redirected to Microsoft's login page.

SAML IdP proxy for G Suite

This recipe describes how to set up FortiAuthenticator as a SAML IdP proxy for Google G Suite.

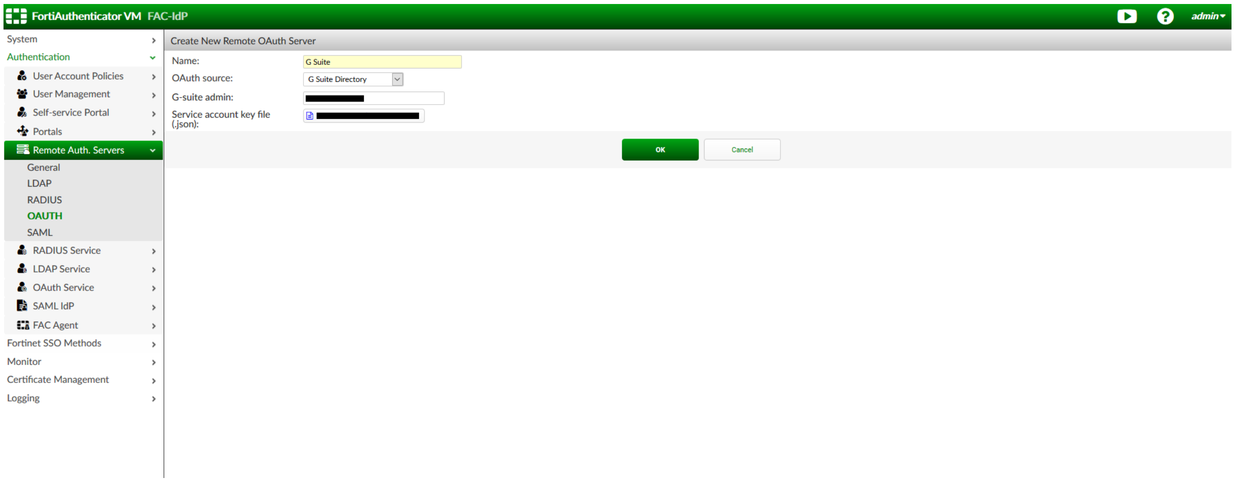
To configure FortiAuthenticator as a SAML IdP proxy for G Suite:

1. Configuring OAuth settings on page 156
2. Configuring the remote SAML server on page 157
3. Enabling the SAML SP FSSO Portal on page 157
4. Configuring a G Suite Realm on page 158
5. Configuring IdP settings on page 158
6. Configuring the login page replacement message on page 159
7. Results on page 160

Configuring OAuth settings

To configure remote OAuth settings:

1. On FortiAuthenticator, go to *Remote Auth. Servers* > *OAUTH*, and click *Create New*.
2. Provide a name for the server and select *G Suite Directory* as the OAuth source.
3. Enter the *G-suite admin*, and upload the *Service account key file* from the SAML application on your G Suite account.
4. Click *OK* to save your changes.



Create New Remote OAuth Server

Name: G Suite

OAuth source: G Suite Directory

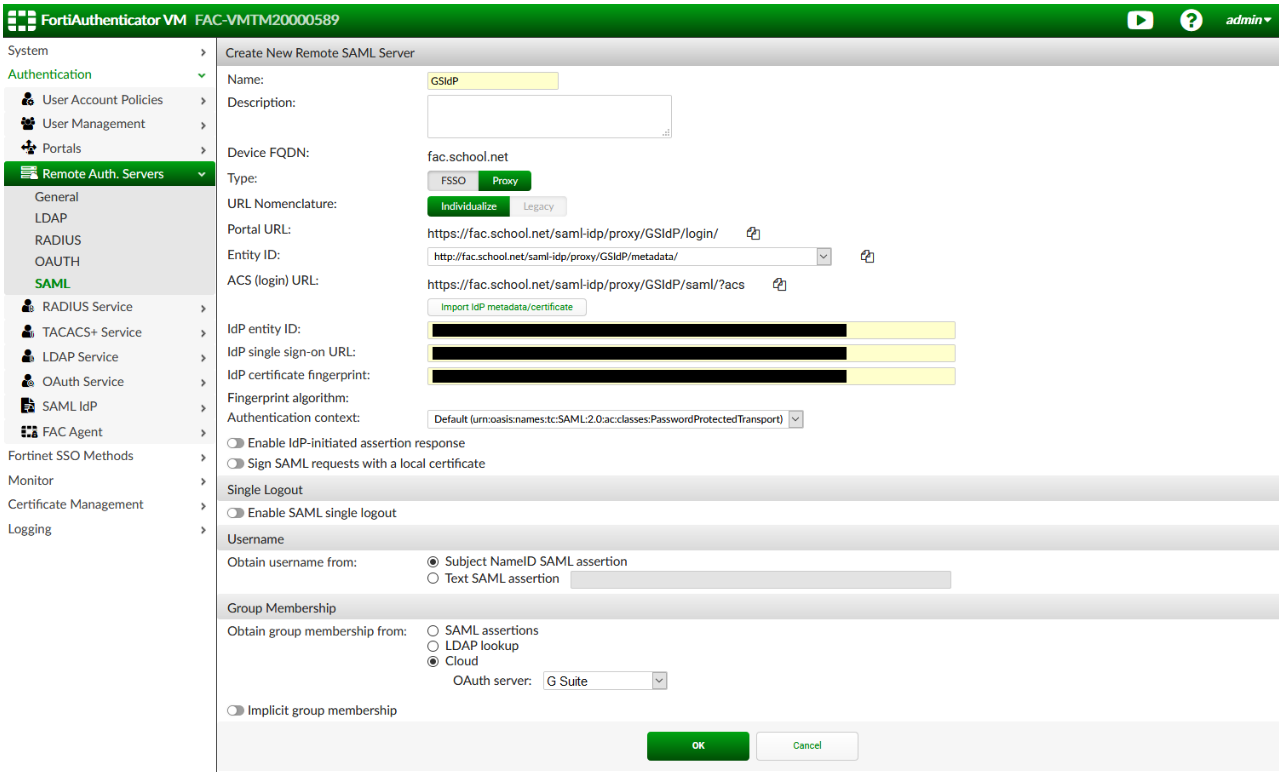
G-suite admin: [redacted]

Service account key file (.json): [redacted]

Configuring the remote SAML server

To configure the remote SAML server:

1. Go to *Remote Auth. Servers* > *SAML*, and click *Create New*.
   The server name must match the one created in G Suite. For example, if the name in G Suite is set as GSIdP, the SAML server should also use GSIdP (case sensitive).
2. Import the IdP metadata obtained from the SAML app on G Suite.
3. In Group Membership, select *Cloud* and choose the previously created G Suite OAuth server.
4. At the top of the page, select *Proxy* as the Type, and copy the *Portal URL* to be used later when customizing the replacement message.



Create New Remote SAML Server

Name: GSIdP

Description:

Device FQDN: fac.school.net

Type: FSSO [✓ Proxy]

URL Nomenclature: [✓ Individualize] Legacy

Portal URL: https://fac.school.net/saml-idp/proxy/GSIdP/login/

Entity ID: http://fac.school.net/saml-idp/proxy/GSIdP/metadata/

ACS (login) URL: https://fac.school.net/saml-idp/proxy/GSIdP/saml/?acs

Import IdP metadata/certificate

IdP entity ID: [redacted]

IdP single sign-on URL: [redacted]

IdP certificate fingerprint: [redacted]

Fingerprint algorithm:

Authentication context: Default (urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport)

Enable IdP-initiated assertion response

Sign SAML requests with a local certificate

Single Logout

Enable SAML single logout

Username

Obtain username from: ● Subject NameID SAML assertion ○ Text SAML assertion

Group Membership

Obtain group membership from: ○ SAML assertions ○ LDAP lookup ● Cloud

OAuth server: G Suite

Implicit group membership

5. Click *OK* to save your changes.

Enabling the SAML SP FSSO Portal

To enable the SAML SP FSSO Portal:

1. Go to *Fortinet FSSO Methods* > *SSO* > *Portal Services* and enable the SAML portal.
2. Go to *Fortinet FSSO Methods* > *SSO* > *SAML Authentication* and create a new SAML server.
   Select the previously created remote SAML server and click *OK*.

Configuring a G Suite Realm

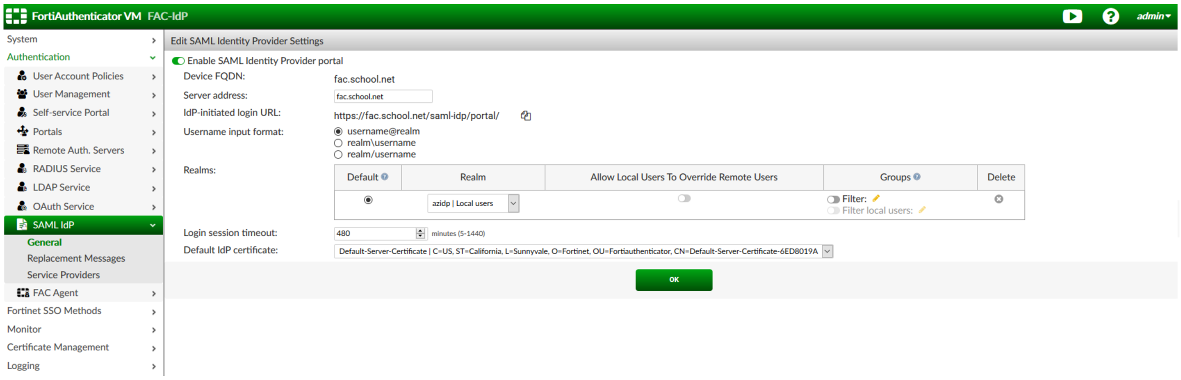
To create a G Suite Realm and add it to the IdP:

1. Go to *Authentication* > *User Management* > *Realms.*
2. Click *Create New*.
3. Add the details of the G Suite realm, and click *OK*.

Configuring IdP settings

To configure general settings:

1. Go to *Authentication* > *SAML IdP* > *General.*
2. Enable the SAML identity provider portal and enter the following:
   a. **Server address**: Enter the FortiAuthenticator FQDN.
   b. **Realms**: Add the realm associated with the remote server for G Suite.
   c. **Default IdP certificate**: Select a default certificate to use.



Edit SAML Identity Provider Settings

Enable SAML Identity Provider portal

Device FQDN: fac.school.net

Server address: fac.school.net

IdP-initiated login URL: https://fac.school.net/saml-idp/portal/

Username input format:
● username@realm
○ realm\username
○ realm/username

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	azidp | Local users		Filter: Filter local users:	

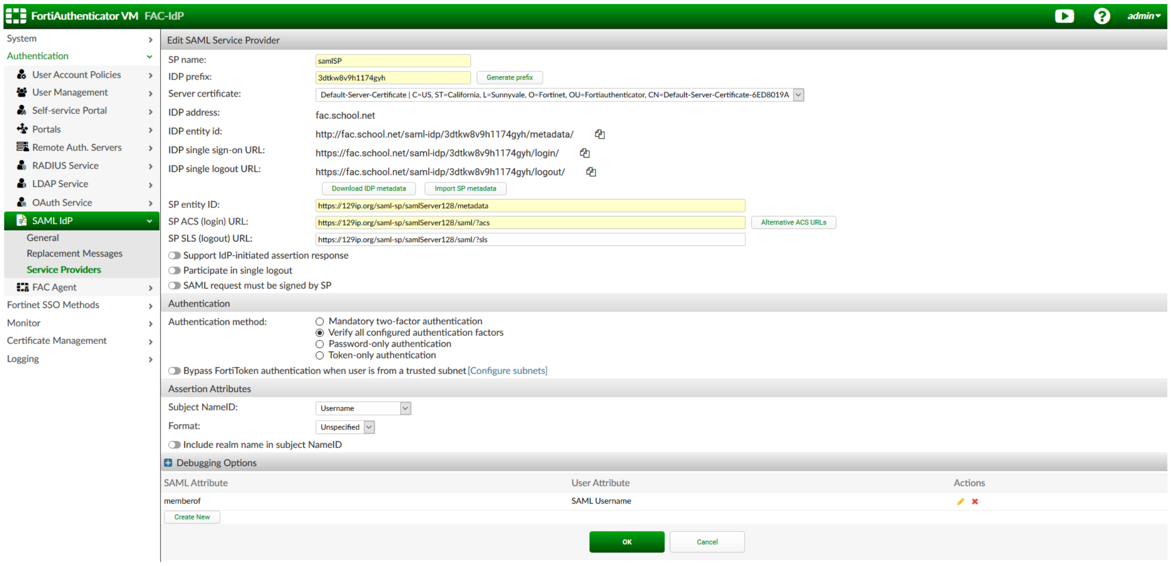
Login session timeout: 480 minutes (5-1440)

Default IdP certificate: Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-6ED8019A

3. Click *OK* to save your changes.

To configure service provider settings:

1. Go to *Authentication* > *SAML IdP* > *Service Providers* and create a new reference for the service provider that you will be using as your SAML client.
   The name can be anything you want.
2. Enter the SP information from the client you will be using as the SAML service provider.
3. Download the IdP metadata.
   This can be used to set up the SAML IdP configuration in your SAML SP client (if allowed by your client).
4. Under *SAML Attribute* click *Create New*, and enter a *SAML Attribute* name that your SAML SP is expecting to identify the user. Select a *User Attribute* for this selection. If you're unsure of which attribute to pick, select *SAML Username*.



Edit SAML Service Provider

SP name: samlSP

IDP prefix: 3dtkw8v9h1174gyh [Generate prefix]

Server certificate: Default-Server-Certificate | C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Fortiauthenticator, CN=Default-Server-Certificate-6ED8019A

IDP address: fac.school.net

IDP entity id: http://fac.school.net/saml-idp/3dtkw8v9h1174gyh/metadata/

IDP single sign-on URL: https://fac.school.net/saml-idp/3dtkw8v9h1174gyh/login/

IDP single logout URL: https://fac.school.net/saml-idp/3dtkw8v9h1174gyh/logout/

[Download IDP metadata] [Import SP metadata]

SP entity ID: https://129ip.org/saml-sp/samlServer128/metadata

SP ACS (login) URL: https://129ip.org/saml-sp/samlServer128/saml/?acs [Alternative ACS URLs]

SP SLS (logout) URL: https://129ip.org/saml-sp/samlServer128/saml/?sls

Support IdP-initiated assertion response

Participate in single logout

SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory two-factor authentication
● Verify all configured authentication factors
○ Password-only authentication
○ Token-only authentication

Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets]

Assertion Attributes

Subject NameID: Username

Format: Unspecified

Include realm name in subject NameID

Debugging Options

SAML Attribute	User Attribute	Actions
memberof	SAML Username	✎ ✖

[Create New]

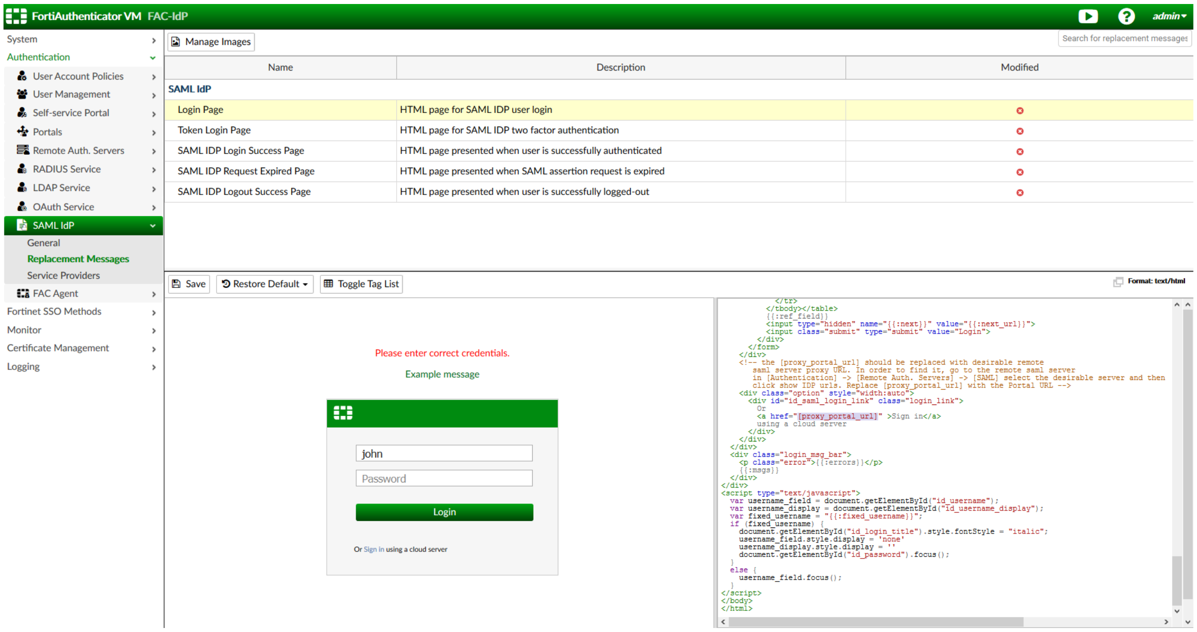
[OK] [Cancel]

5. Click *OK* to save your changes.

Configuring the login page replacement message

To configure the login page replacement message:

1. Go to *Authentication > SAML IdP > Replacement Messages*.
2. On the *Login Page* replacement message, click the *Restore Defaults* dropdown and choose *idp-server-and-proxy*.
3. In the text/html editor, scroll down until you see the `[proxy_portal_url]` placeholder and replace it with the previously saved proxy portal URL.



Name	Description	Modified
SAML IdP		
Login Page	HTML page for SAML IDP user login	✖
Token Login Page	HTML page for SAML IDP two factor authentication	✖
SAML IDP Login Success Page	HTML page presented when user is successfully authenticated	✖
SAML IDP Request Expired Page	HTML page presented when SAML assertion request is expired	✖
SAML IDP Logout Success Page	HTML page presented when user is successfully logged-out	✖

Please enter correct credentials.

Example message

```
          </tr>
         </tbody></table>
         {{:ref_field}}
         <input type="hidden" name="{{:next}}" value="{{:next_url}}">
         <input class="submit" type="submit" value="Login">
       </div>
     </form>
   </div>
   <!-- the [proxy_portal_url] should be replaced with desirable remote
      saml server proxy URL. In order to find it, go to the remote saml server
      in [Authentication] -> [Remote Auth. Servers] -> [SAML] select the desirable server and then
      click show IDP urls. Replace [proxy_portal_url] with the Portal URL -->
   <div class="option" style="width:auto">
     <div id="id_saml_login_link" class="login_link">
       Or
       <a href="[proxy_portal_url]" >Sign in</a>
       using a cloud server
     </div>
   </div>
 </div>
 <div class="login_msg_bar">
   <p class="error">{{:errors}}</p>
   {{:msgs}}
 </div>
</div>
<script type="text/javascript">
  var username_field = document.getElementById("id_username");
  var username_display = document.getElementById("id_username_display");
  var fixed_username = "{{:fixed_username}}";
  if (fixed_username) {
    document.getElementById("id_login_title").style.fontStyle = "italic";
    username_field.style.display = 'none'
    username_display.style.display = ''
    document.getElementById("id_password").focus();
  }
  else {
    username_field.focus();
  }
</script>
</body>
</html>
```

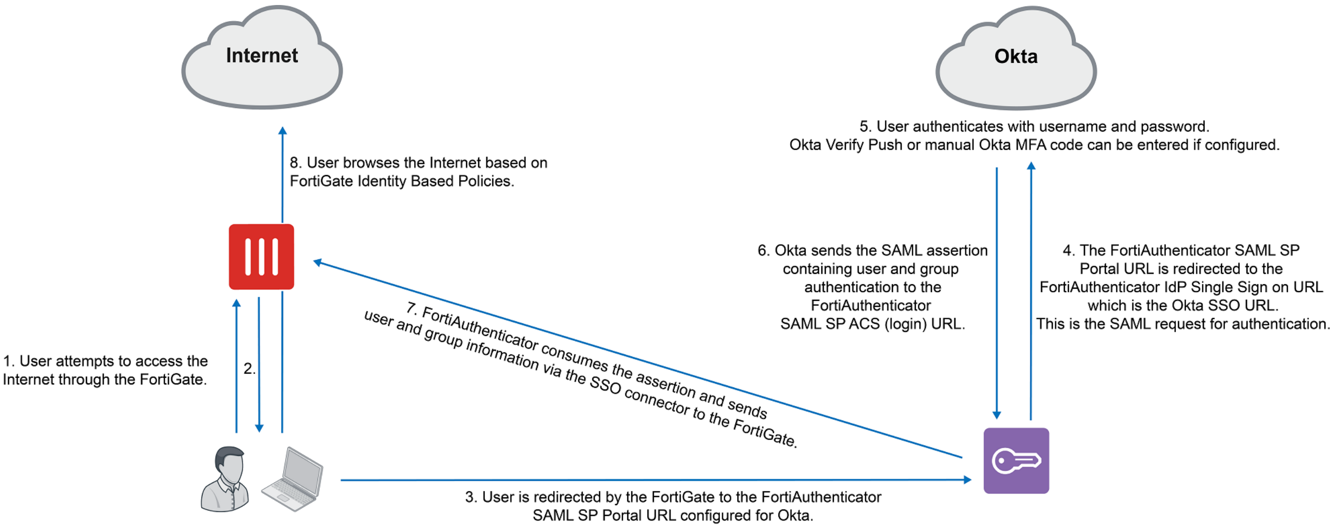
4. Click *Save*.

Results

To test G Suite login through the SP:

1. Enter in the portal login URL from the service provider in a new browser.
   You are redirect you to the FAC's IdP-server and proxy page.
2. Click on the link below the login options to be redirected to Google's login page.

SAML FSSO with FortiAuthenticator and Okta


Internet
Okta
5. User authenticates with username and password.
Okta Verify Push or manual Okta MFA code can be entered if configured.
8. User browses the Internet based on
FortiGate Identity Based Policies.
6. Okta sends the SAML assertion
containing user and group
authentication to the
FortiAuthenticator
SAML SP ACS (login) URL.
4. The FortiAuthenticator SAML SP
Portal URL is redirected to the
FortiAuthenticator IdP Single Sign on URL
which is the Okta SSO URL.
This is the SAML request for authentication.
7. FortiAuthenticator consumes the assertion and sends
user and group information via the SSO connector to the FortiGate.
1. User attempts to access the
Internet through the FortiGate.
2.
3. User is redirected by the FortiGate to the FortiAuthenticator
SAML SP Portal URL configured for 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. The FortiGate’s captive portal will offload the authentication request to the FortiAuthenticator’s SAML SP portal, which in turn redirects that client/browser to the SAML IdP login page. Assuming the user successfully logs into the portal, a positive SAML assertion will be sent back to the FortiAuthenticator, converting the user’s credentials into those of an FSSO user.

In this example configuration, the FortiGate has a DMZ IP address of `192.168.50.1`, and the FortiAuthenticator has the Port1 IP address of `192.168.50.100`. 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.

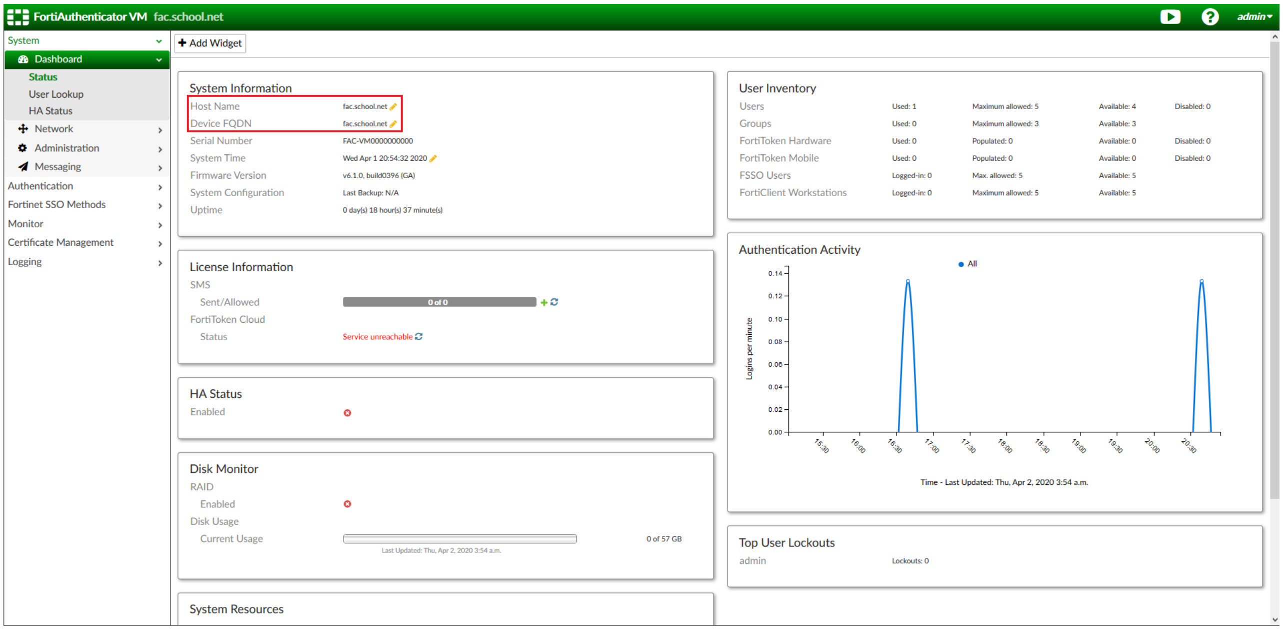
This configuration assumes that you have already created an Okta developer account.

Configuring DNS and FortiAuthenticator's FQDN

1. On FortiAuthenticator, go to *System* > *Dashboard* > *Status*. In the *System Information* widget, select the edit icon 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
Device FQDN	fac.school.net
Serial Number	FAC-VM0000000000
System Time	Wed Apr 1 20:54:32 2020
Firmware Version	v6.1.0, build0396 (GA)
System Configuration	Last Backup: N/A
Uptime	0 day(s) 18 hour(s) 37 minute(s)

License Information

SMS	
Sent/Allowed	0 of 0
FortiToken Cloud	
Status	Service unreachable

HA Status

Enabled	✗

Disk Monitor

RAID		
Enabled	✗	
Disk Usage		
Current Usage	Last Updated: Thu, Apr 2, 2020 3:54 a.m.	0 of 57 GB

System Resources

User Inventory

Users	Used: 1	Maximum allowed: 5	Available: 4	Disabled: 0
Groups	Used: 0	Maximum allowed: 3	Available: 3	
FortiToken Hardware	Used: 0	Populated: 0	Available: 0	Disabled: 0
FortiToken Mobile	Used: 0	Populated: 0	Available: 0	Disabled: 0
FSSO Users	Logged-in: 0	Max. allowed: 5	Available: 5	
FortiClient Workstations	Logged-in: 0	Maximum allowed: 5	Available: 5	

Top User Lockouts

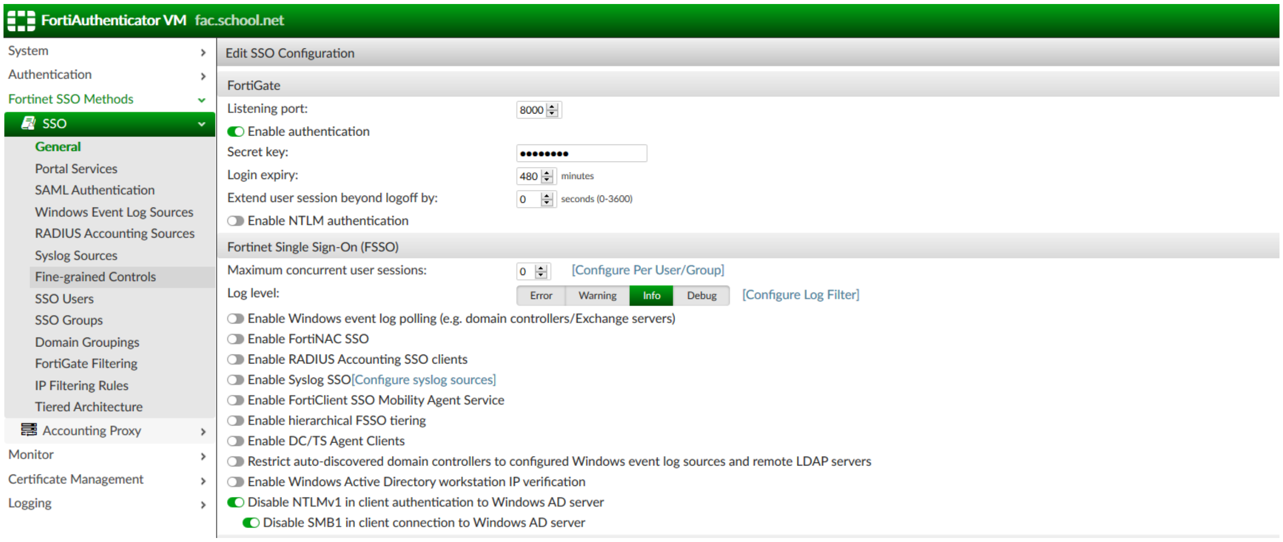
admin	Lockouts: 0

3. On FortiGate, open the CLI Console and enter the following command using the FortiAuthenticator 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 192.168.50.100
         next
      end
      set domain school.net
   next
```

Enabling FSSO and SAML on FortiAuthenticator

1. On 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 FortiGate to add the FortiAuthenticator as the FSSO server.



Edit SSO Configuration

FortiGate

Listening port: 8000

● Enable authentication

Secret key: ••••••••

Login expiry: 480 minutes

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

○ Enable NTLM authentication

Fortinet Single Sign-On (FSSO)

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

Log level: Error | Warning | [✓ Info] | Debug [Configure Log Filter]

○ Enable Windows event log polling (e.g. domain controllers/Exchange servers)

○ Enable FortiNAC SSO

○ Enable RADIUS Accounting SSO clients

○ Enable Syslog SSO[Configure syslog sources]

○ Enable FortiClient SSO Mobility Agent Service

○ Enable hierarchical FSSO tiering

○ Enable DC/TS Agent Clients

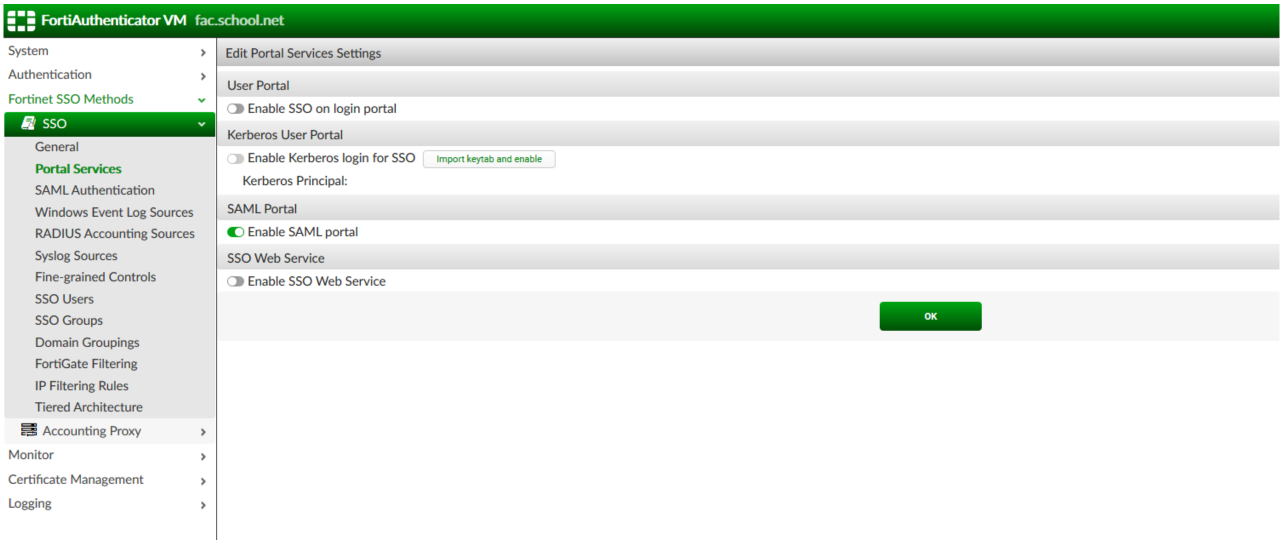
○ Restrict auto-discovered domain controllers to configured Windows event log sources and remote LDAP servers

○ Enable Windows Active Directory workstation IP verification

● Disable NTLMv1 in client authentication to Windows AD server

● Disable SMB1 in client connection to Windows AD server

2. Go to *Fortinet SSO Methods* > *SSO* > *Portal Services* and select *Enable SAML portal*.



Edit Portal Services Settings

User Portal

○ Enable SSO on login portal

Kerberos User Portal

○ Enable Kerberos login for SSO

Kerberos Principal:

SAML Portal

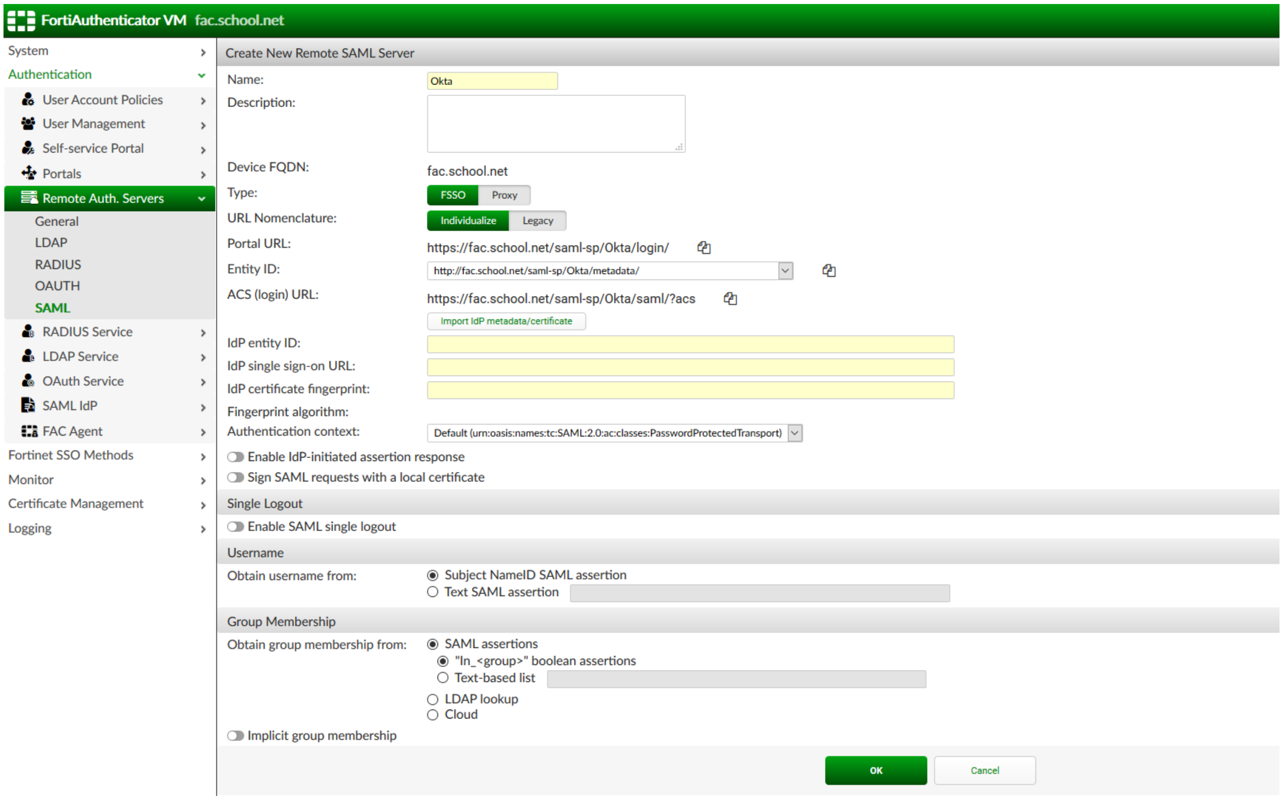
● Enable SAML portal

SSO Web Service

○ Enable SSO Web Service

3. Next, go to *Authentication* > *Remote Auth. Servers* > *SAML*, and click *Create New*. Enter Okta as the name.

> You will not yet be able to save these settings, as the IdP information - *IdP entity ID*, *IdP single sign-on URL*, and *IdP certificate fingerprint* - must be entered. These fields will be filled out later once the IdP application configuration is complete Okta.



Create New Remote SAML Server

Name: Okta

Description:

Device FQDN: fac.school.net

Type: FSSO | Proxy

URL Nomenclature: Individualize | Legacy

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

Entity ID: http://fac.school.net/saml-sp/Okta/metadata/

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

Import IdP metadata/certificate

IdP entity ID:

IdP single sign-on URL:

IdP certificate fingerprint:

Fingerprint algorithm:

Authentication context: Default (urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport)

Enable IdP-initiated assertion response

Sign SAML requests with a local certificate

Single Logout

Enable SAML single logout

Username

Obtain username from: ● Subject NameID SAML assertion
○ Text SAML assertion

Group Membership

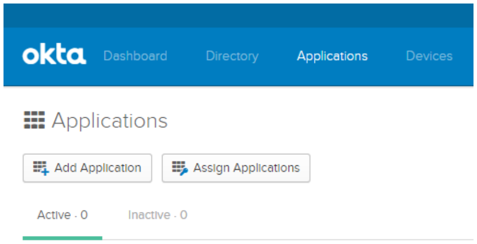
Obtain group membership from: ● SAML assertions
● "In_<group>" boolean assertions
○ Text-based list
○ LDAP lookup
○ Cloud

Implicit group membership

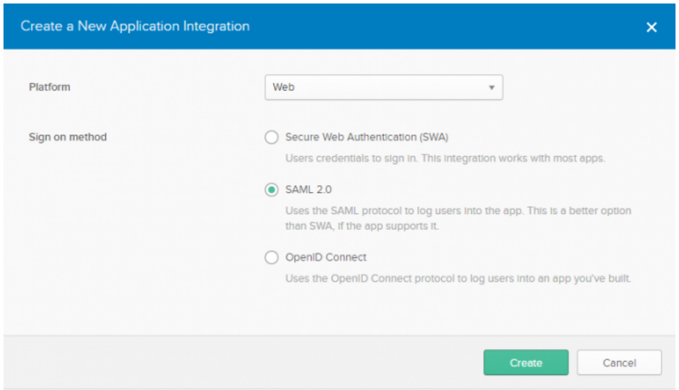
OK Cancel

Configuring the Okta developer account IdP application

1. Open a browser, go to the *Applications* tab and select *Add Application*.



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



Create a New Application Integration

Platform: Web

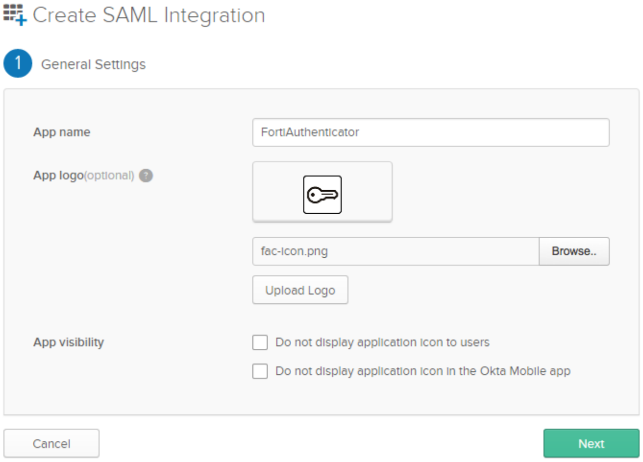
Sign on method

○ Secure Web Authentication (SWA)
Users credentials to sign in. This integration works with most apps.

● SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

○ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

3. Enter a custom app name, and select *Next*. You may upload an app logo if you wish.
   The name entered here is the name of the portal that users will log into.



Create SAML Integration

1 General Settings

App name: FortiAuthenticator

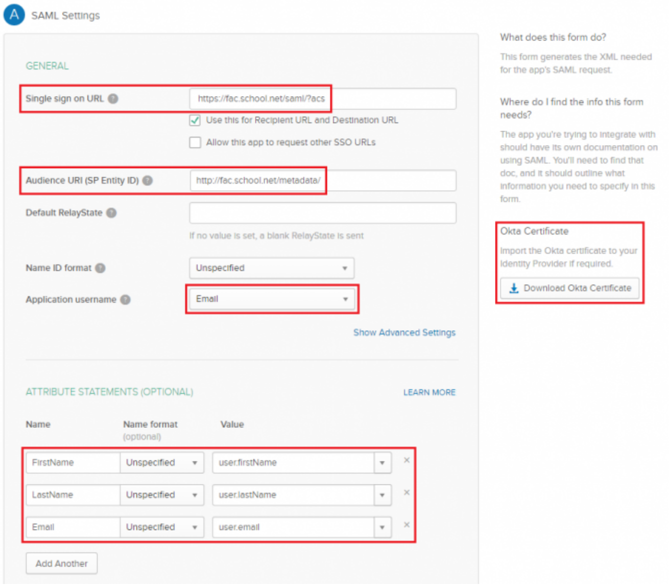
App logo(optional): fac-icon.png Browse..

Upload Logo

App visibility:
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app

Cancel | Next

4. Under *A - SAML Settings*, set *Single sign on URL* and *Audience URL (SP Entity ID)* to the *ACS* and *Entity URLs* (respectively) from 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, select *Download Okta Certificate*. This will be imported to the FortiAuthenticator later.



A SAML Settings

GENERAL

Single sign on URL: https://fac.school.net/saml/?acs

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): http://fac.school.net/metadata/

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Email

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?

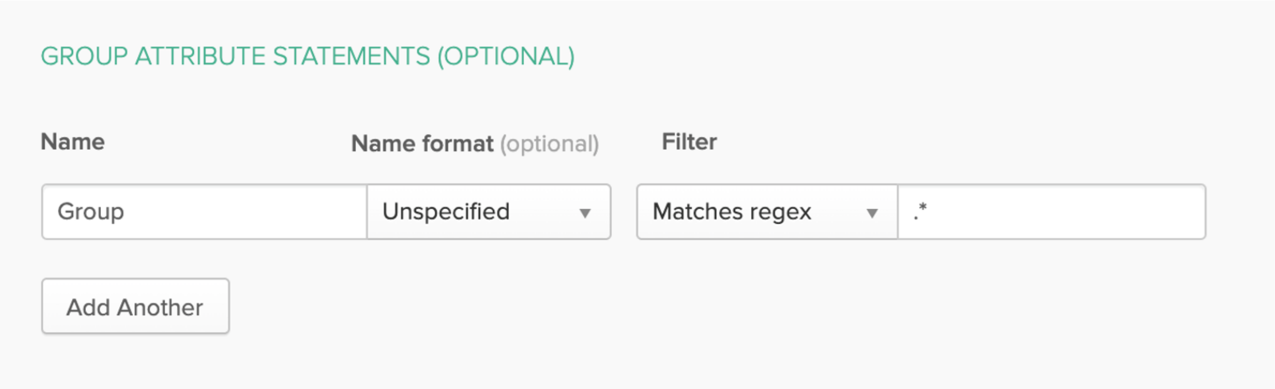
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

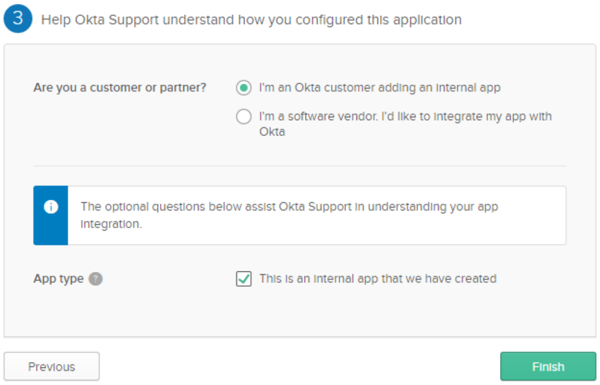
In the section below, configure a *Group* attribute to match on FortiAuthenticator. The word *Group* (case-sensitive) must be entered in *Text-based list* under *Obtain Group Membership from: SAML assertions* inside the remote SAML setup configuration on FortiAuthenticator. Regex matching is the most flexible option for group matching. The below example matches all groups of a single user.



GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
Group	Unspecified	Matches regex	.*

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



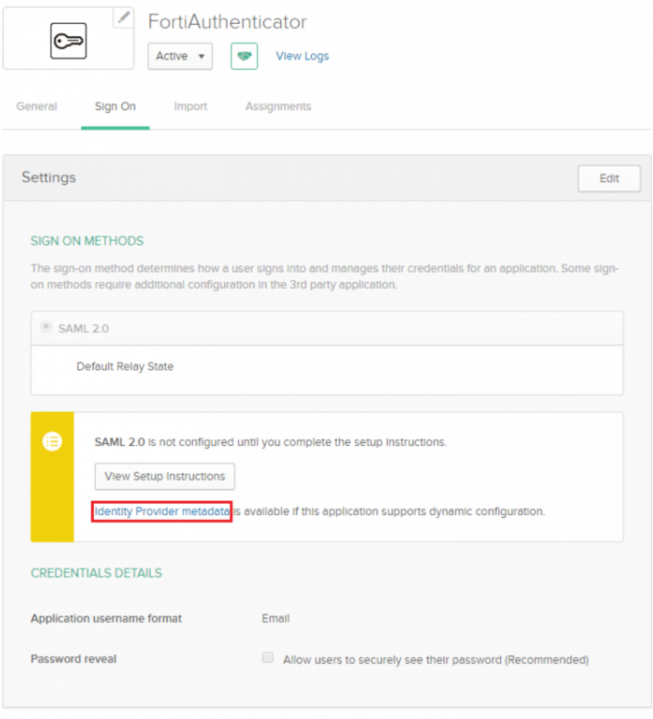
3 Help Okta Support understand how you configured this application

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

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



FortiAuthenticator

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.

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

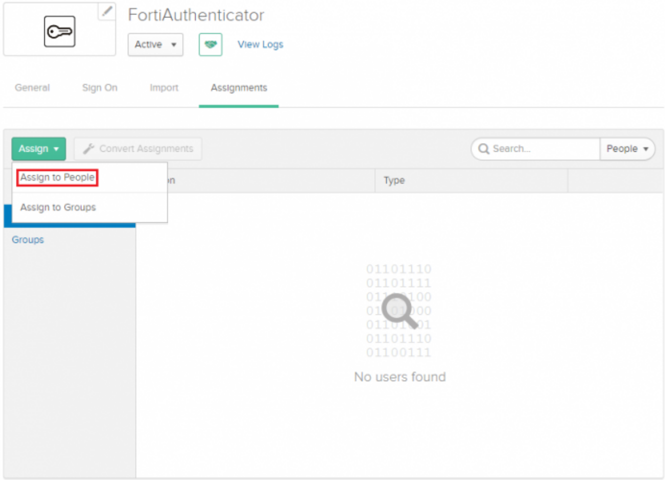
CREDENTIALS DETAILS

Application username format: Email

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

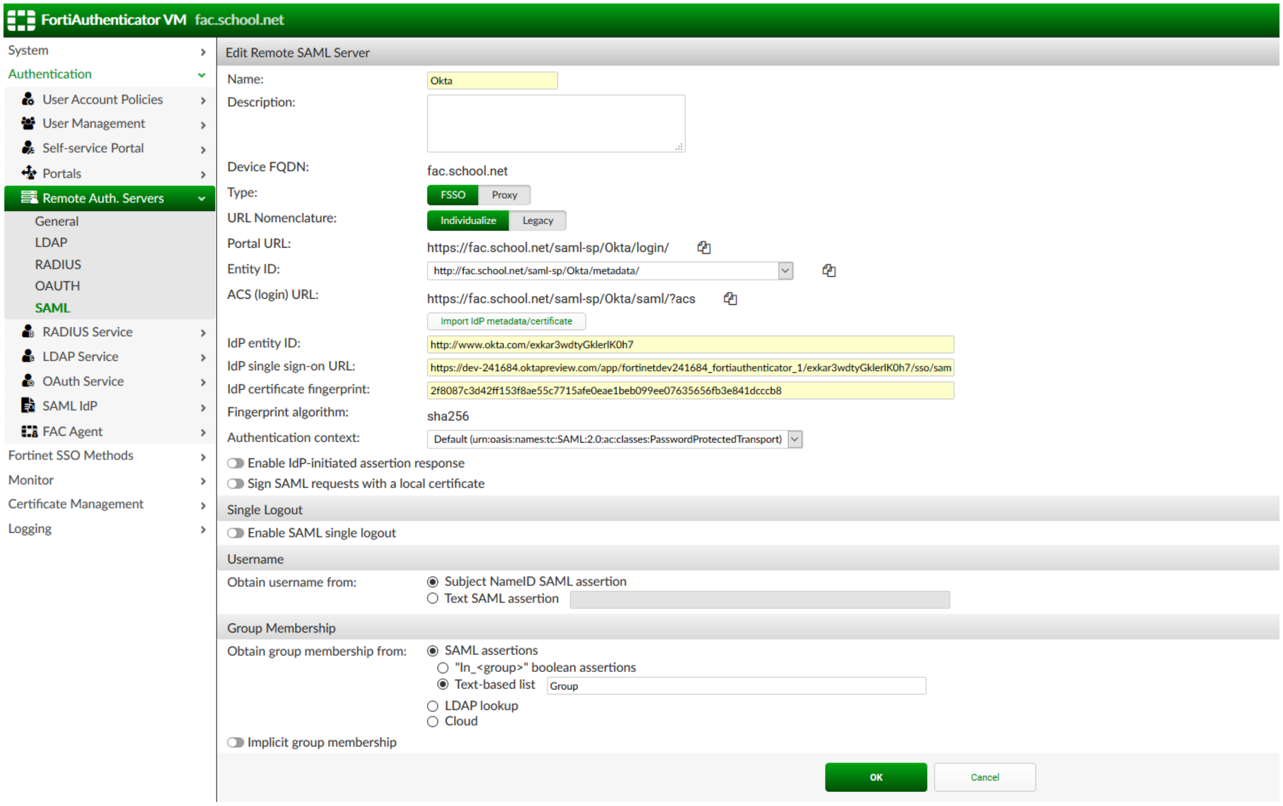
7. Finally, open the *Assignments tab* and select *Assign > Assign to people*.
Assign the users you wish to add to the application. This will permit the user to log in to the application's portal. Save

your changes, and select *Done*.



Importing the IdP certificate and metadata on FortiAuthenticator

1. On FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *SAML*, and import the IdP metadata and certificate downloaded from Okta.
   This will automatically fill in the IdP fields. Select *OK* to save your changes.



Edit Remote SAML Server

Name: Okta

Description:

Device FQDN: fac.school.net

Type: FSSO | Proxy

URL Nomenclature: Individualize | Legacy

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

Entity ID: http://fac.school.net/saml-sp/Okta/metadata/

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

IdP entity ID: http://www.okta.com/exkar3wdtyGklerlK0h7

IdP single sign-on URL: https://dev-241684.oktapreview.com/app/fortinetdev241684_fortiauthenticator_1/exkar3wdtyGklerlK0h7/sso/sam

IdP certificate fingerprint: 2f8087c3d42ff153f8ae55c7715afe0eae1beb099ee07635656fb3e841dcccb8

Fingerprint algorithm: sha256

Authentication context: Default (urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport)

Enable IdP-initiated assertion response

Sign SAML requests with a local certificate

Single Logout

Enable SAML single logout

Username

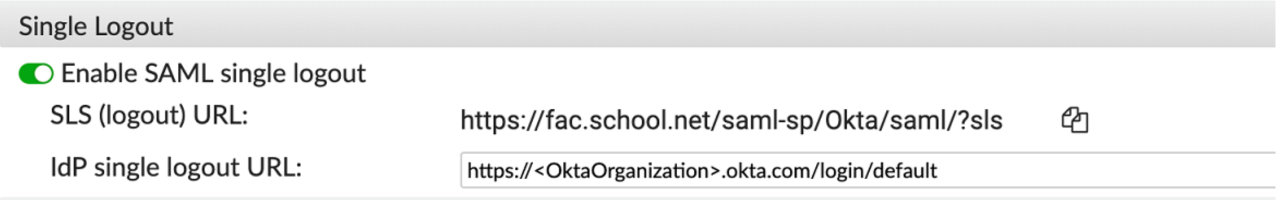
Obtain username from: ● Subject NameID SAML assertion
○ Text SAML assertion

Group Membership

Obtain group membership from: ● SAML assertions
○ "In_<group>" boolean assertions
● Text-based list Group
○ LDAP lookup
○ Cloud

Implicit group membership

2. Enable SAML single logout and add the *IdP single logout URL* under the *Single Logout* section of the Okta Remote SAML Server.
   For example, if your Okta organization is "facschool" then the *IdP single logout URL*: entry would be `https://facschool.okta.com/login/default`.



Single Logout

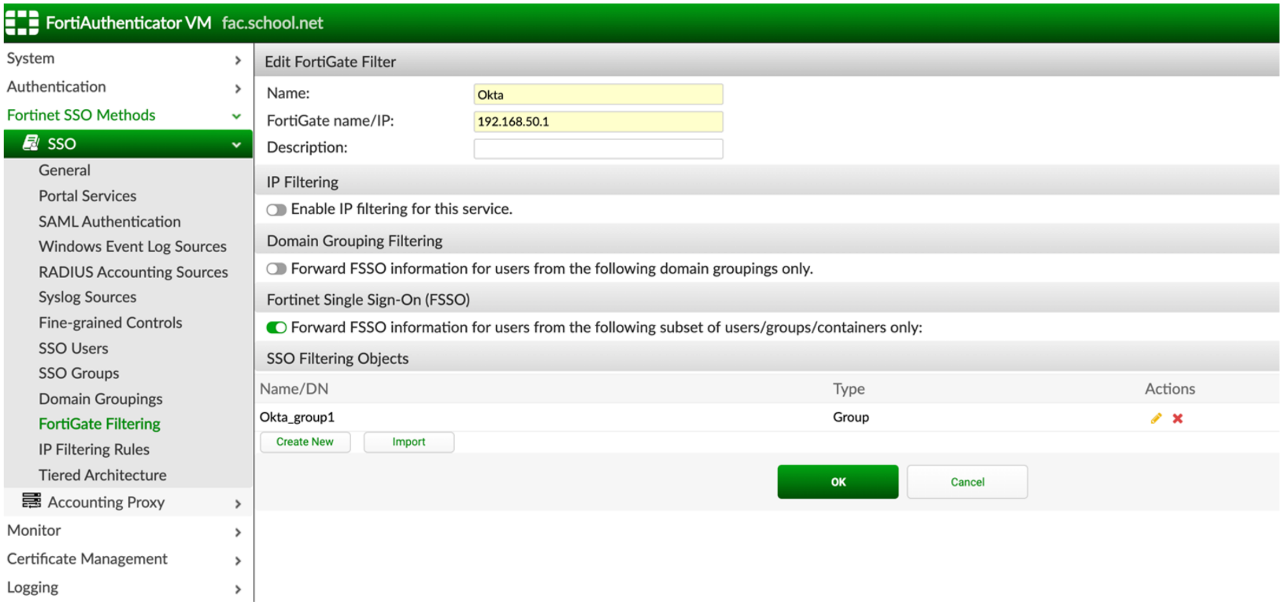
Enable SAML single logout

SLS (logout) URL: https://fac.school.net/saml-sp/Okta/saml/?sls

IdP single logout URL: https://<OktaOrganization>.okta.com/login/default

3. Go to *Fortinet SSO Methods* > *SSO* > *FortiGate Filtering*, and create a new FortiGate filter.
   Enter a name and the FortiGate's DMZ-interface IP address, and click *OK*.
   Once created, enable *Forward FSSO information for users from the following subset of users/groups/containers only*. Select *Create New* to create SSO group filtering objects that match each group inside Okta, and select *OK* to

apply all changes.



Edit FortiGate Filter

Name: Okta

FortiGate name/IP: 192.168.50.1

Description:

IP Filtering

○ Enable IP filtering for this service.

Domain Grouping Filtering

○ Forward FSSO information for users from the following domain groupings only.

Fortinet Single Sign-On (FSSO)

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

SSO Filtering Objects

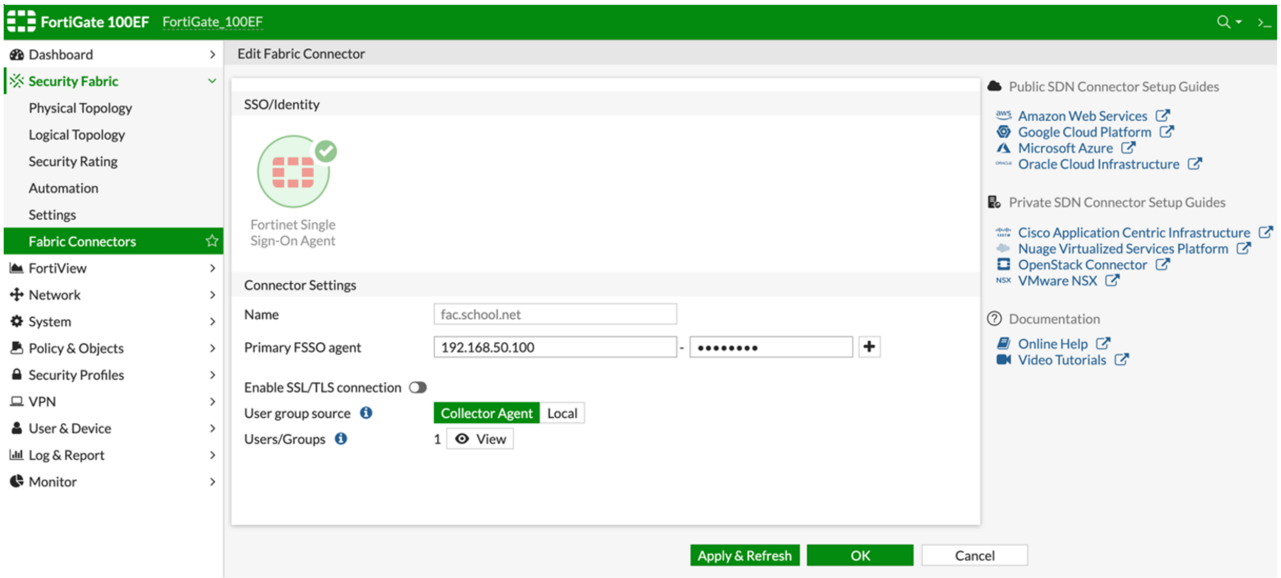
Name/DN	Type	Actions
Okta_group1	Group	✎ ✖

The names entered for the filter must be the same as the group names created in Okta. Failing to enter the exact same names will result in the SSO information not being pushed to FortiGate.

Configuring FSSO on FortiGate

To configure FSSO on FortiGate:

1. On FortiGate, go to *Security Fabric > Fabric Connectors*.
   Create a new FSSO agent connector to the FortiAuthenticator.
2. Select *Apply & Refresh*. The SAML user groups name has been successfully pushed to FortiGate from FortiAuthenticator, appearing when you select *View*.



Edit Fabric Connector

SSO/Identity

Connector Settings

Name: fac.school.net

Primary FSSO agent: 192.168.50.100 - •••••••• +

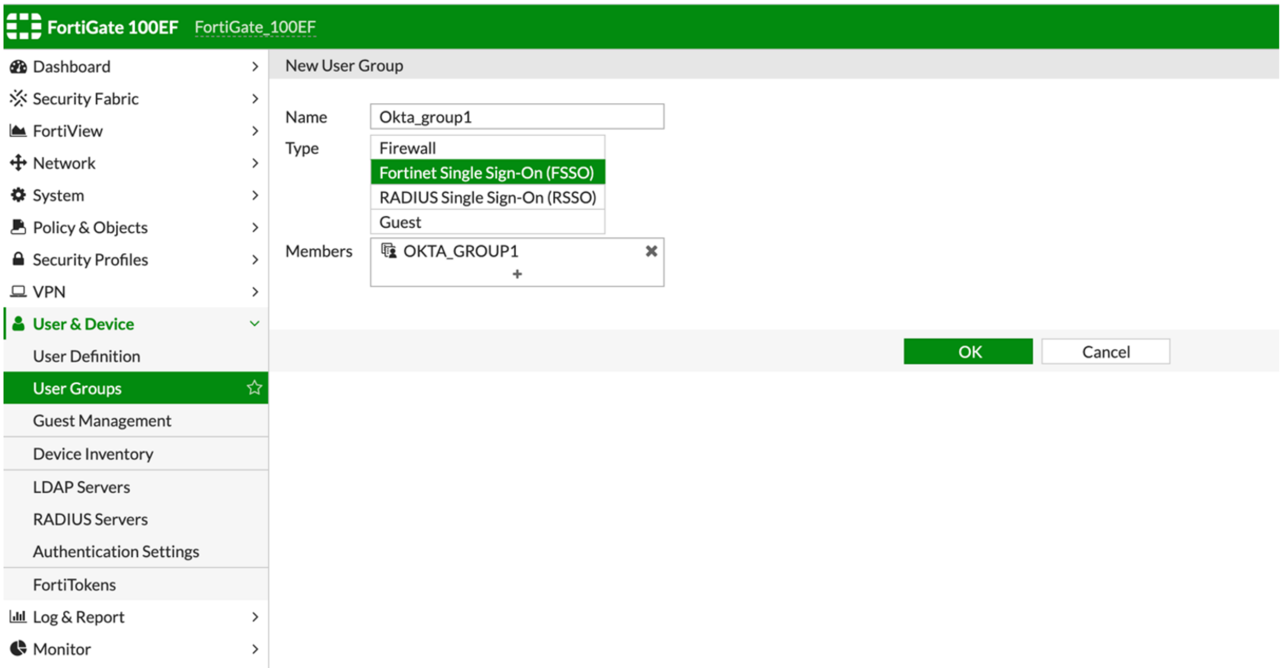
Enable SSL/TLS connection ○

User group source: Collector Agent | Local

Users/Groups: 1 View

Select *View* and make sure that the FSSO group has been pushed to FortiGate.

3. 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.*



New User Group

Name: Okta_group1

Type: Fortinet Single Sign-On (FSSO)

Members: OKTA_GROUP1

Configure automatic redirect

To configure automatic redirect on FortiGate:

In order to automatically redirect the user to the initial website after authentication, erase the existing HTML code and replace it with the following HTML code on the FortiGate in *System > Replacement Messages > Authentication > Login Page.*

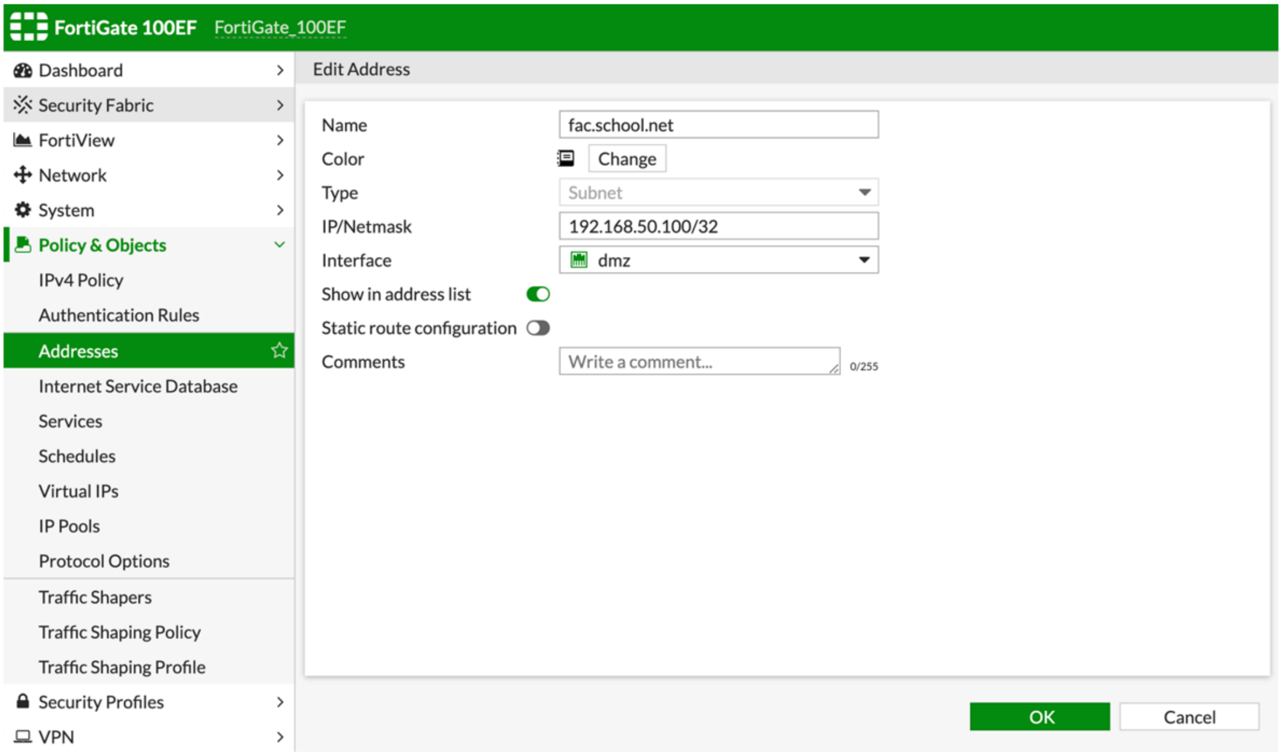
Replace **`<FortiAuthenticator-FQDN>`** with the DNS name of the FortiAuthenticator.

```
<html>

  <head>

    <meta charset="UTF-8">

    <meta http-equiv="refresh" content="1;url=https://<FortiAuthenticator-FQDN>/saml-
sp/Okta/login/?user_continue_url=%%PROTURI%%&userip=%%USER_IP%%">

    <script type="text/javascript">
      window.location.href="https://<FortiAuthenticator-FQDN>/saml-sp/Okta/login/?user_
continue_url=%%PROTURI%%&userip=%%USER_IP%%"
    </script>

    <title>
      Page Redirection
      <title>

        <head>

          <body>
            If you are not redirected automatically,
            <a href="https://<FortiAuthenticator-FQDN>/saml-sp/Okta/login/?user_continue_
url=%%PROTURI%%&userip=%%USER_IP%%">
              login
            </a>

            <body>

              <html>
```

Configure address objects and policies

To configure addresses objects and policies on FortiGate:

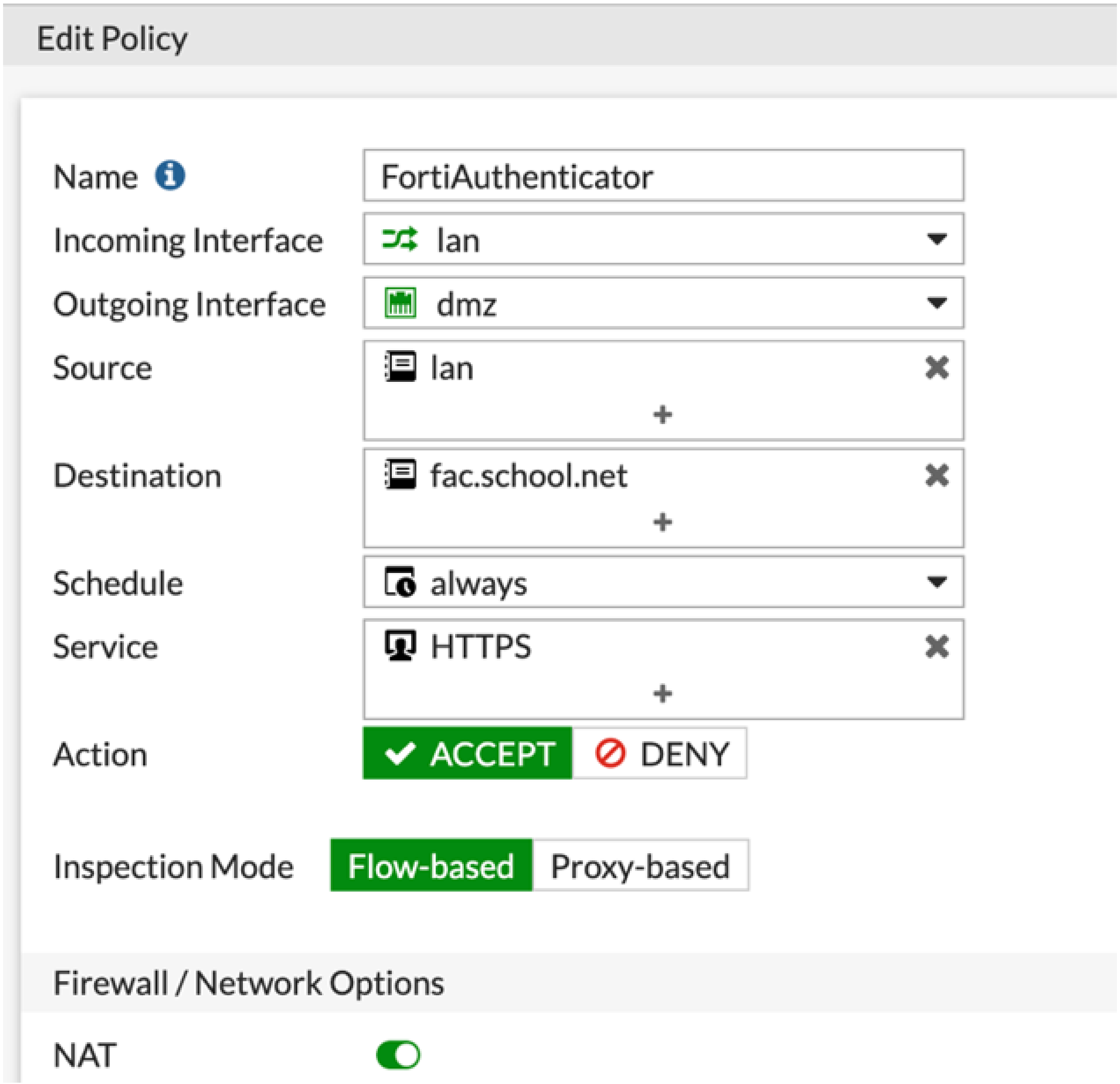
1. Go to *Policy & Objects* > *Addresses* and add the FortiAuthenticator as an address object.



Name	fac.school.net
Color	Change
Type	Subnet
IP/Netmask	192.168.50.100/32
Interface	dmz
Show in address list	●
Static route configuration	○
Comments	Write a comment... 0/255

2. Create the FQDN objects below.
   - *.okta.com
   - *.mtls.okta.com
   - *.oktapreview.com
   - *.mtls.oktapreview.com
   - *.oktacdn.com
   - *.okta-emea.com
   - *.mtls.okta-emea.com
   - *.kerberos.okta.com
   - *.kerberos.okta-emea.com
   - *.kerberos.oktapreview.com

   As these are FQDNs, make sure to set *Type* to *FQDN*.
3. Create an *Address group* and name it *Okta Bypass* and add the FQDNs you created above into the Okta Bypass address group.
4. Go to *Policy & Objects* > *IPv4 Policy* and create all policies shown in the examples below: a policy for DNS, for access to the FortiAuthenticator, for Okta bypass, and for FSSO including the SAML user group.
   Allow access to the FortiAuthenticator on the DMZ from the LAN:



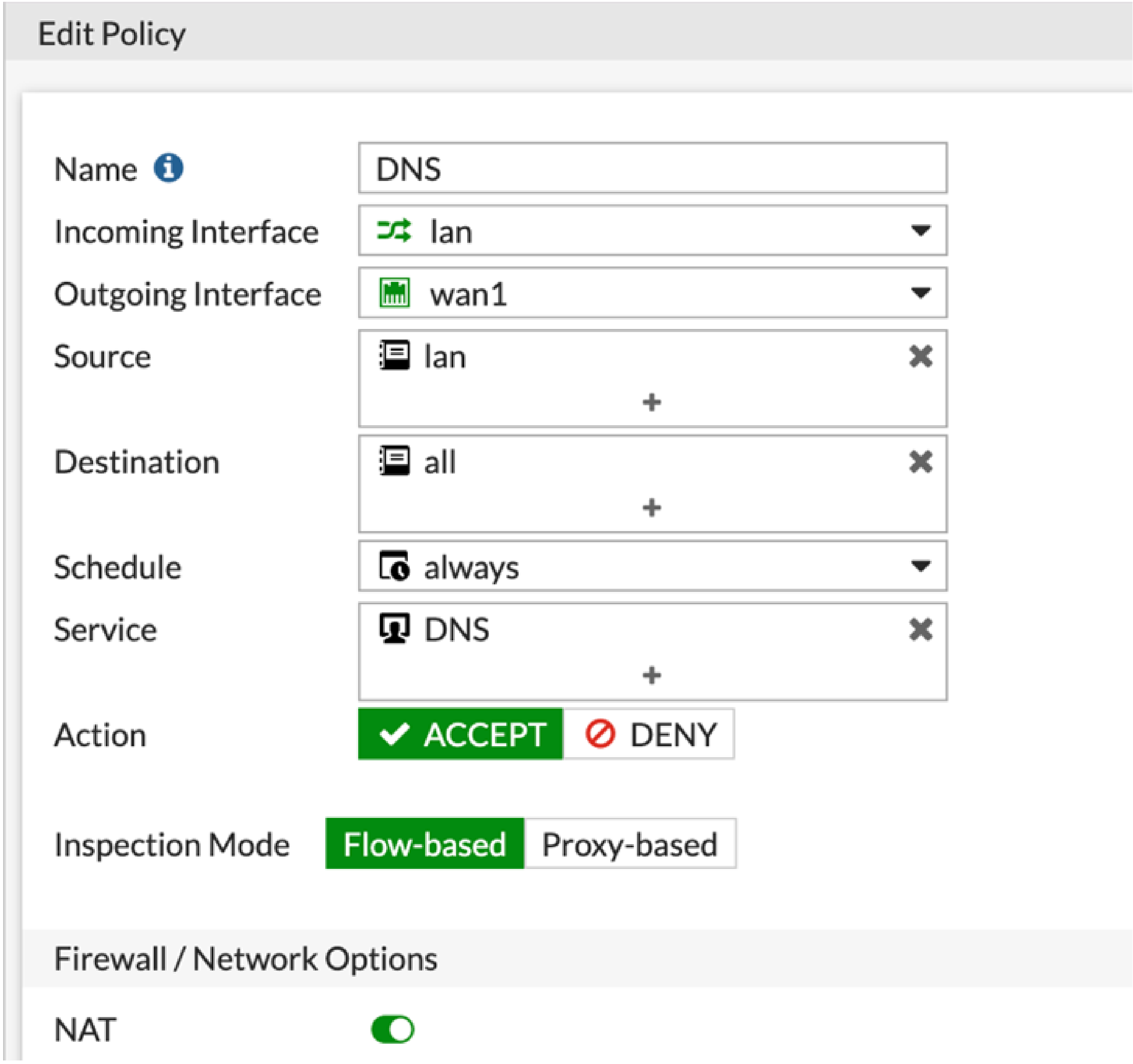
Edit Policy

Name	FortiAuthenticator
Incoming Interface	lan
Outgoing Interface	dmz
Source	lan
Destination	fac.school.net
Schedule	always
Service	HTTPS
Action	● ACCEPT ○ DENY
Inspection Mode	● Flow-based ○ Proxy-based

Firewall / Network Options

NAT	●

Add the following three policies in order:

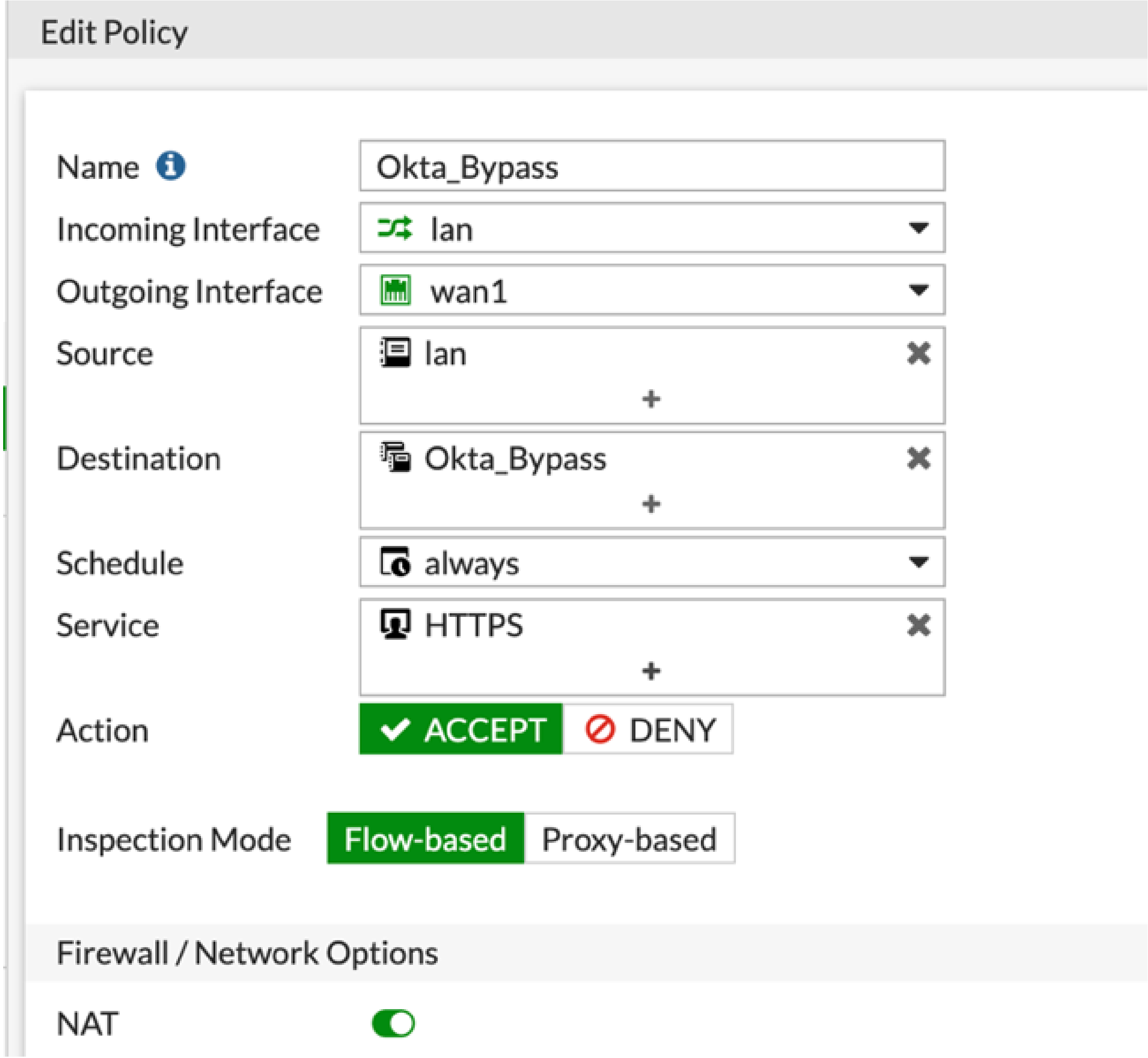


Edit Policy

Name	DNS
Incoming Interface	lan
Outgoing Interface	wan1
Source	lan
Destination	all
Schedule	always
Service	DNS
Action	✓ ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall / Network Options

NAT ●



Edit Policy

Name: Okta_Bypass

Incoming Interface: lan

Outgoing Interface: wan1

Source: lan

Destination: Okta_Bypass

Schedule: always

Service: HTTPS

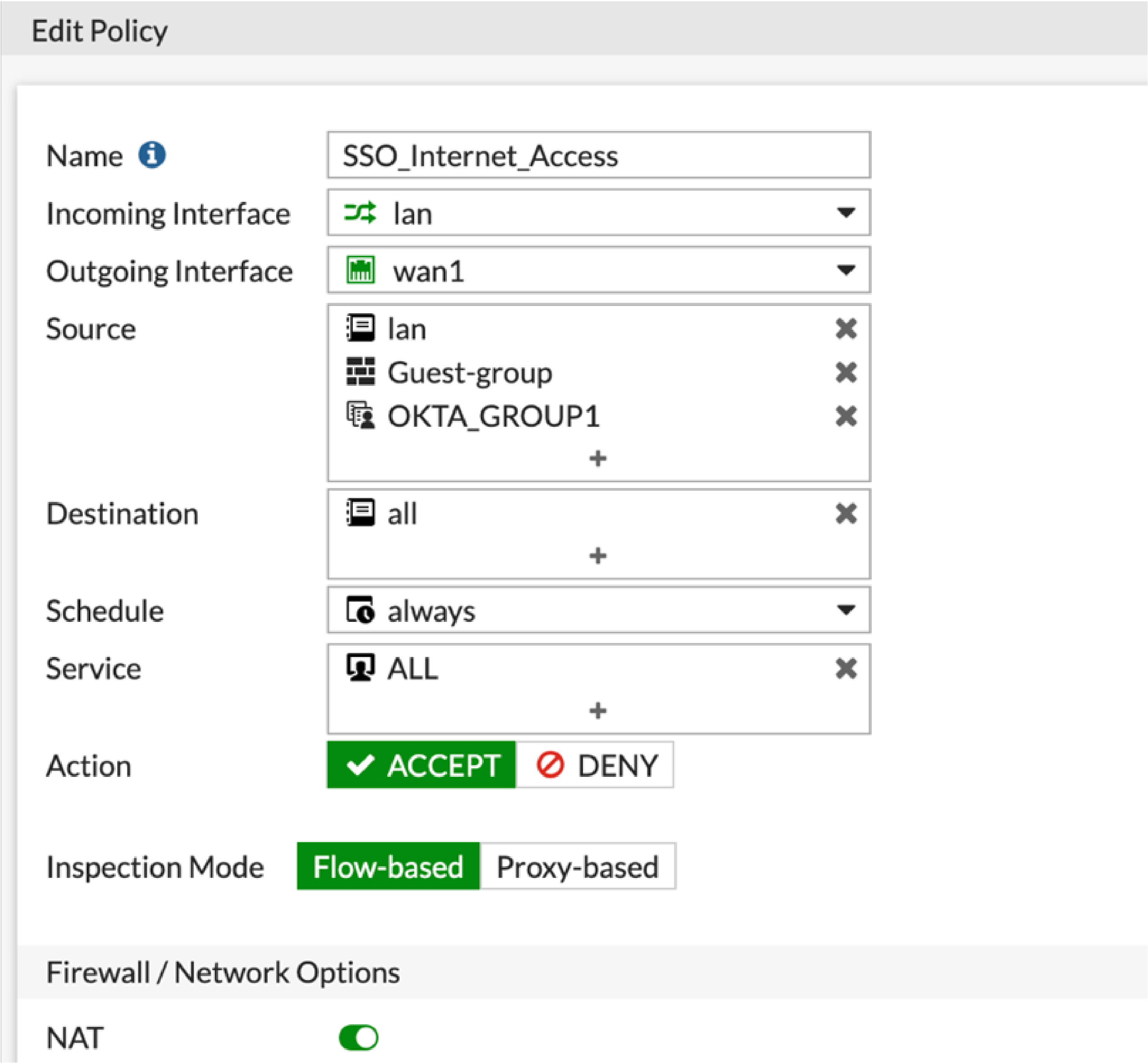
Action: ✓ ACCEPT | DENY

Inspection Mode: Flow-based | Proxy-based

Firewall / Network Options

NAT: ●

In the *SSO_Internet_Access* policy, add the Firewall *Guest-group* and the Okta FSSO group that is received from FortiAuthenticator. The Guest-group redirects the initial Internet access request from the browser to Okta. Once the user is authenticated the browser will automatically redirect to the website from the initial HTTP/HTTPS request matching the Okta SSO group.



Edit Policy

Name: SSO_Internet_Access

Incoming Interface: lan

Outgoing Interface: wan1

Source: lan, Guest-group, OKTA_GROUP1

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT (selected) | DENY

Inspection Mode: Flow-based (selected) | Proxy-based

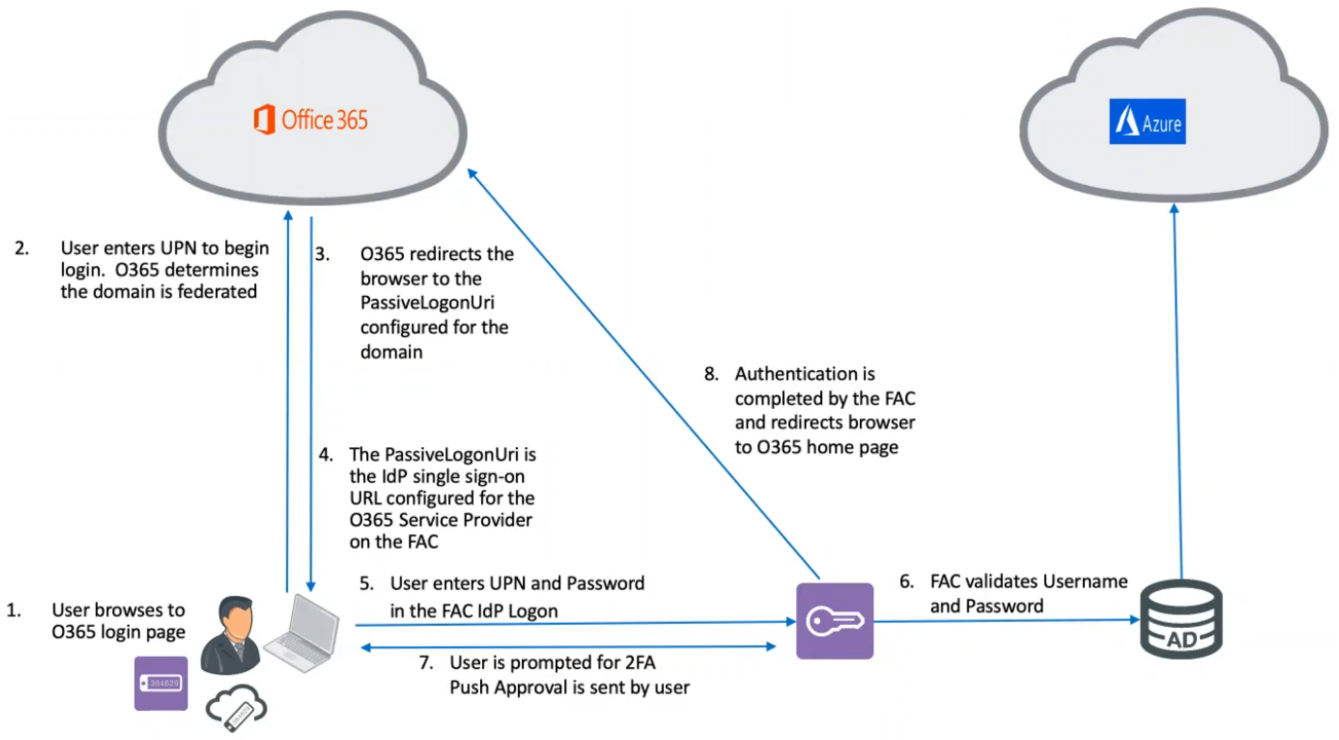
Firewall / Network Options

NAT: ●

Office 365 SAML authentication using FortiAuthenticator with 2FA

FortiAuthenticator can act as the SAML IdP for an Office 365 SP using FortiToken served directly by FortiAuthenticator or from FortiToken Cloud for two-factor authentication.

The configuration outlined in this guide assumes that you have already configured your FortiAuthenticator with FortiToken Cloud. For more information on how to do this, please see the FortiAuthenticator Administration Guide.


Office 365
Azure
2. User enters UPN to begin login. O365 determines the domain is federated
3. O365 redirects the browser to the PassiveLogonUri configured for the domain
4. The PassiveLogonUri is the IdP single sign-on URL configured for the O365 Service Provider on the FAC
8. Authentication is completed by the FAC and redirects browser to O365 home page
1. User browses to O365 login page
5. User enters UPN and Password in the FAC IdP Logon
6. FAC validates Username and Password
7. User is prompted for 2FA Push Approval is sent by user
AD

To configure Office 365 SAML authentication using FortiAuthenticator with two-factor authentication:

1. Configure the remote LDAP server on FortiAuthenticator on page 176
2. Configure SAML settings on FortiAuthenticator on page 177
3. Configure two-factor authentication on FortiAuthenticator on page 178
4. Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 179
5. Configure Microsoft Azure AD Connect on page 181

Configure the remote LDAP server on FortiAuthenticator

To configure the LDAP server:

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP* and click *Create New*.
2. Configure the following settings:
   a. **Name**: Provide a name for the remote LDAP server.
   b. **Primary server name/IP**: Enter the IP address for the AD (Active Directory) source.
   c. **Base distinguished name**: Configure the based distinguished name for your AD source.
   d. **Bind type**: Select *Regular*.
   e. **Username/Password**: Enter the username and password for your AD source.
   The remaining settings can be left in their default state.
3. Click *OK* to save your changes.

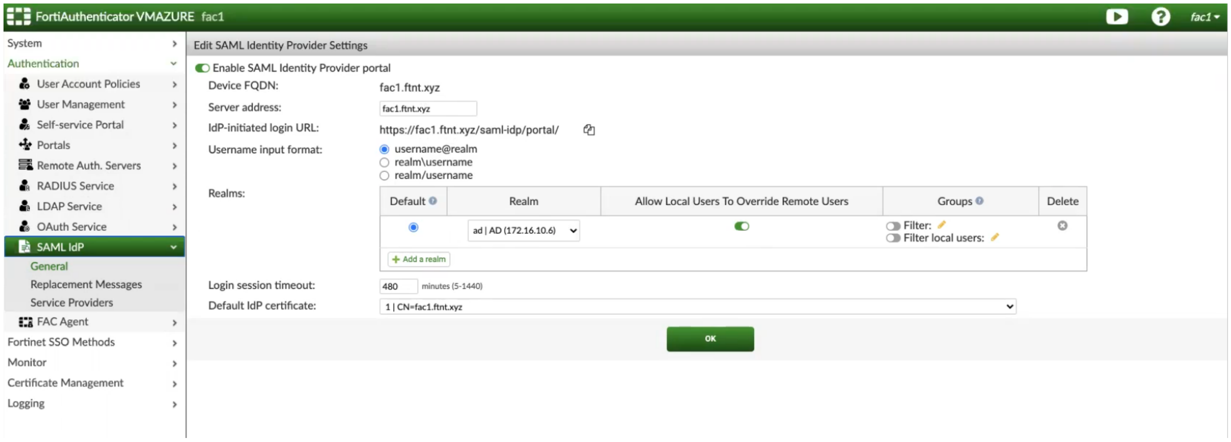
To configure the Active Directory realm:

1. Go to *Authentication* > *User Management* > *Realms* and click *Create New*.
2. Configure a name for the realm and select your LDAP server as the *User source*.
3. Click *OK* to save your changes.

Configure SAML settings on FortiAuthenticator

To configure FortiAuthenticator IdP settings:

1. Go to *Authentication* > *SAML IdP* > *General* and click *Enable SAML Identity Provider portal*.
2. Configure the following settings:
    a. **Server address**: The IP address or FQDN of the FortiAuthenticator.
    b. **Realms**: Select the previously created LDAP realm.
    c. **Default IdP certificate**: Choose a certificate. The default can be used if desired.
    The remaining settings can be left in their default state.



Edit SAML Identity Provider Settings

Enable SAML Identity Provider portal

Device FQDN: fac1.ftnt.xyz

Server address: fac1.ftnt.xyz

IdP-initiated login URL: https://fac1.ftnt.xyz/saml-idp/portal/

Username input format:
● username@realm
○ realm\username
○ realm/username

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	ad | AD (172.16.10.6)	✓	Filter: Filter local users:	⊗

+ Add a realm

Login session timeout: 480 minutes (5-1440)

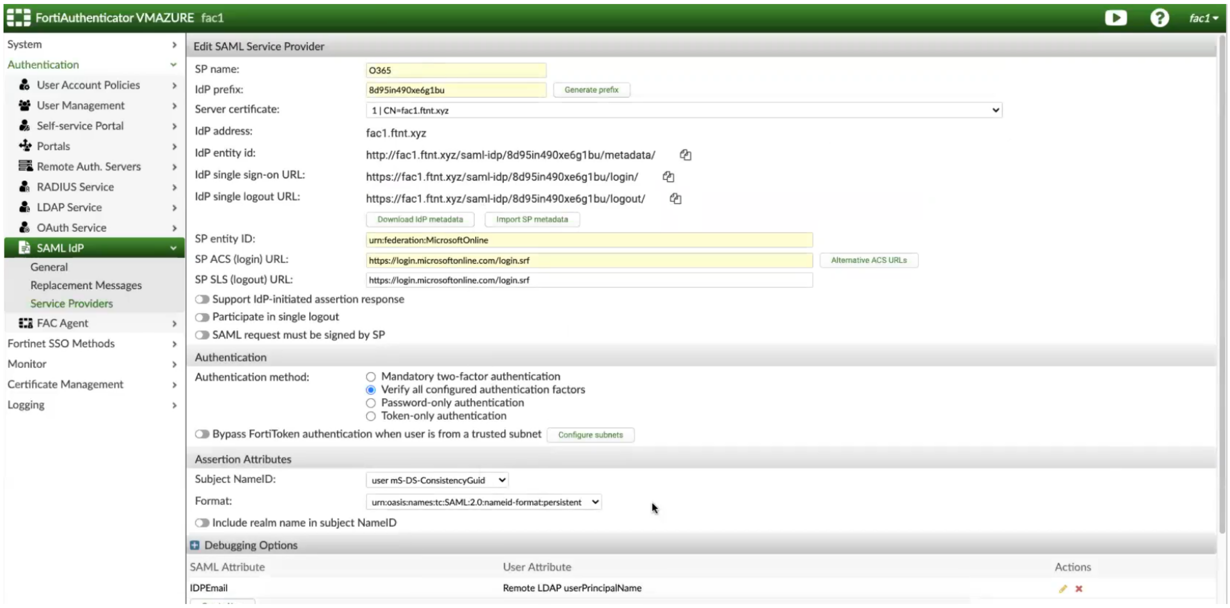
Default IdP certificate: 1 | CN=fac1.ftnt.xyz

3. Click *OK* to save your changes.

To configure the service provider settings on FortiAuthenticator:

1. Go to *Authentication* > *SAML IdP* > *Service Providers* and click *Create New*.
2. Configure the following settings:
    a. **SP Name**: enter a name for your service provider.
    b. **IdP Prefix**: Click *Generate prefix* to create a new IdP prefix.
    c. **Server certificate**: Select the certificate to be used in your configuration or choose *Use default setting in SAML IdP General page*.
    d. **SP entity ID**: Enter `urn:federation:MicrosoftOnline`.
    e. **SP ACS (login) URL**: Enter `https://login.microsoftonline.com/login.srf`.
    f. **SP SLS (logout) URL**: Enter `https://login.microsoftonline.com/login.srf`.
    g. **Participate in single logout**: Can be enabled if you wish this SP to participate in SAML single logout.
3. In the *Assertion Attributes* section, configure the following settings:
    a. **Subject NameID**: Select *user mS-DS-Consistency Guid*.
    b. **Format**: Select *urn:oasis:names:tc:SAML:2.0:nameid-format:persistent*.
    Press `Enter` and then SAML attributes can be created.

4. In the *Debugging Options* section click *Create New* to create a SAML attribute with the following settings:
   - a. **SAML attribute**: Enter `IDPEmail`.
   - b. **User attribute**: In the dropdown, select *userPrincipalName* under *Remote LDAP server*.



Edit SAML Service Provider

SP name: O365
IdP prefix: 8d95in490xe6g1bu
Server certificate: 1 | CN=fac1.ftnt.xyz
IdP address: fac1.ftnt.xyz
IdP entity id: http://fac1.ftnt.xyz/saml-idp/8d95in490xe6g1bu/metadata/
IdP single sign-on URL: https://fac1.ftnt.xyz/saml-idp/8d95in490xe6g1bu/login/
IdP single logout URL: https://fac1.ftnt.xyz/saml-idp/8d95in490xe6g1bu/logout/
SP entity ID: urn:federation:MicrosoftOnline
SP ACS (login) URL: https://login.microsoftonline.com/login.srf
SP SLS (logout) URL: https://login.microsoftonline.com/login.srf
Support IdP-initiated assertion response
Participate in single logout
SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory two-factor authentication
● Verify all configured authentication factors
○ Password-only authentication
○ Token-only authentication

Bypass FortiToken authentication when user is from a trusted subnet

Assertion Attributes

Subject NameID: user mS-DS-ConsistencyGuid
Format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
Include realm name in subject NameID

Debugging Options

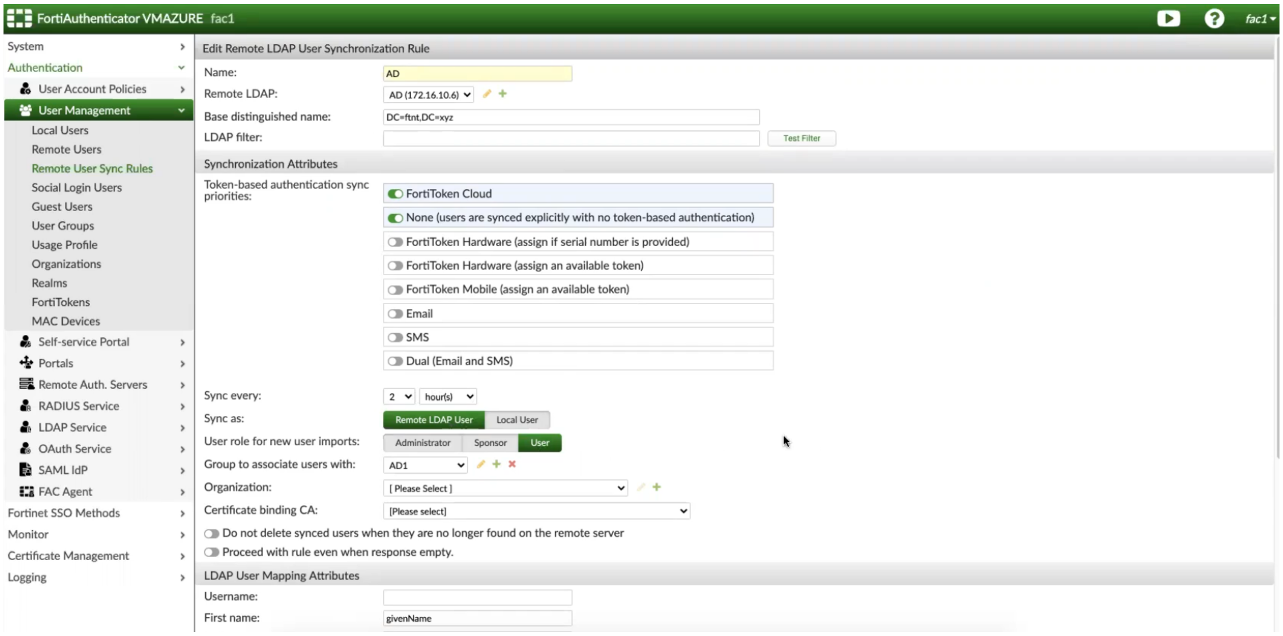
SAML Attribute	User Attribute	Actions
IDPEmail	Remote LDAP userPrincipalName	✎ ✖

5. Click *OK* to save your changes.

Configure two-factor authentication on FortiAuthenticator

To configure a remote user sync rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rules*, and click *Create New*.
2. Configure the following settings:
   - a. **Name**: Enter a name for the sync rule (e.g. AD).
   - b. **Remote LDAP**: Select your remote LDAP server.
3. Configure the token-based sync priority settings under *Synchronization Attributes* by enabling and ordering the authentication sync priorities.
   This example scenario uses FortiToken Cloud for two-factor authentication, so the priority is *FortiToken Cloud* followed by *None (users are synced explicitly with no token-based authentication)*.



Edit Remote LDAP User Synchronization Rule

Name: AD

Remote LDAP: AD (172.16.10.6)

Base distinguished name: DC=ftnt,DC=xyz

LDAP filter:

Synchronization Attributes

Token-based authentication sync priorities:

- ● FortiToken Cloud
- ● None (users are synced explicitly with no token-based authentication)
- ○ FortiToken Hardware (assign if serial number is provided)
- ○ FortiToken Hardware (assign an available token)
- ○ FortiToken Mobile (assign an available token)
- ○ Email
- ○ SMS
- ○ Dual (Email and SMS)

Sync every: 2 hour(s)

Sync as: [✓ Remote LDAP User] Local User

User role for new user imports: Administrator Sponsor [✓ User]

Group to associate users with: AD1

Organization: [Please Select]

Certificate binding CA: [Please select]

○ Do not delete synced users when they are no longer found on the remote server

○ Proceed with rule even when response empty.

LDAP User Mapping Attributes

Username:

First name: givenName

4. Select or create a user group to associate users with from the dropdown menu.
5. The remaining settings can be configured to your preference or left in their default state.
6. Click *OK* to save your changes when completed.

To configure remote users with two-factor authentication:

1. Go to *Authentication* > *User Management* > *Remote Users* and *Import* users from your Active Directory account.
2. Edit a user and enable *Token-based authentication*, and select *FortiToken* > *Cloud* as the delivery method.
3. Click *OK* to save your changes.

Configure the domain and SAML SP in Microsoft Azure AD PowerShell

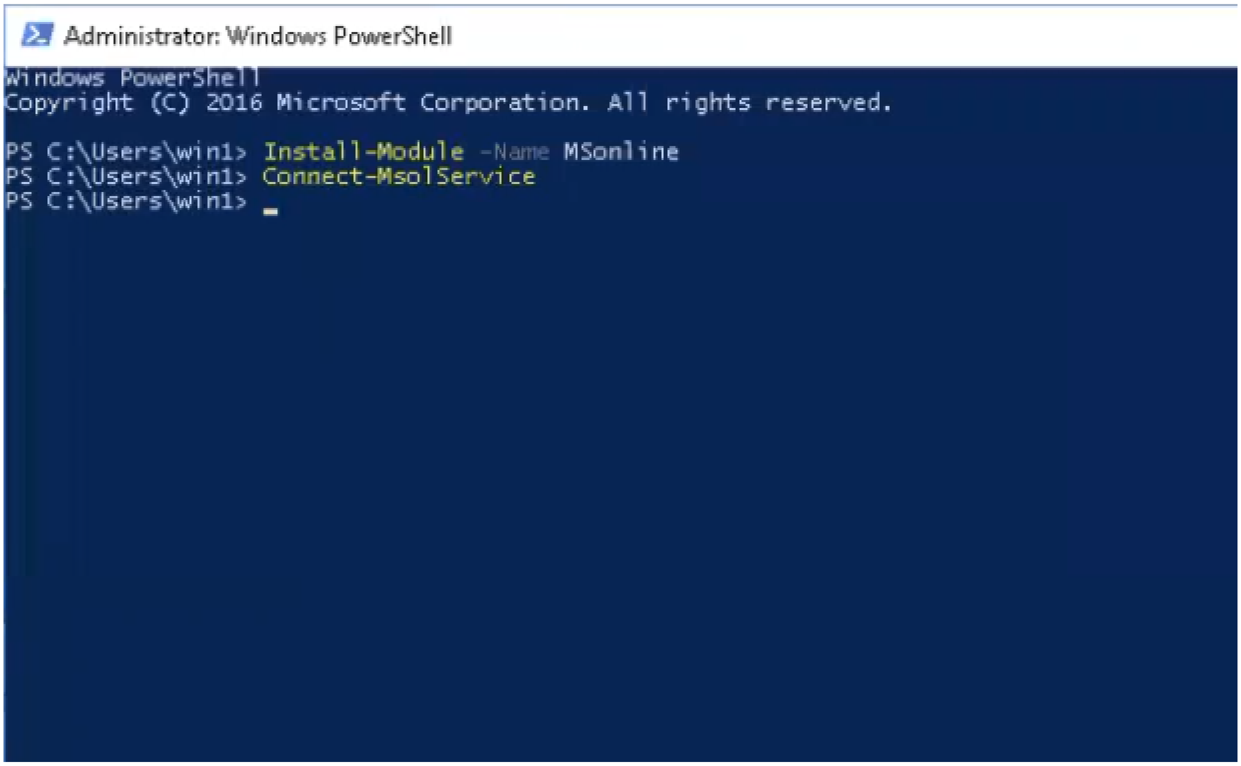
FortiAuthenticator currently supports use with Microsoft Azure Active Directory Module for Windows PowerShell.

To configure the domain and SAML SP using Microsoft Azure AD PowerShell:

1. Launch the Microsoft Azure Active Directory Module for Windows PowerShell.
2. Enter the following command in PowerShell:
   ```
   Install-Module -Name MSonline.
   ```
   Accept the next two default ("Y") prompts for installing the NuGet Provider and installing from PSGallery.

   1. If you are using Windows 2016 or earlier, you must first enable TLS 1.2 enforcement for Azure AD Connect. For instructions on enabling TLS 1.2 eforcement, see Azure AD Connect: TLS 1.2 enforcement for Azure Active Directory Connect.

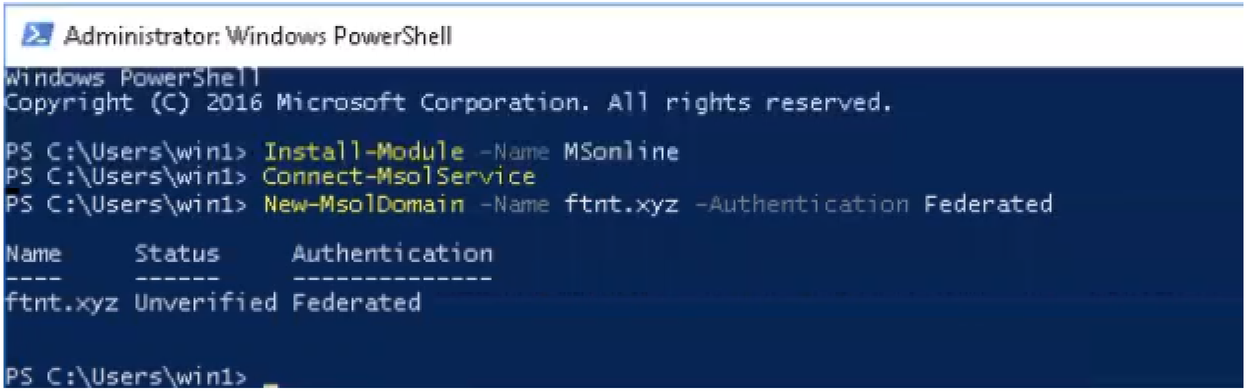
3. Enter the following command:
   ```
   Connect-MsolService .
   ```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\win1> Install-Module -Name MSonline
PS C:\Users\win1> Connect-MsolService
PS C:\Users\win1> _
```

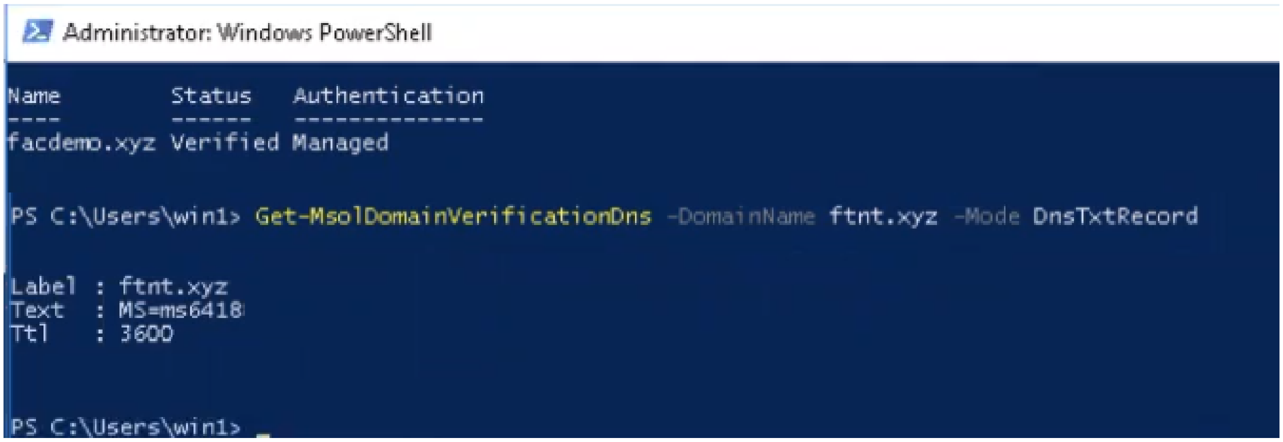
The Microsoft Sign in window opens. Login with your Azure ID.

4. Add a federated domain by entering the following command.
`New-MsolDomain -Name <your domain> -Authentication Federated`



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\win1> Install-Module -Name MSonline
PS C:\Users\win1> Connect-MsolService
PS C:\Users\win1> New-MsolDomain -Name ftnt.xyz -Authentication Federated

Name     Status     Authentication
----     ------     --------------
ftnt.xyz Unverified Federated


PS C:\Users\win1> _
```

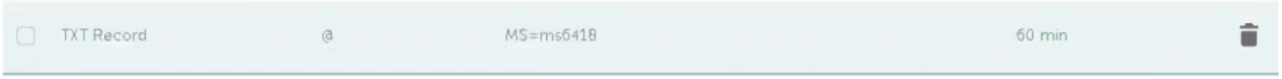
5. Obtain the DNS record and create a new text record in your domain provider to allow the domain to be verified. To obtain the DNS record, use the following command:
`Get-MsolDomainVerificationDns -DomainName ftnt.xyz -Mode DnsTxtRecord`



Administrator: Windows PowerShell

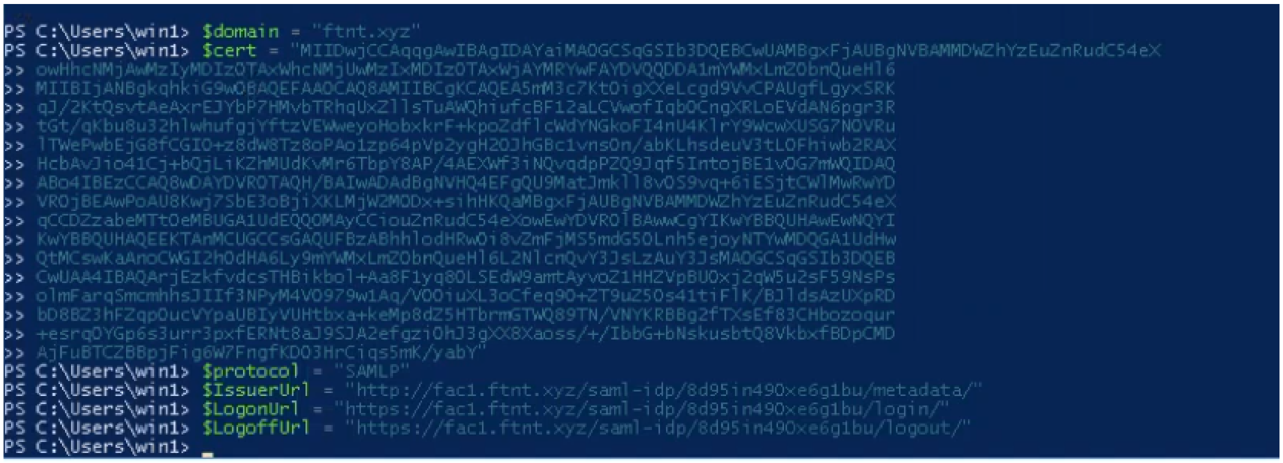
```
Name        Status   Authentication
----        ------   --------------
facdemo.xyz Verified Managed

PS C:\Users\win1> Get-MsolDomainVerificationDns -DomainName ftnt.xyz -Mode DnsTxtRecord

Label : ftnt.xyz
Text  : MS=ms6418
Ttl   : 3600

PS C:\Users\win1> _
```

From the output, copy the *Text* field results and create a new text record in your domain with a 60 minute interval.



□ TXT Record	@	MS=ms6418	60 min

6. Configure the domain as a SAML service provider.
   You can create these variables inside a text editor and then copy and paste them into a PowerShell window.
   `$domain = "`*`<your domain>`*`"`
   `$cert = "`*`<your certificate. This can be obtained by downloading your certificate from FortiAuthenticator and opening it with a text editor.>`*`"`
   `$protocol = "SAMLP"`
   `$IssuerUrl = "`*`<The IdP entity ID from FortiAuthenticator>`*`"`
   `$LogonUrl = "`*`<The IdP single sign-on URL from FortiAuthenticator>`*`"`
   `$LogoffUrl = "`*`<The IdP single logout URL from FortiAuthenticator>`*`"`



```
PS C:\Users\win1> $domain = "ftnt.xyz"
PS C:\Users\win1> $cert = "MIIDwjCCAqqgAwIBAgIDAYaiMA0GCSqGSIb3DQEBCwUAMBgxFjAUBgNVBAMMDWZhYzEuZnRudC54eX
>> owHhcNMjAwMzIyMDIzOTAxWhcNMjUwMzIxMDIzOTAxWjAYMRYwFAYDVQQDDA1mYWMxLmZ0bnQueHl6
>> MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5mM3c7KtOigXXeLcgd9VvCPAUgfLgyxSRK
>> qJ/2KtQsvtAeAxrEJYbP7HMvbTRhqUxZllsTuAWQhiufcBF12aLCVwofIqbOCngXRLoEVdAN6pgr3R
>> tGt/qKbu8u32hlwhufgjYftzVEWweyoHobxkrF+kpoZdflcWdYNGkoFI4nU4KlrY9WcwXUSG7NOVRu
>> lTWePwbEjG8fCGIO+z8dW8Tz8oPAo1zp64pVp2ygH2OJhGBc1vnsOn/abKLhsdeuV3tLOFhiwb2RAX
>> HcbAvJio41Cj+bQjLiKZhMUdKvMr6TbpY8AP/4AEXWf3iNQvqdpPZQ9Jqf5IntojBE1vOG7mWQIDAQ
>> ABo4IBEzCCAQ8wDAYDVROTAQH/BAIwADAdBgNVHQ4EFgQU9MatJmkll8vOS9vq+6iESjtCWlMwRwYD
>> VROjBEAwPoAU8Kwj7SbE3oBjiXKLMjW2MODx+sihHKQaMBgxFjAUBgNVBAMMDWZhYzEuZnRudC54eX
>> qCCDZzabeMTtOeMBUGA1UdEQQOMAyCCiouZnRudC54eXowEwYDVROlBAwwCgYIKwYBBQUHAwEwNQYI
>> KwYBBQUHAQEEKTAnMCUGCCsGAQUFBzABhhlodHRwOi8vZmFjMS5mdG5OLnh5ejoyNTYwMDQGA1UdHw
>> QtMCswKaAnoCWGI2hOdHA6Ly9mYWMxLmZObnQueHl6L2NlcnQvY3JsLzAuY3JsMAOGCSqGSIb3DQEB
>> CwUAA4IBAQArjEzkfvdcsTHBikbol+Aa8F1yq8OLSEdW9amtAyvoZ1HHZVpBUOxj2qW5u2sF59NsPs
>> olmFarqSmcmhhsJIIf3NPyM4VO979w1Aq/VOOiuXL3oCfeq9O+ZT9uZ5Os41tiFlK/BJldsAzUXpRD
>> bD8BZ3hFZqpOucVYpaUBIyVUHtbxa+keMp8dZ5HTbrmGTWQ89TN/VNYKRBBg2fTXsEf83CHbozoqur
>> +esrqOYGp6s3urr3pxfERNt8aJ9SJA2efgziOhJ3gXX8Xaoss/+/IbbG+bNskusbtQ8VkbxfBDpCMD
>> AjFuBTCZBBpjFig6W7FngfKDO3HrCiqs5mK/yabY"
PS C:\Users\win1> $protocol = "SAMLP"
PS C:\Users\win1> $IssuerUrl = "http://fac1.ftnt.xyz/saml-idp/8d95in490xe6g1bu/metadata/"
PS C:\Users\win1> $LogonUrl = "https://fac1.ftnt.xyz/saml-idp/8d95in490xe6g1bu/login/"
PS C:\Users\win1> $LogoffUrl = "https://fac1.ftnt.xyz/saml-idp/8d95in490xe6g1bu/logout/"
PS C:\Users\win1> _
```

   Once completed, enter the following command into PowerShell to verify the domain:

```
Confirm-MsolDomain -DomainName $domain -SigningCertificate $cert -
PreferredAuthenticationProtocol $protocol -IssuerUri $IssuerUrl -PassiveLogOnUri
$LogonURL -LogOffUri $LogOffUrl
```

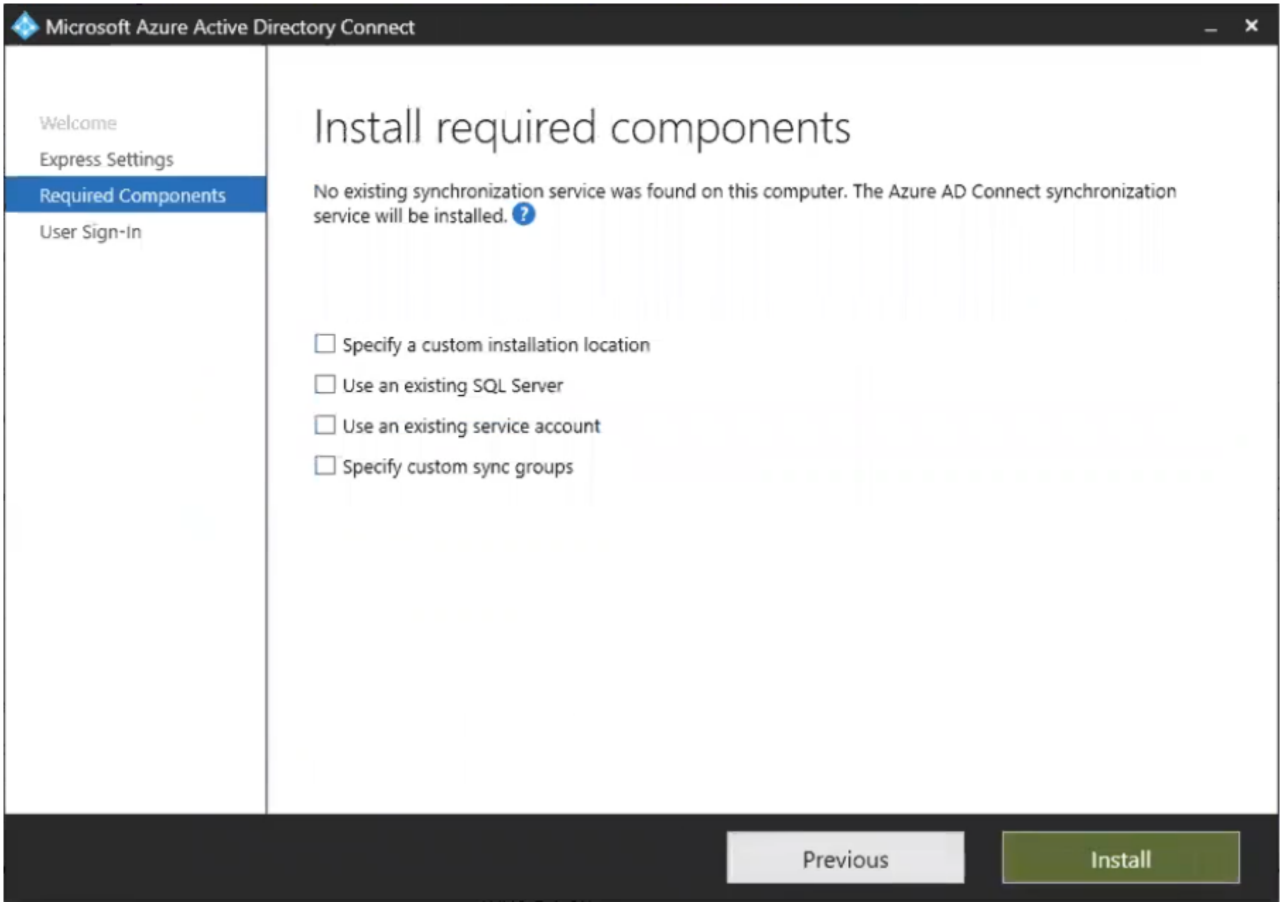
   The return text from the above command should read "AvailableImmediately The domain has been successfully verified for your account."

Configure Microsoft Azure AD Connect

You will first need to download Azure AD Connect from Microsoft on your Active Directory Domain Controller.

To configure Microsoft Azure AD Connect:

1. Launch Microsoft Azure Active Directory Connect to create a synchronization service to sync attributes from Active Directory to Office365.
2. Select *Customize* to begin a customized installation, and click *Install*.



Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.

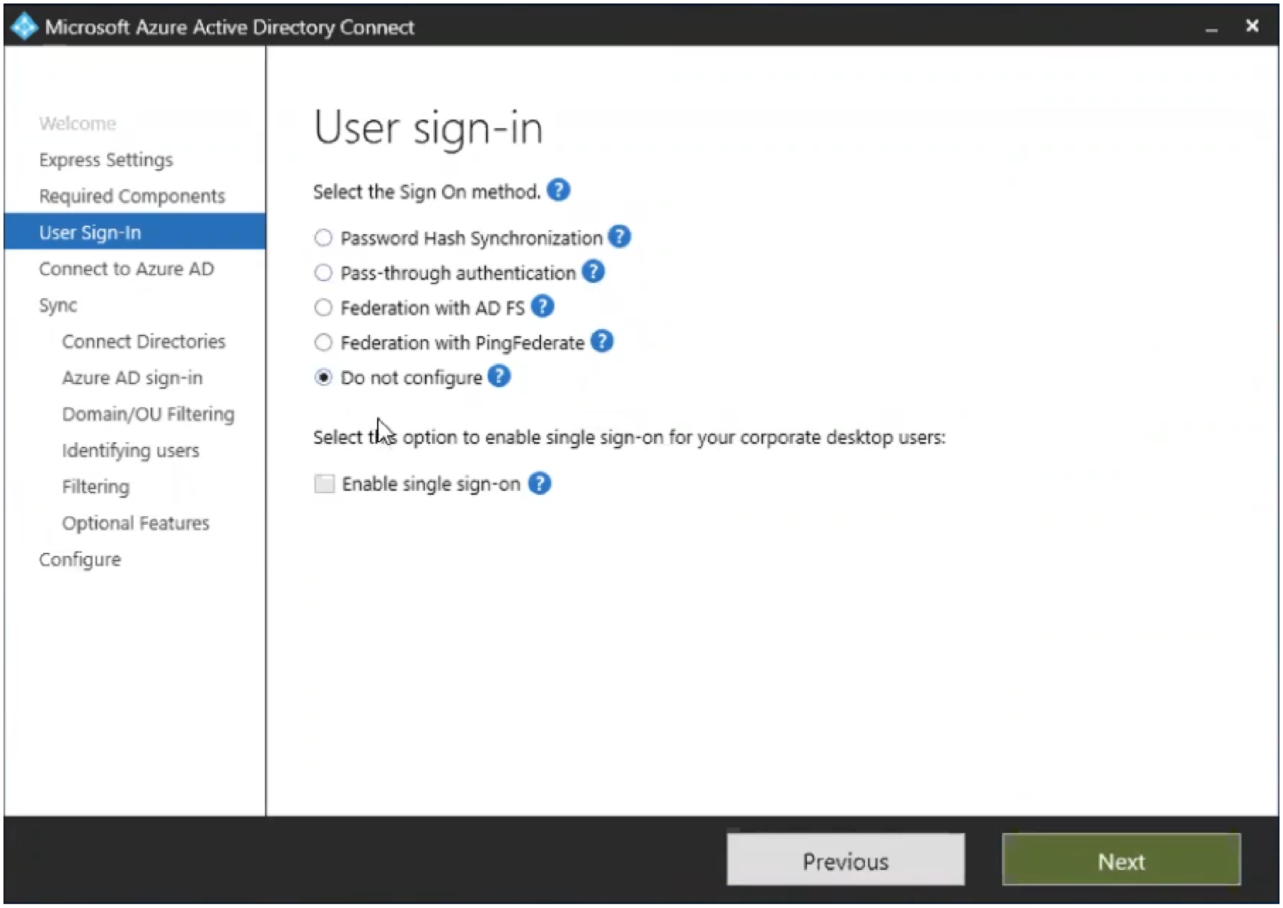
□ Specify a custom installation location

□ Use an existing SQL Server

□ Use an existing service account

□ Specify custom sync groups

3. On the *User sign-in* page, select *Do not configure*, and click *Next*.



Microsoft Azure Active Directory Connect

User sign-in

Select the Sign On method.

○ Password Hash Synchronization

○ Pass-through authentication

○ Federation with AD FS

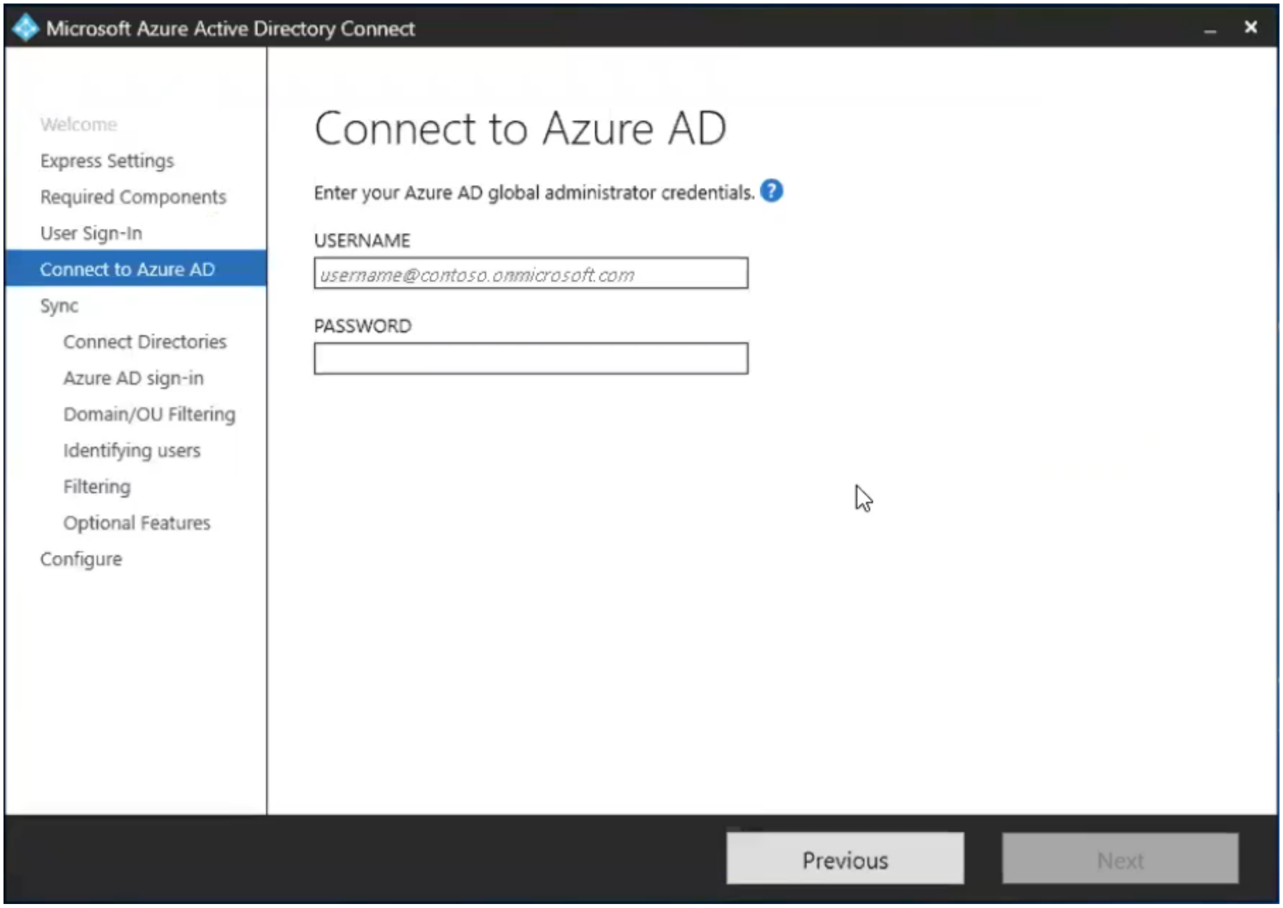
○ Federation with PingFederate

● Do not configure

Select this option to enable single sign-on for your corporate desktop users:

□ Enable single sign-on

4. On the *Connect to Azure AD* page, enter your Azure AD global administrator credentials, and click *Next*.



Connect to Azure AD

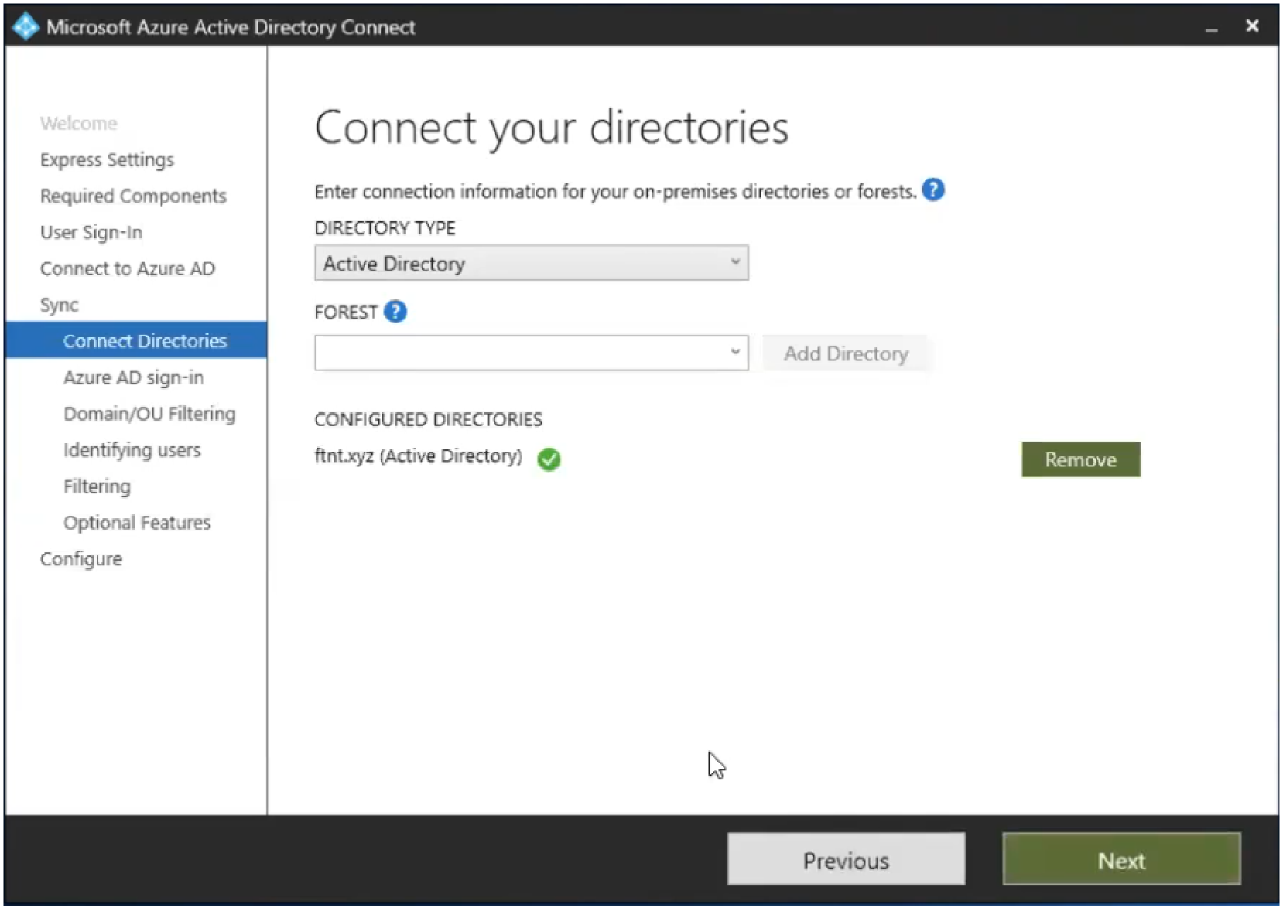
Enter your Azure AD global administrator credentials.

USERNAME

username@contoso.onmicrosoft.com

PASSWORD

5. Select your Active Directory Forest, and click *Add Directory*. Create your on-premise AD admin user account.



Connect your directories

Enter connection information for your on-premises directories or forests.

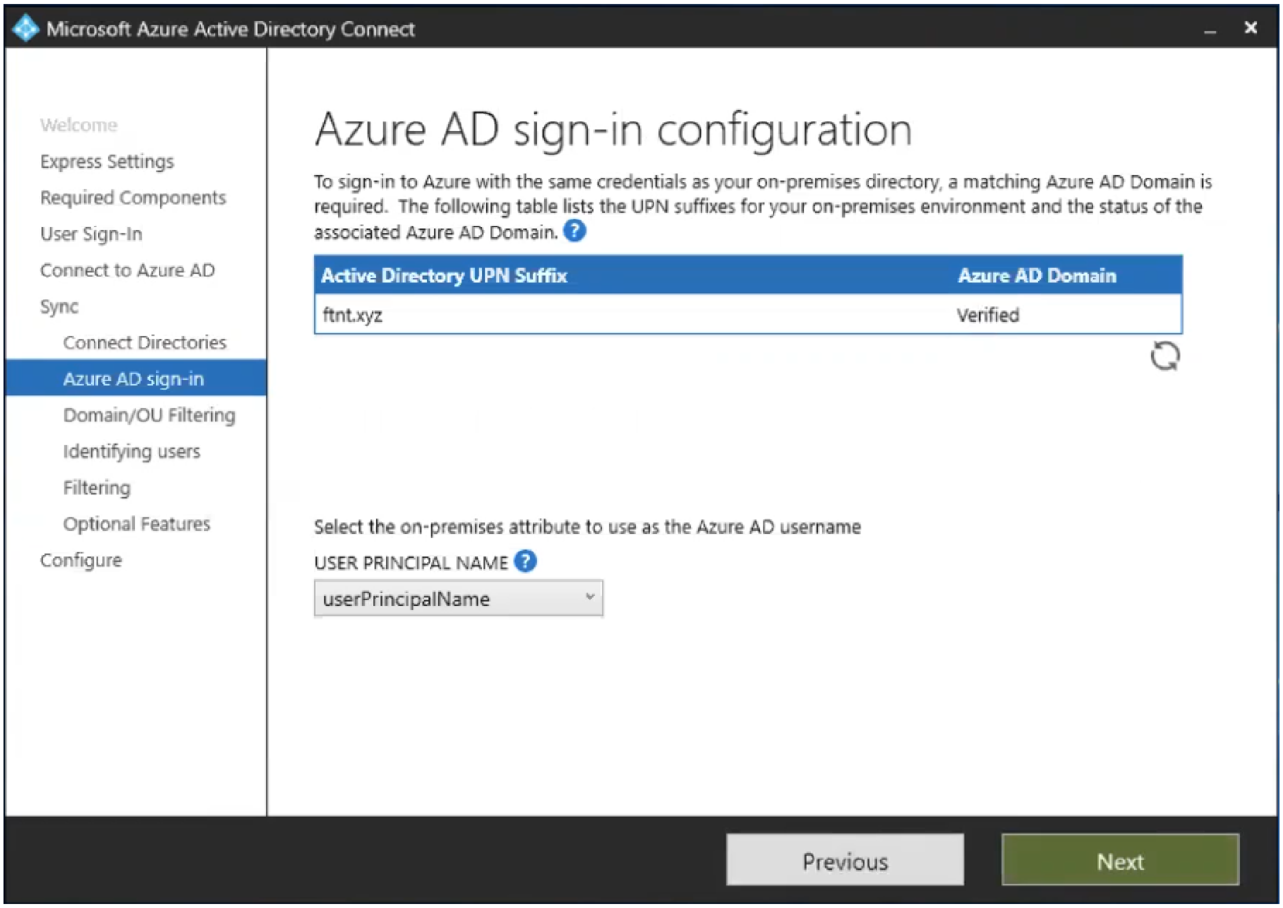
DIRECTORY TYPE: Active Directory

FOREST:

CONFIGURED DIRECTORIES

ftnt.xyz (Active Directory) ✓

When finished, click *Next*. If completed successfully, you will see your domain has been verified.
Click *Next* again.



Azure AD sign-in configuration

To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain.

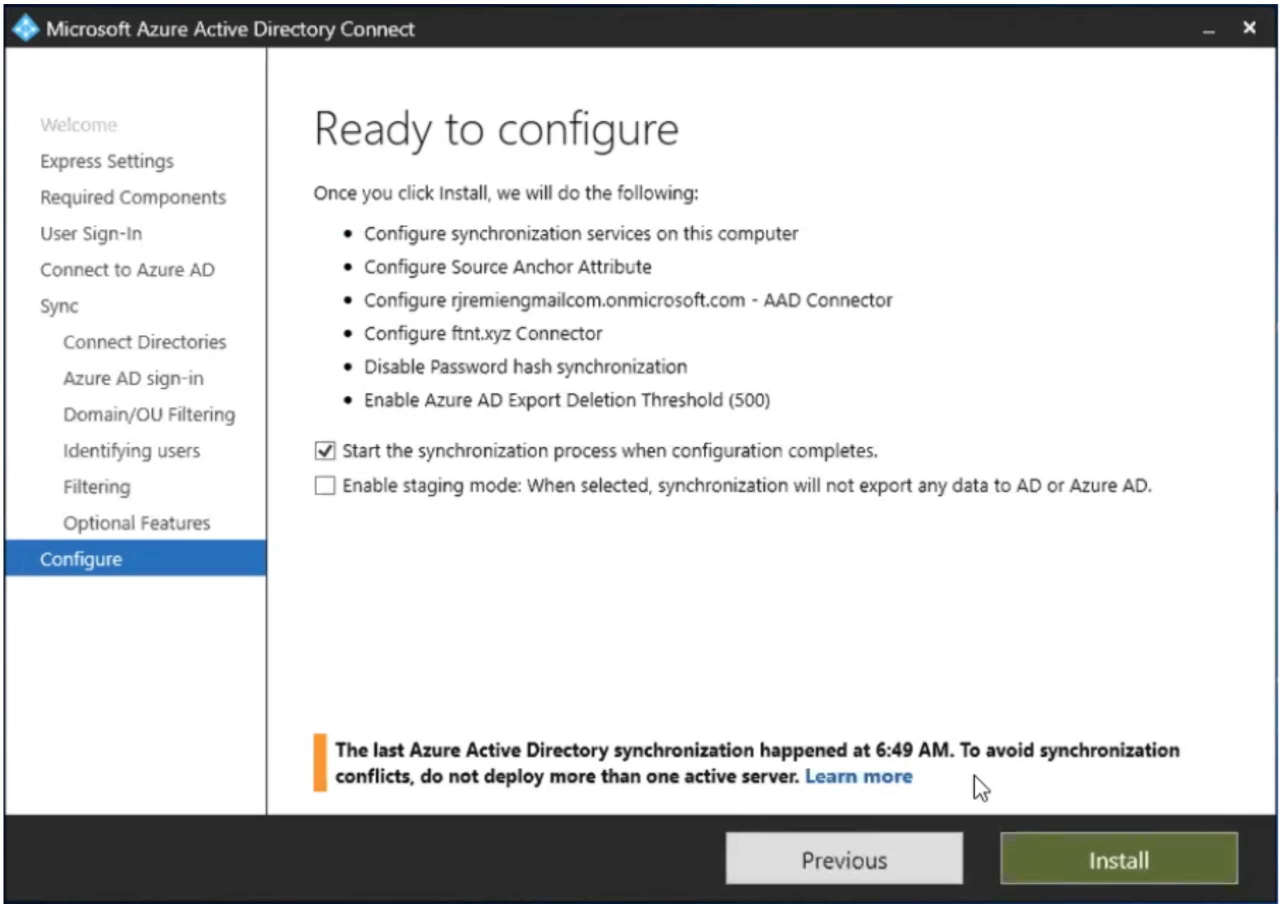
Active Directory UPN Suffix	Azure AD Domain
ftnt.xyz	Verified

Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME

userPrincipalName

6. Click *Next* on the remaining pages in the configuration wizard, and click *Install* on the *Ready to configure* page.



Ready to configure

Once you click Install, we will do the following:

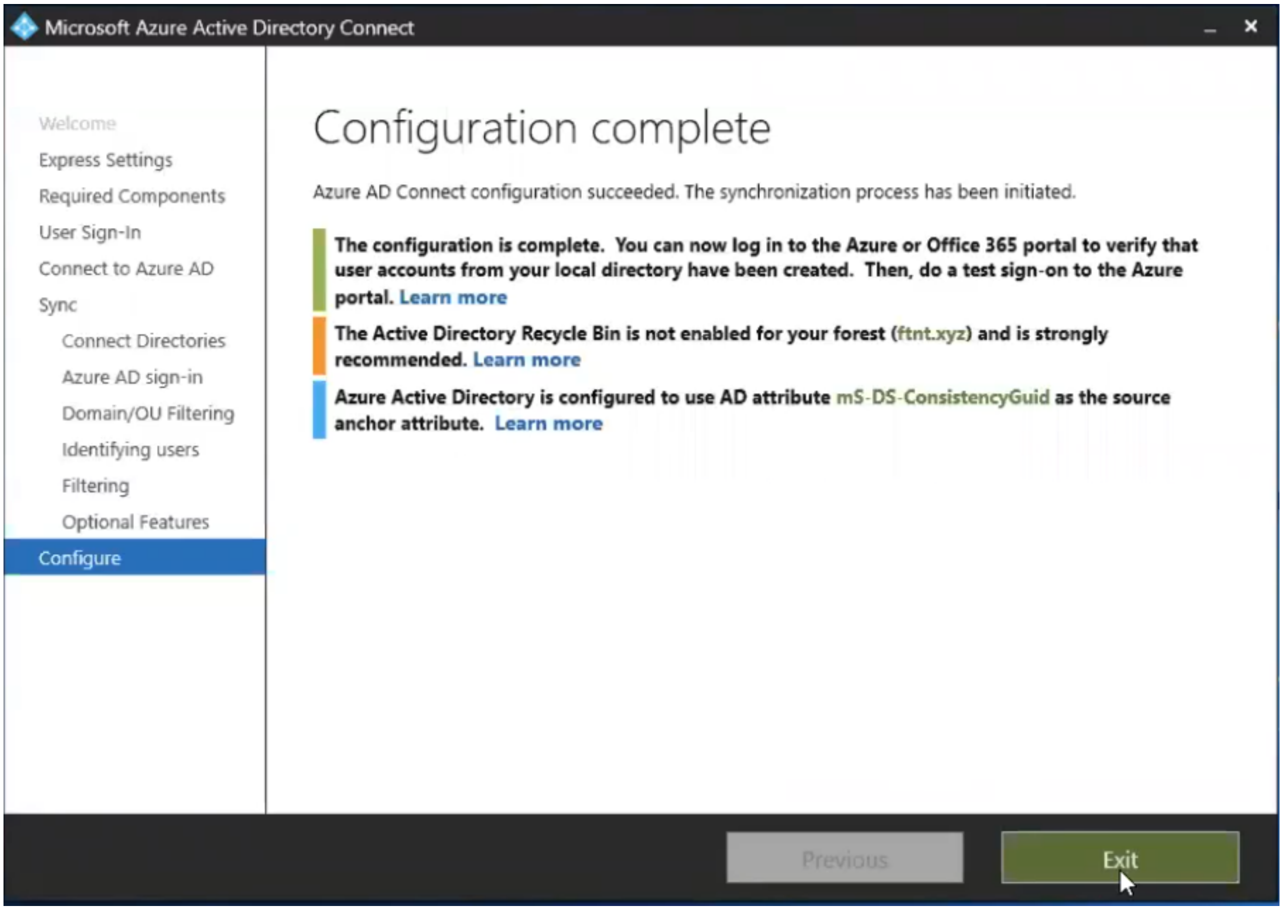
- Configure synchronization services on this computer
- Configure Source Anchor Attribute
- Configure rjremiengmailcom.onmicrosoft.com - AAD Connector
- Configure ftnt.xyz Connector
- Disable Password hash synchronization
- Enable Azure AD Export Deletion Threshold (500)

☑ Start the synchronization process when configuration completes.

□ Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

The last Azure Active Directory synchronization happened at 6:49 AM. To avoid synchronization conflicts, do not deploy more than one active server. Learn more

7. Once the installation is complete, you are presented with the Configuration complete page which provides a summary of the configuration changes.



Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more

The Active Directory Recycle Bin is not enabled for your forest (ftnt.xyz) and is strongly recommended. Learn more

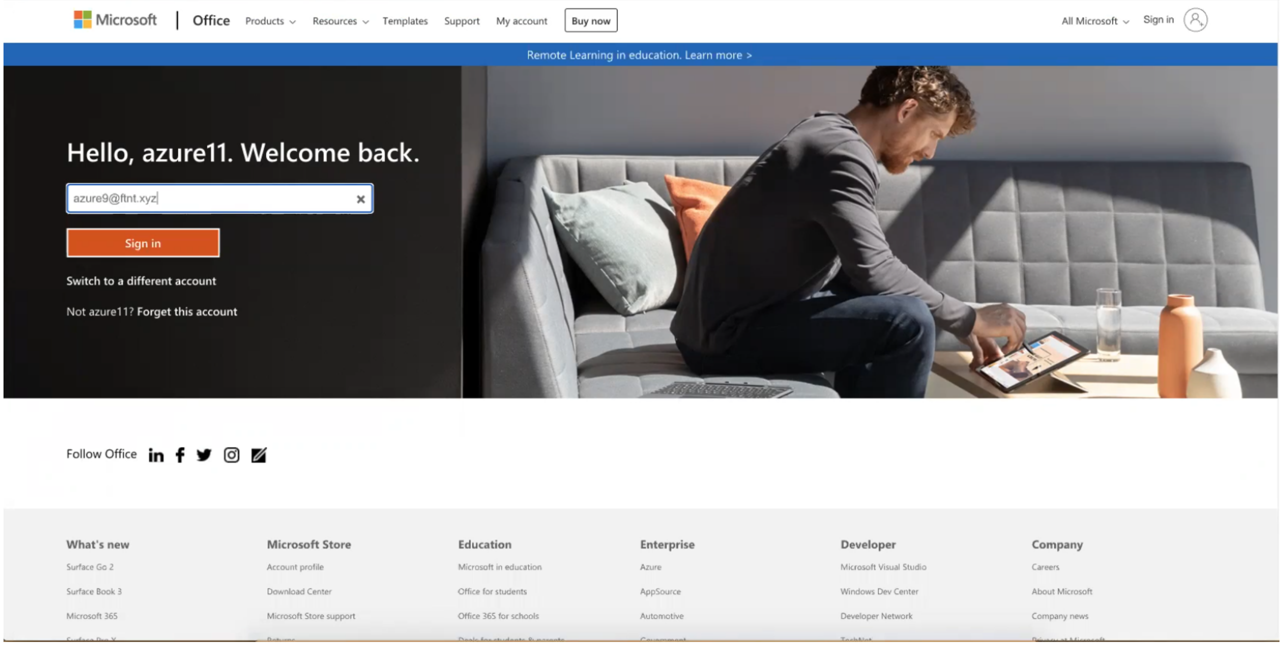
Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute. Learn more

Results

Once configured, Active Directory synchronized users can sign in to Office 365 using two-factor authentication from FortiAuthenticator.

To sign in to Office 365 using FortiAuthenticator with two-factor authentication:

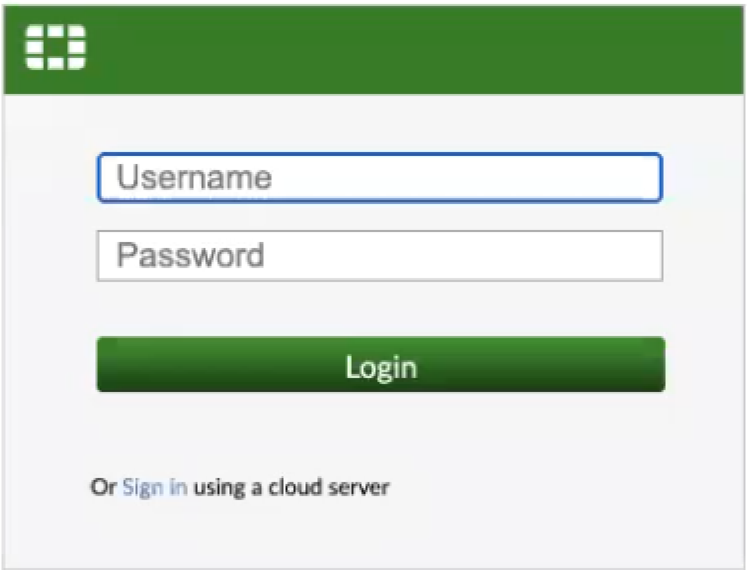
1. Navigate to Office 365 and click *Sign in* or *Switch to a different account*.
2. Enter a user account with domain and click *Sign in*.



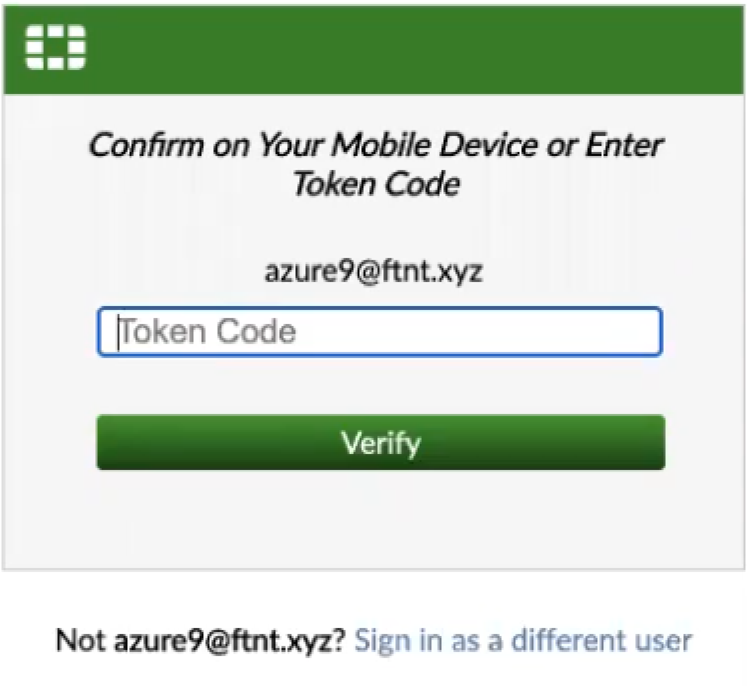
Hello, azure11. Welcome back.

azure9@ftnt.xyz

3. Authentication is redirected to FortiAuthenticator. Enter your user credentials, and click *Login*.



Enter your 2FA token or approve the access request from your FortiToken push request.



Confirm on Your Mobile Device or Enter Token Code

azure9@ftnt.xyz

Not azure9@ftnt.xyz? Sign in as a different user

Once approved you are logged in to your Office 365 account.