Cookbook

FortiAuthenticator 6.5.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

January 10, 2024
FortiAuthenticator 6.5.0 Cookbook
23-650-779541-20240110

TABLE OF CONTENTS

Change Log

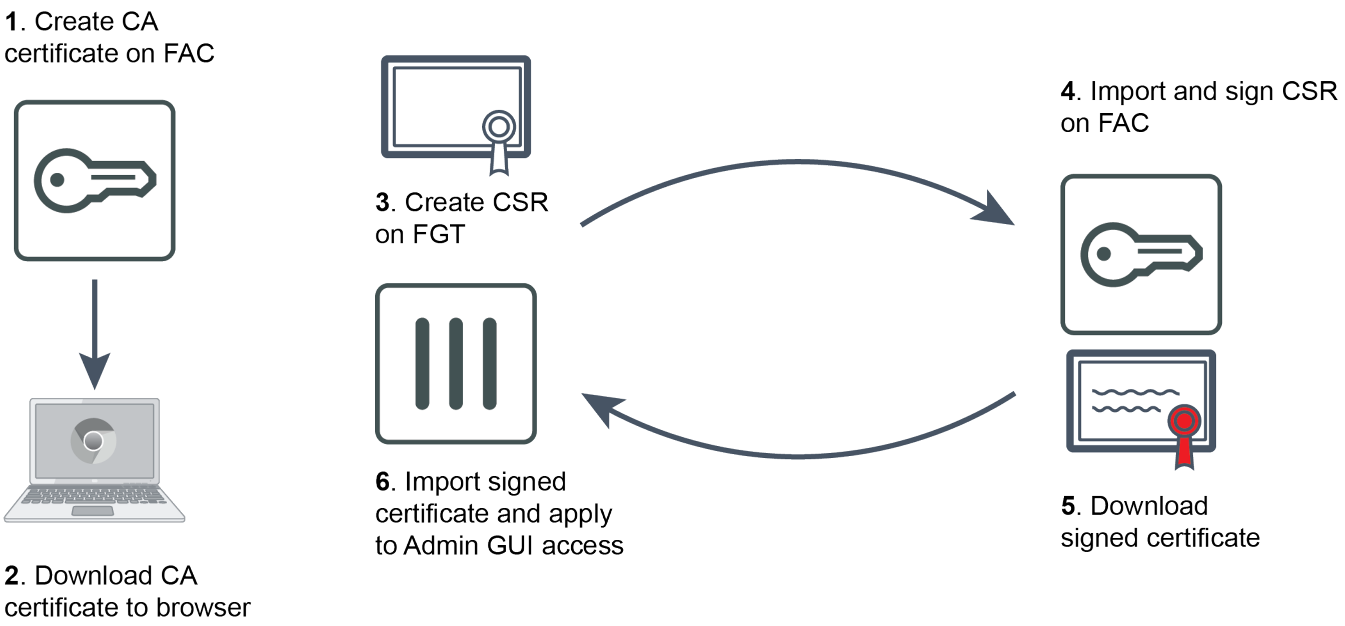
Date	Change Description
2023-02-21	Initial release.
2023-03-06	Updated Generating the Google Workspace certificate on page 169 and Configuring LDAP on the FortiAuthenticator on page 172.
2023-03-28	Added Debugging on page 340. Updated: • Setting up a zero trust tunnel on page 334 • Configuring a zero trust tunnel on FortiAuthenticator on page 334 • Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator on page 335 • Configuring certificate authentication for FortiAuthenticator on page 335 • Configuring a ZTNA server on page 338
2023-06-09	Updated Configuring FSSO on FortiGate on page 193.
2023-07-11	Updated Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 204.
2023-08-21	Updated Configuring RADIUS client on FortiAuthenticator on page 128.
2023-12-05	Updated Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 204.
2024-01-10	Updated Creating a remote OAuth server with Azure application ID and authentication key on page 233.

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.

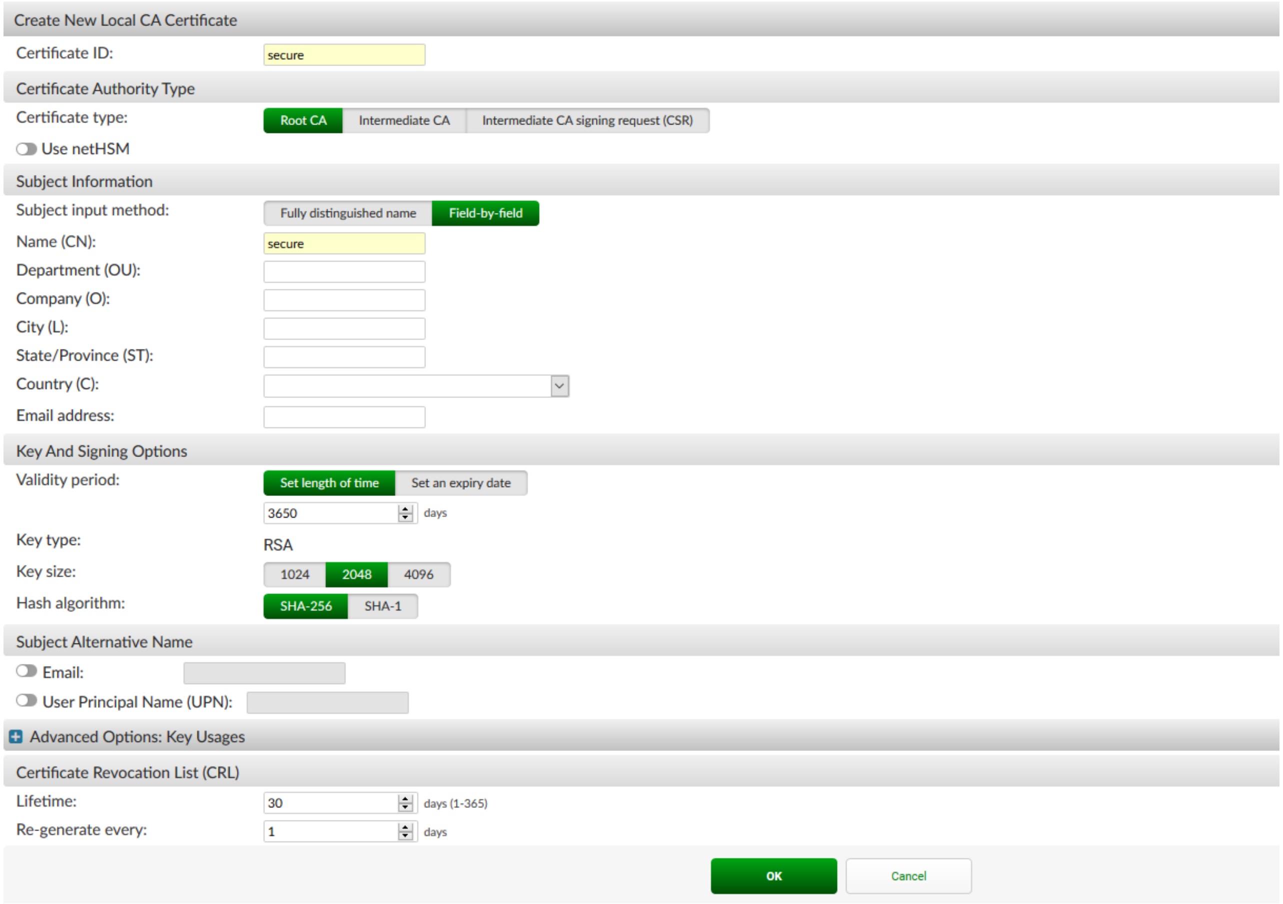
This scenario includes creating a certificate request on the FortiGate, downloading the certificate to the network's computers, and then importing it to the FortiAuthenticator. You will sign the certificate with the FortiAuthenticator's own certificate, then download and import the signed certificate 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 (selected) | Intermediate CA | Intermediate CA signing request (CSR)
○ Use netHSM	

Subject Information

Subject input method:	Fully distinguished name | Field-by-field (selected)
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 (selected) | Set an expiry date
	3650 days
Key type:	RSA
Key size:	1024 | 2048 (selected) | 4096
Hash algorithm:	SHA-256 (selected) | SHA-1

Subject Alternative Name

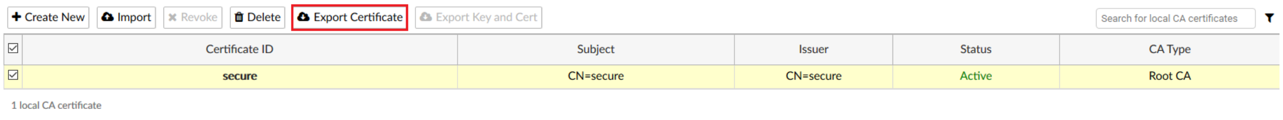
○ Email:	
○ User Principal Name (UPN):	

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

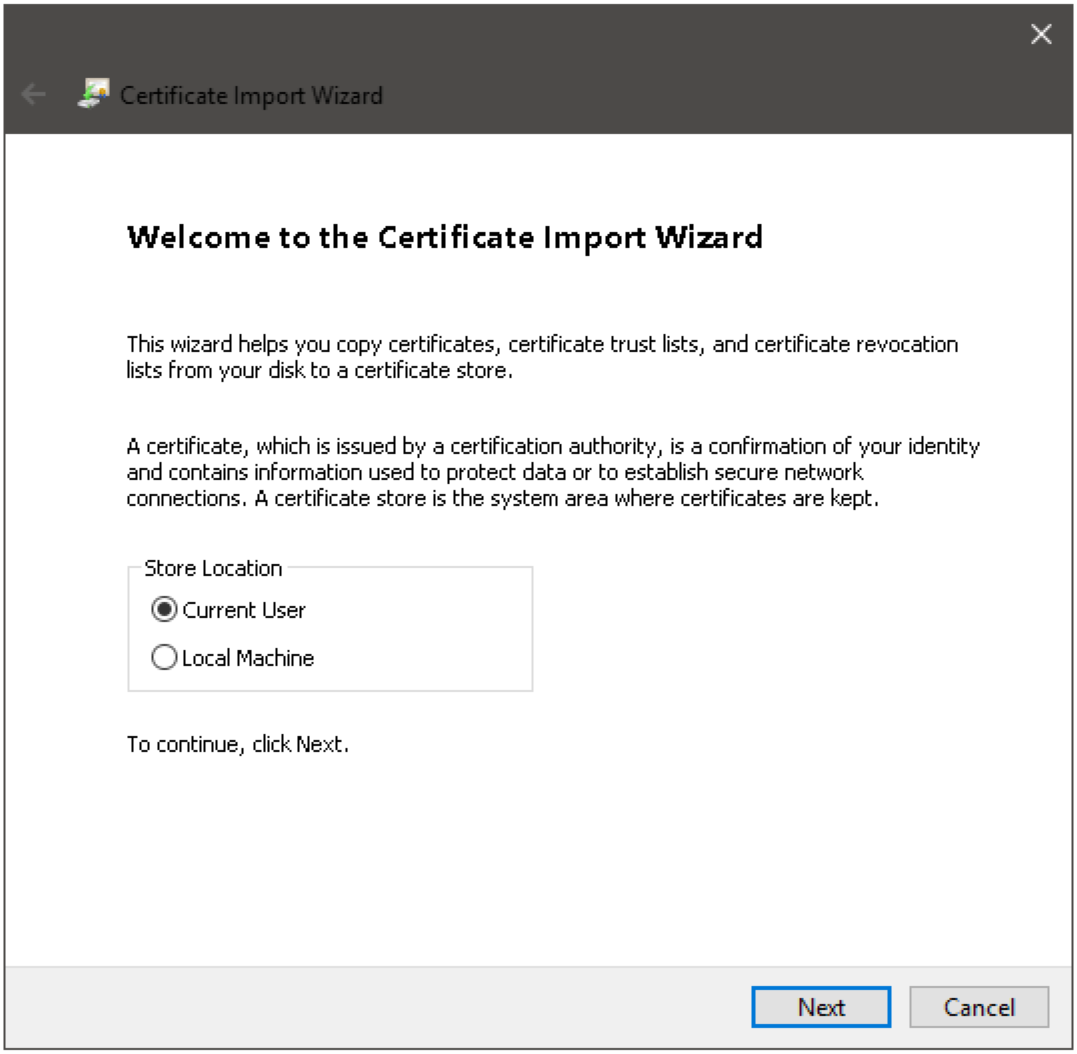
This will save a *.crt* file to your local drive.

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*.



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.

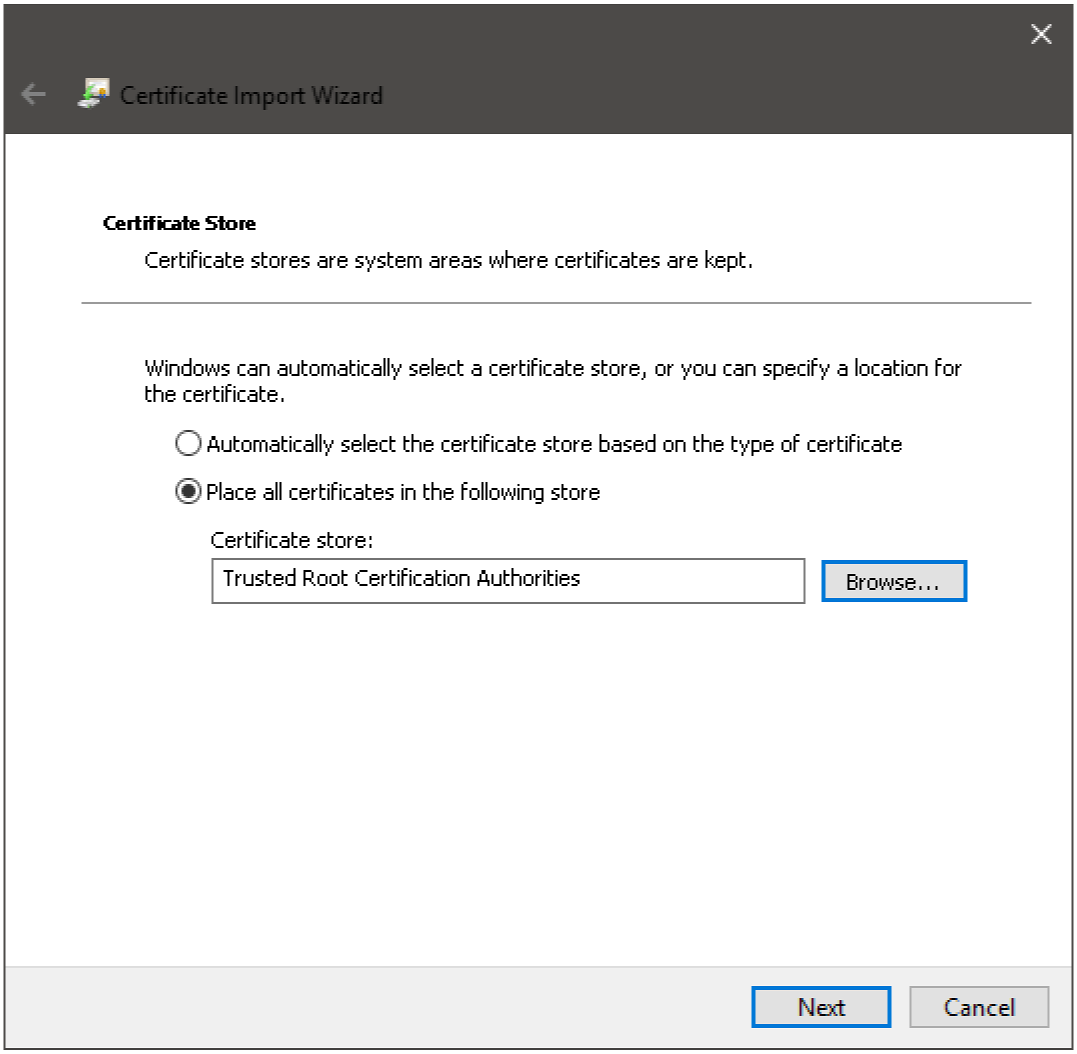
Store Location

● 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.

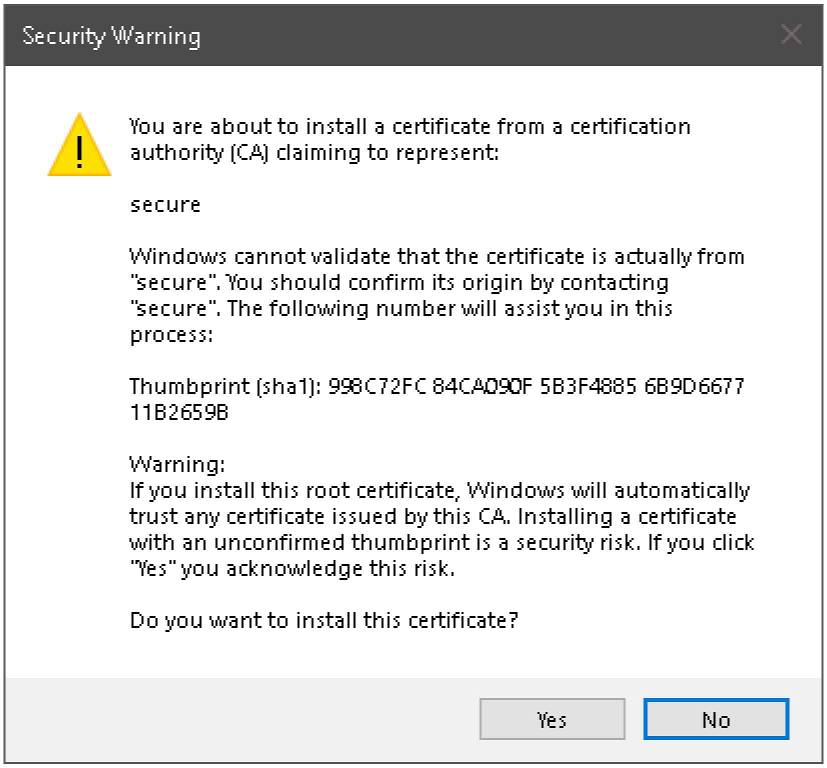
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ 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:

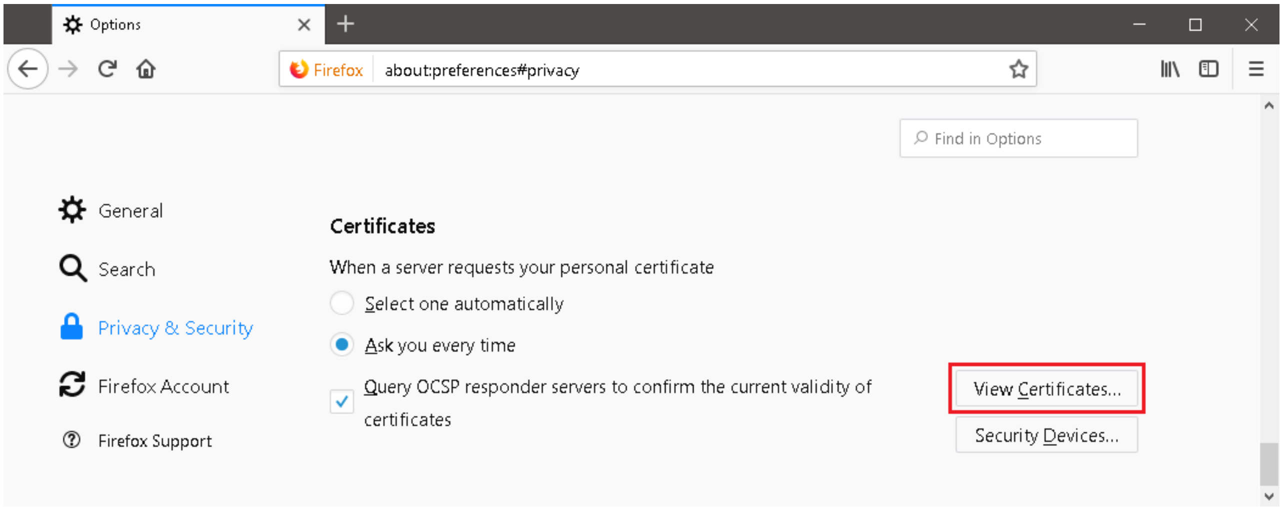
Thumbprint (sha1): 998C72FC 84CA090F 5B3F4885 6B9D6677 11B2659B

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

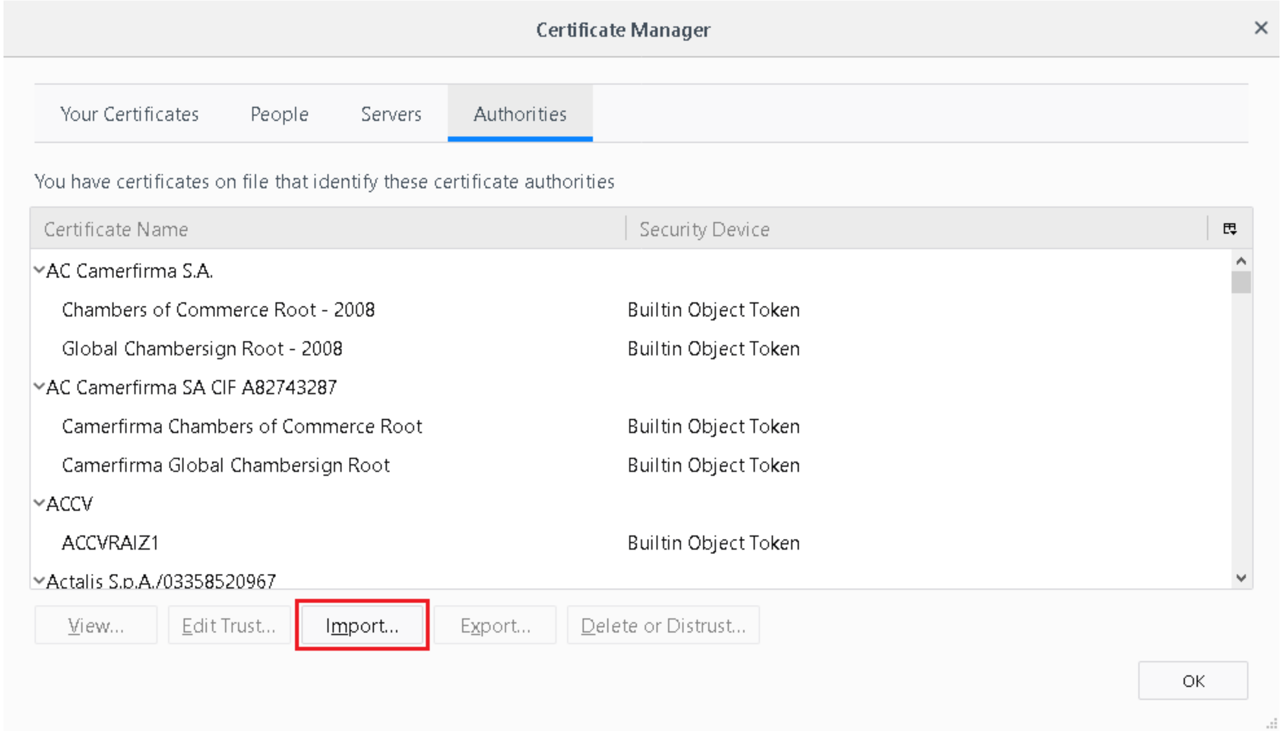
When a server requests your personal certificate

○ 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*.

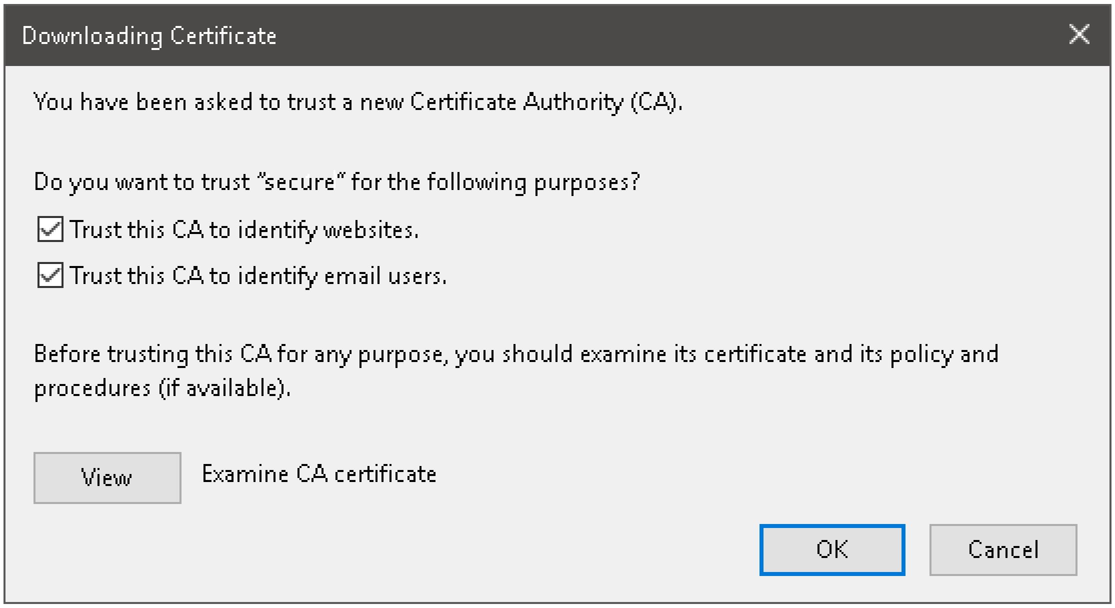


Certificate Manager

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*.



Downloading Certificate

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).

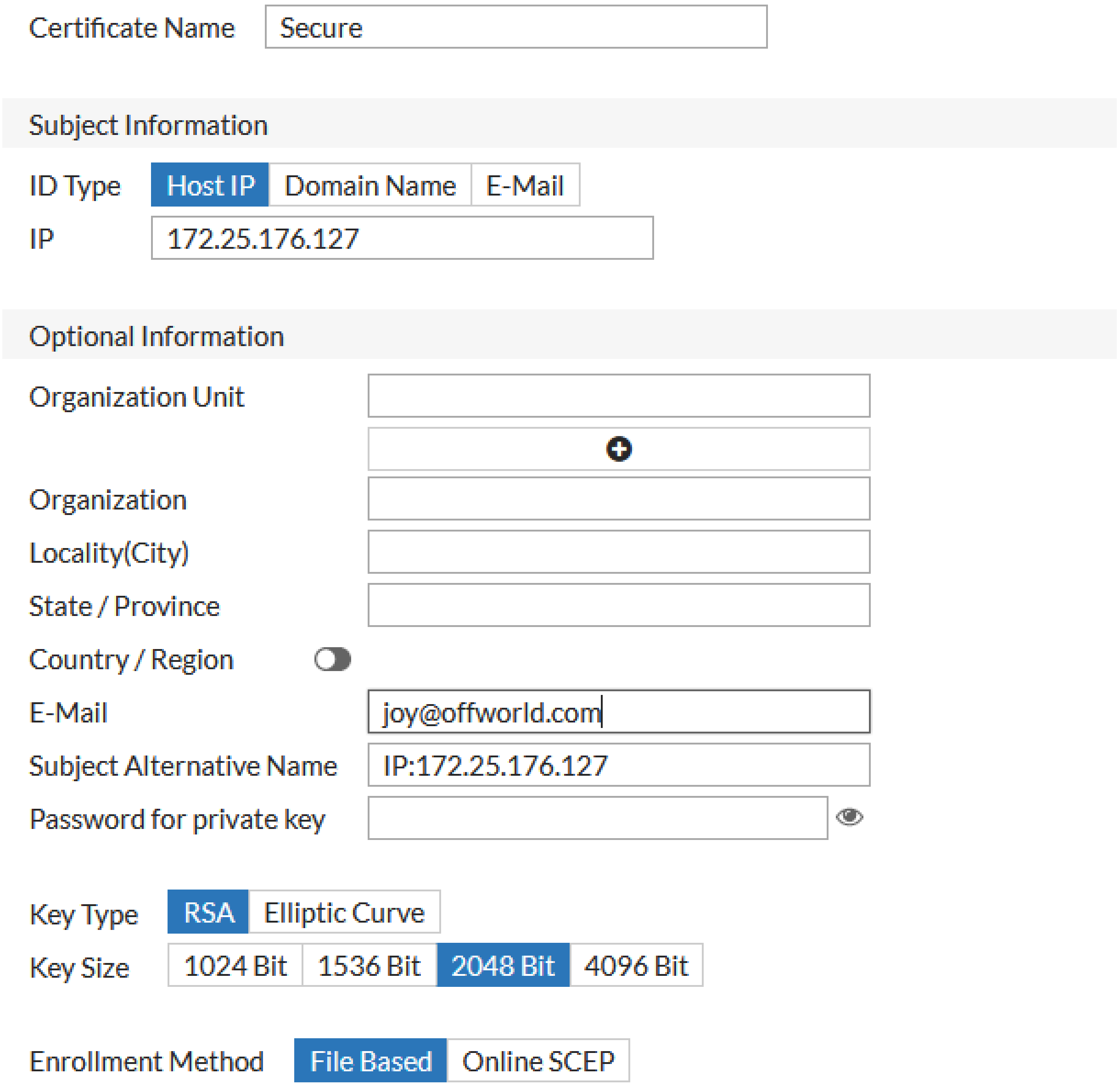
Examine CA certificate

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

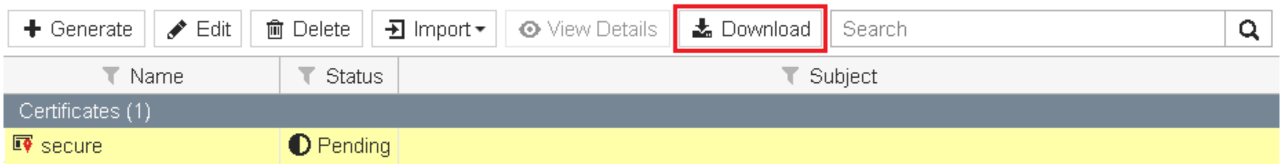
   Password for private key:

   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*.



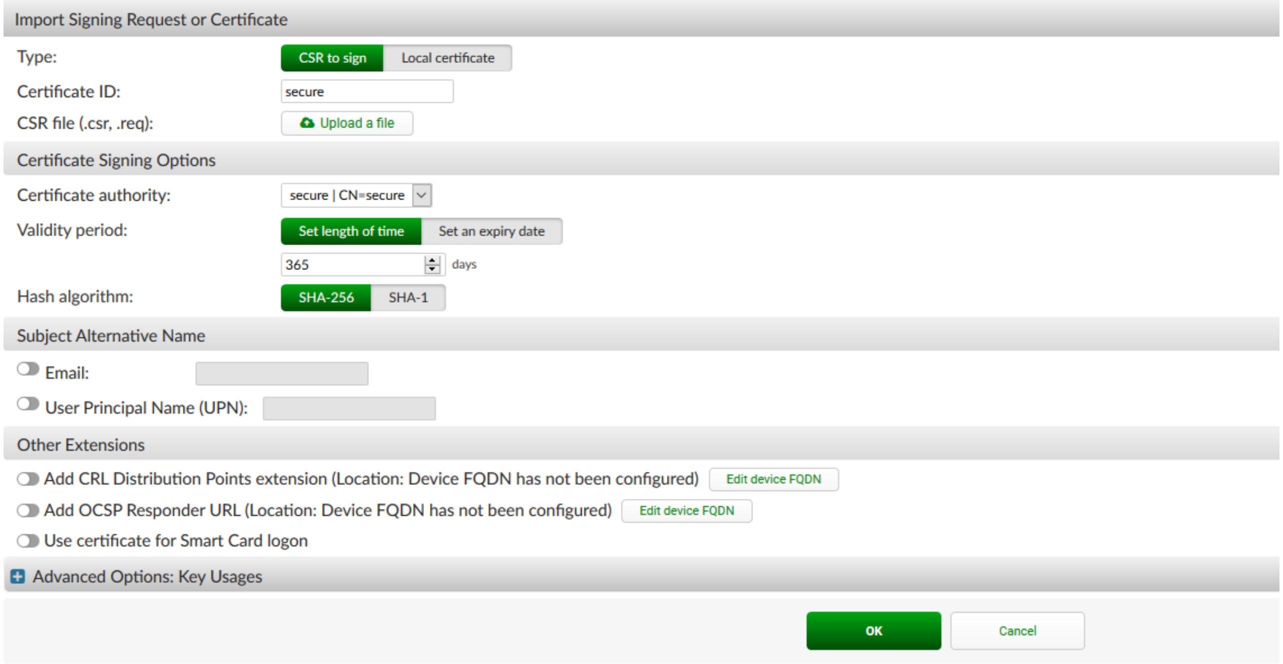
Name	Status	Subject
Certificates (1)		
secure	Pending	

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 (selected) / 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 (selected) / Set an expiry date
	365 days
Hash algorithm:	SHA-256 (selected) / SHA-1

Subject Alternative Name

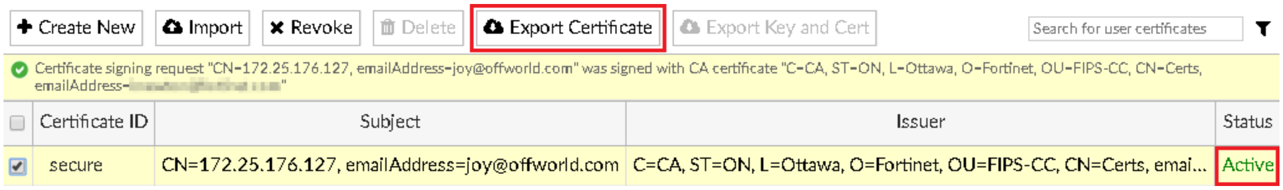
- ○ Email:
- ○ User Principal Name (UPN):

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

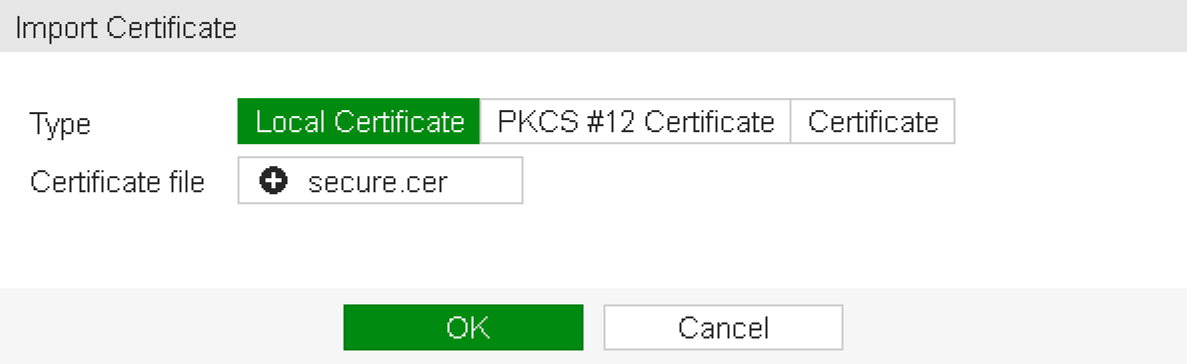
This will save a **.cer** file to your local drive.

secure.cer

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*.

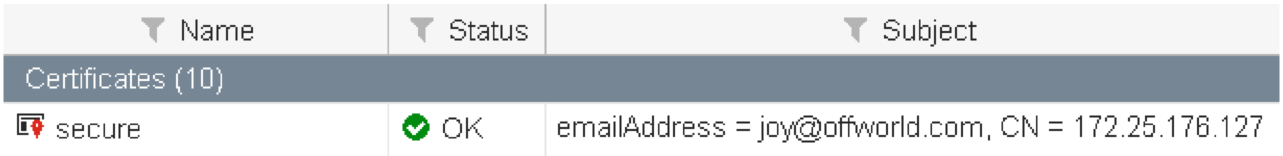


Import Certificate

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.



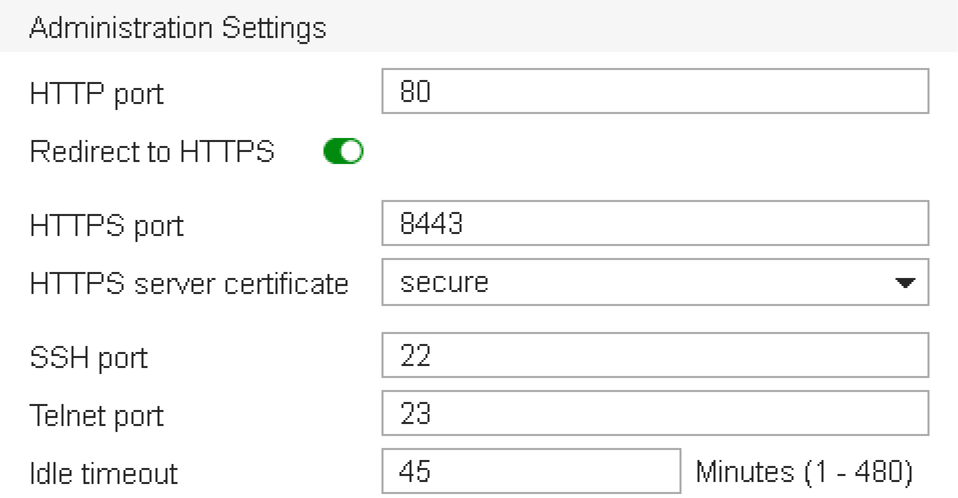
Name	Status	Subject
Certificates (10)		
secure	✓ OK	emailAddress = joy@offworld.com, CN = 172.25.176.127

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.

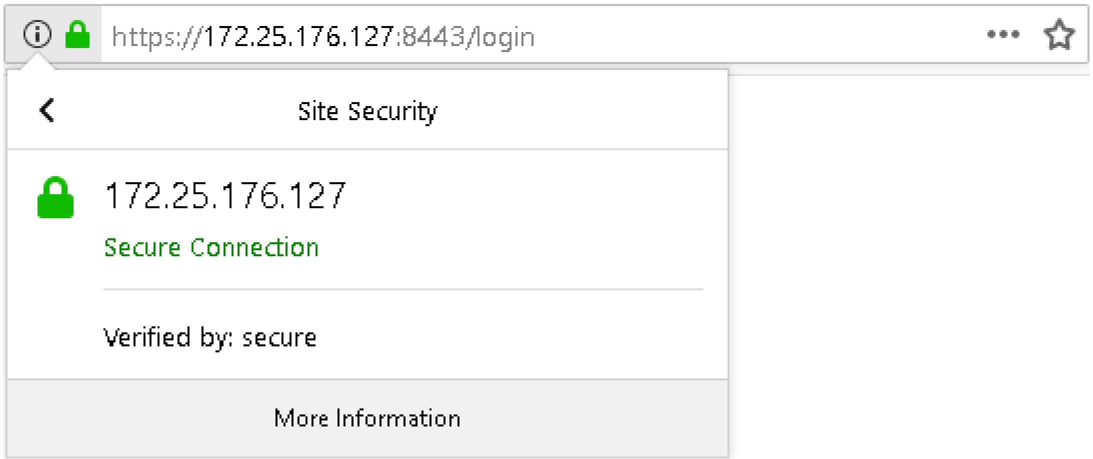


Administration Settings

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

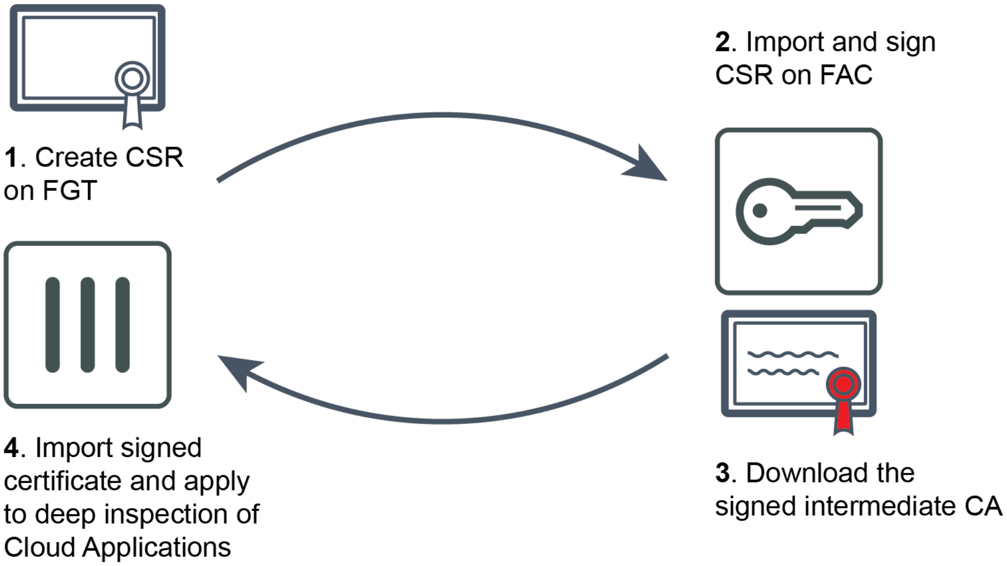
Site Security

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.

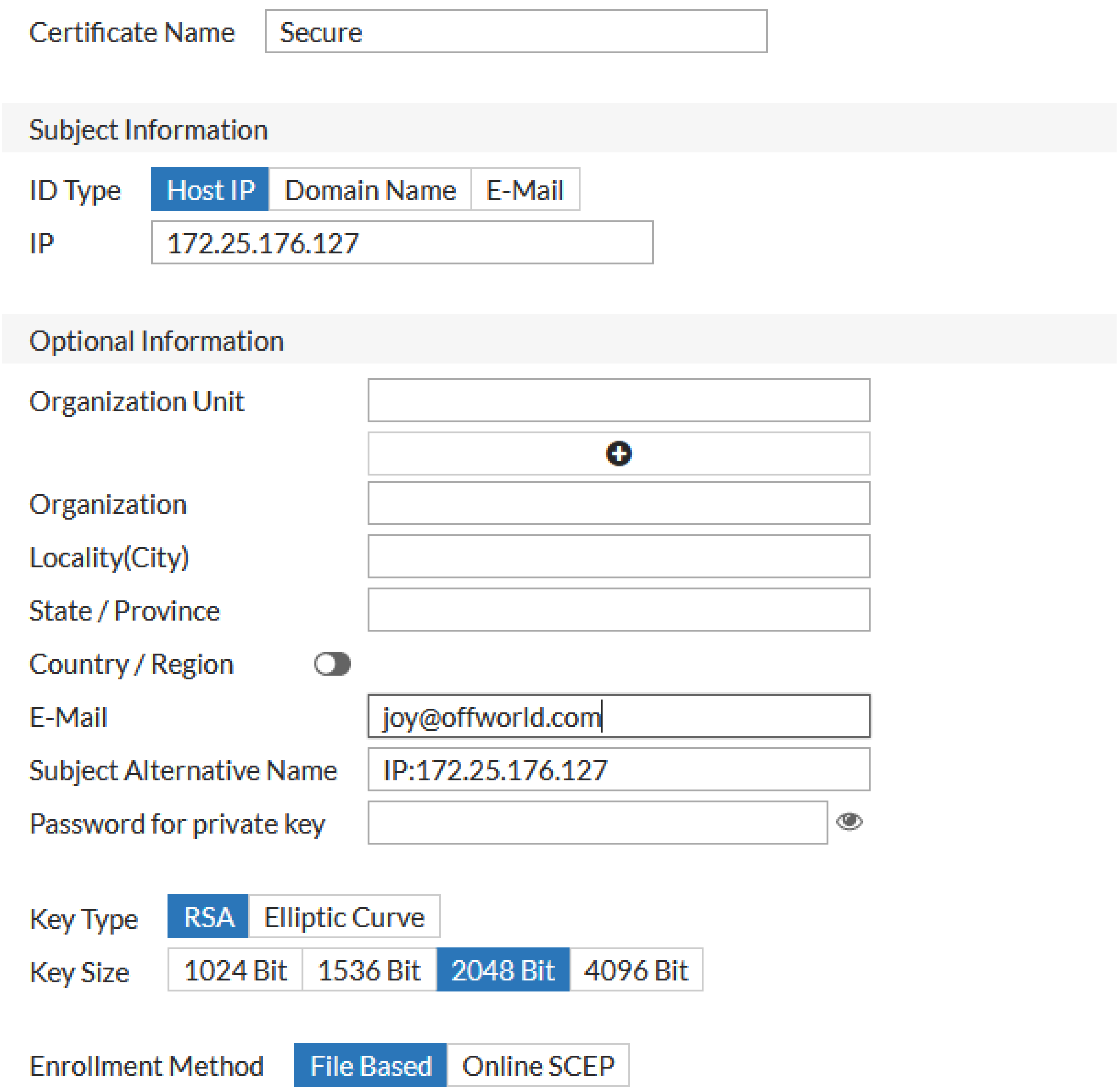
As an example, you will also have *Application Control* with *Deep Inspection of Cloud Applications* enabled. This will apply inspection to HTTPS traffic. Note that you may use another security profile instead of *Application Control*.

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

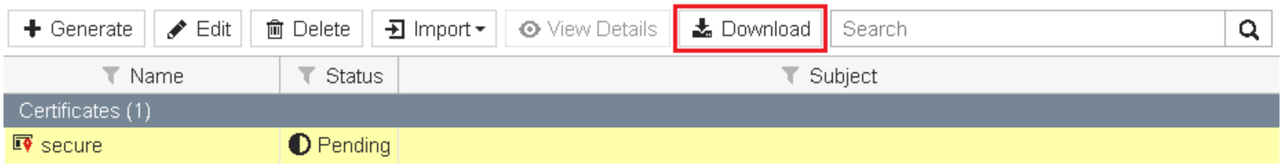
Password for private key:

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*.



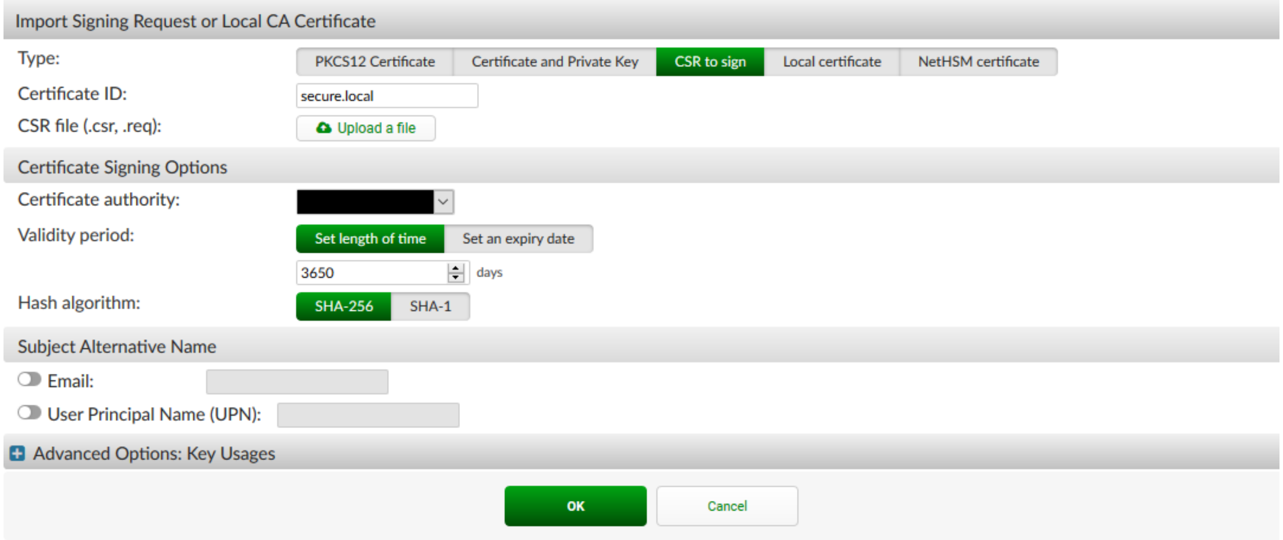
Name	Status	Subject
Certificates (1)		
secure	Pending	

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

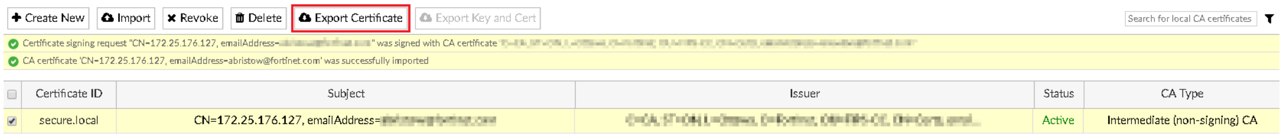
Certificate authority:	[redacted]
Validity period:	**Set length of time** / Set an expiry date
	3650 days
Hash algorithm:	**SHA-256** / SHA-1

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

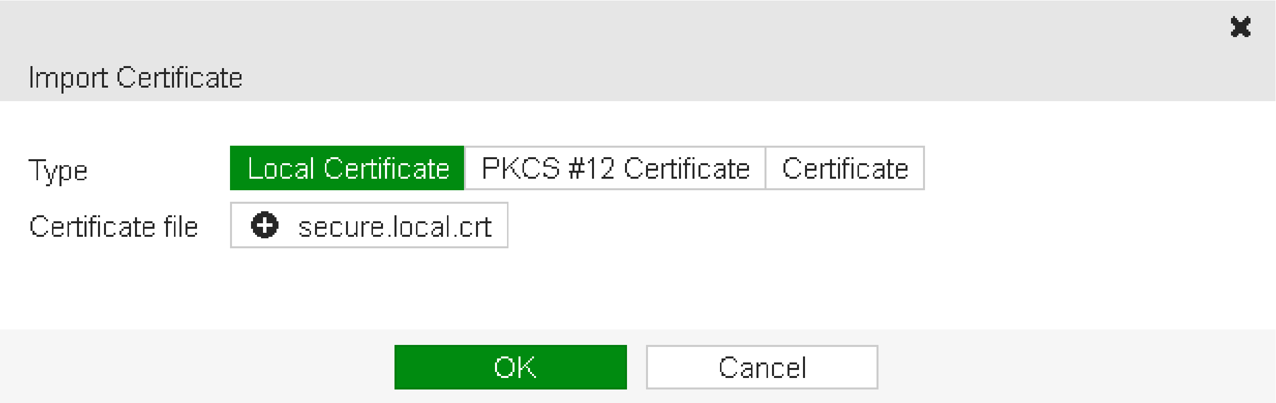
This will save a *.crt* file to your local drive.

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*.

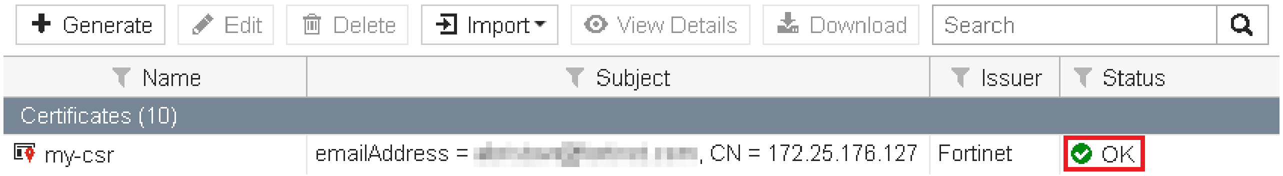


Import Certificate

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*.

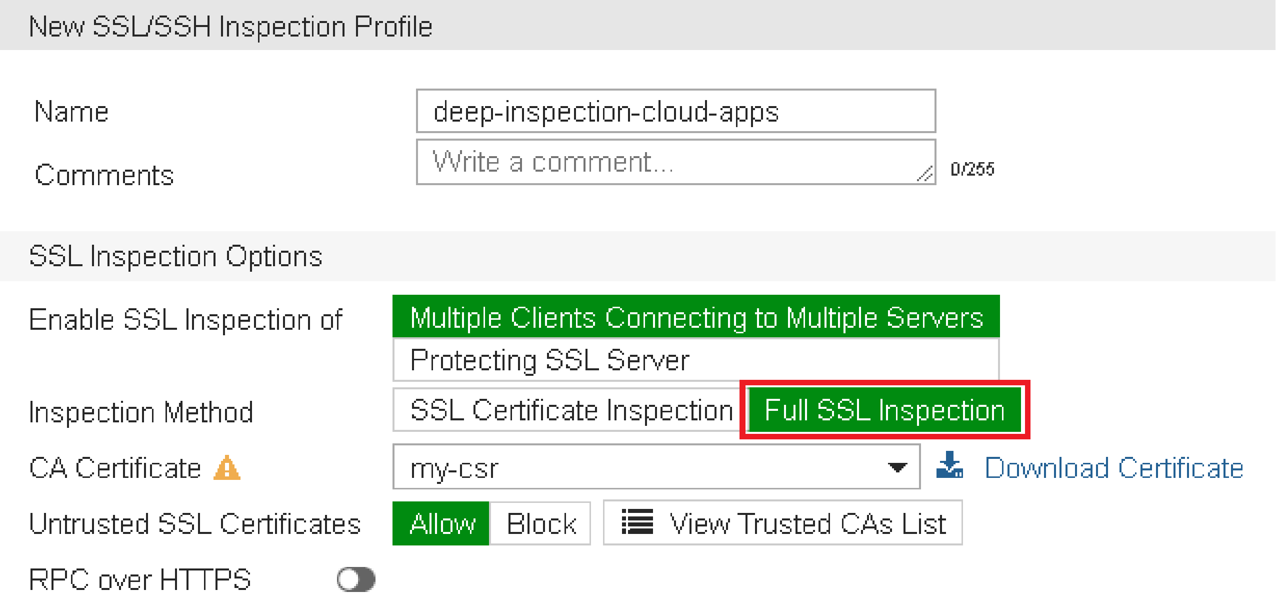


Name	Subject	Issuer	Status
Certificates (10)			
my-csr	emailAddress = [redacted], CN = 172.25.176.127	Fortinet	✓ OK

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]

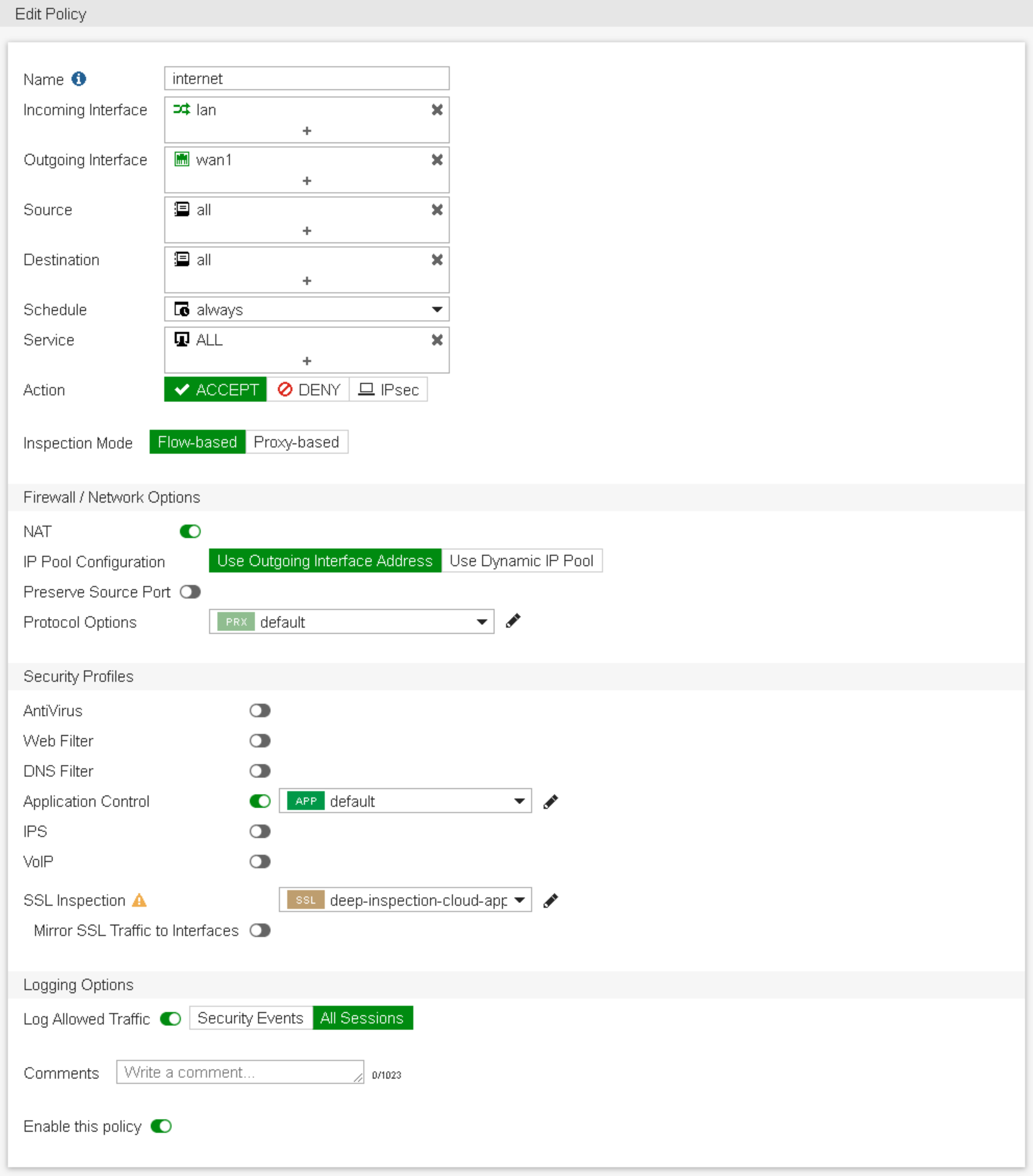
CA Certificate ⚠: my-csr

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 (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

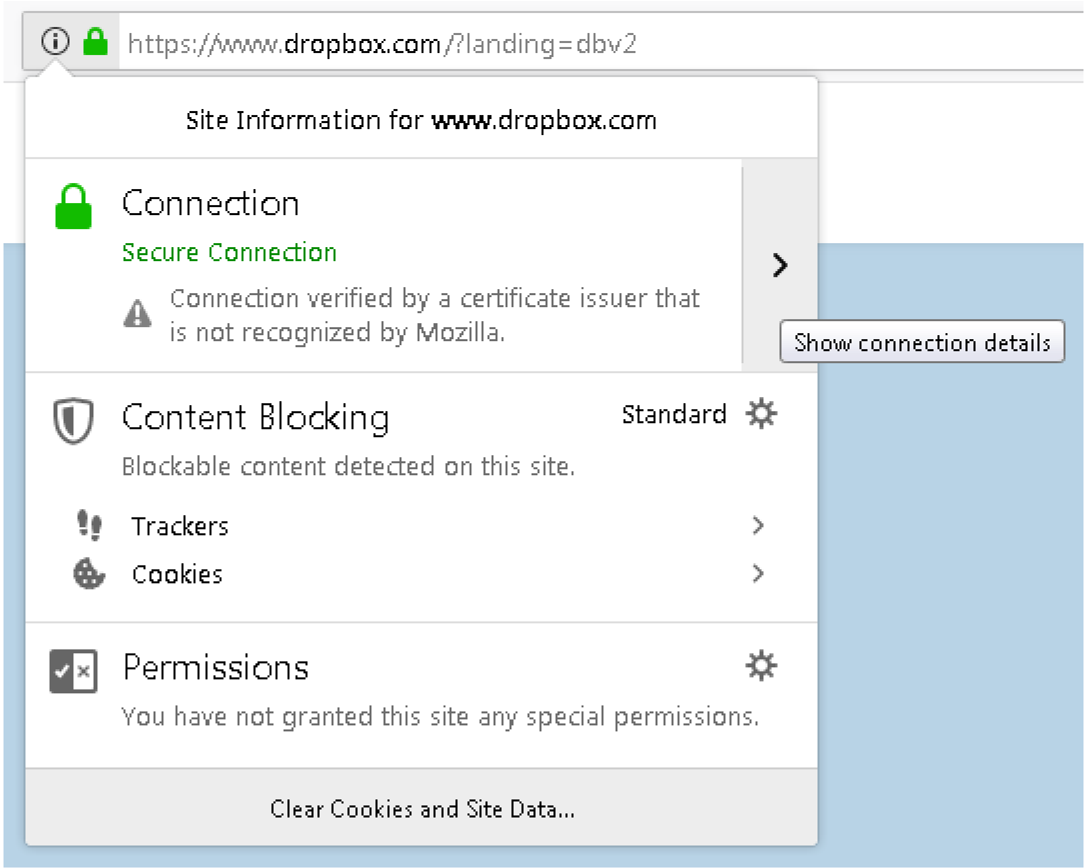
AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	● APP default
IPS	○
VoIP	○
SSL Inspection ⚠	SSL deep-inspection-cloud-apr
Mirror SSL Traffic to Interfaces	○

Logging Options

Log Allowed Traffic	● Security Events / All Sessions (selected)
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.

Content Blocking

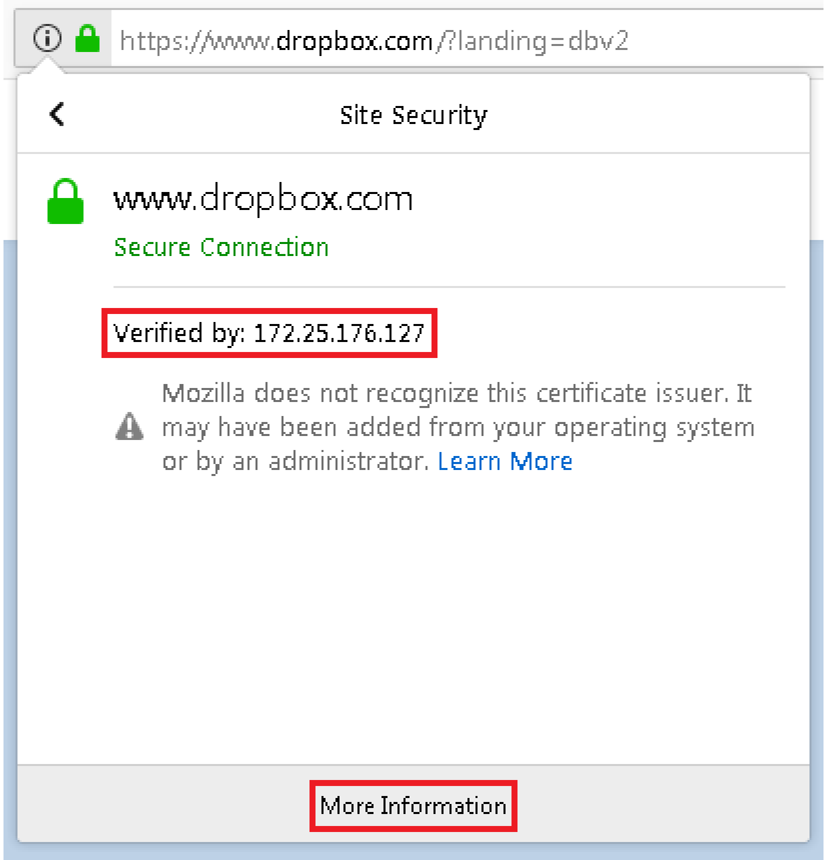
Blockable content detected on this site.

Permissions

You have not granted this site any special permissions.

2. You should now see that the certificate from the FortiGate (`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

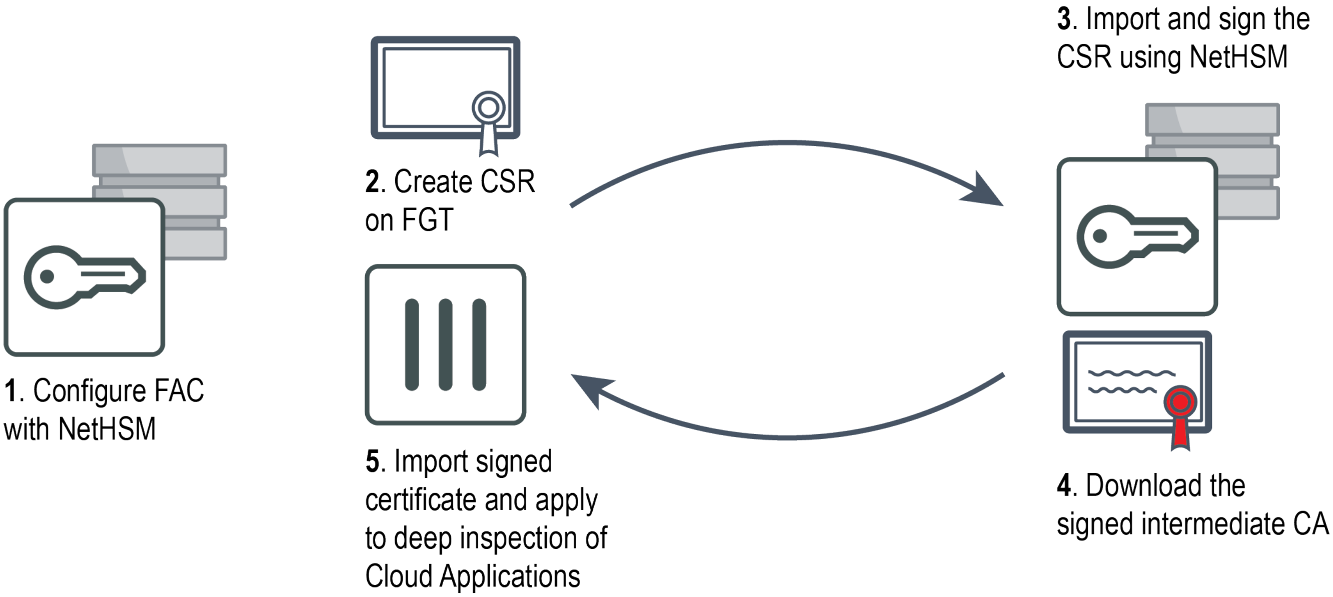
www.dropbox.com

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 27
2. Creating a local CA certificate using an HSM server on page 28
3. Creating a CSR on the FortiGate on page 29
4. Creating an Intermediate CA on the FortiAuthenticator on page 30
5. Importing the signed certificate on the FortiGate on page 31
6. Configuring full SSL inspection on page 31
7. Results on page 34

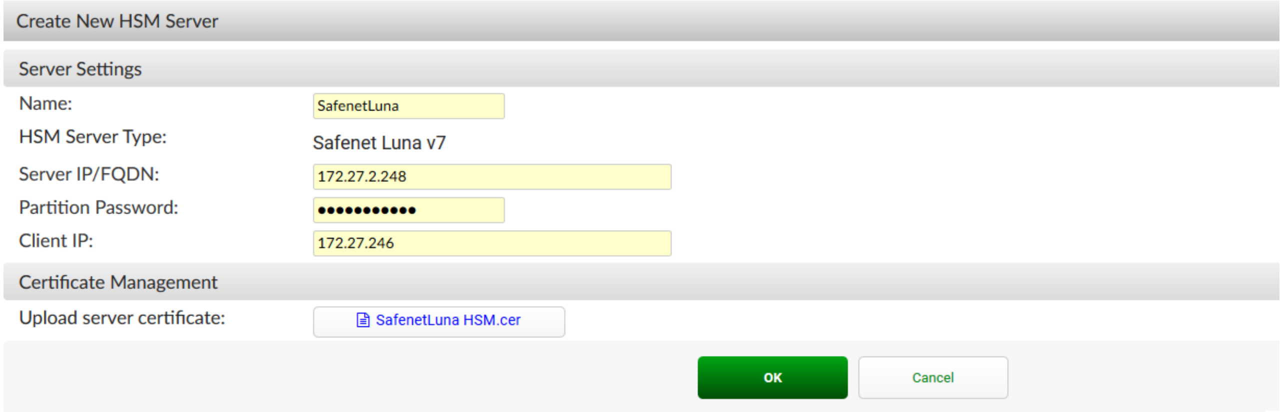
In order for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this recipe will not be trusted. For more information on how to do this, see Creating a local CA certificate using an HSM server on page 28 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:

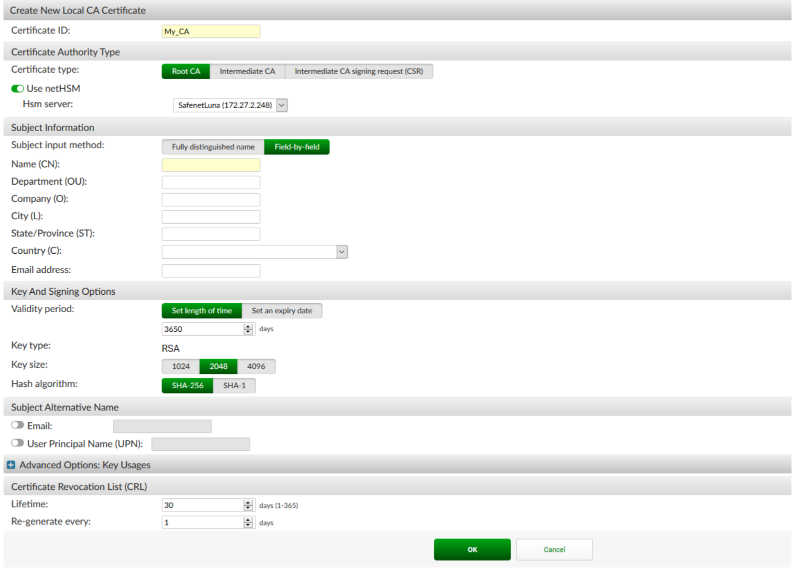
1. Make sure the FortiAuthenticator client certificate uses the `<FAC IP>.pem` naming convention. For example: `172.16.68.47.pem`
2. Upload the FortiAuthenticator client certificate to Safenet Luna HSM using SCP transfer.
   ```
   scp [certificate filename] admin@[HSM address]:
   ```
3. Use SSH to connect to the HSM, then register your FortiAuthenticator, and associate it with a partition.
   ```
   ssh -l 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 10.

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

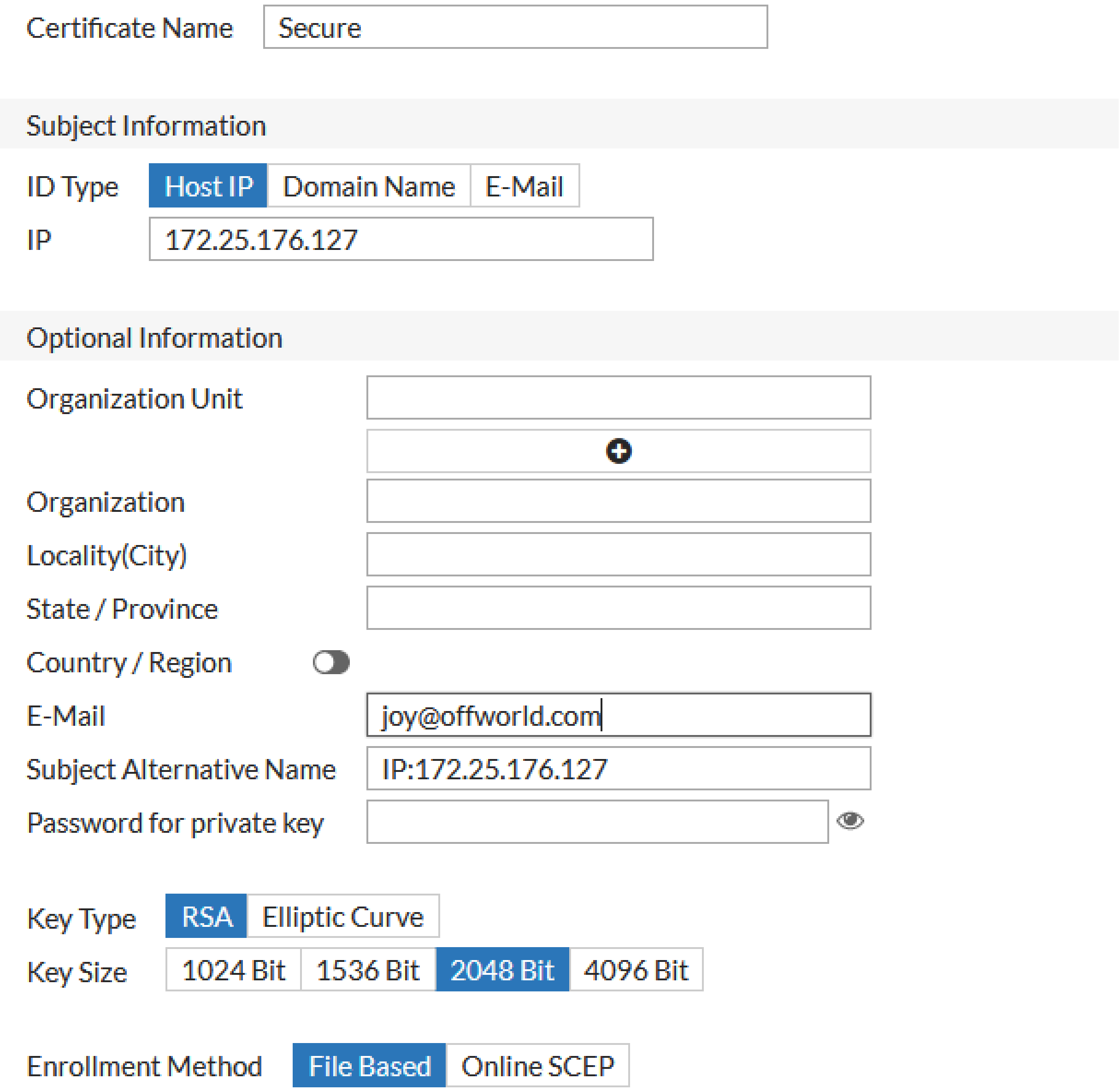
2. Enter a name for the CA certificate, for example *My_CA*.
3. Select *Root CA* as the *Certificate type*.
4. Enable *Use NetHSM*, and choose an HSM server from the dropdown menu.
5. Configure the remaining settings as desired, and click *OK* to save your changes.
   Once your CA certificate has been 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 10.

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

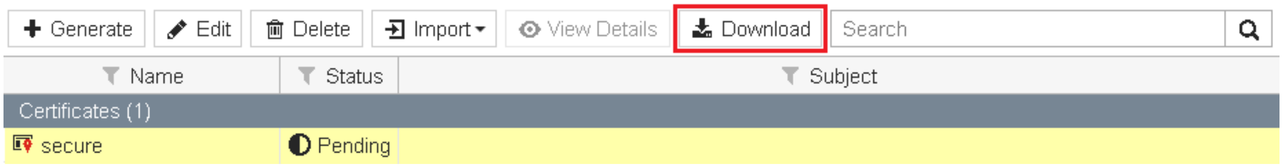
   Password for private key:

   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*.



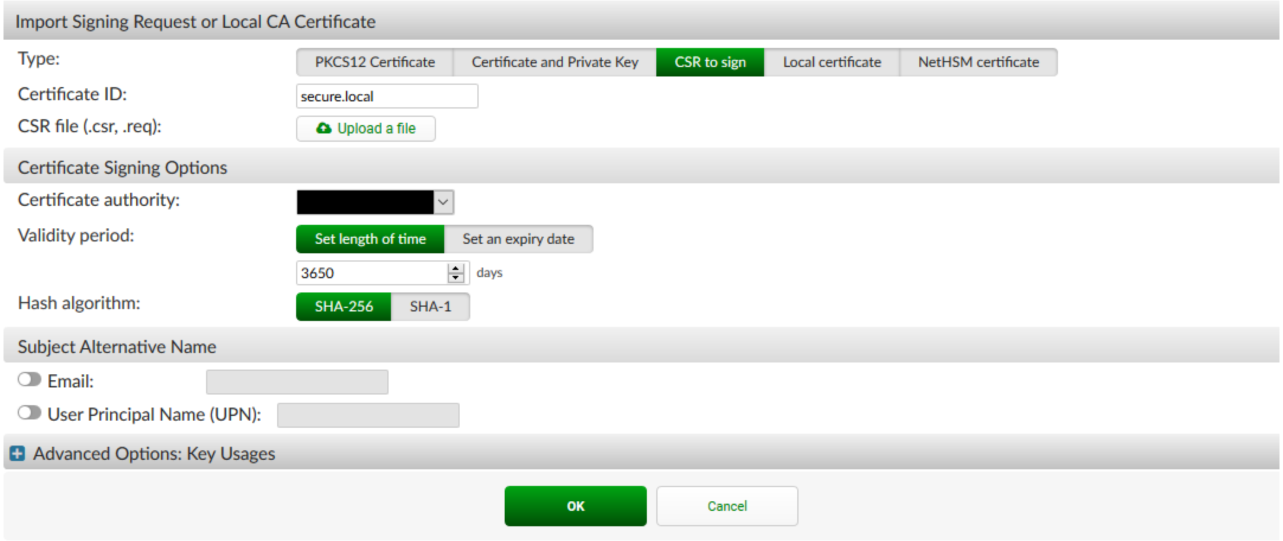
Name	Status	Subject
Certificates (1)		
secure	Pending	

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.
2. Select the *Certificate authority* configured with the HSM from the dropdown menu, and set the *Hash algorithm* to *SHA-256*. Click *OK*.



Type: CSR to sign

Certificate ID: secure.local

CSR file (.csr, .req):

Certificate authority: [redacted]

Validity period: Set length of time

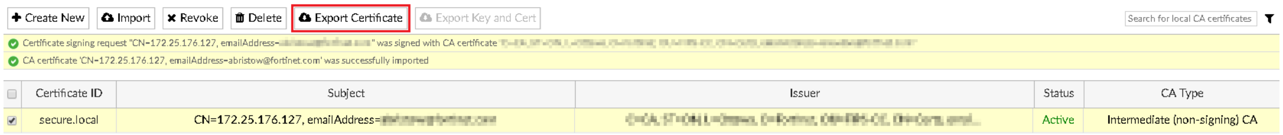
3650 days

Hash algorithm: SHA-256

Email:

User Principal Name (UPN):

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

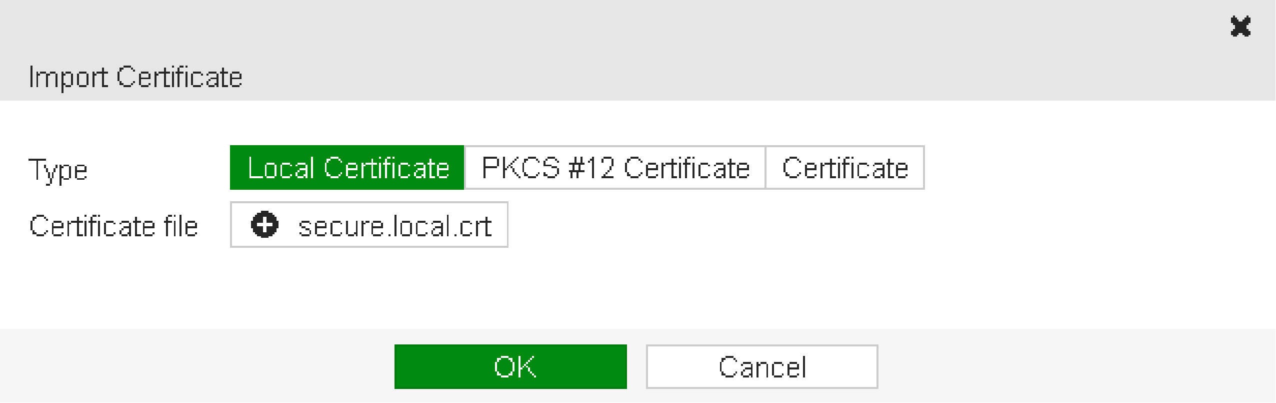
☐	Certificate ID	Subject	Issuer	Status	CA Type
☑	secure.local	CN=172.25.176.127, emailAddress=[redacted]	[redacted]	Active	Intermediate (non-signing) CA

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

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*.

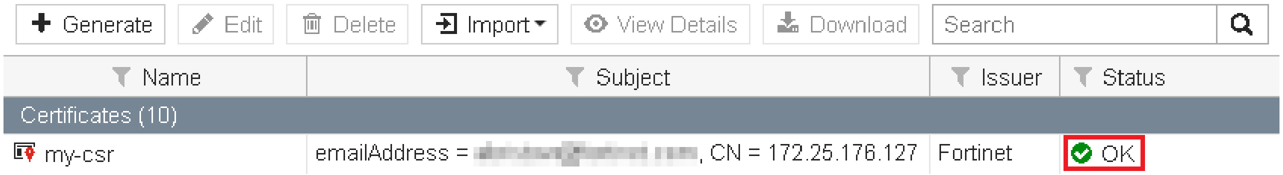


Import Certificate

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*.

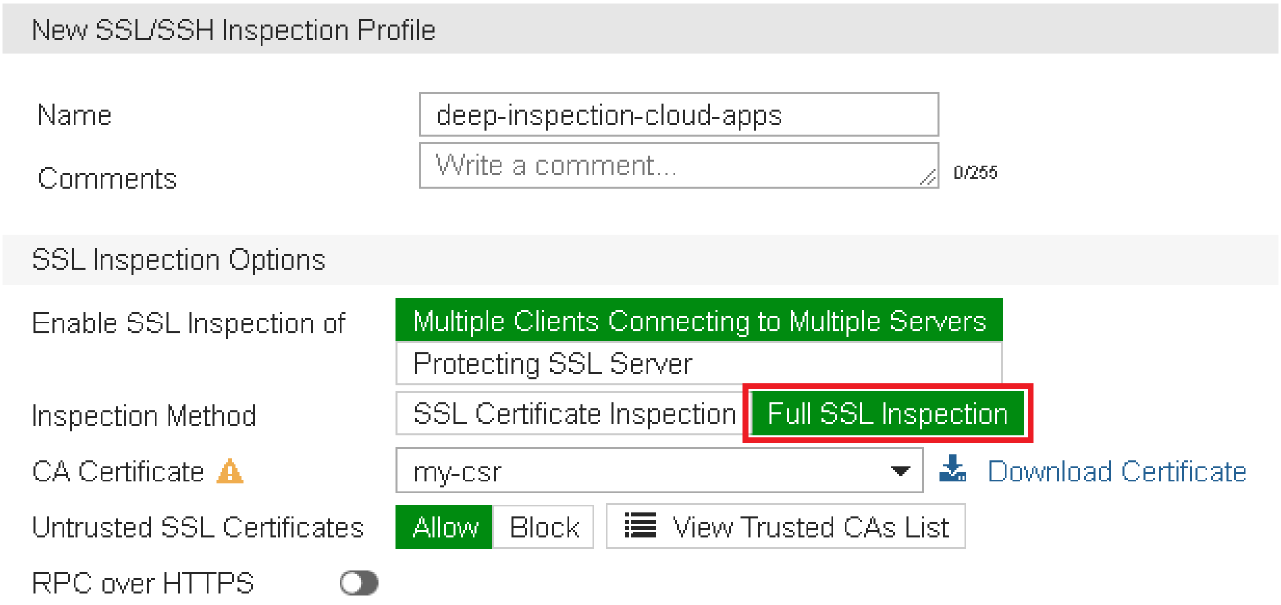


Name	Subject	Issuer	Status
Certificates (10)			
my-csr	emailAddress = [redacted], CN = 172.25.176.127	Fortinet	✓ OK

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]

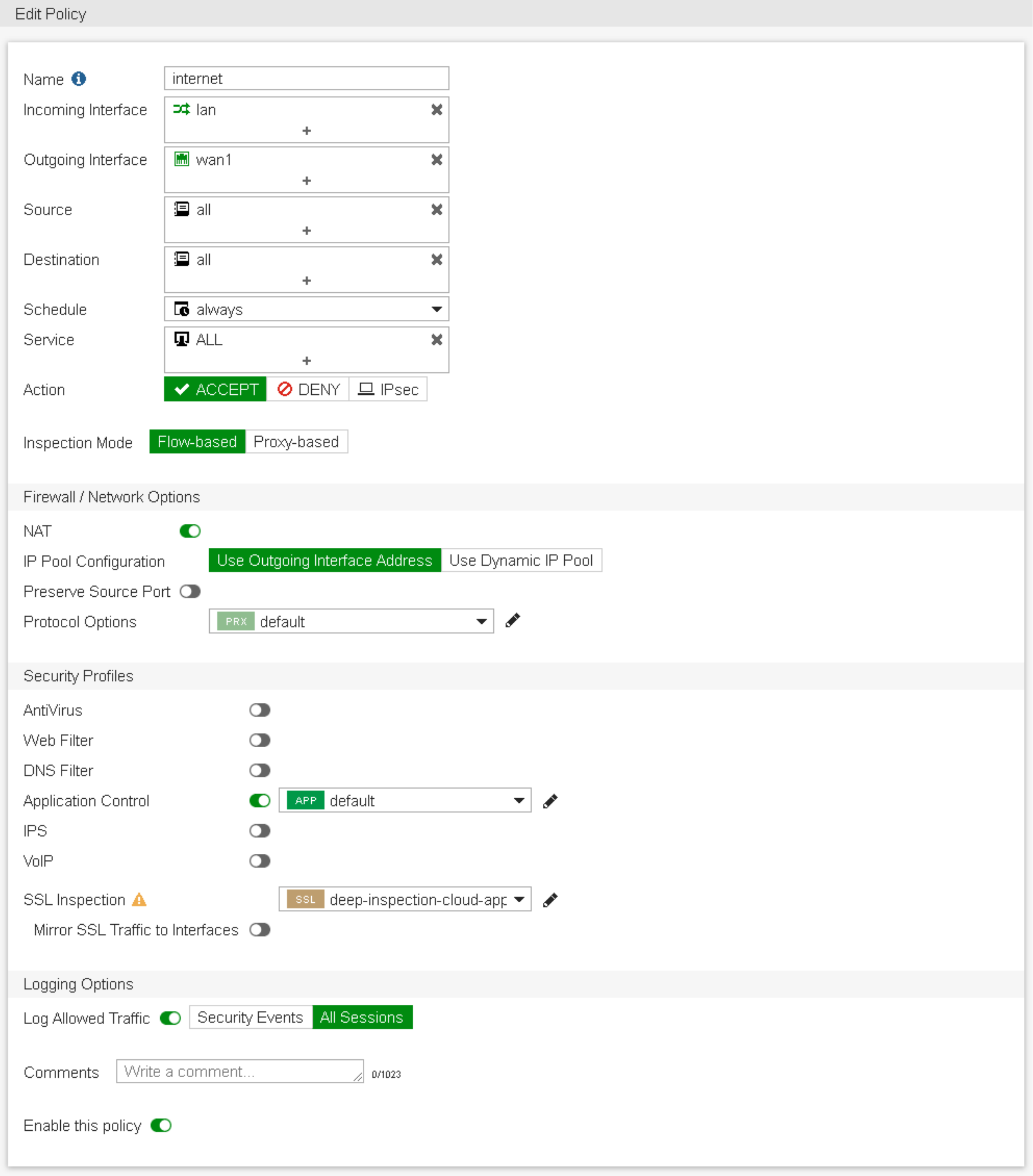
CA Certificate ⚠: my-csr — Download Certificate

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	○

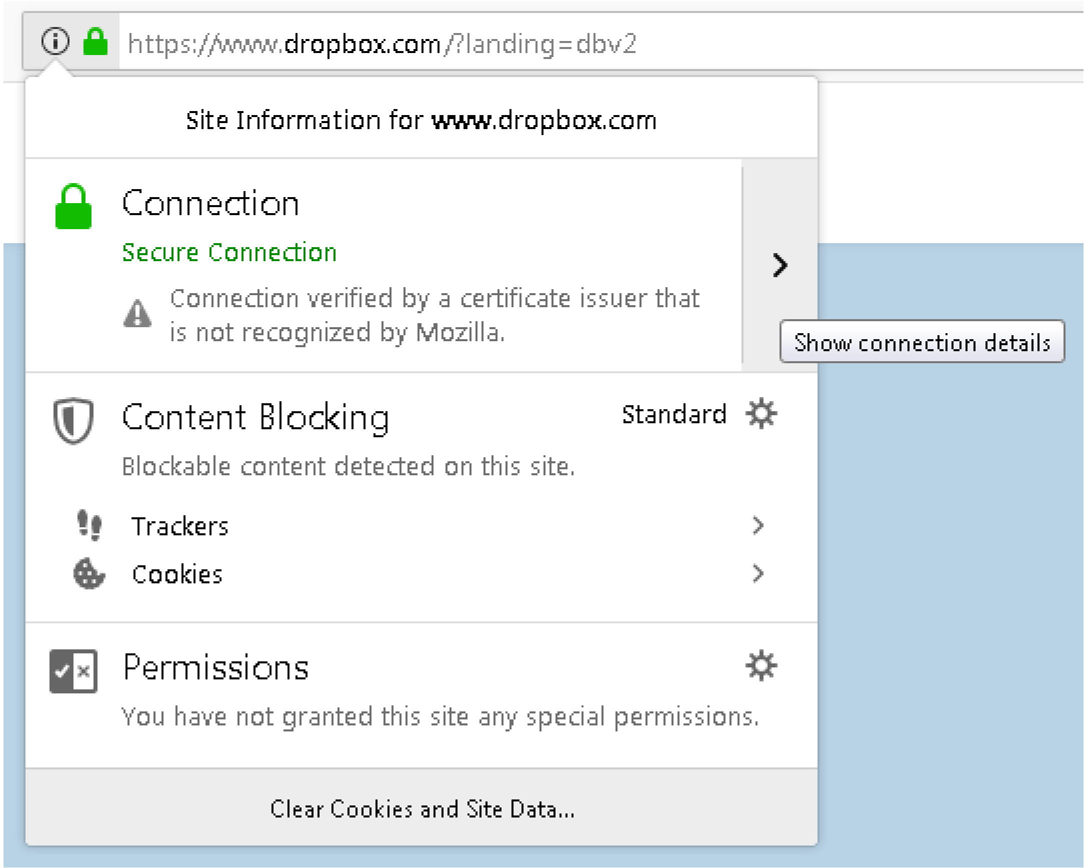
Logging Options

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

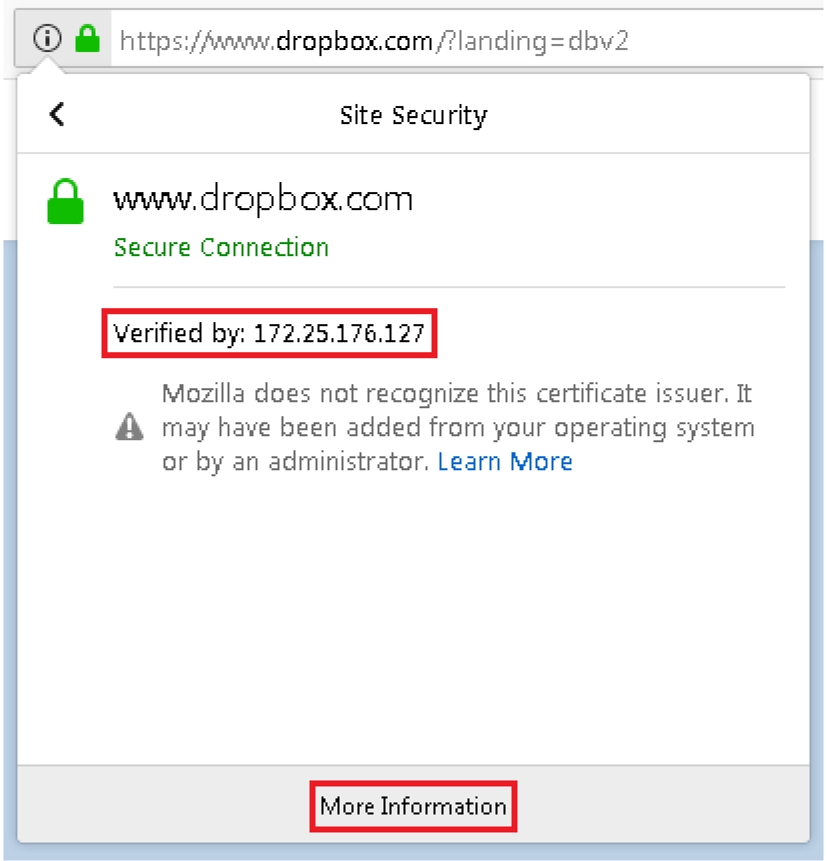
   Blockable content detected on this site.

   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

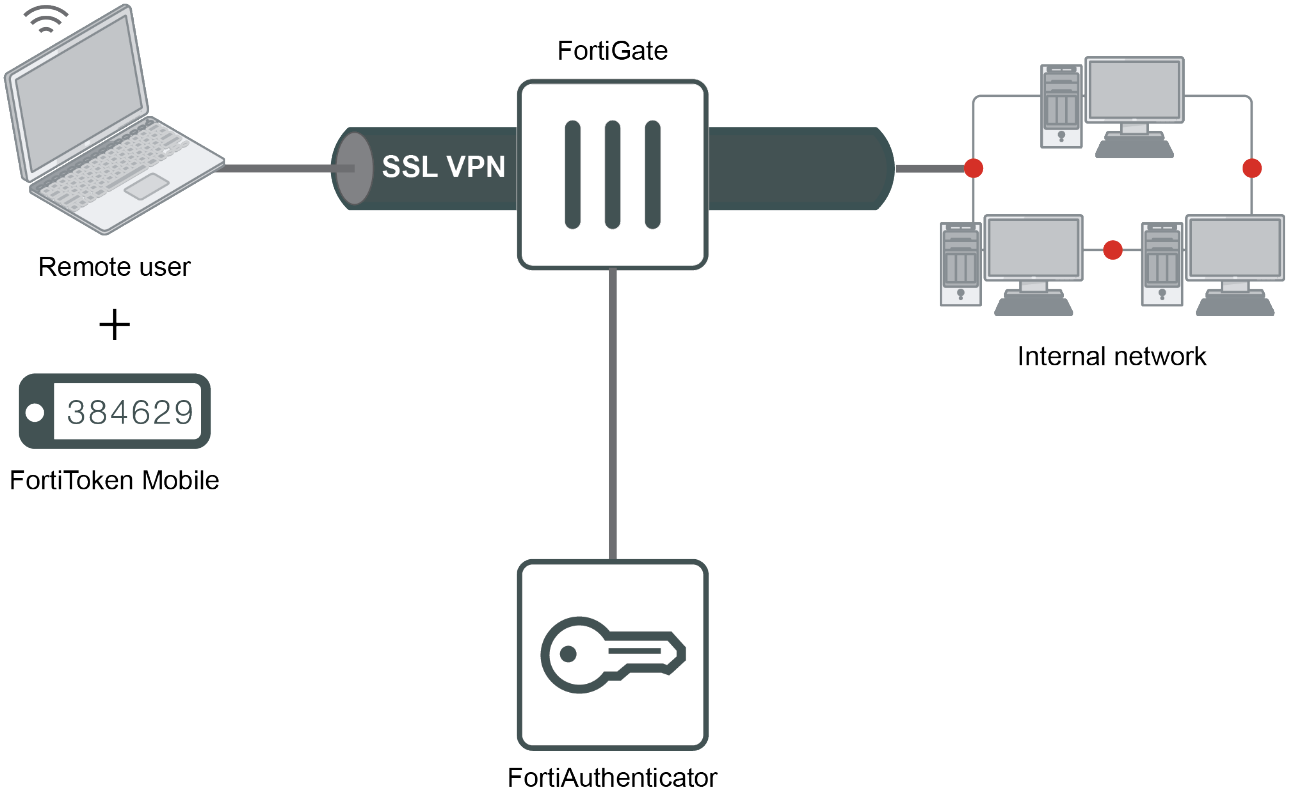
Mozilla does not recognize this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

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.

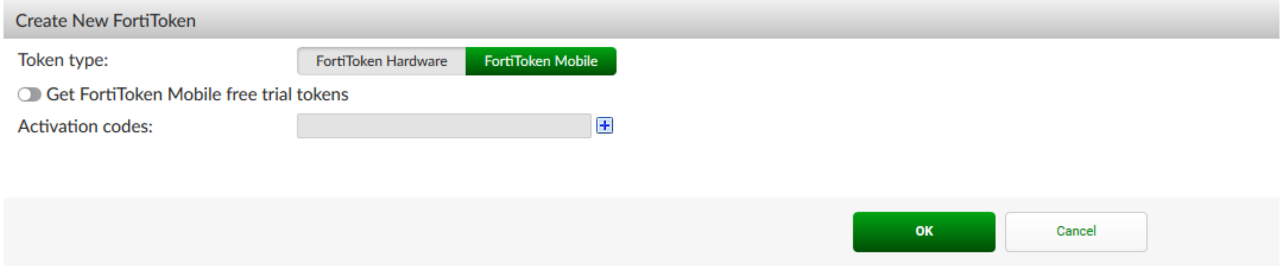
The interface that receives the approve/deny FTM push responses must have the *FortiToken Mobile API* service enabled.

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

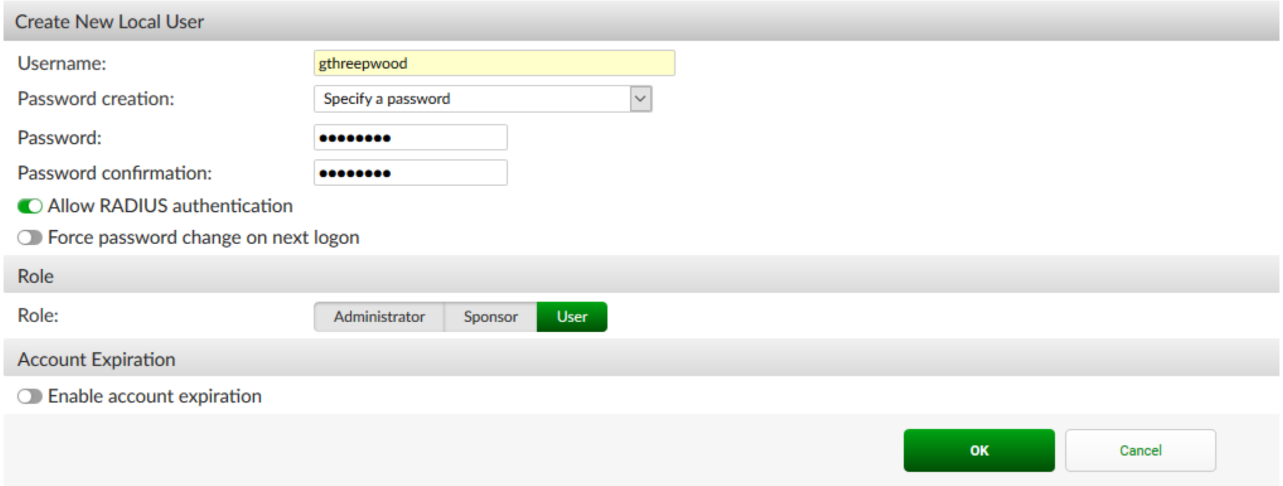
Activation codes:

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

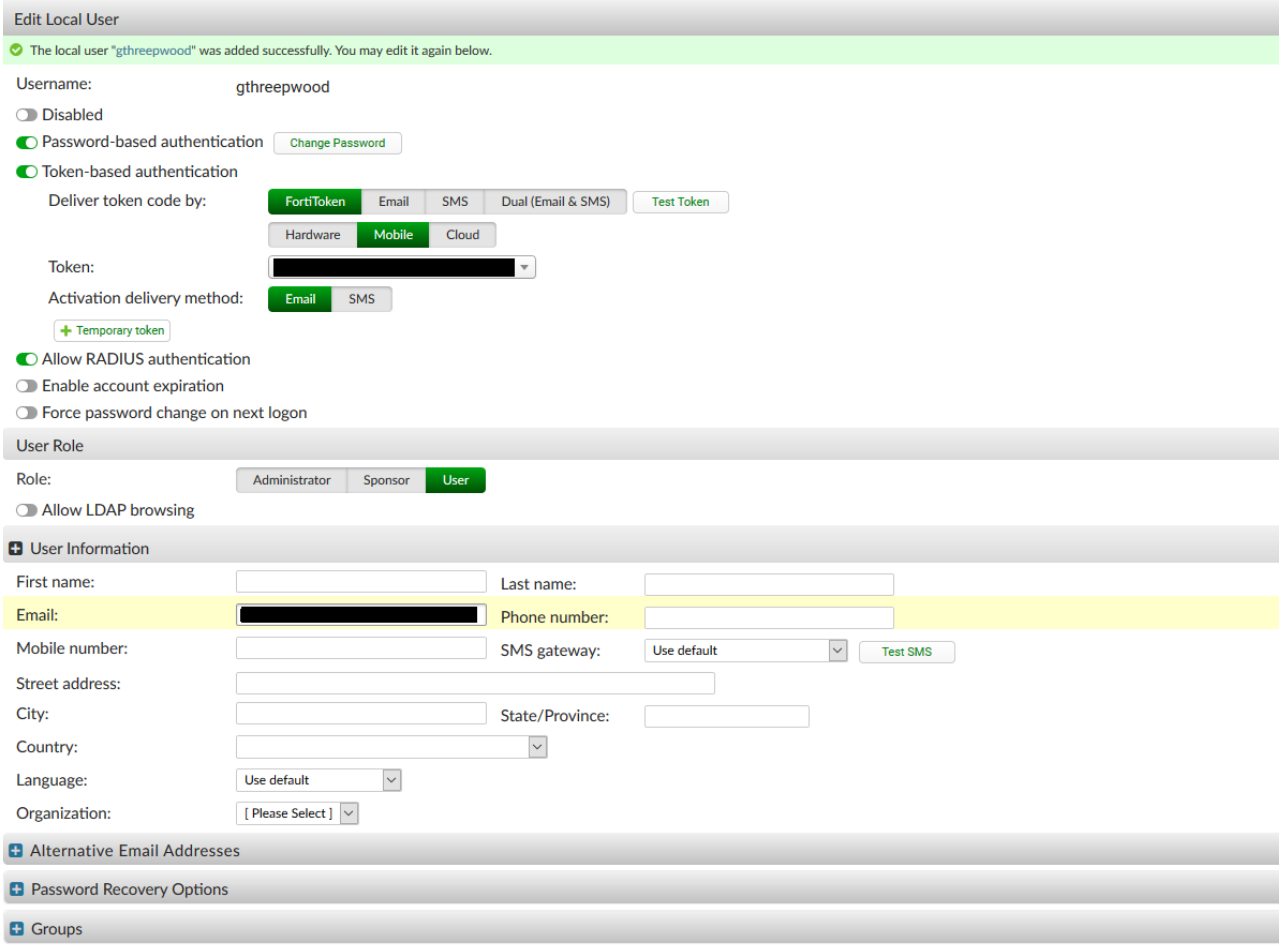
   Role

   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 [Change Password]

Token-based authentication

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

Hardware | Mobile | Cloud

Token: [redacted]

Activation delivery method: Email | SMS

+ Temporary token

Allow RADIUS authentication

Enable account expiration

Force password change on next logon

User Role

Role: Administrator | Sponsor | User

Allow LDAP browsing

User Information

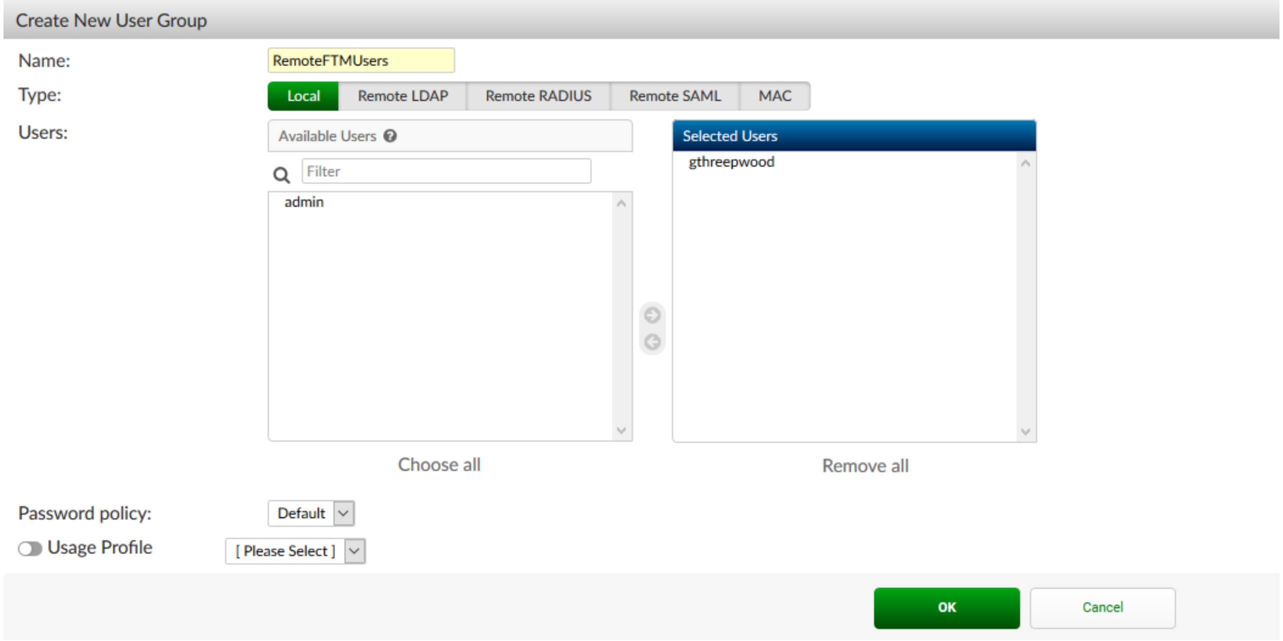
First name:		Last name:	
Email:	[redacted]	Phone number:	
Mobile number:		SMS gateway:	Use default [Test SMS]
Street address:			
City:		State/Province:	
Country:			
Language:	Use default		
Organization:	[Please Select]		

Alternative Email Addresses

Password Recovery Options

Groups

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

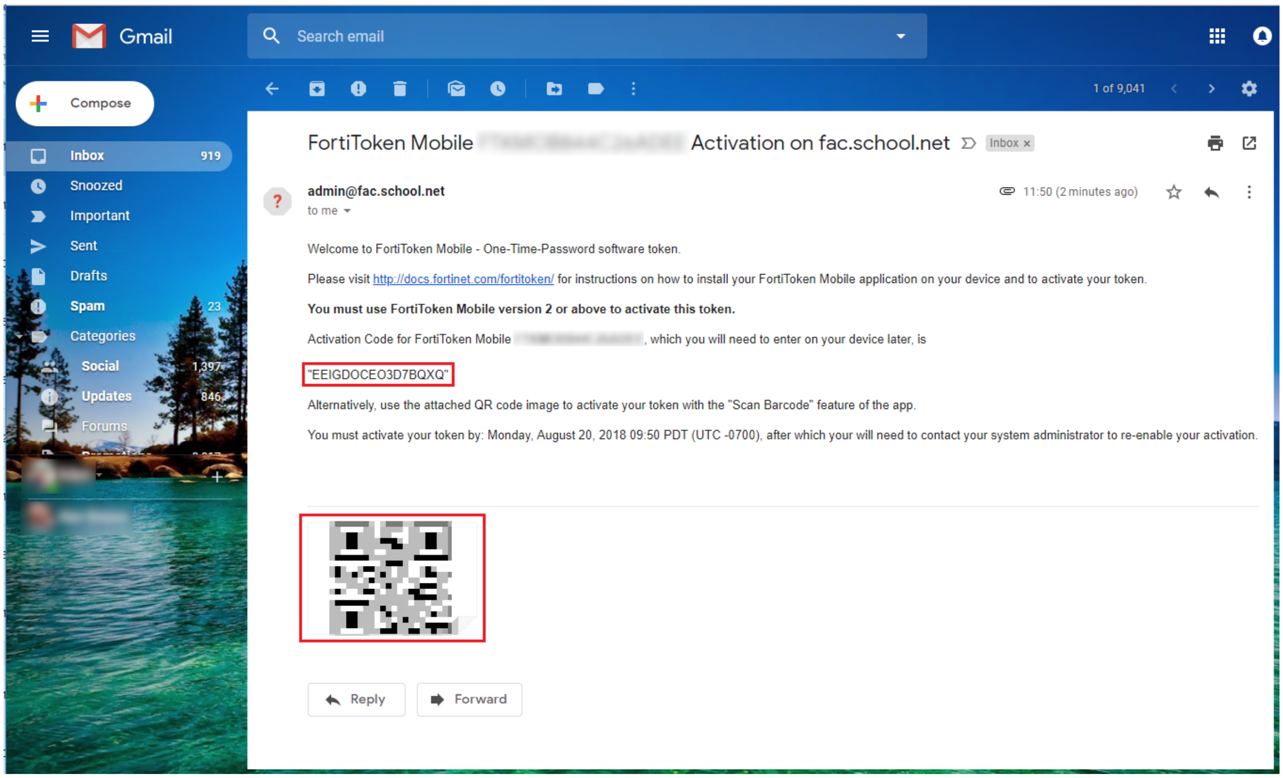
Users:

Available Users	Selected Users
admin	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.

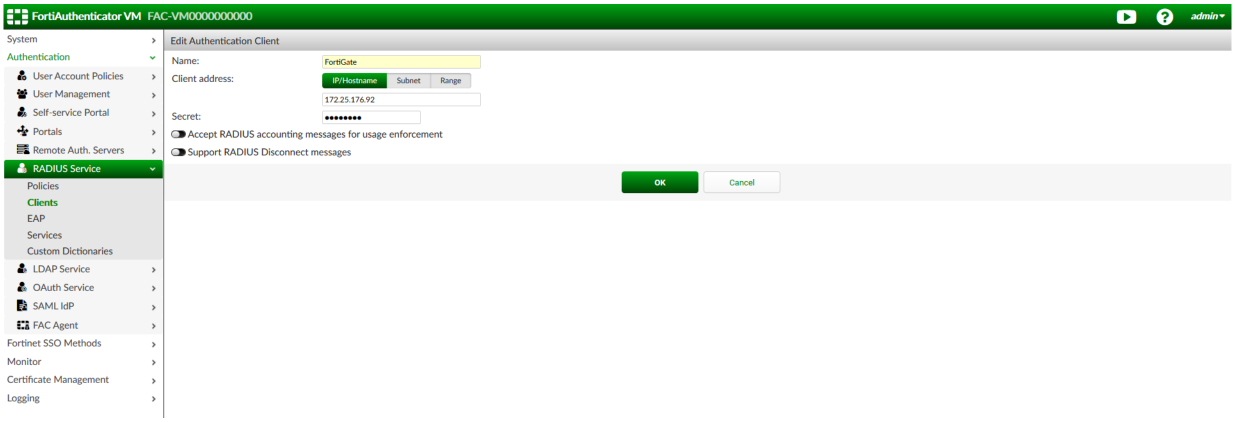
For more information, see the FortiToken Mobile user instructions.

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

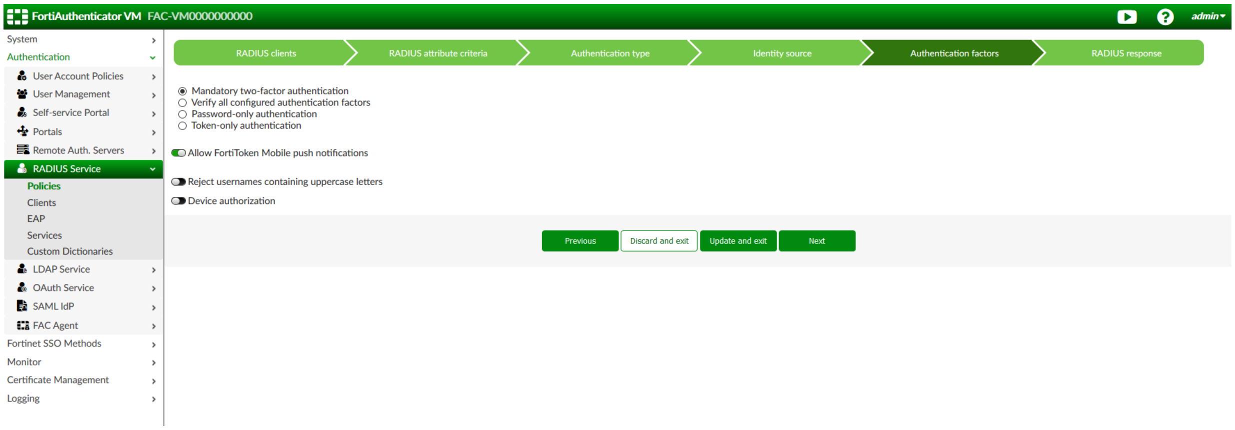
Secret: ••••••••

○ 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`.

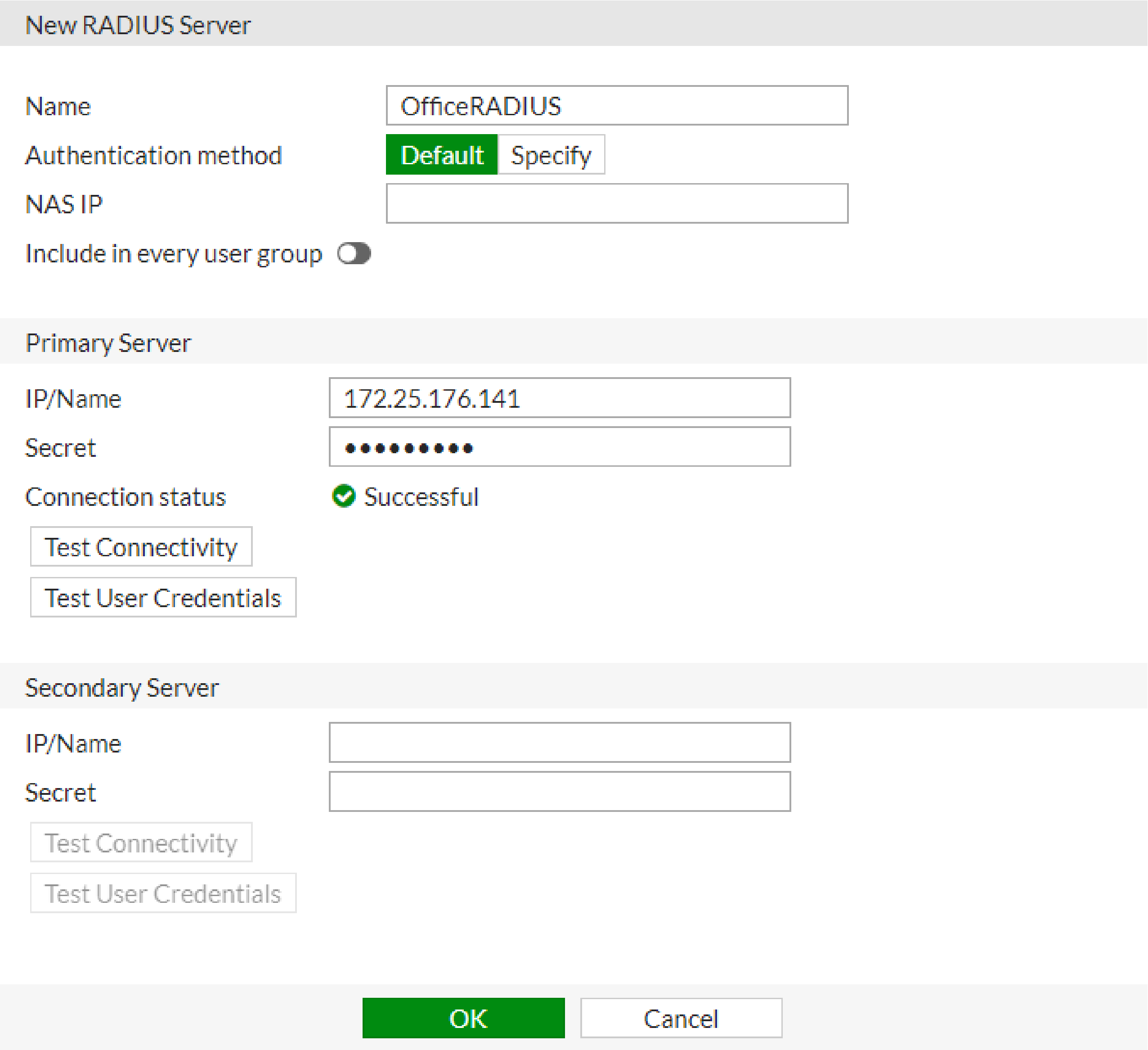
Connecting the FortiGate to the RADIUS server

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	○

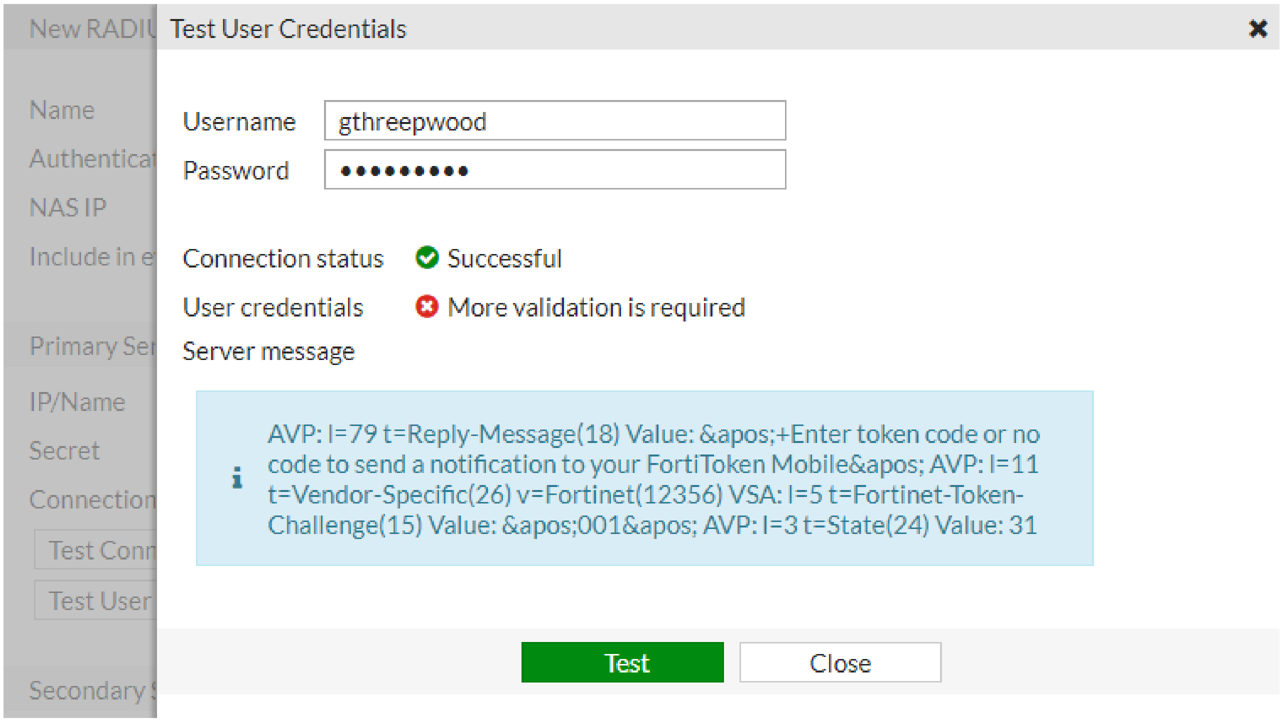
Primary Server

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*.



Test User Credentials

Username: gthreepwood

Password: ●●●●●●●●●

Connection status: ✓ Successful

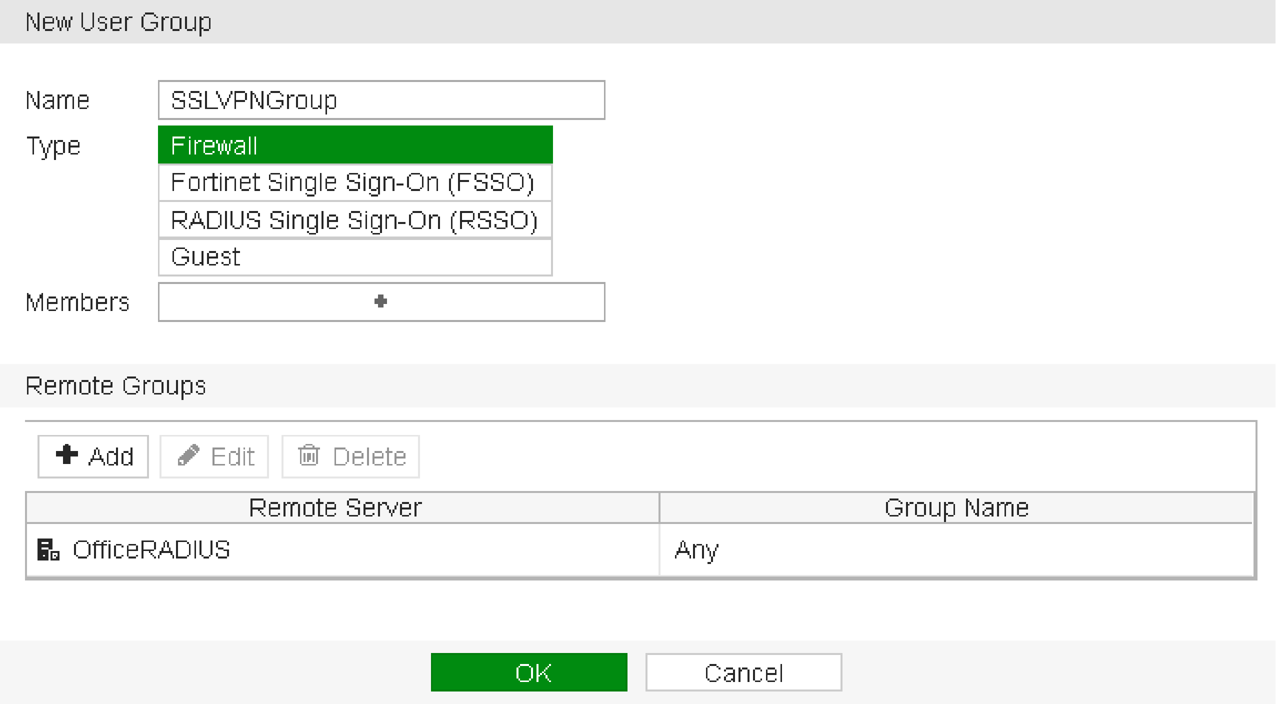
User credentials: ✖ More validation is required

Server message

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

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

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



New User Group

Name: SSLVPNGroup

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

Members

Remote Groups

Remote Server	Group Name
OfficeRADIUS	Any

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

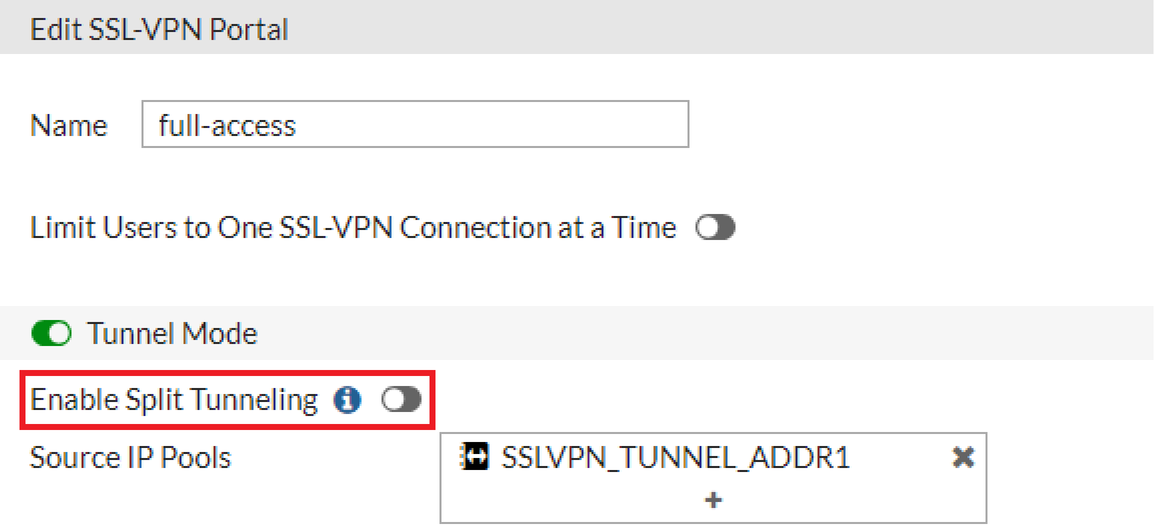
```
#config system global
```

```
    #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: off

Tunnel Mode: on

Enable Split Tunneling: off

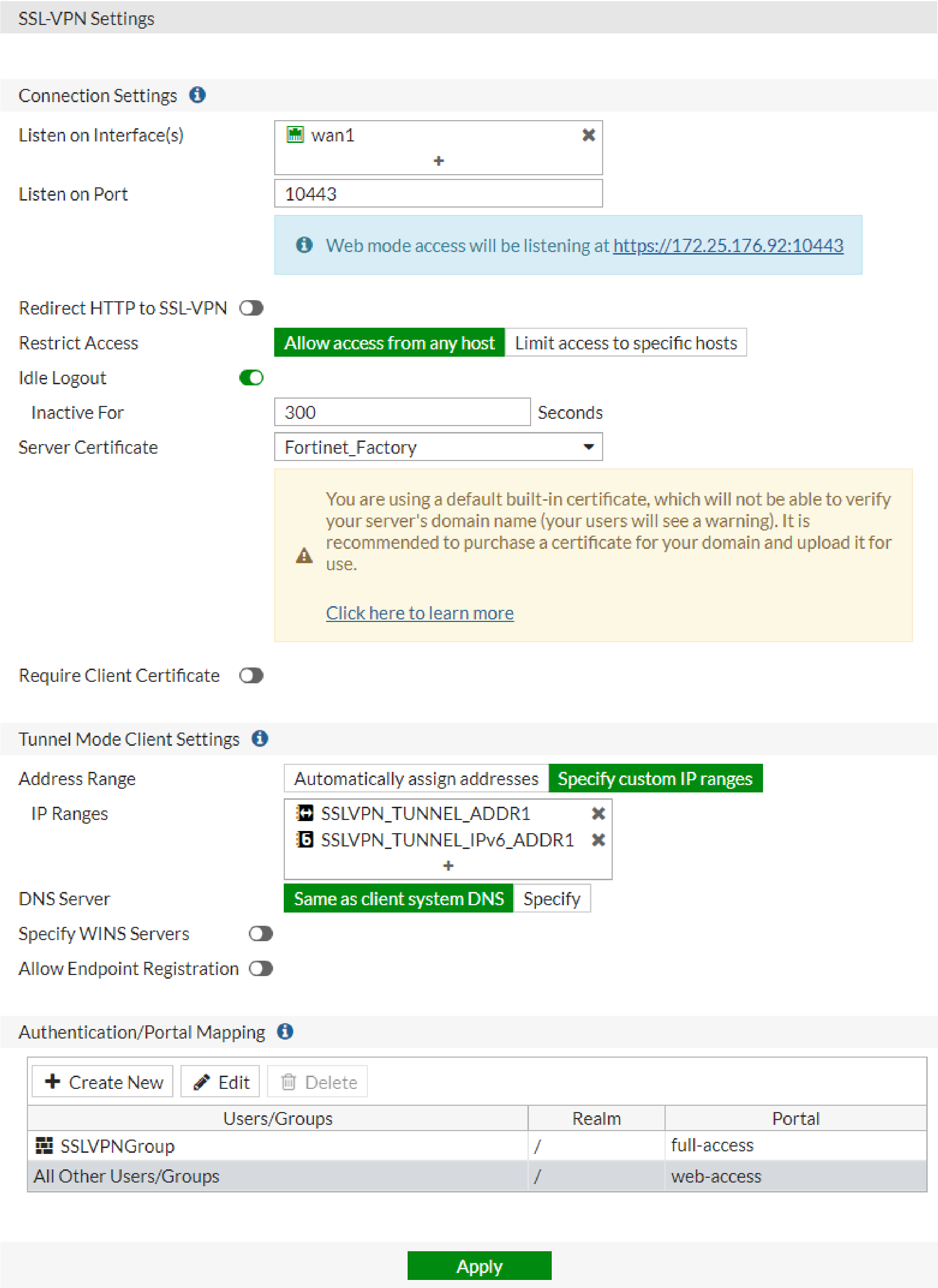
Source IP Pools: SSLVPN_TUNNEL_ADDR1

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: ○

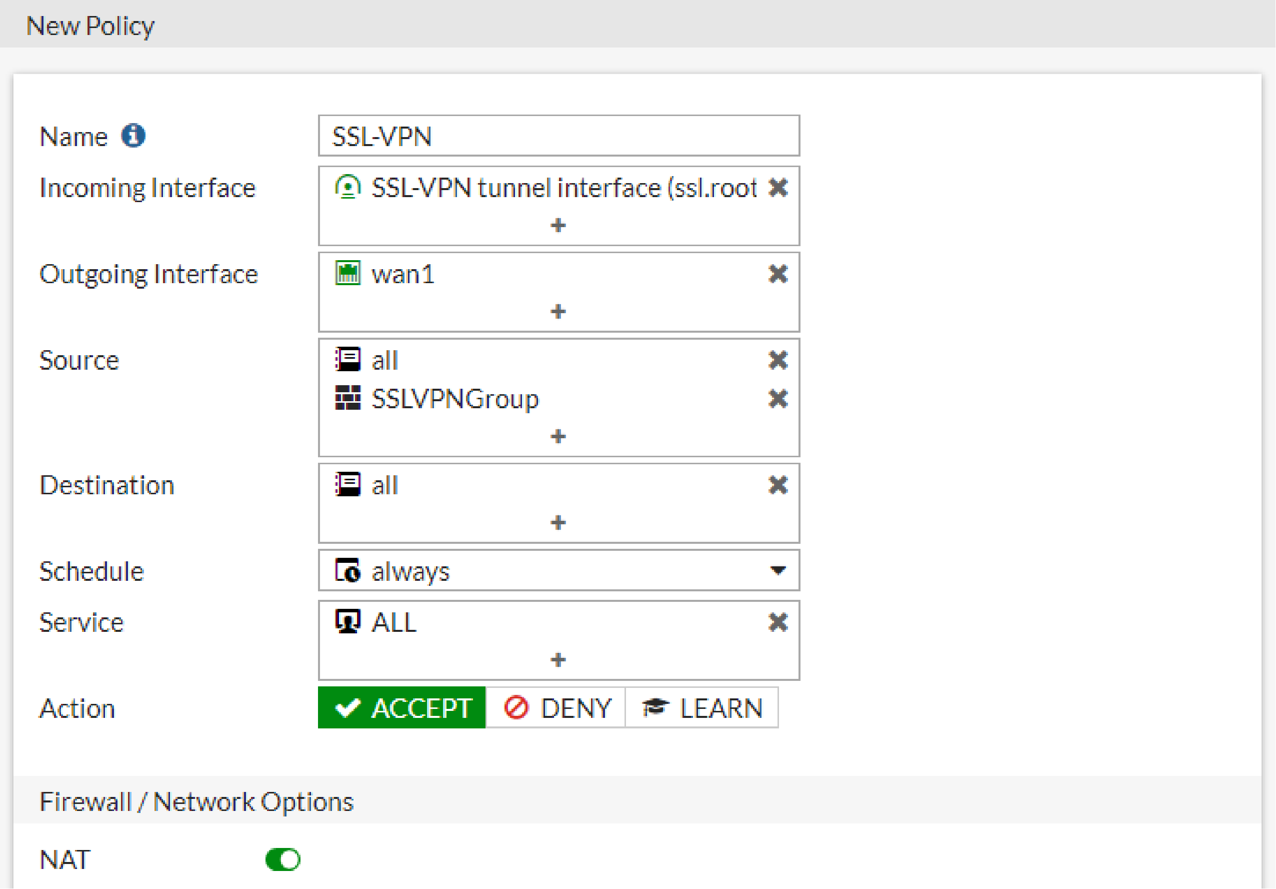
Authentication/Portal Mapping

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

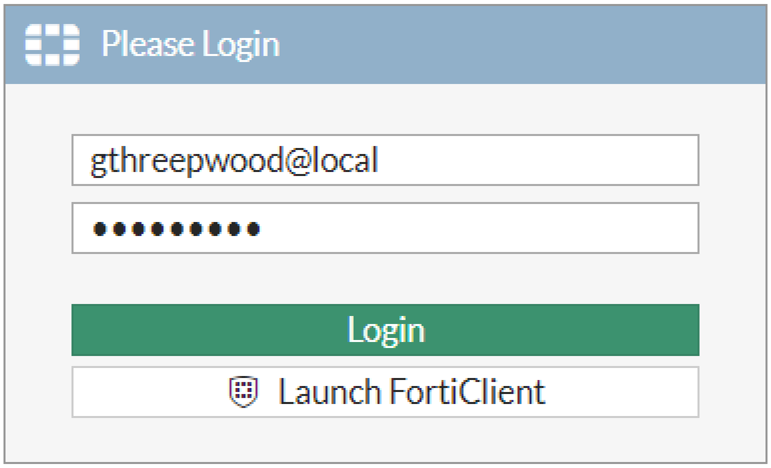
Name	SSL-VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.root
Outgoing Interface	wan1
Source	all SSLVPNGroup
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT

Firewall / Network Options

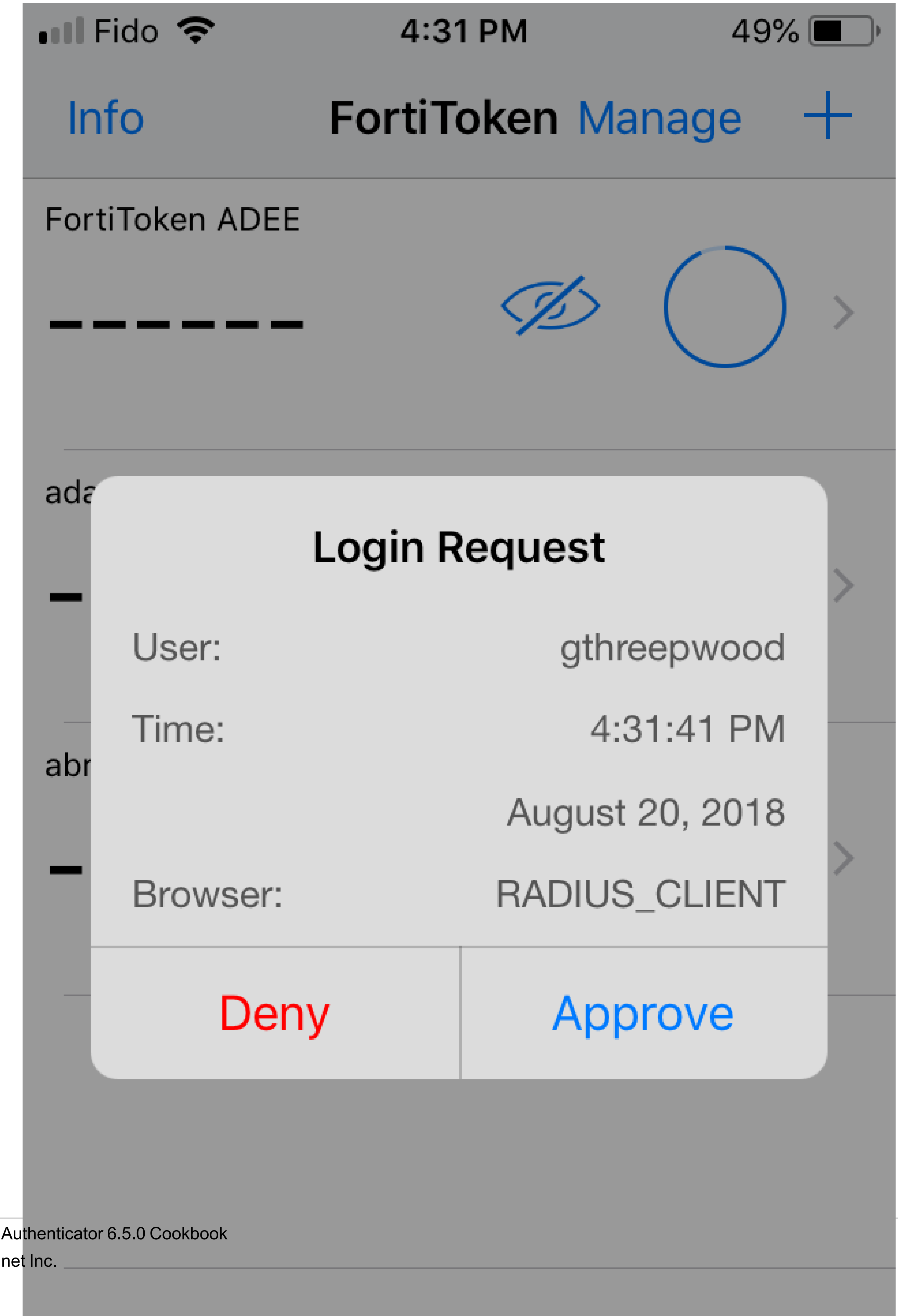
NAT ●

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.



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



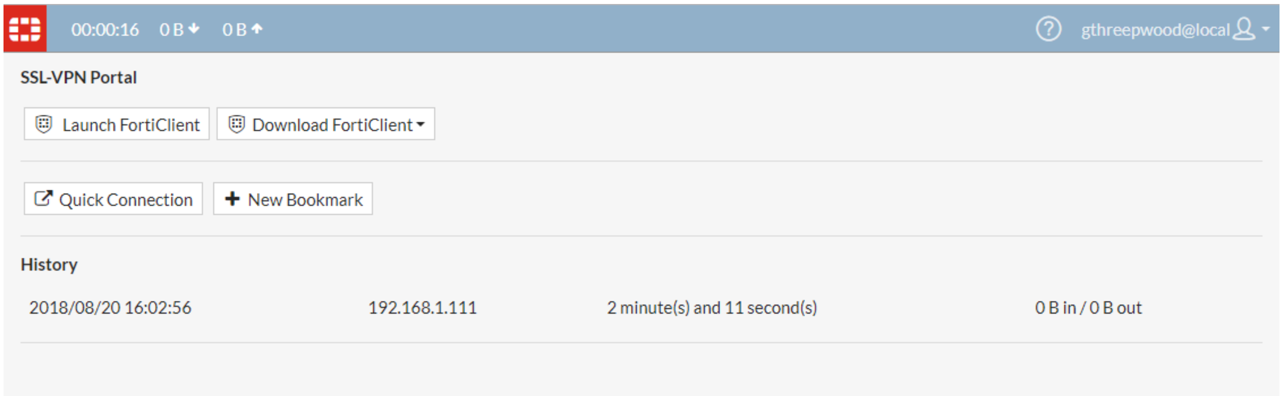
Login Request

User: gthreepwood

Time: 4:31:41 PM
August 20, 2018

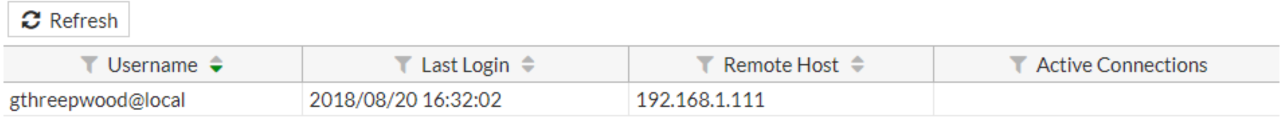
Browser: RADIUS_CLIENT

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



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.

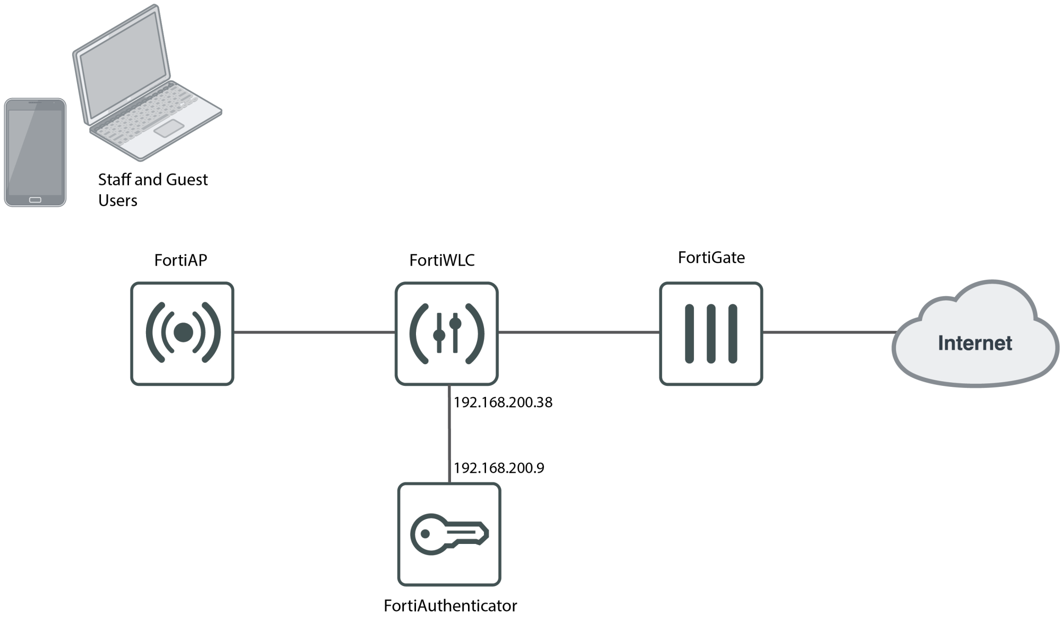


Username	Last Login	Remote Host	Active Connections
gthreepwood@local	2018/08/20 16:32:02	192.168.1.111	

Guest Portals

This section contains information about creating and using guest portals.

FortiAuthenticator as Guest Portal for FortiWLC

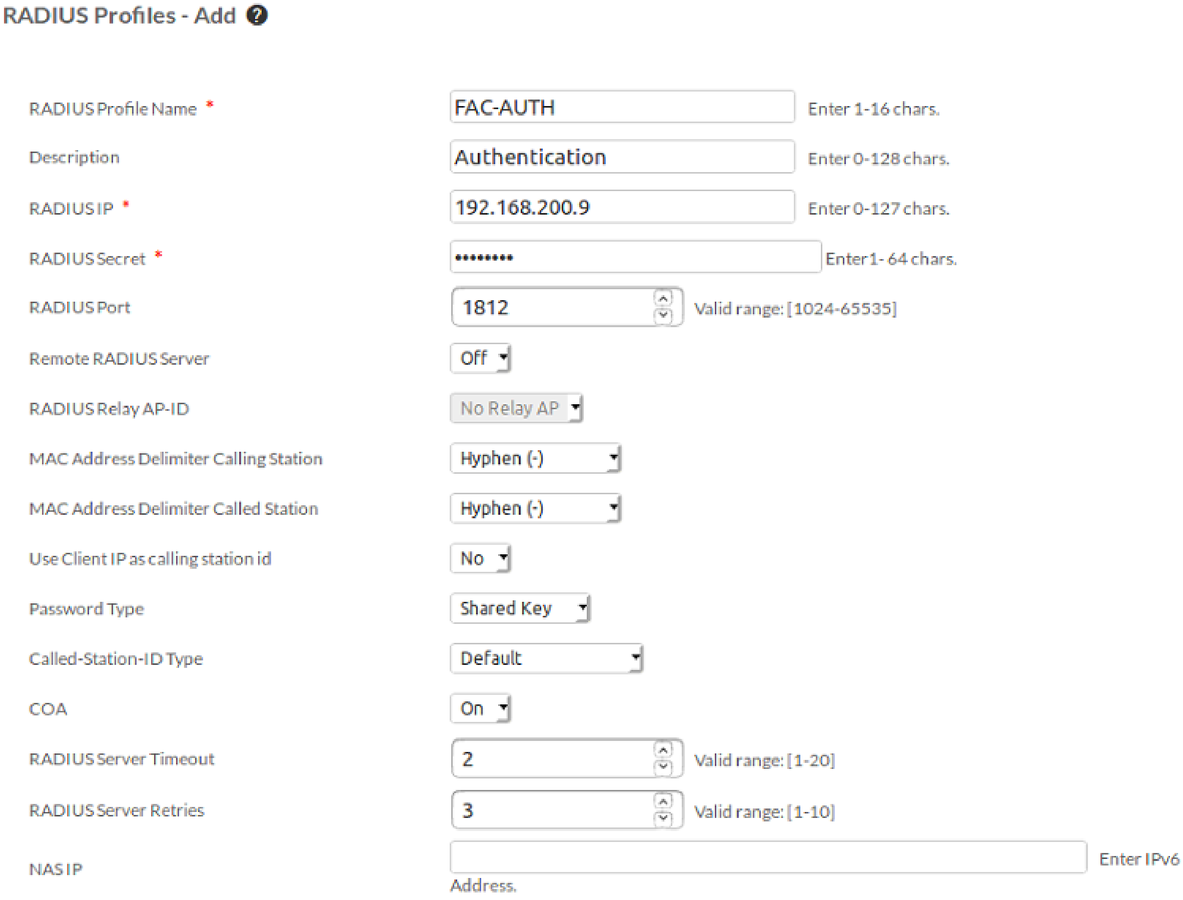


In this recipe we will use FortiAuthenticator as Guest Portal for users getting wireless connection provided by FortiWLC.

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.



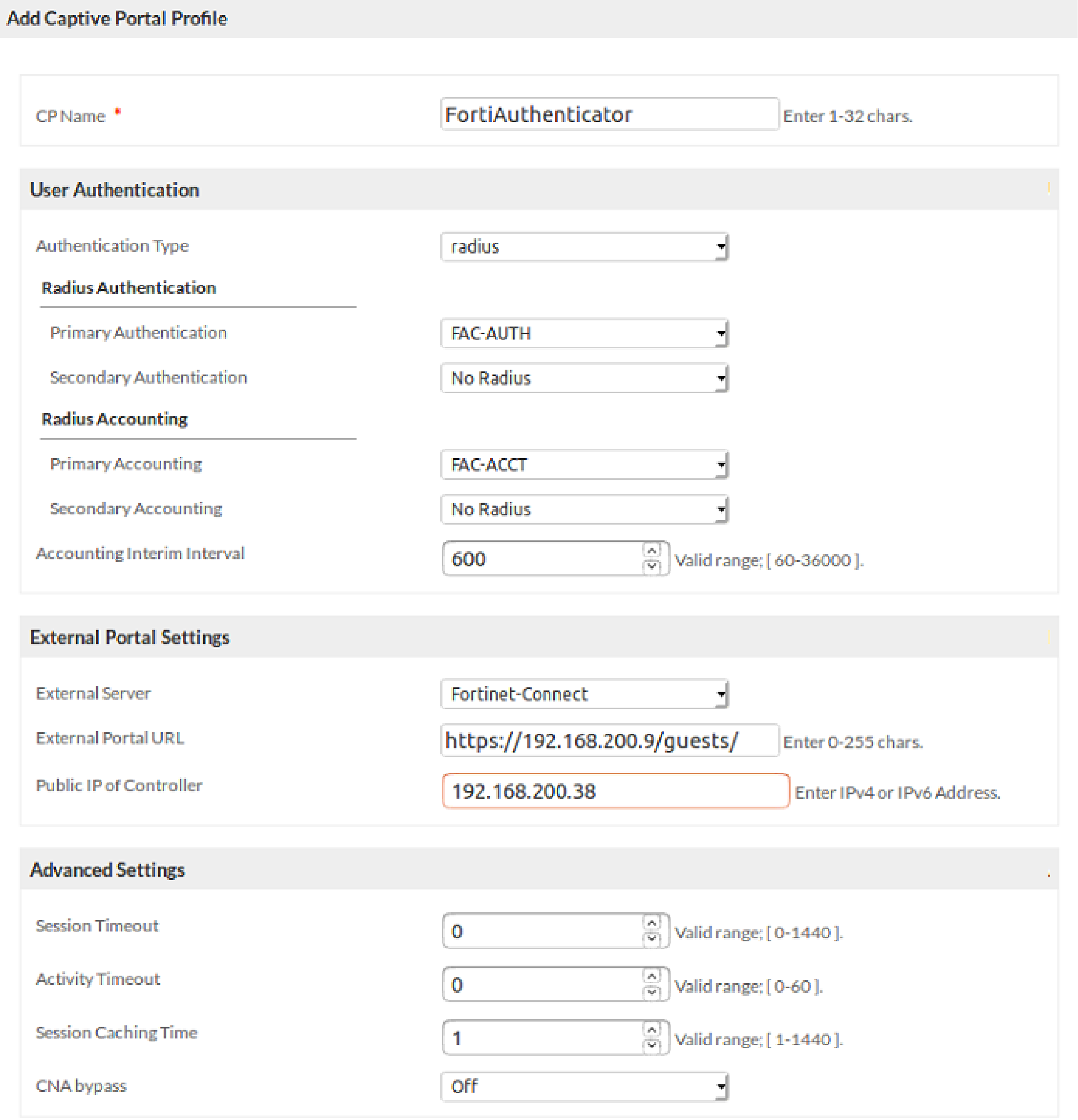
RADIUS Profiles - Add

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.

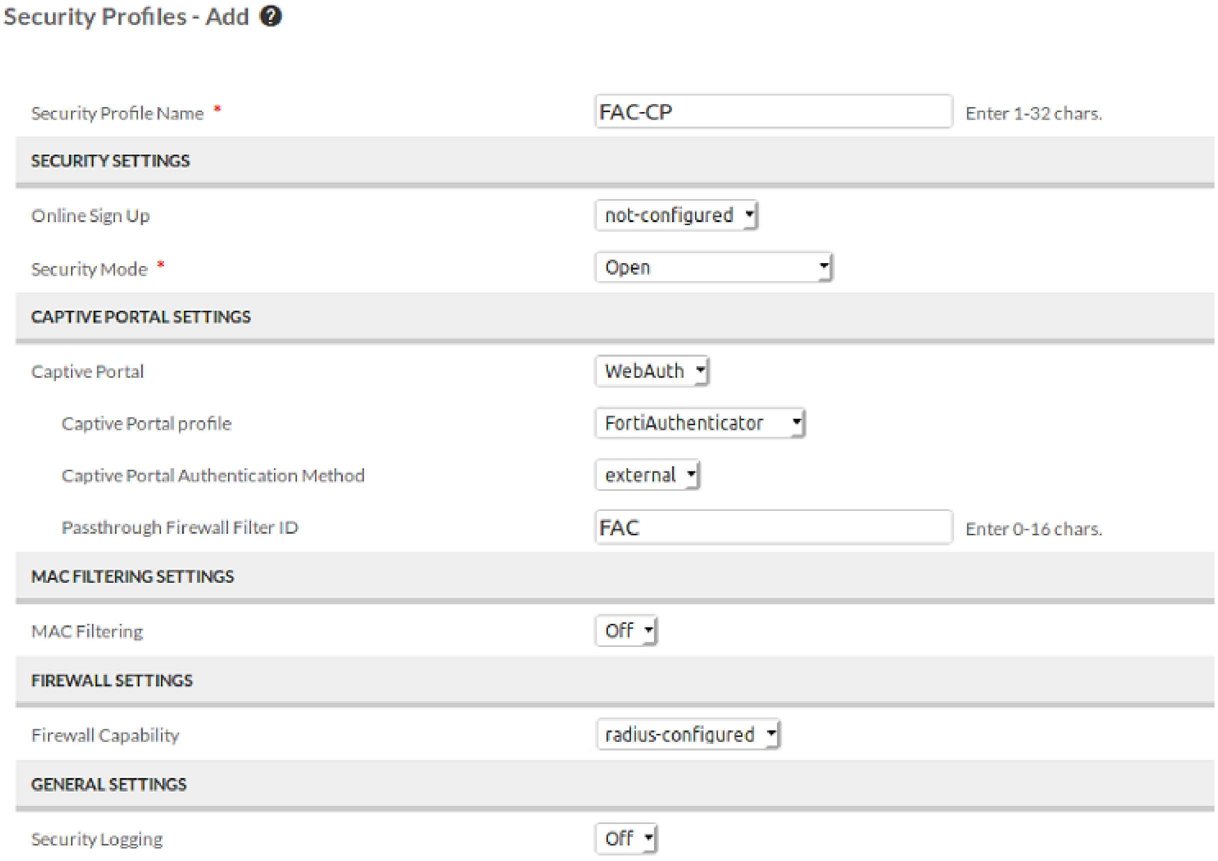
Advanced Settings

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.



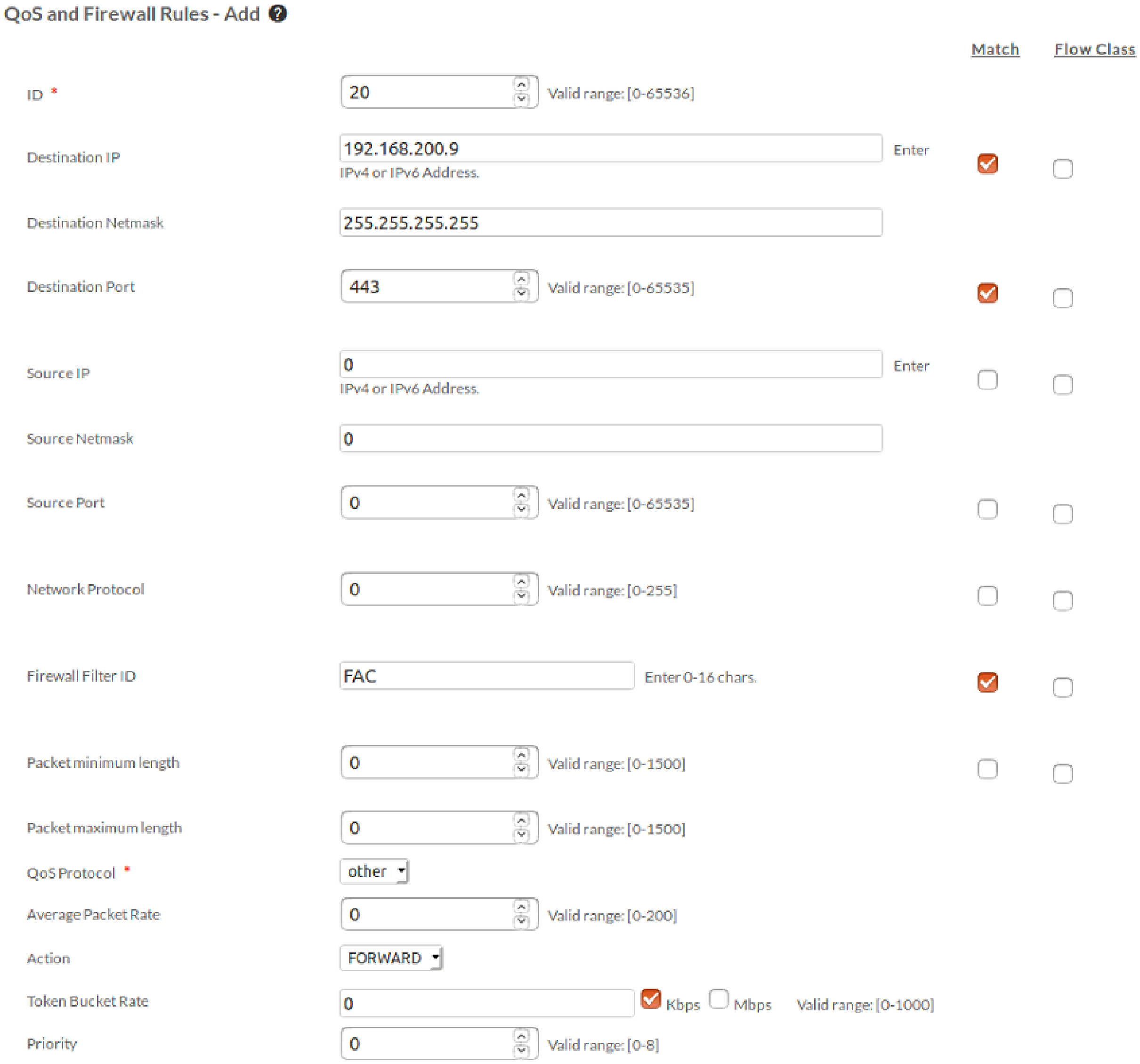
Security Profiles - Add

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.

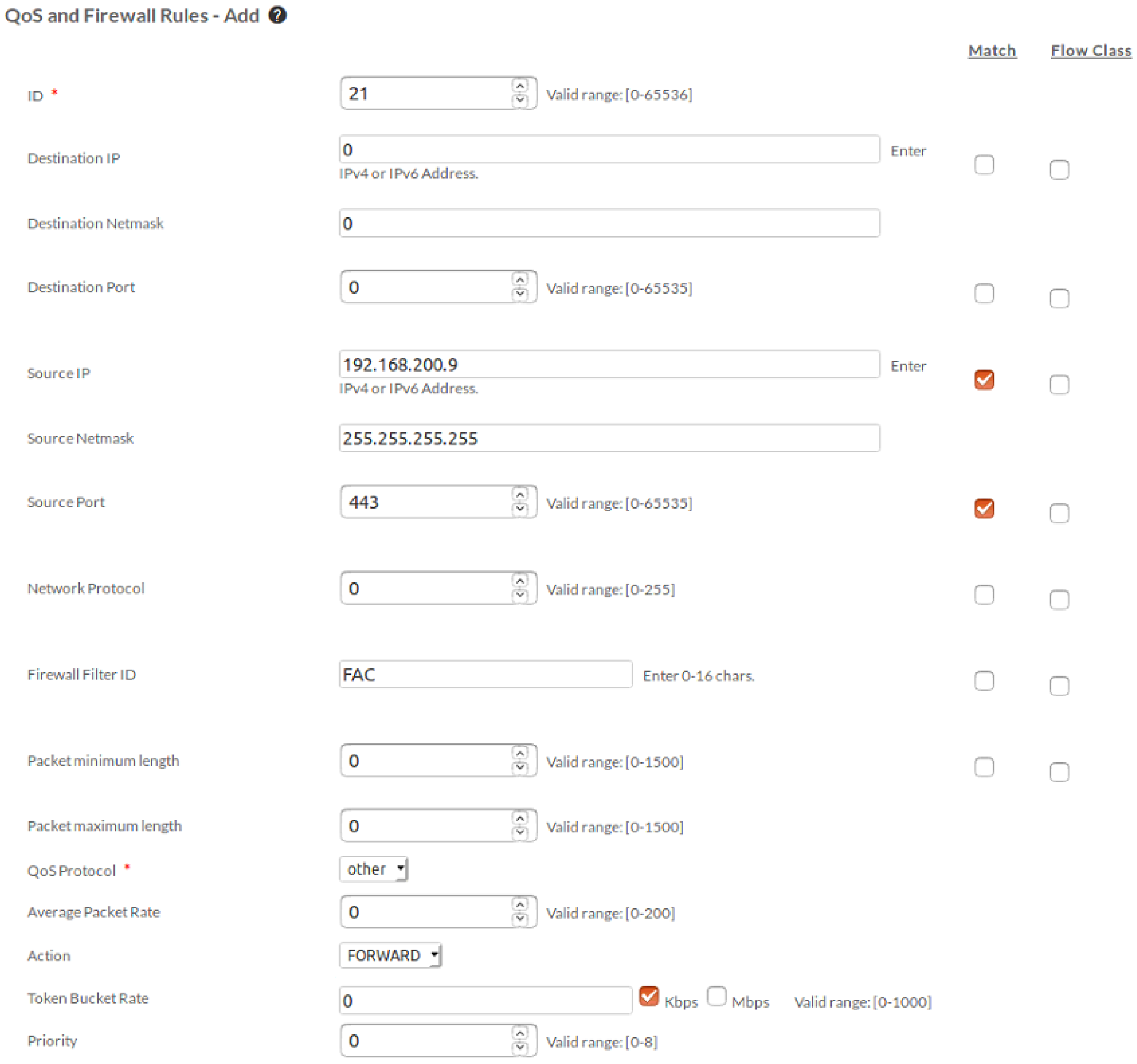


QoS and Firewall Rules - Add ❓

			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.



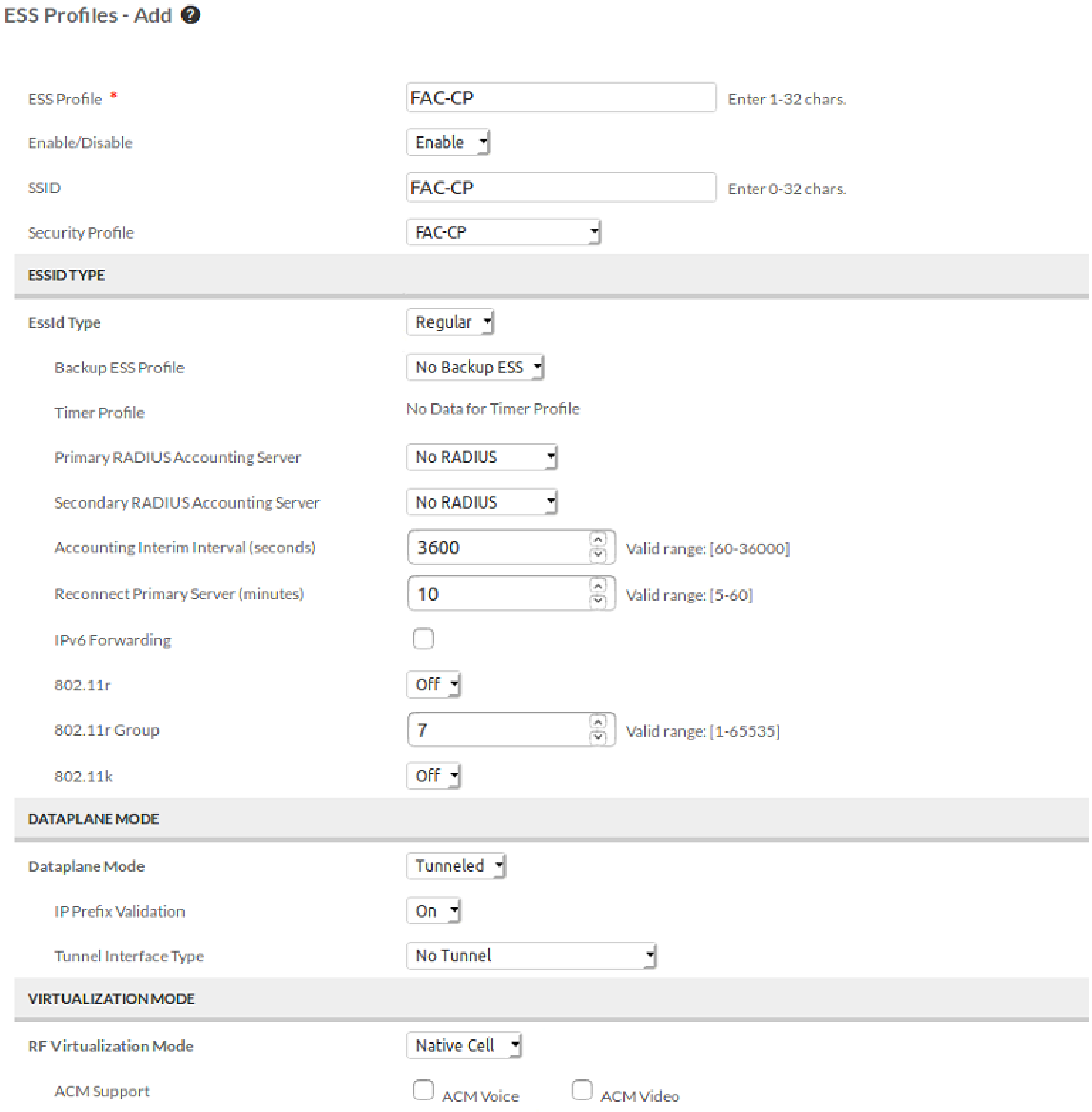
QoS and Firewall Rules - Add

			Match	Flow Class
ID *	21	Valid range: [0-65536]		
Destination IP	0	Enter IPv4 or IPv6 Address.	□	□
Destination Netmask	0			
Destination Port	0	Valid range: [0-65535]	□	□
Source IP	192.168.200.9	Enter IPv4 or IPv6 Address.	☑	□
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

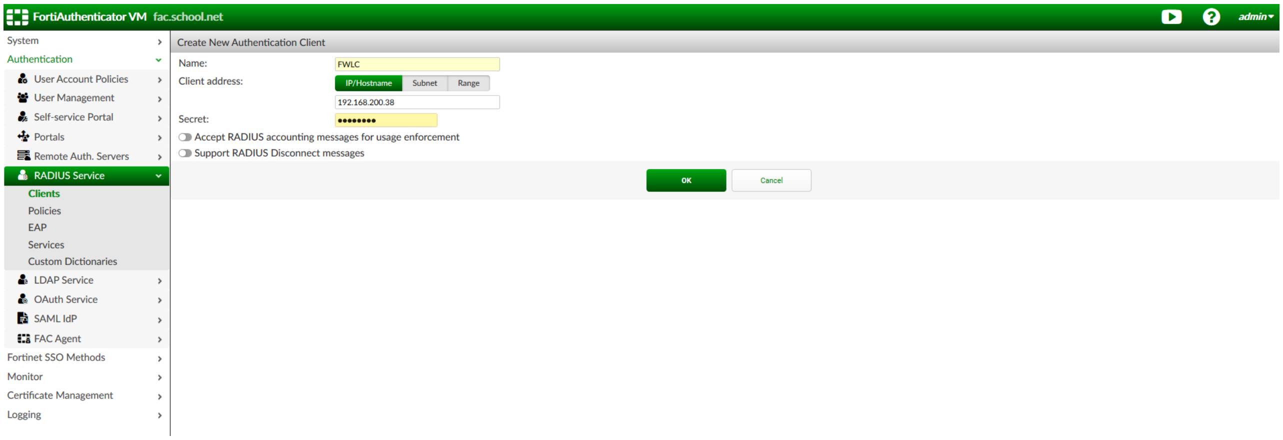
ESS Profile *	FAC-CP	Enter 1-32 chars.
Enable/Disable	Enable	
SSID	FAC-CP	Enter 0-32 chars.
Security Profile	FAC-CP	
ESSID TYPE		
EssId Type	Regular	
Backup ESS Profile	No Backup ESS	
Timer Profile	No Data for Timer Profile	
Primary RADIUS Accounting Server	No RADIUS	
Secondary RADIUS Accounting Server	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

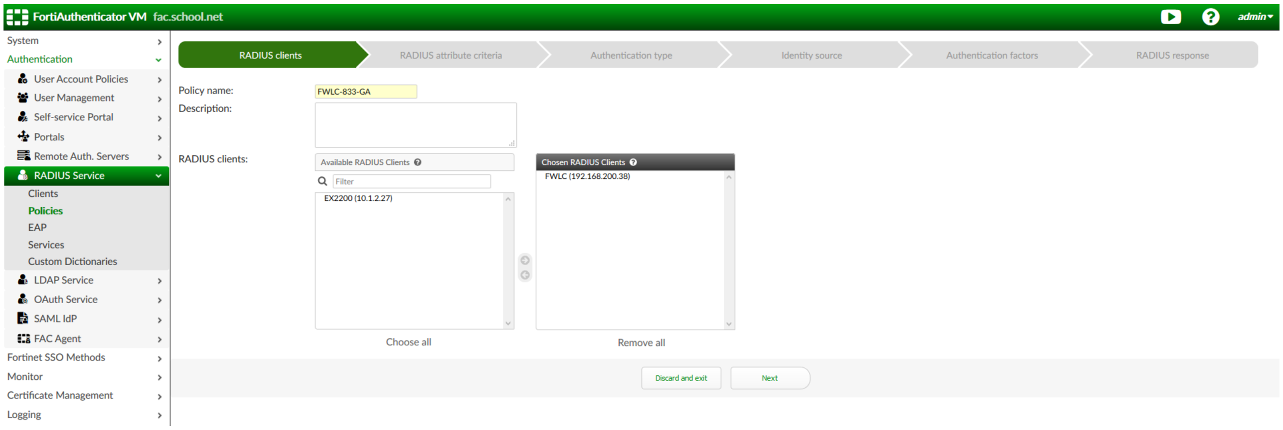
Secret: ●●●●●●●●●

○ 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:

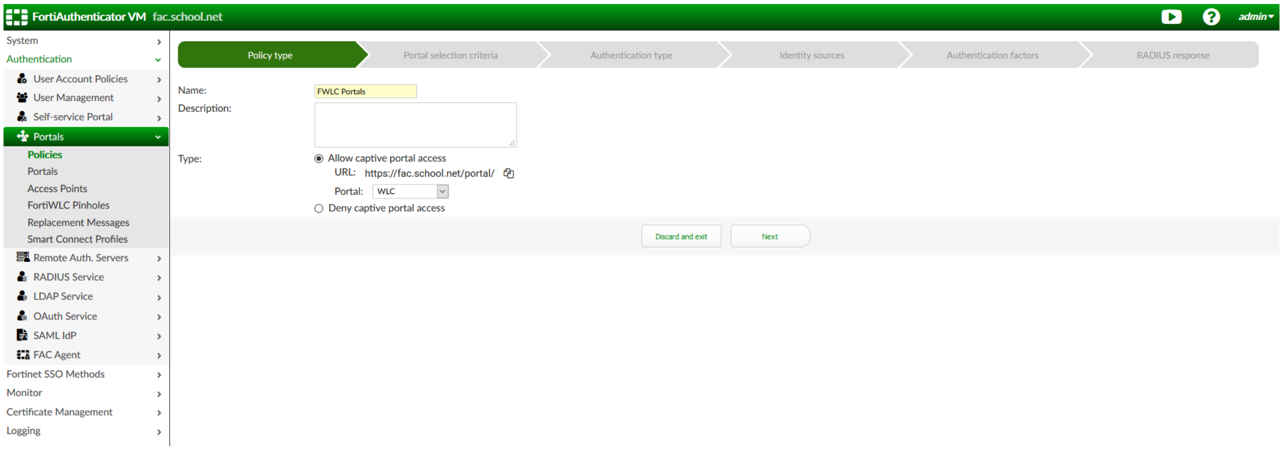
1. On the FortiAuthenticator, go to *Authentication* > *Portals* > *Portals*, and create a new portal.
2. Enter a name for the portal, and click *OK*.

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:

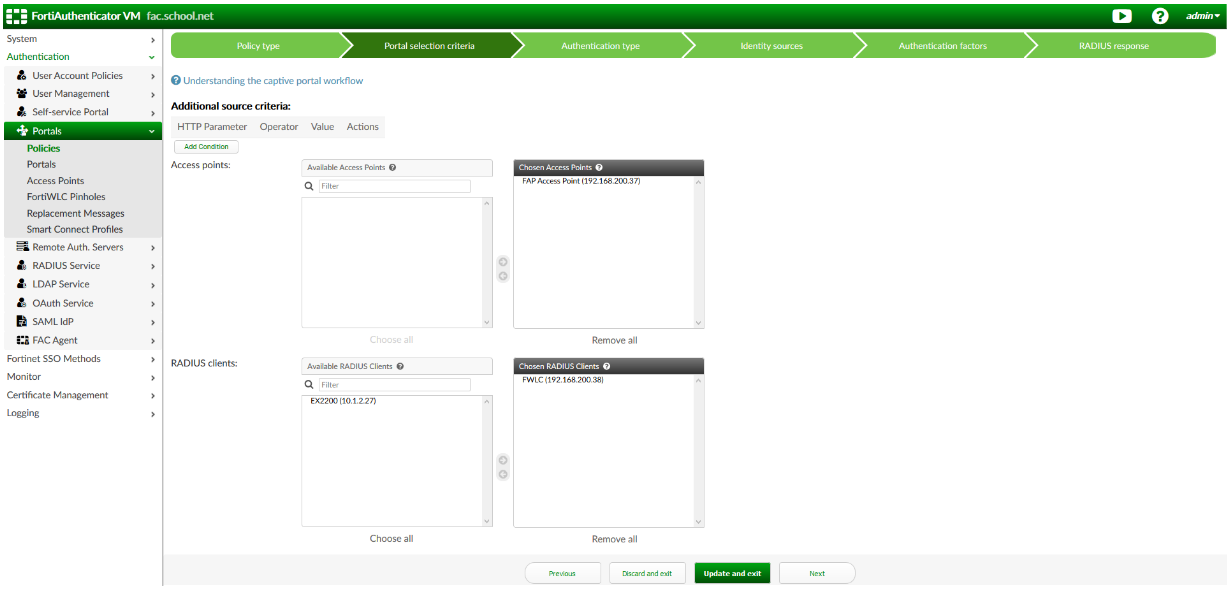
Type: ● Allow captive portal access

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:

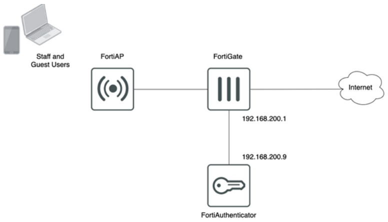
Available RADIUS Clients	Chosen RADIUS Clients
EX2200 (10.1.2.27)	FWLC (192.168.200.38)

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.

FortiAuthenticator as a Wireless Guest Portal for FortiGate



This recipe walks you through setting up FortiAuthenticator as a guest portal for users receiving a wireless connection from a FortiGate.

To set up FortiAuthenticator as a wireless guest portal:

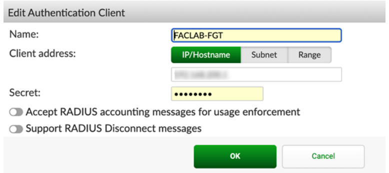
1. Configuring FortiGate as a RADIUS client on page 60.
2. Creating a user group on FortiAuthenticator for guest users on page 61.
3. Creating a guest portal on FortiAuthenticator on page 61.
4. Configuring an access point on FortiAuthenticator on page 62.
5. Configuring a captive portal policy on FortiAuthenticator on page 62.
6. Configuring FortiAuthenticator as a RADIUS server on FortiGate on page 64.
7. Creating a guest group on FortiGate on page 64.
8. Creating a wireless guest SSID on FortiGate on page 65.
9. Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet on page 67.
10. Configuring firewall authentication portal settings on FortiGate on page 67.

Configuring FortiGate as a RADIUS client

To configure FortiGate as a RADIUS client:

1. In *Authentication* > *RADIUS Service* > *Clients*, click *Create New*.
2. Enter a unique name for the RADIUS client and the IP address from which it will be connecting.
   This is the IP address of the RADIUS client itself, here, FortiGate, not the IP address of the end-user's device.
   You may enter a subnet or a range if this configuration applies to multiple FortiGates.

3. Enter a password for *Secret*.
   The secret is a pre-shared secure password that the device, here, FortiGate, uses to authenticate to FortiAuthenticator.
4. Click *OK* to save changes to the RADIUS client.



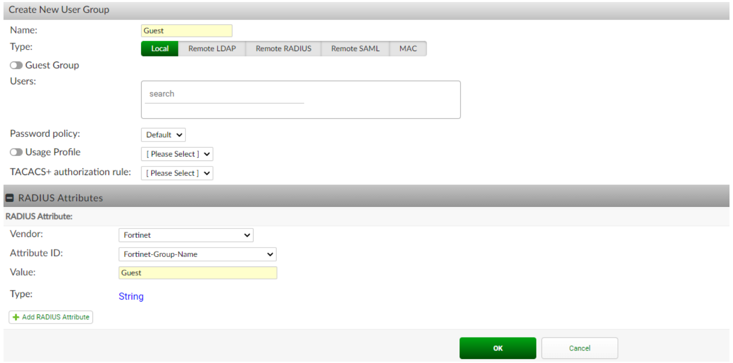
Edit Authentication Client

Name: FACLAB-FGT
Client address: IP/Hostname
[redacted]
Secret: ••••••••
Accept RADIUS accounting messages for usage enforcement
Support RADIUS Disconnect messages

Creating a user group on FortiAuthenticator for guest users

To create a user group:

1. Go to *Authentication* > *User Management* > *User Groups* and select *Create New*.
2. Enter a name for the group.
3. Select *Local* as the *Type*.
4. In *RADIUS Attributes* pane, select *Add RADIUS Attribute*:
   a. In *Vendor*, select *Fortinet*.
   b. In *Attribute ID*, select *Fortinet-Group-Name*.
   c. In *Value*, enter the group name that you will match on the FortiGate.
   FortiAuthenticator sends the RADIUS attribute to the FortiGate on successful authentication.
5. Click *OK*.



Create New User Group

Name: Guest
Type: Local
Guest Group
Users:
Password policy: Default
Usage Profile [Please Select]
TACACS+ authorization rule: [Please Select]

RADIUS Attributes

RADIUS Attribute:
Vendor: Fortinet
Attribute ID: Fortinet-Group-Name
Value: Guest
Type: String

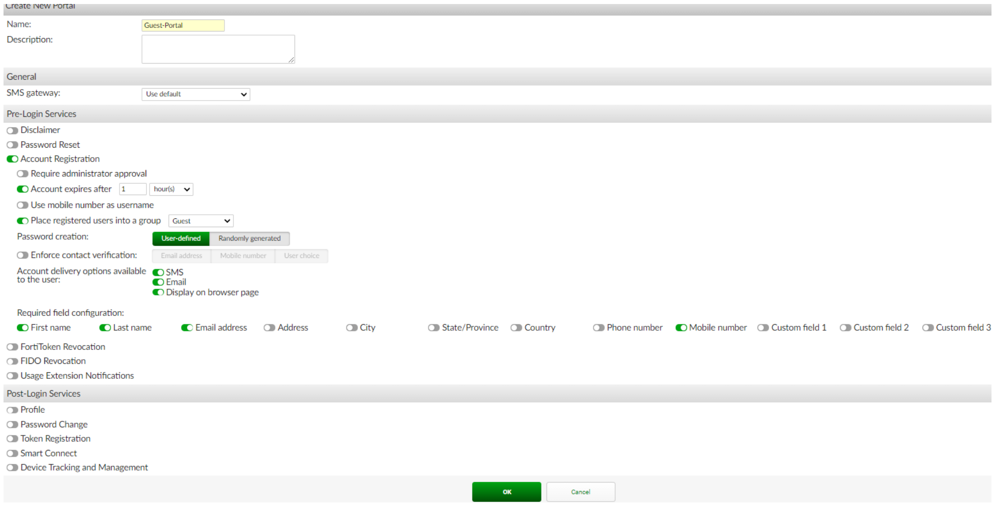
Creating a guest portal on FortiAuthenticator

To create a guest portal:

1. Go to *Authentication* > *Portals* > *Portals* and select *Create New*.
2. Enter a name for the portal.
3. Enable *Account Registration* to allow guest users to create an account.
4. In the *Account Registration* toggle, enable *Place registered users into a group*, and select the user group created in Creating a user group.
   Users are made members of the group when they create an account.

You can configure additional settings as required. For instance, you may want to enable account expiry and enforcing contact verification using Email or SMS.

5. Click *OK*.



Create New Portal

Name: Guest-Portal

Description:

General

SMS gateway: Use default

Pre-Login Services

- ○ Disclaimer
- ○ Password Reset
- ● Account Registration
  - ○ Require administrator approval
  - ● Account expires after 1 hour(s)
  - ○ Use mobile number as username
  - ● Place registered users into a group Guest
  - Password creation: [✓ User-defined] Randomly generated
  - ○ Enforce contact verification: Email address | Mobile number | User choice
  - Account delivery options available to the user: ● SMS ● Email ● Display on browser page
  - 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
- ○ FortiToken Revocation
- ○ FIDO Revocation
- ○ Usage Extension Notifications

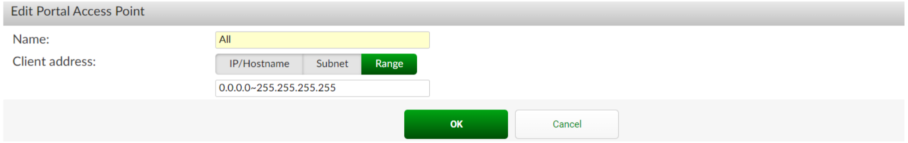
Post-Login Services

- ○ Profile
- ○ Password Change
- ○ Token Registration
- ○ Smart Connect
- ○ Device Tracking and Management

Configuring an access point on FortiAuthenticator

To configure an access point:

1. Go to *Authentication* > *Portals* > *Access Points* and select *Create New*.
2. Enter a name for the access point.
3. In *Client address*, select *Range*, and enter `0.0.0.0-255.255.255.255`.
4. Click *OK*.



Edit Portal Access Point

Name: All

Client address: IP/Hostname | Subnet | [✓ Range]

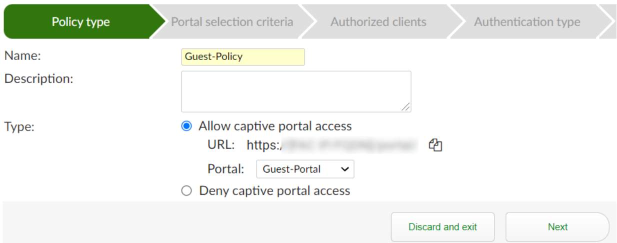
0.0.0.0-255.255.255.255

Configuring a captive portal policy on FortiAuthenticator

To configure an allow access captive portal policy:

1. Go to *Authentication* > *Portals* > *Policies*, click *Captive Portal* and *Create New*.
2. In the *Policy type* tab:
   a. Enter a name for the policy. Optionally, enter a description for the policy.
   b. In *Type*, select *Allow captive portal access*. Copy the URL and keep it on Notepad. The URL needs to be entered in the FortiGate configuration later.
   c. Choose a portal created in Creating a guest portal on FortiAuthenticator on page 61.

   d. Click *Next*.



Name: Guest-Policy

Description:

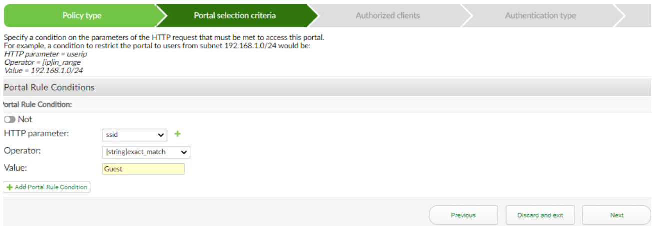
Type: ● Allow captive portal access

URL: https:/[redacted]

Portal: Guest-Portal

○ Deny captive portal access

3. In the *Portal selection criteria* tab:
   a. In the *HTTP parameter* dropdown, select *ssid* to match.
   b. In the *Operator* dropdown, *select [string]exact_match*.
   c. In *Value*, enter the name of the SSID configured on the FortiGate. Here, `Guest`.
   d. Click *Next*.



Specify a condition on the parameters of the HTTP request that must be met to access this portal.
For example, a condition to restrict the portal to users from subnet 192.168.1.0/24 would be:
HTTP parameter = userip
Operator = [ip]in_range
Value = 192.168.1.0/24

Portal Rule Conditions

'ortal Rule Condition:

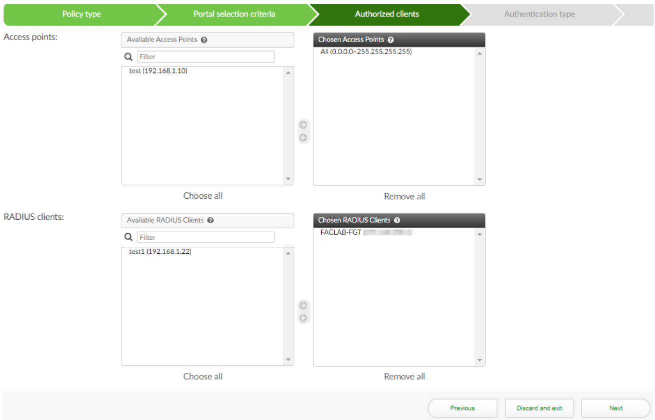
Not

HTTP parameter: ssid

Operator: [string]exact_match

Value: Guest

4. In the *Authorized clients* tab:
   a. From *Access points*, select the access point defined in Access points.
   b. From *RADIUS clients*, select the FortiGate RADIUS client defined in RADIUS clients.
   c. Click *Next*.



Access points:

Available Access Points: test (192.168.1.10)

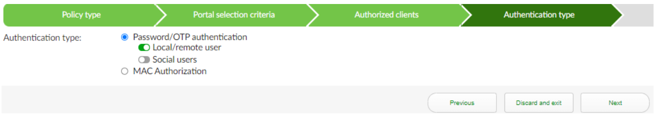
Chosen Access Points: All (0.0.0.0~255.255.255.255)

RADIUS clients:

Available RADIUS Clients: test1 (192.168.1.22)

Chosen RADIUS Clients: FACLAB-FGT [redacted]

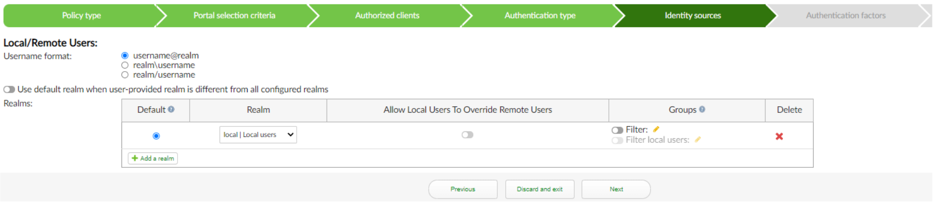
5. In the *Authentication type* tab, select *Password/OTP authentication*, then enable *Local/remote user* to verify credentials against one of the local or remote user accounts, and click *Next*.



Authentication type: ● Password/OTP authentication
- Local/remote user (enabled)
- Social users
○ MAC Authorization

6. In the *Identity sources* tab:
   a. For *Username format*, select *username@realm*.
   b. For *Realms*, select *local* realm. Optionally, enable *Filter*, click the pen icon, and from *Available User Groups*, move the group created in User Group to *Chosen User Groups*.

c. Click *Next*.



Local/Remote Users:

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

Use default realm when user-provided realm is different from all configured realms

Realms:

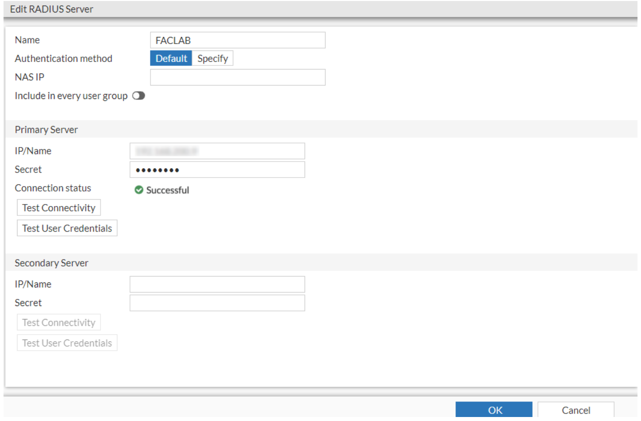
Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	local | Local users		Filter: Filter local users:	✖

7. In the *Authentication Factors* tab, click *Next*.
8. In the *RADIUS response* tab, review the policy, and click *Save and exit*.

Configuring FortiAuthenticator as a RADIUS server on FortiGate

To configure FortiGate authentication settings:

1. Go to *User & Authentication > RADIUS Servers* and click *Create New*.
2. Enter a name for the RADIUS server.
3. For *Authentication method*, select *Default*.
4. In *IP/Name*, enter the IP address or DNS name of the RADIUS server.
5. In *Secret*, enter the shared secret key.
   The secret is the same as the one used when setting up the RADIUS client, here, FortiGate.
6. Click *Test Connectivity* to test the connection to the server, and ensure that the connection status is *Successful*.
7. Click *OK* to save changes.



Name: FACLAB

Authentication method: [✓ Default] Specify

NAS IP:

Include in every user group

Primary Server

IP/Name: [redacted]

Secret: ••••••••

Connection status: ✓ Successful

Secondary Server

IP/Name:

Secret:

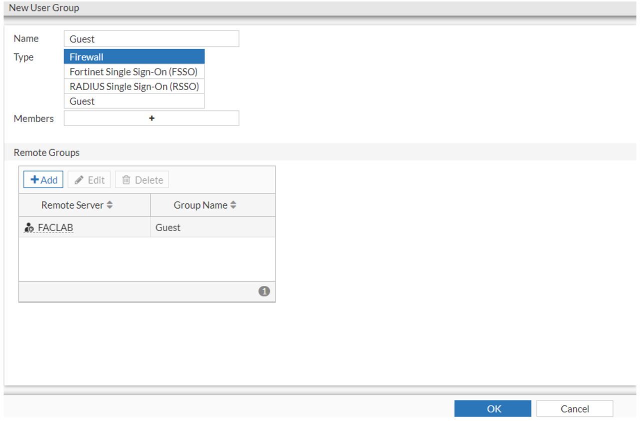
Creating a guest group on FortiGate

To create a guest group:

1. Go to *User & Authentication > User Groups* and click *Create New*.
2. Enter a name for the group.
3. In *Type*, select *Firewall*.

4. In *Remote Groups*, select *Add*, and then select the remote server created in Remote Server. Click *OK*.
   Optionally, you may specify the group to be matched on the remote server. The group name must be configured as a RADIUS attribute on the group configured on FortiAuthenticator. See Groups.

   The RADIUS attribute will be sent to the FortiGate by the FortiAuthenticator on successful authentication.
5. Click *OK*.



New User Group

Name: Guest

Type: Firewall

Members

Remote Groups

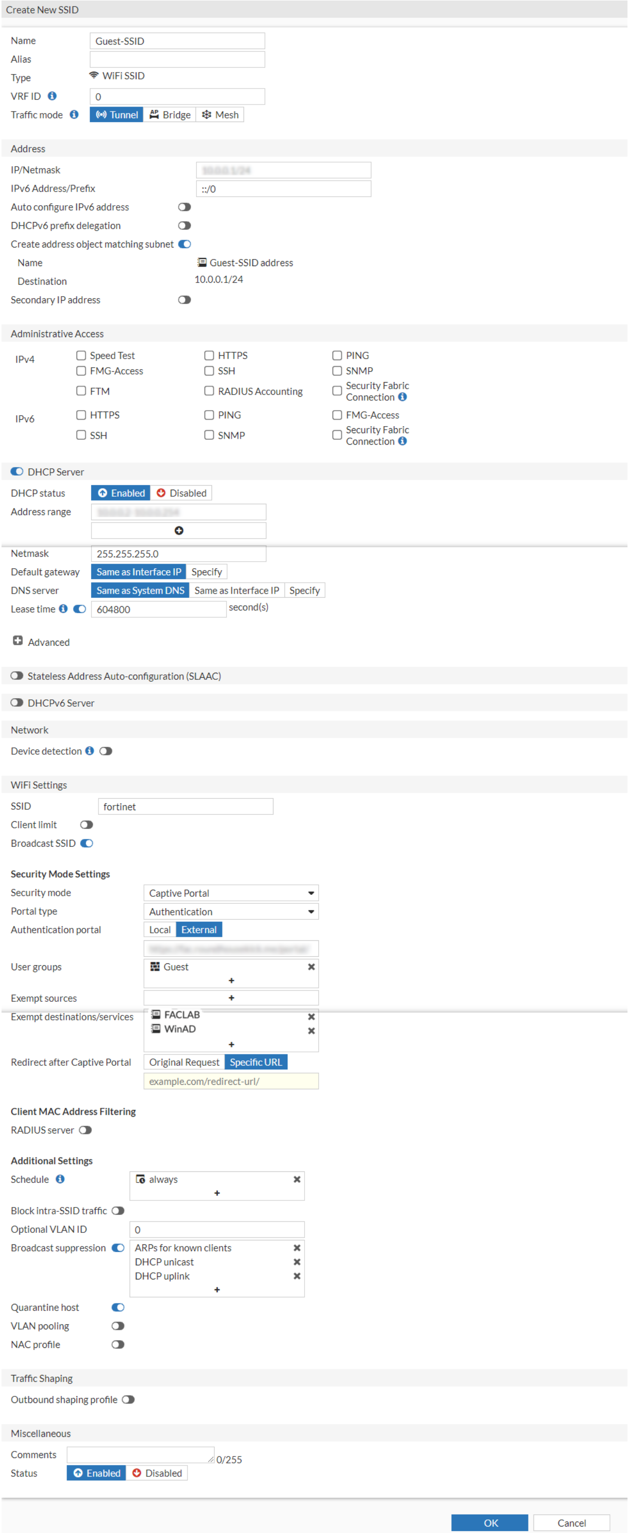
Remote Server	Group Name
FACLAB	Guest

Creating a wireless guest SSID on FortiGate

To create a wireless guest SSID:

1. Go to *WiFi & Switch Controller > SSIDs*.
2. From the *Create New* dropdown, select *SSID*.
3. Enter a *Name* for the interface. Optionally, you can enter an alias.
4. In *Traffic* mode, select *Tunnel*. Alternatively, you can select *Bridge*.
5. In the *Address* pane, enter an IP address/netmask for *IP/Netmask*.
6. Enable *DHCP Server*, and keep the default settings in the *DHCP Server* pane.
7. In the *WiFi Settings* pane:
   a. Enter SSID name that is broadcasted to the WiFi clients.
   b. In the *Security mode* dropdown, select *Captive Portal*.
   c. In the *Portal type* dropdown, ensure *Authentication* is selected.
   d. In *Authentication* portal, select *External*, and enter the portal URL for the captive portal policy configured on FortiAuthenticator. See Captive portal policy.
   e. In *User groups*, select *Guest*. See Guest group on FortiGate.
   f. In *Exempt destinations/services*, select the address objects for the FortiAuthenticator and DNS servers. For the selected addresses and services, FortiGate does not present the captive portal page when the policy for the selected traffic is matched.
      In the *Select Entries* window, go to *Create > Create New* to create new addresses and services.
   g. Optionally, in *Redirect after Captive Portal*, select *Specific URL*, and enter a URL to redirect users to a specific URL once authenticated.

8. Click *OK*.



Create New SSID

Name: Guest-SSID
Alias:
Type: WiFi SSID
VRF ID: 0
Traffic mode: [✓ Tunnel] Bridge Mesh

Address

IP/Netmask: [redacted]
IPv6 Address/Prefix: ::/0
Auto configure IPv6 address: ○
DHCPv6 prefix delegation: ○
Create address object matching subnet: ●
Name: Guest-SSID address
Destination: 10.0.0.1/24
Secondary IP address: ○

Administrative Access

IPv4: □ Speed Test □ HTTPS □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection
IPv6: □ HTTPS □ PING □ FMG-Access □ SSH □ SNMP □ Security Fabric Connection

● DHCP Server

DHCP status: [✓ Enabled] Disabled
Address range: [redacted]
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify
Lease time ●: 604800 second(s)

Advanced

○ Stateless Address Auto-configuration (SLAAC)

○ DHCPv6 Server

Network

Device detection: ○

WiFi Settings

SSID: fortinet
Client limit: ○
Broadcast SSID: ●

Security Mode Settings

Security mode: Captive Portal
Portal type: Authentication
Authentication portal: Local [✓ External]
[redacted]
User groups: Guest
Exempt sources:
Exempt destinations/services: FACLAB, WinAD
Redirect after Captive Portal: Original Request [✓ Specific URL]
example.com/redirect-url/

Client MAC Address Filtering

RADIUS server: ○

Additional Settings

Schedule: always
Block intra-SSID traffic: ○
Optional VLAN ID: 0
Broadcast suppression ●: ARPs for known clients, DHCP unicast, DHCP uplink
Quarantine host: ●
VLAN pooling: ○
NAC profile: ○

Traffic Shaping

Outbound shaping profile: ○

Miscellaneous

Comments: 0/255
Status: [✓ Enabled] Disabled

Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet

To create a firewall policy for guest access to DNS and FortiAuthenticator:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Enter a name for the policy.
3. In *Incoming Interface*, select the guest SSID created in Wireless Guest SSID.
4. In *Outgoing Interface*, select interfaces for FortiAuthenticator and DNS access.
5. In *Source*, select an *Address* object.
6. In *Destination*, select address objects for the FortiAuthenticator and DNS servers.
7. Enable or disable *NAT* as required.
8. Optionally, enable other options including *Security Profiles* for performing inspection using the security features of FortiGate.
9. Click *OK*.

To create firewall policy for guest user internet access:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Enter a name for the policy.
3. In *Incoming Interface*, select the guest SSID created in Wireless Guest SSID.
4. In *Outgoing Interface*, select the interface for internet access.
5. In *Source*, select the *All* address object and the guest group configured in Guest group on FortiGate.
6. In *Destination*, select the *All* address object.
7. Enable *NAT*.
8. Optionally, enable other options including *Security Profiles* for performing inspection using the security features of FortiGate.
9. Click *OK*.

Configuring firewall authentication portal settings on FortiGate

The following settings are required to avoid certificate and security errors on the client. After the user is authenticated using the external captive portal, the browser redirects briefly to the firewall authentication portal over HTTPS. The browser then redirects the user to the original URL or a specific URL.

The specific URL needs to be configured in the *Redirect after Captive Portal* option in *Create New SSID* dialog.

To configure firewall authentication portal address from the CLI:

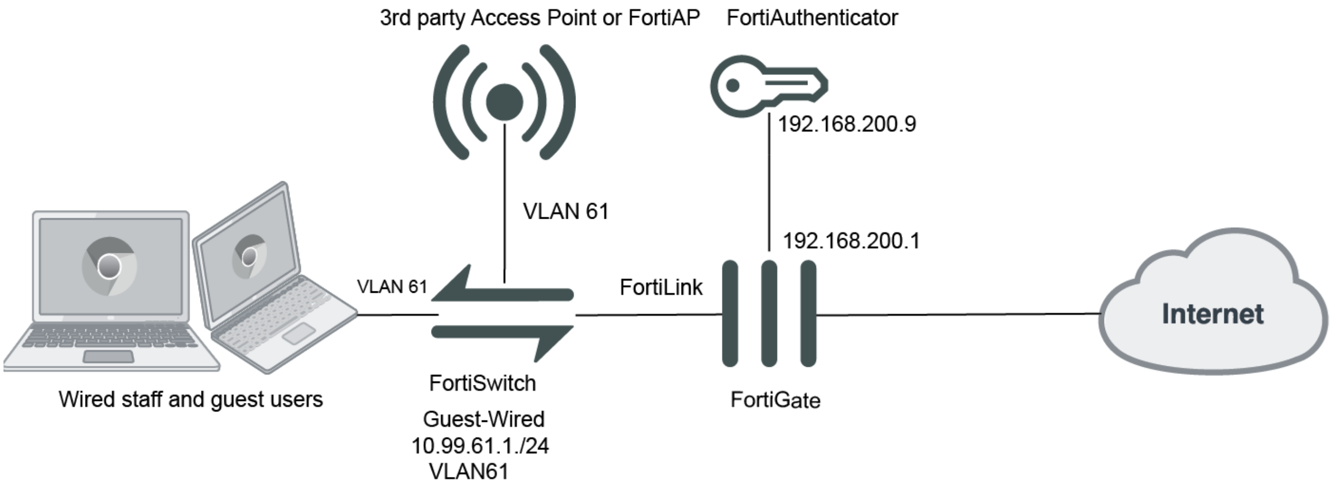
1. Enter the following commands to set to the firewall authentication portal address:
```
config firewall auth-portal
   set portal-addr <addr> #portal-addr setting must be an FQDN that resolves to the
         interface IP address of the guest SSID. The client must be able to resolve
         this using the DNS server configured in the DHCP scope.
end
```

To configure the firewall user settings from the CLI:

1. Enter the following commands to set to the firewall user settings:
```
config user setting
```

```
        set auth-type https
        set auth-cert "STAR-Aug21" #auth-cert must be a valid certificate that has been
             imported to the FortiGate and matches the FQDN used for the interface IP of
             the SSID. A wildcard certificate may be used.
        set auth-secure-http enable
    end
```

FortiAuthenticator as a Wired Guest Portal for FortiGate



In the topology above:

- FortiSwitch is connected to FortiGate via FortiLink.
- VLAN 61 is the FortiSwitch VLAN.
- A FortiAP or a 3rd party AP is connected to FortiSwitch on VLAN 61, thereby assigning IPs in that range to clients in bridge mode.
- Other wired users are directly connected to the FortiSwitch ports on VLAN 61, receiving IPs in that range and hitting the captive portal.

This recipe walks you through setting up FortiAuthenticator as a wired guest portal.

The recipe may be used where 3rd party access point is using a bridged SSID to place client traffic into a specific VLAN (here, VLAN 61).

A 3rd party switch can also be used instead of FortiSwitch. When a 3rd party switch is used, FortiGate will connect to the switch's trunk port.

To set up FortiAuthenticator as a wired guest portal:

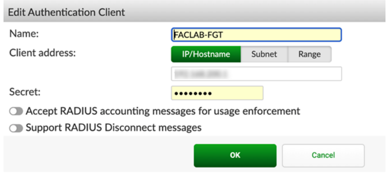
1. Configuring FortiGate as a RADIUS client on page 69.
2. Creating a user group on FortiAuthenticator for guest users on page 69.
3. Creating a guest portal on FortiAuthenticator on page 70.
4. Configuring an access point on FortiAuthenticator on page 71.
5. Configuring a captive portal policy on FortiAuthenticator on page 71.
6. Configuring FortiAuthenticator as a RADIUS server on FortiGate on page 72.
7. Creating a guest group on FortiGate on page 73.
8. Creating a wired guest interface on FortiSwitch on page 73.
9. Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet on page 75.
10. Configuring firewall authentication portal settings on FortiGate on page 76.

Configuring FortiGate as a RADIUS client

To configure FortiGate as a RADIUS client:

1. In *Authentication* > *RADIUS Service* > *Clients*, click *Create New*.
2. Enter a unique name for the RADIUS client and the IP address from which it will be connecting.
   This is the IP address of the RADIUS client itself, here, FortiGate, not the IP address of the end-user's device.

   You may enter a subnet or a range if this configuration applies to multiple FortiGates.
3. Enter a password for *Secret*.
   The secret is a pre-shared secure password that the device, here, FortiGate, uses to authenticate to FortiAuthenticator.
4. Click *OK* to save changes to the RADIUS client.



Edit Authentication Client

Name: FACLAB-FGT

Client address: IP/Hostname | Subnet | Range

[redacted]

Secret: ••••••••

○ Accept RADIUS accounting messages for usage enforcement

○ Support RADIUS Disconnect messages

If FortiGate provides RADIUS services to other users and for other tasks, you should configure a loopback interface. You can specify the RADIUS source IP address in the FortiGate CLI for the loopback interface.

To configure a loopback interface using the FortiGate CLI:

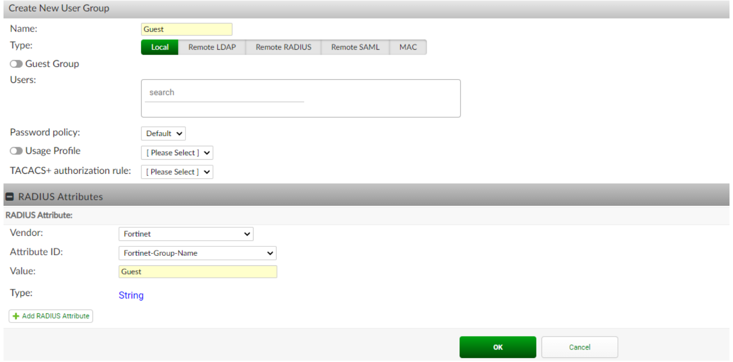
```
config user radius
   edit FAC
   set source-ip <ip address> #use the IP address configured in the
         RADIUS client on FortiAuthenticator.
end
```

Creating a user group on FortiAuthenticator for guest users

To create a user group:

1. Go to *Authentication* > *User Management* > *User Groups* and select *Create New*.
2. Enter a name for the group.
3. Select *Local* as the *Type*.

4. In *RADIUS Attributes* pane, select *Add RADIUS Attribute*:
   a. In *Vendor*, select *Fortinet*.
   b. In *Attribute ID*, select *Fortinet-Group-Name*.
   c. In *Value*, enter the group name that you will match on the FortiGate.
      FortiAuthenticator sends the RADIUS attribute to the FortiGate on successful authentication.
5. Click *OK*.



Create New User Group

Name: Guest

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

○ Guest Group

Users: search

Password policy: Default

○ Usage Profile [Please Select]

TACACS+ authorization rule: [Please Select]

RADIUS Attributes

RADIUS Attribute:

Vendor: Fortinet

Attribute ID: Fortinet-Group-Name

Value: Guest

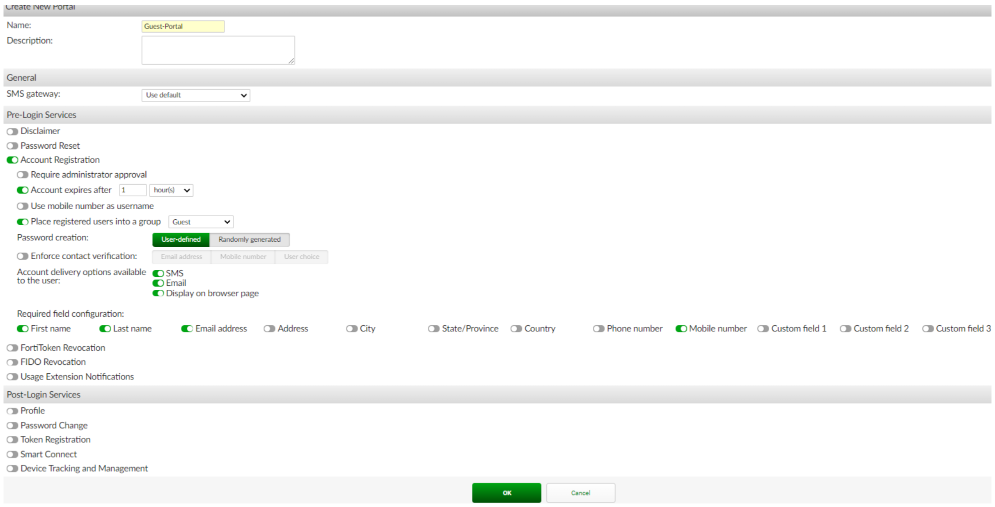
Type: String

Creating a guest portal on FortiAuthenticator

To create a guest portal:

1. Go to *Authentication* > *Portals* > *Portals* and select *Create New*.
2. Enter a name for the portal.
3. Enable *Account Registration* to allow guest users to create an account.
4. In the *Account Registration* toggle, enable *Place registered users into a group*, and select the user group created in Creating a user group.
   Users are made members of the group when they create an account.

   You can configure additional settings as required. For instance, you may want to enable account expiry and enforcing contact verification using Email or SMS.
5. Click *OK*.



Create New Portal

Name: Guest-Portal

Description:

General

SMS gateway: Use default

Pre-Login Services

○ Disclaimer

○ Password Reset

● Account Registration

○ Require administrator approval

● Account expires after 1 hour(s)

○ Use mobile number as username

● Place registered users into a group Guest

Password creation: User-defined | Randomly generated

○ Enforce contact verification: Email address | Mobile number | User choice

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

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

○ FortiToken Revocation

○ FIDO Revocation

○ Usage Extension Notifications

Post-Login Services

○ Profile

○ Password Change

○ Token Registration

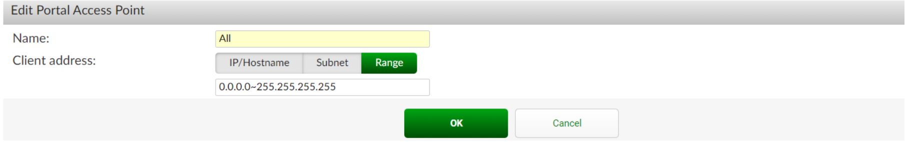
○ Smart Connect

○ Device Tracking and Management

Configuring an access point on FortiAuthenticator

To configure an access points:

1. Go to *Authentication* > *Portals* > *Access Points* and select *Create New*.
2. Enter a name for the access point.
3. In *Client address*, select *Range*, and enter `0.0.0.0-255.255.255.255`.
4. Click *OK*.



Edit Portal Access Point

Name: All

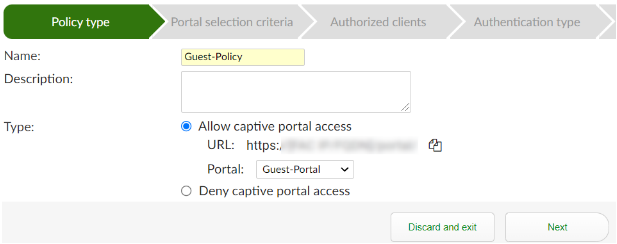
Client address: IP/Hostname | Subnet | Range

0.0.0.0-255.255.255.255

Configuring a captive portal policy on FortiAuthenticator

To configure an allow access captive portal policy:

1. Go to *Authentication* > *Portals* > *Policies*, click *Captive Portal* and *Create New*.
2. In the *Policy type* tab:
   - a. Enter a name for the policy. Optionally, enter a description for the policy.
   - b. In *Type*, select *Allow captive portal access*. Copy the URL and store it on Notepad. The URL needs to be entered in the FortiGate configuration later.
   - c. Choose a portal created in Creating a guest portal on FortiAuthenticator on page 70.
   - d. Click *Next*.



Name: Guest-Policy

Description:

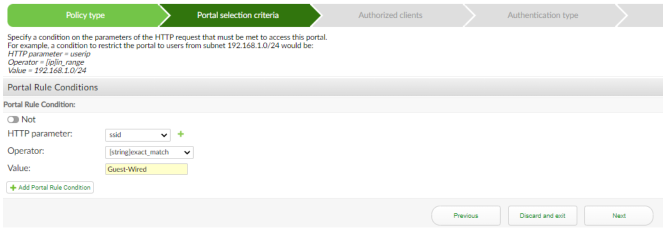
Type: ● Allow captive portal access

URL: https:[redacted]

Portal: Guest-Portal

○ Deny captive portal access

3. In the *Portal selection criteria* tab:
   - a. In the *HTTP parameter* dropdown, select *ssid* to match.
   - b. In the *Operator* dropdown, *select [string]exact_match*.
   - c. In *Value*, enter the name of the interface configured on the FortiGate with captive portal authentication required. Here, `Guest-Wired`.
   - d. Click *Next*.



Specify a condition on the parameters of the HTTP request that must be met to access this portal.
For example, a condition to restrict the portal to users from subnet 192.168.1.0/24 would be:
HTTP parameter = userip
Operator = [ip]in_range
Value = 192.168.1.0/24

Portal Rule Conditions

Portal Rule Condition:

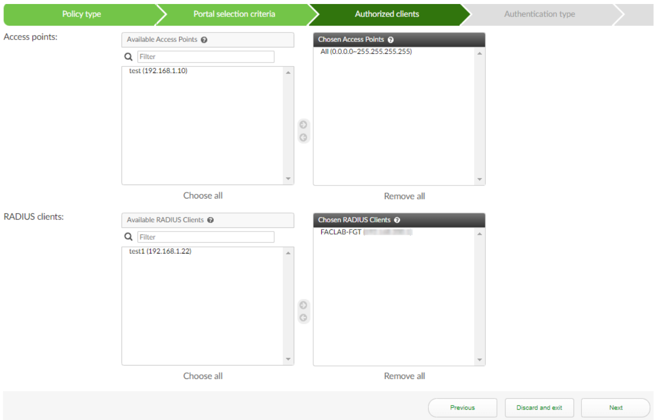
Not

HTTP parameter: ssid

Operator: [string]exact_match

Value: Guest-Wired

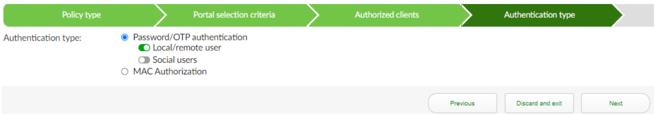
4. In the *Authorized clients* tab:
    a. From *Access points*, select the access point defined in Access points.
    b. From *RADIUS clients*, select the FortiGate RADIUS client defined in RADIUS clients.
    c. Click *Next*.



Access points:
Available Access Points: test (192.168.1.10)
Chosen Access Points: All (0.0.0.0~255.255.255.255)

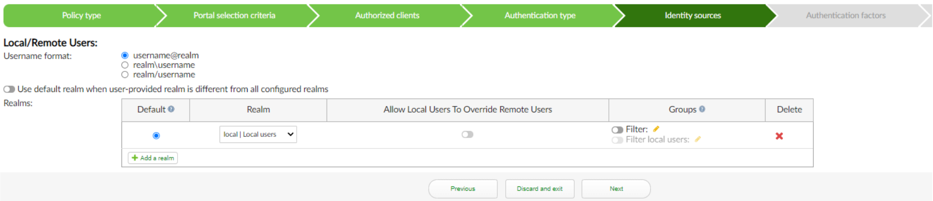
RADIUS clients:
Available RADIUS Clients: test1 (192.168.1.22)
Chosen RADIUS Clients: FACLAB-FGT [redacted]

5. In the *Authentication type* tab, select *Password/OTP authentication*, then enable *Local/remote user* to verify credentials against one of the local or remote user accounts, and click *Next*.



Authentication type:
● Password/OTP authentication
  Local/remote user (enabled)
  Social users
○ MAC Authorization

6. In the *Identity sources* tab:
    a. For *Username format*, select *username@realm*.
    b. For *Realms*, select *local* realm. Optionally, enable *Filter*, click the pen icon, and from *Available User Groups*, move the group created in User Group to *Chosen User Groups*.
    c. Click *Next*.



Local/Remote Users:
Username format:
● username@realm
○ realm\username
○ realm/username

Use default realm when user-provided realm is different from all configured realms

Realms:

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

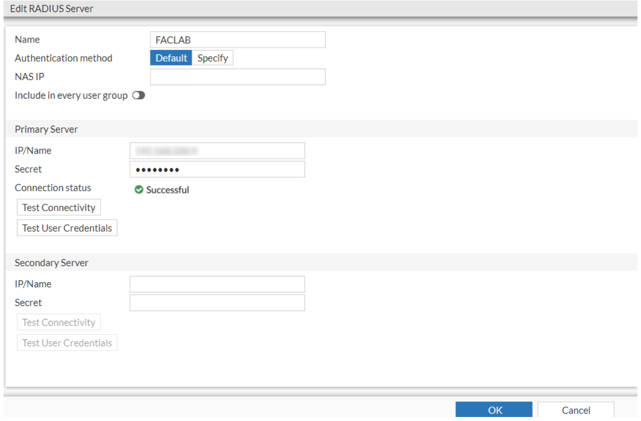
7. In the *Authentication Factors* tab, click *Next*.
8. In the *RADIUS response* tab, review the policy, and click *Save and exit*.

Configuring FortiAuthenticator as a RADIUS server on FortiGate

To configure FortiGate authentication settings:

1. Go to *User & Authentication > RADIUS Servers* and click *Create New*.
2. Enter a name for the RADIUS server.
3. For *Authentication method*, select *Default*.
4. In *IP/Name*, enter the IP address or DNS name of the RADIUS server.
5. In *Secret*, enter the shared secret key.
   The secret is the same as the one used when setting up the RADIUS client, here, FortiGate.
6. Click *Test Connectivity* to test the connection to the server, and ensure that the connection status is *Successful*.

7. Click *OK* to save changes.



Edit RADIUS Server

Name: FACLAB

Authentication method: Default | Specify

NAS IP:

Include in every user group

Primary Server

IP/Name: [redacted]

Secret: ••••••••

Connection status: Successful

Secondary Server

IP/Name:

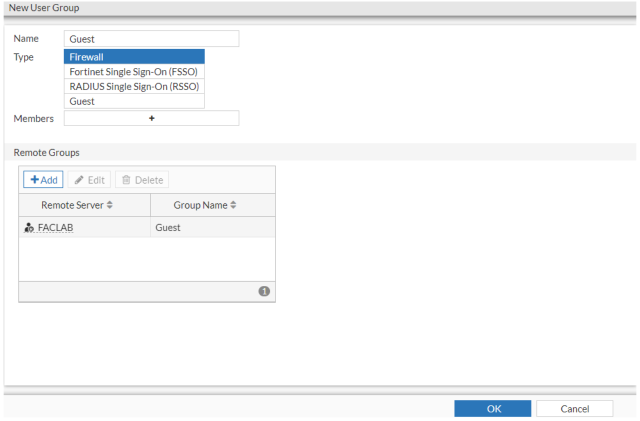
Secret:

Creating a guest group on FortiGate

To create a guest group:

1. Go to *User & Authentication* > *User Groups* and click *Create New*.
2. Enter a name for the group.
3. In *Type*, select *Firewall*.
4. In *Remote Groups*, select *Add*, and then select the remote server created in Remote Server. Click *OK*. Optionally, you may specify the group to be matched on the remote server. The group name must be configured as a RADIUS attribute on the group configured on FortiAuthenticator. See Groups.

   The RADIUS attribute will be sent to the FortiGate by the FortiAuthenticator on successful authentication.
5. Click *OK*.



New User Group

Name: Guest

Type: Firewall

Members:

Remote Groups

Remote Server	Group Name
FACLAB	Guest

Creating a wired guest interface on FortiSwitch

This solution demonstrates the configuration when a FortiSwitch is used.

When a 3rd party switch is used instead, create a VLAN sub-interface instead of a FortiSwitch VLAN. Connect the FortiGate interface to the trunk port of the switch.

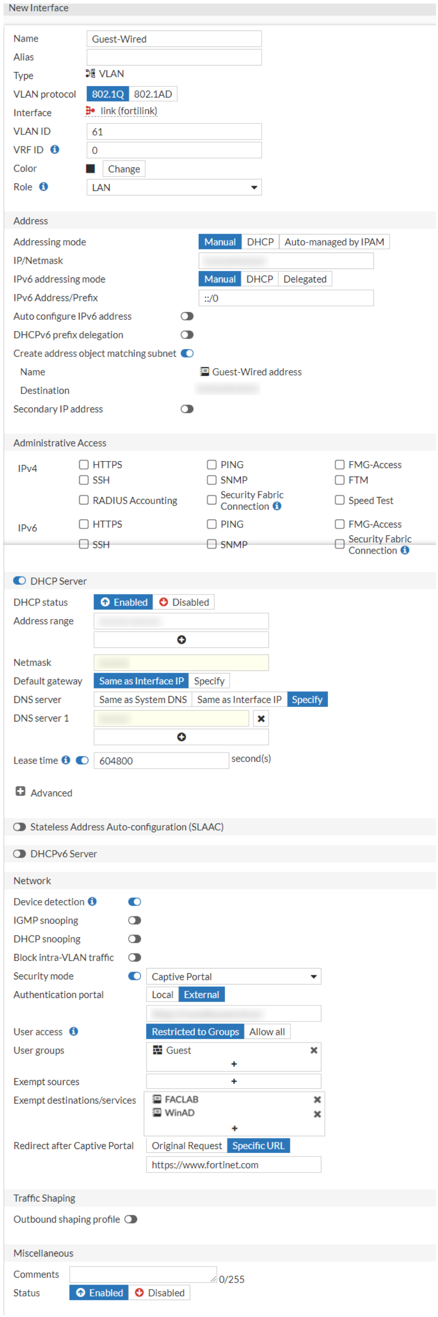
To create a wired guest interface:

1. Go to *WiFi & Switch Controller > FortiSwitch VLANs*.
2. Select *Create New*.
3. In the *New Interface* window, enter a name for the interface. Optionally, enter an alias.
4. Select *802.1Q* as the *VLAN protocol*.
5. Ensure that a FortiLink interface member is selected in *Interface*.
6. In *VLAN ID*, enter a VLAN ID, here `61`.
7. Ensure that the *Role* is set as *LAN*.
8. In the *Address pane*:
   1. In *Addressing mode*, select *Manual*.
   2. In *IP/Netmask*, enter an *IP address/netmask*.
   3. In *IPv6 addressing* mode, select *Manual*.
   4. Ensure that the *Create address object matching subnet* is enabled.
9. Enable *DHCP Server*, and in the *DHCP server* pane:
   1. Enter an address range.
   2. For *DNS server*, select *Specify*, click the *Add* icon, and enter the IP address of the FortiSwitch.
10. In the *Network* pane:
    1. Ensure that *Device detection* is enabled.
    2. Enable *Security mode*, and from the dropdown, ensure that *Captive Portal* is selected.
    3. In *Authentication portal*, select *External*, and enter the portal URL for the captive portal policy configured on FortiAuthenticator.
       See Captive portal policy.
    4. In *User access*, select *Restricted to Groups*.
    5. In *User groups*, select *Guest*.
       See Guest group on FortiGate.
    6. In *Exempt destinations/services*, select the address objects for the FortiAuthenticator and DNS servers.

       > For the selected addresses and services, FortiGate does not present the captive portal page when the policy for the selected traffic is matched.

       In the *Select Entries* window, go to *Create > Create New* to create new addresses and services.
    7. Optionally, in *Redirect after Captive Portal*, select *Specific Request*, and enter a URL to redirect users to a specific URL once authenticated.

11. Click *OK*.



New Interface

Name: Guest-Wired
Alias:
Type: VLAN
VLAN protocol: [✓ 802.1Q] 802.1AD
Interface: link (fortilink)
VLAN ID: 61
VRF ID: 0
Color: ■ Change
Role: LAN

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask: [redacted]
IPv6 addressing mode: [✓ Manual] DHCP Delegated
IPv6 Address/Prefix: ::/0
Auto configure IPv6 address: ○
DHCPv6 prefix delegation: ○
Create address object matching subnet: ●
Name: Guest-Wired address
Destination: [redacted]
Secondary IP address: ○

Administrative Access

IPv4: ☐ HTTPS ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection ☐ Speed Test
IPv6: ☐ HTTPS ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ Security Fabric Connection

● DHCP Server

DHCP status: [✓ Enabled] Disabled
Address range: [redacted]
Netmask: [redacted]
Default gateway: [✓ Same as Interface IP] Specify
DNS server: Same as System DNS Same as Interface IP [✓ Specify]
DNS server 1: [redacted]
Lease time: ● 604800 second(s)
Advanced

○ Stateless Address Auto-configuration (SLAAC)

○ DHCPv6 Server

Network

Device detection: ●
IGMP snooping: ○
DHCP snooping: ○
Block intra-VLAN traffic: ○
Security mode: ● Captive Portal
Authentication portal: Local [✓ External]
[redacted]
User access: [✓ Restricted to Groups] Allow all
User groups: Guest
Exempt sources:
Exempt destinations/services: FACLAB, WinAD
Redirect after Captive Portal: Original Request [✓ Specific URL]
https://www.fortinet.com

Traffic Shaping

Outbound shaping profile: ○

Miscellaneous

Comments: 0/255
Status: [✓ Enabled] Disabled

Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet

To create a firewall policy for guest access to DNS and FortiAuthenticator:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Enter a name for the policy.
3. In *Incoming Interface*, select the wired guest interface created in Wired Guest Interface.
4. In *Outgoing Interface*, select the interface for FortiAuthenticator and DNS access.

5. In *Source*, select an *Address* object.
6. In *Destination*, select address objects for the FortiAuthenticator and DNS servers.
7. Enable or disable *NAT* as required.
8. Optionally, enable other options including *Security Profiles* for performing inspection using the security features of FortiGate.
9. Click *OK*.

To create firewall policy for guest user internet access:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Enter a name for the policy.
3. In *Incoming Interface*, select the wired guest interface created in Wired Guest Interface.
4. In *Outgoing Interface*, select the interface for internet access.
5. In *Source*, select an address object and the guest group configured in Guest group on FortiGate.
6. In *Destination*, select the *All* address object.
7. Enable *NAT*.
8. Optionally, enable other options including *Security Profiles* for performing inspection using the security features of FortiGate.
9. Click *OK*.

Configuring firewall authentication portal settings on FortiGate

The following settings are required to avoid certificate and security errors on the client. After the user is authenticated using the external captive portal, the browser redirects briefly to the firewall authentication portal over HTTPS. The browser then redirects the user to the original URL or a specific URL.

The specific URL needs to be configured in the *Redirect after Captive Portal* option in the New Interface dialog.

To configure firewall authentication portal address from the CLI:

1. Enter the following commands to set to the firewall authentication portal address:

```
config firewall auth-portal
   set portal-addr <addr> #portal-addr setting must be an FQDN that resolves to the
         interface IP address of the guest SSID. The client must be able to resolve
         this using the DNS server configured in the DHCP scope.
end
```

To configure firewall user settings from the CLI:

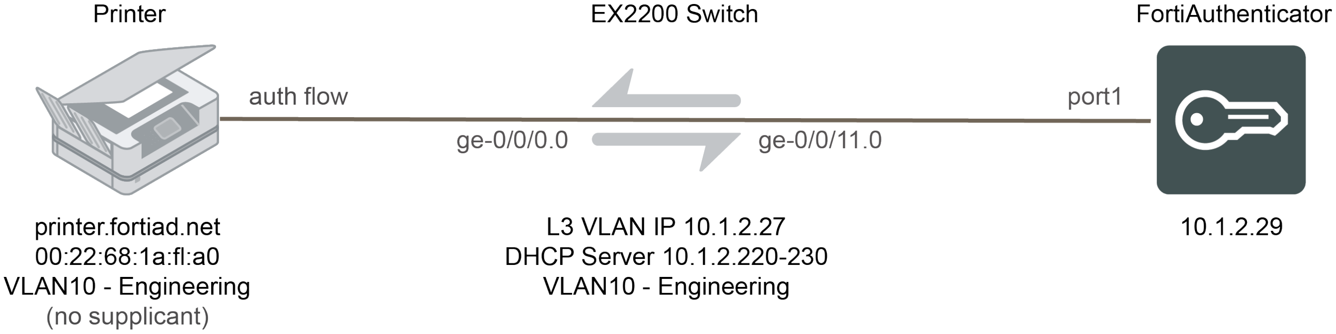
1. Enter the following commands to set to the firewall user settings:

```
config user setting
   set auth-type https
   set auth-cert "STAR-Aug21" #auth-cert must be a valid certificate that has been
         imported to the FortiGate and matches the FQDN used for the interface IP of
         the SSID. A wildcard certificate may be used.
   set auth-secure-http enable
end
```

MAC authentication bypass

This section describes configuring MAC address bypass with FortiAuthenticator.

MAC authentication bypass with dynamic VLAN assignment

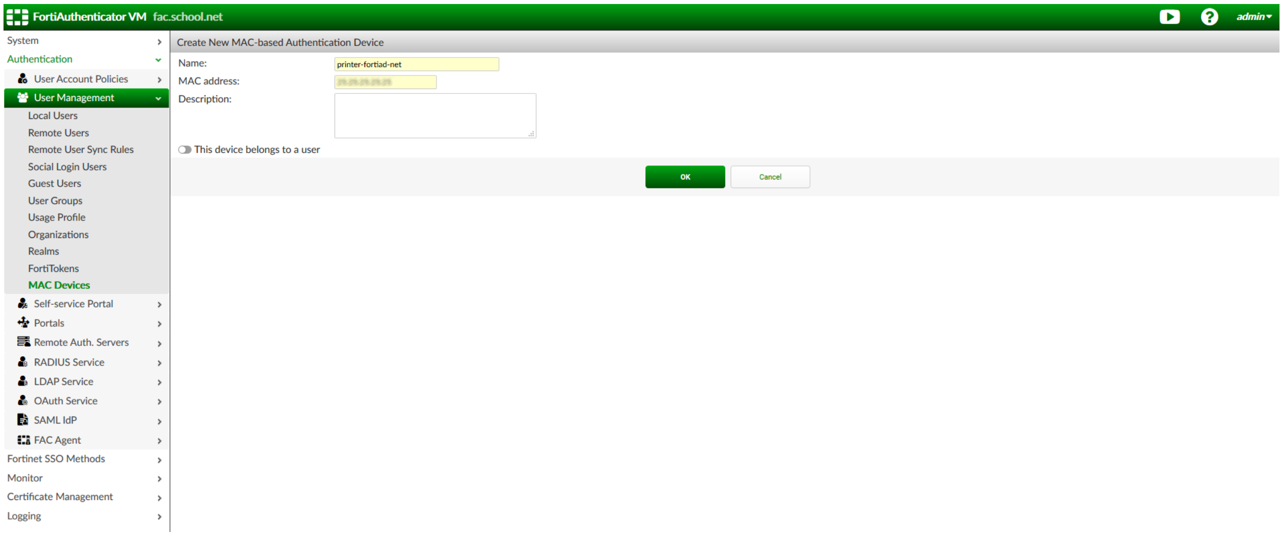


In this recipe, you will configure MAC authentication bypass (MAB) in a wired network with dynamic VLAN assignment.

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

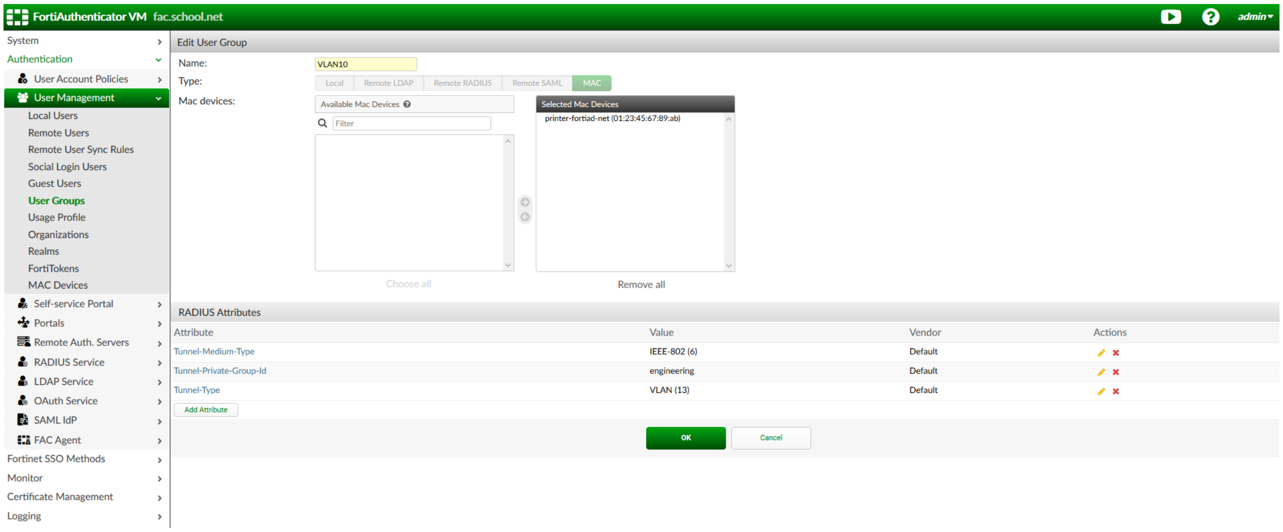
MAC address: [redacted]

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: MAC

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

RADIUS Attributes

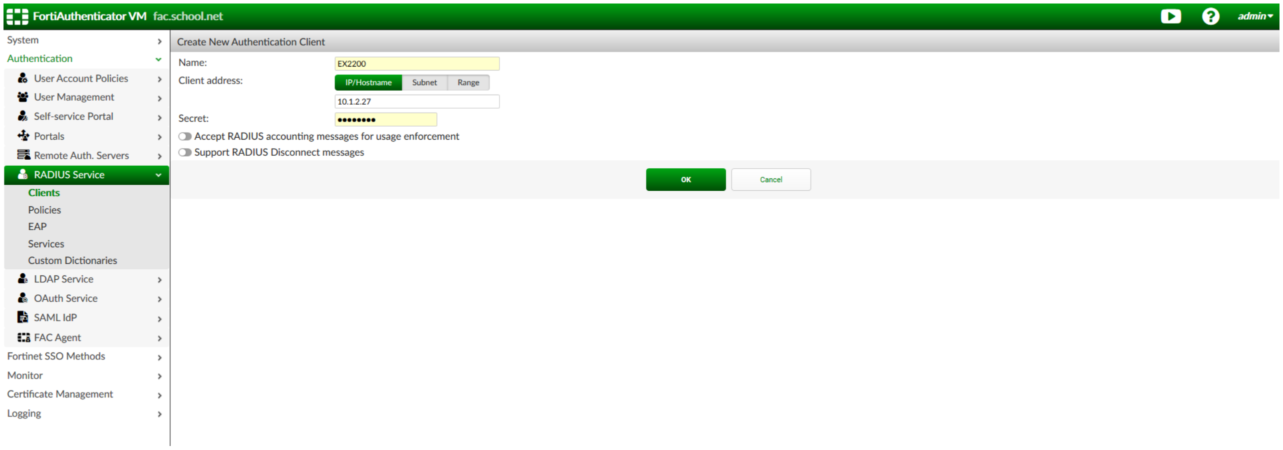
Attribute	Value	Vendor	Actions
Tunnel-Medium-Type	IEEE-802 (6)	Default	✎ ✖
Tunnel-Private-Group-Id	engineering	Default	✎ ✖
Tunnel-Type	VLAN (13)	Default	✎ ✖

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

10.1.2.27

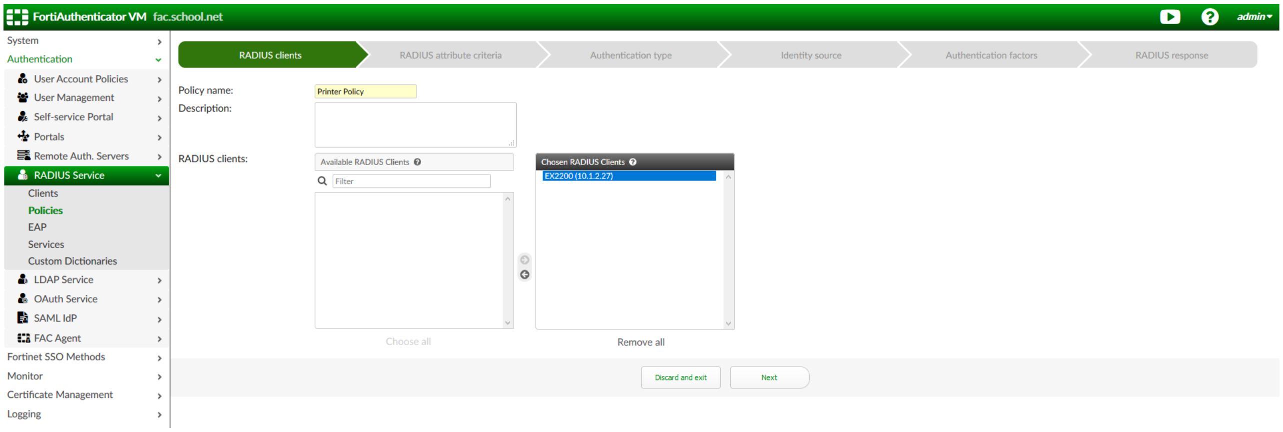
Secret: ●●●●●●●●●

○ Accept RADIUS accounting messages for usage enforcement

○ Support RADIUS Disconnect messages

To create the RADIUS policy:

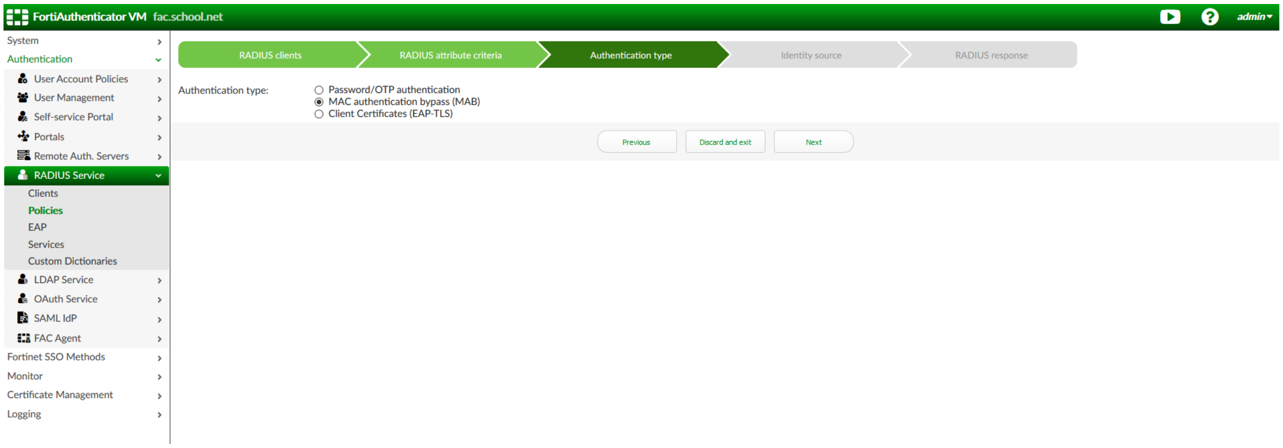
1. Go to *Authentication* > *RADIUS Service* > *Policies* and create a new RADIUS policy.
   In *RADIUS clients*, enter a policy name, and add the previously configured RADIUS client.



Policy name: Printer Policy
Description:
RADIUS clients: Available RADIUS Clients | Chosen RADIUS Clients: EX2200 (10.1.2.27)

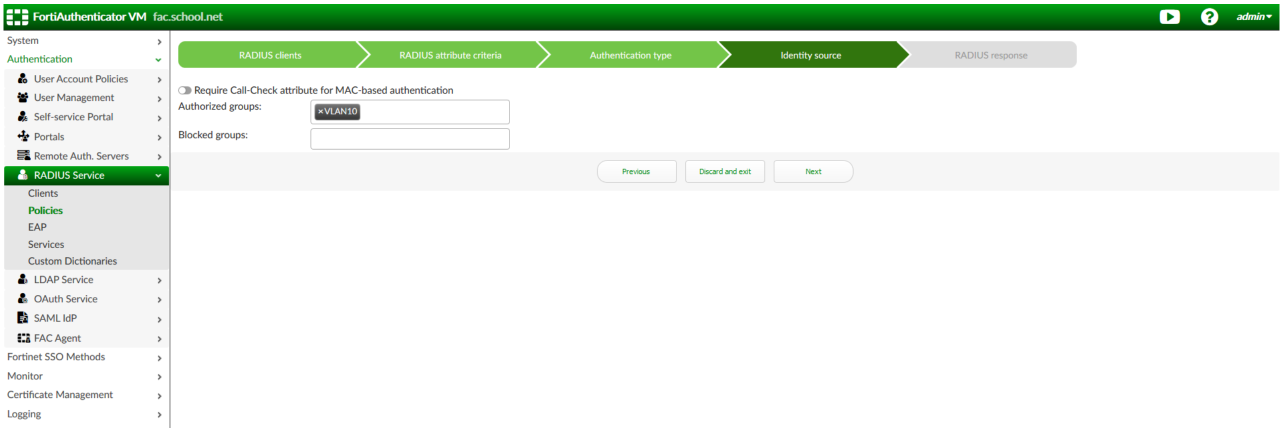
   RADIUS attribute criteria can be left blank.

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



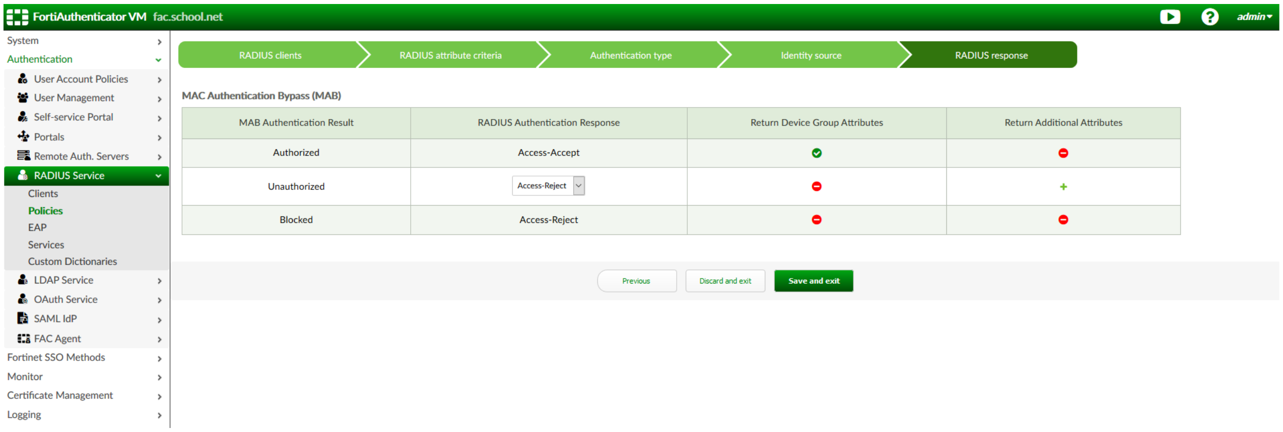
Authentication type:
○ Password/OTP authentication
● MAC authentication bypass (MAB)
○ Client Certificates (EAP-TLS)

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

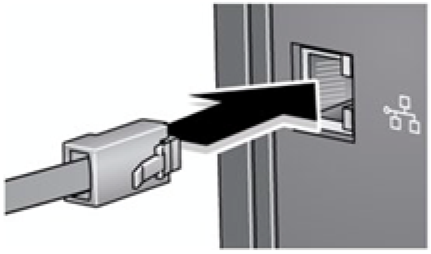
The switch configuration provided below is intended for demonstration only. Your switch configuration is likely to differ significantly.

```
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*
   ```

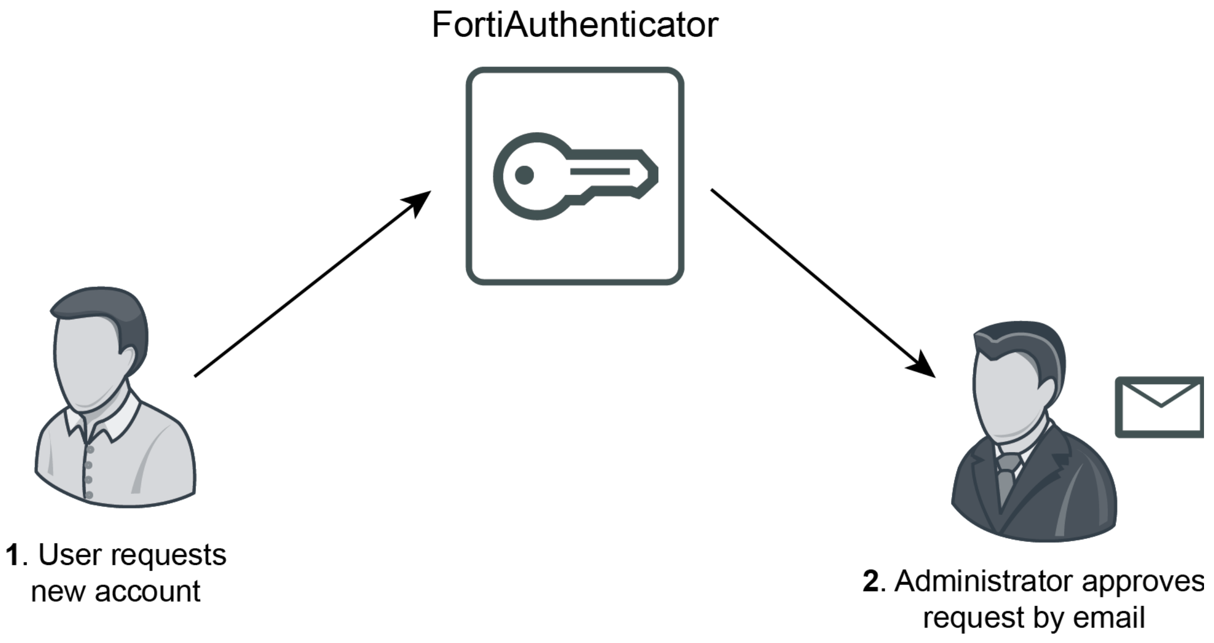
   Additionally, the printer shows as available on the network:

   ```
   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:fl:a0 10.1.2.224 10.1.2.224 vlan.10 none
   a4:c3:61:24:b9:07 10.1.2.228 10.1.2.228 vlan.10 none
   Total entries: 5

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

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

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.

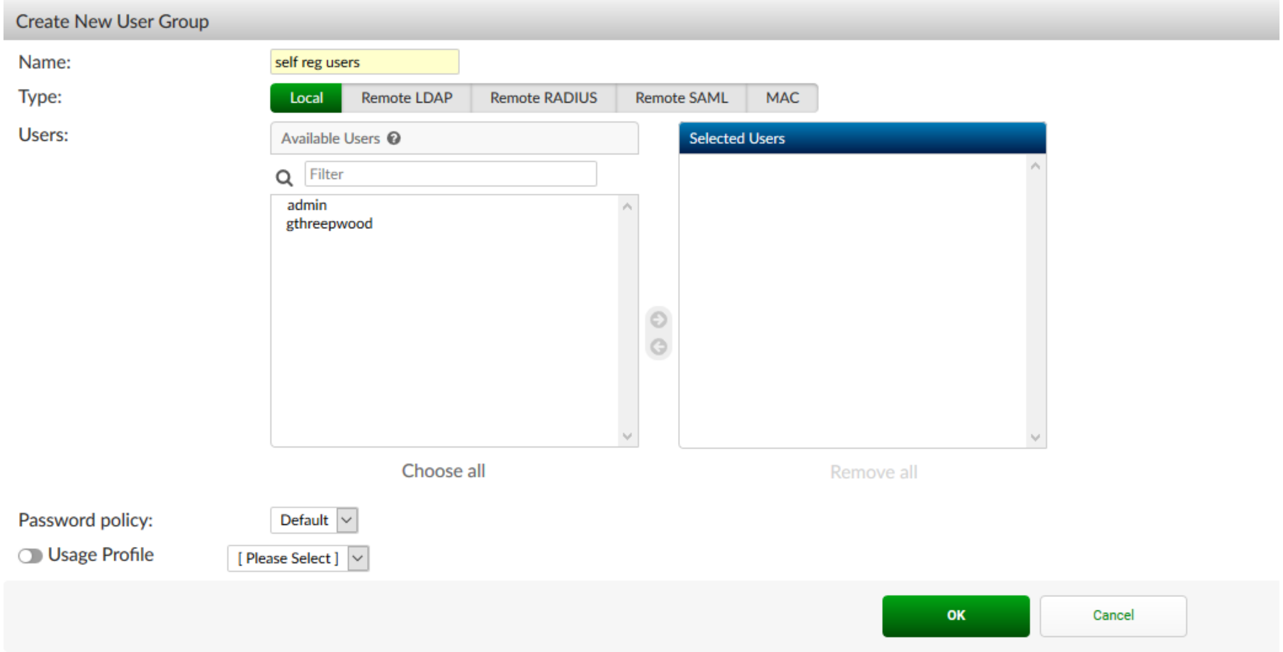
Note that enabling and using administrator approval requires the use of an email server, or SMTP server. Since administrators will approve requests by email, this recipe describes how to add an email server to your FortiAuthenticator. You will create and use a new server instead of the unit's default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

Users:

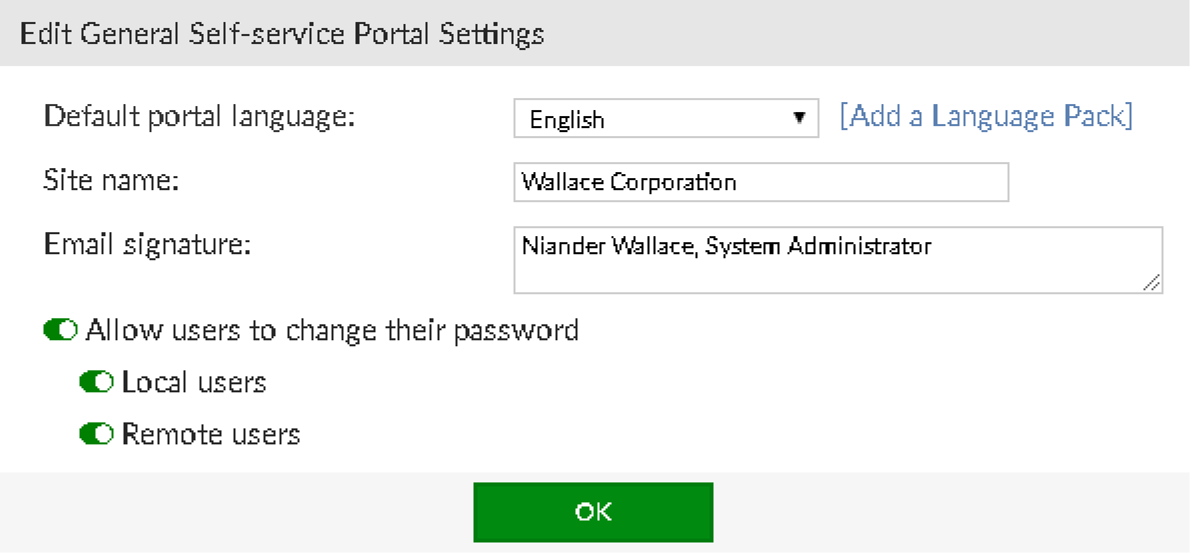
Password policy: Default

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: on

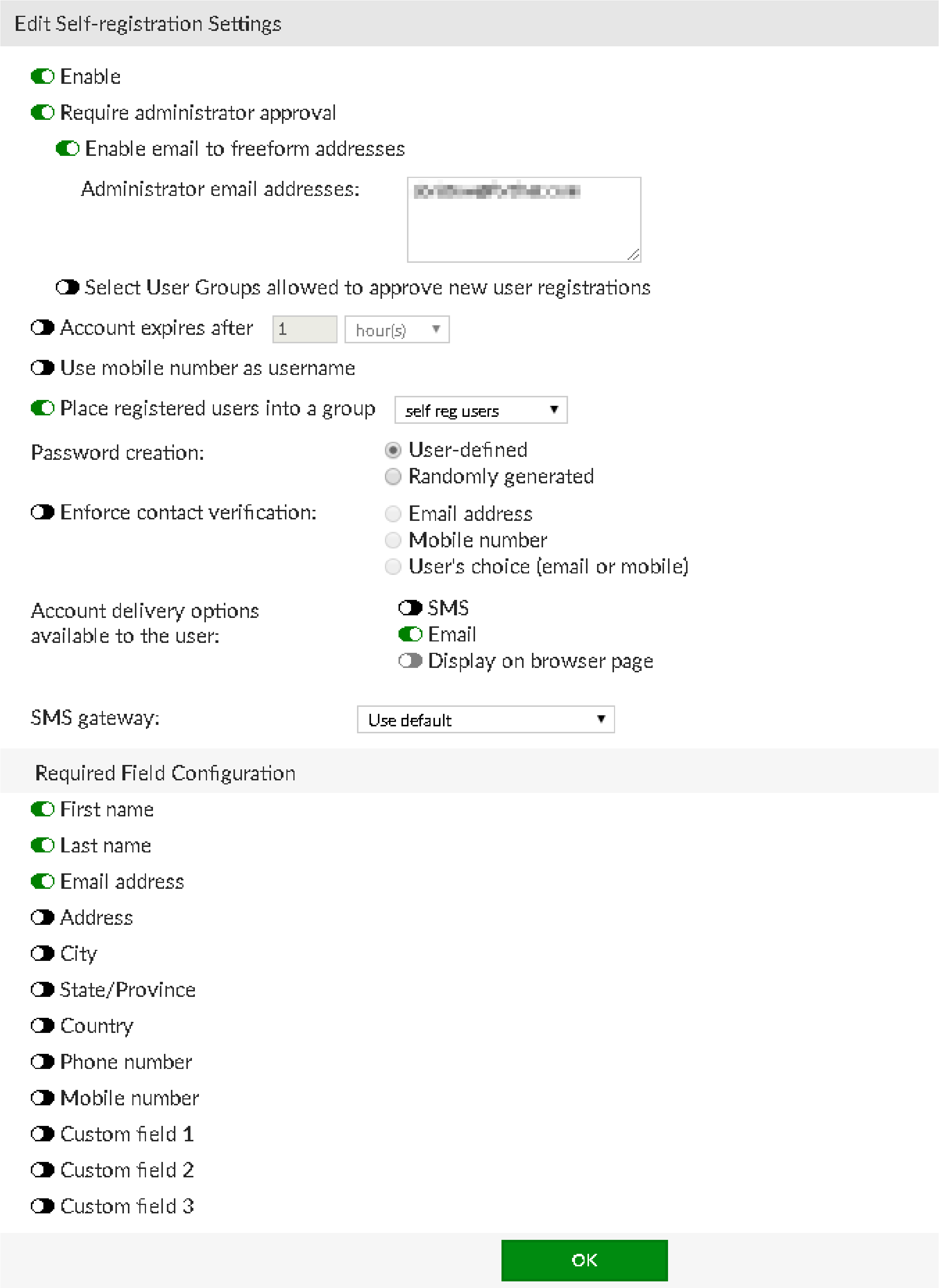
Local users: on

Remote users: on

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

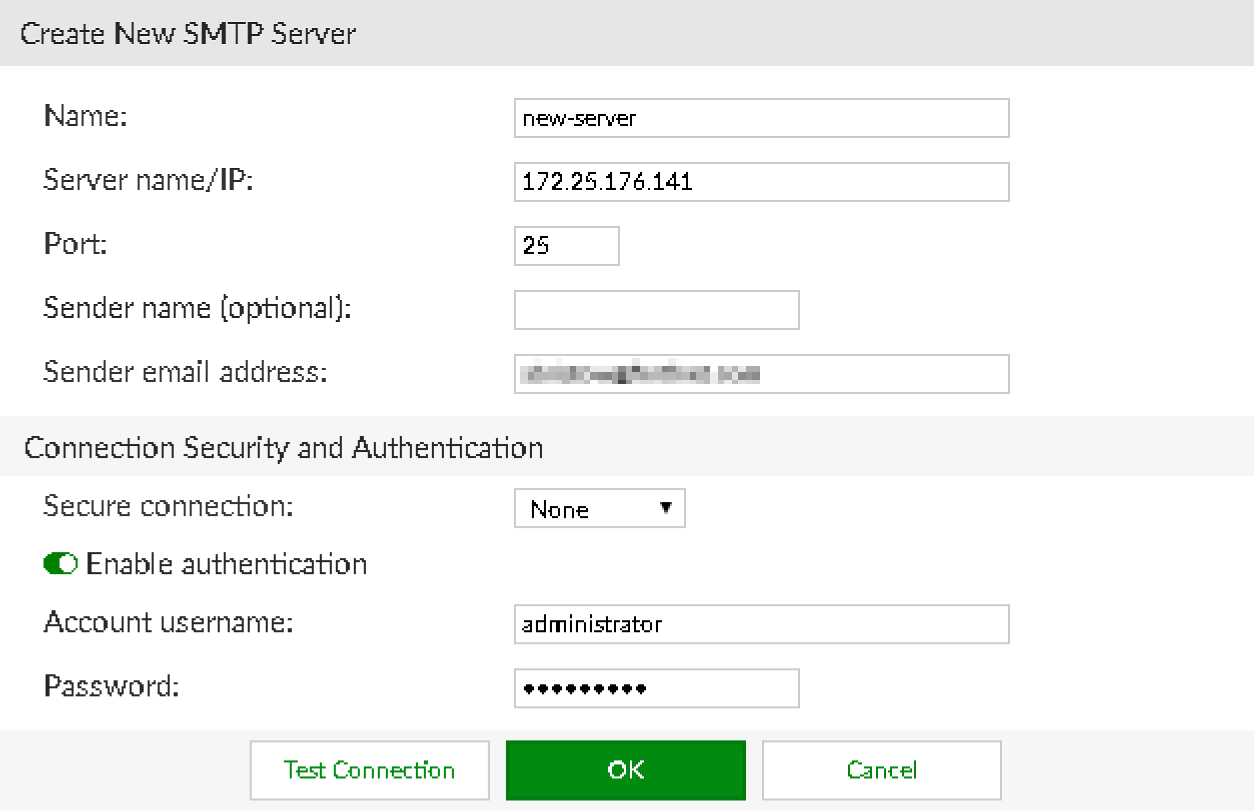
☐ Custom field 2

☐ 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.



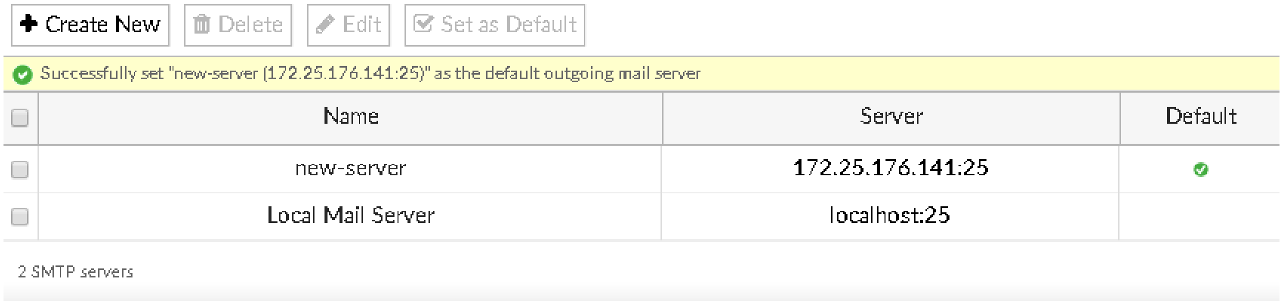
Create New SMTP Server

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

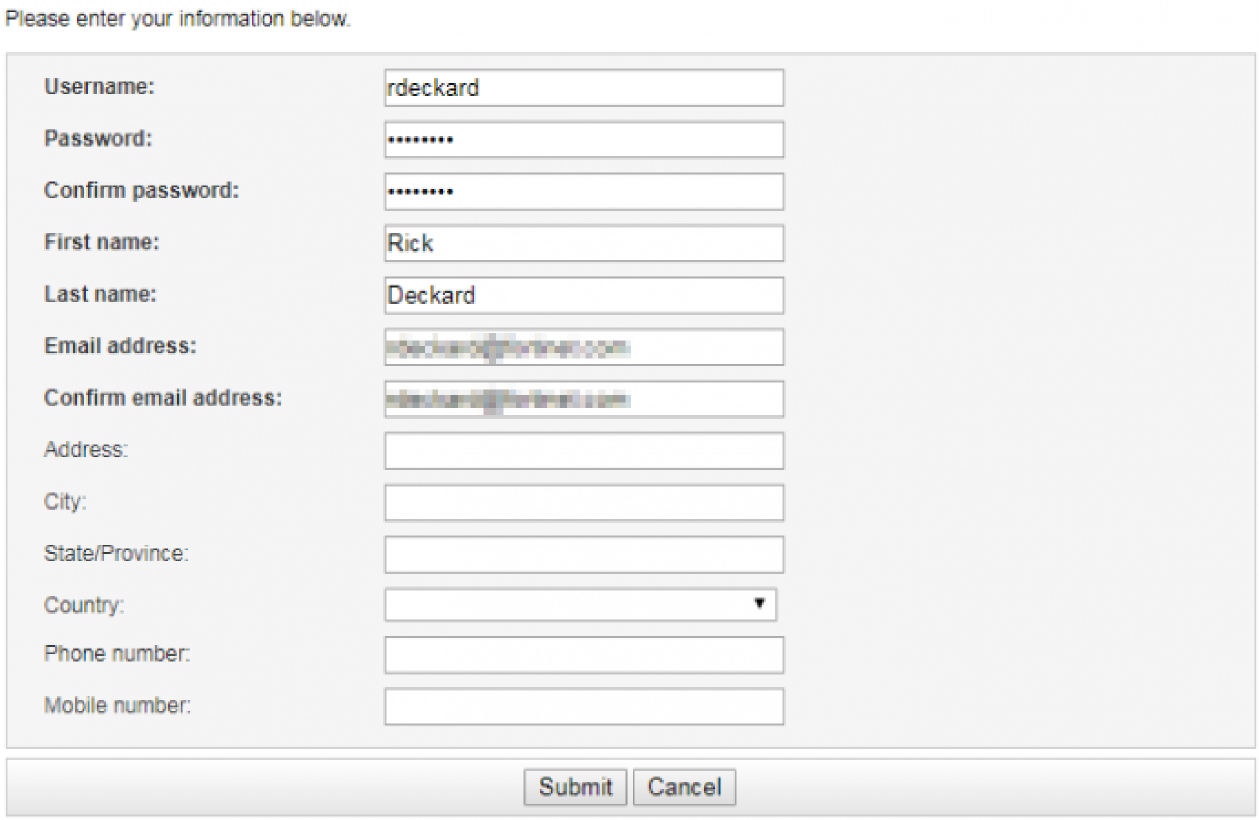
□	Name	Server	Default
□	new-server	172.25.176.141:25	✓
□	Local Mail Server	localhost:25	

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.

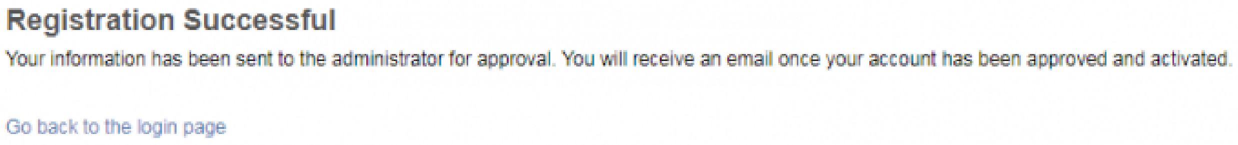
   Select *Submit*.



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.

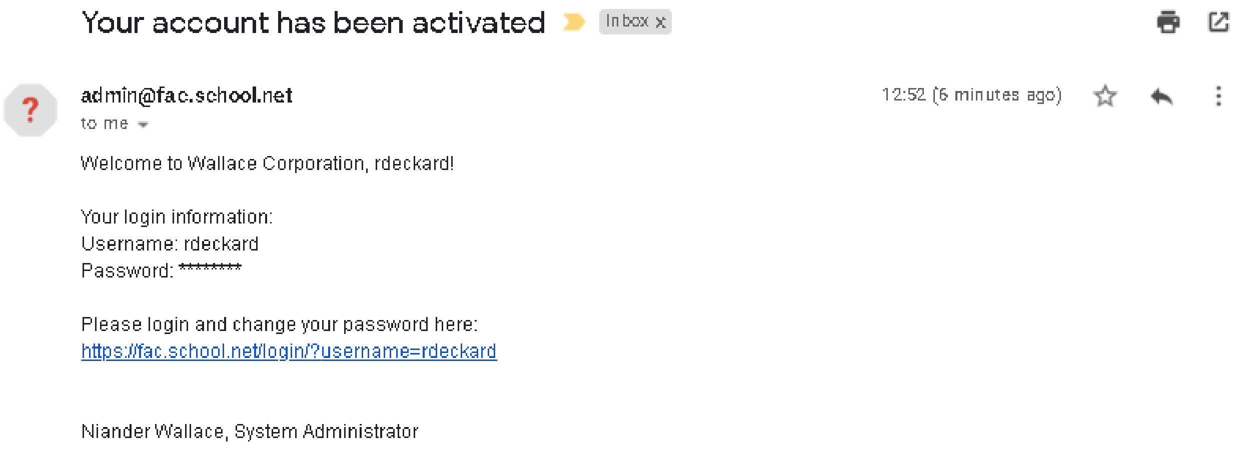


Registration Successful

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

Go back to the login page

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

12:52 (6 minutes ago)

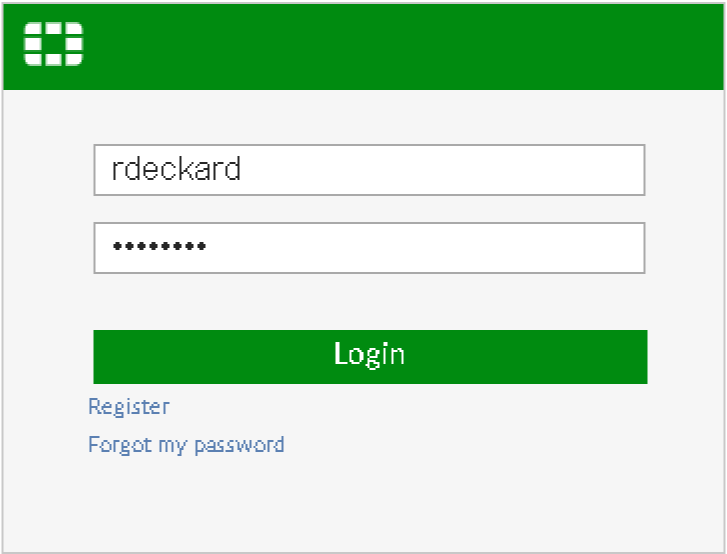
Welcome to Wallace Corporation, rdeckard!

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

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

Niander Wallace, System Administrator

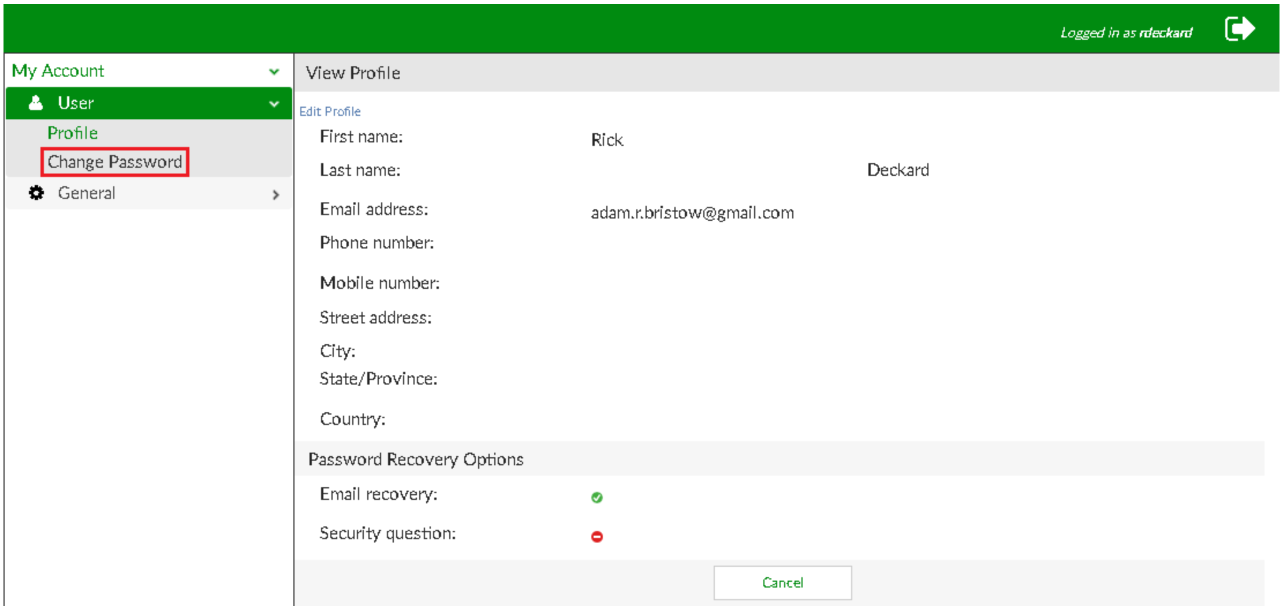
4. Select the link and log in to the user's portal.



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:

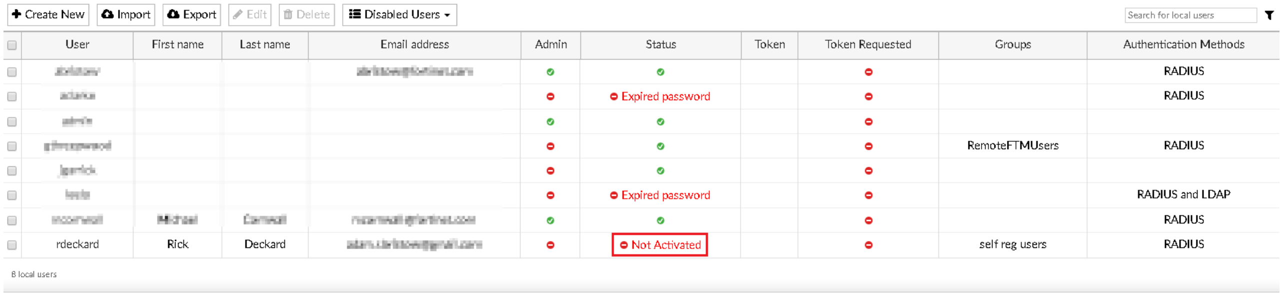
Password Recovery Options

Email recovery: ✓

Security question: ⛔

Results - Administrator approval

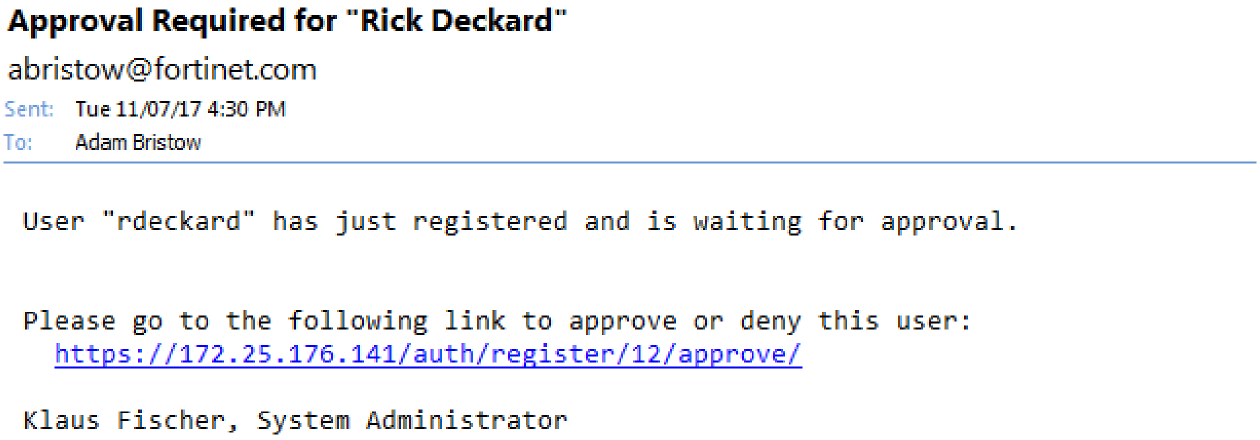
1. After receiving the user's registration request, in the FortiAuthenticator as the administrator, go to *Authentication > User Management > Local Users*. The user has been added, but their *Status* is listed as *Not Activated*.



☐	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"

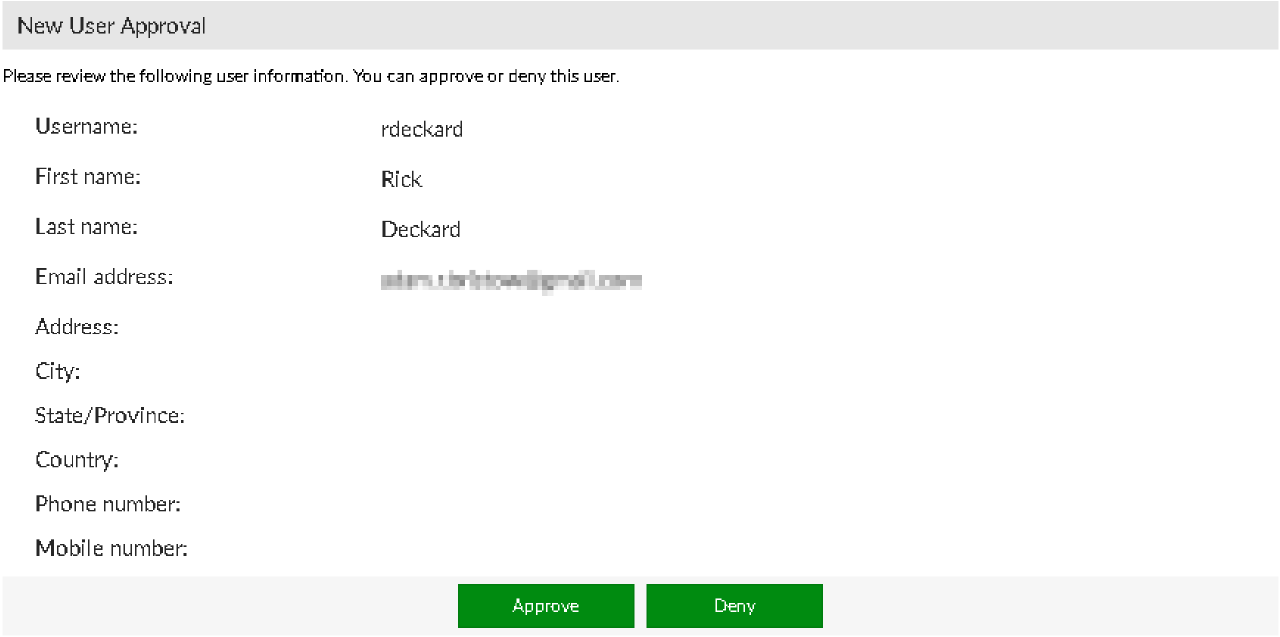
abristow@fortinet.com

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*.

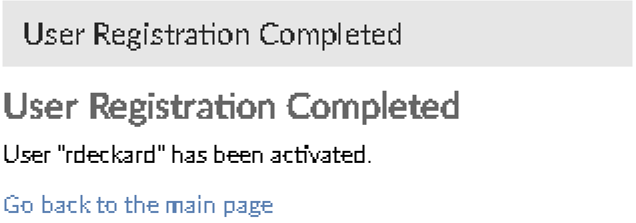


New User Approval

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.



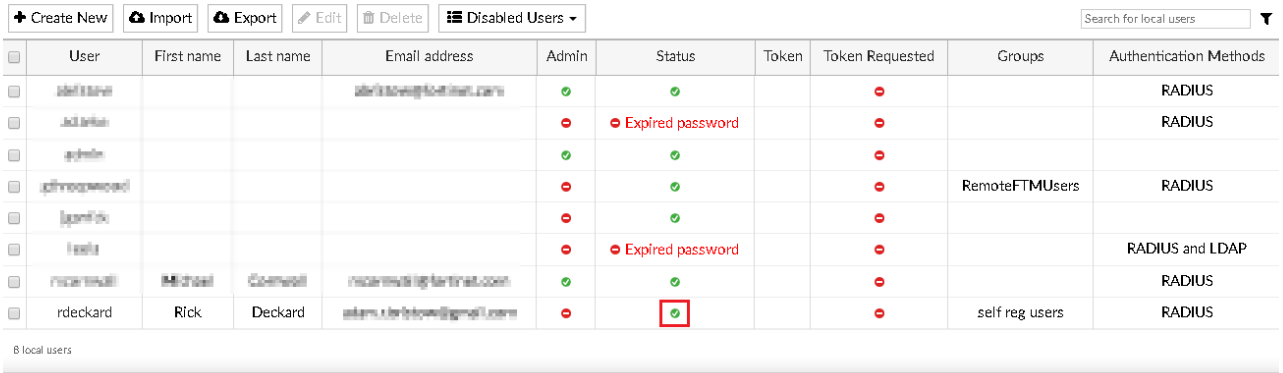
User Registration Completed

User Registration Completed

User "rdeckard" has been activated.

Go back to the main page

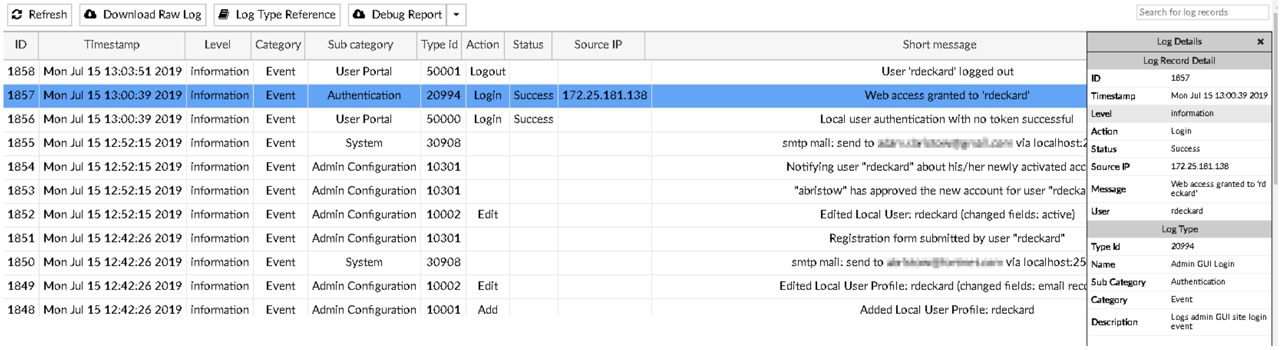
This can be confirmed by going back to *Authentication* > *User Management* > *Local Users*. The user's **Status** has changed to **Enabled**.



□	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.



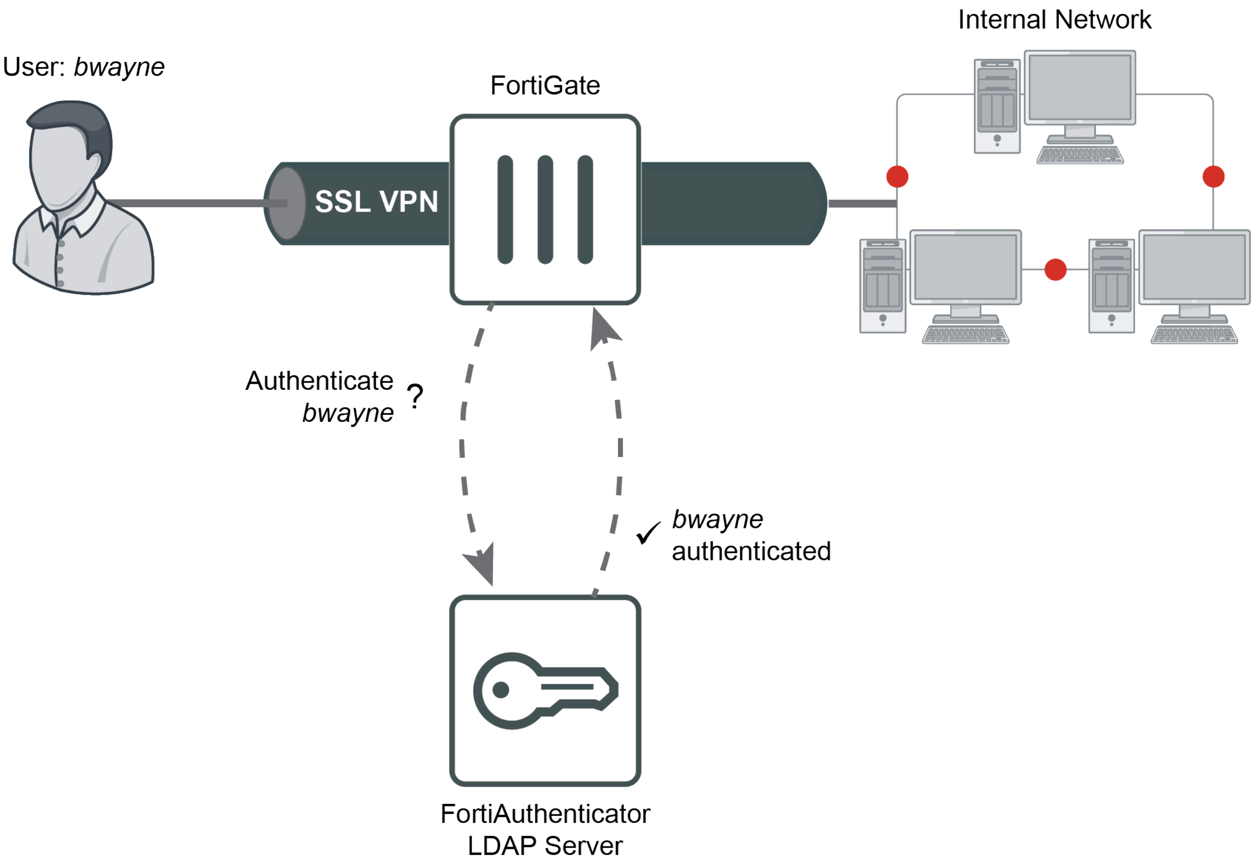
ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message
1858	Mon Jul 15 13:03:51 2019	information	Event	User Portal	50001	Logout			User 'rdeckard' logged out
1857	Mon Jul 15 13:00:39 2019	information	Event	Authentication	20994	Login	Success	172.25.181.138	Web access granted 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 recc
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



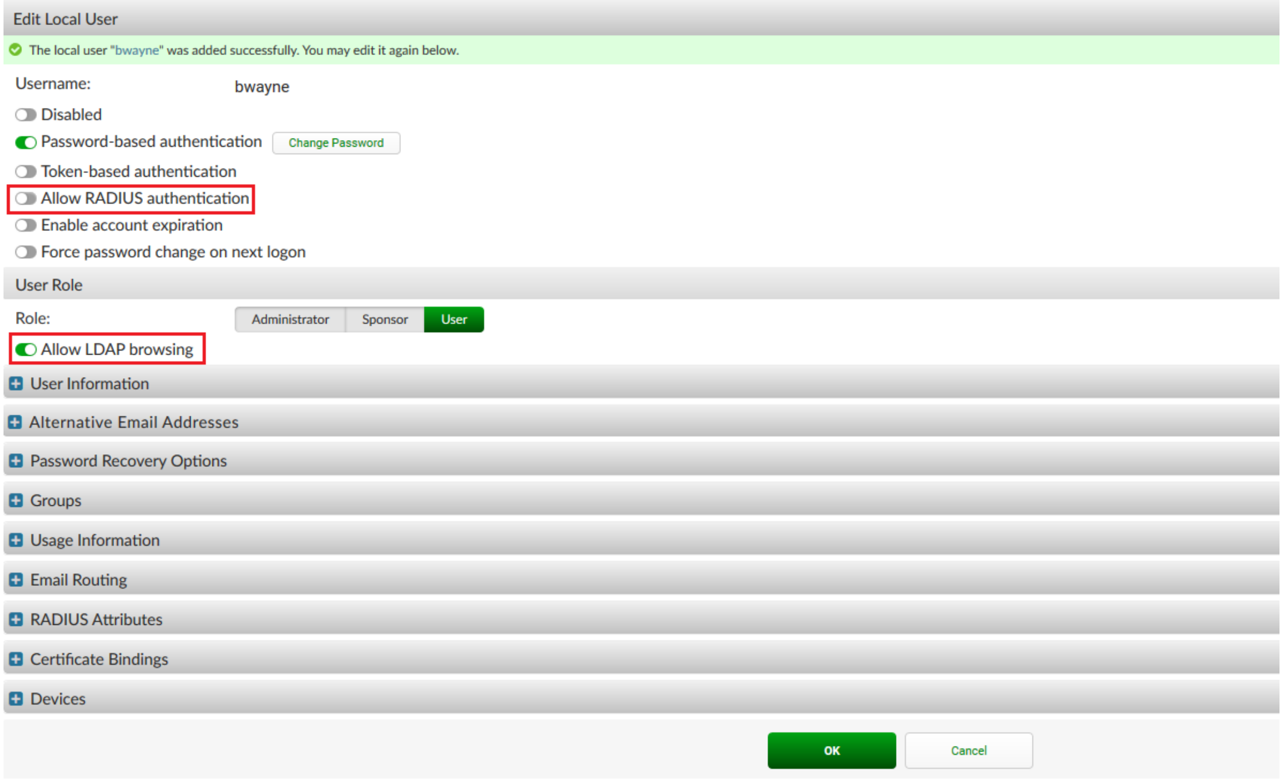
This recipe describes how to set up FortiAuthenticator to function as an LDAP server for FortiGate SSL VPN authentication. It involves adding users to FortiAuthenticator, setting up the LDAP server on the FortiAuthenticator, and then configuring the FortiGate to use the FortiAuthenticator as an LDAP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

○ Token-based authentication

○ Allow RADIUS authentication

○ Enable account expiration

○ Force password change on next logon

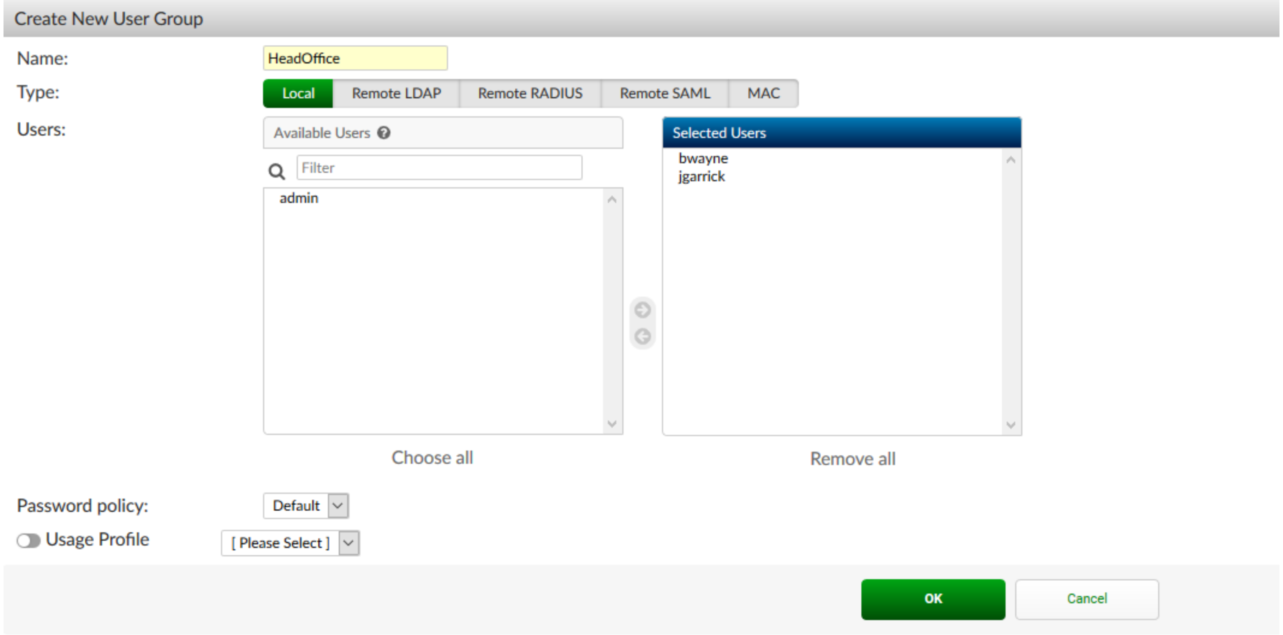
User Role

Role: 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

Users:

Available Users: admin

Selected Users: bwayne, jgarrick

Password policy: Default

○ Usage Profile [Please Select]

Creating the LDAP directory tree on the FortiAuthenticator

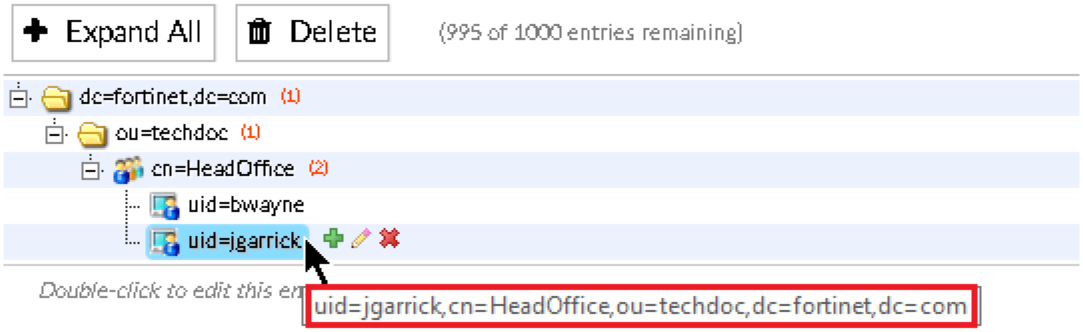
To create the LDAP directory tree:

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.



```
dc=fortinet,dc=com (1)
  ou=techdoc (1)
    cn=HeadOffice (2)
      uid=bwayne
      uid=jgarrick
```

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*.

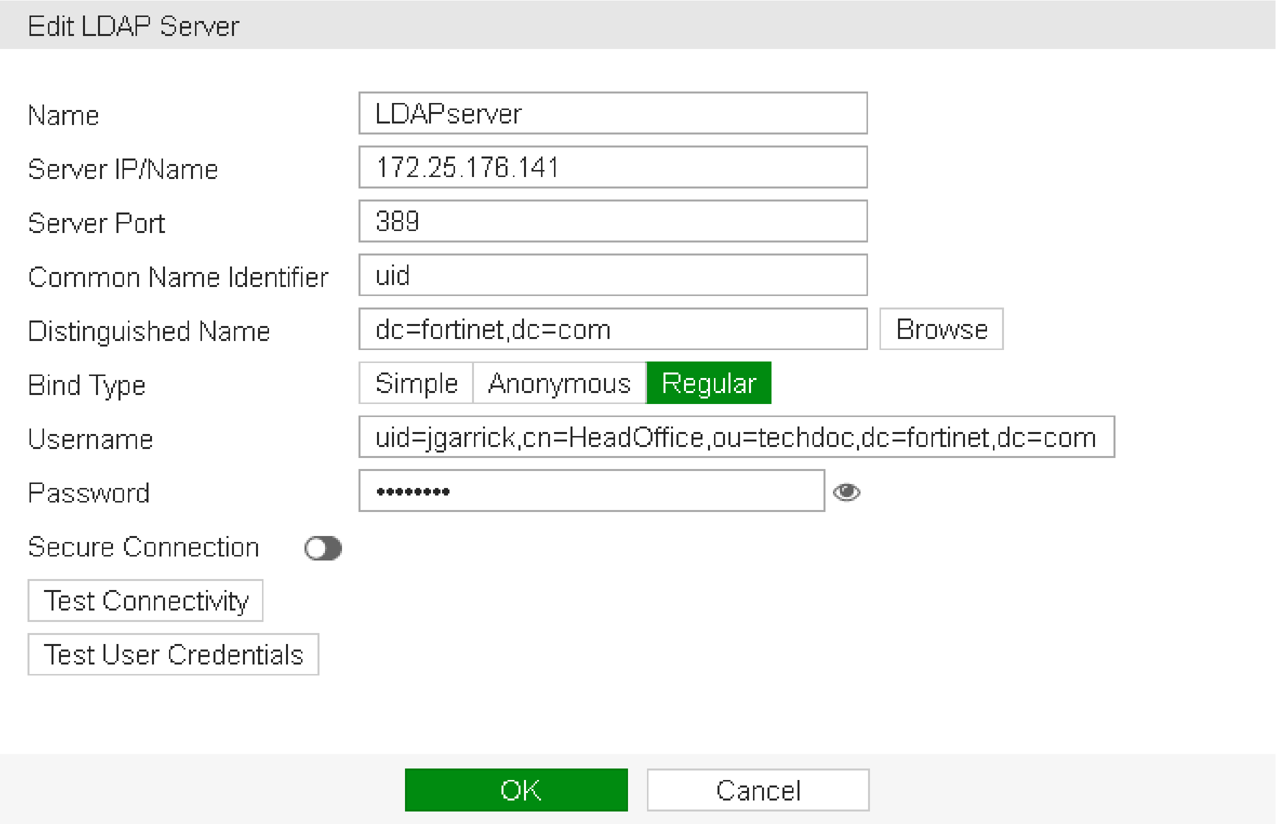
   Enter a name for the LDAP server connection.

   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*.

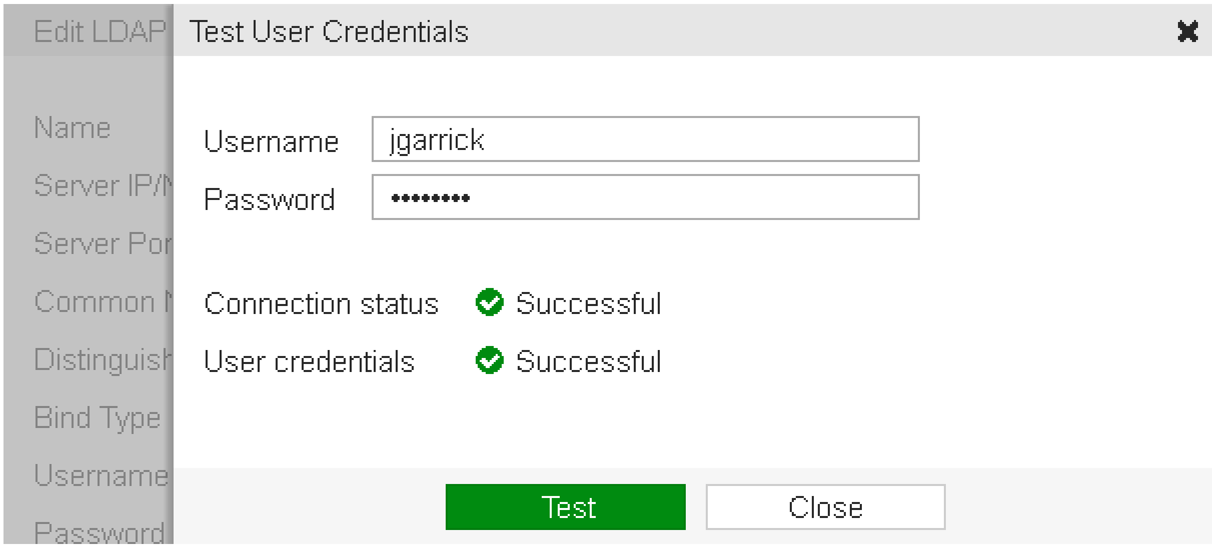
   The DN is an account that the FortiGate uses to query the LDAP server.



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	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.



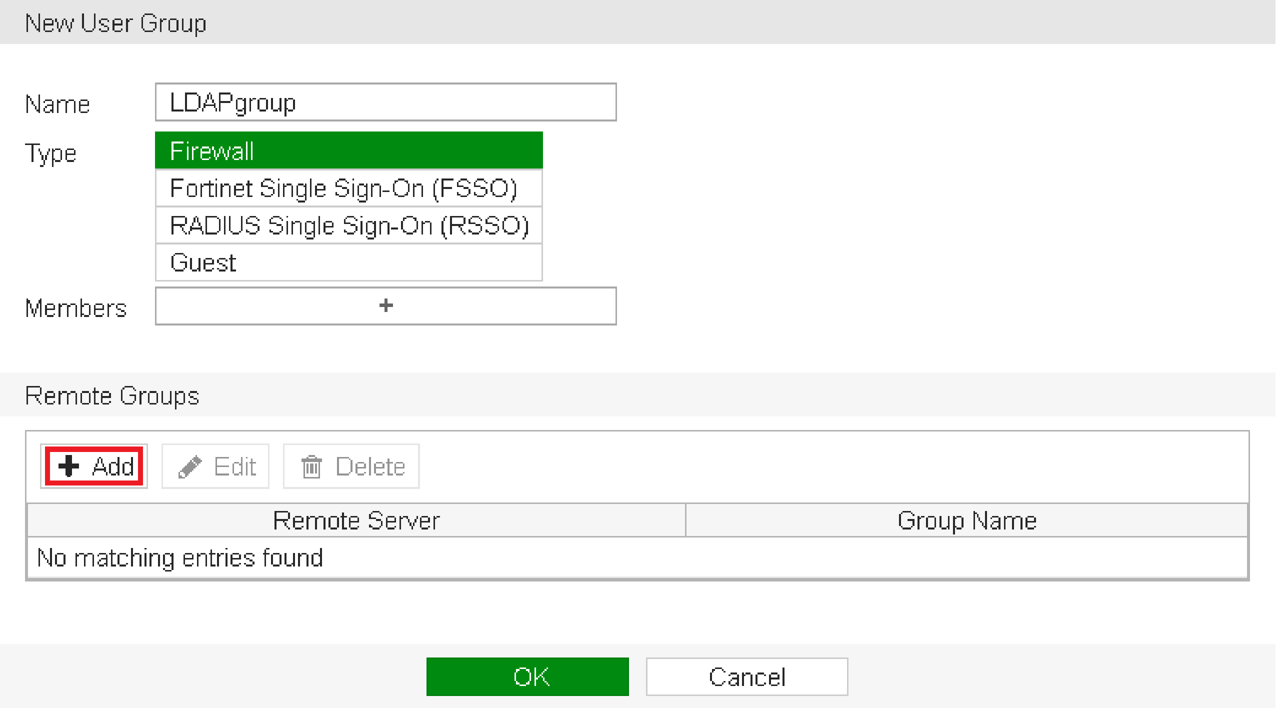
Test User Credentials

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*.



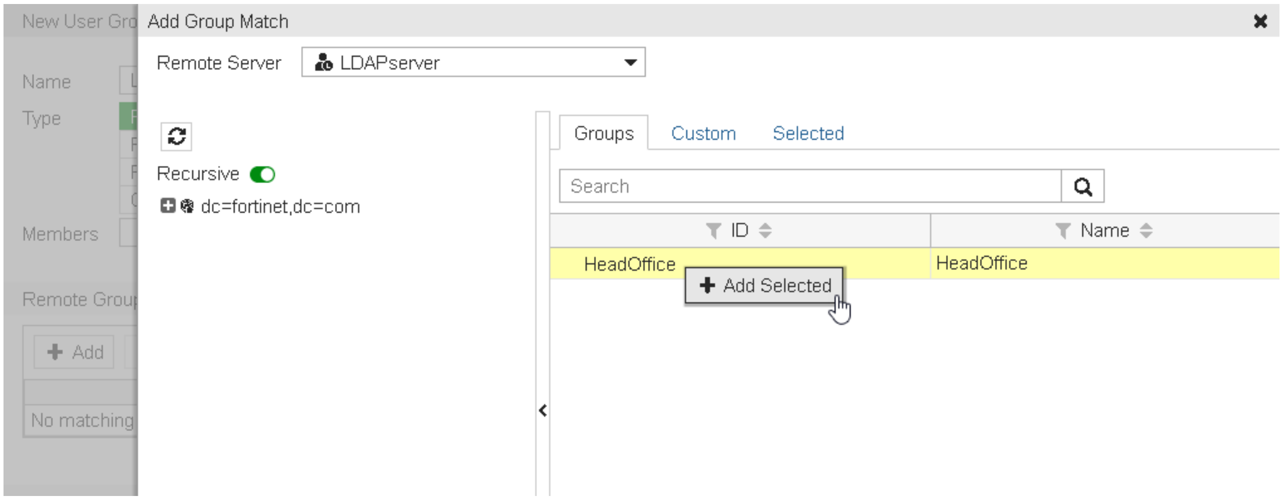
New User Group

Name: LDAPgroup

Type: Firewall

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

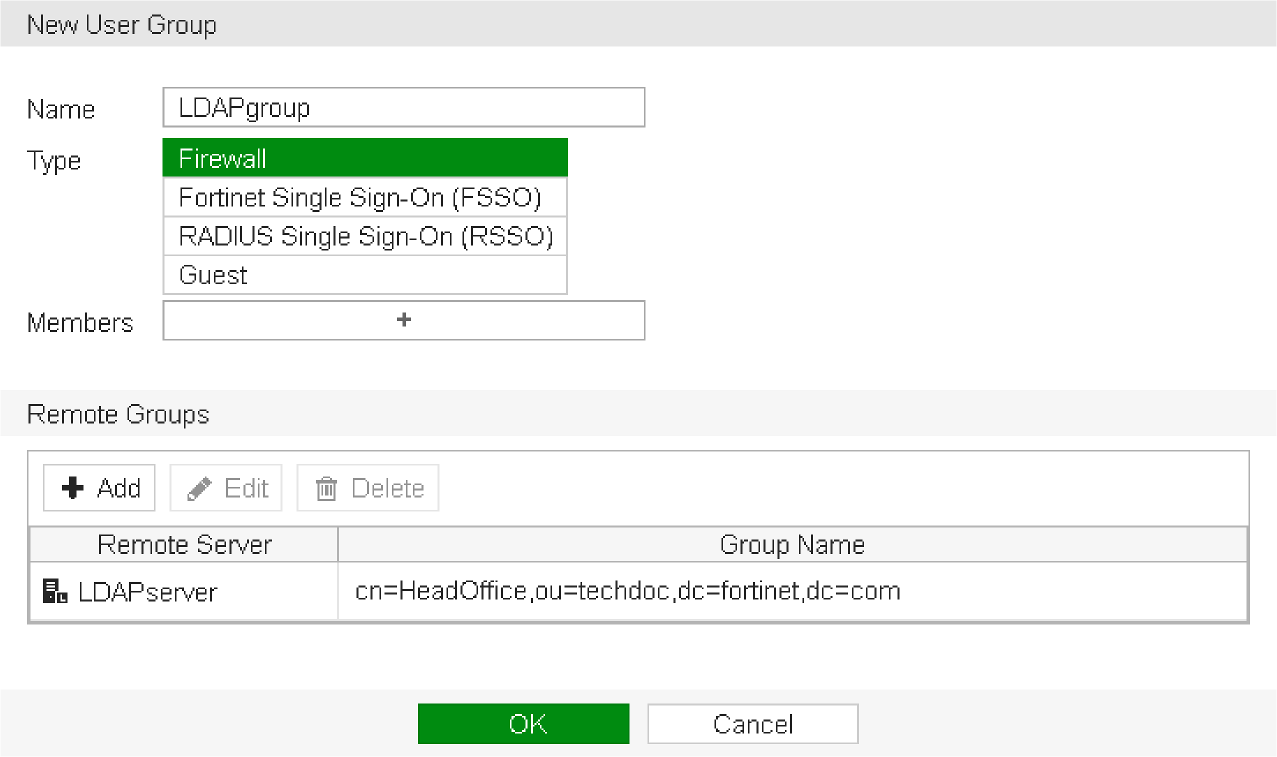
Remote Server: LDAPserver

Recursive: on

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: +

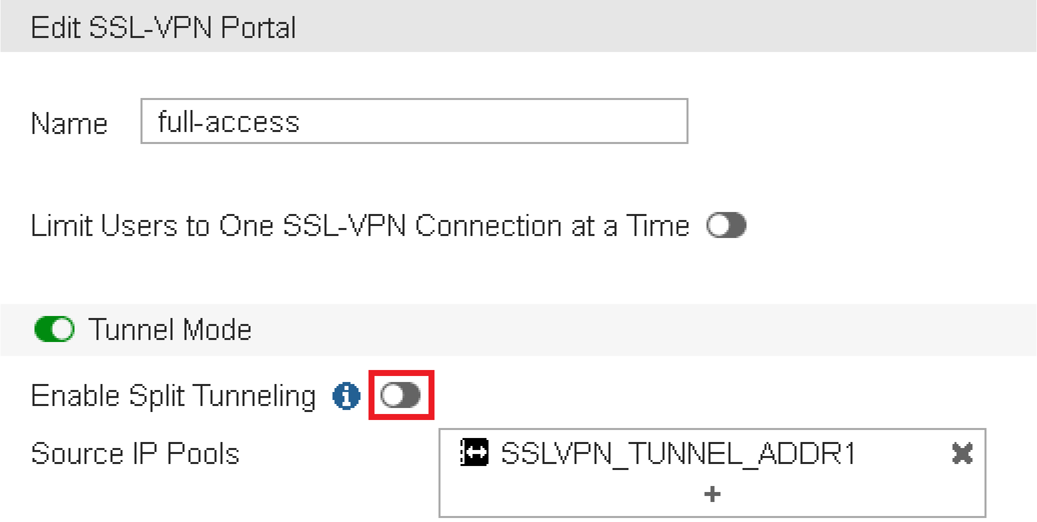
Remote Groups

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: off

Tunnel Mode: on

Enable Split Tunneling: off

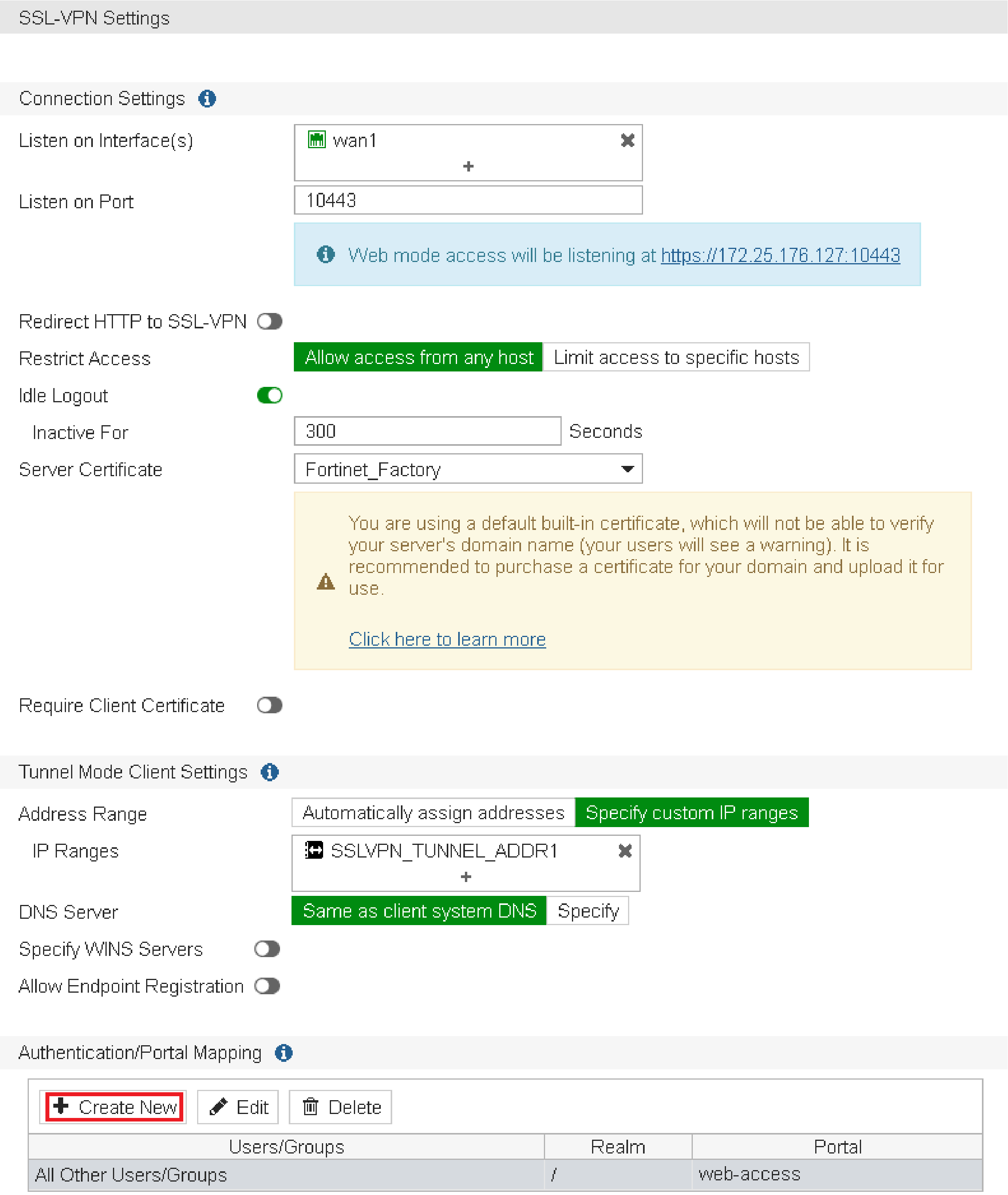
Source IP Pools: SSLVPN_TUNNEL_ADDR1

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

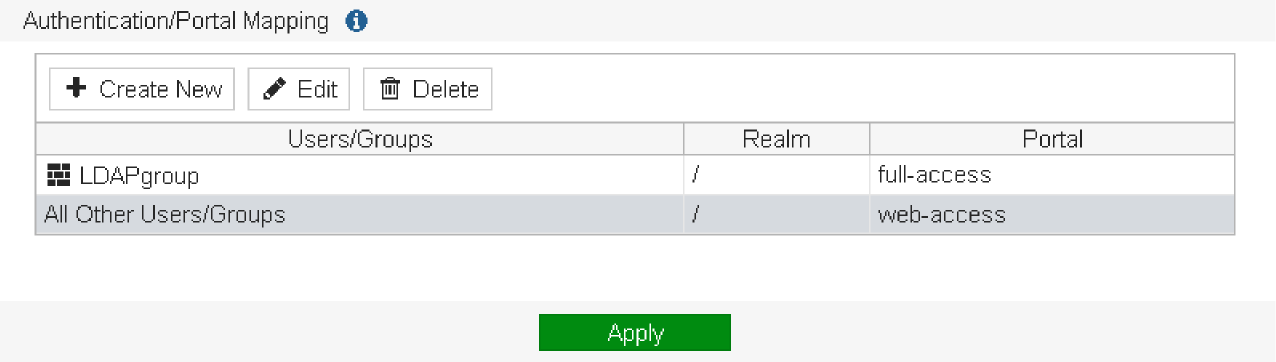
Specify WINS Servers: ○

Allow Endpoint Registration: ○

Authentication/Portal Mapping

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

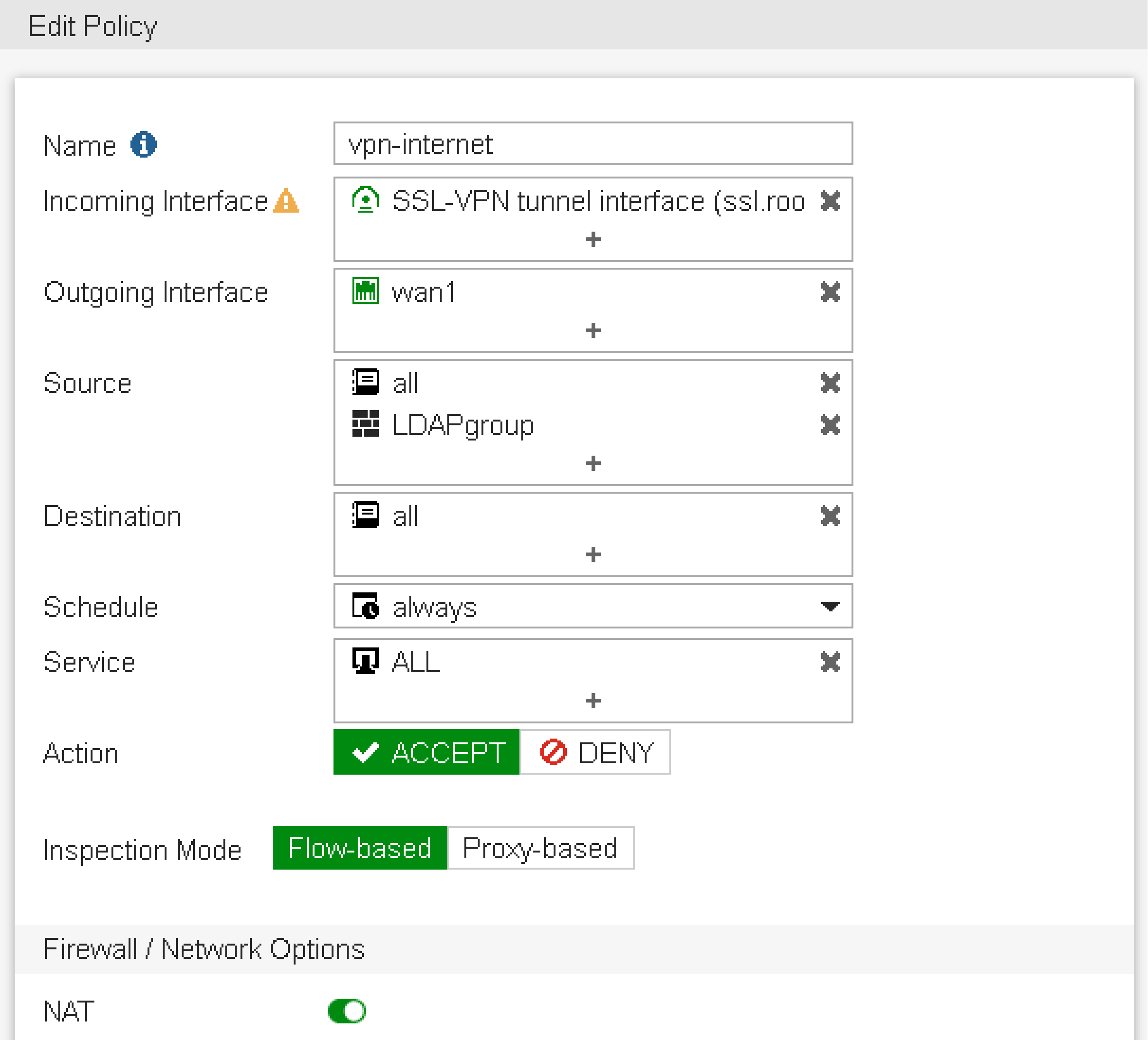
3. Assign the *LDAPgroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to the desired portal. Select *Apply*.



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

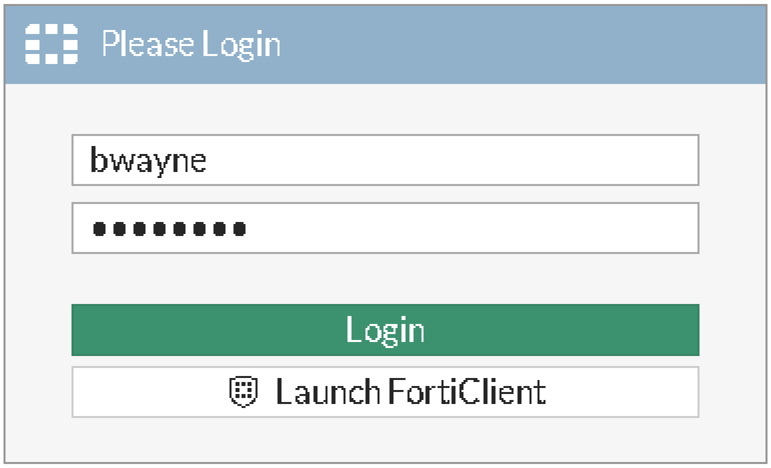
Name	vpn-internet
Incoming Interface	SSL-VPN tunnel interface (ssl.roo
Outgoing Interface	wan1
Source	all LDAPgroup
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT ● DENY
Inspection Mode	Flow-based ● Proxy-based

Firewall / Network Options

NAT ●

Results

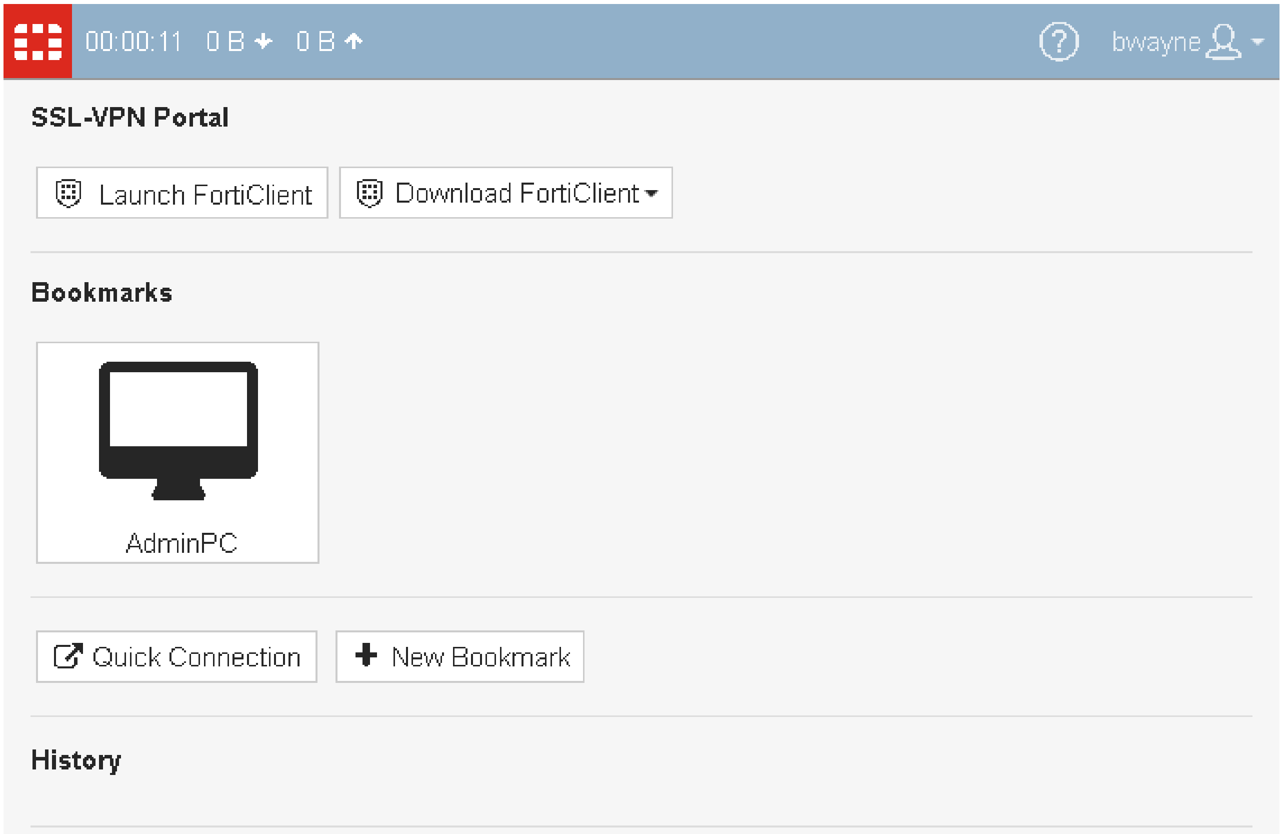
1. From a remote device, access the SSL VPN Web Portal.
   Enter valid LDAP credentials (in the example, bwayne).



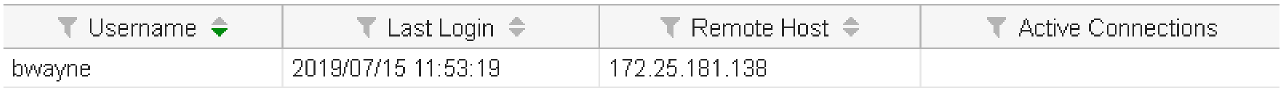
bwayne

●●●●●●●●●

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

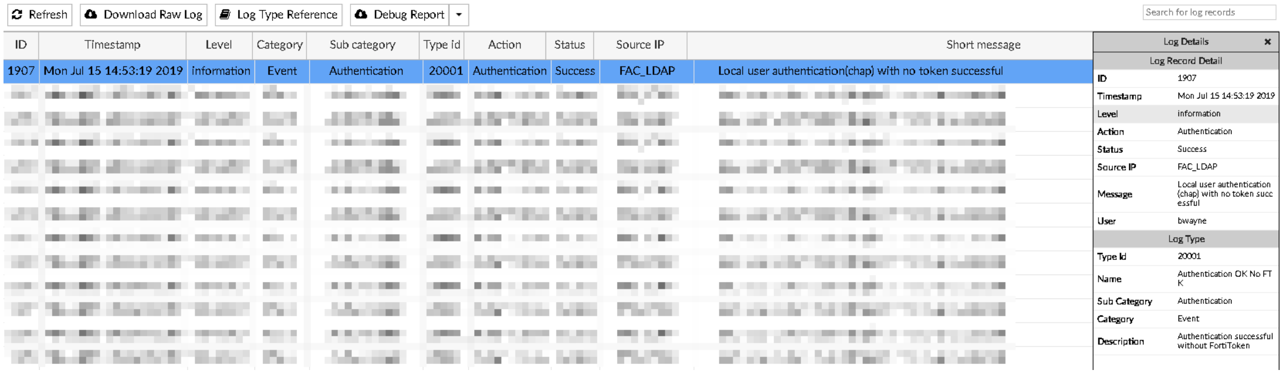


3. On the FortiGate, go to *Monitor* > *SSL-VPN Monitor* to confirm the connection.



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.

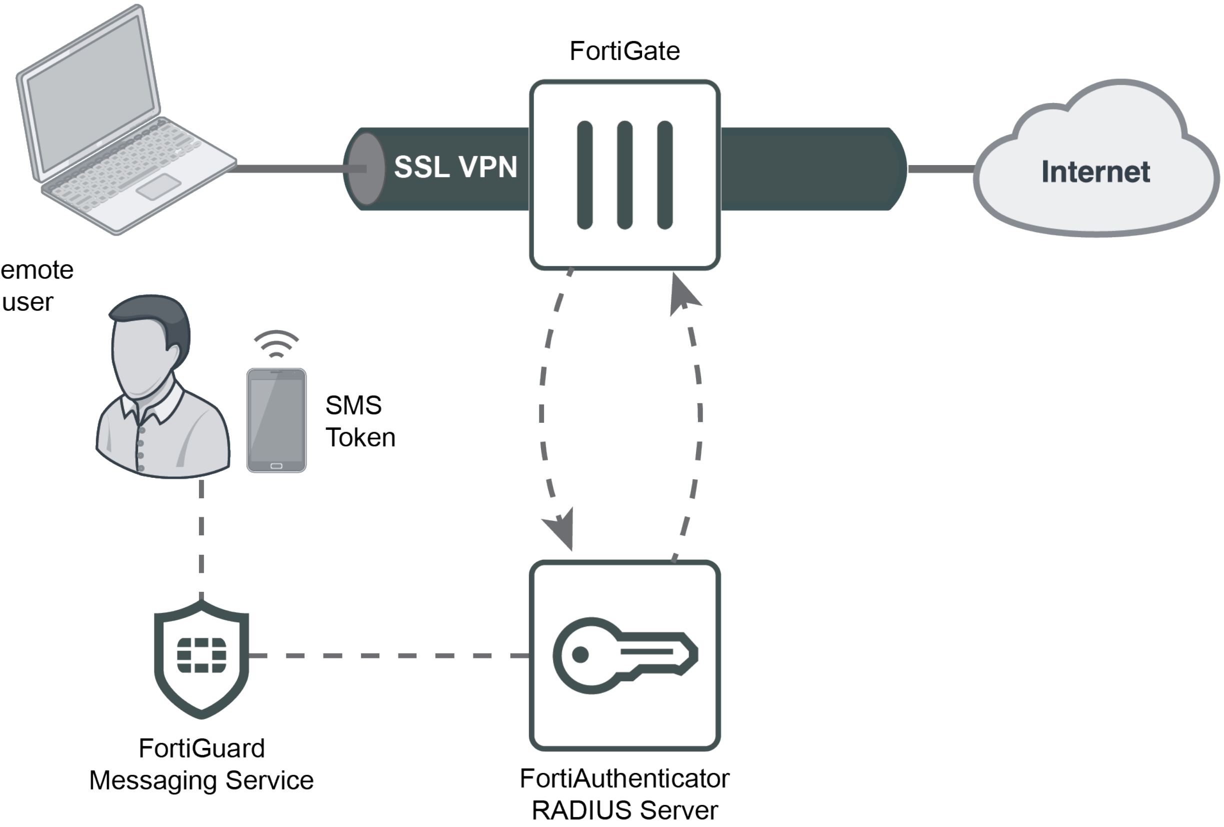


ID	Timestamp	Level	Category	Sub category	Type id	Action	Status	Source IP	Short message
1907	Mon Jul 15 14:53:19 2019	information	Event	Authentication	20001	Authentication	Success	FAC_LDAP	Local user authentication(chap) with no token successful

[redacted]

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.

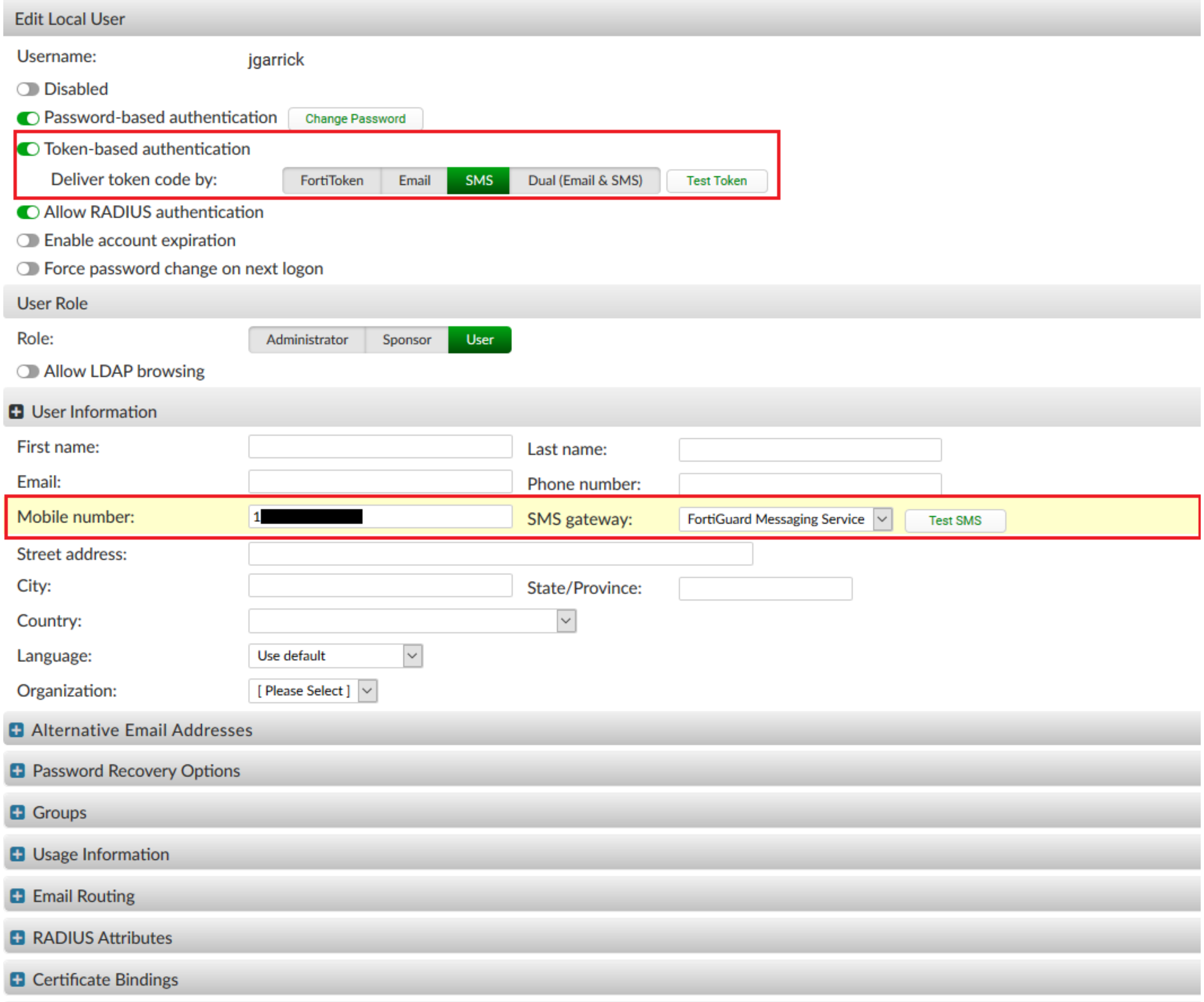
When a user attempts to connect to this SSL VPN, they are prompted to enter their username and password. After successfully entering their credentials, they receive an SMS message on their mobile phone containing a 6-digit number (called the FortiToken code). They must also enter this number to get access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

● Token-based authentication

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

● 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 [Test SMS]
Street address:			
City:		State/Province:	
Country:			
Language:	Use default		
Organization:	[Please Select]		

Alternative Email Addresses

Password Recovery Options

Groups

Usage Information

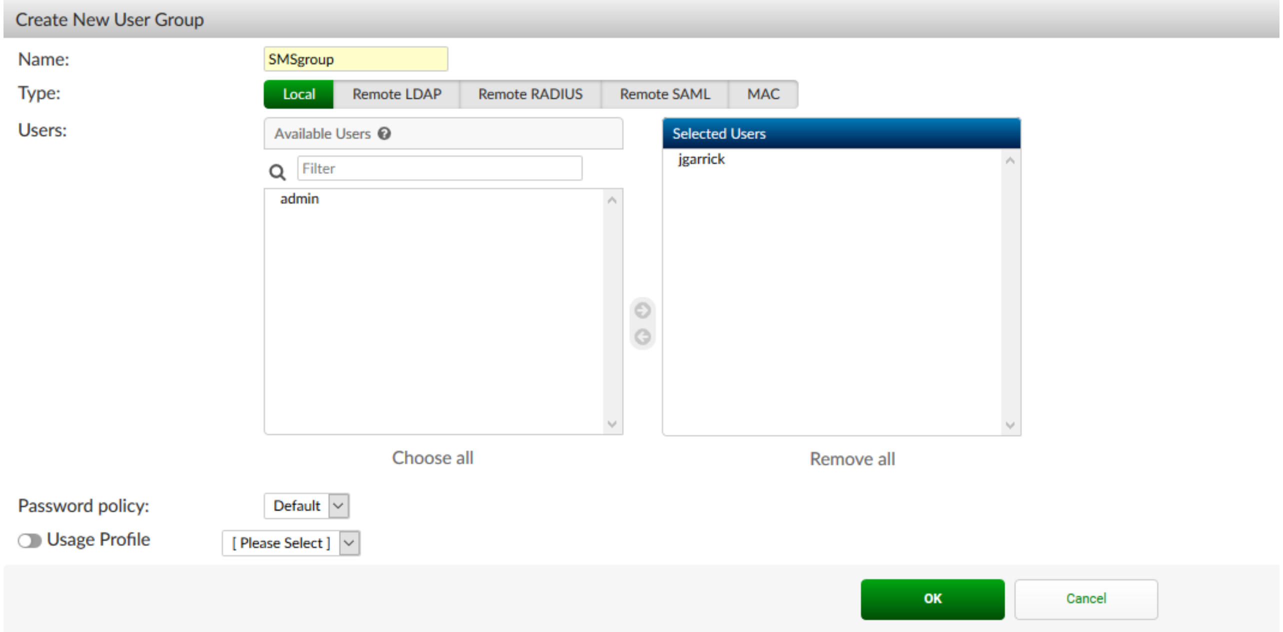
Email Routing

RADIUS Attributes

Certificate Bindings

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:

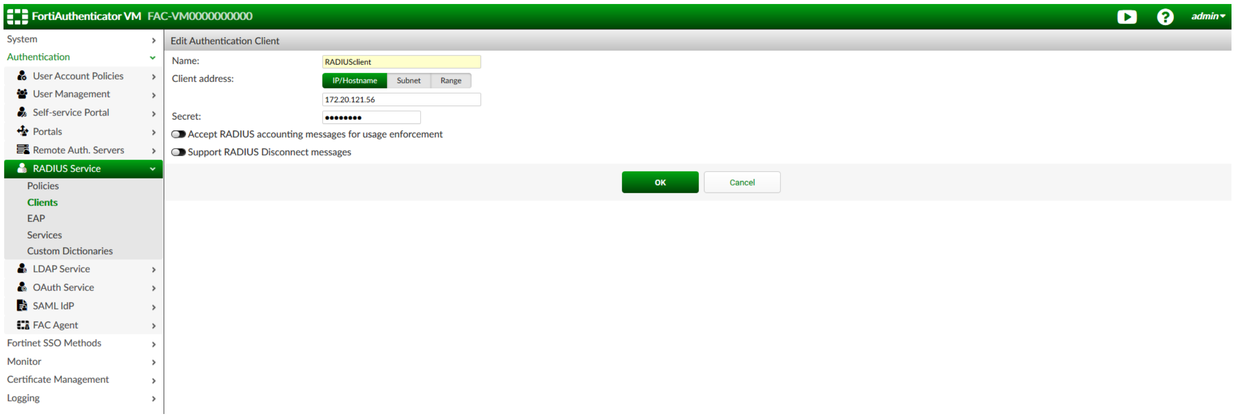
Selected Users: jgarrick

Password policy: Default

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

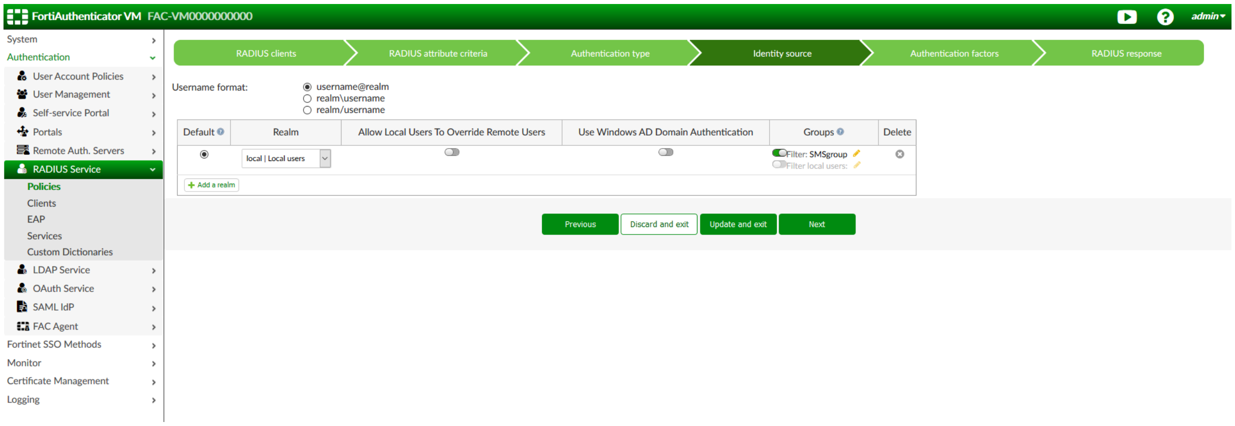
172.20.121.56

Secret: ••••••••

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

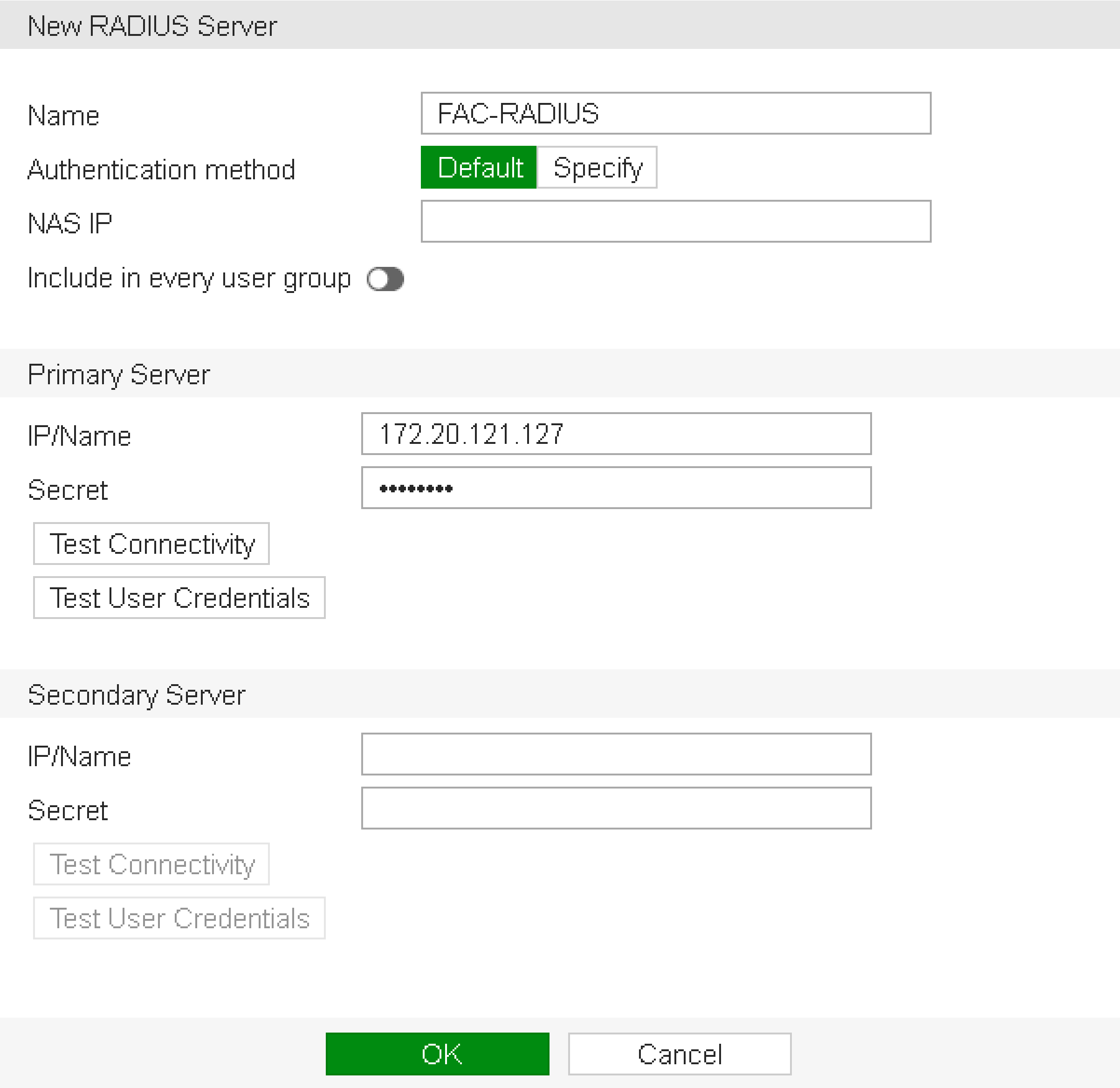
Default	Realm	Allow Local Users To Override Remote Users	Use Windows AD Domain Authentication	Groups	Delete
●	local | Local users			Filter: SMSgroup Filter local users:	

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

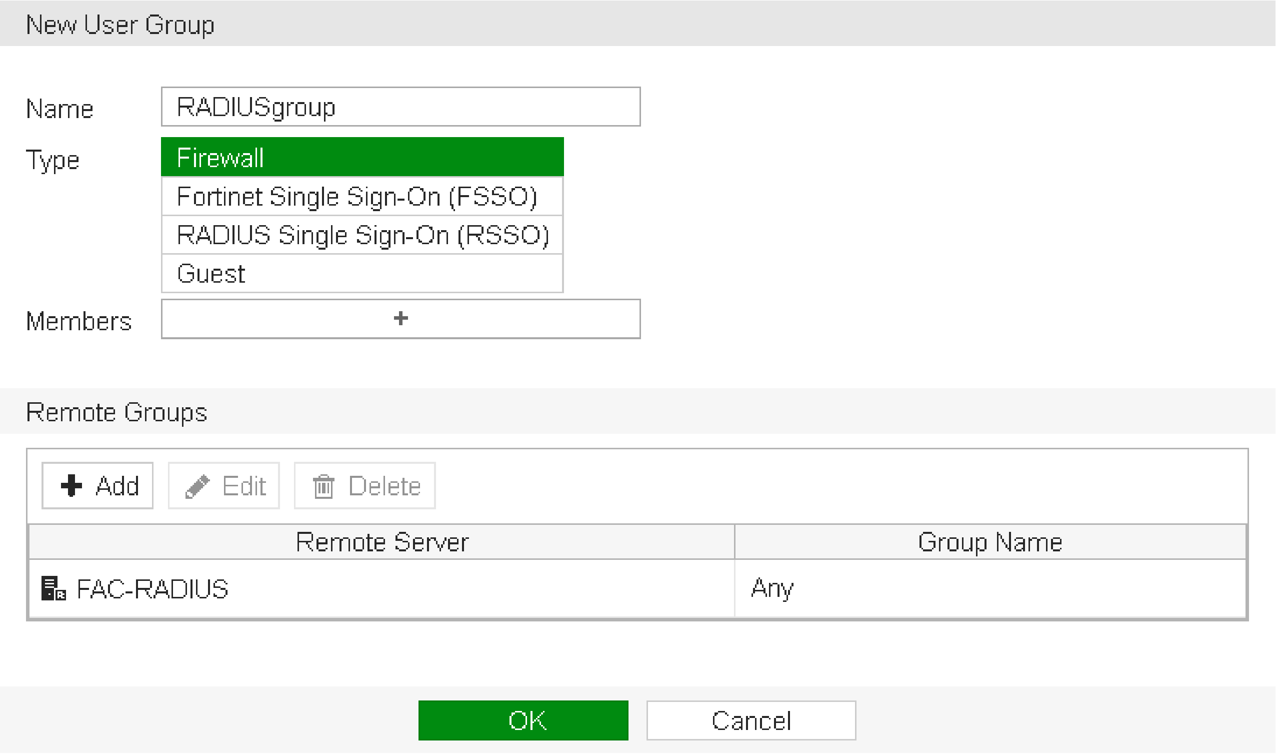
Secret: •••••••••

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
Members	+

Remote Groups

Remote Server	Group Name
FAC-RADIUS	Any

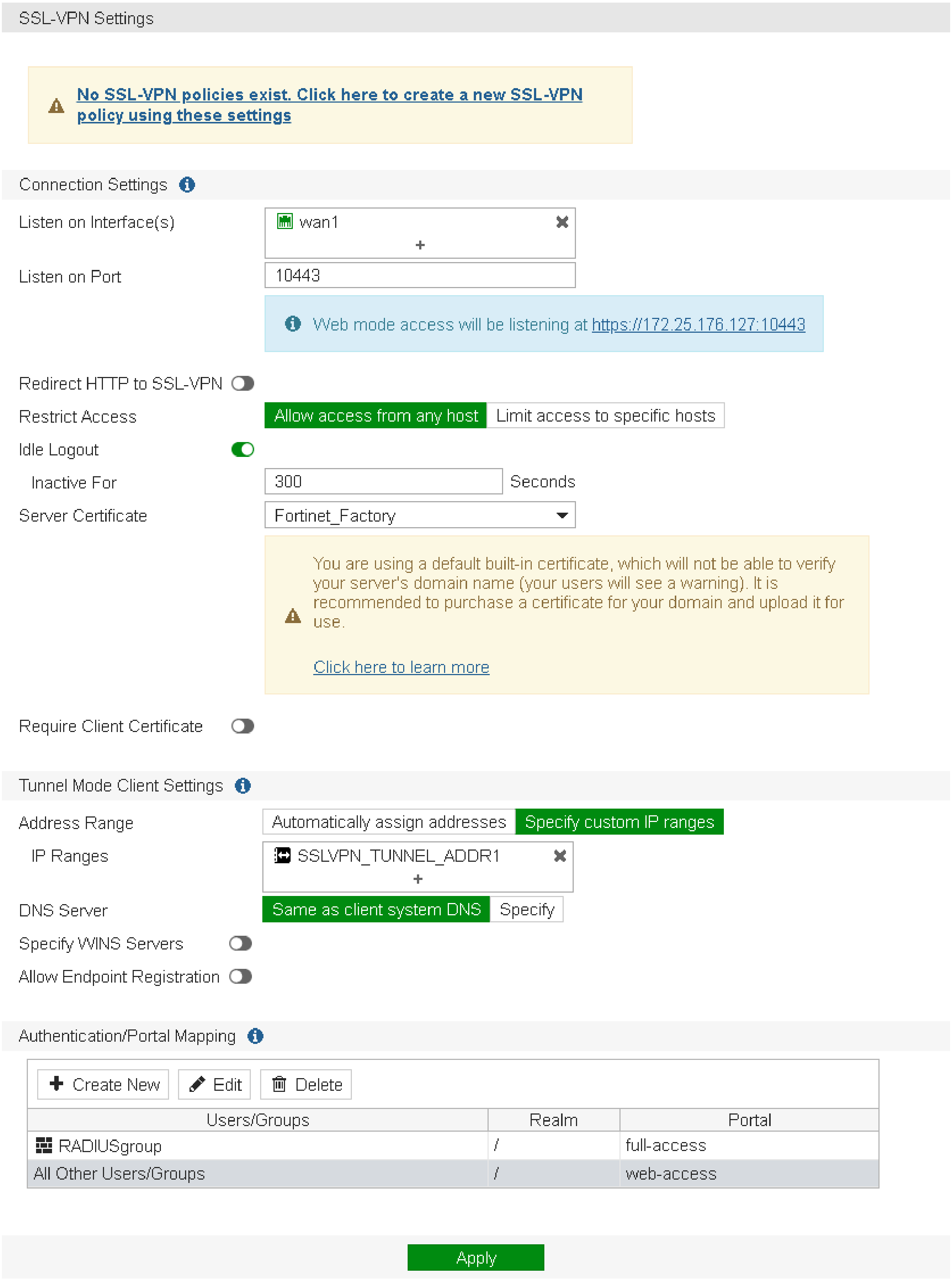
Configuring the SSL-VPN

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

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: ○

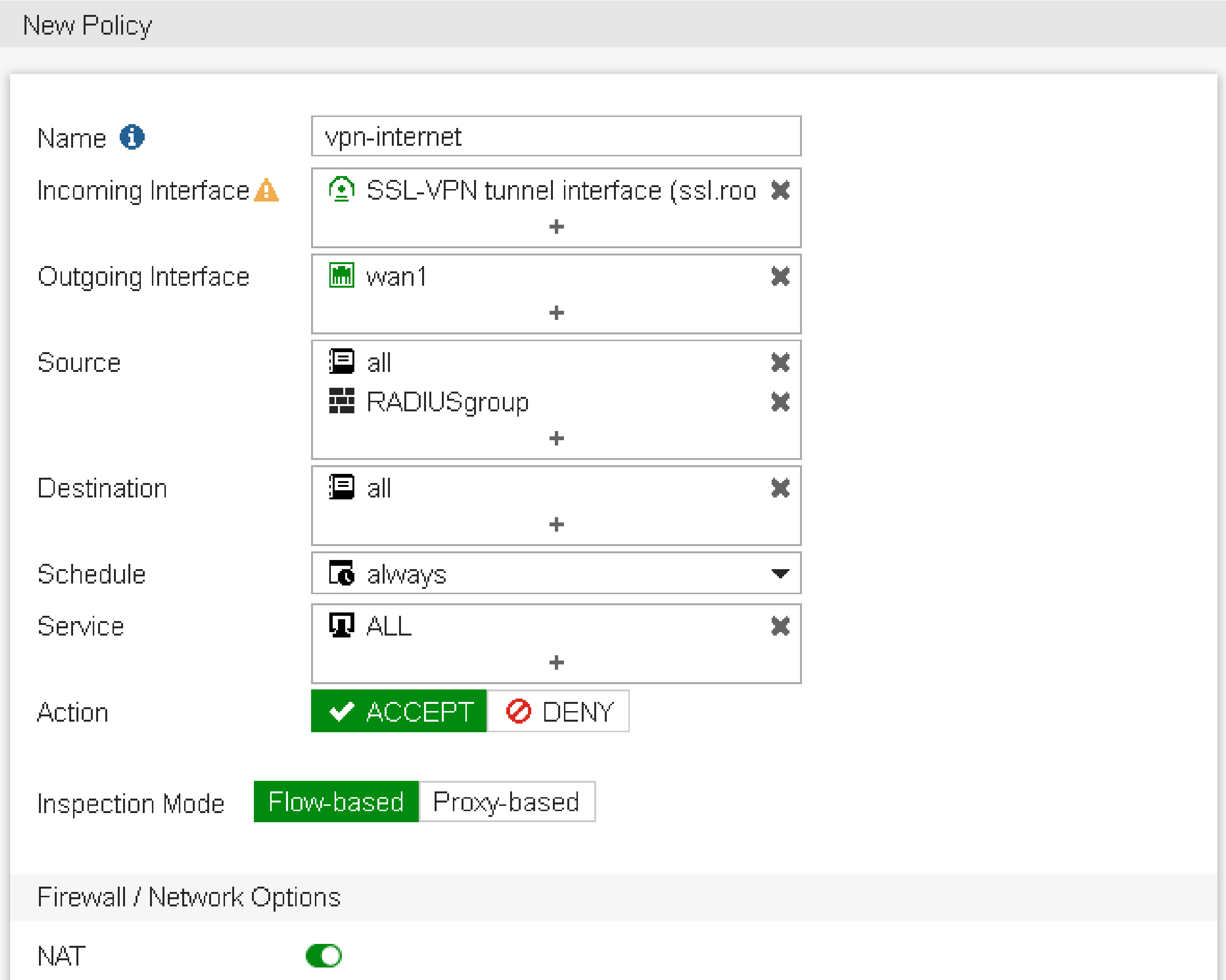
Authentication/Portal Mapping

Users/Groups	Realm	Portal
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

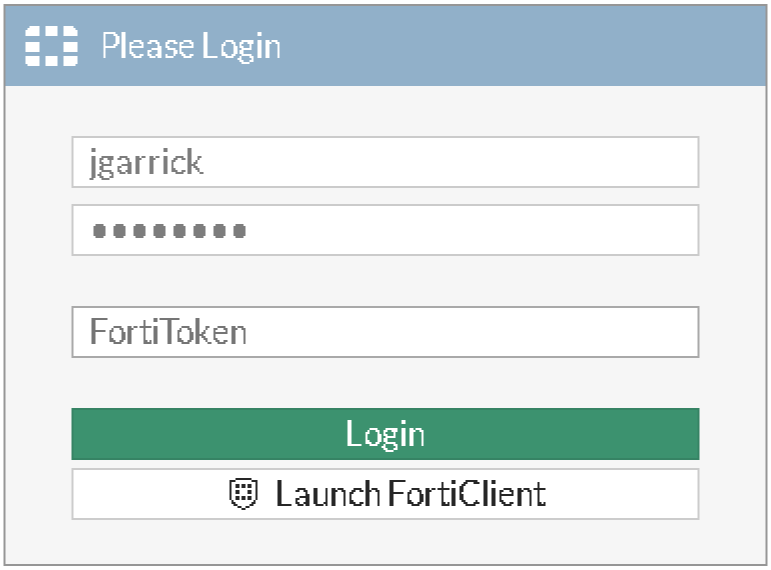
NAT	●

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:

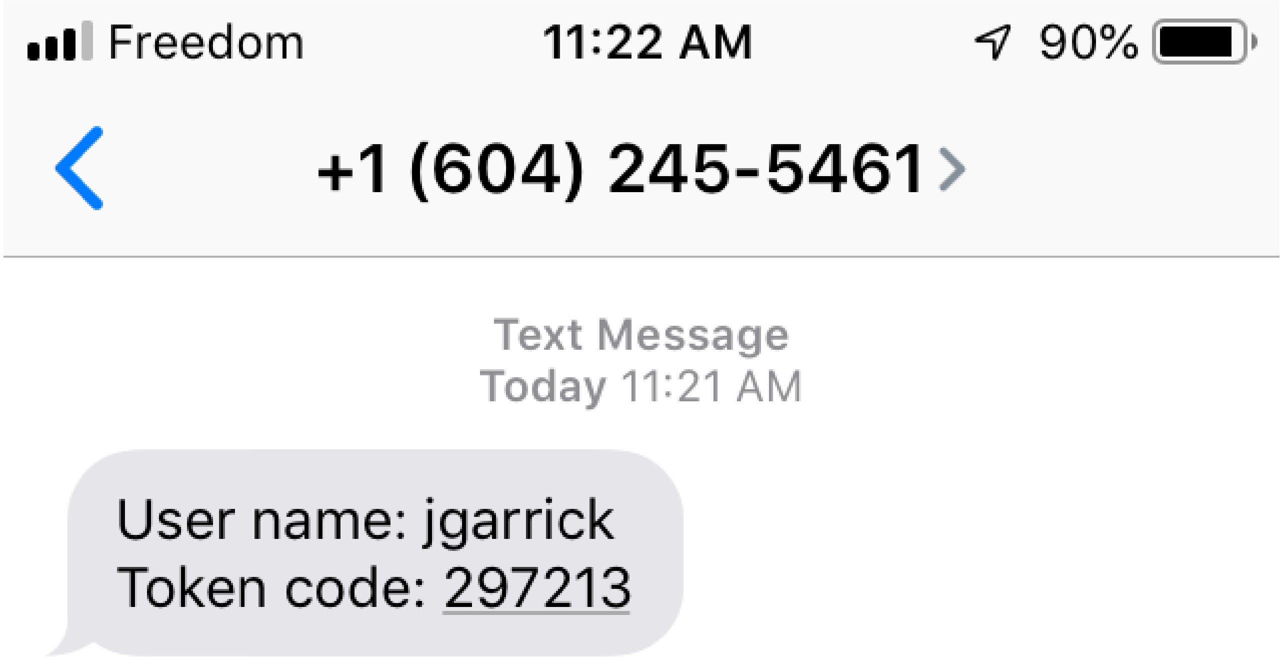
1. Open a browser and navigate to the SSL VPN web portal, in this case *https://172.25.176.127:10443*.
   Enter a valid username and password and select *Login*. You should be prompted to enter a *FortiToken Code*.



jgarrick

•••••••••

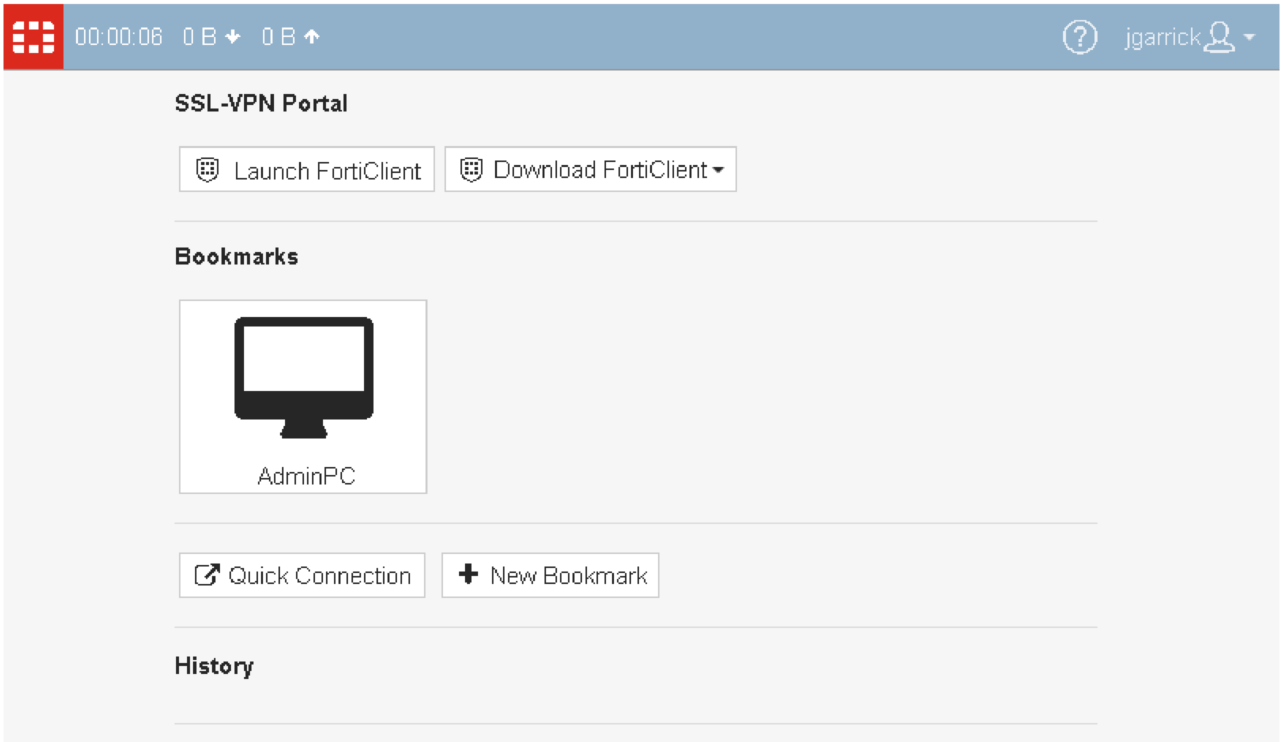
2. The *FortiToken Code* should have been sent to your mobile phone as a text message containing a 6-digit number. Enter the number into the SSL VPN login portal and select *Login*.



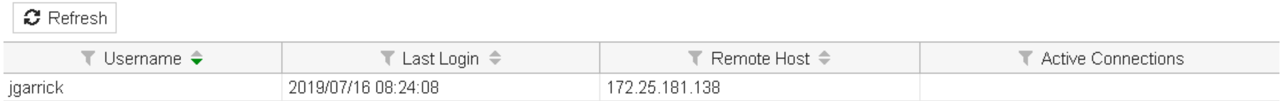
Text Message
Today 11:21 AM

User name: jgarrick
Token code: 297213

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

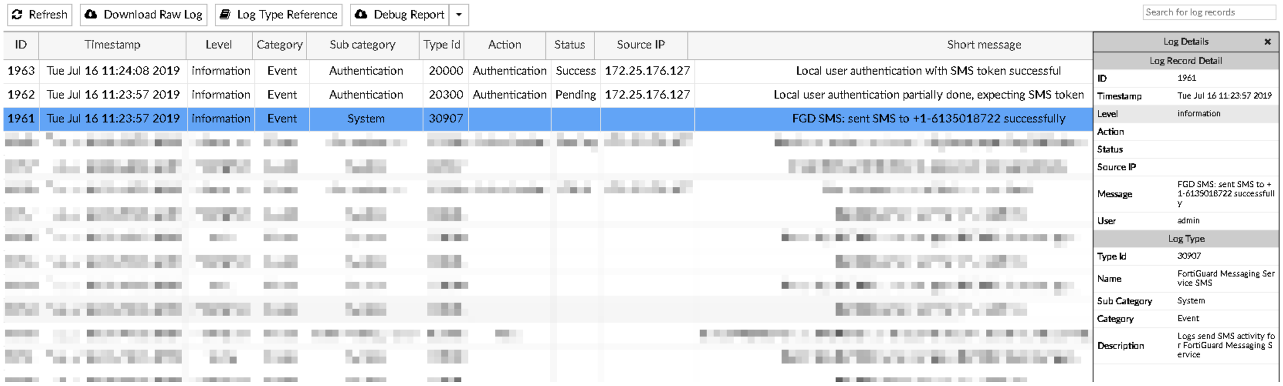


4. To verify that the user has connected to the tunnel, on the FortiGate, go to *Monitor* > *SSL-VPN Monitor*.



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.



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

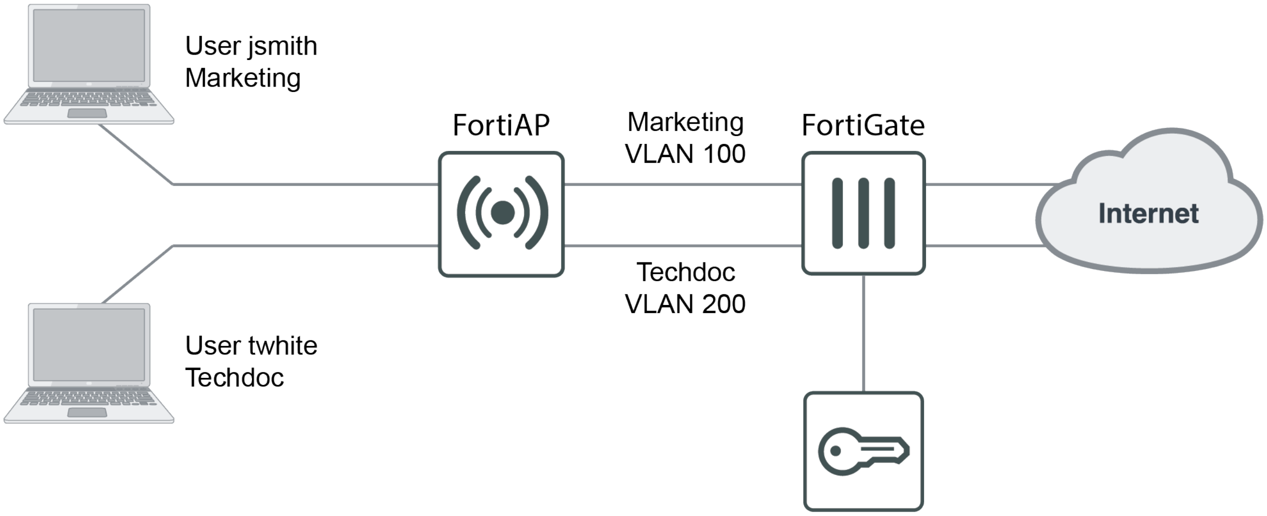
Log Details

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.

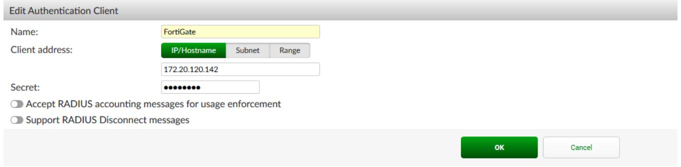
This example creates dynamic VLANs for the Techdoc and Marketing departments. The RADIUS server is a FortiAuthenticator. It is assumed a user group on the FortiAuthenticator has already been created (in this example, *employees*).

```
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

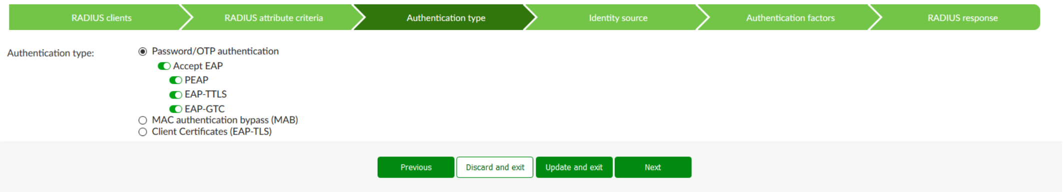
Secret: ●●●●●●●●

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

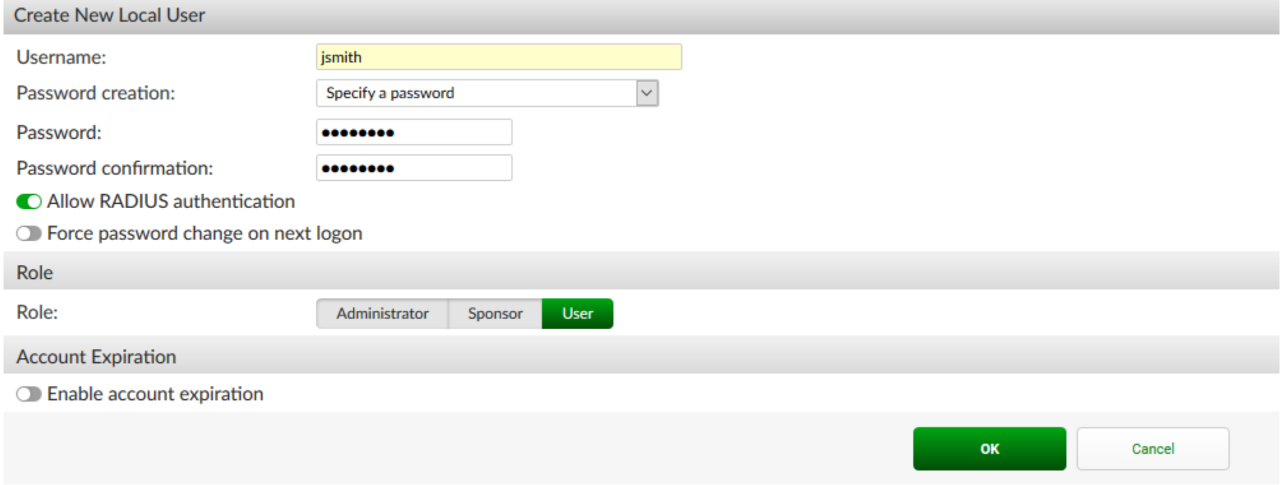
○ MAC authentication bypass (MAB)

○ 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

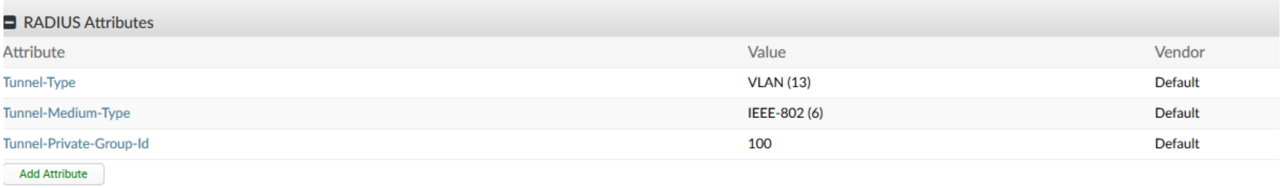
Account Expiration

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

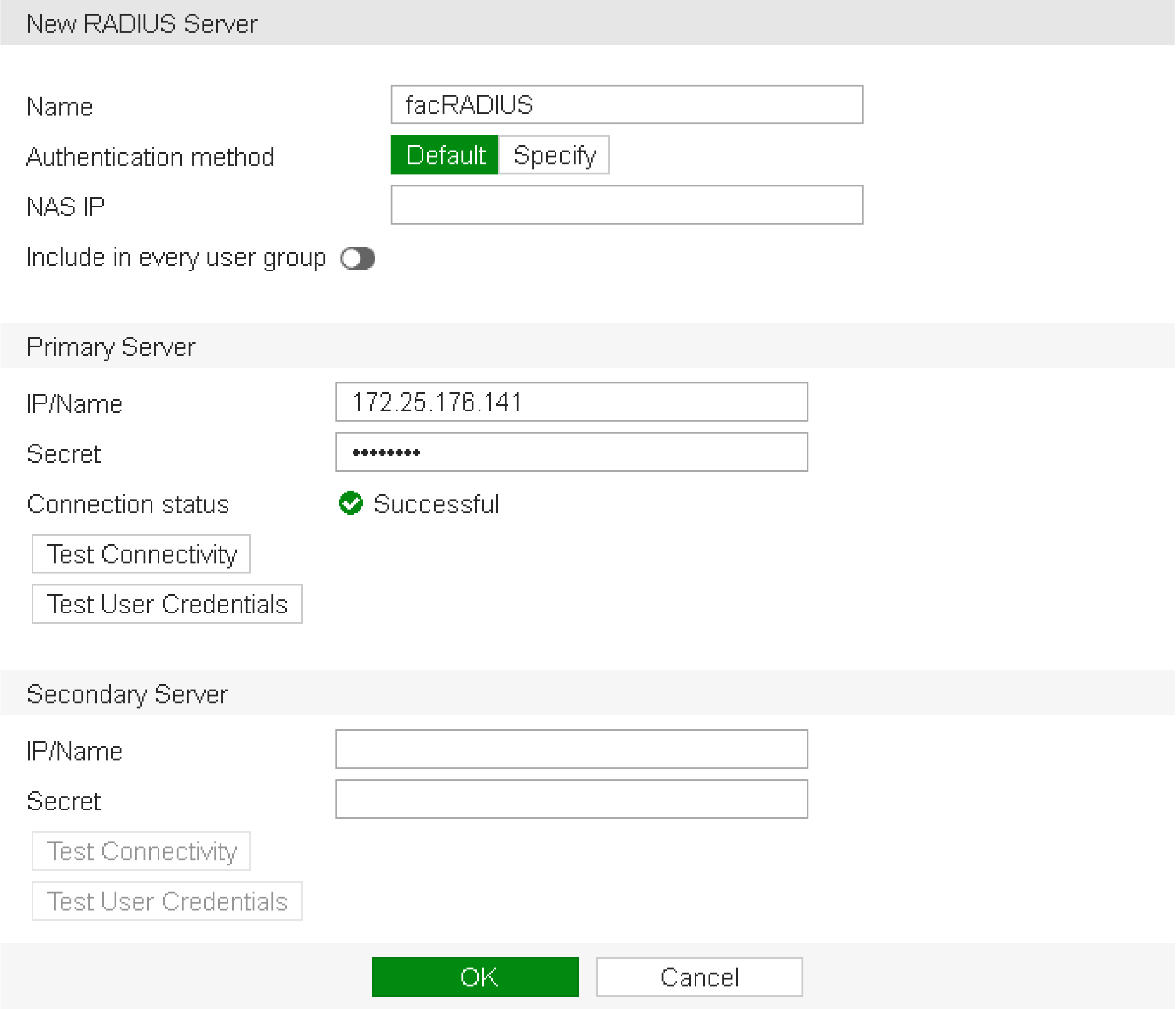
Attribute	Value	Vendor
Tunnel-Type	VLAN (13)	Default
Tunnel-Medium-Type	IEEE-802 (6)	Default
Tunnel-Private-Group-Id	100	Default

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 (selected) / Specify
NAS IP	
Include in every user group	○

Primary Server

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

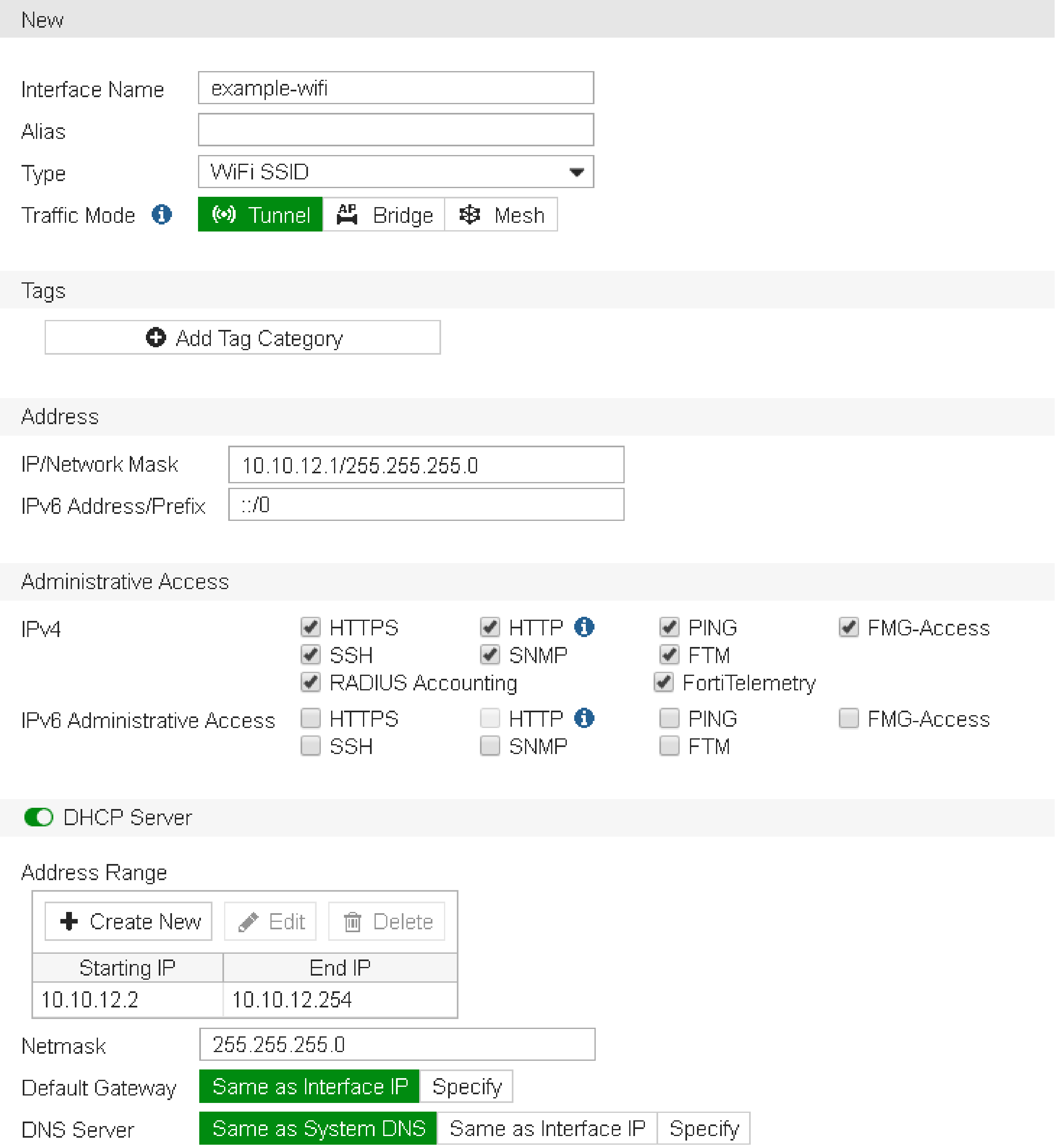
Secondary Server

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

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 (enabled)

Address Range

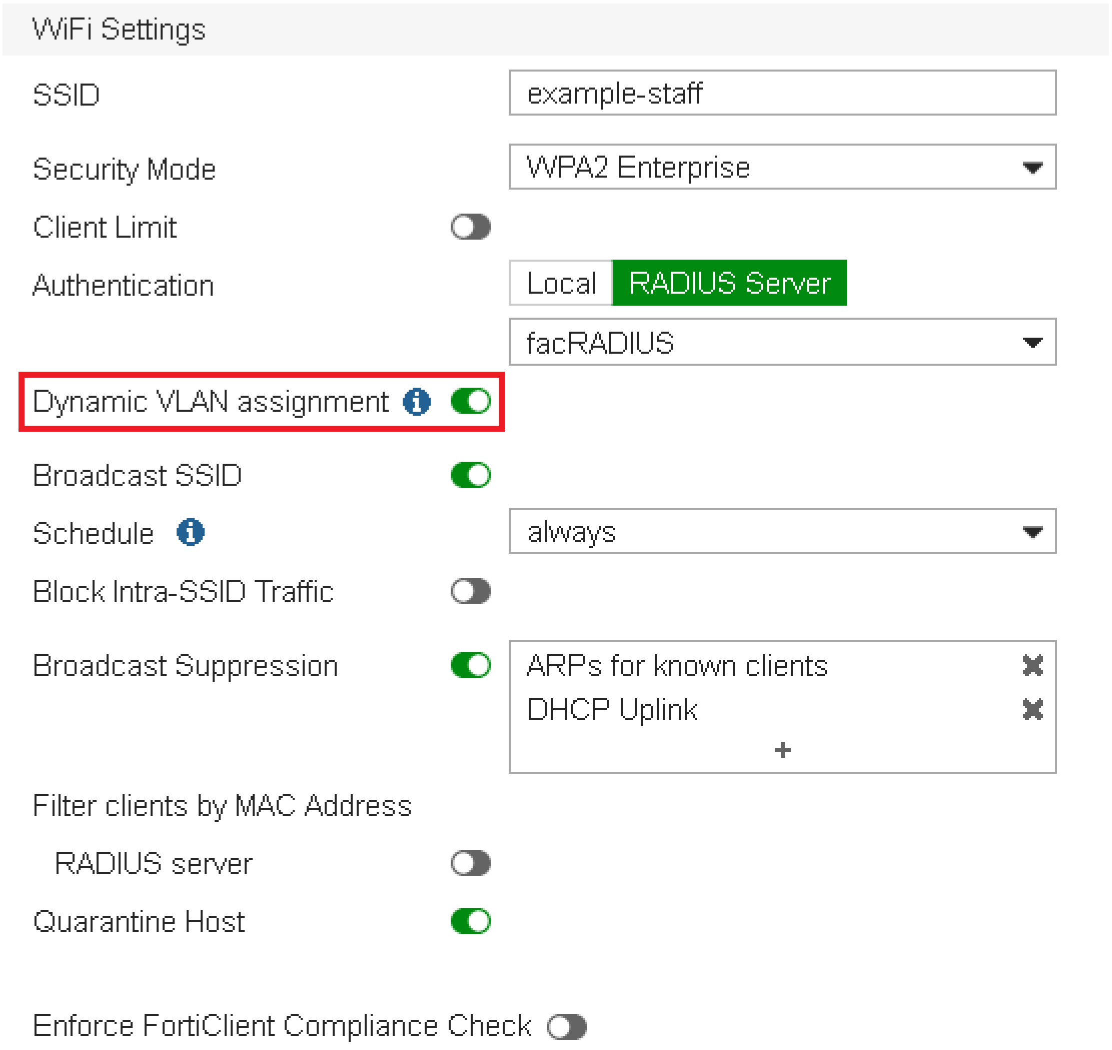
Starting IP	End IP
10.10.12.2	10.10.12.254

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	○

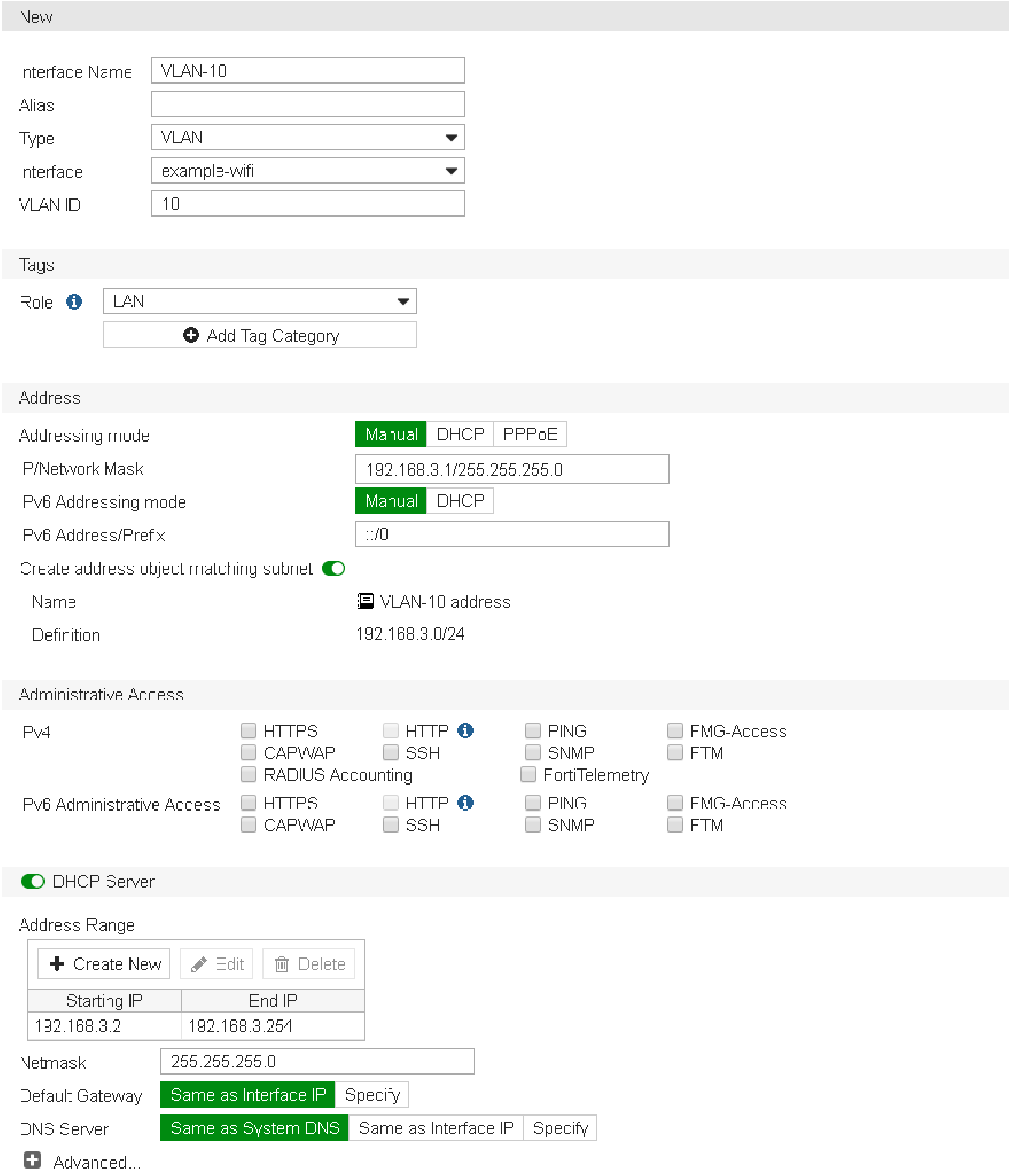
3. Then open the *CLI Console* and enter the following command to assignment and set the VLAN ID to `10`. This VLAN is used when RADIUS does not assign a VLAN:

```
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

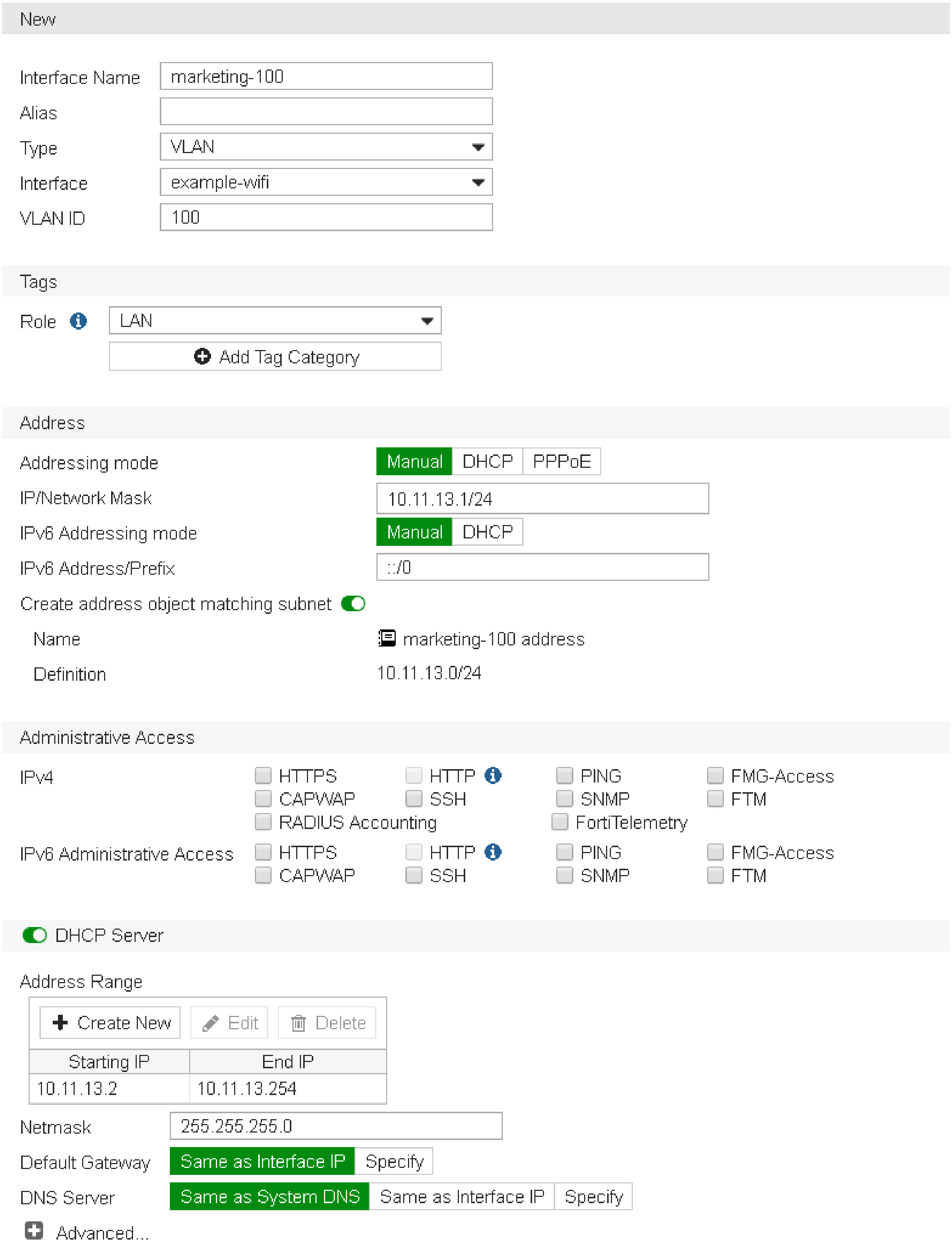
● DHCP Server

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

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

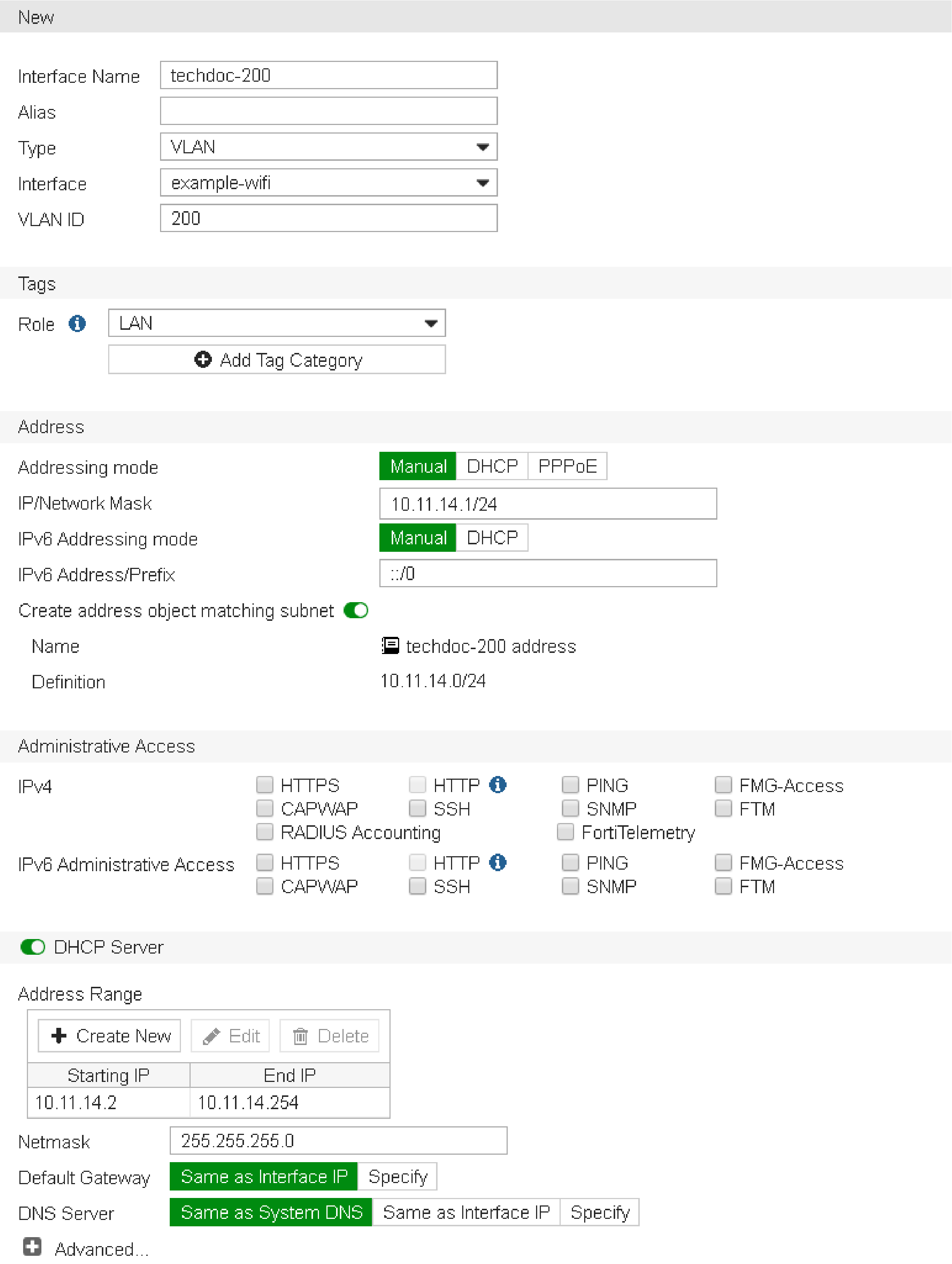
IPv6 Administrative Access: □ HTTPS □ HTTP □ PING □ FMG-Access □ CAPWAP □ SSH □ SNMP □ FTM

● DHCP Server

Address Range

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



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

Create New | Edit | Delete

Starting IP	End IP
10.11.14.2	10.11.14.254

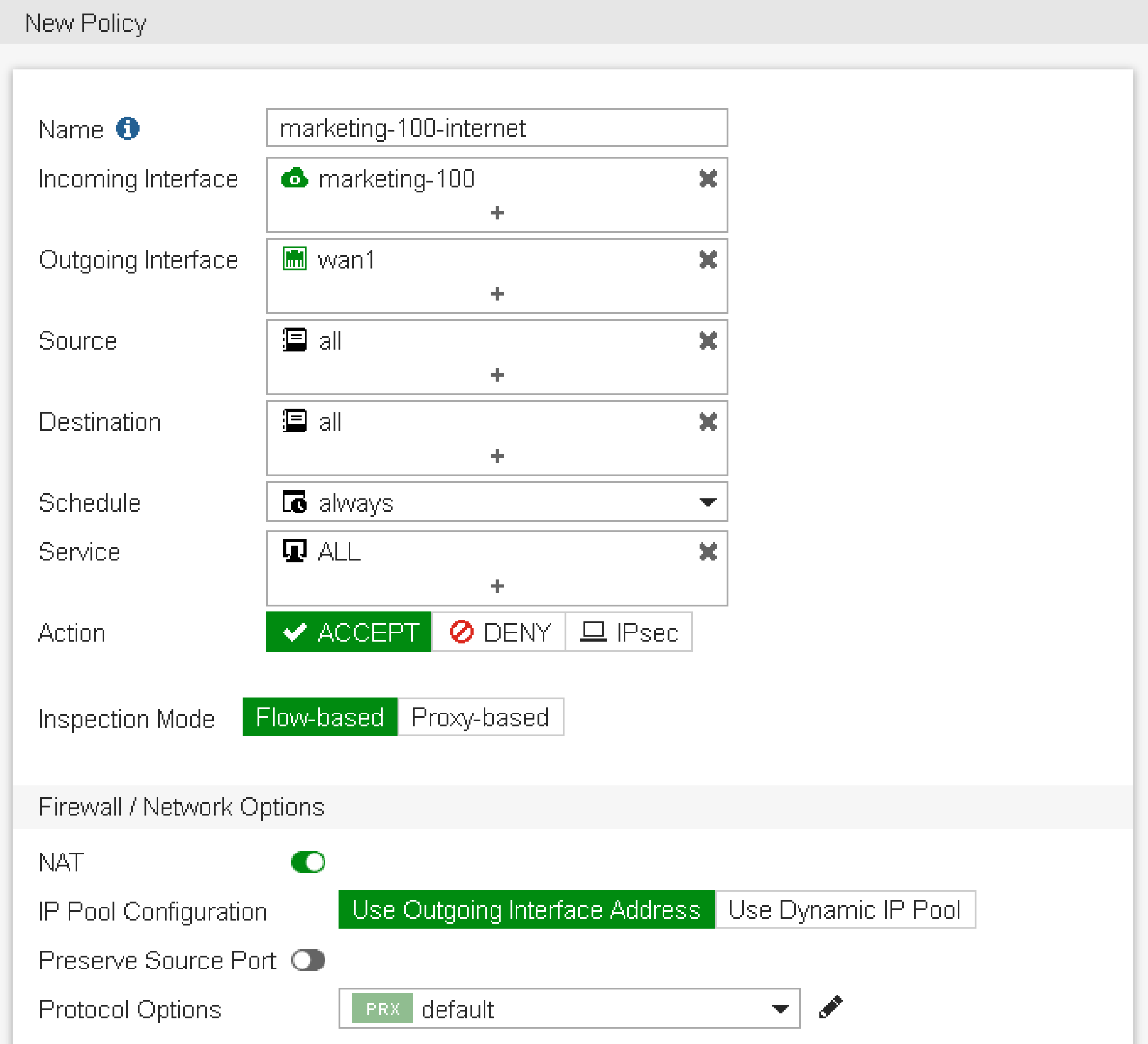
Netmask	255.255.255.0
Default Gateway	[✓ Same as Interface IP] Specify
DNS Server	[✓ Same as System DNS] Same as Interface IP Specify

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.



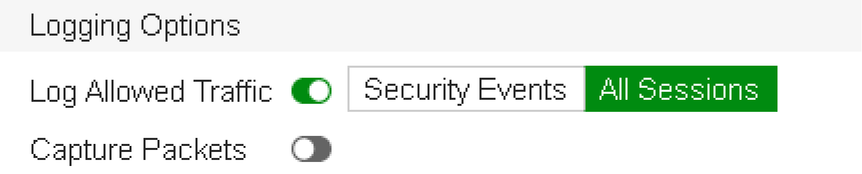
New Policy

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*.

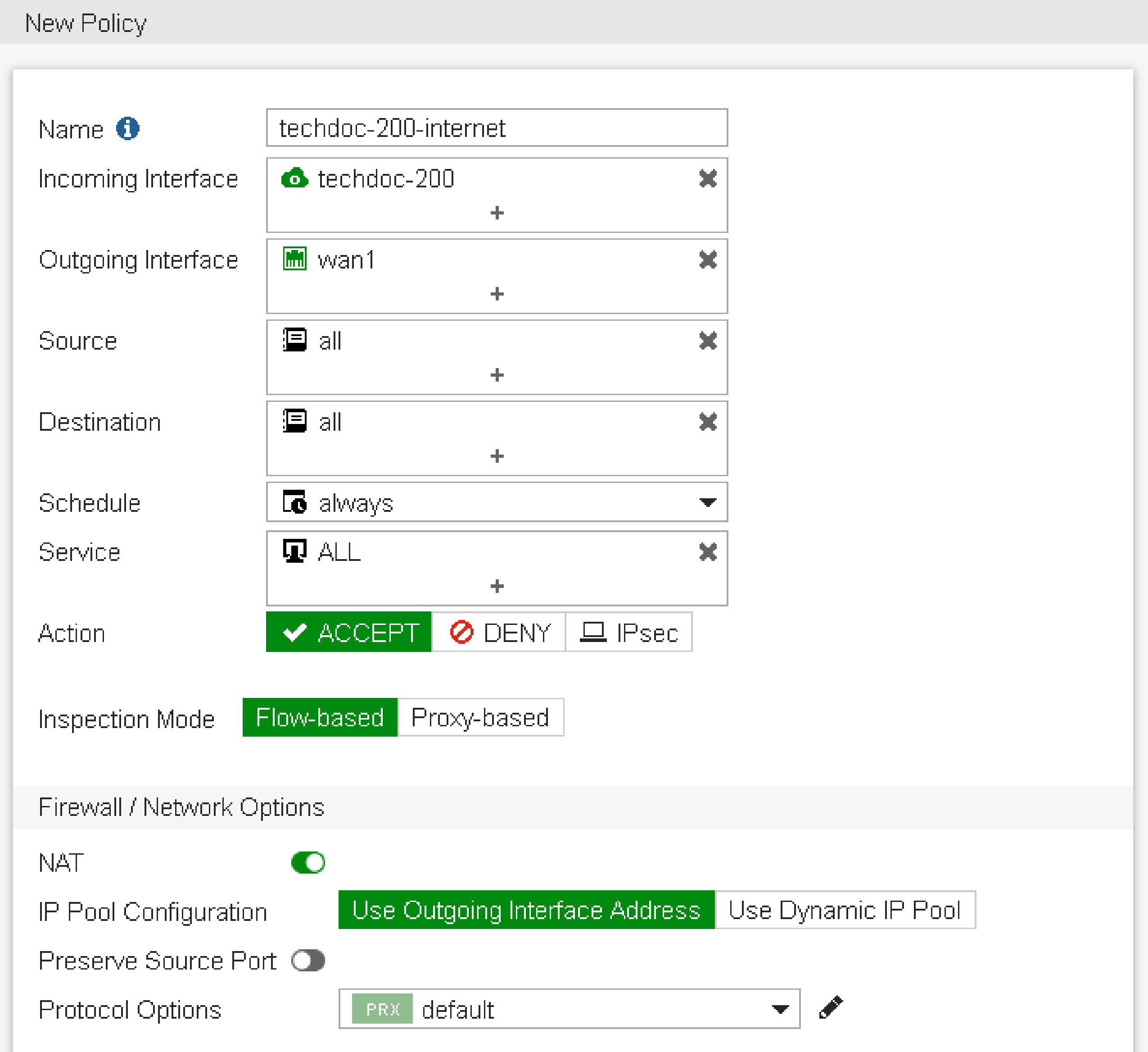


Logging Options

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

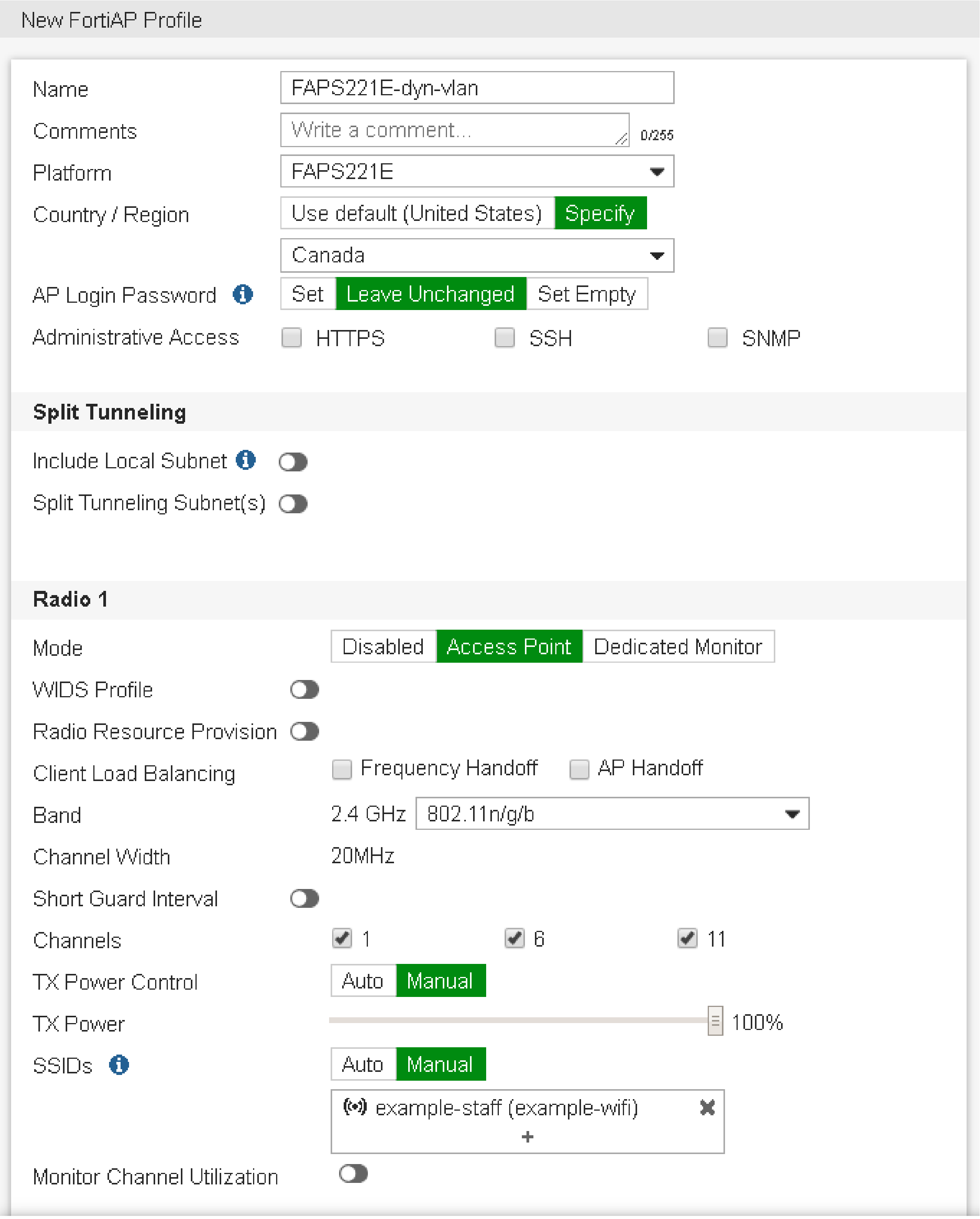
Firewall / Network Options

NAT	● on
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	○ off
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

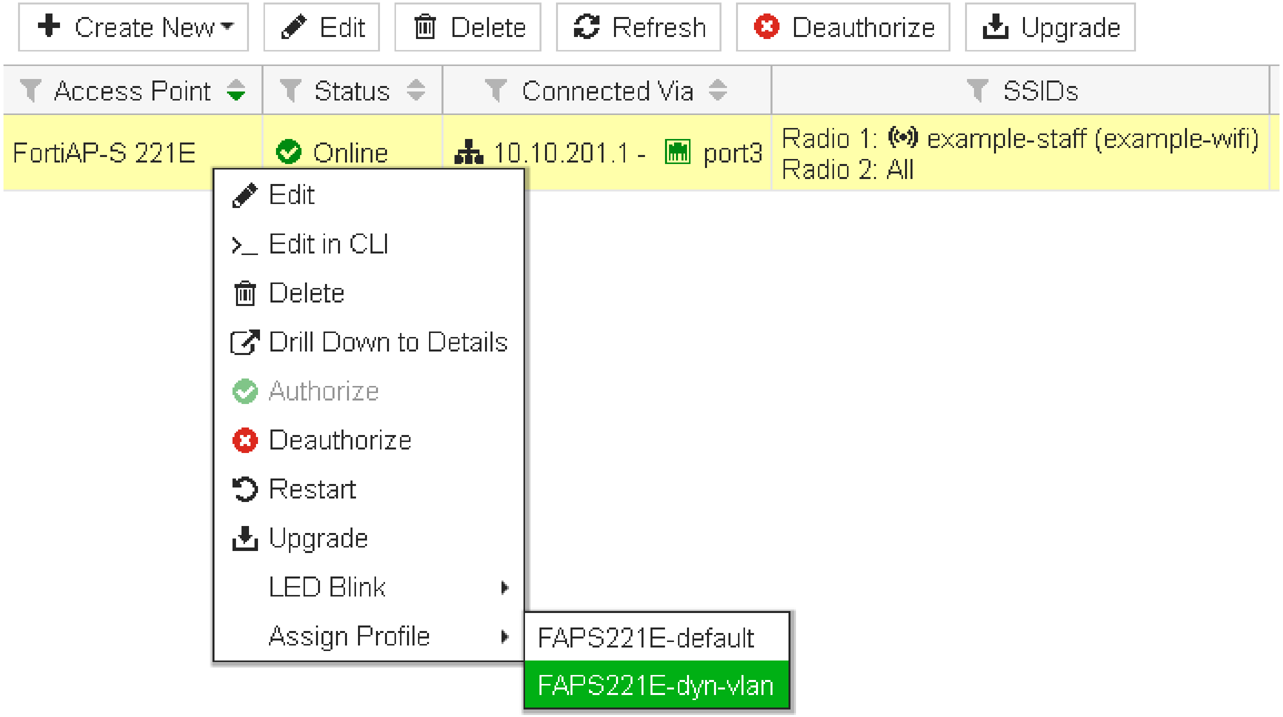
To connect and authorize the FortiAP:

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

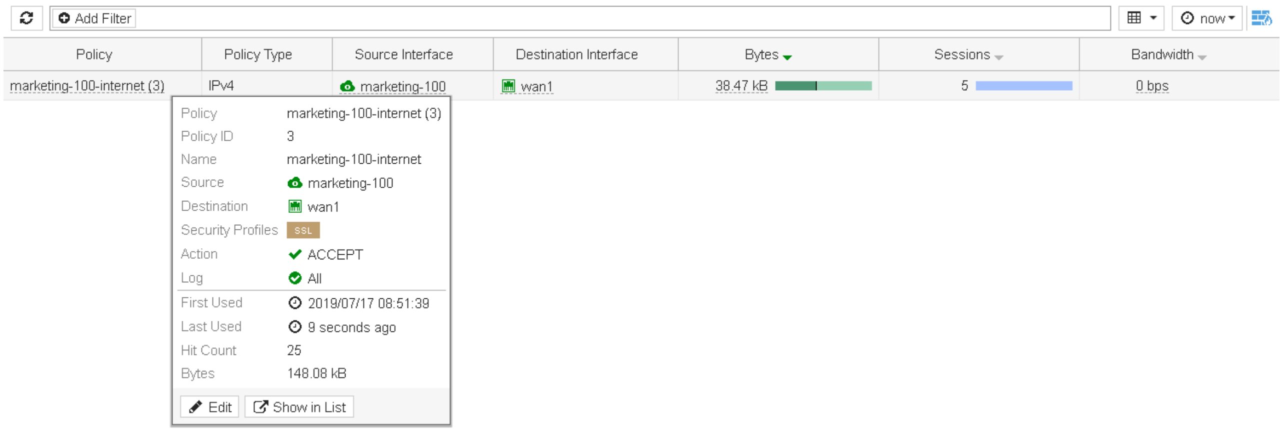
Results

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.

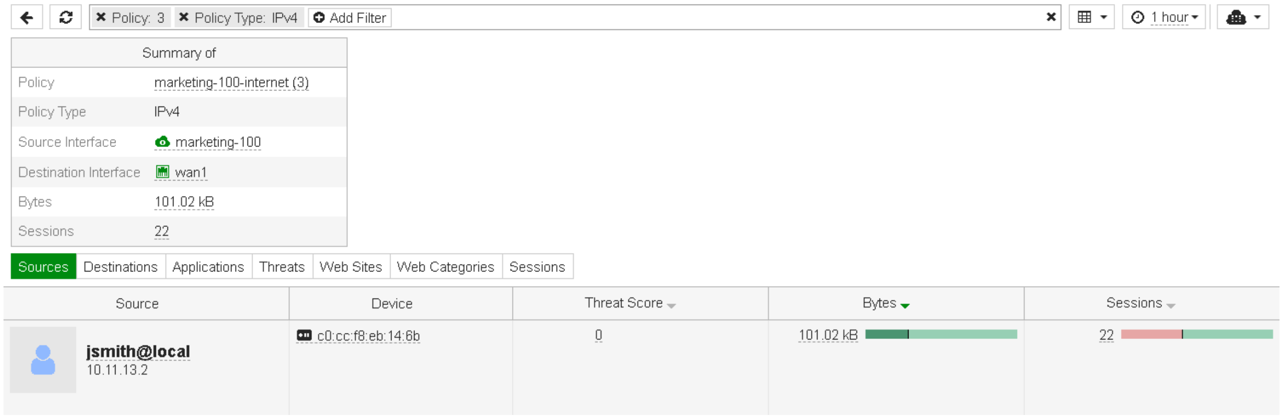
1. Go to *FortiView* > *Policies*.
   Note that traffic for jsmith and twhite will pass through different policies. In this example, the *marketing-100-internet* policy is displayed, indicating that jsmith has connected to the WiFi.



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

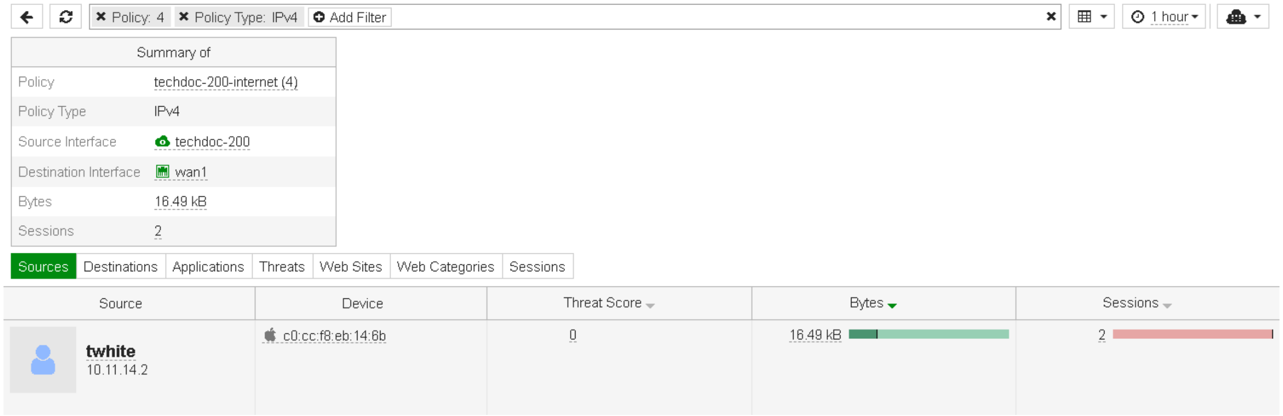
2. Double-click to drill-down, where the user's identity (including username, source IP, and device address) is confirmed.



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.

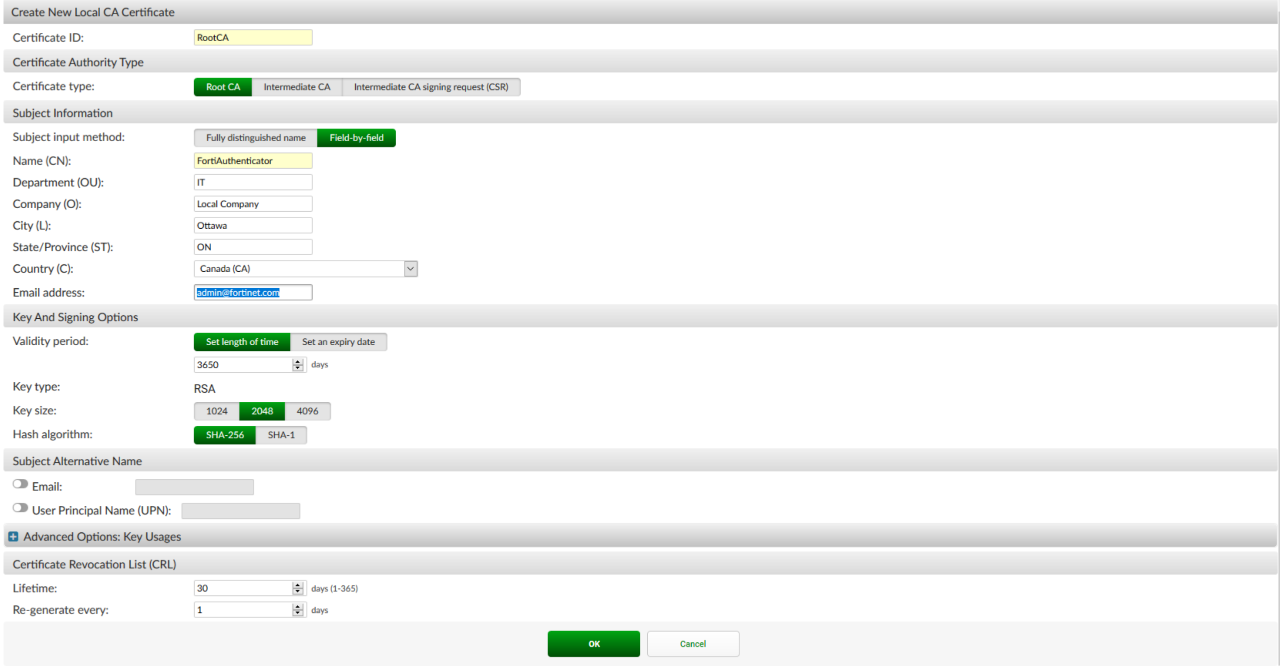
This recipe specifically focuses on the configuration of the FortiAuthenticator, FortiGate, and Windows 10 computer.

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

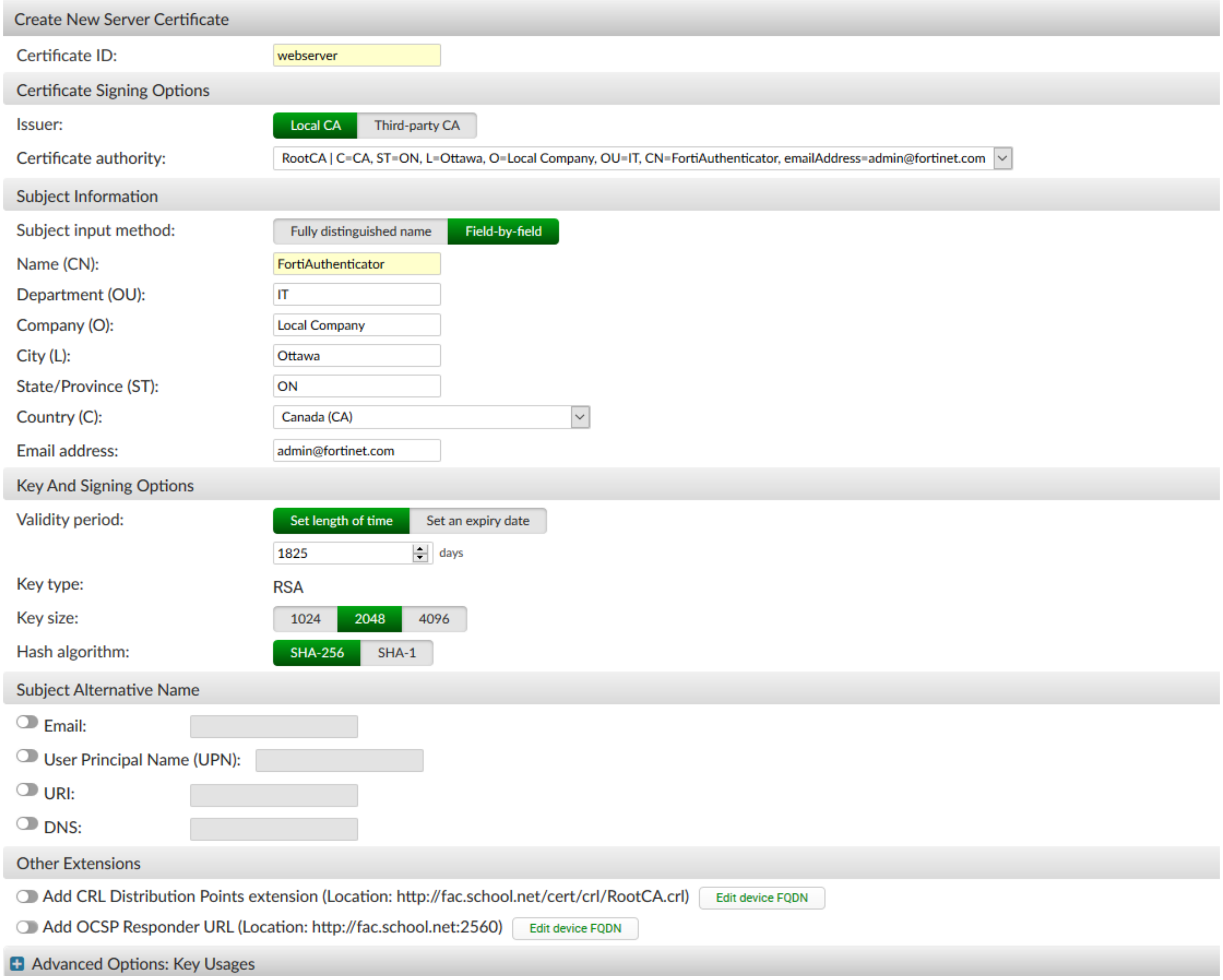
Certificate ID:	RootCA
Certificate Authority Type	
Certificate type:	[✓ Root CA] Intermediate CA Intermediate CA signing request (CSR)
Subject Information	
Subject input method:	Fully distinguished name [✓ Field-by-field]
Name (CN):	FortiAuthenticator
Department (OU):	IT
Company (O):	Local Company
City (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] 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

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] 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]

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] Set an expiry date

1825 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

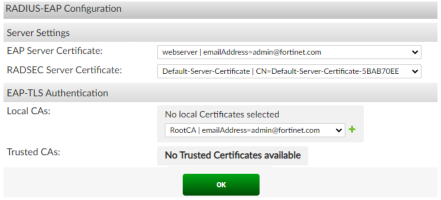
⊞ Advanced Options: Key Usages

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* > *Certificates*.
2. Select the corresponding Local Services certificate in *EAP Server Certificate*.
3. Choose the Local CA certificate previously configured in *Local CAs*.
4. Click *OK*.



RADIUS-EAP Configuration

Server Settings

EAP Server Certificate: webserver | emailAddress=admin@fortinet.com

RADSEC Server Certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE

EAP-TLS Authentication

Local CAs: No local Certificates selected
RootCA | emailAddress=admin@fortinet.com

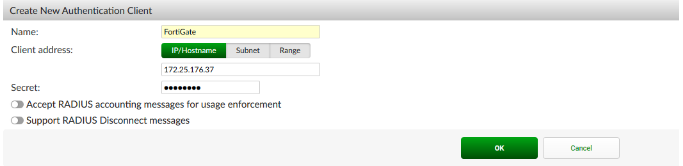
Trusted CAs: No Trusted Certificates available

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

172.25.176.37

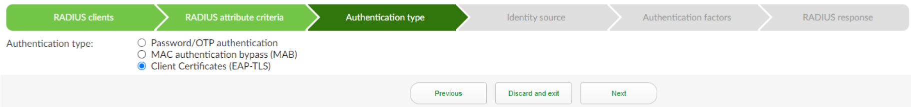
Secret: •••••••••

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 *Client Certificates (EAP-TLS)*.



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

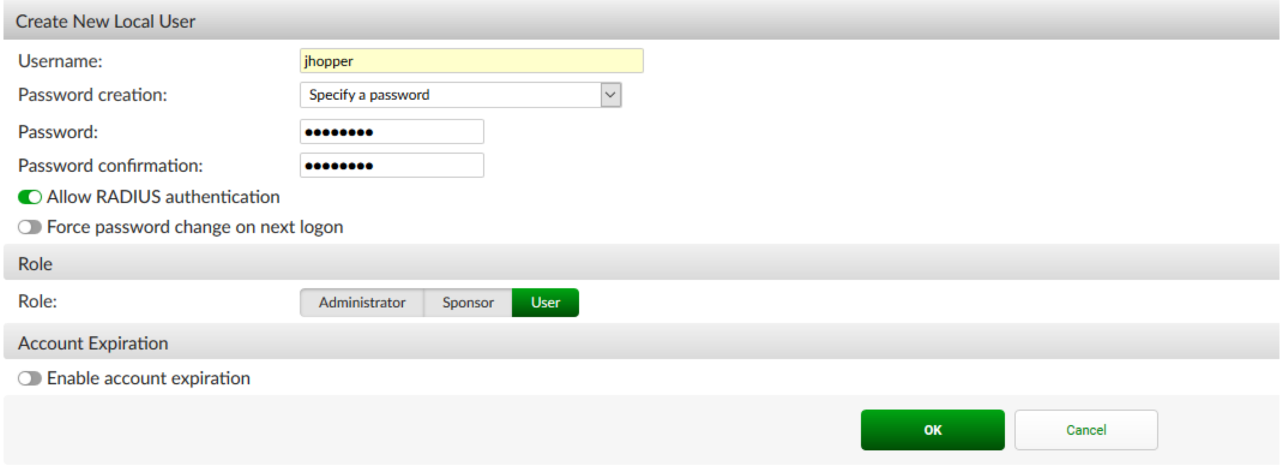
5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
6. Set the authentication method to *Password only authentication*.
7. Review the RADIUS response, and click *Save and Exit*.

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: enabled

Force password change on next logon: disabled

Role

Role: User

Account Expiration

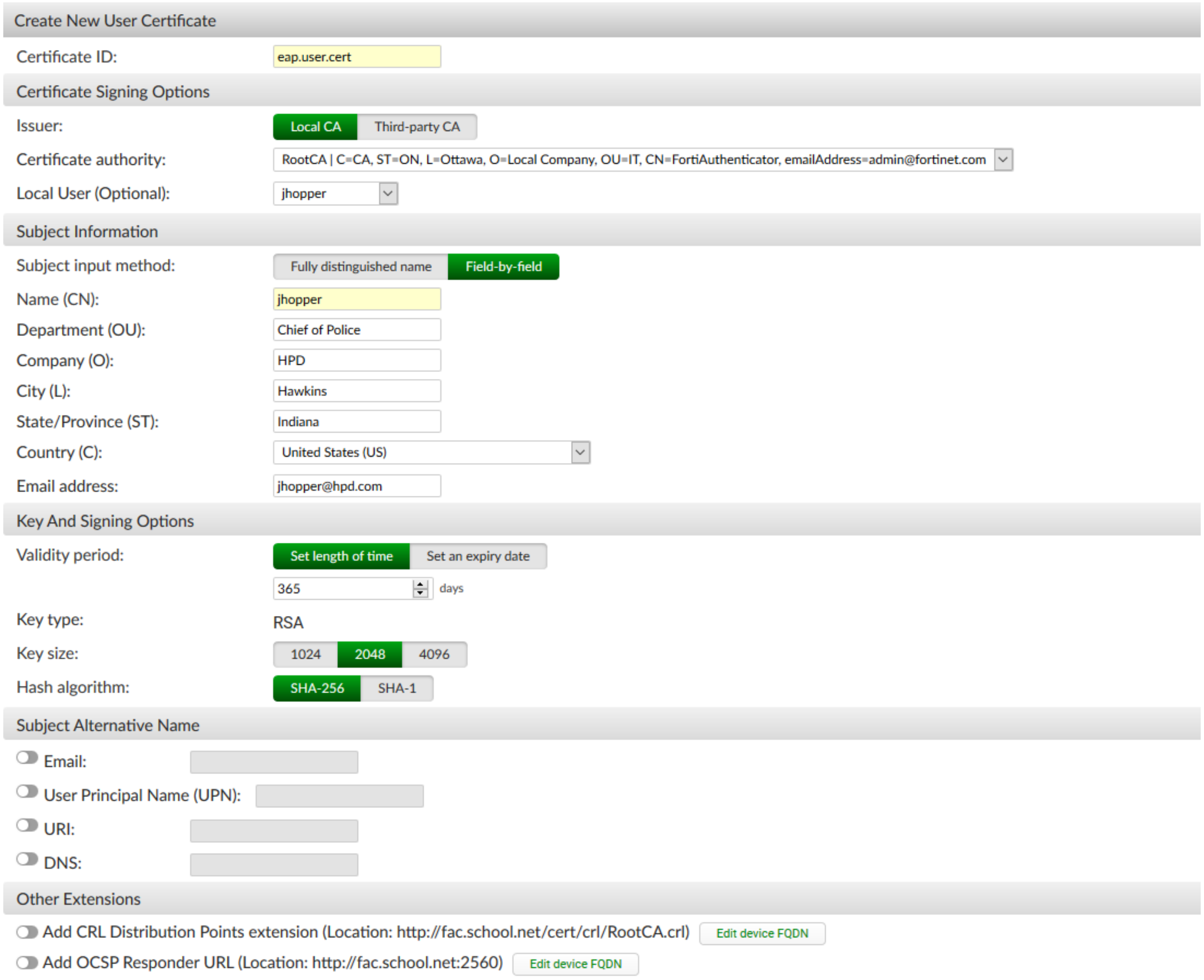
Enable account expiration: disabled

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

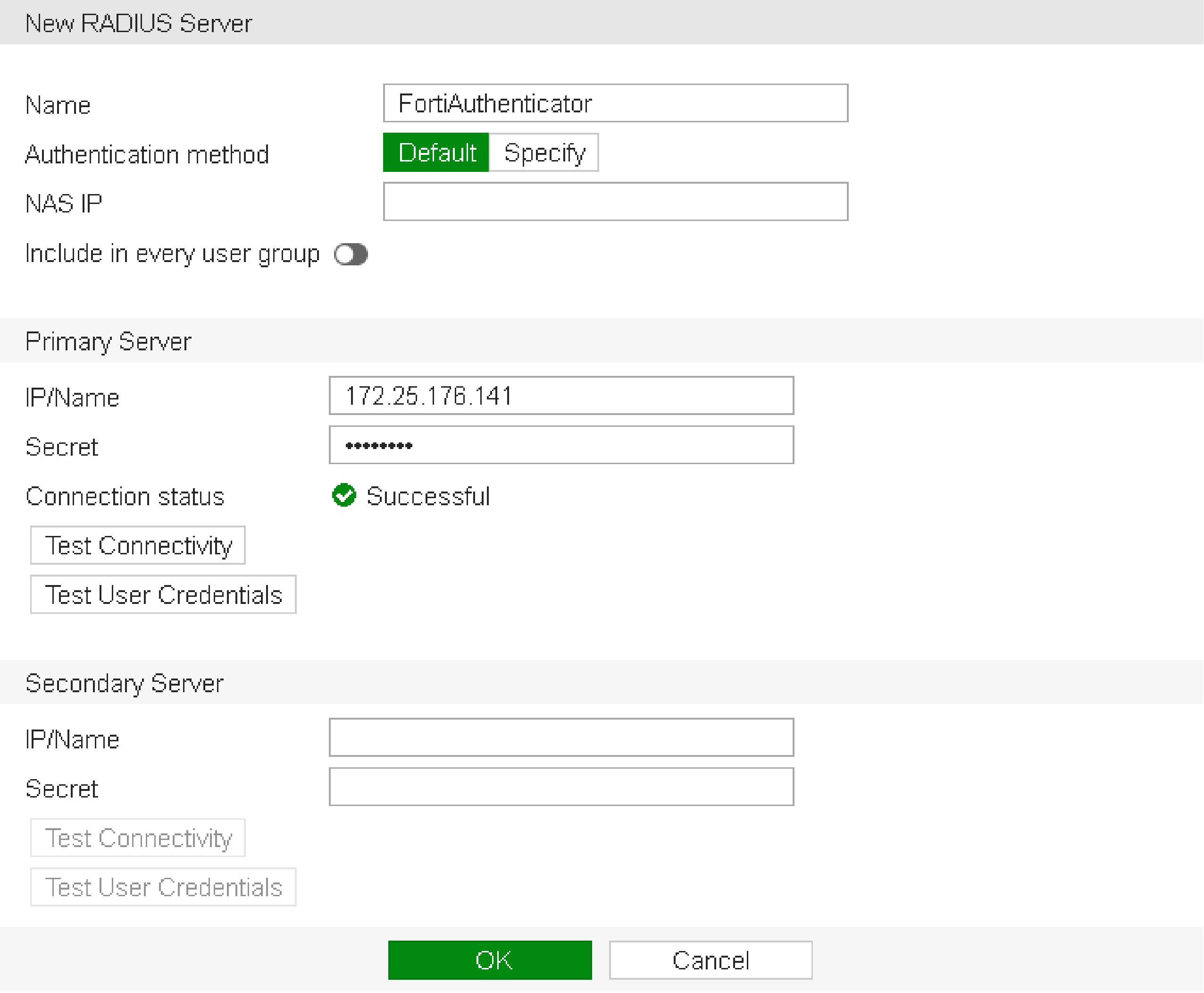
Creating RADIUS server on FortiGate

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:

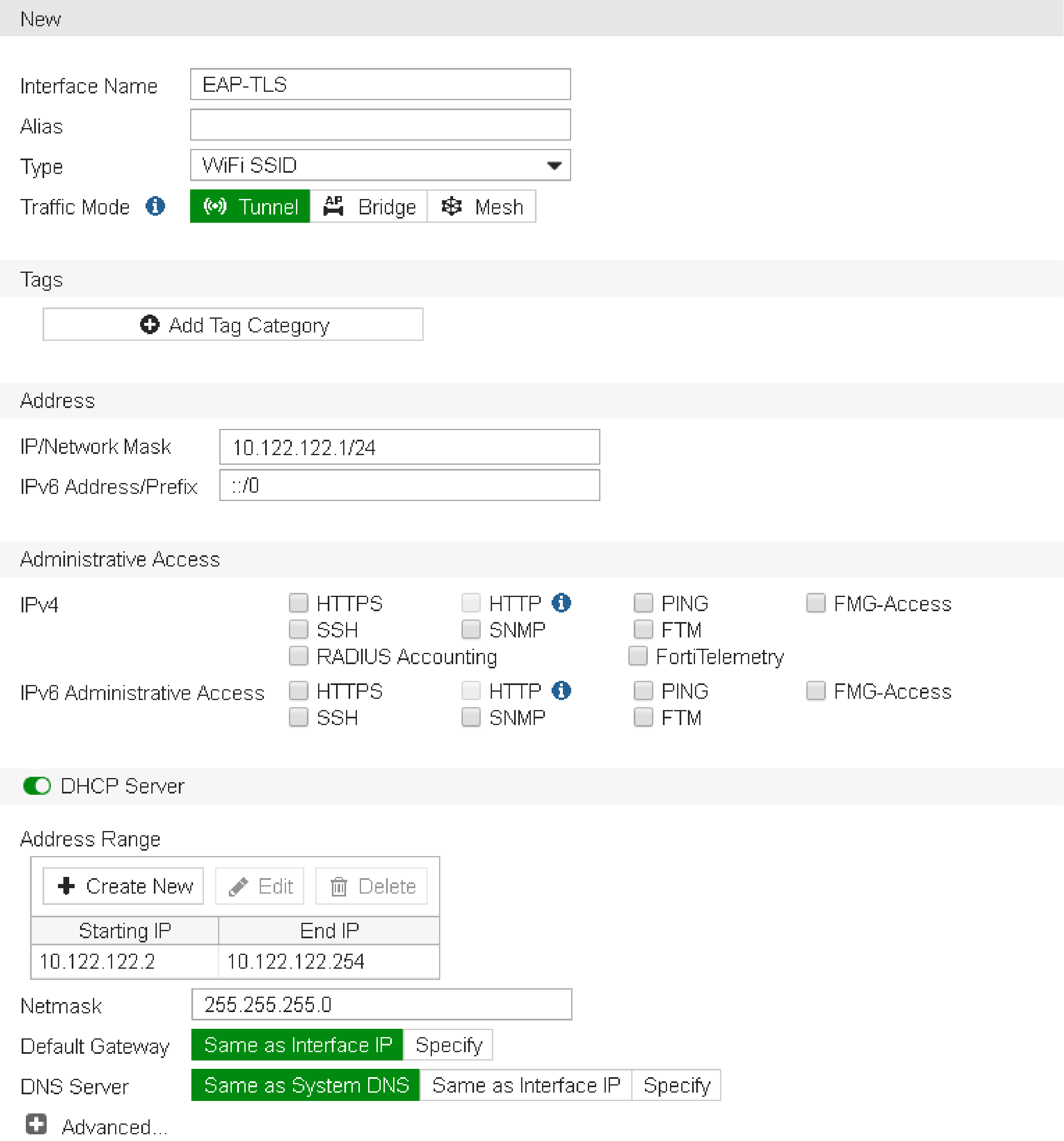
Secret:

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 (enabled)

Address Range

Create New | Edit | Delete

Starting IP	End IP
10.122.122.2	10.122.122.254

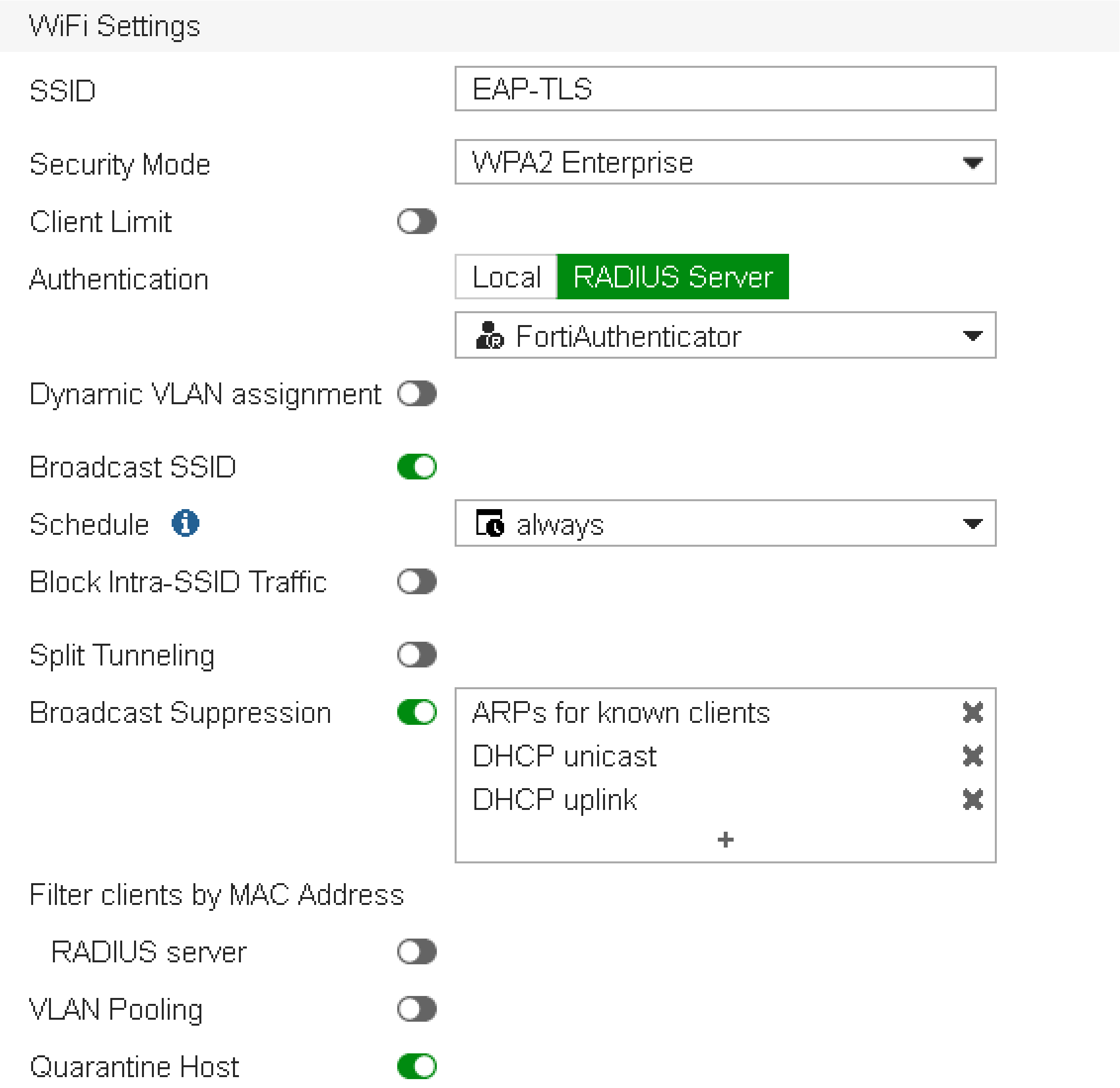
Netmask: 255.255.255.0

Default Gateway: [✓ Same as Interface IP] Specify

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

Advanced...

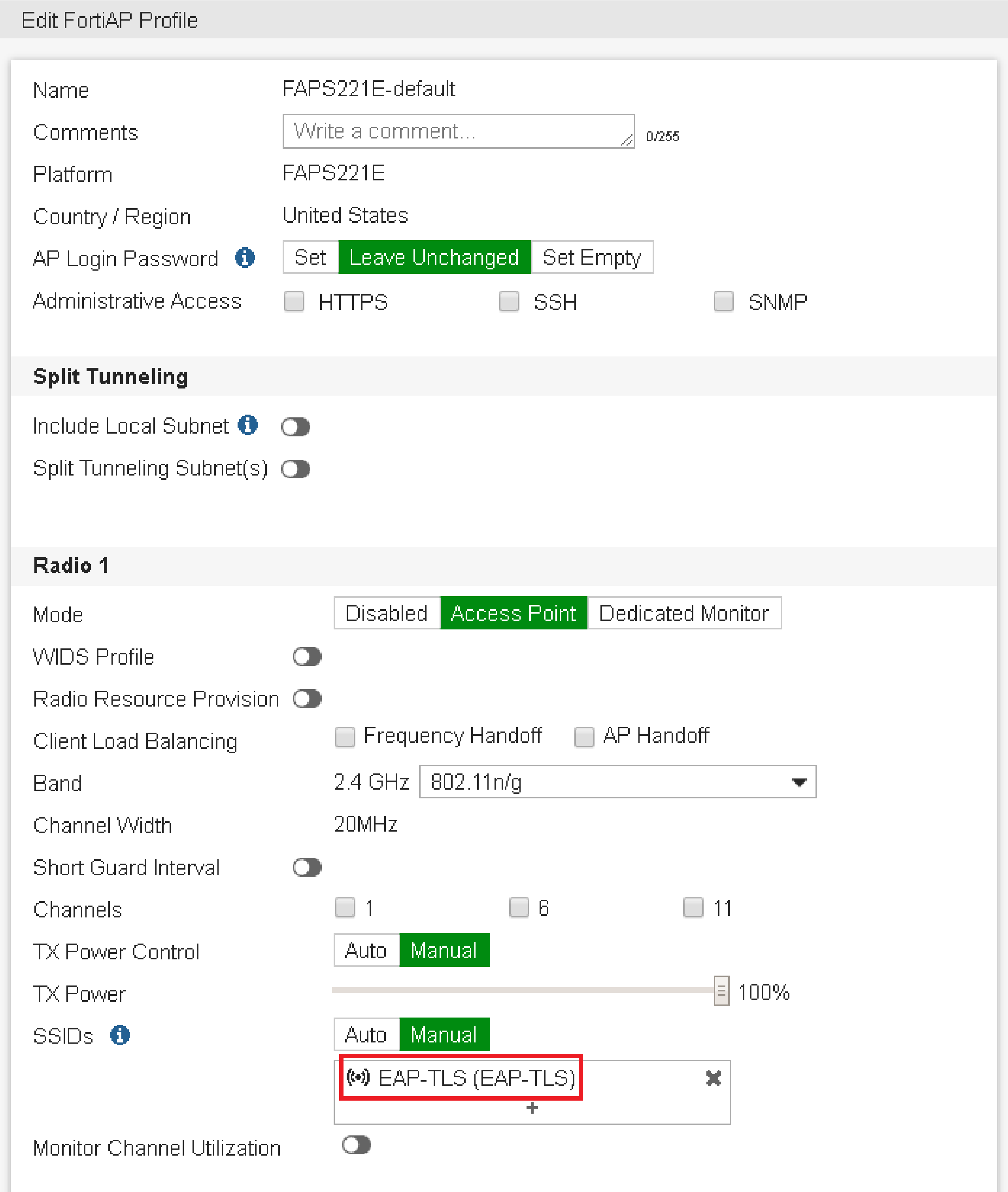
2. Set the following *WiFi Settings*, assigning the *RADIUS Server* configured earlier.



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	○

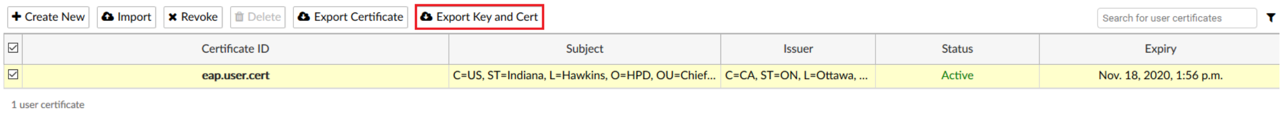
4. Then go to *Policy & Objects* > *IPv4 Policy* and create a policy that allows outbound traffic from the *EAP-TLS* wireless interface to the Internet.

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:

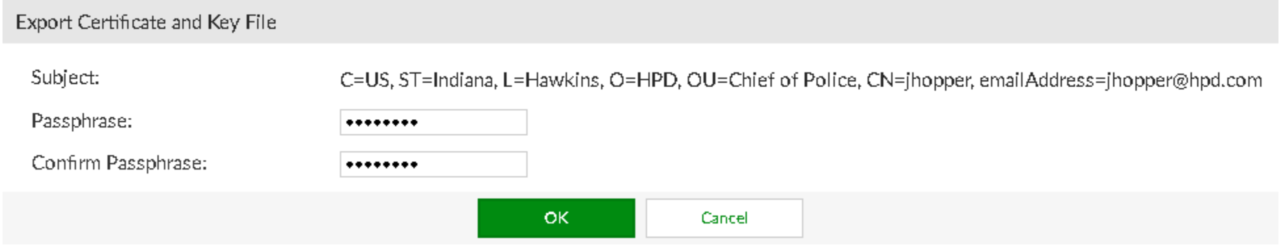
1. On the FortiAuthenticator, go to *Certificate Management* > *End Entities* > *Users*. Select the certificate and select *Export Key and Cert*.



☑	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

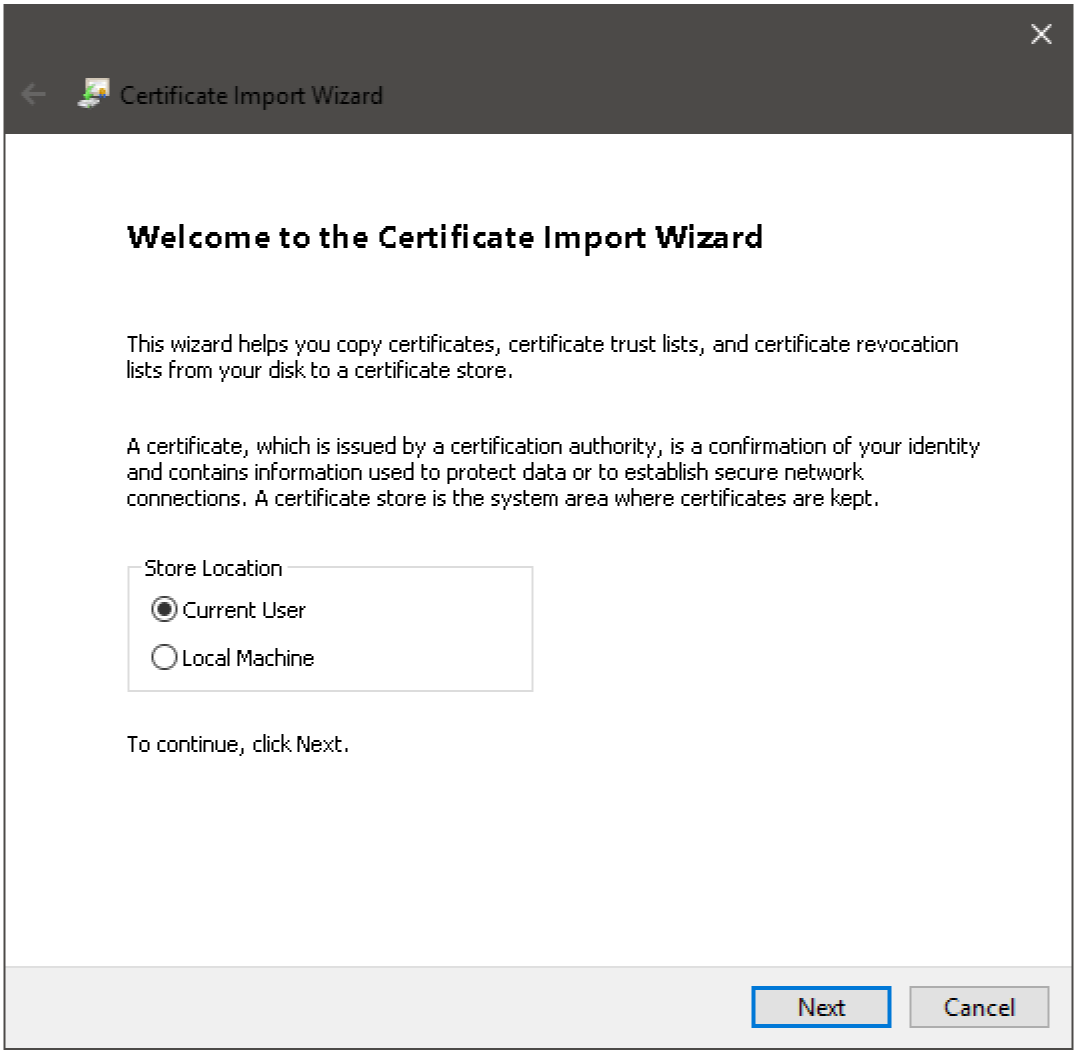
Subject:	C=US, ST=Indiana, L=Hawkins, O=HPD, OU=Chief of Police, CN=jhopper, emailAddress=jhopper@hpd.com
Passphrase:	••••••••
Confirm Passphrase:	••••••••

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.

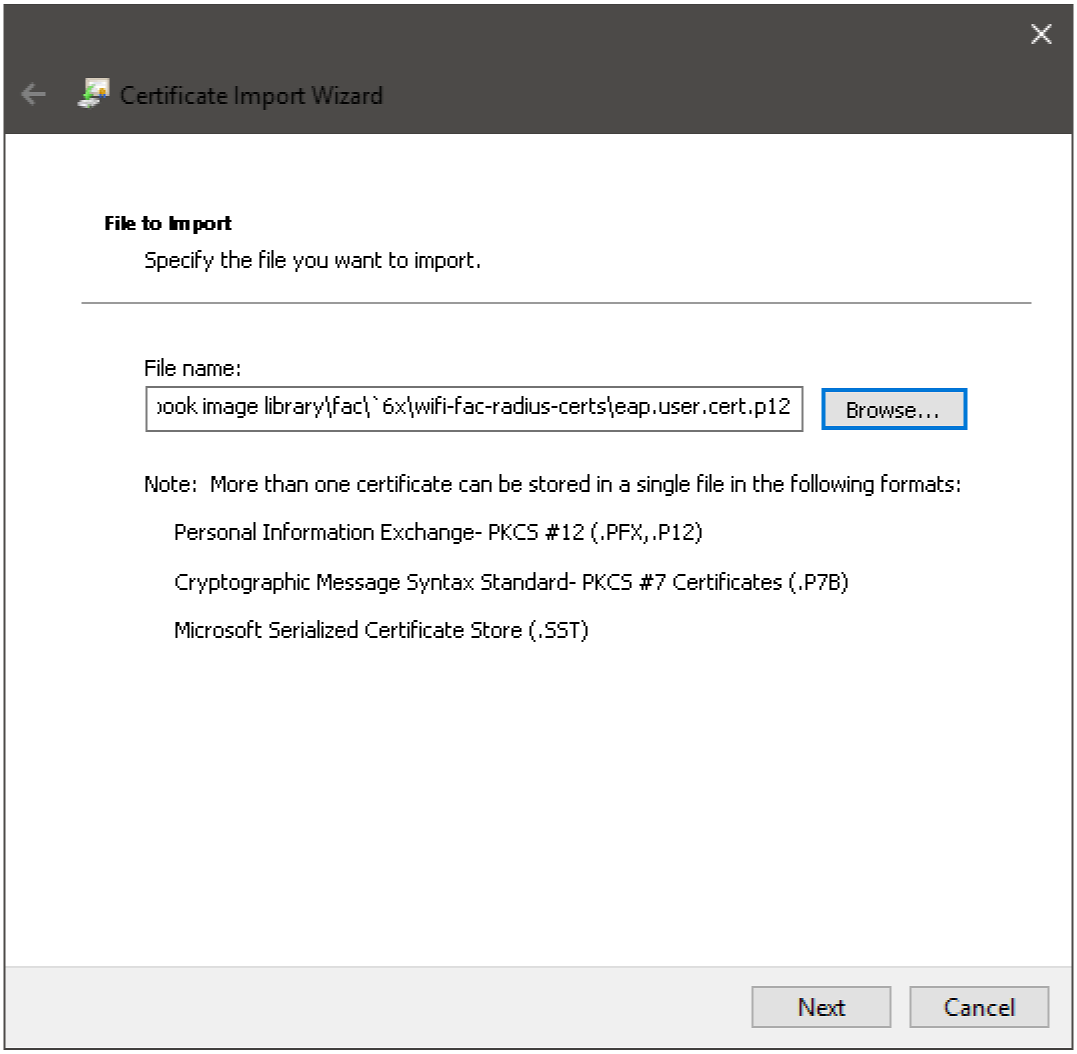
Store Location

● 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*.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

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

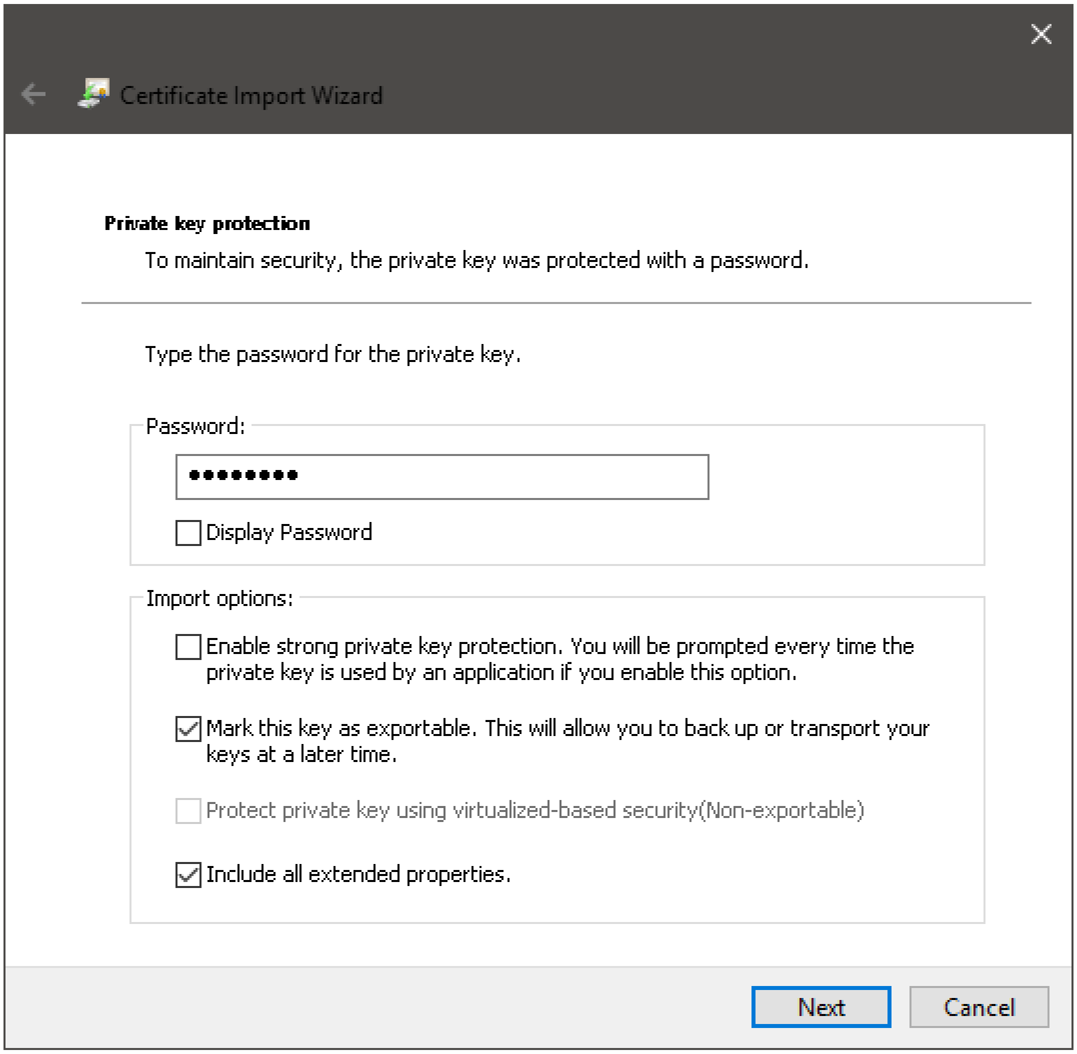
Note: More than one certificate can be stored in a single file in the following formats:

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:

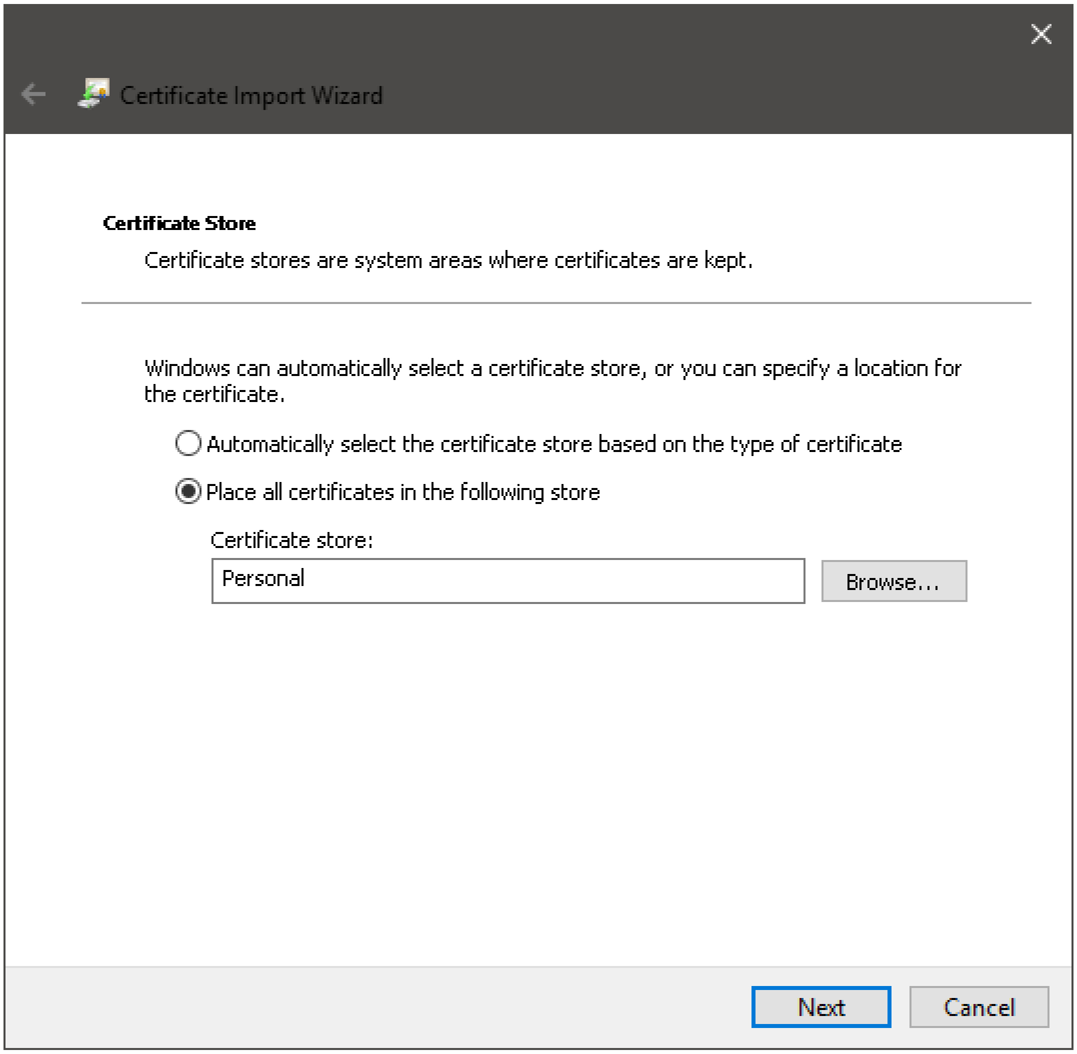
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ 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

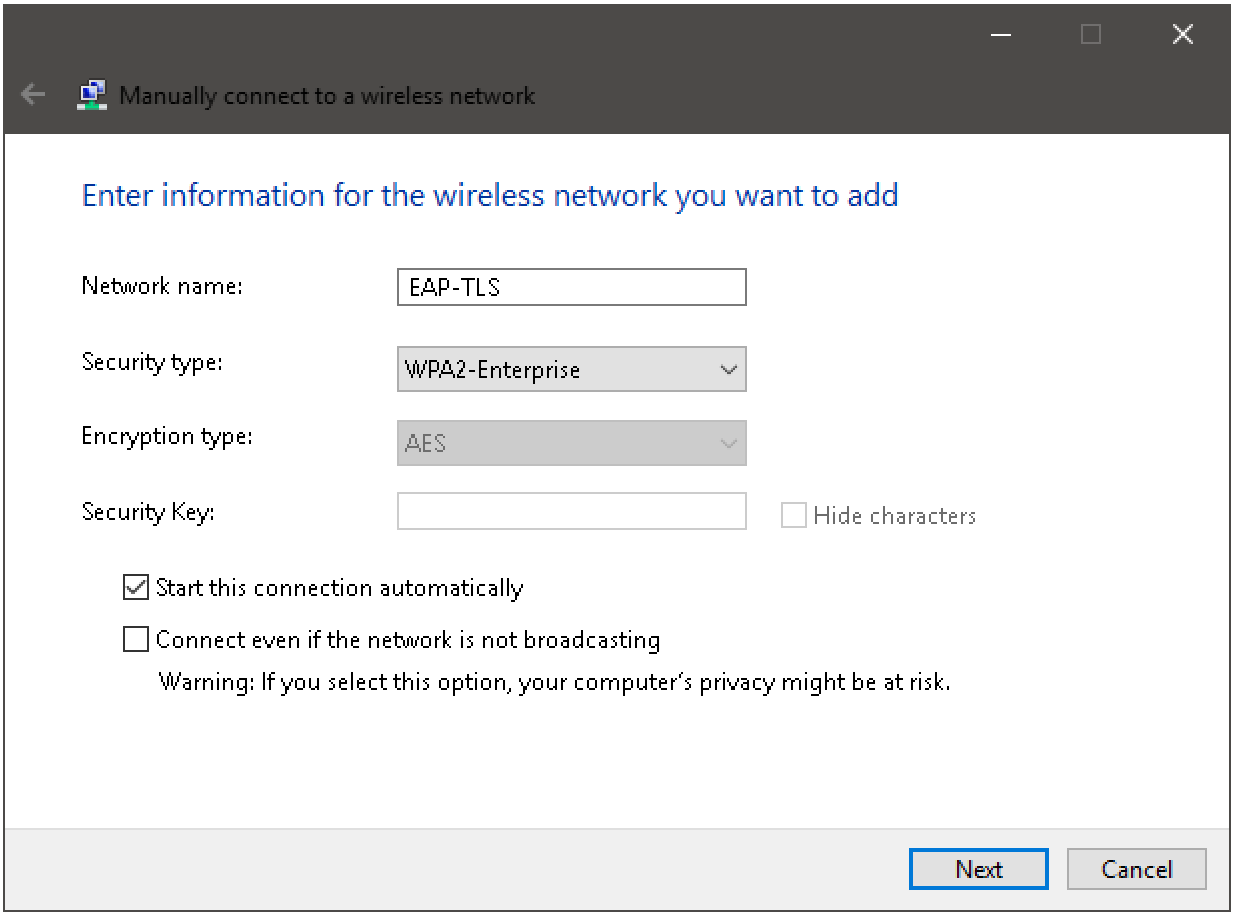
Certificate store: Personal

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*.



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: EAP-TLS

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

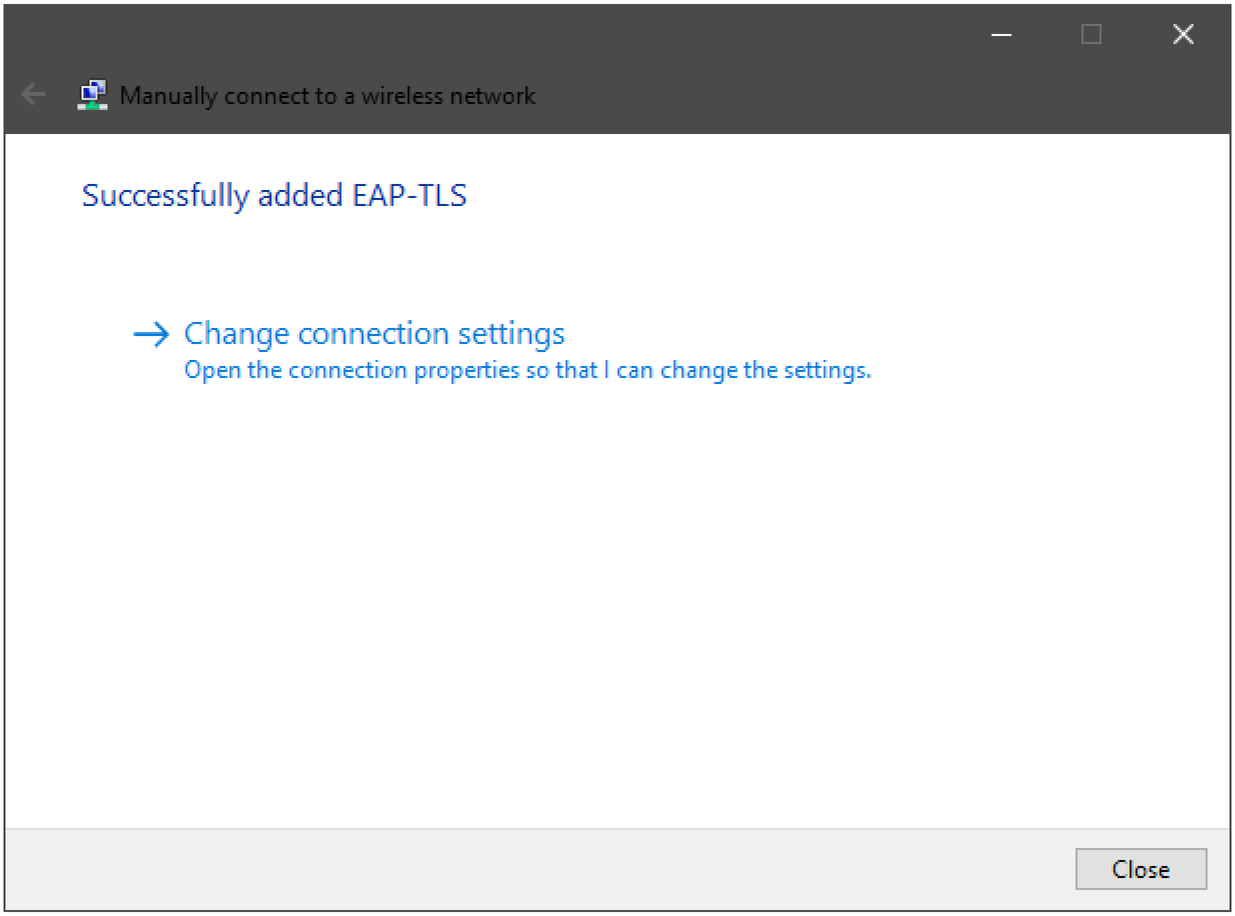
□ Hide characters

☑ 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*.

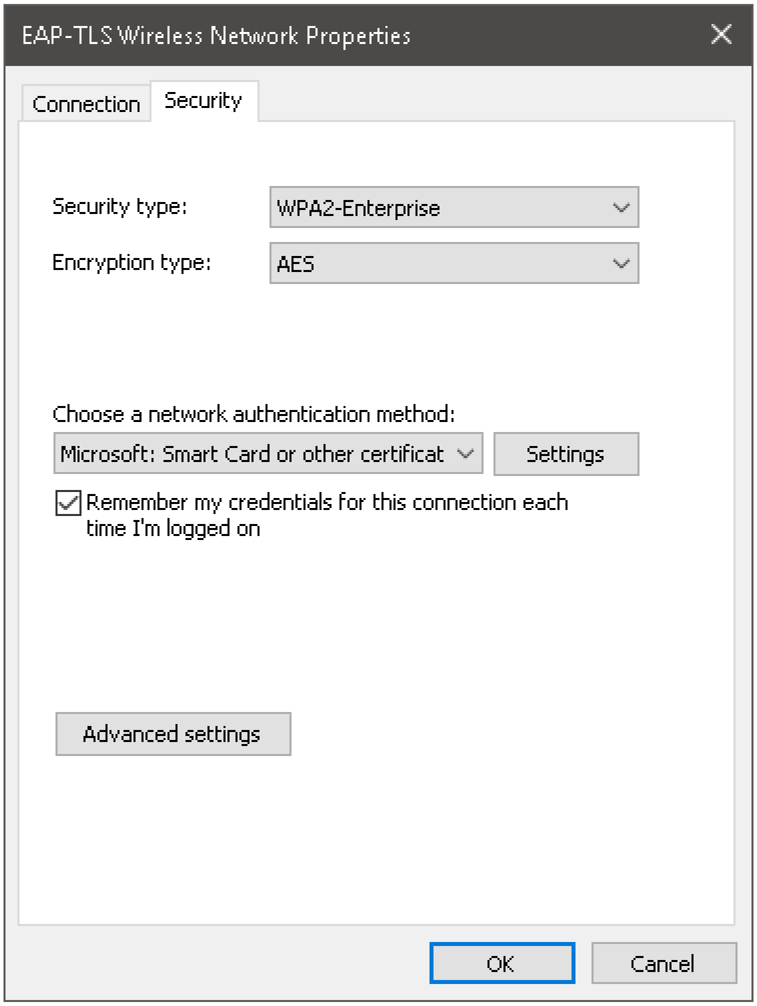


Successfully added EAP-TLS

→ 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*.



Security type: WPA2-Enterprise

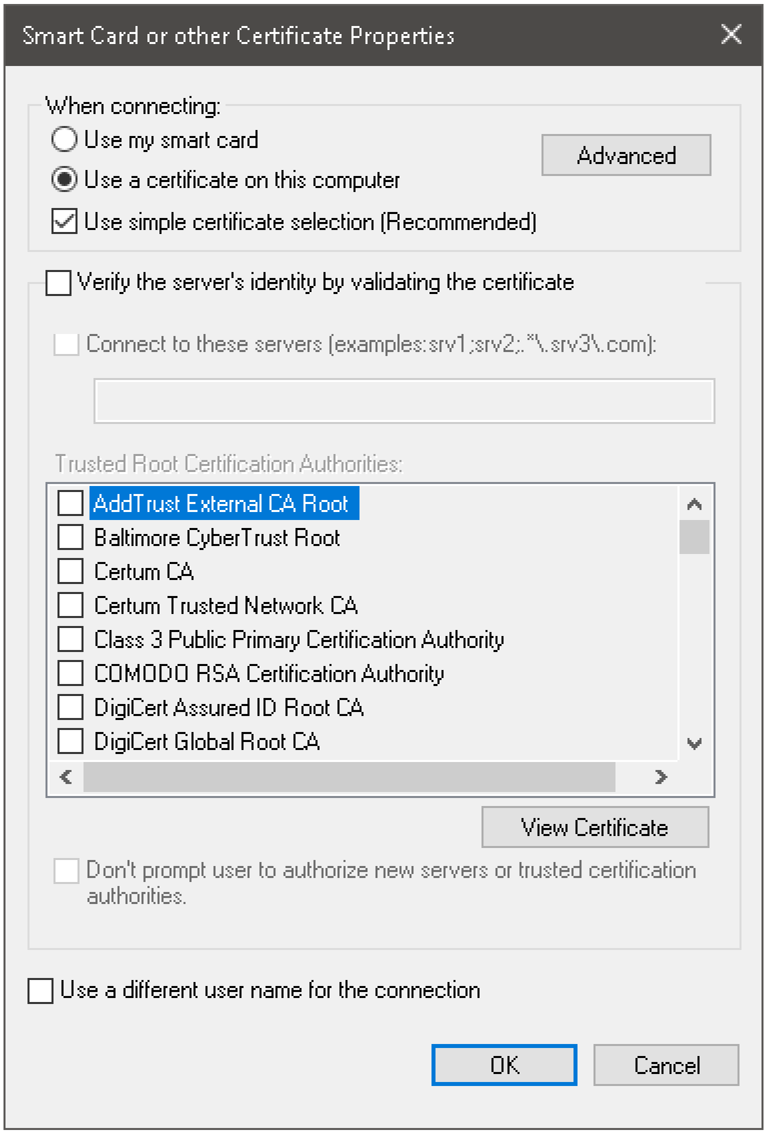
Encryption type: AES

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:

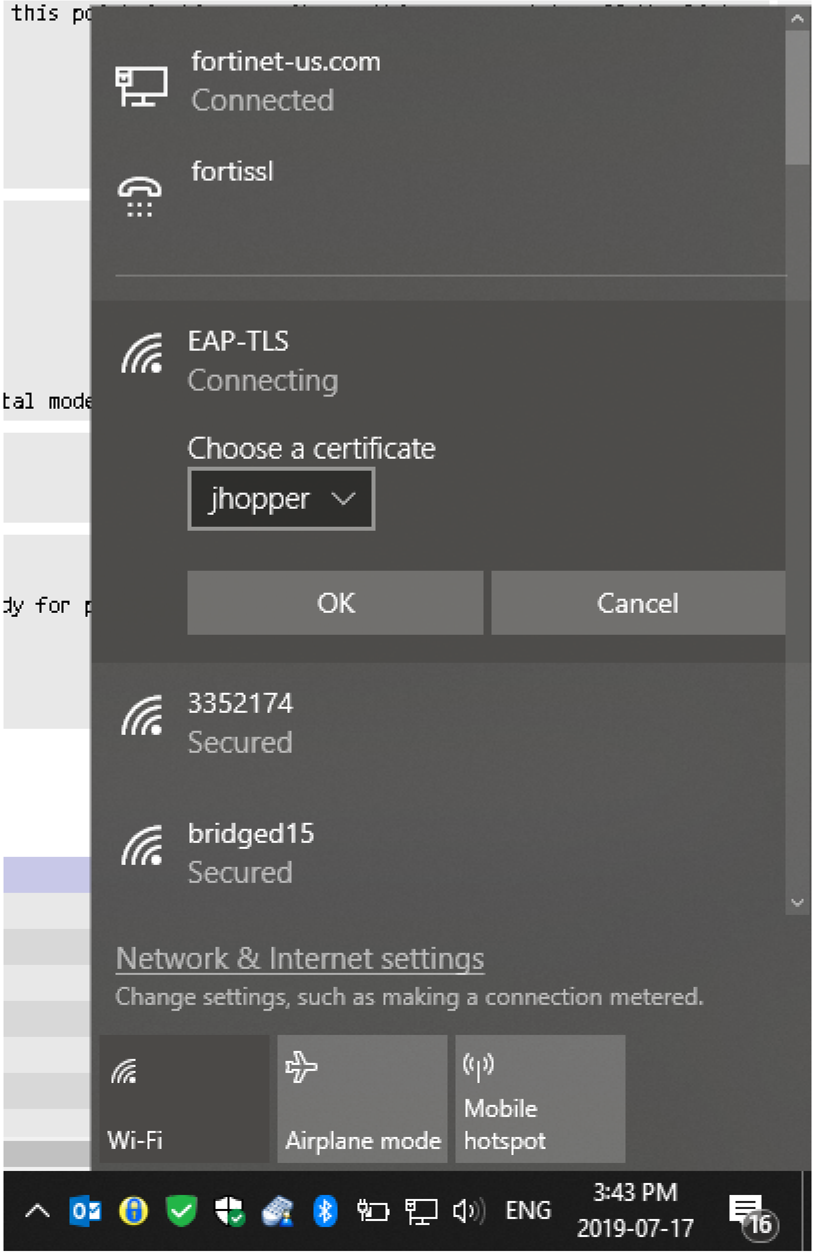
- □ AddTrust External CA Root
- □ Baltimore CyberTrust Root
- □ Certum CA
- □ Certum Trusted Network CA
- □ Class 3 Public Primary Certification Authority
- □ COMODO RSA Certification Authority
- □ DigiCert Assured ID Root CA
- □ DigiCert Global Root CA

□ 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*.



fortinet-us.com
Connected

fortissl

EAP-TLS
Connecting

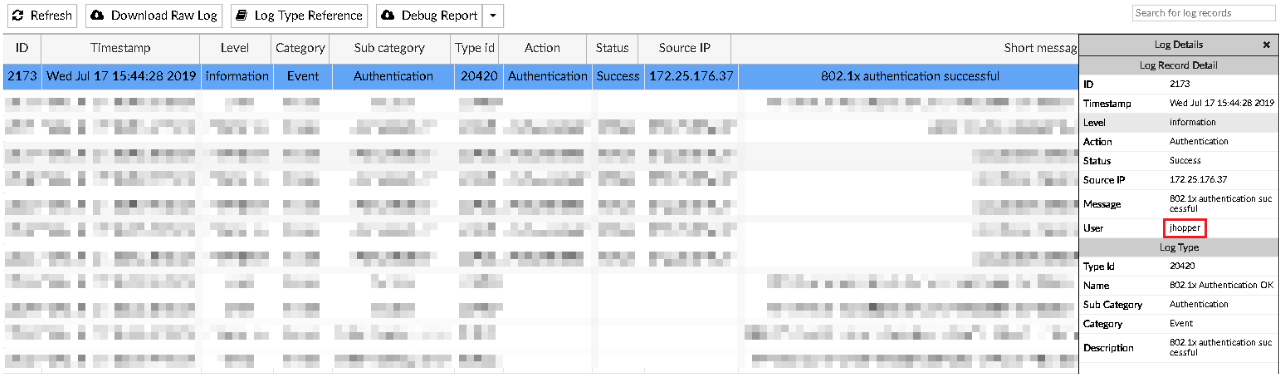
Choose a certificate
jhopper

3352174
Secured

bridged15
Secured

Network & Internet settings
Change settings, such as making a connection metered.

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

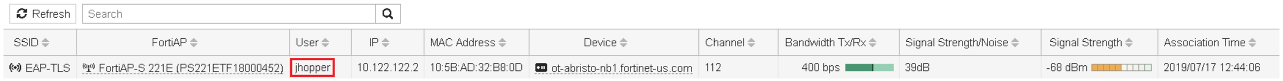


ID	Timestamp	Level	Category	Sub category	Type Id	Action	Status	Source IP	Short messag
2173	Wed Jul 17 15:44:28 2019	Information	Event	Authentication	20420	Authentication	Success	172.25.176.37	802.1x authentication successful

[redacted]

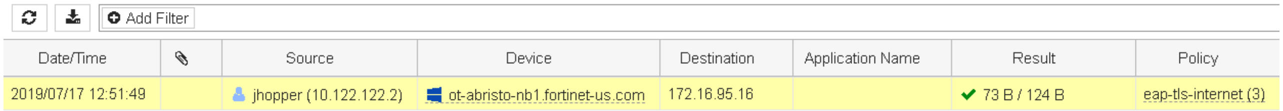
Log Details	
Log Record Detail	
ID	2173
Timestamp	Wed Jul 17 15:44:28 2019
Level	information
Action	Authentication
Status	Success
Source IP	172.25.176.37
Message	802.1x authentication successful
User	jhopper
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

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

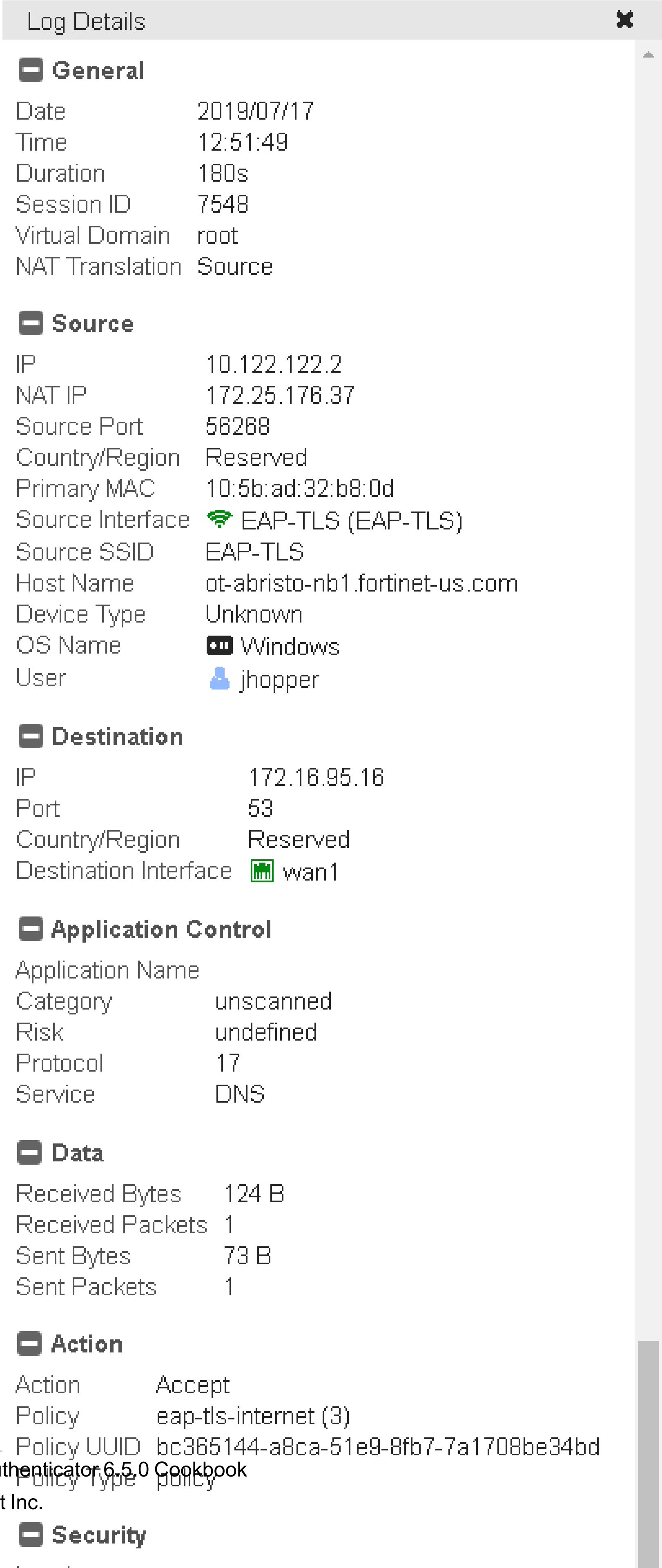


SSID	FortiAP	User	IP	MAC Address	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal Strength	Association Time
EAP-TLS	FortiAP-S 221E (PS221ETF18000452)	jhopper	10.122.122.2	10:5B:AD:32:B8:0D	ot-abristo-nb1.fortinet-us.com	112	400 bps	39dB	-68 dBm	2019/07/17 12:44:06

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

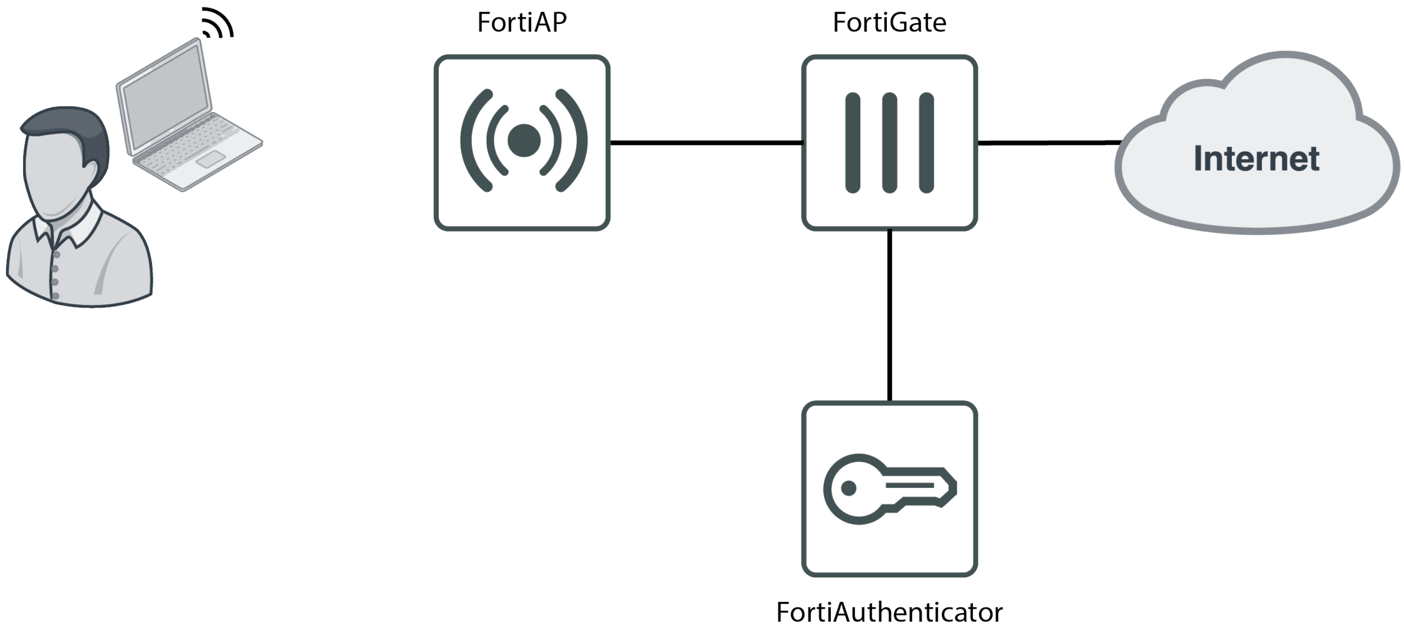
Received Bytes	124 B
Received Packets	1
Sent Bytes	73 B
Sent Packets	1

Action

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

Security

WiFi RADIUS authentication with FortiAuthenticator



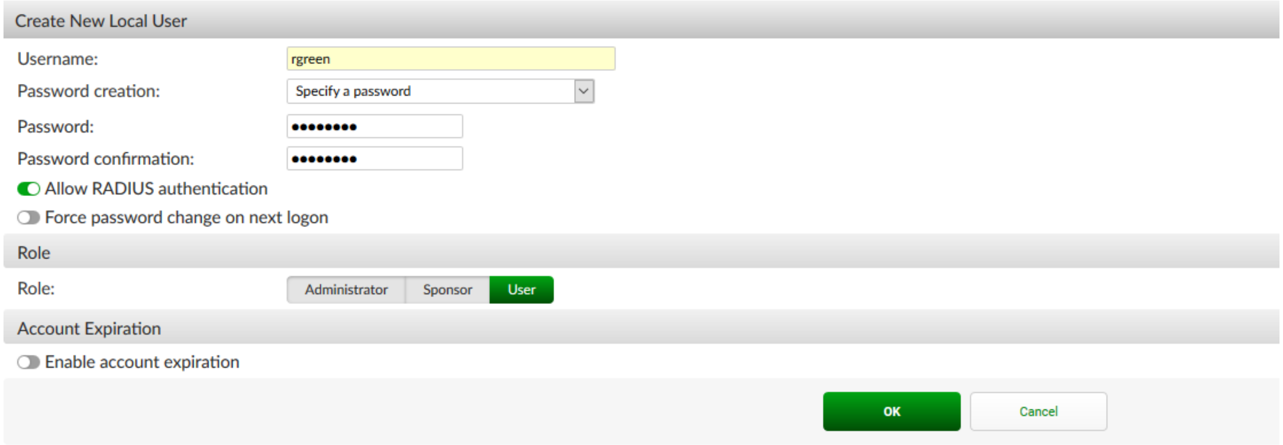
In this example, you use a RADIUS server to authenticate your WiFi clients.

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

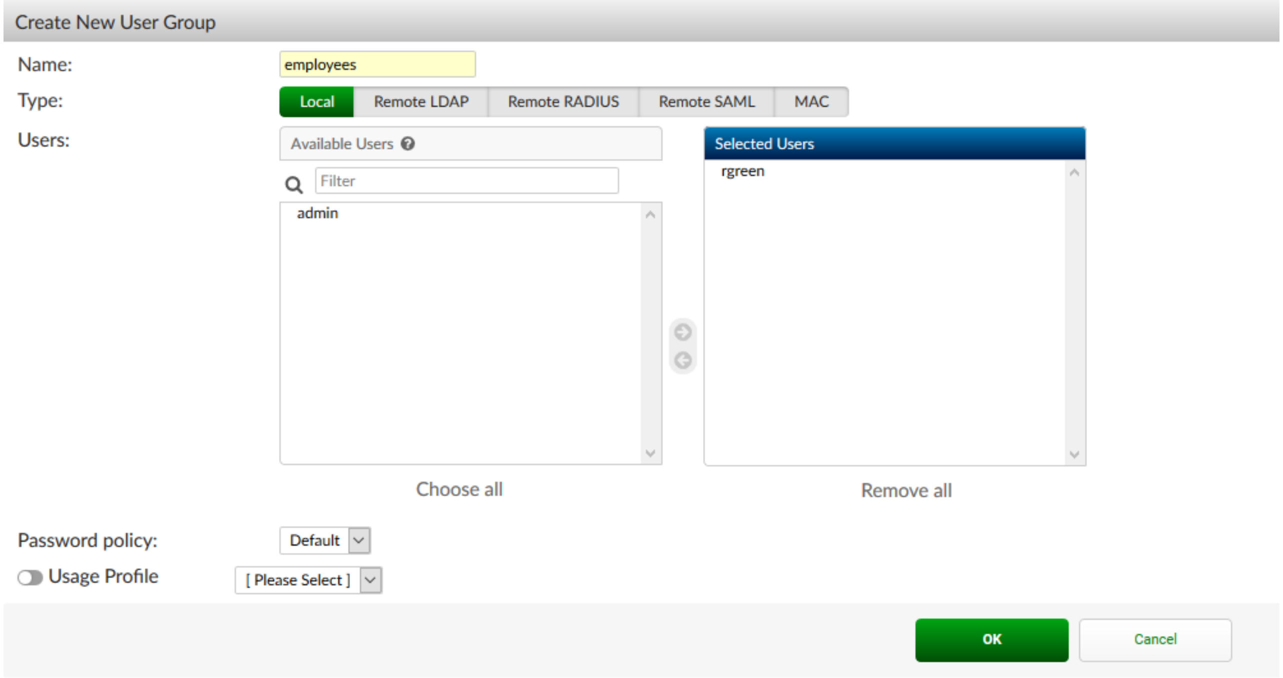
Role: Administrator | Sponsor | [✓ User]

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

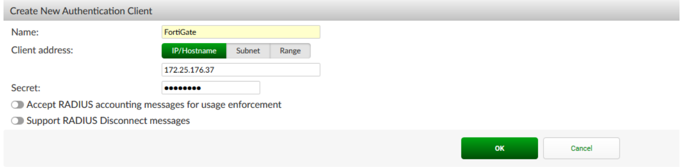
Users: Selected Users: rgreen

Password policy: Default

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: ●●●●●●●●●

Subnet
Range
Accept RADIUS accounting messages for usage enforcement
Support RADIUS Disconnect messages
OK
Cancel

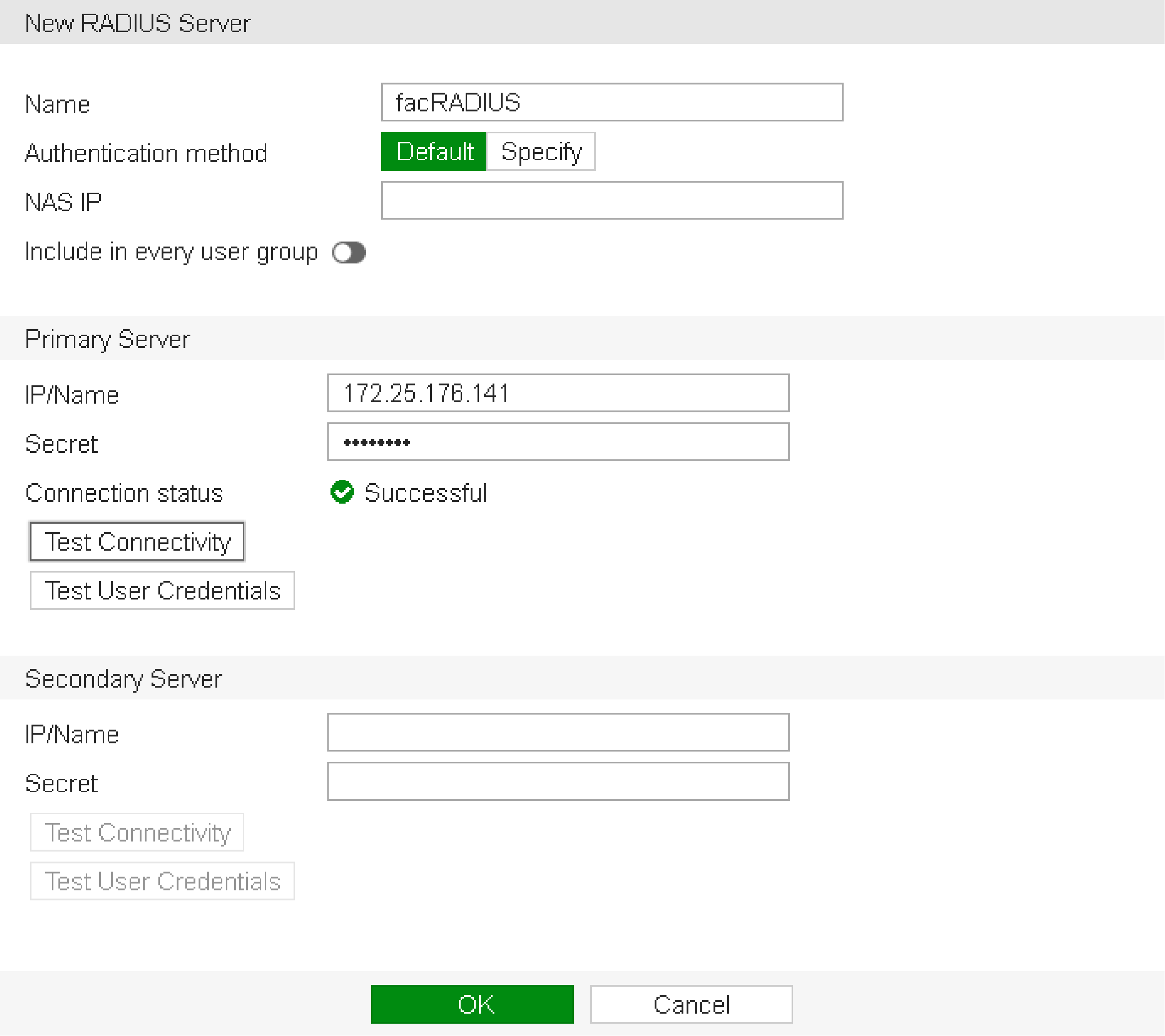
To create the RADIUS policy:

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
NAS IP	
Include in every user group	○

Primary Server

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

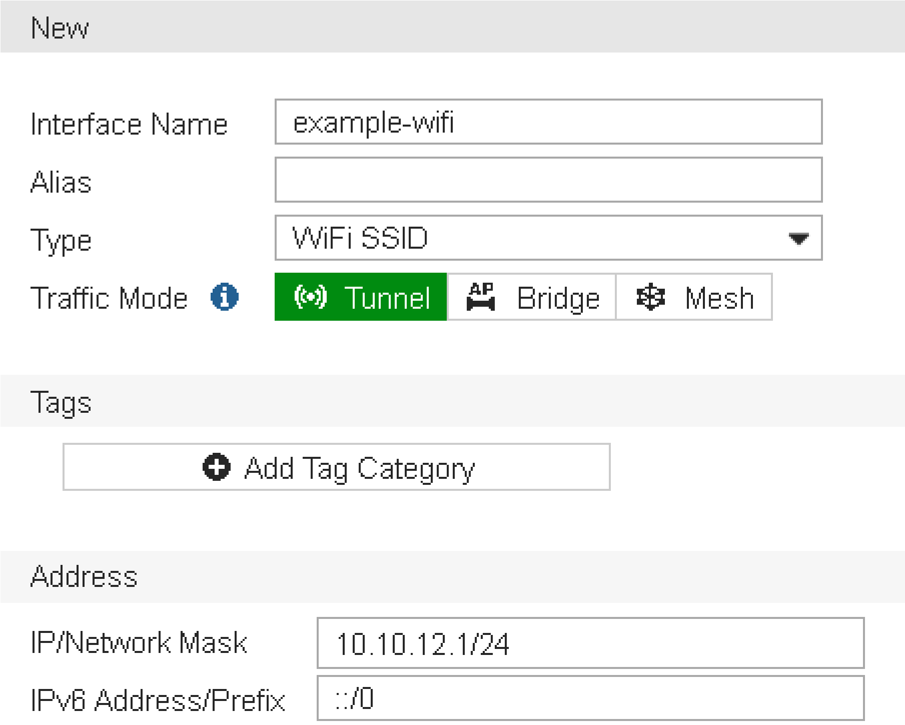
Secondary Server

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

Tags

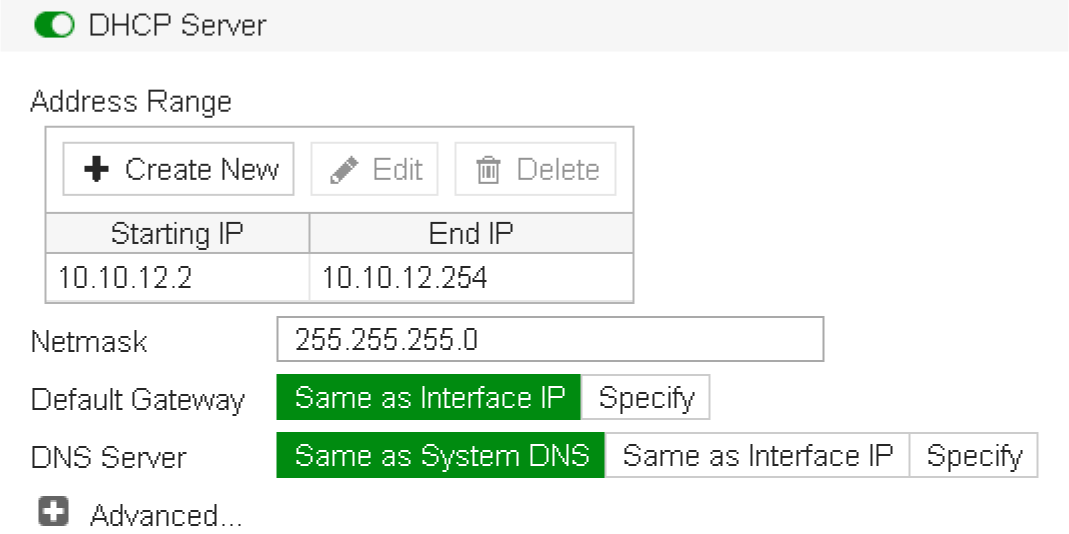
Add Tag Category

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

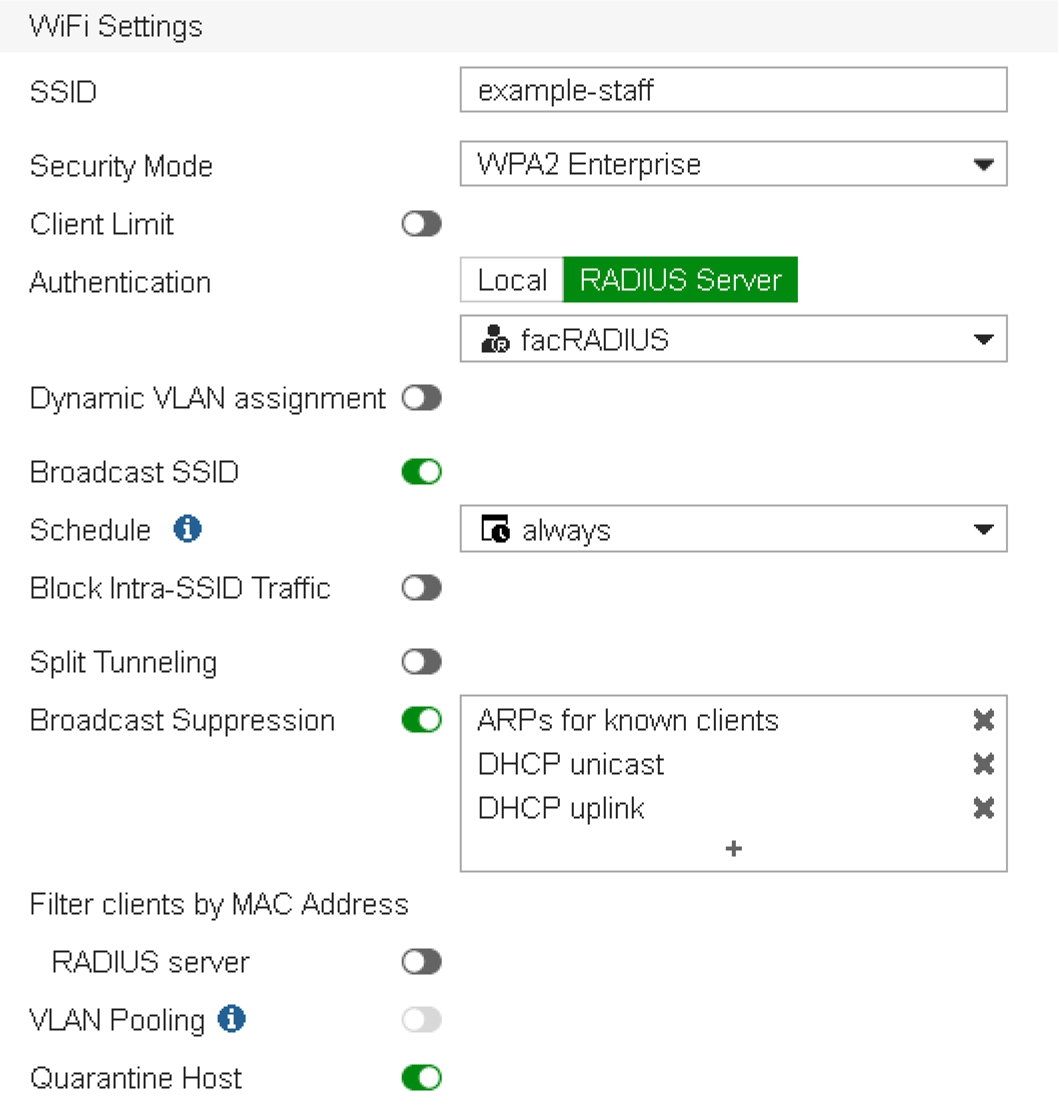
Netmask: 255.255.255.0

Default Gateway: [✓ Same as Interface IP] Specify

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

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: always

Block Intra-SSID Traffic ○

Split Tunneling ○

Broadcast Suppression ●
- ARPs for known clients
- DHCP unicast
- DHCP uplink

Filter clients by MAC Address

RADIUS server ○

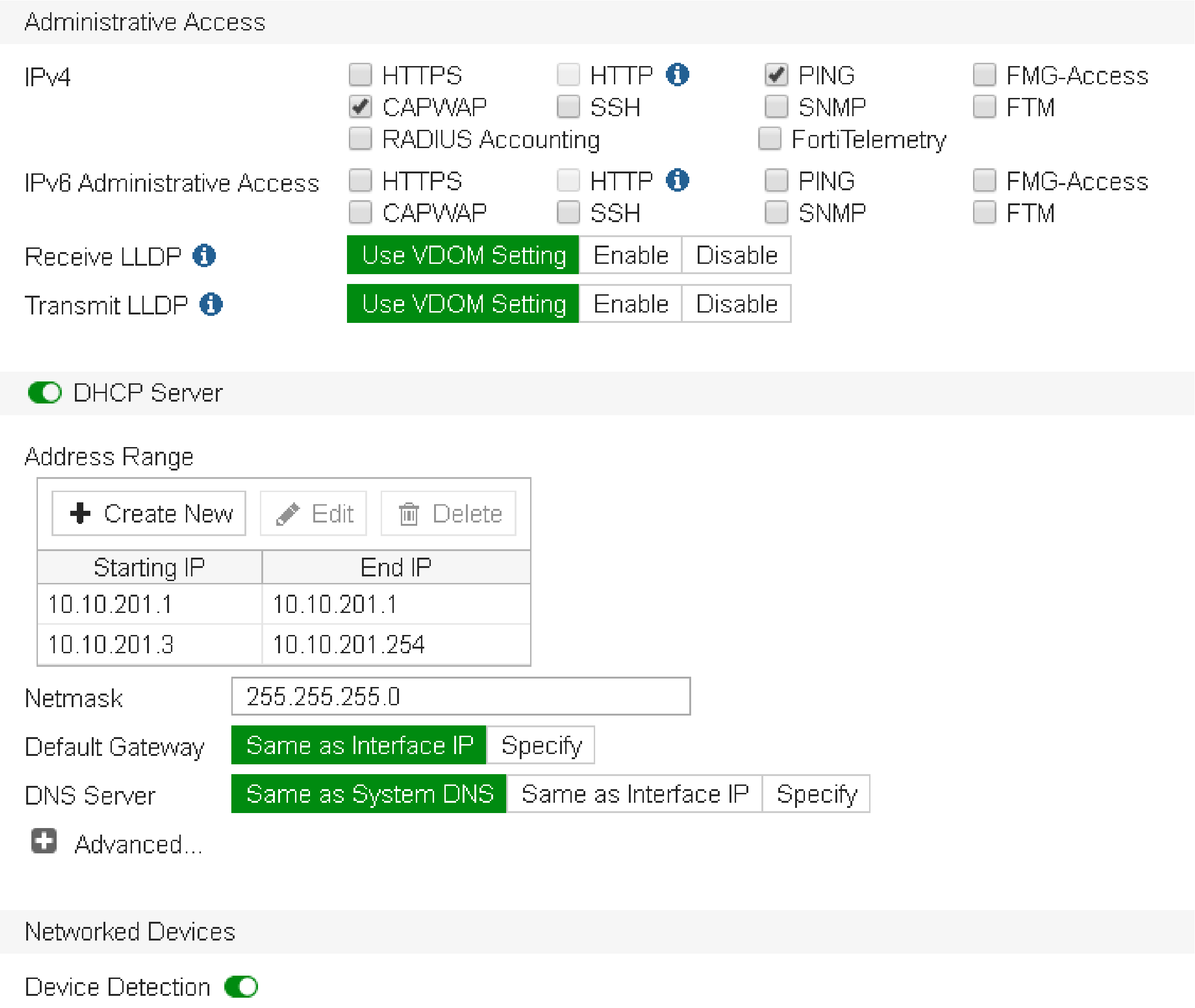
VLAN Pooling ○

Quarantine Host ●

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

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

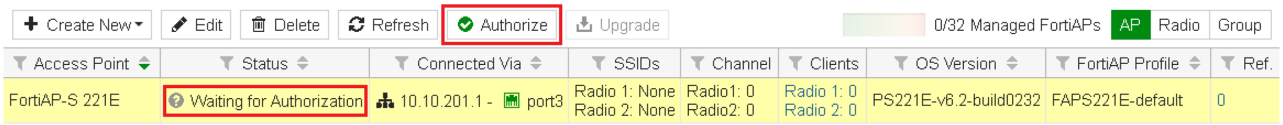
DNS Server: [✓ Same as System DNS] Same as Interface IP Specify

Advanced...

Networked Devices

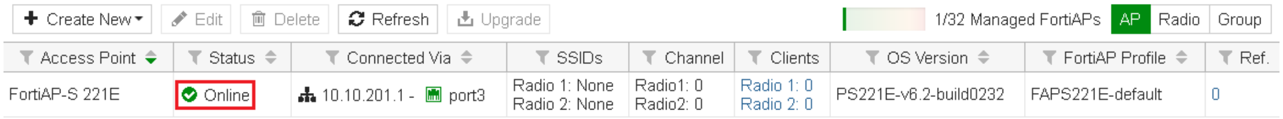
Device Detection

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.



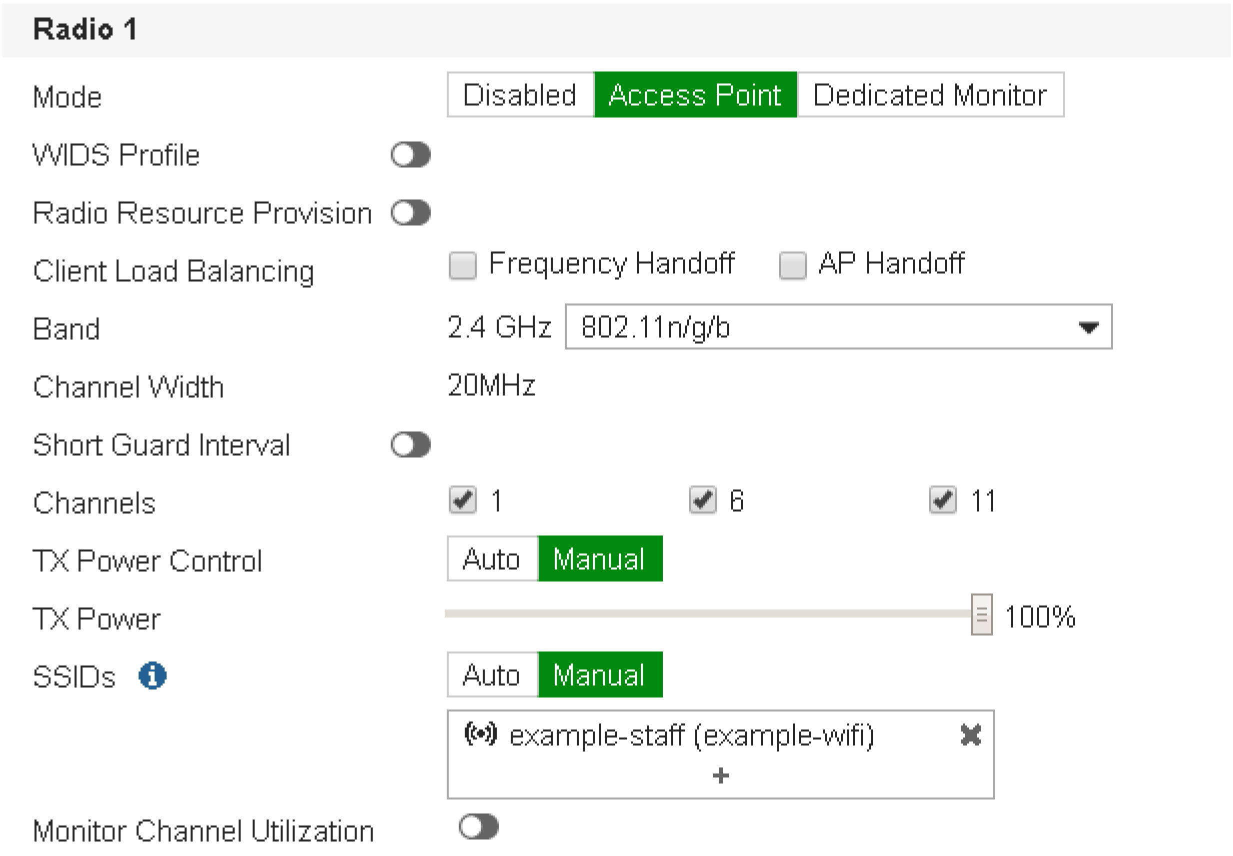
Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Ref.
FortiAP-S 221E	Waiting for Authorization	10.10.201.1 - port3	Radio 1: None Radio 2: None	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	PS221E-v6.2-build0232	FAPS221E-default	0

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*.



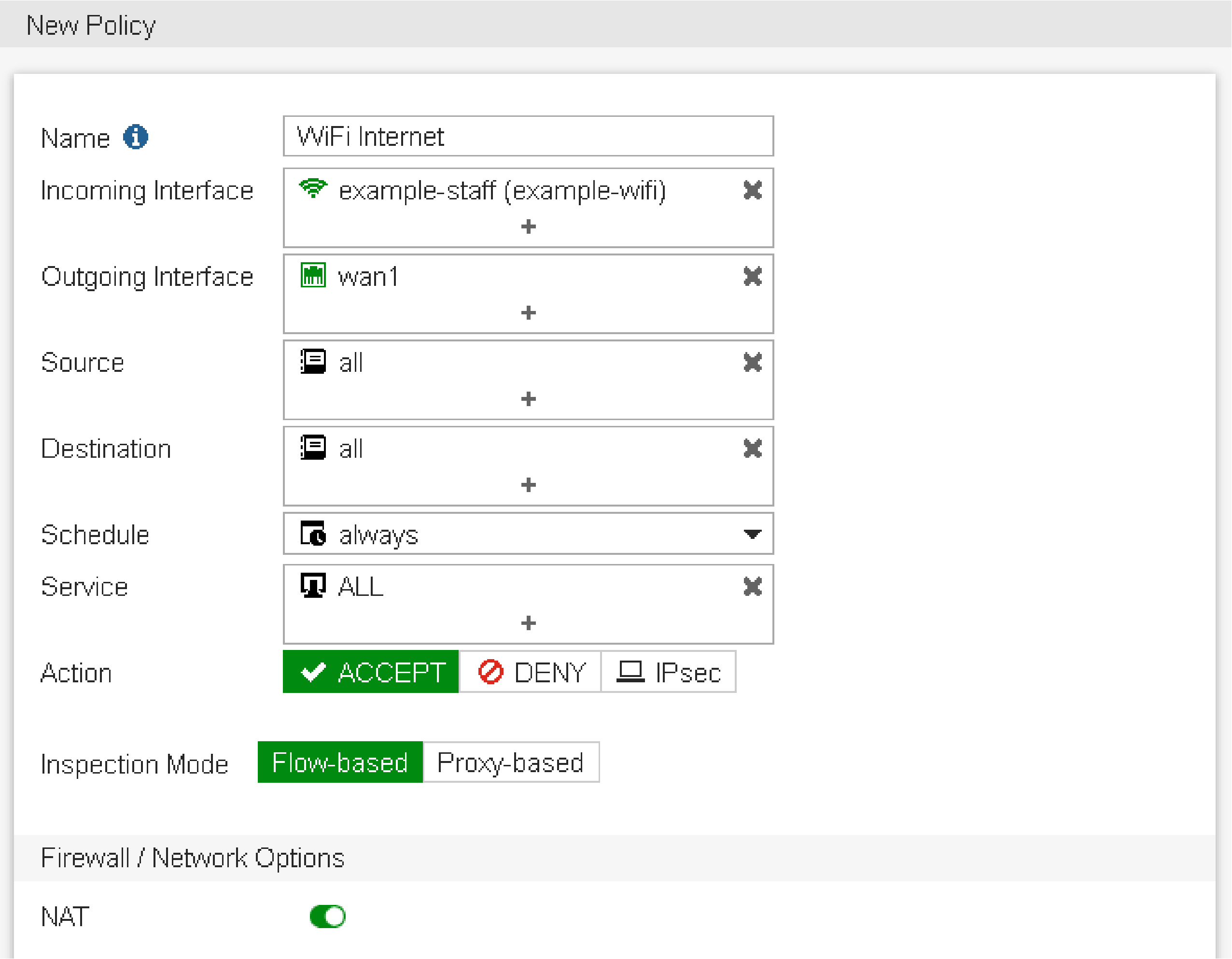
Radio 1

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	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.



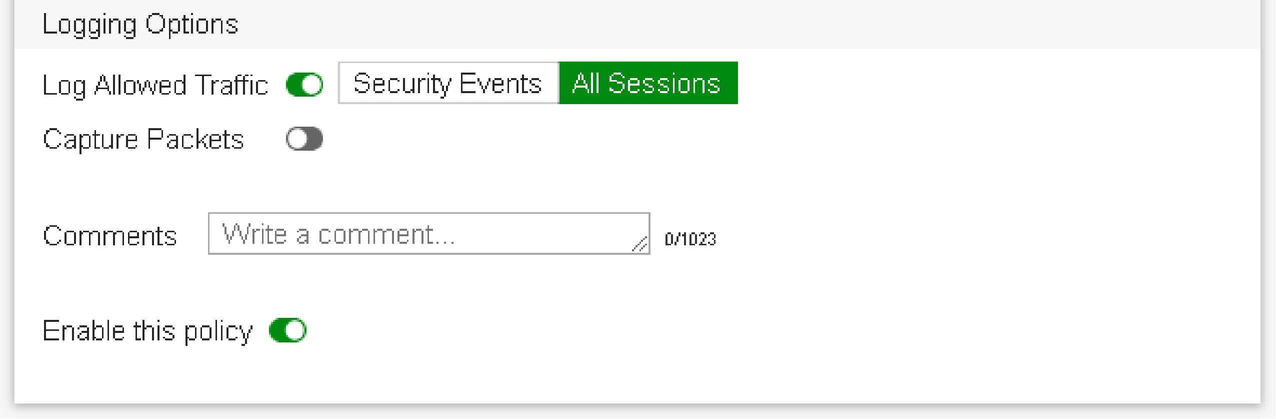
New Policy

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*.

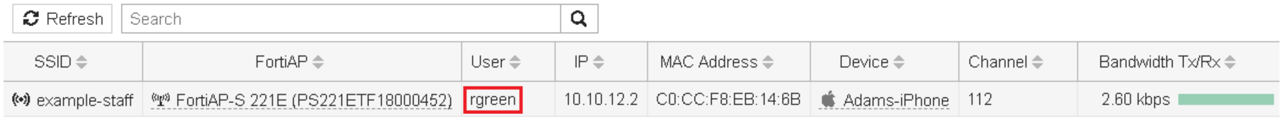


Logging Options

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

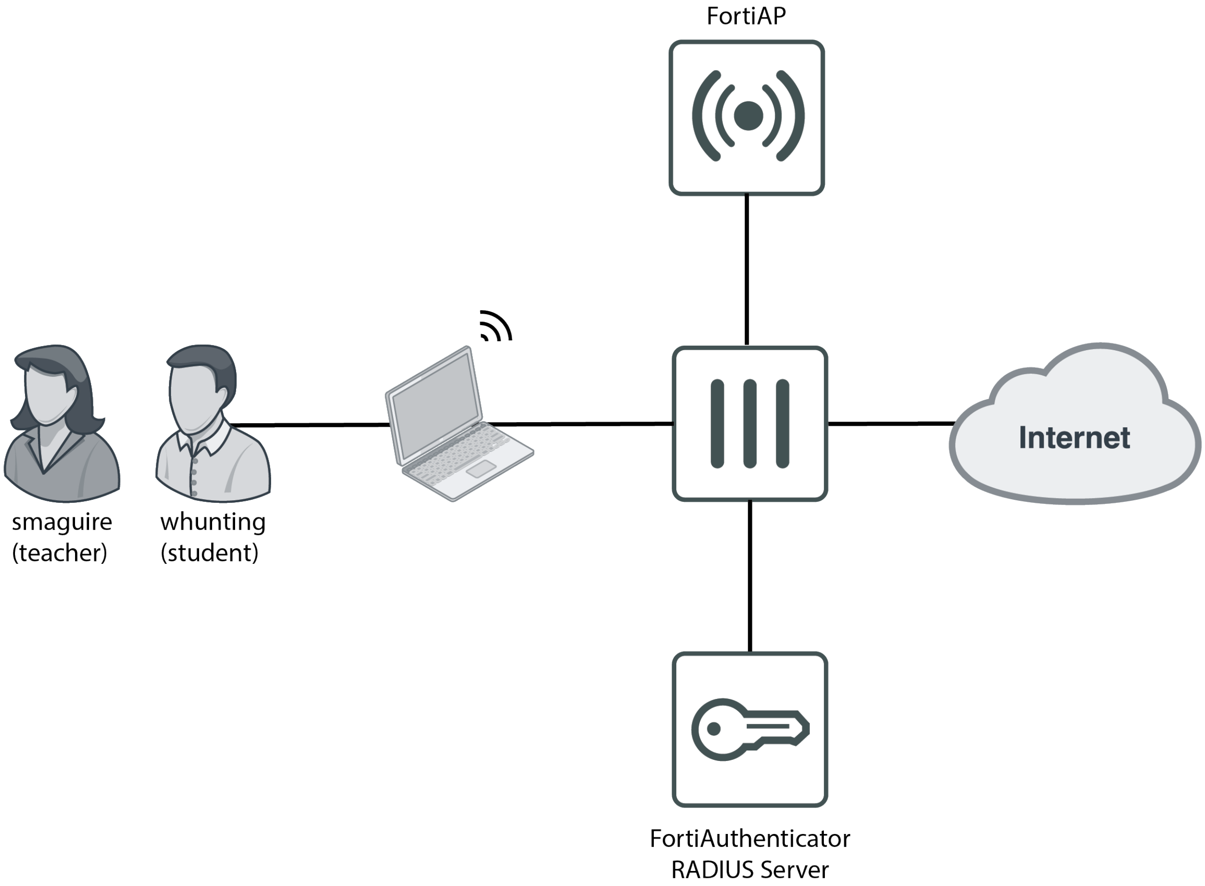
Results

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.

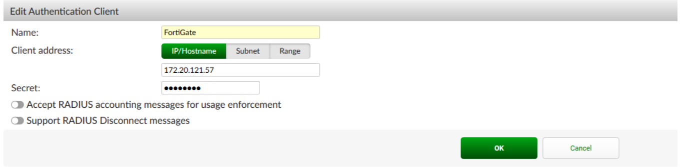
This recipe assumes that an SSID and a FortiAP are configured on the FortiGate unit. In this configuration, you will be changing the existing SSID's WiFi settings so authentication is provided by the RADIUS server.

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

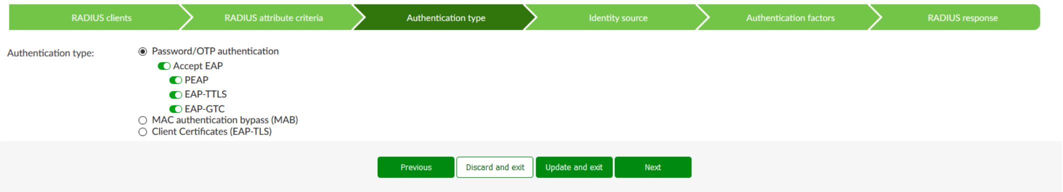
Name:	FortiGate
Client address:	IP/Hostname
	172.20.121.57
Secret:	•••••••••

○ 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)

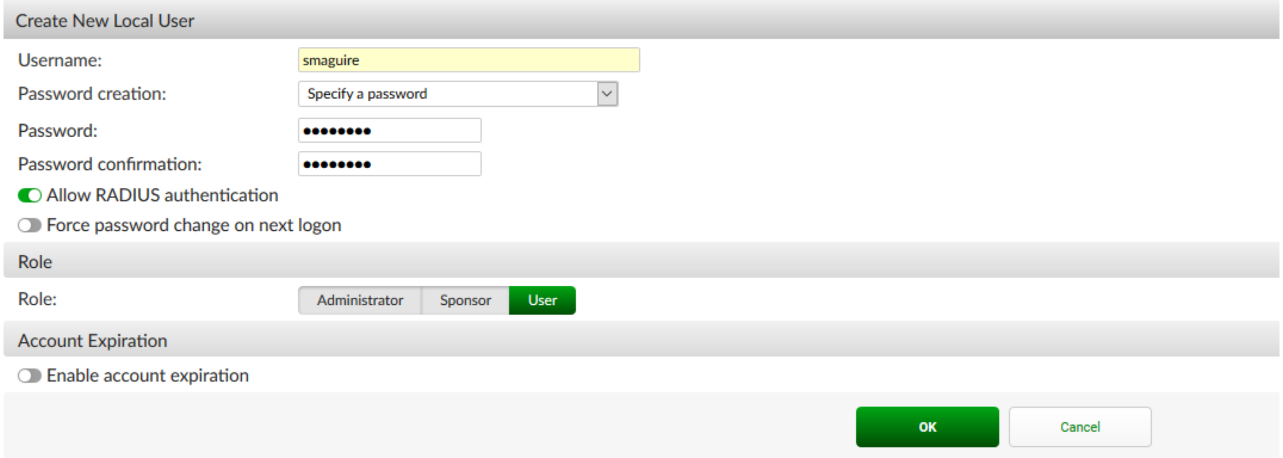
○ Client Certificates (EAP-TLS)

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

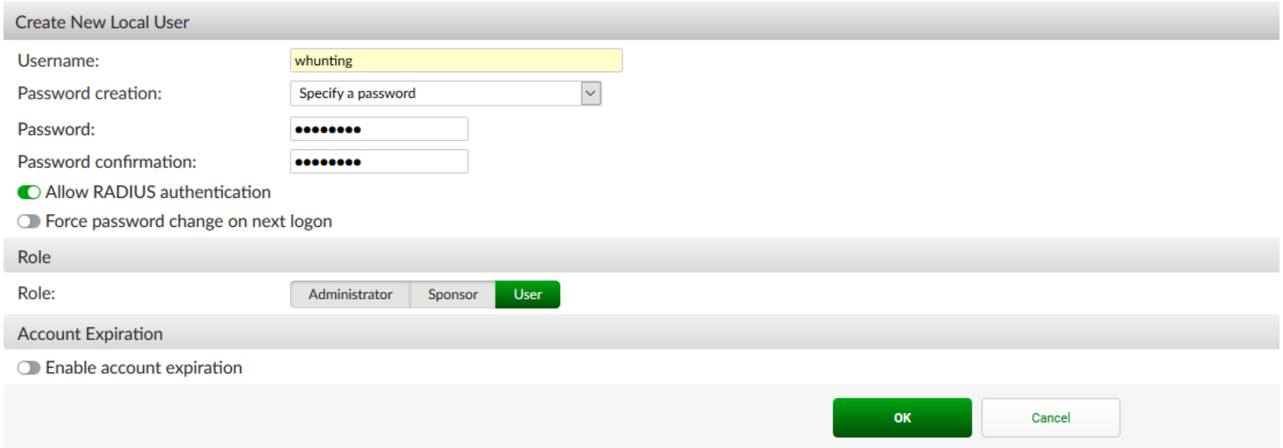
○ Force password change on next logon

Role

Role: User

Account Expiration

○ Enable account expiration



Create New Local User

Username: whunting

Password creation: Specify a password

Password: ••••••••

Password confirmation: ••••••••

Allow RADIUS authentication (on)

Force password change on next logon (off)

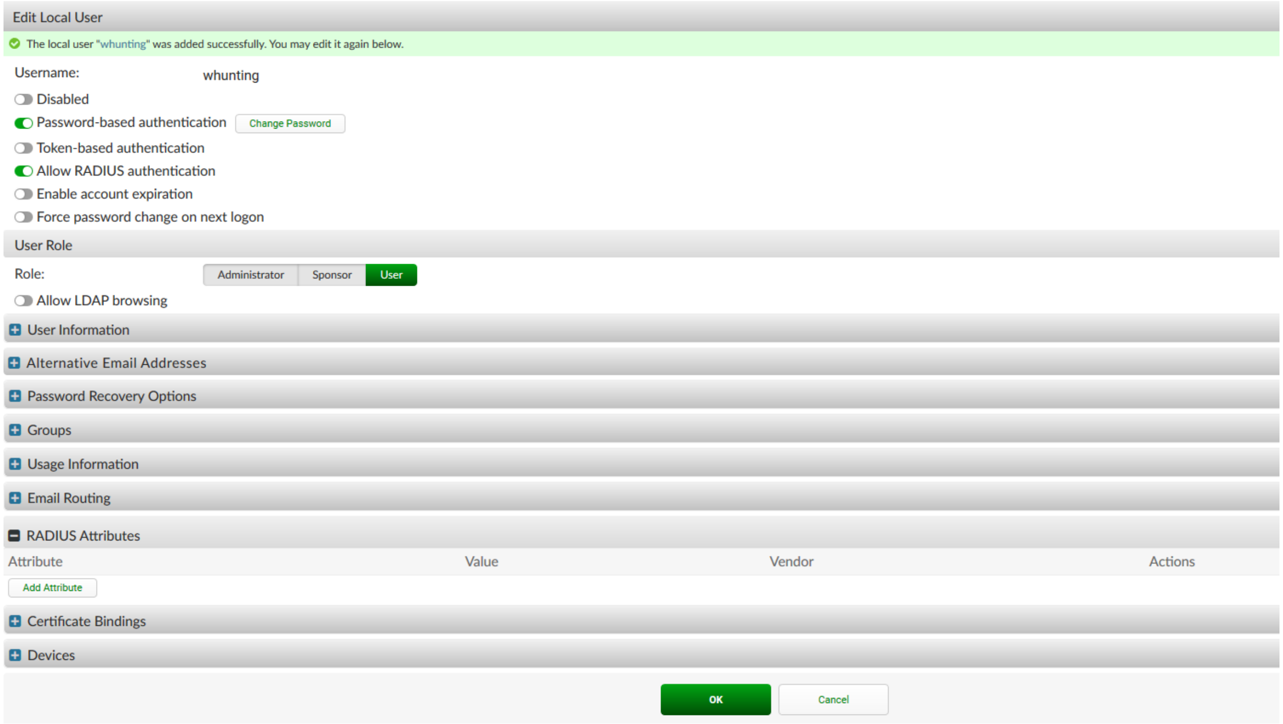
Role

Role: Administrator | Sponsor | User (User selected)

Account Expiration

Enable account expiration (off)

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 (off)

Password-based authentication (on)

Token-based authentication (off)

Allow RADIUS authentication (on)

Enable account expiration (off)

Force password change on next logon (off)

User Role

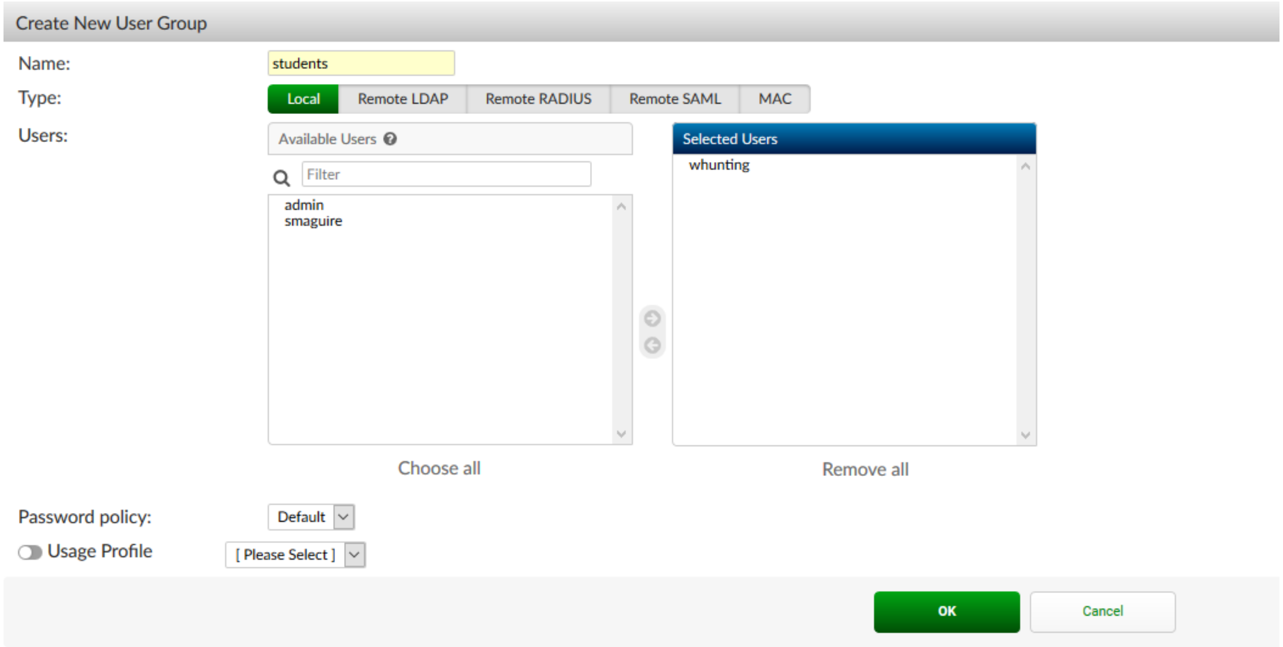
Role: Administrator | Sponsor | User (User selected)

Allow LDAP browsing (off)

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:

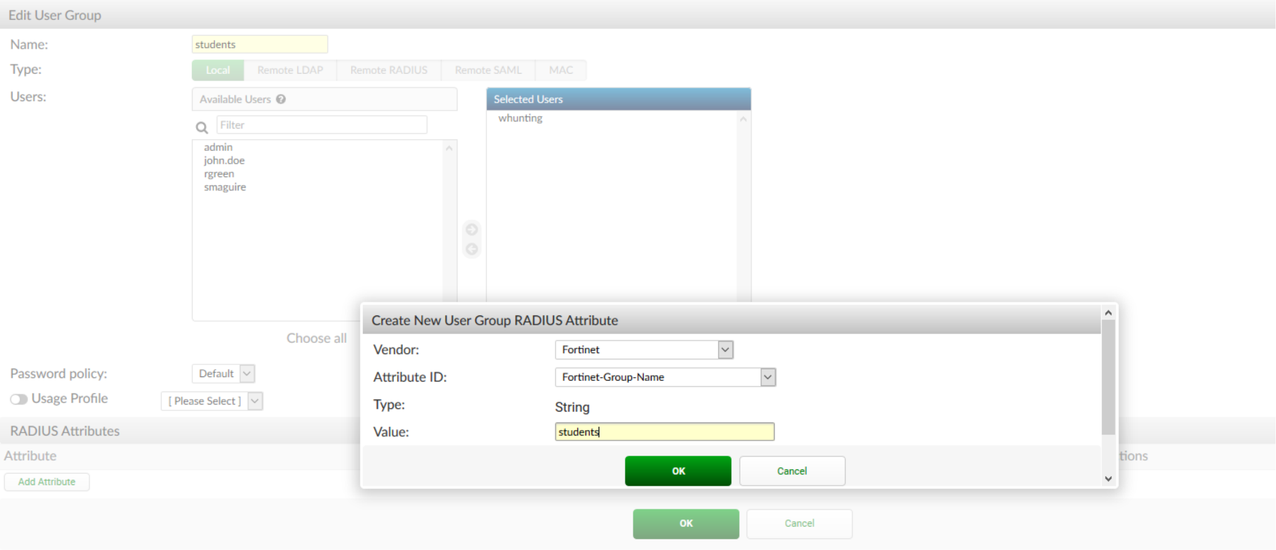
Available Users: admin, smaguire

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

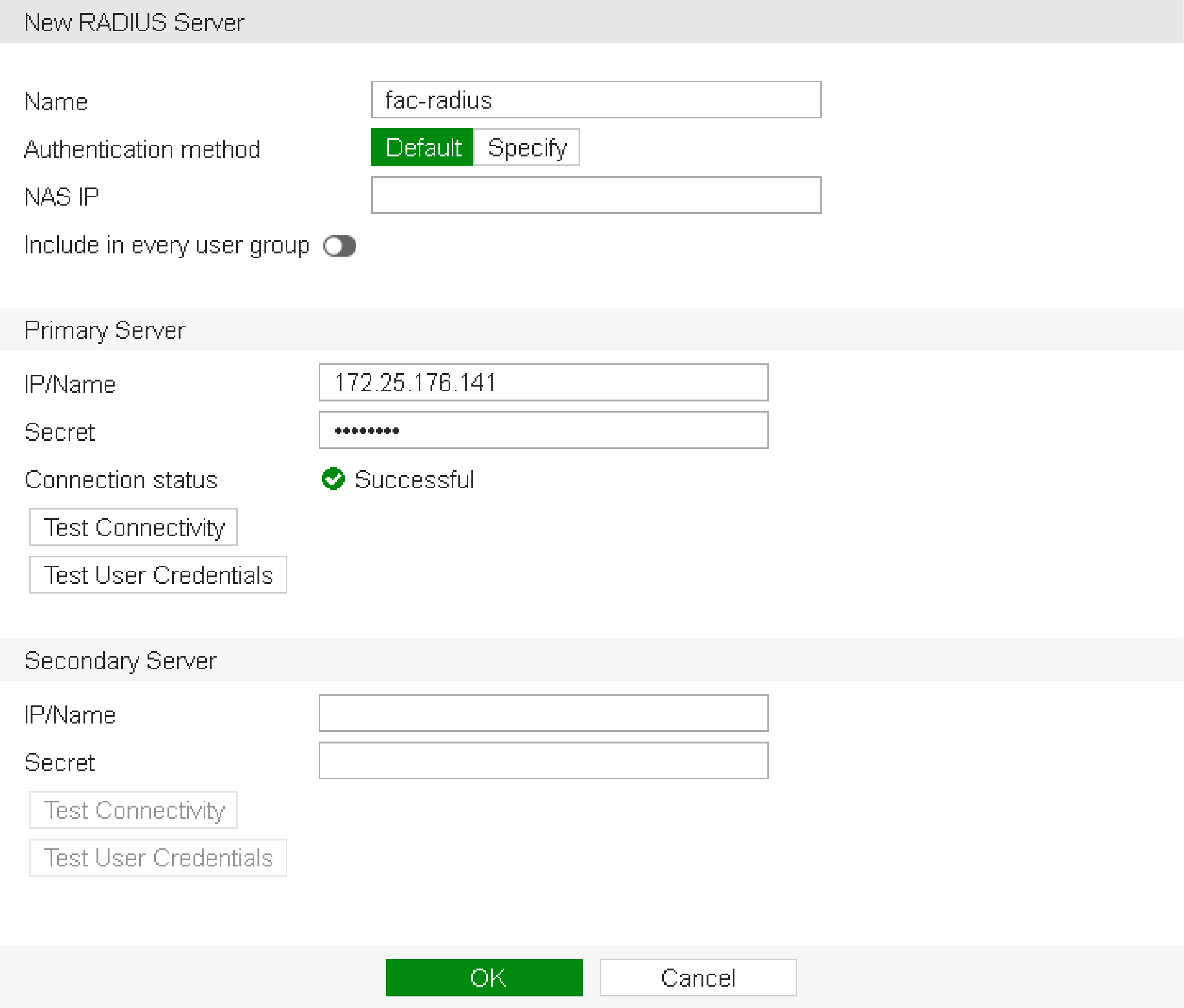
Value: students

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

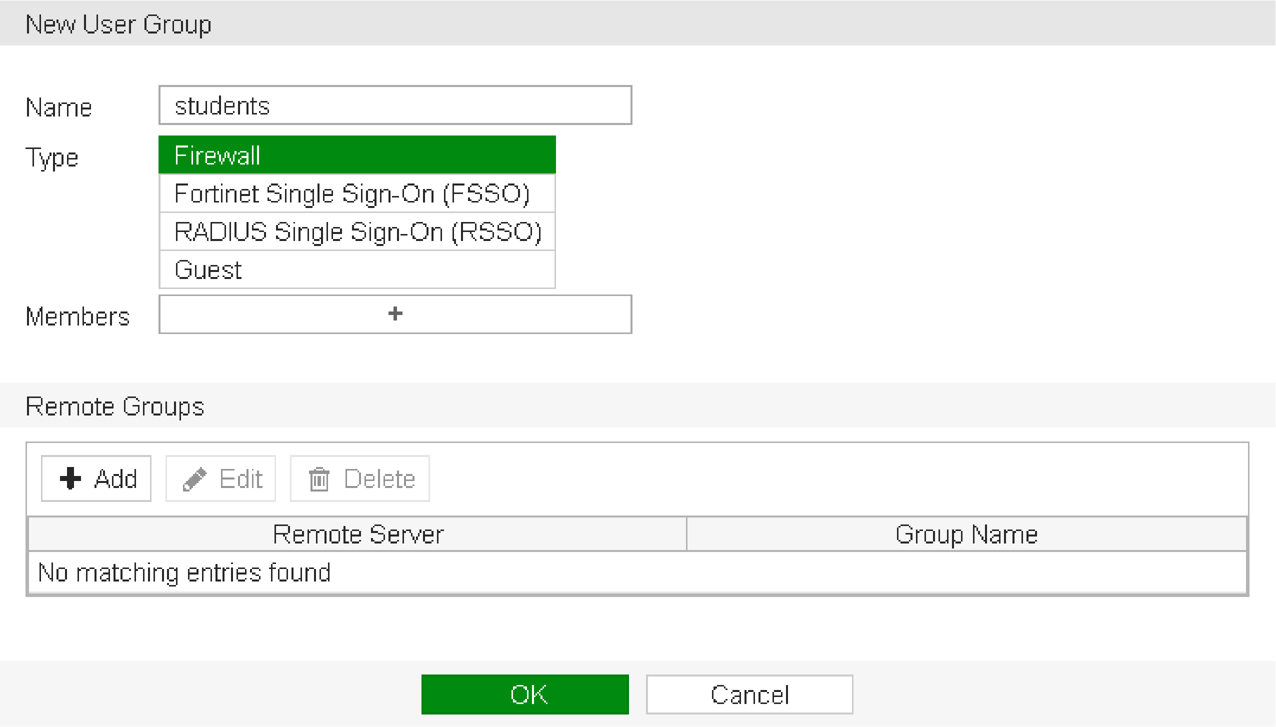
IP/Name:

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

Members:

Remote Groups

Remote Server	Group Name
No matching entries found	

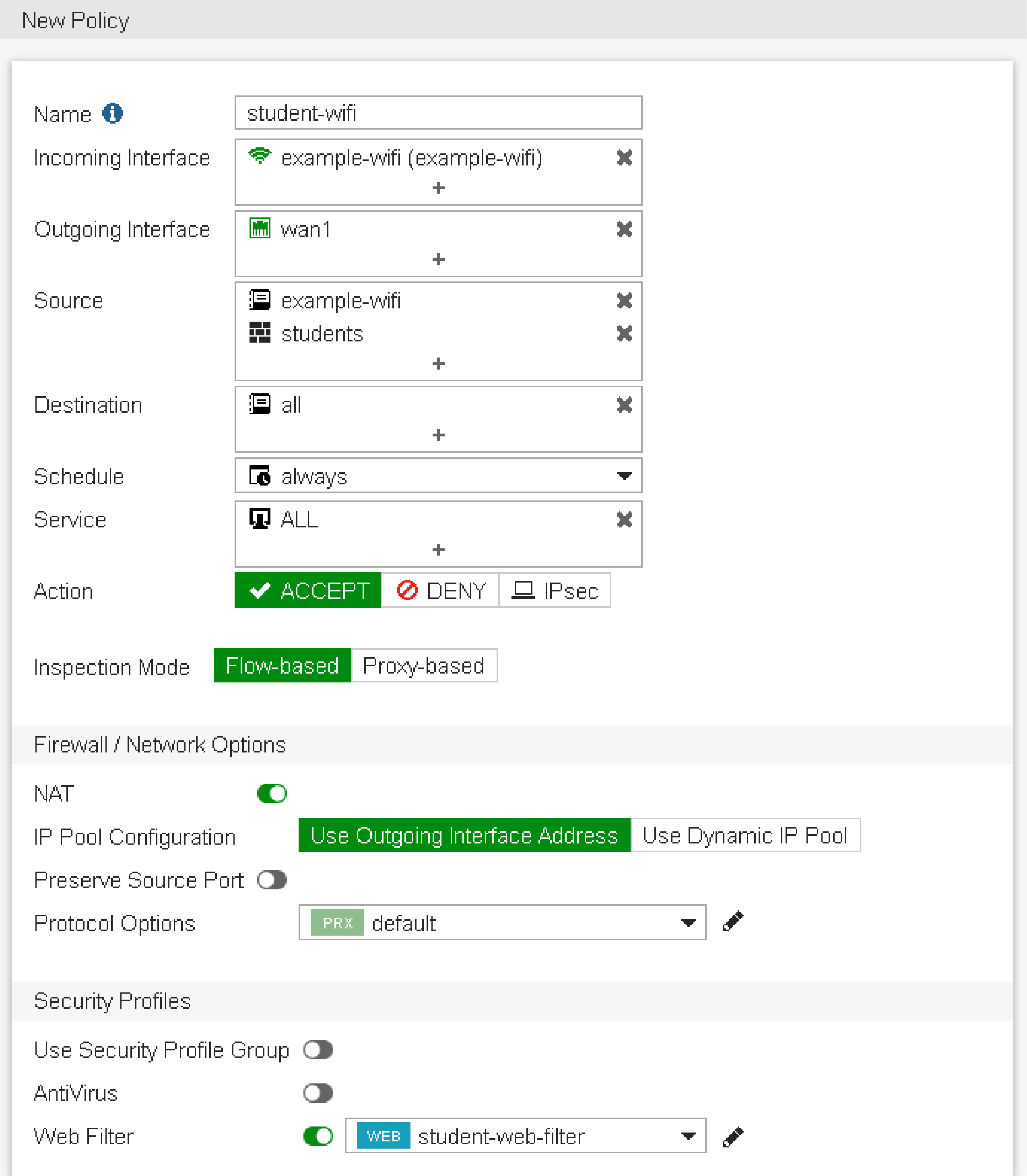
Do not add any members to either group.

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

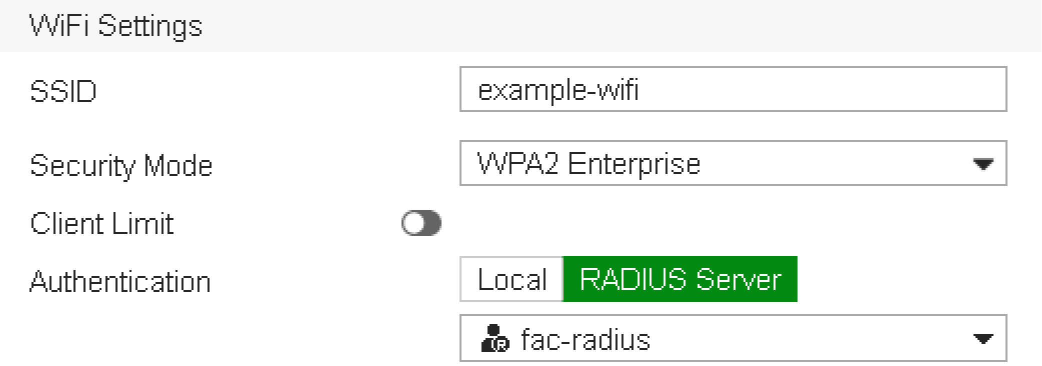
Security Profiles

Use Security Profile Group	○ off
AntiVirus	○ off
Web Filter	● on 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

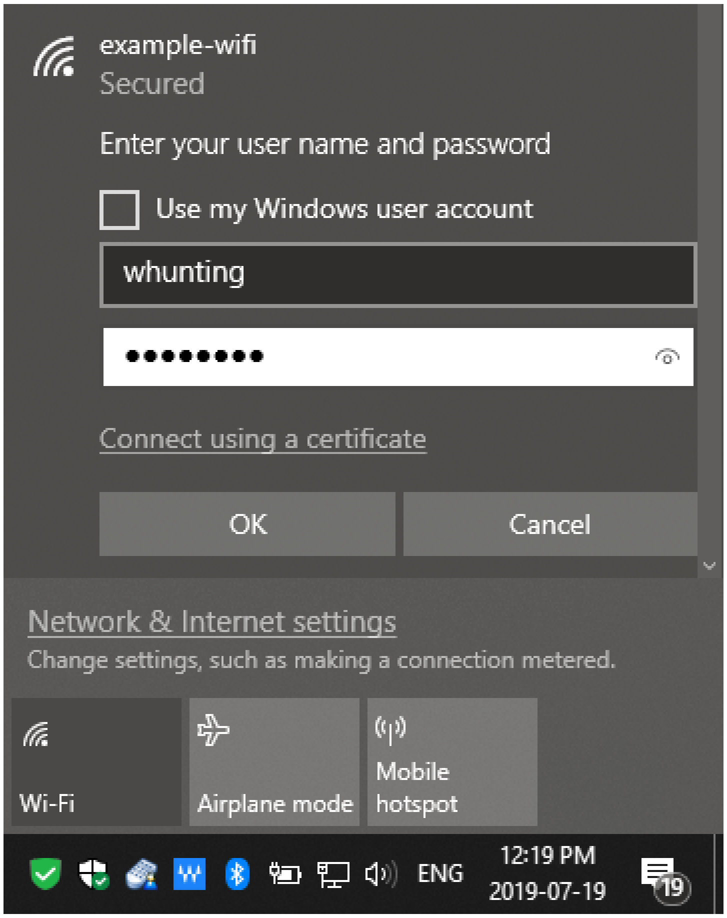
Client Limit

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

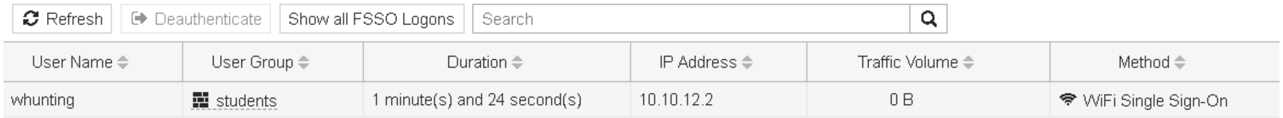
whunting

●●●●●●●●●

Connect using a certificate

Network & Internet settings
Change settings, such as making a connection metered.

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.



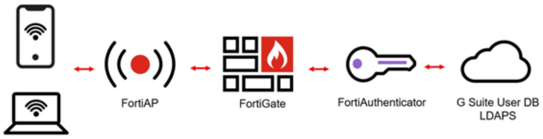
User Name	User Group	Duration	IP Address	Traffic Volume	Method
whunting	students	1 minute(s) and 24 second(s)	10.10.12.2	0 B	WiFi Single Sign-On

802.1X authentication using FortiAuthenticator with Google Workspace User Database

This recipe walks you through integrating FortiAP using a WPA2-Enterprise WLAN encryption with 802.1X authentication using FortiAuthenticator against Google Workspace as the user database with Secure LDAP.

The customer uses Google Workspace user database to validate that a corporate user has a valid username and password and that they can authenticate to join the corporate network. FortiAuthenticator also provides dynamic VLAN here.

Topology



In this example, the user attempts to join the corporate WLAN; a WPA2-Enterprise WLAN, using FortiAuthenticator as a RADIUS server. FortiGate acts as an authenticator forwarding the request to FortiAuthenticator.

FortiAuthenticator is the authentication server and forwards the user request to a remote LDAP server. Here, Google Workspace using Secure LDAP.

If authentication succeeds, the user joins the corporate WLAN and receives attributes from FortiAuthenticator, such as a dynamic VLAN.

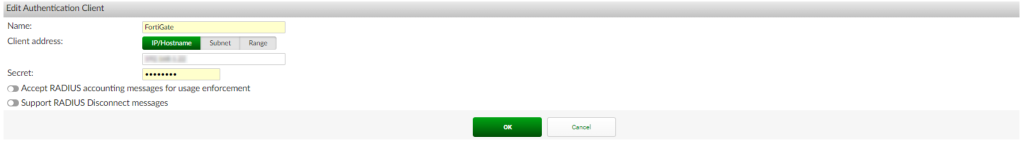
To configure 802.1X authentication using FortiAuthenticator with Google Workspace User Database:

1. Configuring FortiGate as a RADIUS client on page 164.
2. Configuring Google Workspace as an LDAP server. See Google Workspace integration using LDAP on page 169.
3. Creating a realm and RADIUS policy with EAP-TTLS authentication on page 165.
4. Configuring FortiAuthenticator as a RADIUS server in FortiGate on page 166.
5. Configuring a WPA2-Enterprise with FortiAuthenticator as the RADIUS server on page 166.
6. Configuring Windows or macOS to use EAP-TTLS and PAP on page 167.

Configuring FortiGate as a RADIUS client

To configure FortiGate as a RADIUS client:

1. In *Authentication* > *RADIUS Service* > *Clients*, click *Create New*.
2. Enter a unique name for the RADIUS client and the IP address from which it will be connecting.
   This is the IP address of the RADIUS client itself, here, FortiGate, not the IP address of the end-user's device.
3. Enter a password for *Secret*.
   The secret is a pre-shared secure password that the device, here, FortiGate, uses to authenticate to FortiAuthenticator.
4. Click *OK* to save changes to the RADIUS client.



Edit Authentication Client

Name: FortiGate

Client address: IP/Hostname | Subnet | Range

[redacted]

Secret: ••••••••

○ Accept RADIUS accounting messages for usage enforcement

○ Support RADIUS Disconnect messages

Creating a realm and RADIUS policy with EAP-TTLS authentication

To create a realm for the Google Workspace LDAP server:

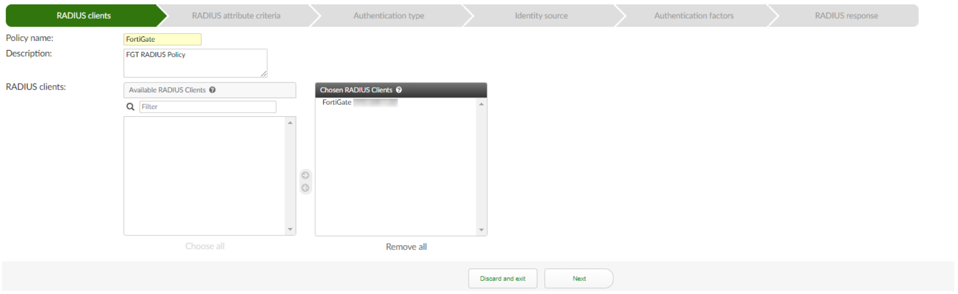
1. Go to *Authentication* > *User Management* > *Realms*, click *Create New*.
2. Enter a *Name* for the realm.

The realm name may only contain letters, numbers, periods, hyphens, and underscores. It cannot start or end with a special character.

3. Select the previously set Google Workspace LDAP server for the realm from the *User source* dropdown.
4. Click *OK* to create the new realm.

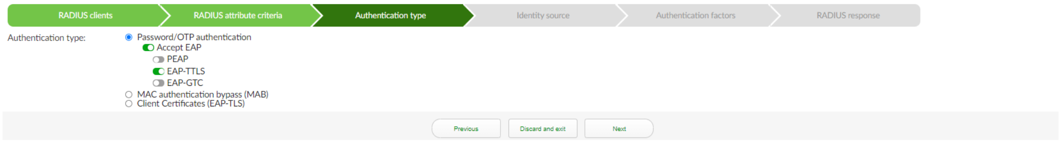
To create a RADIUS policy:

1. In *Authentication* > *RADIUS Service* > *Policies*, click *Create New*.
2. For RADIUS clients, enter an identifiable policy name and description, and add the newly created RADIUS client to the policy. Click *Next*.



Policy name: FortiGate
Description: FGT RADIUS Policy
RADIUS clients:
Chosen RADIUS Clients: FortiGate [redacted]

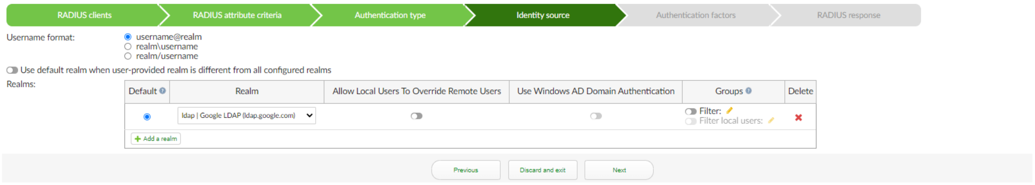
3. For *RADIUS attribute criteria*, no settings are required. Click *Next*.
   a. For *Authentication type*, select *Password/OTP authentication*, enable *Accept EAP*, then enable *EAP-TTLS*. Click *Next*.



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

This allows using EAP-TTLS and PAP in the user's device Wireless settings.

4. For *Identity source*, choose a username format, and select the realm related to Google Workspace Secure LDAP. Click *Next*.



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

Use default realm when user-provided realm is different from all configured realms (disabled)

Realms:

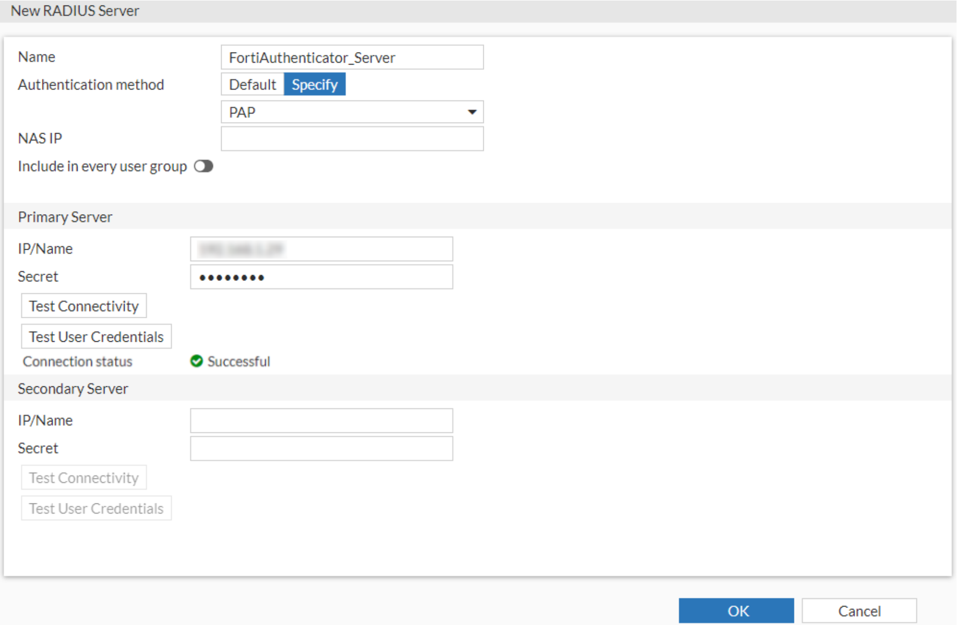
Default	Realm	Allow Local Users To Override Remote Users	Use Windows AD Domain Authentication	Groups	Delete
●	ldap | Google LDAP (ldap.google.com)	off	off	Filter: Filter local users:	✖

5. For *Authentication factors*, select *Every configured password and OTP factors*, and click *Next*. In this menu you can also enable the option to *Allow FortiToken Mobile push notifications*.
6. For *RADIUS response*, review the policy, and click *Save and exit*.

Configuring FortiAuthenticator as a RADIUS server in FortiGate

To configure the FortiGate authentication settings:

1. Go to *User & Authentication > RADIUS Servers*, and click *Create New*.
2. Enter a *Name* for the RADIUS server.
3. For *Authentication method*, select *Specify*, then select *PAP* from the dropdown.
4. Enter the IP address of the RADIUS server.
5. Enter the shared *Secret* key, and click *OK*.
   The secret is the same as the one used when setting up the RADIUS client, here, FortiGate.
6. Click *Test Connectivity* to test the connection to the server, and ensure that the connection status is *Successful*.
7. Click *OK* to save changes.



New RADIUS Server

Name: FortiAuthenticator_Server
Authentication method: Default **Specify**
PAP
NAS IP:
Include in every user group ○

Primary Server
IP/Name: [redacted]
Secret: ••••••••

Connection status: ✓ Successful

Secondary Server
IP/Name:
Secret:

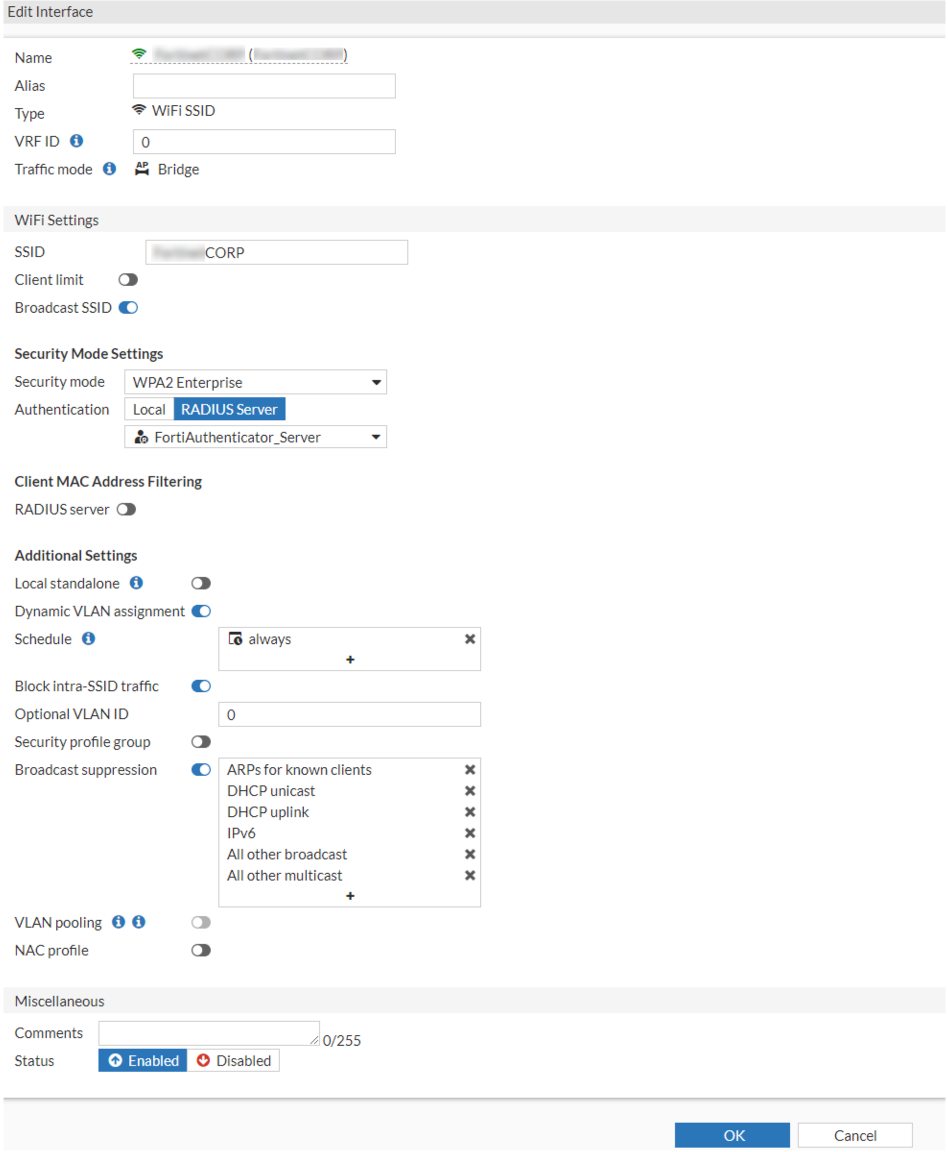
Configuring a WPA2-Enterprise with FortiAuthenticator as the RADIUS server

To configure a WPA2-Enterprise WLAN:

1. Go to *WiFi & Switch Controller > SSIDs*.
2. From the *Create New* dropdown, select *SSID*.
3. Enter a *Name* for the interface. Optionally, you can enter an alias.
4. In *Traffic* mode, select *Bridge*.
5. In the *WiFi settings* pane:
   a. Enter a name in the *SSID* field.
   b. Enable *Broadcast SSID*.
   c. In *Security mode* dropdown, select *WPA2 Enterprise*.
   d. In *Authentication*, select *RADIUS Server*, and from the dropdown select the FortiAuthenticator RADIUS server you created.
   e. Optionally, enable *Dynamic VLAN assignment*.

   f. For *Schedule*, select *always*.
   g. Optionally, enable *Block intra-SSID traffic*.
   h. Optionally, enable *Broadcast suppression*, and select *ARPs for known clients*, *DHCP unicast*, *DHCP uplink*, *IPv6*, *ALL other broadcast*, and *All other multicast*.

6. Click *OK* to save changes.



Edit Interface

Name: [redacted] ([redacted])
Alias:
Type: WiFi SSID
VRF ID: 0
Traffic mode: Bridge

WiFi Settings

SSID: [redacted]CORP
Client limit: ○
Broadcast SSID: ●

Security Mode Settings

Security mode: WPA2 Enterprise
Authentication: Local | RADIUS Server (selected)
FortiAuthenticator_Server

Client MAC Address Filtering

RADIUS server: ○

Additional Settings

Local standalone: ○
Dynamic VLAN assignment: ●
Schedule: always
Block intra-SSID traffic: ●
Optional VLAN ID: 0
Security profile group: ○
Broadcast suppression: ●
ARPs for known clients
DHCP unicast
DHCP uplink
IPv6
All other broadcast
All other multicast
VLAN pooling: ○
NAC profile: ○

Miscellaneous

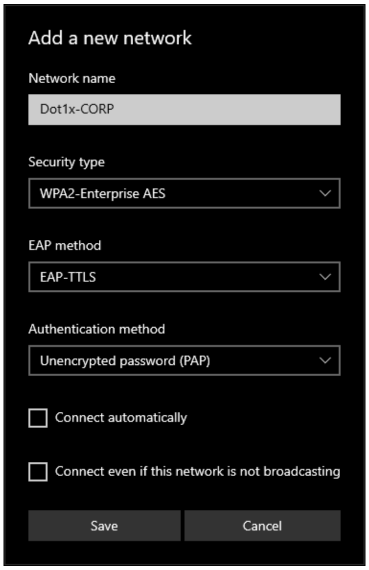
Comments: 0/255
Status: Enabled (selected) | Disabled

Configuring Windows or macOS to use EAP-TTLS and PAP

To configure Windows to use EAP-TTLS and PAP:

1. Go to *Settings* > *Network & Internet*.
2. Select the *Wi-Fi* tab, and click *Manage known networks*.
3. Select *Add a new network*.

4. In the *Add a new network* dialog:
   a. Enter a *Network Name*.
   b. In the *Security type* dropdown, select *WPA2-Enterprise AES*.
   c. In the *EAP method* dropdown, select *EAP-TTLS*.
   d. In the *Authentication method* dropdown, select *Unencrypted password (PAP)*.
5. Click *Save*.



Add a new network

Network name

Dot1x-CORP

Security type

WPA2-Enterprise AES

EAP method

EAP-TTLS

Authentication method

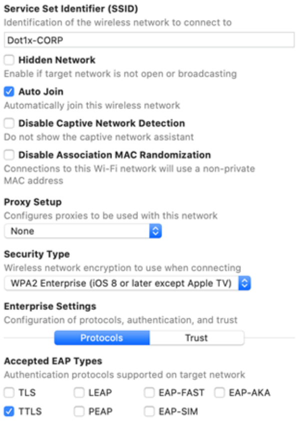
Unencrypted password (PAP)

□ Connect automatically

□ Connect even if this network is not broadcasting

To configure macOS to use EAP-TTLS and PAP:

1. In the menu bar, click the Wi-Fi icon.
2. Click *Create Network*.
3. In the dialog that appears:
   a. Enter a name for *Service Set Identifier (SSID)*.
   b. In the *Security Type* dropdown, select *WPA2-Enterprise (ios 8 or later except Apple TV)*.
   c. Under *Enterprise Settings*, select *Protocols*, then select the *TTLS* checkbox.
   d. In the *Inner Authentication* dropdown, select *PAP*.
4. Click *Create*.



Service Set Identifier (SSID)
Identification of the wireless network to connect to

Dot1x-CORP

□ **Hidden Network**
Enable if target network is not open or broadcasting

☑ **Auto Join**
Automatically join this wireless network

□ **Disable Captive Network Detection**
Do not show the captive network assistant

□ **Disable Association MAC Randomization**
Connections to this Wi-Fi network will use a non-private MAC address

Proxy Setup
Configures proxies to be used with this network

None

Security Type
Wireless network encryption to use when connecting

WPA2 Enterprise (iOS 8 or later except Apple TV)

Enterprise Settings
Configuration of protocols, authentication, and trust

Accepted EAP Types
Authentication protocols supported on target network

□ TLS □ LEAP □ EAP-FAST □ EAP-AKA
☑ TTLS □ PEAP □ EAP-SIM

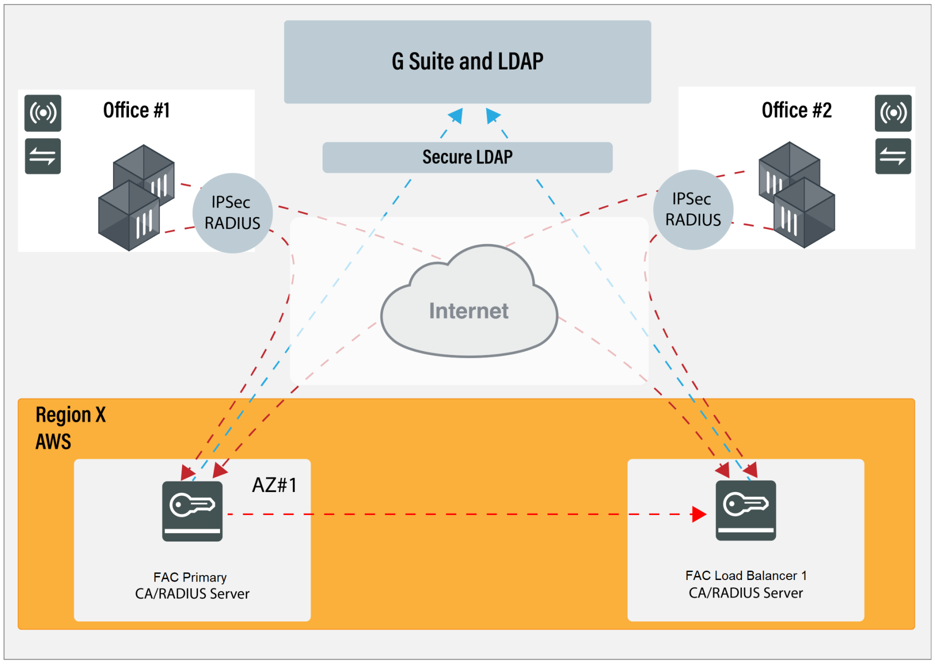
LDAP Authentication

This section describes configuring LDAP authentication.

Google Workspace integration using LDAP

This article explains how to integrate the FortiAuthenticator with Google Workspace 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 Google Workspace certificate on page 169
2. Importing the certificate to FortiAuthenticator on page 171
3. Configuring LDAP on the FortiAuthenticator on page 172
4. Troubleshooting on page 172



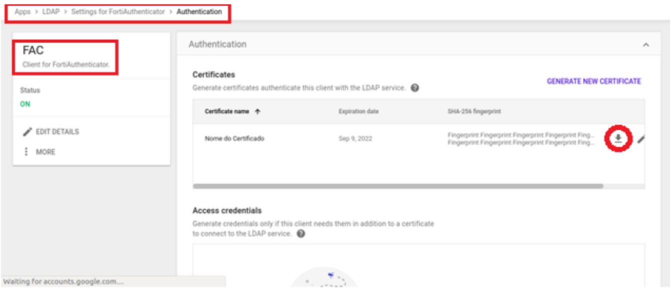
Generating the Google Workspace certificate

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

Authentication

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...

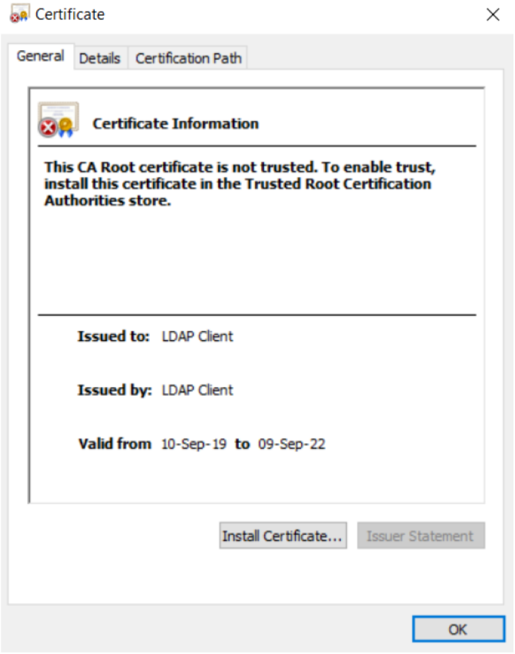
Access credentials
Generate credentials only if this client needs them in addition to a certificate to connect to the LDAP service.

Waiting for accounts.google.com...

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

Example:

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



Certificate

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

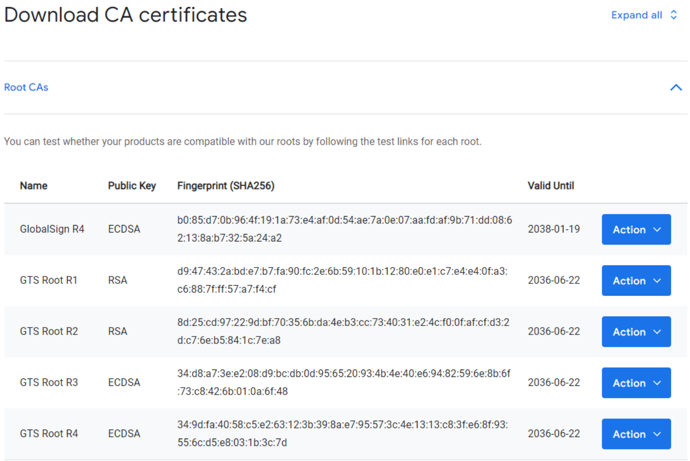
Issued by: LDAP Client

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 Google Trusted CAs to match the chain group, which can be downloaded at https://pki.goog/.

- `GTS Root R1`
- `GTS Root R2`



Download CA certificates

Root CAs

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

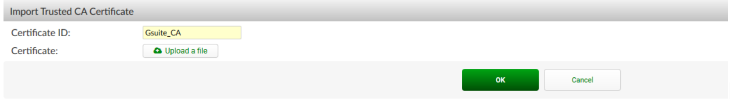
Name	Public Key	Fingerprint (SHA256)	Valid Until	
GlobalSign R4	ECDSA	b0:85:d7:0b:96:4f:19:1a:73:e4:af:0d:54:ae:7a:0e:07:aa:fd:af:9b:71:dd:08:62:13:8a:b7:32:5a:24:a2	2038-01-19	Action
GTS Root R1	RSA	d9:47:43:2a:bd:e7:b7:fa:90:fc:2e:6b:59:10:1b:12:80:e0:e1:c7:e4:e4:0f:a3:c6:88:7f:ff:57:a7:f4:cf	2036-06-22	Action
GTS Root R2	RSA	8d:25:cd:97:22:9d:bf:70:35:6b:da:4e:b3:cc:73:40:31:e2:4c:f0:0f:af:cf:d3:2d:c7:6e:b5:84:1c:7e:a8	2036-06-22	Action
GTS Root R3	ECDSA	34:d8:a7:3e:e2:08:d9:bc:db:0d:95:65:20:93:4b:4e:40:e6:94:82:59:6e:8b:6f:73:c8:42:6b:01:0a:6f:48	2036-06-22	Action
GTS Root R4	ECDSA	34:9d:fa:40:58:c5:e2:63:12:3b:39:8a:e7:95:57:3c:4e:13:13:c8:3f:e6:8f:93:55:6c:d5:e8:03:1b:3c:7d	2036-06-22	Action

Importing the certificate to FortiAuthenticator

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

To import the trusted CA certificate:

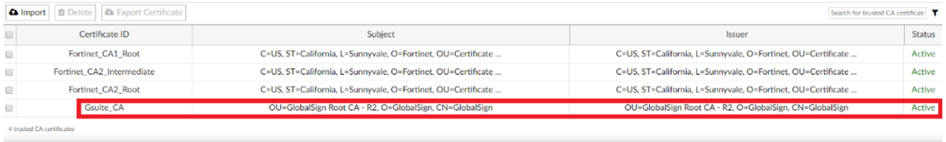
1. Go to *Certificate Management > Certificate Authorities > Trusted CAs > Import*.
2. Enter a Certificate ID, upload a file, and click *OK*.



Import Trusted CA Certificate

Certificate ID:	Gsuite_CA
Certificate:	Upload a file

Results:



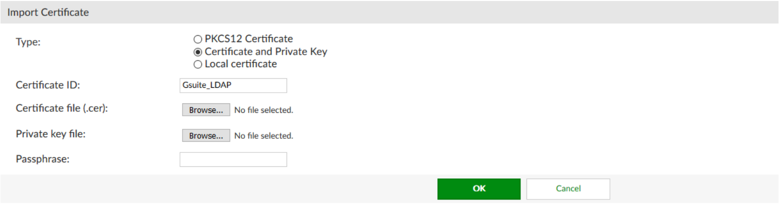
☐	Certificate ID	Subject	Issuer	Status
☐	Fortinet_CA1_Root	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	Active
☐	Fortinet_CA2_Intermediate	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate ...	C=US, ST=California, 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 Google Workspace.

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*.

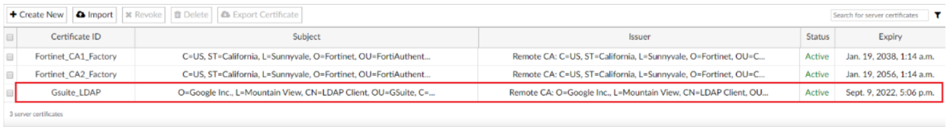


Import Certificate

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:



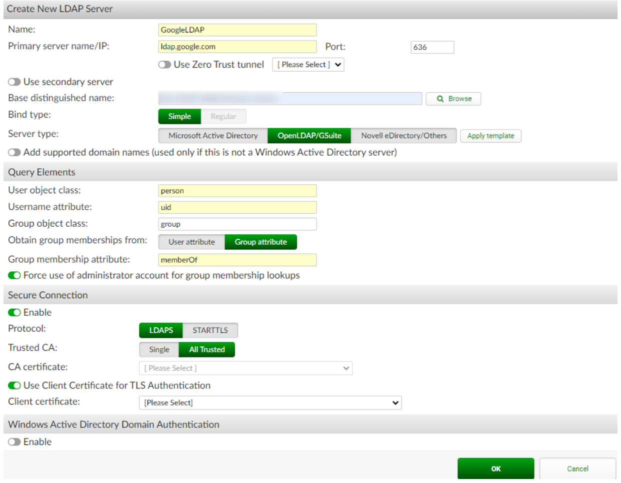
□	Certificate ID	Subject	Issuer	Status	Expiry
□	Fortinet_CA1_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthent...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active	Jan. 19, 2038, 1:14 a.m.
□	Fortinet_CA2_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuthent...	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 *All Trusted* in the *Trusted CA* option.
   - **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 Zero Trust tunnel [Please Select]

Use secondary server

Base distinguished name: [redacted]

Bind type: Simple

Server type: OpenLDAP/GSuite

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

Query Elements

User object class: person

Username attribute: uid

Group object class: group

Obtain group memberships from: Group attribute

Group membership attribute: memberOf

Force use of administrator account for group membership lookups (enabled)

Secure Connection

Enable (enabled)

Protocol: LDAPS

Trusted CA: All Trusted

CA certificate: [Please Select]

Use Client Certificate for TLS Authentication (enabled)

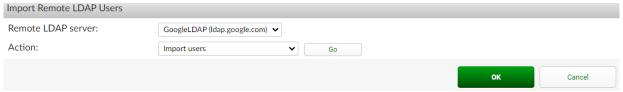
Client certificate: [Please Select]

Windows Active Directory Domain Authentication

Enable

2. Select *OK*.

   If required, you can now import users by selecting *Import users* when editing the LDAP server, selecting the LDAP server from the *Remote LDAP server* dropdown, and 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.



Import Remote LDAP Users

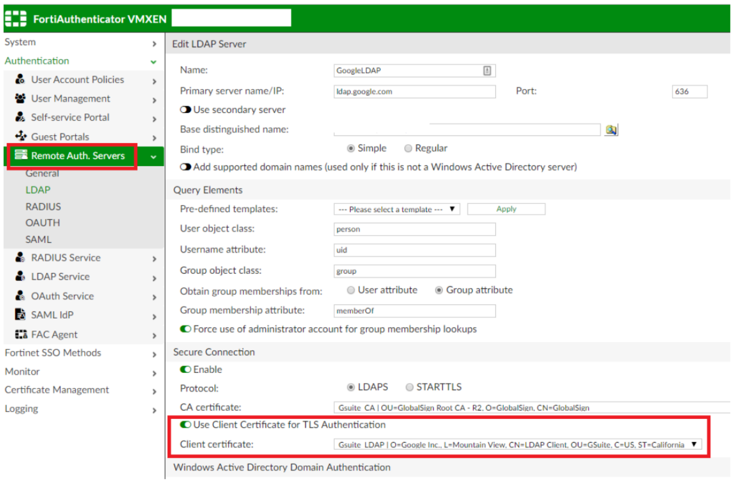
Remote LDAP server: GoogleLDAP (ldap.google.com)

Action: Import users

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.



FortiAuthenticator VMXEN

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

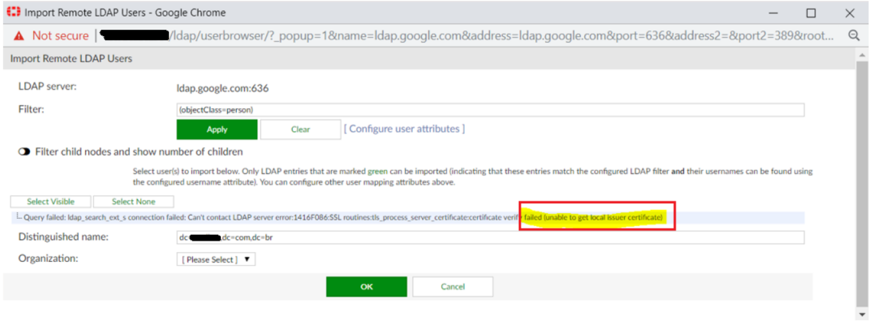
Secure Connection

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 Google Workspace certificate on page 169.



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

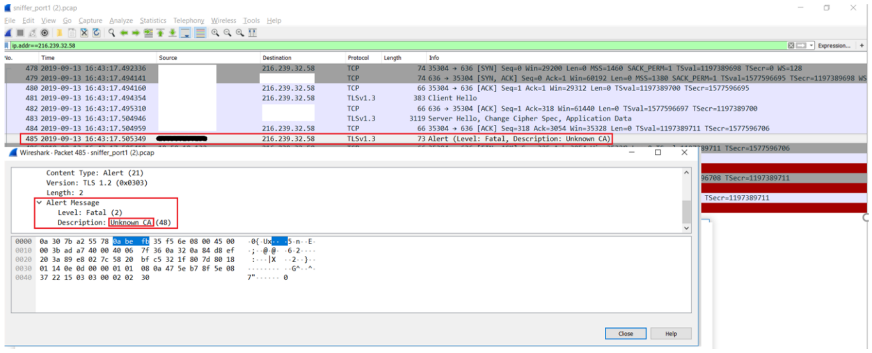
LDAP server: ldap.google.com:636
Filter: (objectClass=person)

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.

```
└ 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] ▼



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 add OTP to the Azure IdP authentication.

To configure FortiAuthenticator as a SAML IdP proxy for Azure:

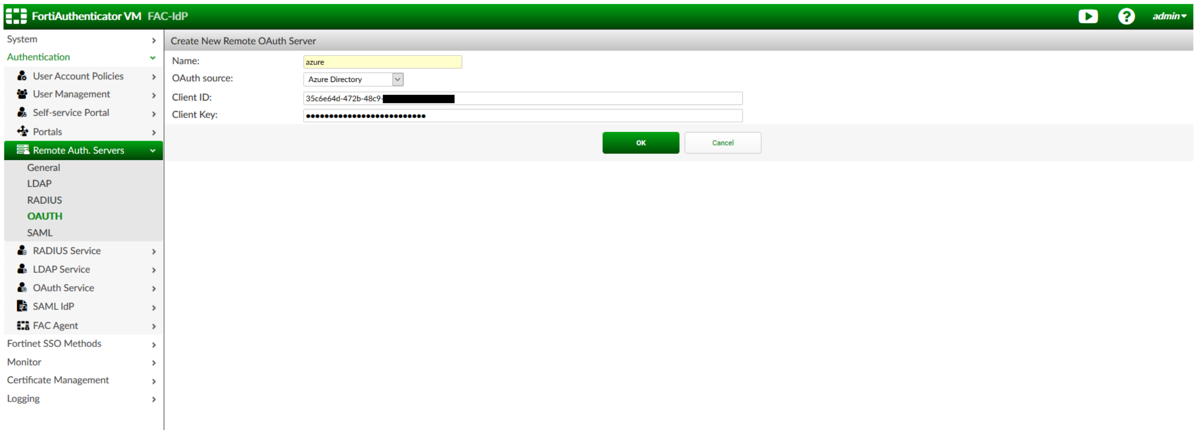
1. Configuring OAuth settings on page 174
2. Configuring the remote SAML server on page 175
3. Creating a remote SAML user synchronization rule on page 175
4. Configuring an Azure realm on page 176
5. Configuring SAML IdP settings on page 176
6. Configuring SP settings on FortiAuthenticator on page 177
7. Configuring the login page replacement message on page 178
8. Results on page 179

Configuring OAuth settings

A remote OAuth server is configured to import SAML users and assign an OTP method through a sync rule import. See Configuring the remote SAML server on page 175 and Creating a remote SAML user synchronization rule on page 175.

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]

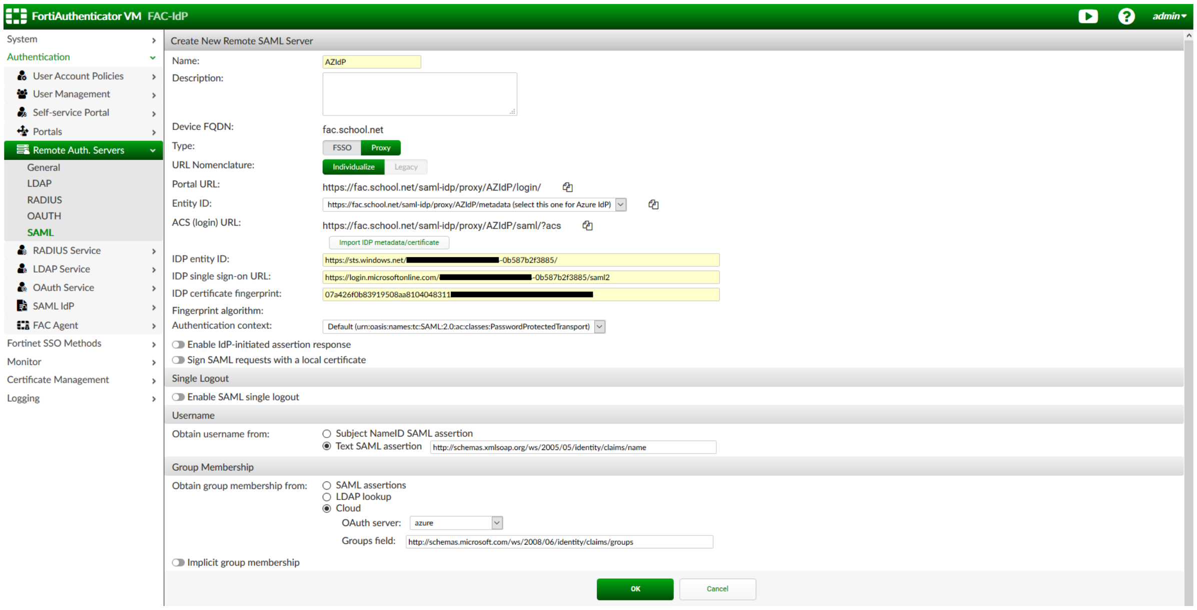
Client Key: ••••••••••••••••••••••••••

4. Click *OK* to save 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. See Configuring OAuth settings on page 174.
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

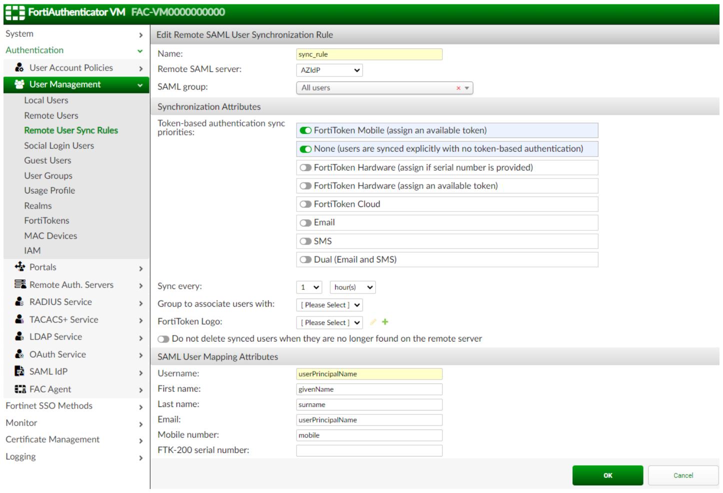
6. Click *OK* to save changes.

Creating a remote SAML user synchronization rule

To create a SAML synchronization rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rules*.
2. In the *Remote User Sync Rules* tab, select *SAML*, and then select *Create New*.
   The *Create New Remote SAML User Synchronization Rule* window opens.
3. Enter a name for the synchronization rule.

4. In *Remote SAML server*, select the remote SAML server created in Configuring the remote SAML server on page 175.
5. In *SAML group*, select *All users*.
6. In *Token-based authentication sync priorities*, set the priority by enabling and dragging *FortiToken Mobile (assign an available token)* to the top and enabling *None (users are synced explicitly with no token-based authentication)*.



Edit Remote SAML User Synchronization Rule

Name: sync_rule

Remote SAML server: AZIdP

SAML group: All users

Synchronization Attributes

Token-based authentication sync priorities:

- ● FortiToken Mobile (assign an available token)
- ● 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 Cloud
- ○ Email
- ○ SMS
- ○ Dual (Email and SMS)

Sync every: 1 hour(s)

Group to associate users with: [Please Select]

FortiToken Logo: [Please Select]

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

SAML User Mapping Attributes

Username: userPrincipalName

First name: givenName

Last name: surname

Email: userPrincipalName

Mobile number: mobile

FTK-200 serial number:

7. Click *OK* to create the new SAML synchronization rule.

Configuring an Azure realm

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

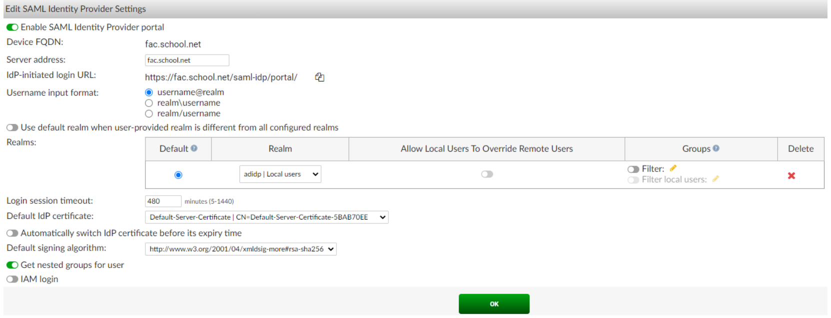
1. Go to *Authentication > User Management > Realms*
2. Click *Create New*.
3. Add the details of the Azure realm, and click *OK*.

Configuring SAML IdP settings

To configure general settings:

1. Go to *Authentication > SAML IdP > General.*
2. Enable *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

○ Use default realm when user-provided realm is different from all configured realms

Realms:

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

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE

○ Automatically switch IdP certificate before its expiry time

Default signing algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

● Get nested groups for user

○ IAM login

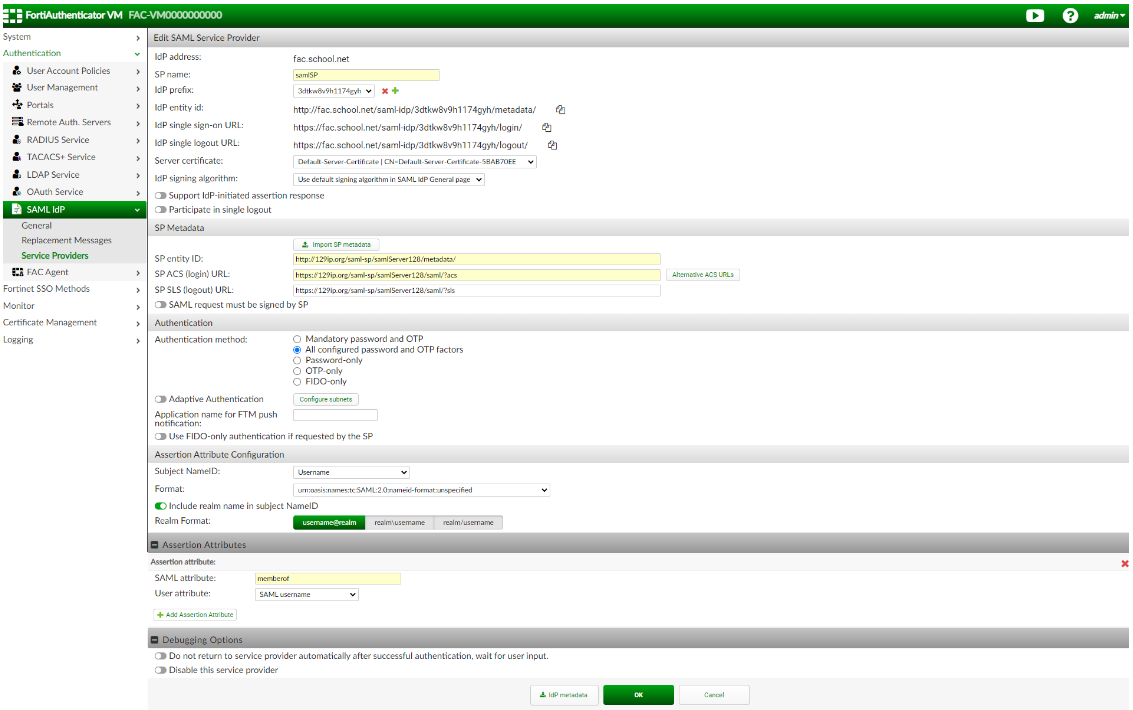
3. Click *OK* to save changes.

Configuring SP settings on FortiAuthenticator

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.
2. Enter the following information:
   a. **SP name**: Enter a name for the SP device.
   b. **IdP prefix**: Select +, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
   c. **Server certificate**: Select the same certificate as the default IdP certificate used in *Authentication > SAML IdP > General*. See Configuring SAML IdP settings on page 176.
3. Click *Save*.
4. In the *SP Metadata* pane, enter the SP information from the client you will be using as the SAML service provider.
5. 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).
6. Click *OK*.
7. Select and click *Edit* to edit the recently created SP.
8. In *Assertion Attribute Configuration*:
   a. Select *Username* from the *Subject NameID* dropdown.
   b. Select *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified* in *Format*.

9. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. Enter a *SAML Attribute* name that your SAML SP is expecting to identify the user.
   b. Select a *User Attribute* for this selection. If you are unsure of which attribute to pick, select *SAML username*.



Edit SAML Service Provider

IdP address: fac.school.net
SP name: samlSP
IdP prefix: 3dtkw8v9h1174gyh
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/
Server certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE
IdP signing algorithm: Use default signing algorithm in SAML IdP General page
Support IdP-initiated assertion response
Participate in single logout

SP Metadata

Import SP metadata
SP entity ID: http://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
SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory password and OTP
● All configured password and OTP factors
○ Password-only
○ OTP-only
○ FIDO-only

Adaptive Authentication
Configure subnets
Application name for FTM push notification:
Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

Subject NameID: Username
Format: urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified
Include realm name in subject NameID
Realm Format: [✓ username@realm] realm\username realm/username

Assertion Attributes

Assertion attribute:
SAML attribute: memberof
User attribute: SAML username
Add Assertion Attribute

Debugging Options

Do not return to service provider automatically after successful authentication, wait for user input.
Disable this service provider

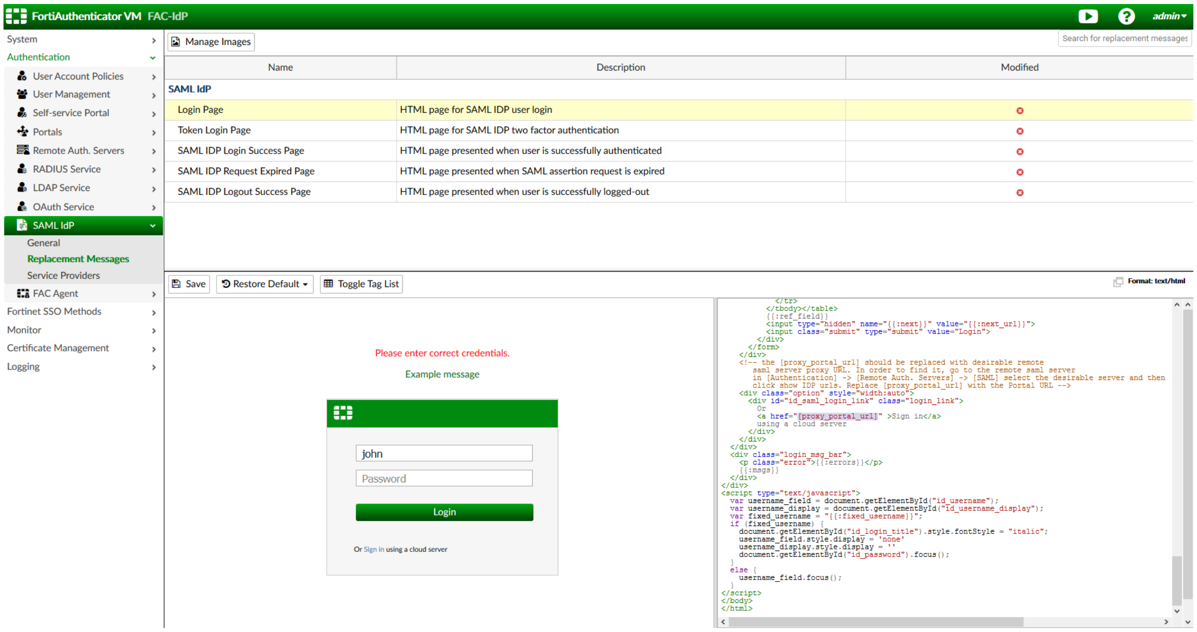
IdP metadata OK Cancel

10. Click *OK* to save 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	⊗

```
          </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 Google Workspace

This recipe describes how to set up FortiAuthenticator as a SAML IdP proxy for Google Workspace to add OTP to the Google Workspace IdP authentication.

To configure FortiAuthenticator as a SAML IdP proxy for Google Workspace:

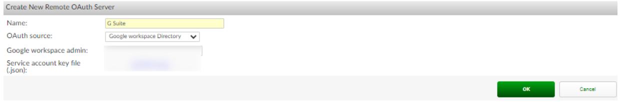
1. Configuring OAuth settings on page 180
2. Configuring the remote SAML server on page 180
3. Creating a remote SAML user synchronization rule on page 181
4. Configuring a Google Workspace Realm on page 182
5. Configuring IdP settings on page 182
6. Configuring SP settings on FortiAuthenticator on page 183
7. Configuring the login page replacement message on page 184
8. Results on page 184

Configuring OAuth settings

A remote OAuth server is configured to import SAML users and assign an OTP method through a sync rule import. See Configuring the remote SAML server on page 180 and Creating a remote SAML user synchronization rule on page 181.

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 *Google Workspace Directory* as the OAuth source.
3. Enter the *Google workspace admin*, and upload the *Service account key file* from the SAML application on your Google Workspace account.
4. Click *OK* to save your changes.



Create New Remote OAuth Server

Name: G Suite

OAuth source: Google workspace Directory

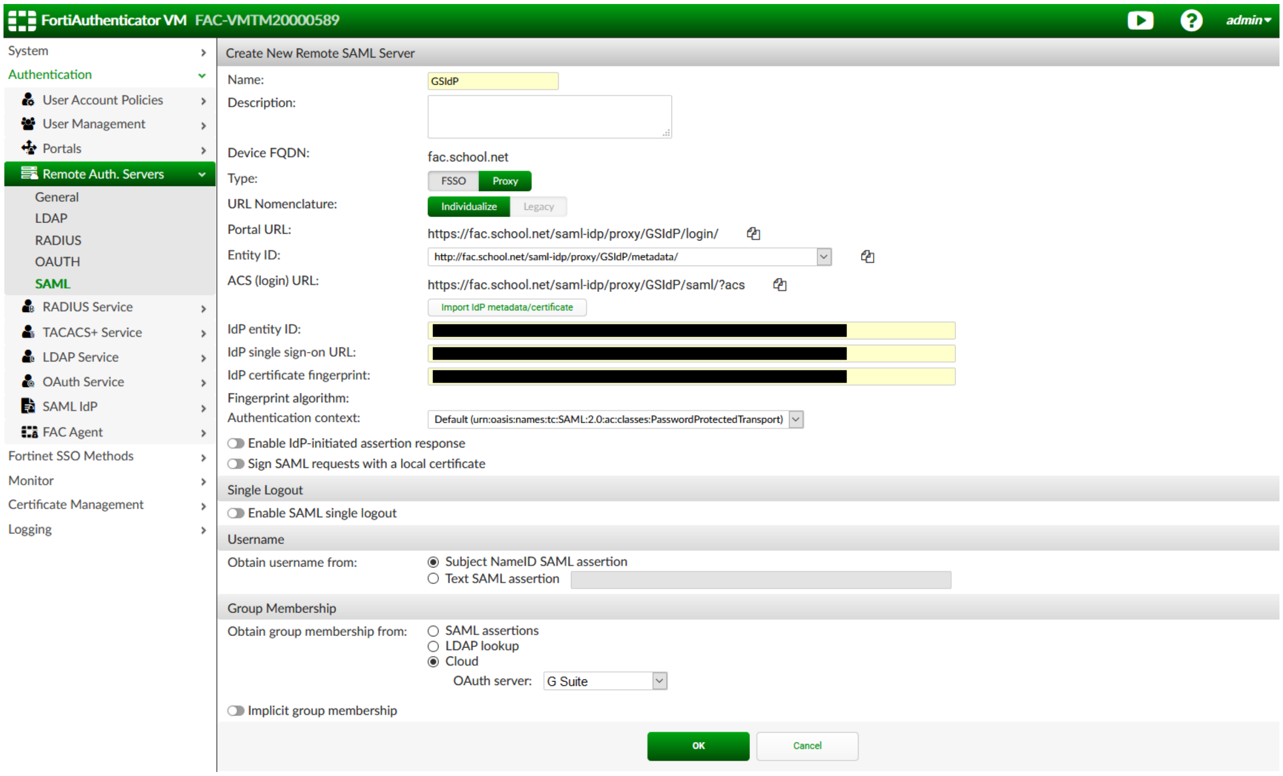
Google workspace admin:

Service account key file (.json):

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 Google Workspace. For example, if the name in Google Workspace is set as GSIdP, the SAML server should also use GSIdP (case sensitive).
2. Import the IdP metadata obtained from the SAML app on Google Workspace.
3. In *Username*, select *Subject NameID SAML assertion*.
4. In *Group Membership*, select *Cloud* and choose the previously created Google Workspace OAuth server. See Configuring OAuth settings on page 180.
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: 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

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

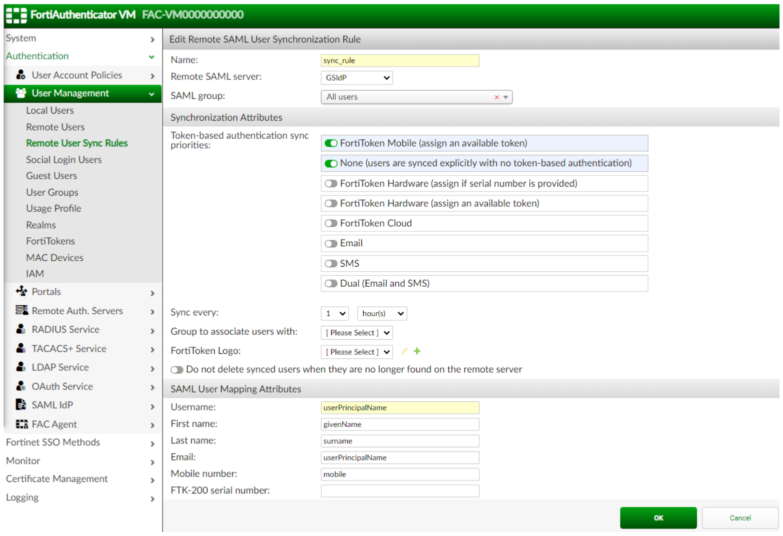
○ Implicit group membership

6. Click *OK* to save your changes.

Creating a remote SAML user synchronization rule

To create a SAML synchronization rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rules*.
2. In the *Remote User Sync Rules* tab, select *SAML*, and then select *Create New*.
   The *Create New Remote SAML User Synchronization Rule* window opens.
3. Enter a name for the synchronization rule.
4. In *Remote SAML server*, select the remote SAML server created in Configuring the remote SAML server on page 180.
5. In *SAML group*, select *All users*.
6. In *Token-based authentication sync priorities*, set the priority by enabling and dragging *FortiToken Mobile (assign an available token)* to the top and enabling *None (users are synced explicitly with no token-based authentication)*.



Edit Remote SAML User Synchronization Rule

Name: sync_rule

Remote SAML server: GSIdP

SAML group: All users

Synchronization Attributes

Token-based authentication sync priorities:

- ● FortiToken Mobile (assign an available token)
- ● 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 Cloud
- ○ Email
- ○ SMS
- ○ Dual (Email and SMS)

Sync every: 1 hour(s)

Group to associate users with: [Please Select]

FortiToken Logo: [Please Select]

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

SAML User Mapping Attributes

Username: userPrincipalName

First name: givenName

Last name: surname

Email: userPrincipalName

Mobile number: mobile

FTK-200 serial number:

7. Click *OK* to create the new SAML synchronization rule.

Configuring a Google Workspace Realm

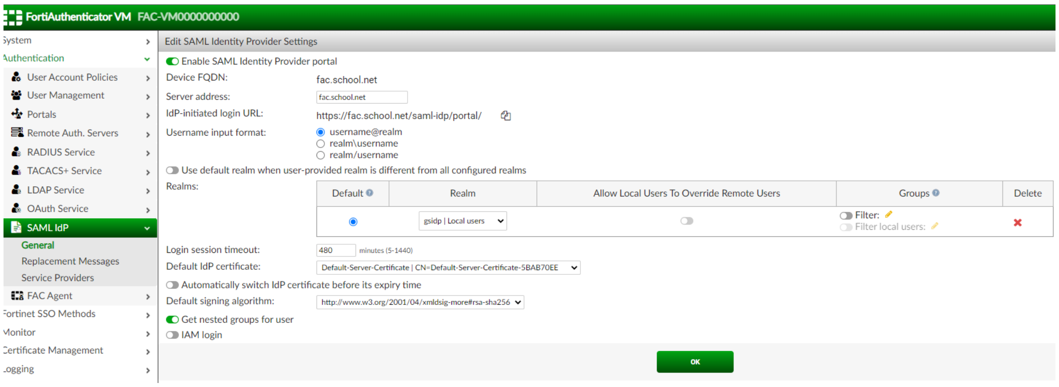
To create a Google Workspace Realm and add it to the IdP:

1. Go to *Authentication* > *User Management* > *Realms.*
2. Click *Create New*.
3. Add the details of the Google Workspace 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 Google Workspace.
   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

○ Use default realm when user-provided realm is different from all configured realms

Realms:

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

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE

○ Automatically switch IdP certificate before its expiry time

Default signing algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

● Get nested groups for user

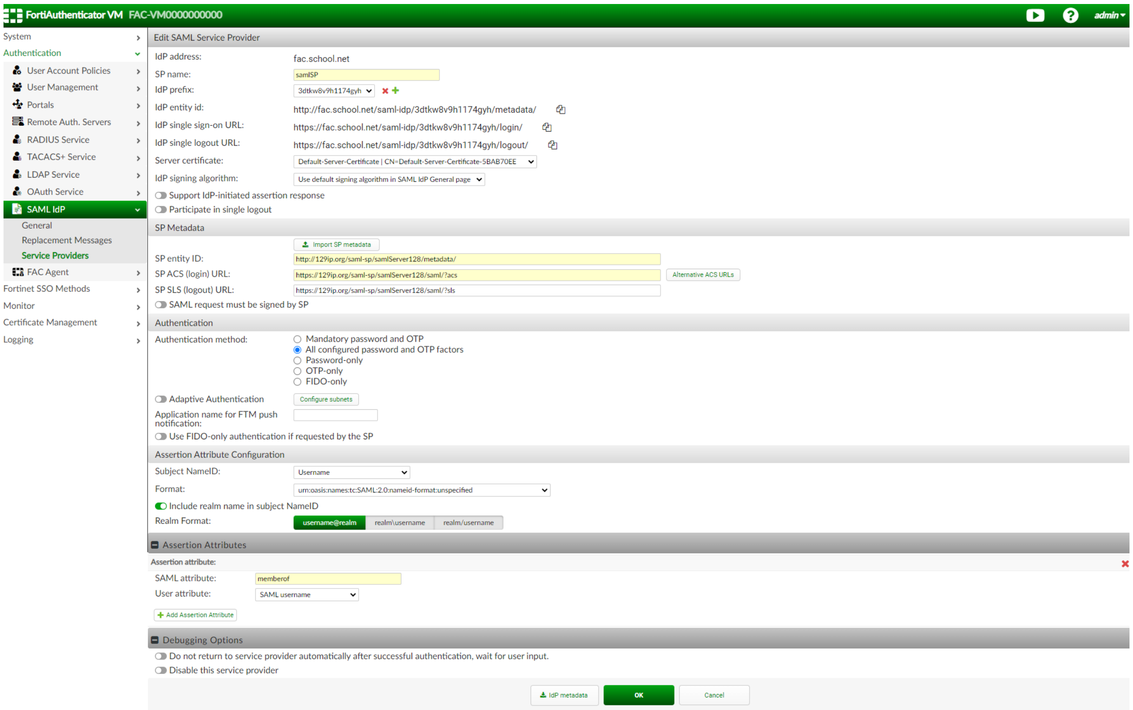
○ IAM login

3. Click *OK* to save your changes.

Configuring SP settings on FortiAuthenticator

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.
2. Enter the following information:
   a. **SP name**: Enter a name for the SP device.
   b. **IdP prefix**: Select +, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
   c. **Server certificate**: Select the same certificate as the default IdP certificate used in *Authentication* > *SAML IdP* > *General*. See Configuring IdP settings on page 182.
3. Click *Save*.
4. In the *SP Metadata* pane, enter the SP information from the client you will be using as the SAML service provider.
5. 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).
6. Click *OK*.
7. Select and click *Edit* to edit the recently created SP.
8. In *Assertion Attribute Configuration*:
   a. Select *Username* from the *Subject NameID* dropdown.
   b. Select *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified* in *Format*.
9. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. Enter a *SAML Attribute* name that your SAML SP is expecting to identify the user.
   b. Select a *User Attribute* for this selection. If you are unsure of which attribute to pick, select *SAML username*.



Edit SAML Service Provider

IdP address: fac.school.net
SP name: samlSP
IdP prefix: 3dtkw8v9h1174gyh
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/
Server certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE
IdP signing algorithm: Use default signing algorithm in SAML IdP General page
Support IdP-initiated assertion response
Participate in single logout

SP Metadata

SP entity ID: http://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
SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory password and OTP
● All configured password and OTP factors
○ Password-only
○ OTP-only
○ FIDO-only

Adaptive Authentication
Application name for FTM push notification:
Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

Subject NameID: Username
Format: urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified
Include realm name in subject NameID
Realm Format: username@realm | realm\username | realm/username

Assertion Attributes

Assertion attribute:
SAML attribute: memberof
User attribute: SAML username

Debugging Options

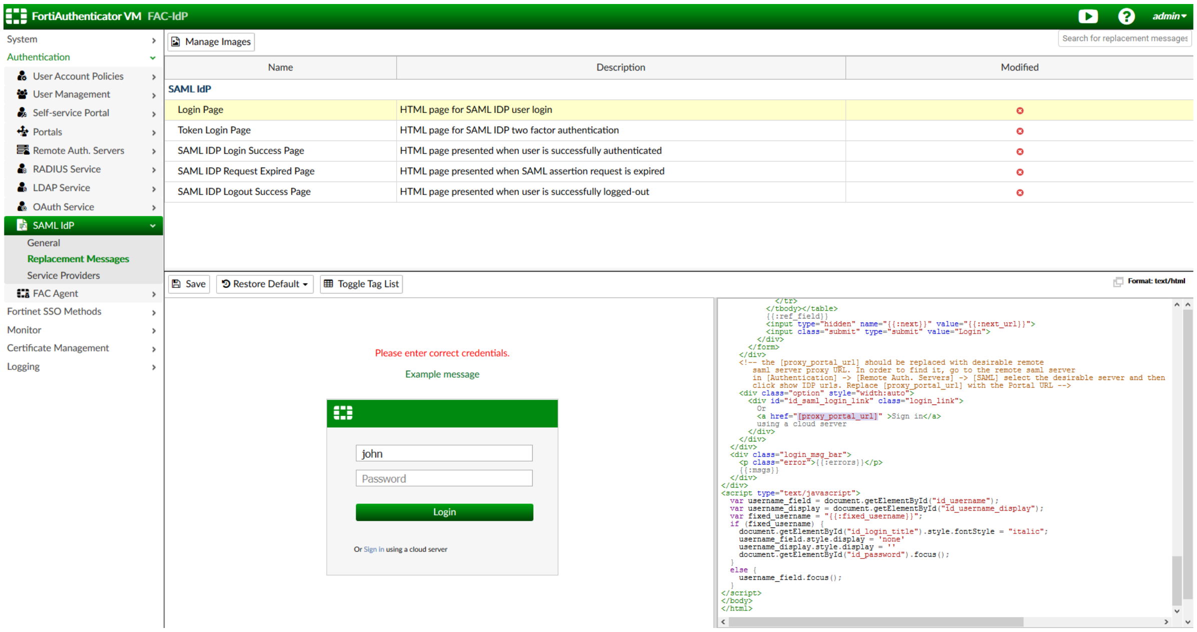
Do not return to service provider automatically after successful authentication, wait for user input.
Disable this service provider

10. Click *OK* to save 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	✖

```
          </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>
```

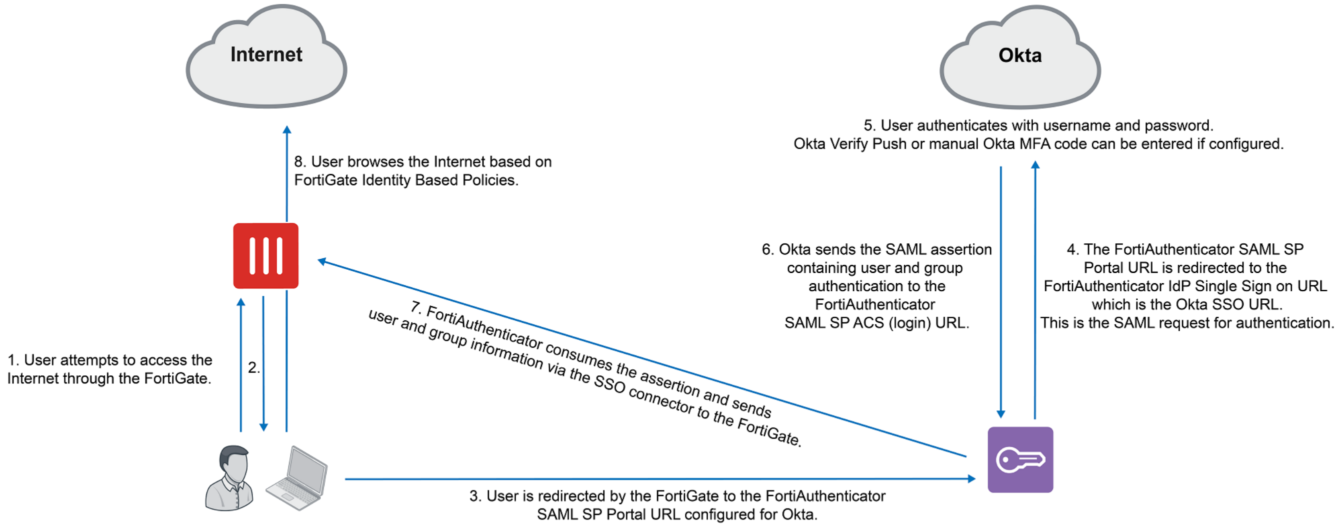
4. Click *Save*.

Results

To test Google Workspace 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
8. User browses the Internet based on FortiGate Identity Based Policies.
5. User authenticates with username and password. Okta Verify Push or manual Okta MFA code can be entered if configured.
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, Google Workspace, 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.

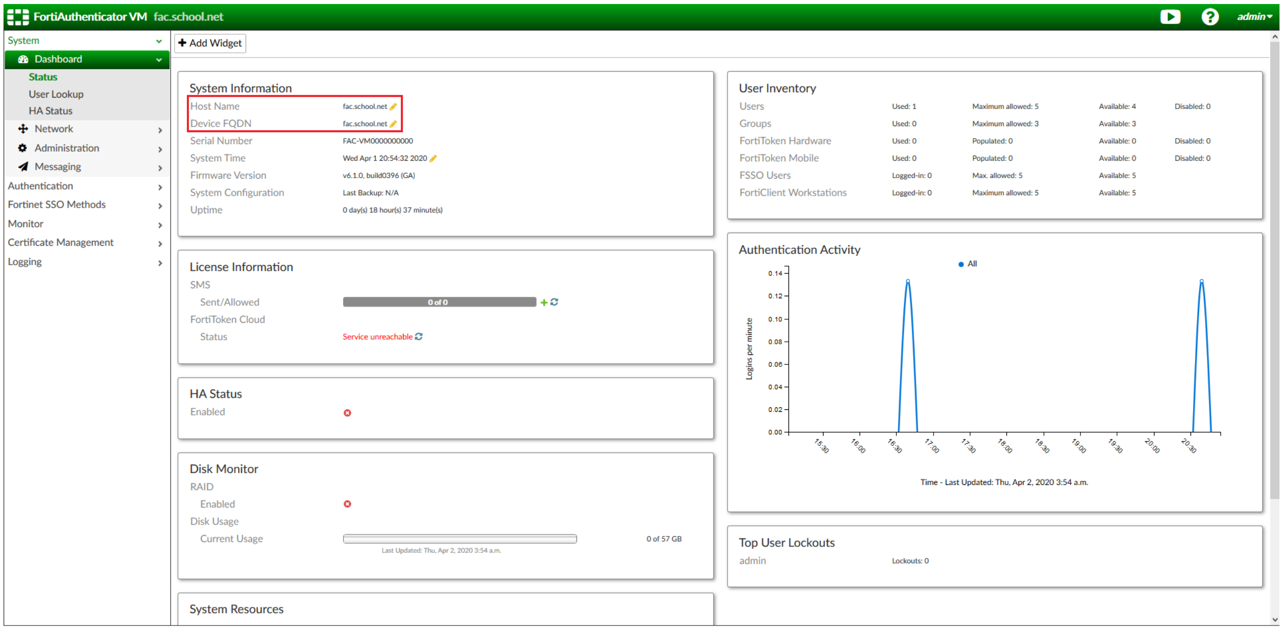
In this example configuration, the FortiGate has a DMZ IP address of `192.168.50.1`, and the FortiAuthenticator has the Port1 IP address of `192.168.50.100`. Note that, for testing purposes, the FortiAuthenticator's IP and FQDN have been added to the host's file of trusted host names; this is not necessary 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)

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	

License Information

SMS

Sent/Allowed: 0 of 0

FortiToken Cloud

Status: Service unreachable

HA Status

Enabled: ☒

Disk Monitor

RAID

Enabled: ☒

Disk Usage

Current Usage: 0 of 57 GB

Last Updated: Thu, Apr 2, 2020 3:54 a.m.

Top User Lockouts

admin Lockouts: 0

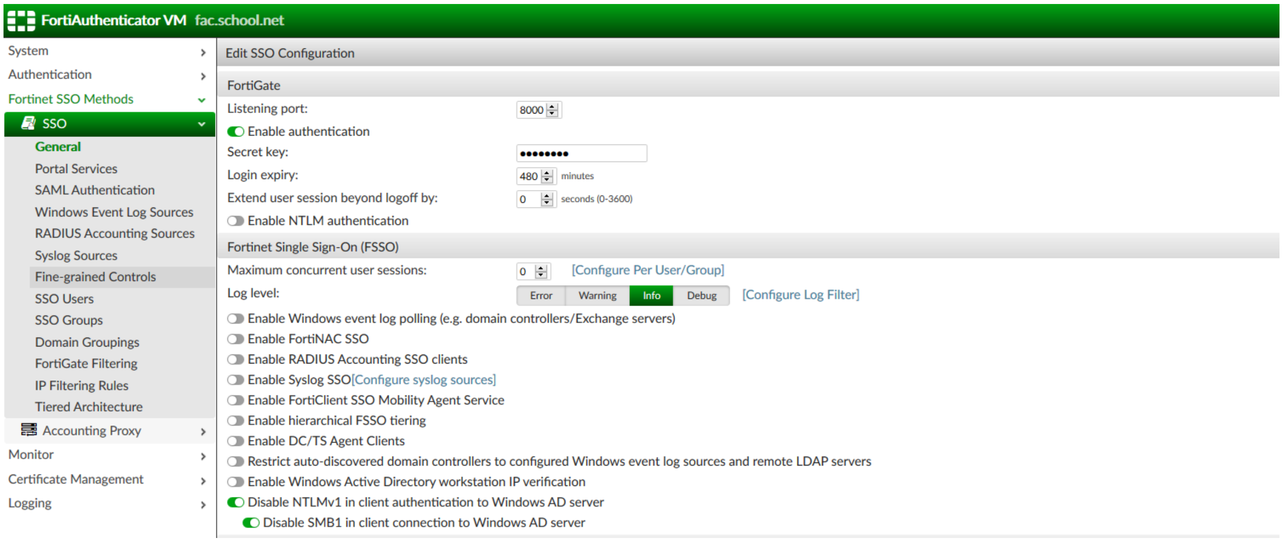
System Resources

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

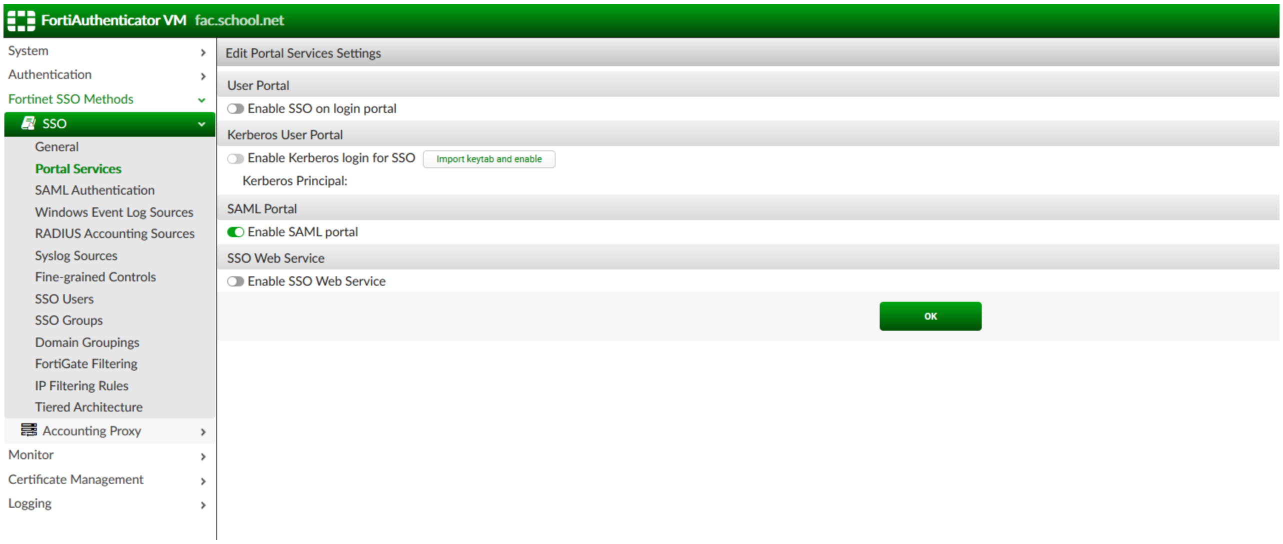
○ Restrict auto-discovered domain controllers to configured Windows event log sources and remote LDAP servers

○ 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 [Import keytab and enable]

Kerberos Principal:

SAML Portal

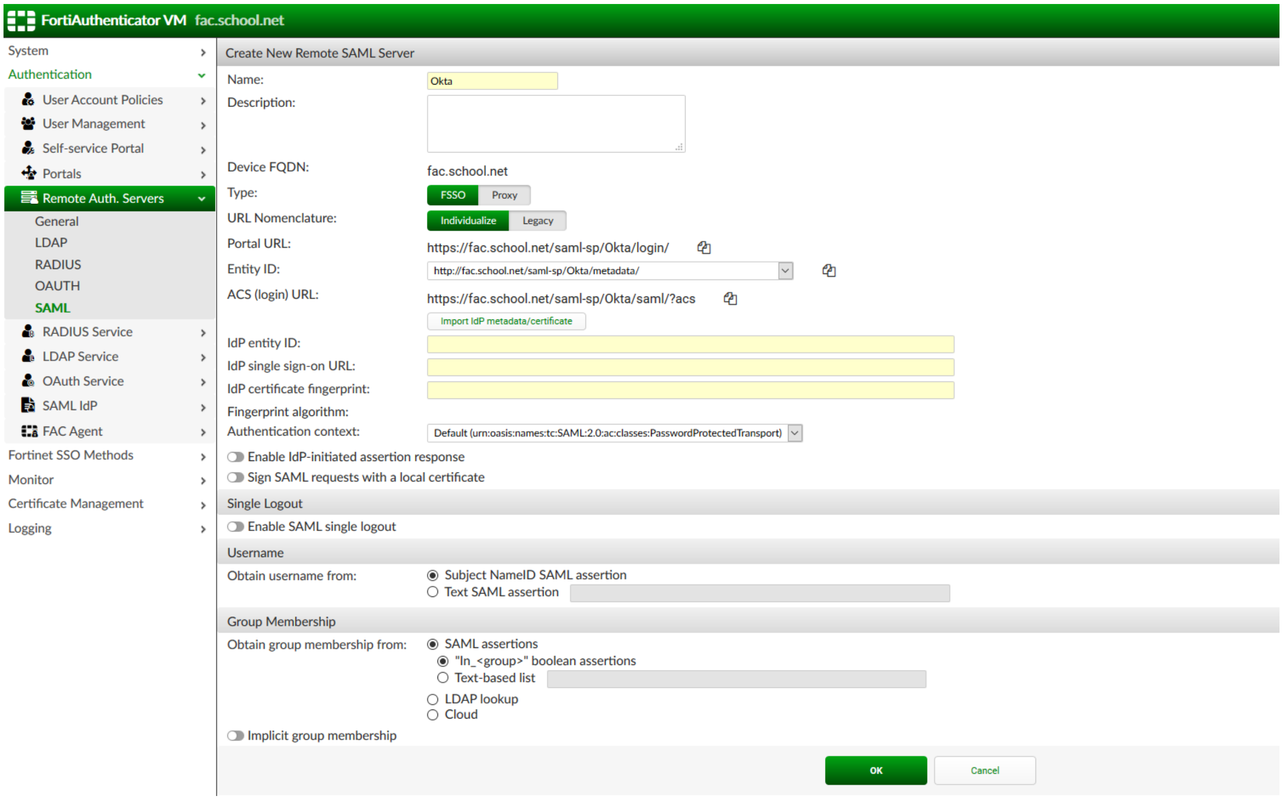
● Enable SAML portal

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

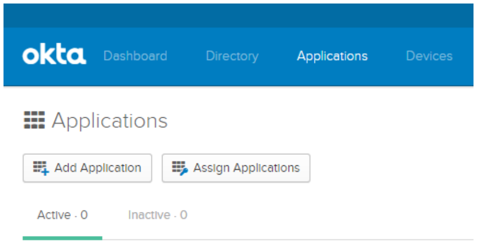
Group Membership

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

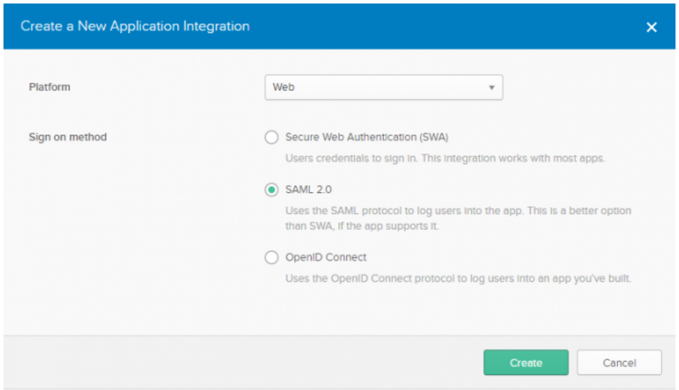
Implicit group membership

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

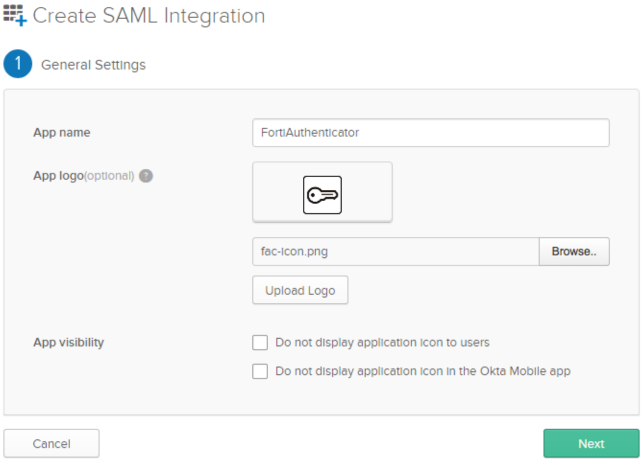
Sign on method

○ 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.



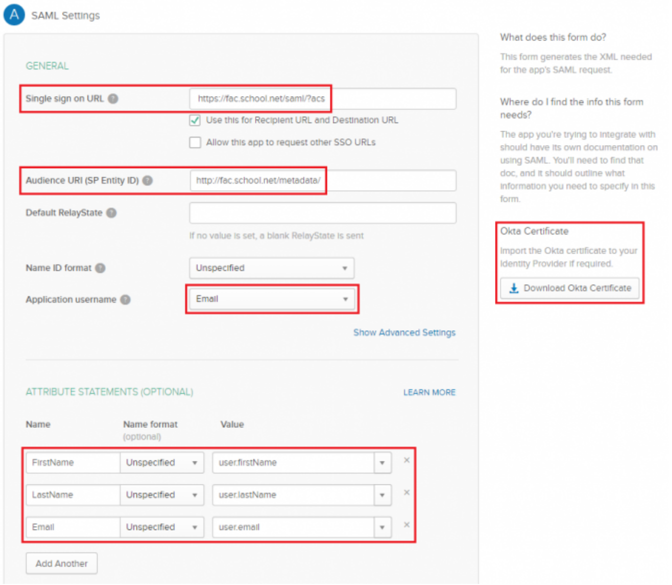
Create SAML Integration

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?

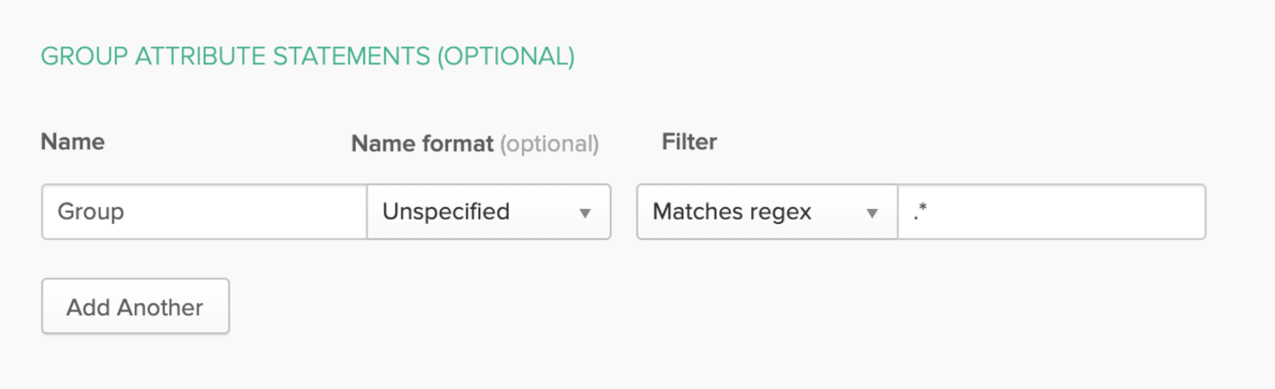
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

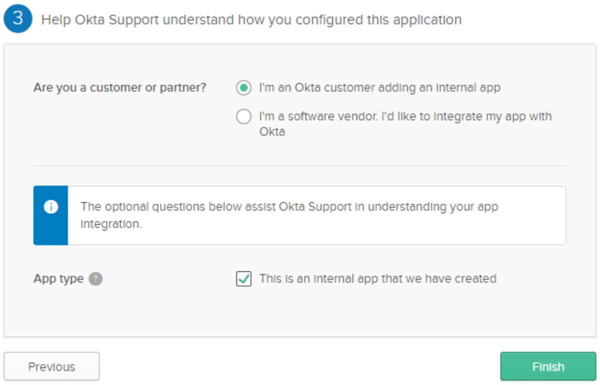
In the section below, configure a *Group* attribute to match on FortiAuthenticator. The word *Group* (case-sensitive) must be entered in *Text-based list* under *Obtain Group Membership from: SAML assertions* inside the remote SAML setup configuration on FortiAuthenticator. Regex matching is the most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



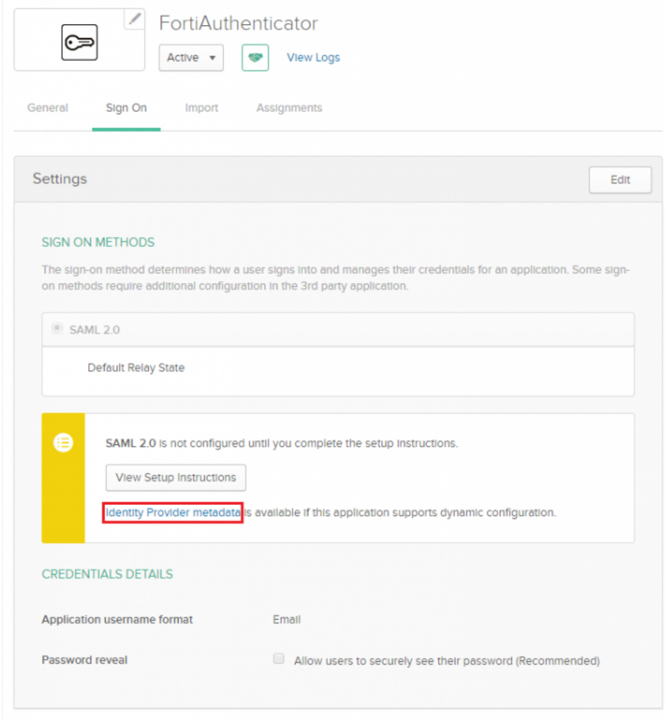
3 Help Okta Support understand how you configured this application

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.

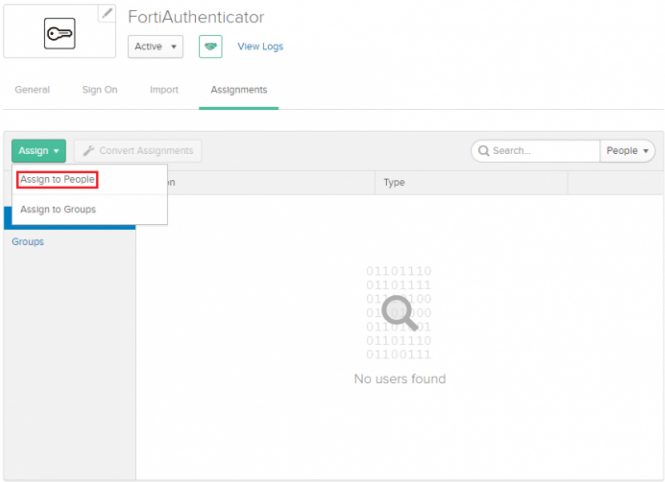
CREDENTIALS DETAILS

Application username format Email

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

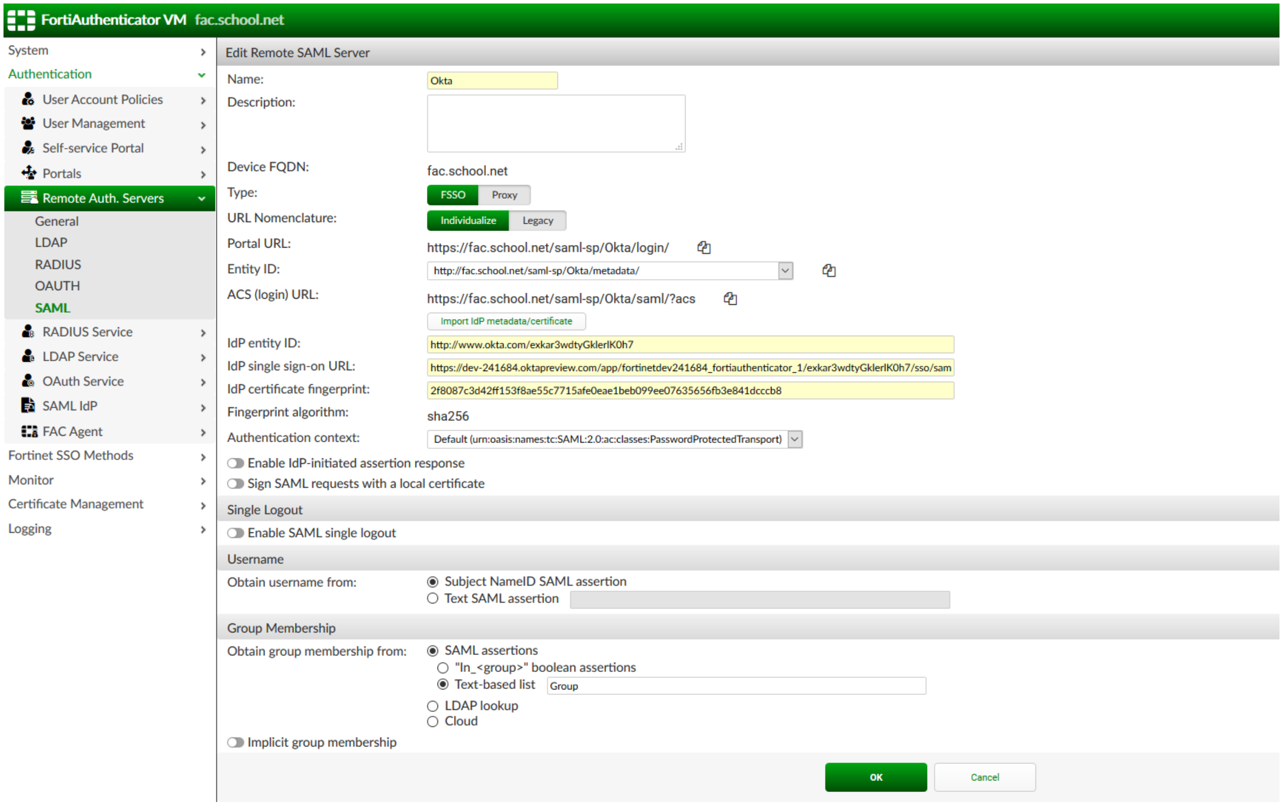
7. Finally, open the *Assignments tab* and select *Assign* > *Assign to people*.
Assign the users you wish to add to the application. This will permit the user to log in to the application's portal. Save

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

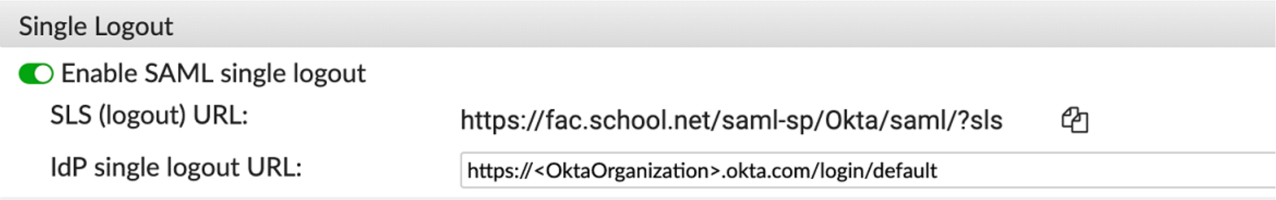
Name: Okta
Description:
Device FQDN: fac.school.net
Type: FSSO | Proxy
URL Nomenclature: Individualize | Legacy
Portal URL: https://fac.school.net/saml-sp/Okta/login/
Entity ID: http://fac.school.net/saml-sp/Okta/metadata/
ACS (login) URL: https://fac.school.net/saml-sp/Okta/saml/?acs
IdP entity ID: http://www.okta.com/exkar3wdtyGklerIK0h7
IdP single sign-on URL: https://dev-241684.oktapreview.com/app/fortinetdev241684_fortiauthenticator_1/exkar3wdtyGklerIK0h7/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

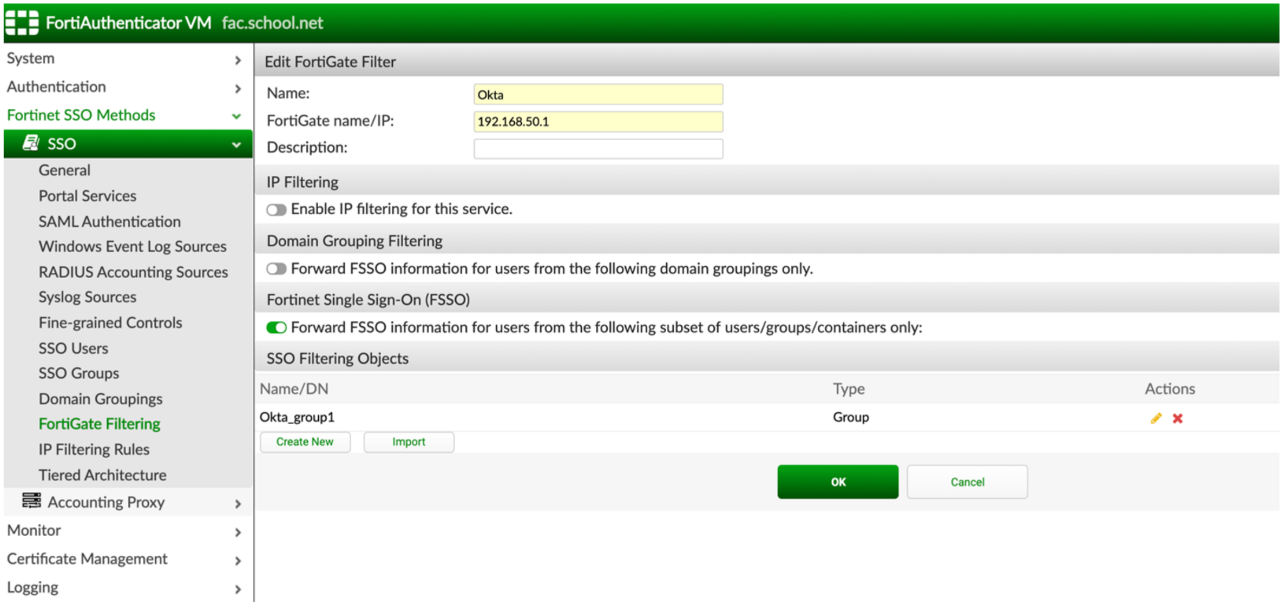
2. Enable SAML single logout and add the *IdP single logout URL* under the *Single Logout* section of the Okta Remote SAML Server.
   For example, if your Okta organization is "facschool" then the *IdP single logout URL*: entry would be `https://facschool.okta.com/login/default`.



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

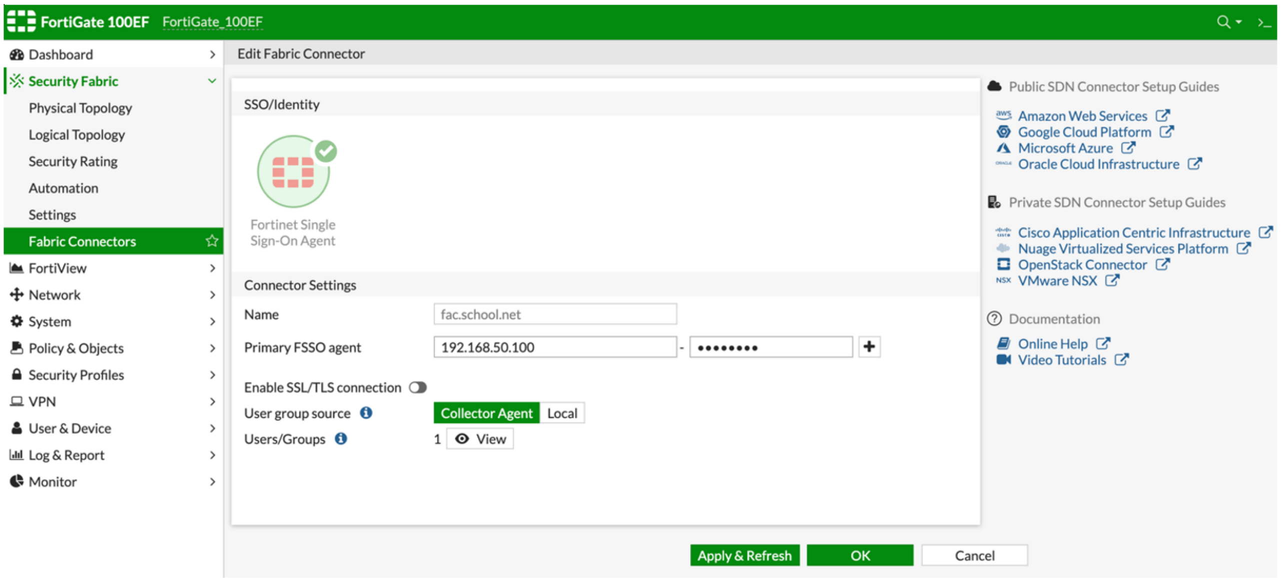
Name/DN	Type	Actions
Okta_group1	Group	

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 - ••••••••

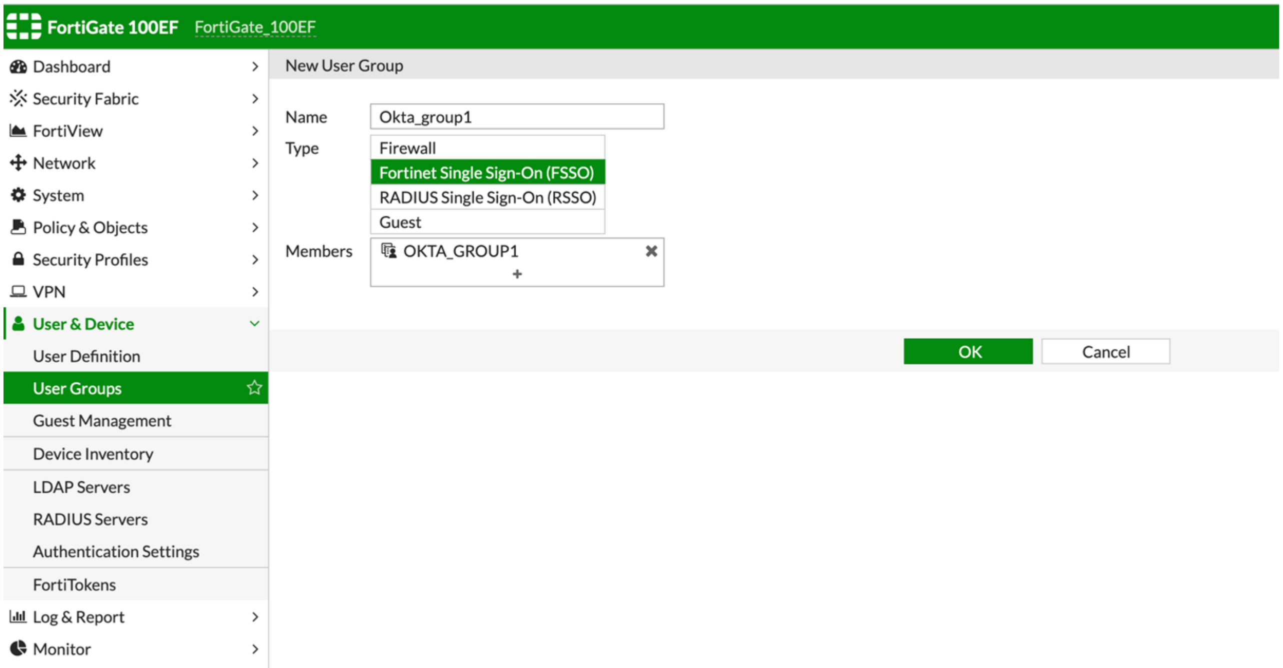
Enable SSL/TLS connection

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.*

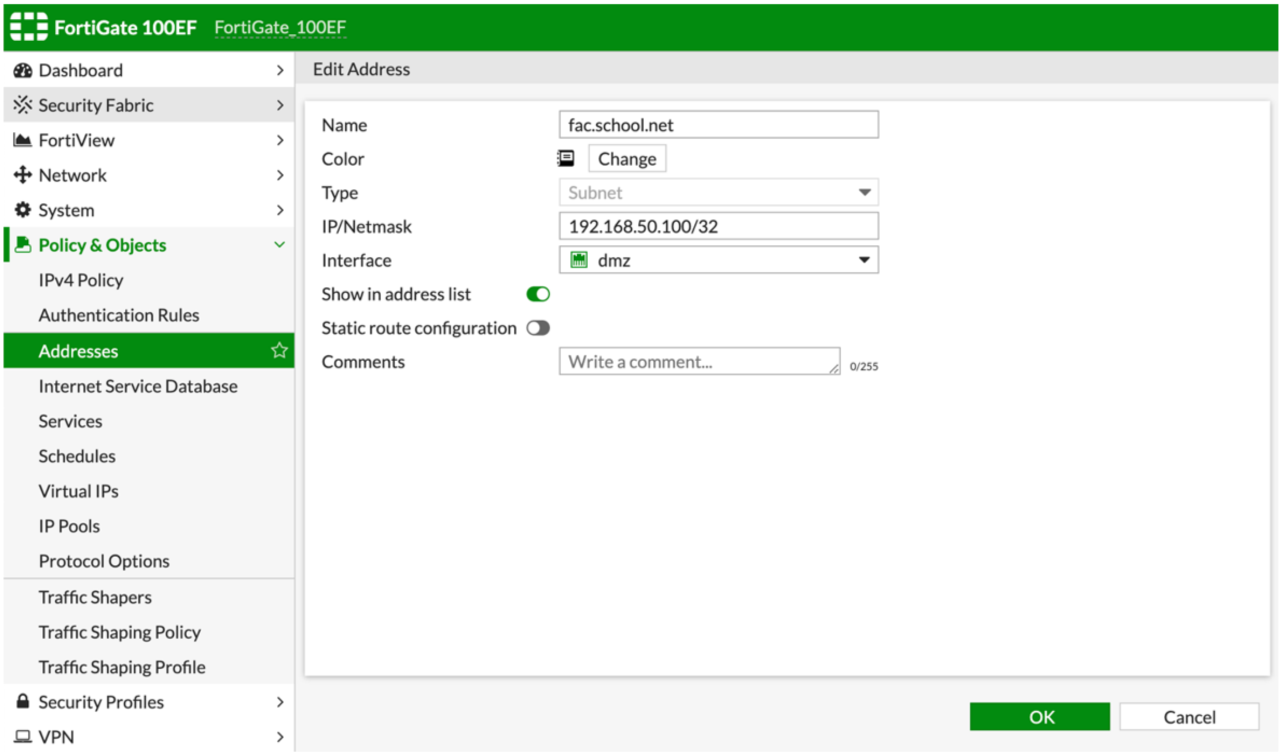
Replace **`<FortiAuthenticator-FQDN>`** with the DNS name of the FortiAuthenticator.

```
<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.

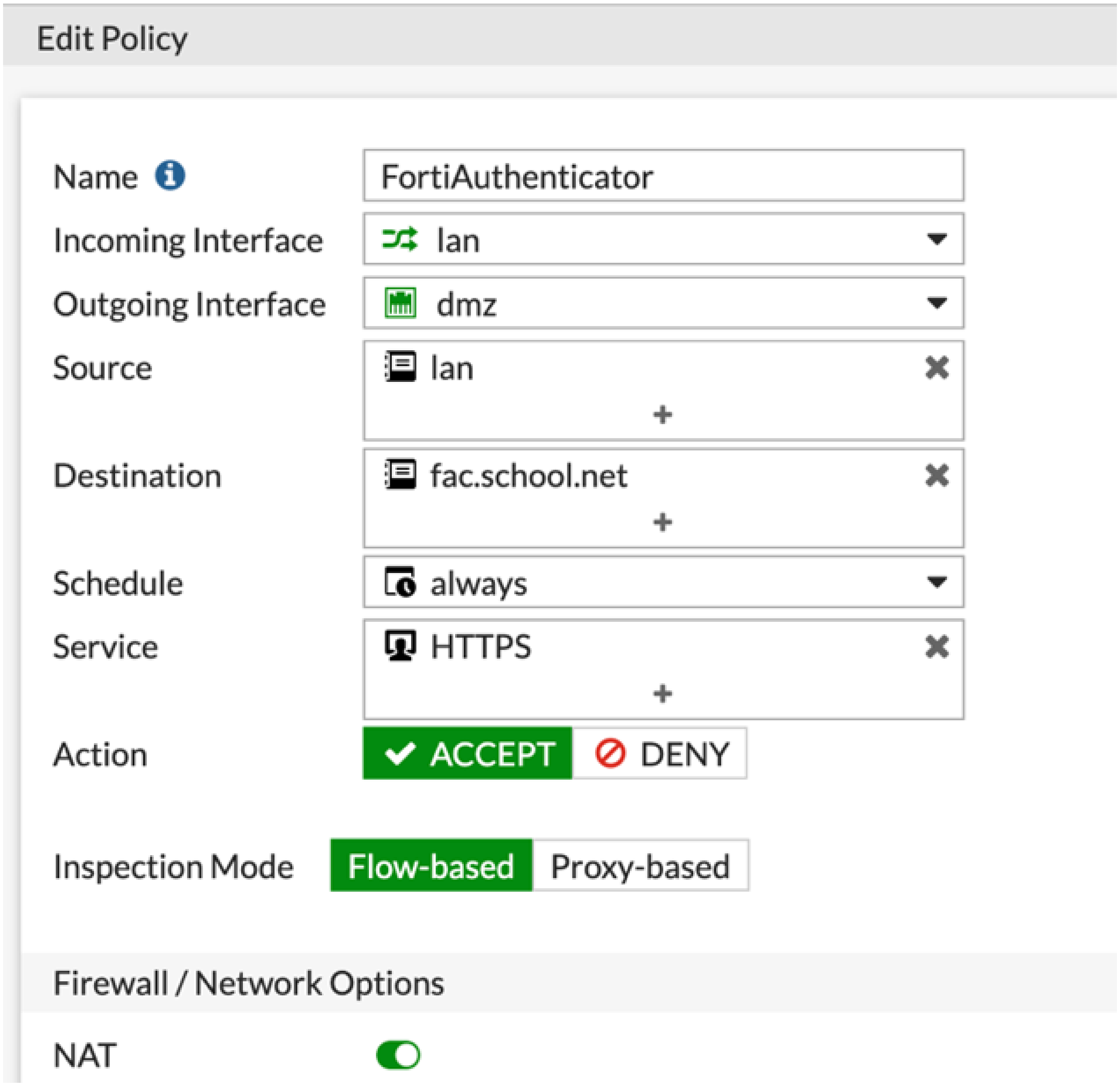


Edit Address

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

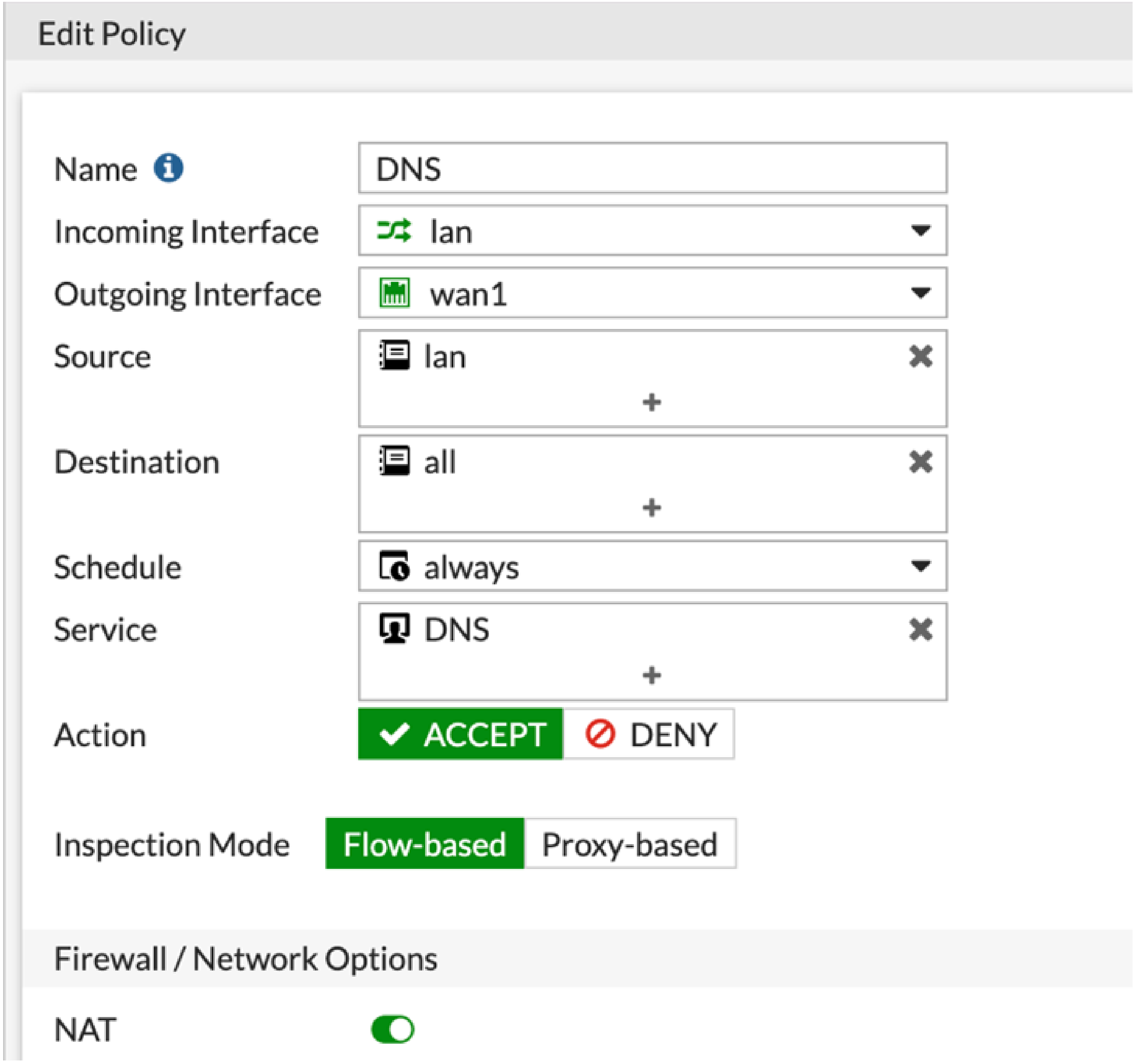
Action: [✓ ACCEPT] DENY

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

Firewall / Network Options

NAT: ●

Add the following three policies in order:

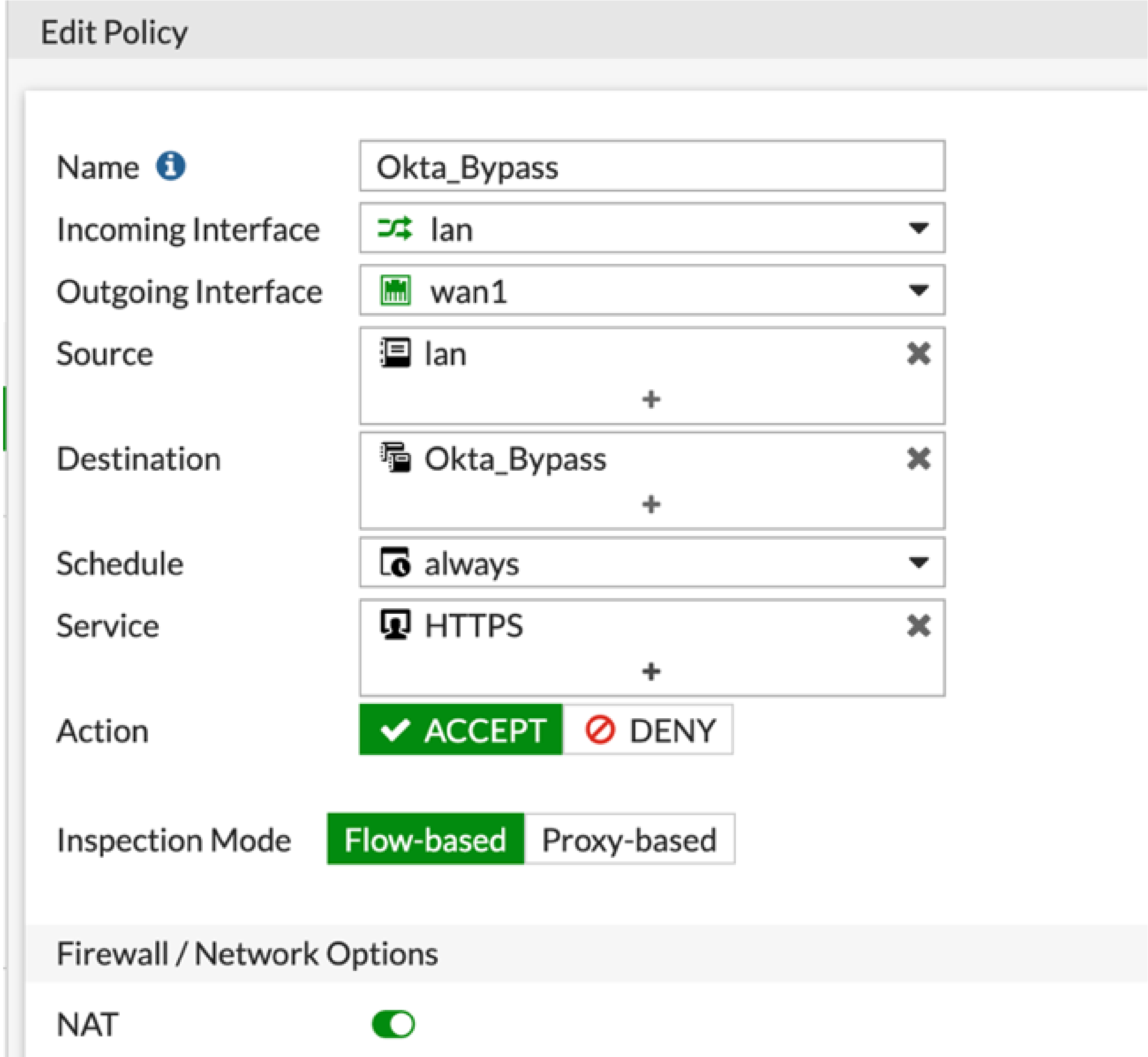


Edit Policy

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

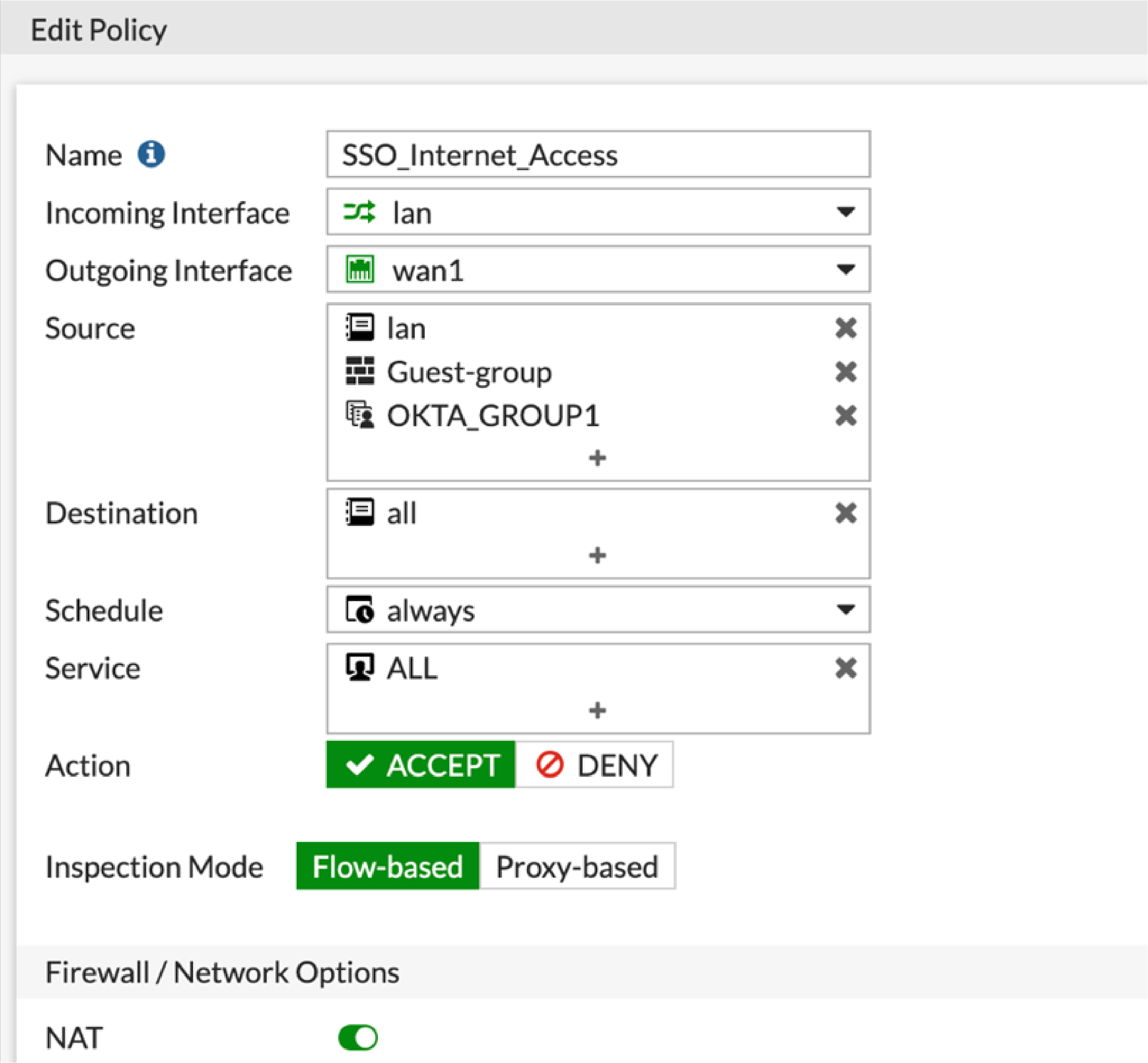
Action: ✓ ACCEPT | DENY

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

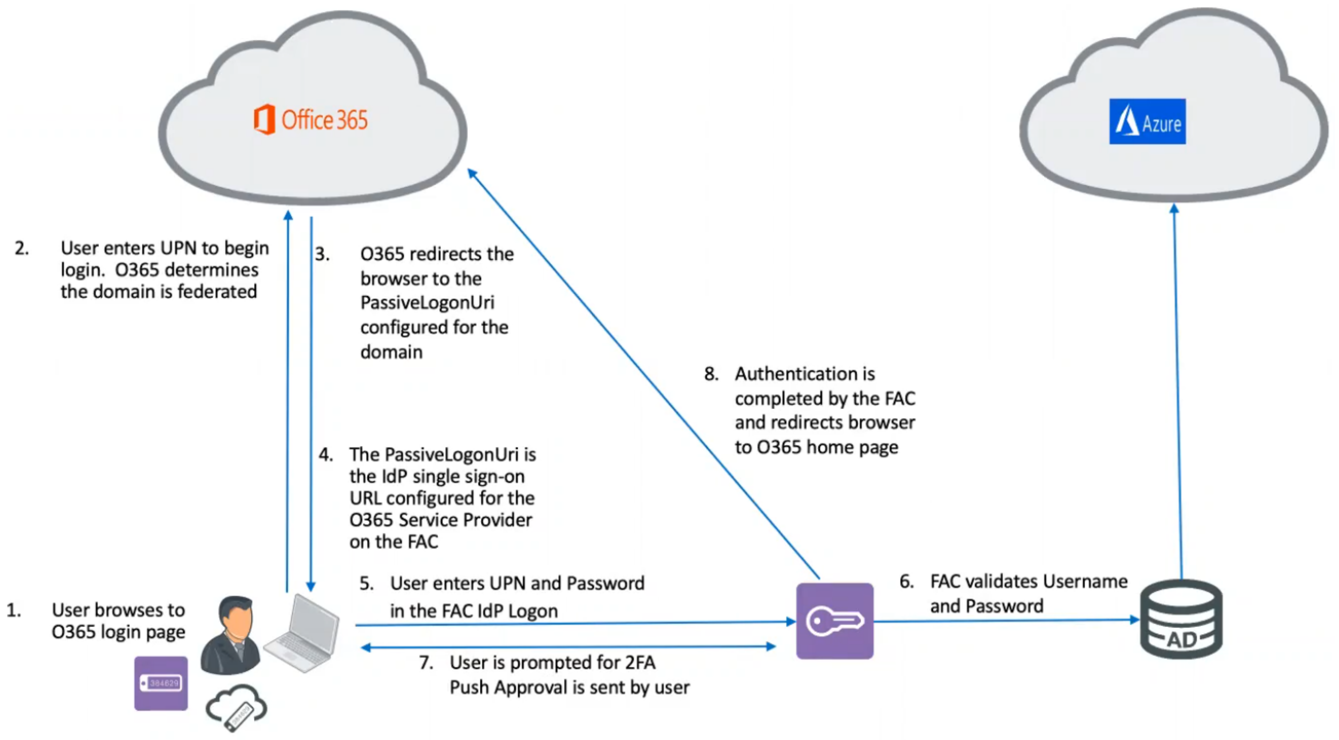
Firewall / Network Options

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 201
2. Configure SAML settings on FortiAuthenticator on page 202
3. Configure two-factor authentication on FortiAuthenticator on page 203
4. Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 204
5. Configure Microsoft Azure AD Connect on page 207

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.

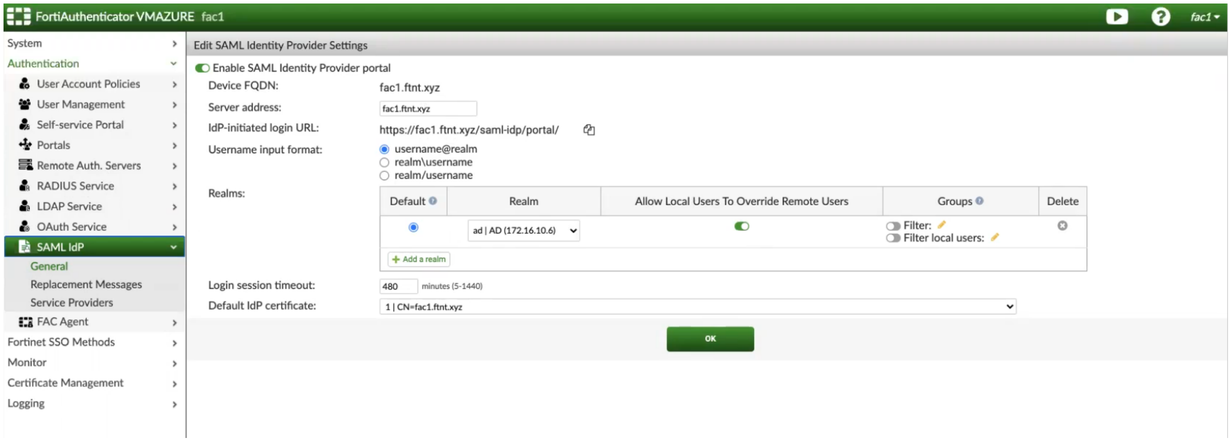
To configure the Active Directory realm:

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)	On	Filter: Filter local users:	⊗

+ Add a realm

Login session timeout: 480 minutes (5-1440)

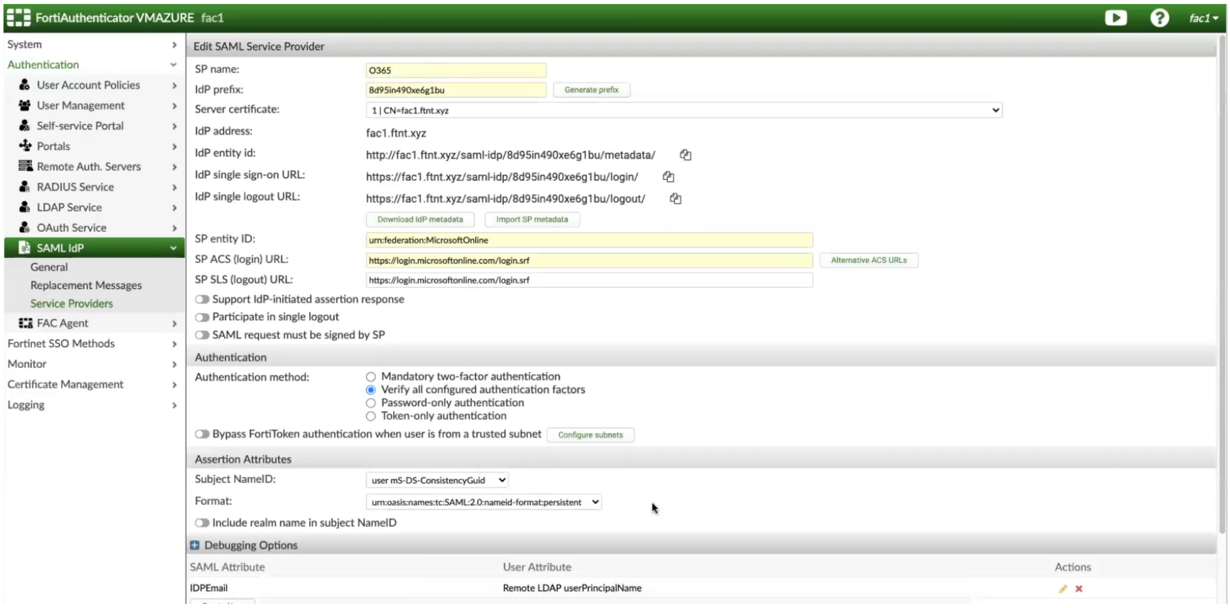
Default IdP certificate: 1 | CN=fac1.ftnt.xyz

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	

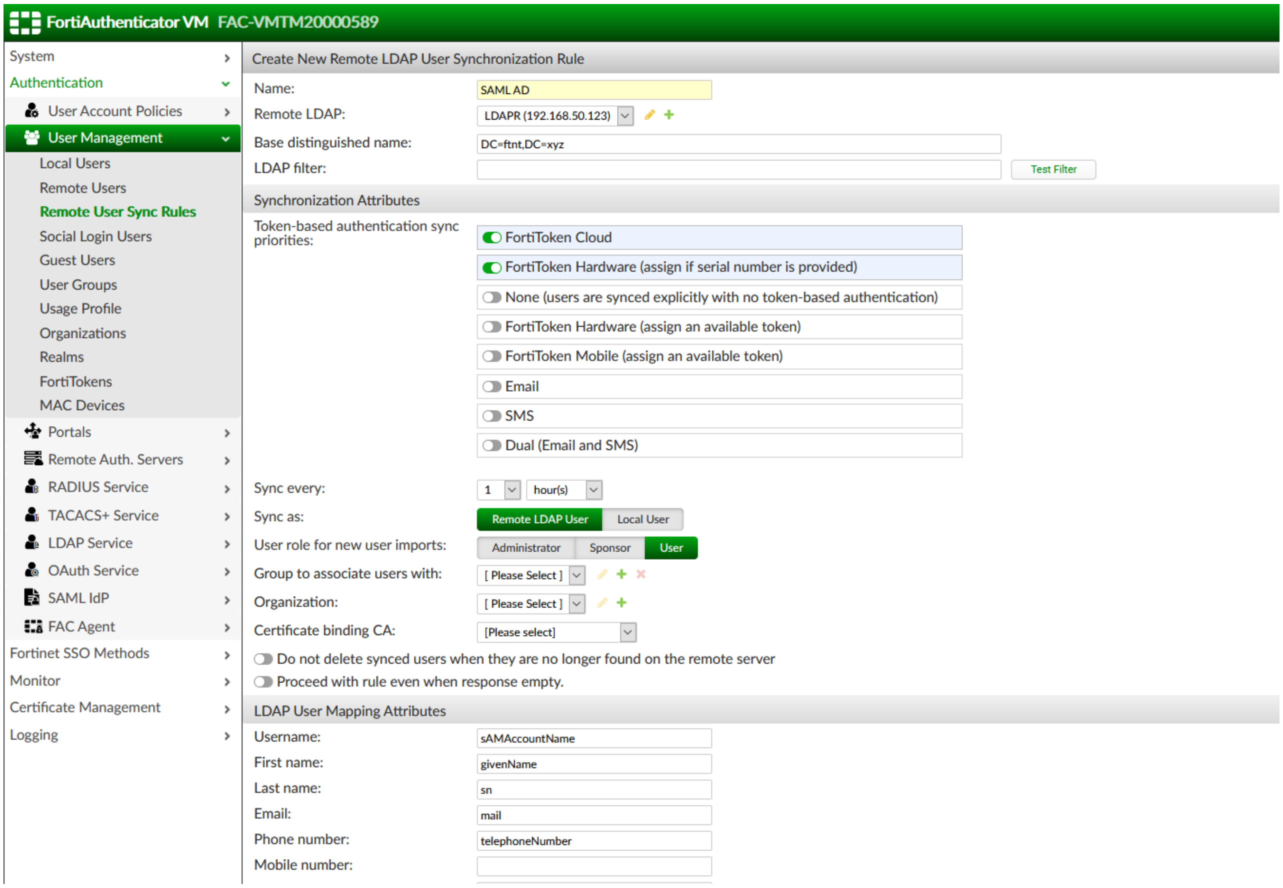
5. Click *OK* to save your changes.

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)*.



Create New Remote LDAP User Synchronization Rule

Name: SAML AD

Remote LDAP: LDAPR (192.168.50.123)

Base distinguished name: DC=ftnt,DC=xyz

LDAP filter:

Synchronization Attributes

Token-based authentication sync priorities:

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

Sync every: 1 hour(s)

Sync as: Remote LDAP User | Local User

User role for new user imports: Administrator | Sponsor | User

Group to associate users with: [Please Select]

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: sAMAccountName

First name: givenName

Last name: sn

Email: mail

Phone number: telephoneNumber

Mobile number:

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

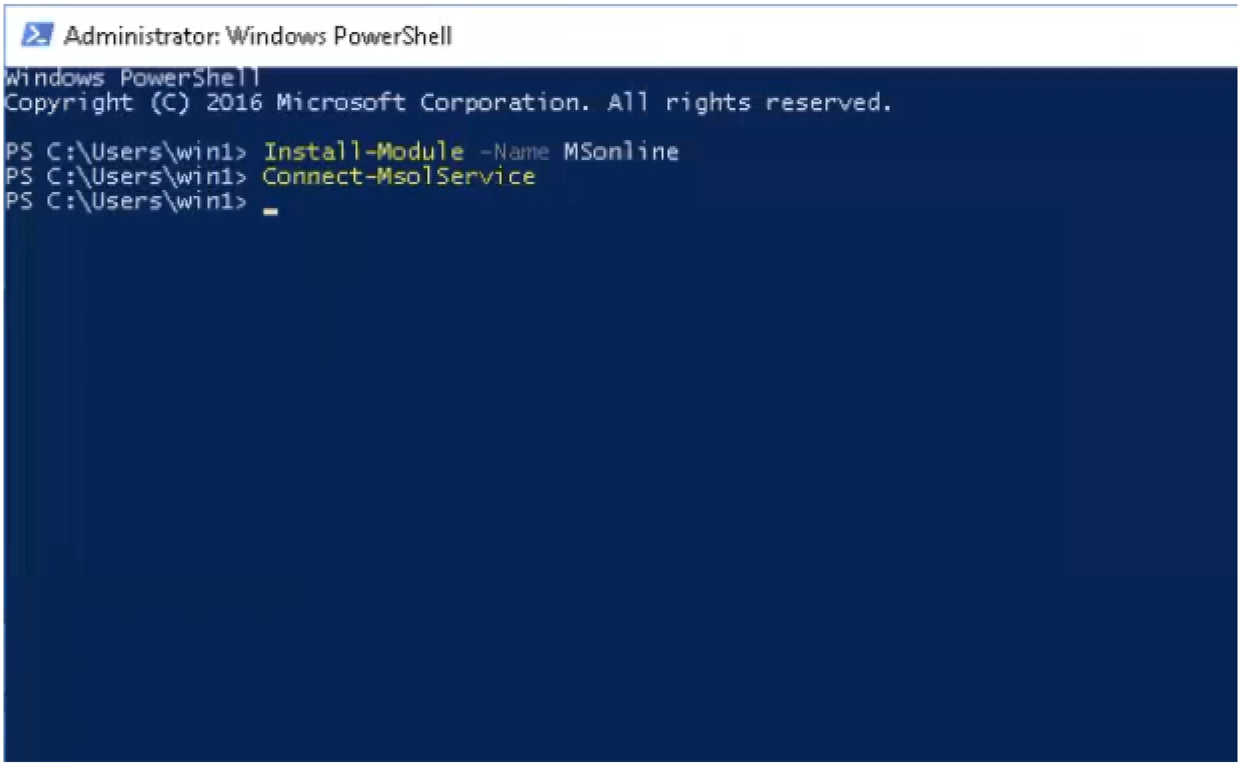
FortiAuthenticator currently supports use with Microsoft Azure Active Directory Module for Windows PowerShell.

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 .`

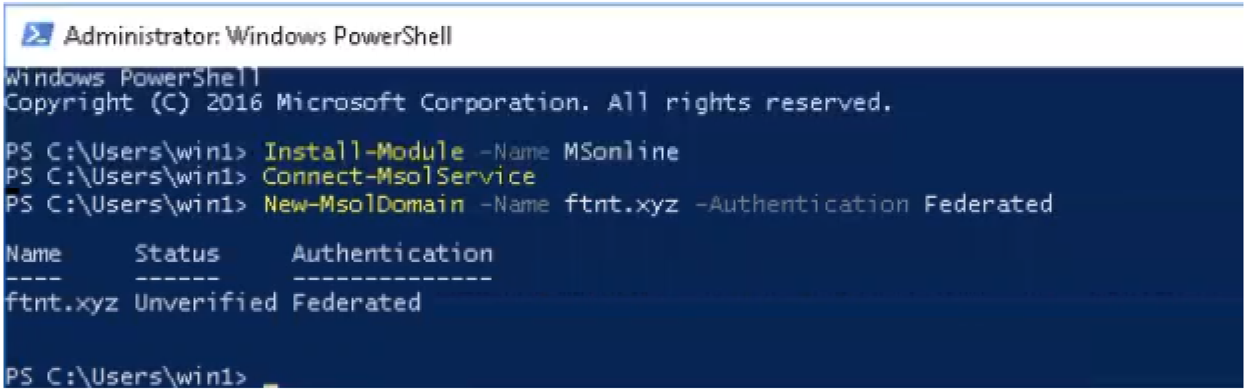


Administrator: Windows PowerShell

```
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.

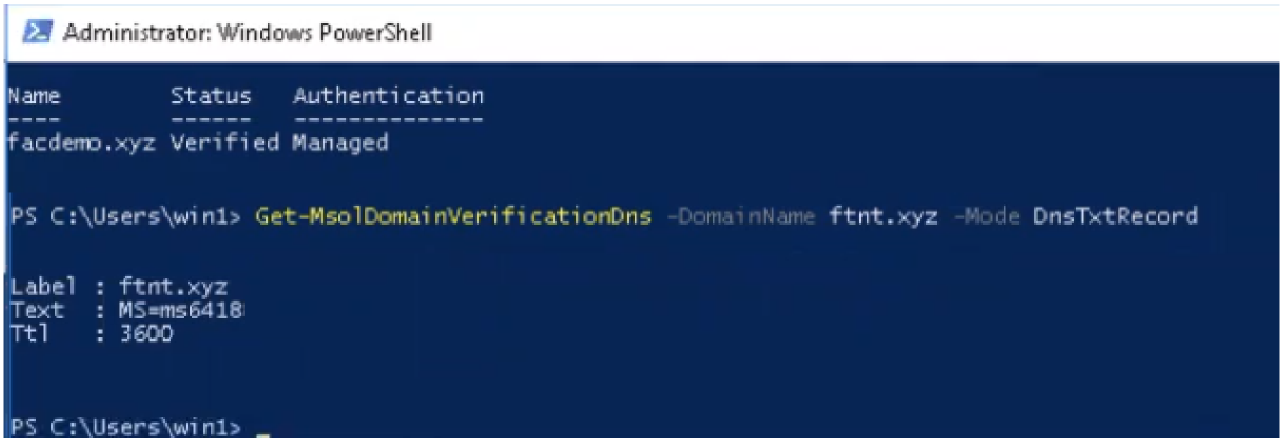
4. Add a federated domain by entering the following command.
`New-MsolDomain -Name <your domain> -Authentication Federated`



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> _
```

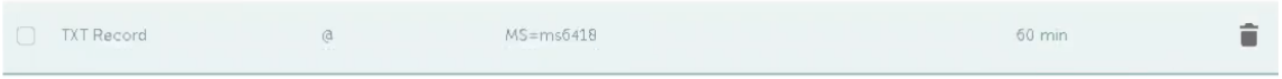
5. Obtain the DNS record and create a new text record in your domain provider to allow the domain to be verified. To obtain the DNS record, use the following command:
`Get-MsolDomainVerificationDns -DomainName ftnt.xyz -Mode DnsTxtRecord`



Administrator: Windows PowerShell

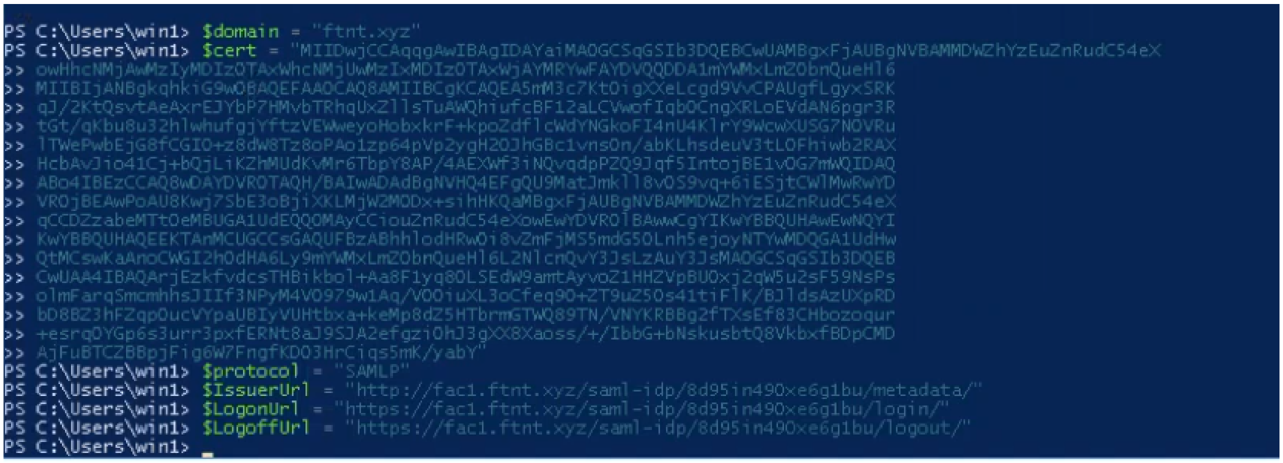
```
Name        Status   Authentication
----        ------   --------------
facdemo.xyz Verified Managed

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 = "MIIDwjCCAqqgAwIBAgIDAYaiMAOGCSqGSIb3DQEBCwUAMBgxFjAUBgNVBAMMDWZhYzEuZnRudC54eX
>> 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> _
```

7. To change the authentication type for the domain, enter the following command into PowerShell:

```
Set-MsolDomainAuthentication -DomainName $domain -FederationBrandName $domain -
     Authentication Federated -IssuerUri $IssuerUrl -LogOffUri $LogoffUrl -
     PassiveLogOnUri $LogonUrl -SigningCertificate $cert -
     PreferredAuthenticationProtocol $protocol
```

8. 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
```

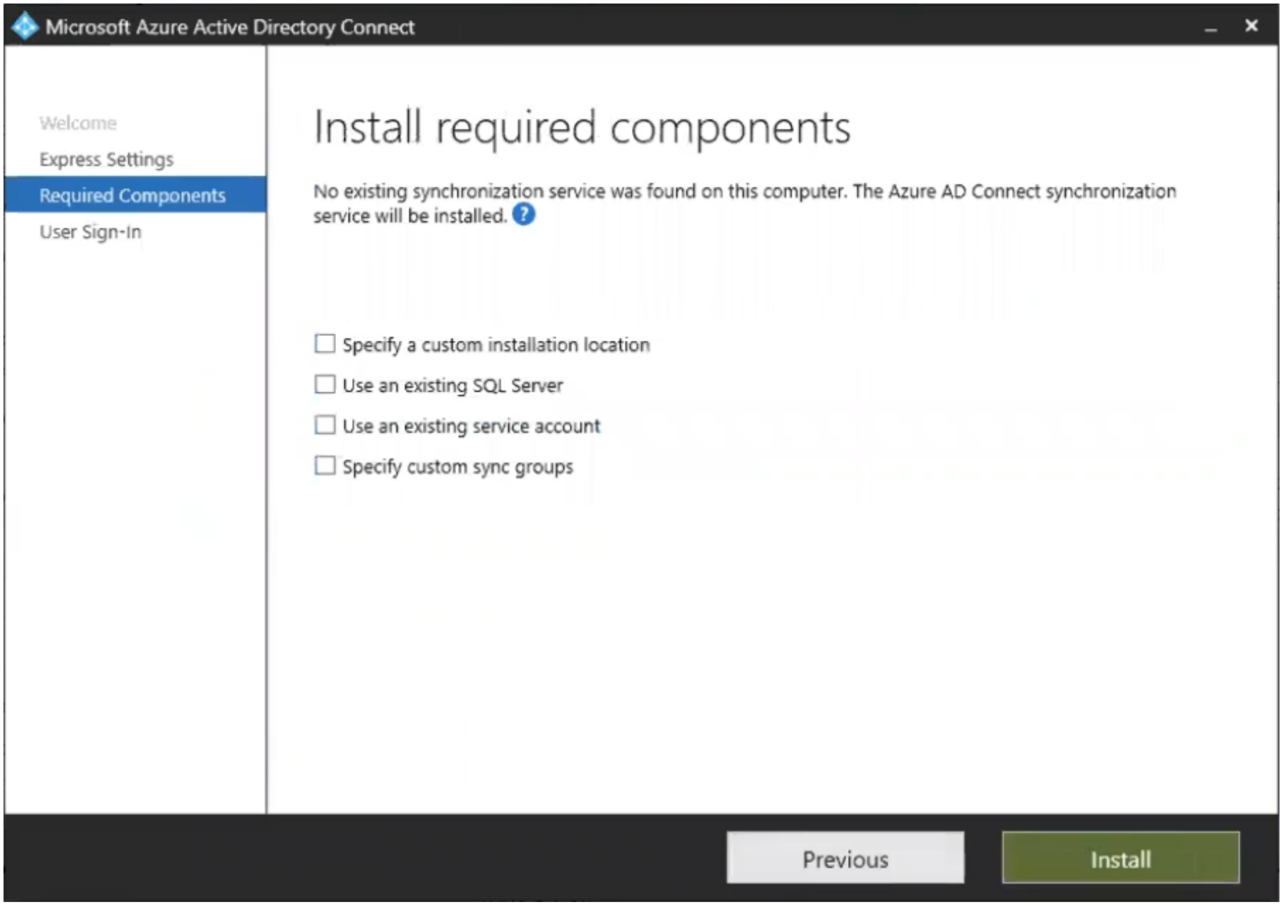
   The return text from the above command should read "AvailableImmediately The domain has been successfully verified for your account."

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.

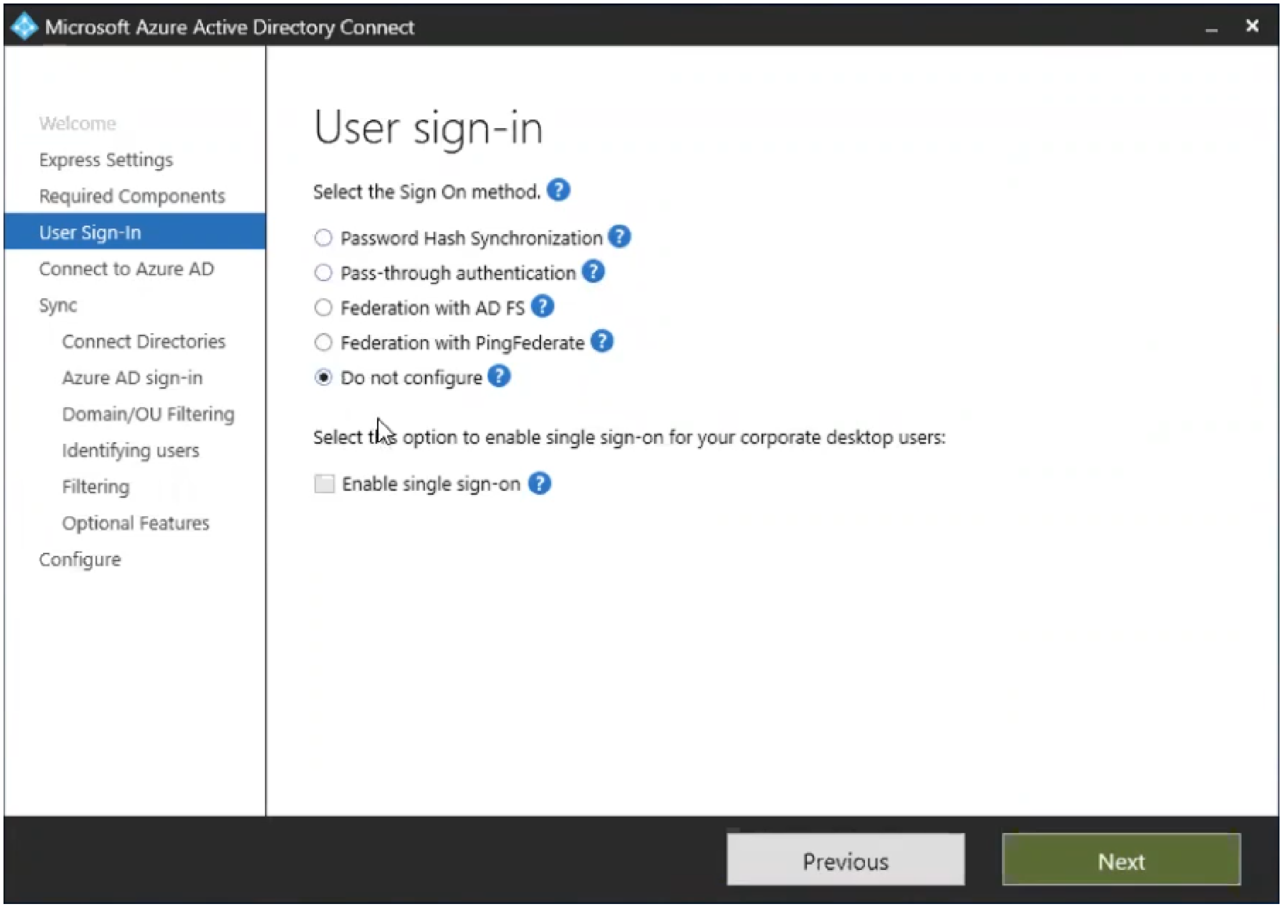
□ Specify a custom installation location

□ 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*.



User sign-in

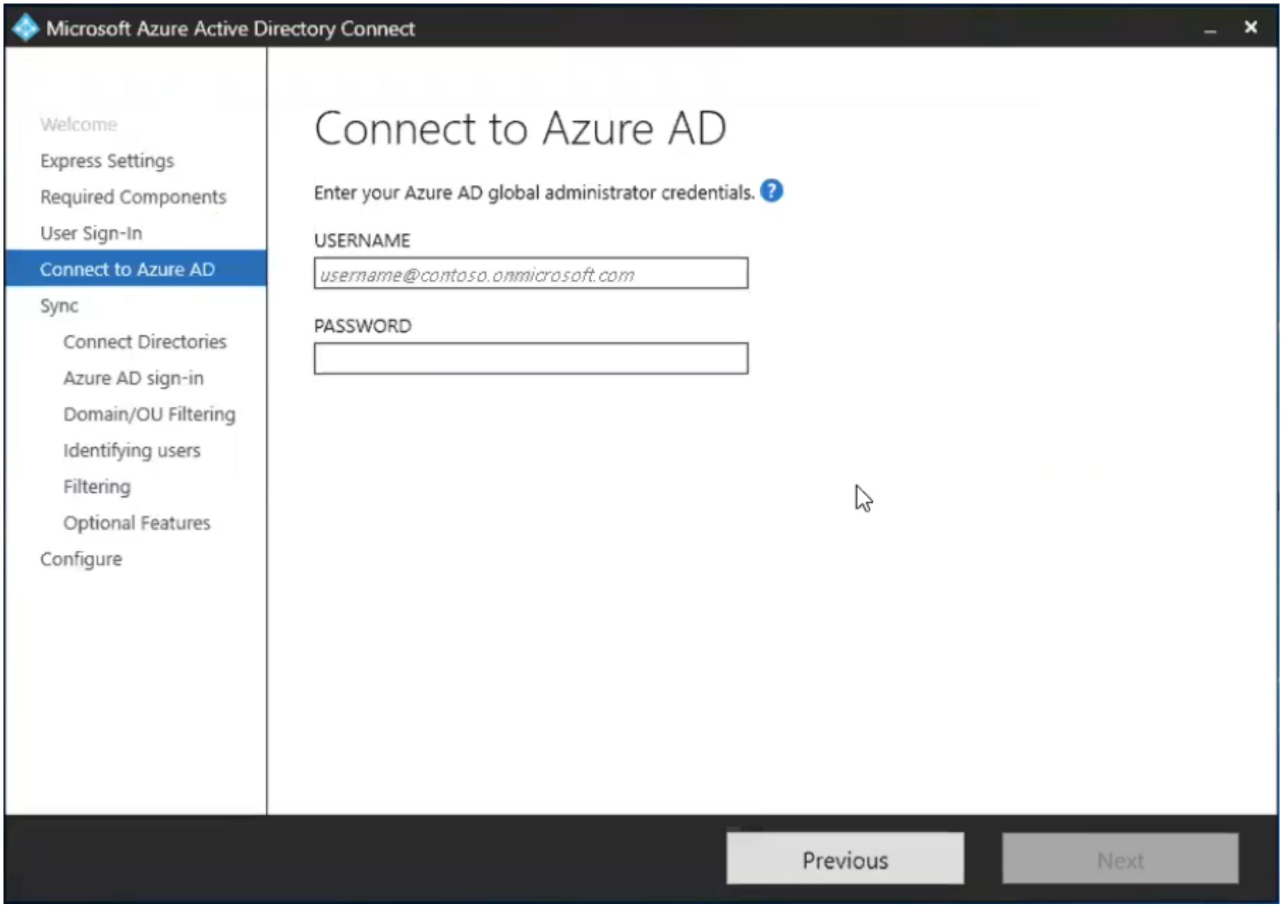
Select the Sign On method.

○ 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

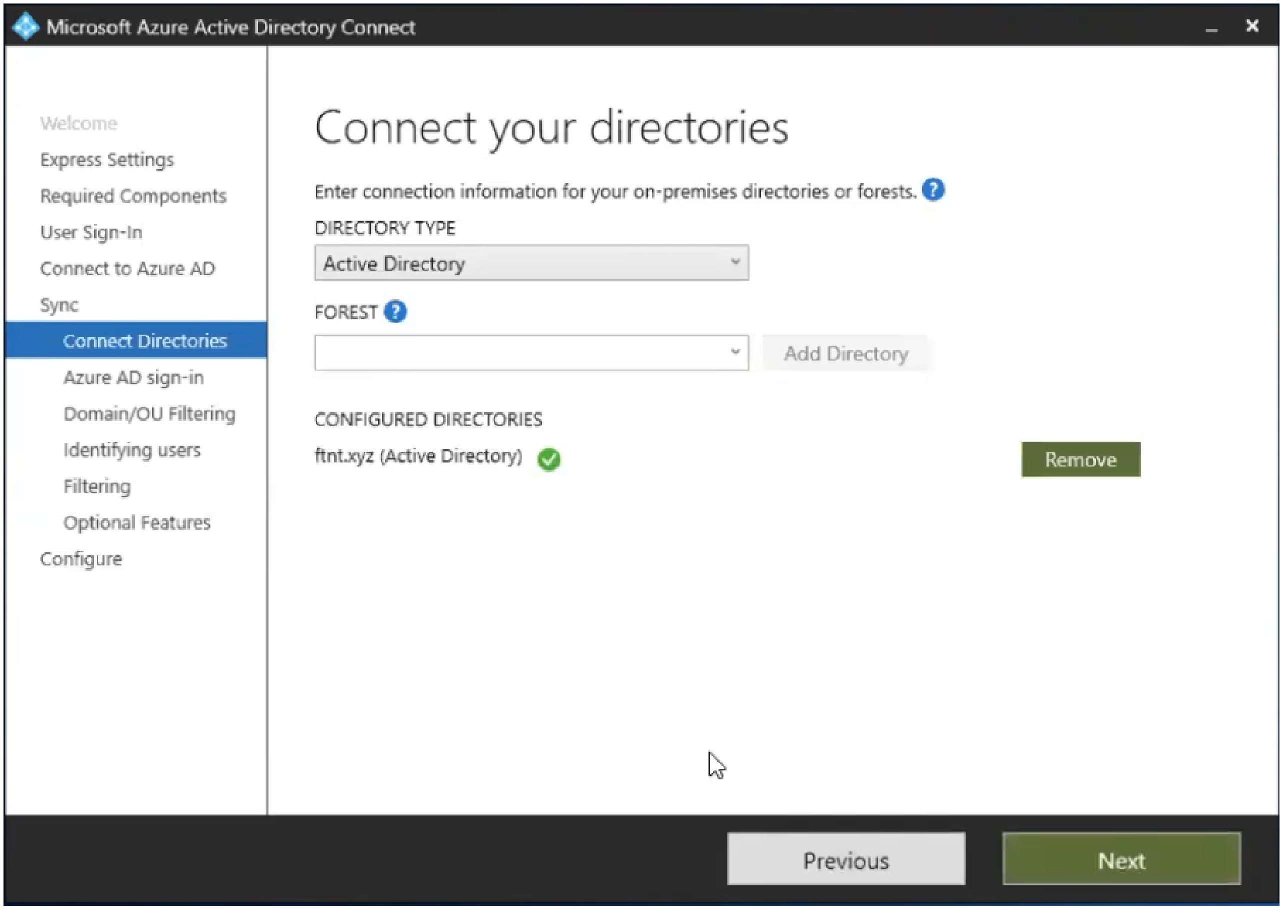
Enter your Azure AD global administrator credentials.

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.

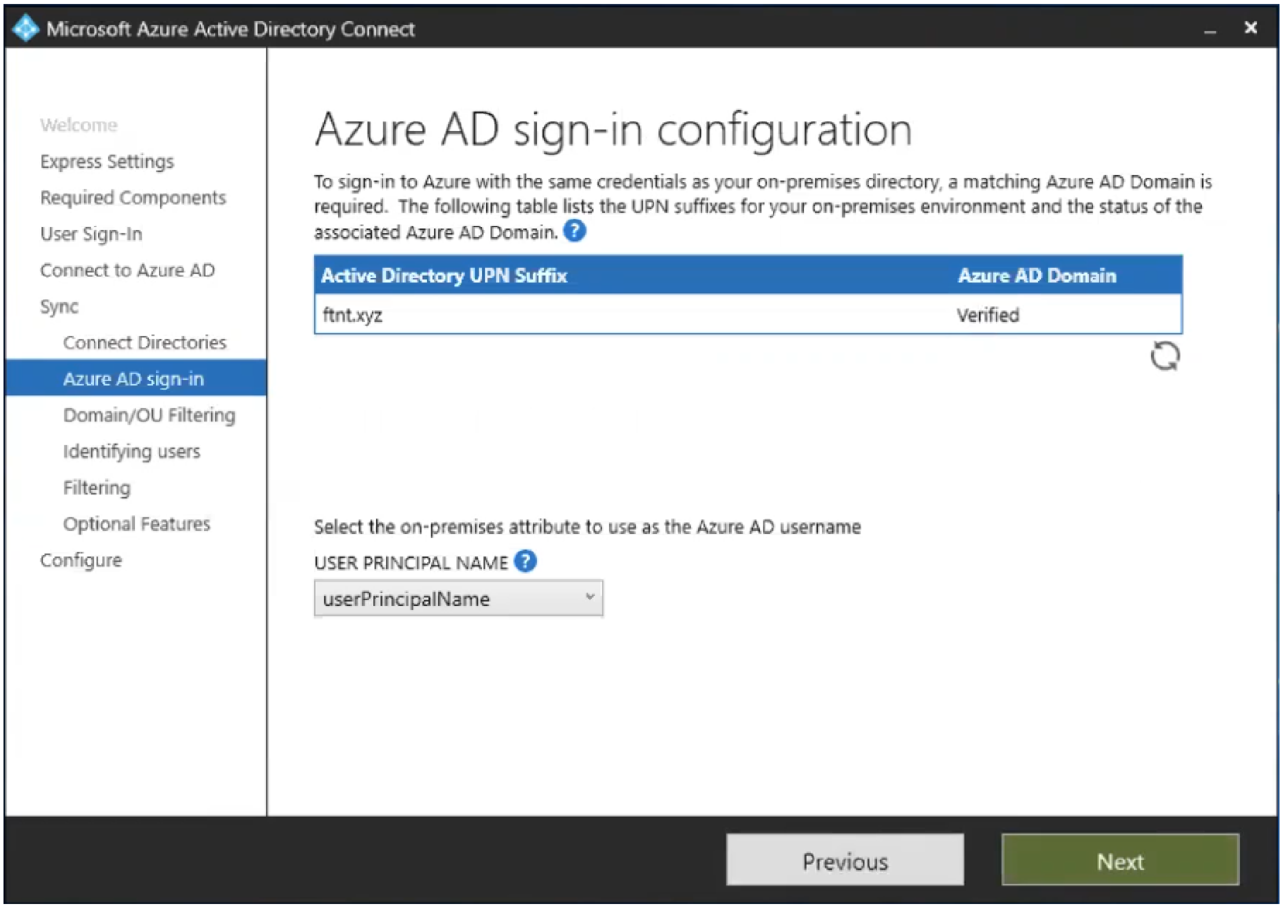
DIRECTORY TYPE: Active Directory

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.

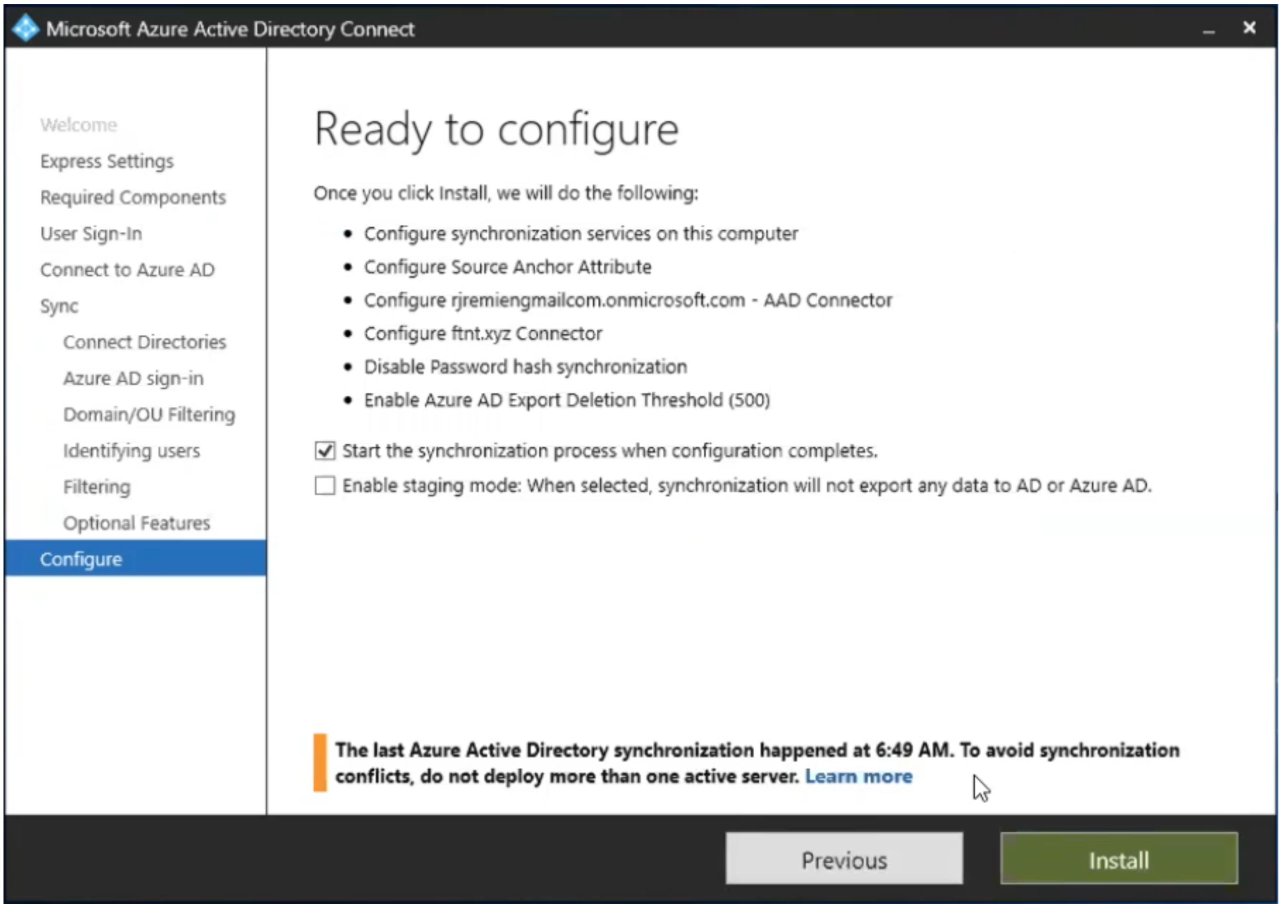
Active Directory UPN Suffix	Azure AD Domain
ftnt.xyz	Verified

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:

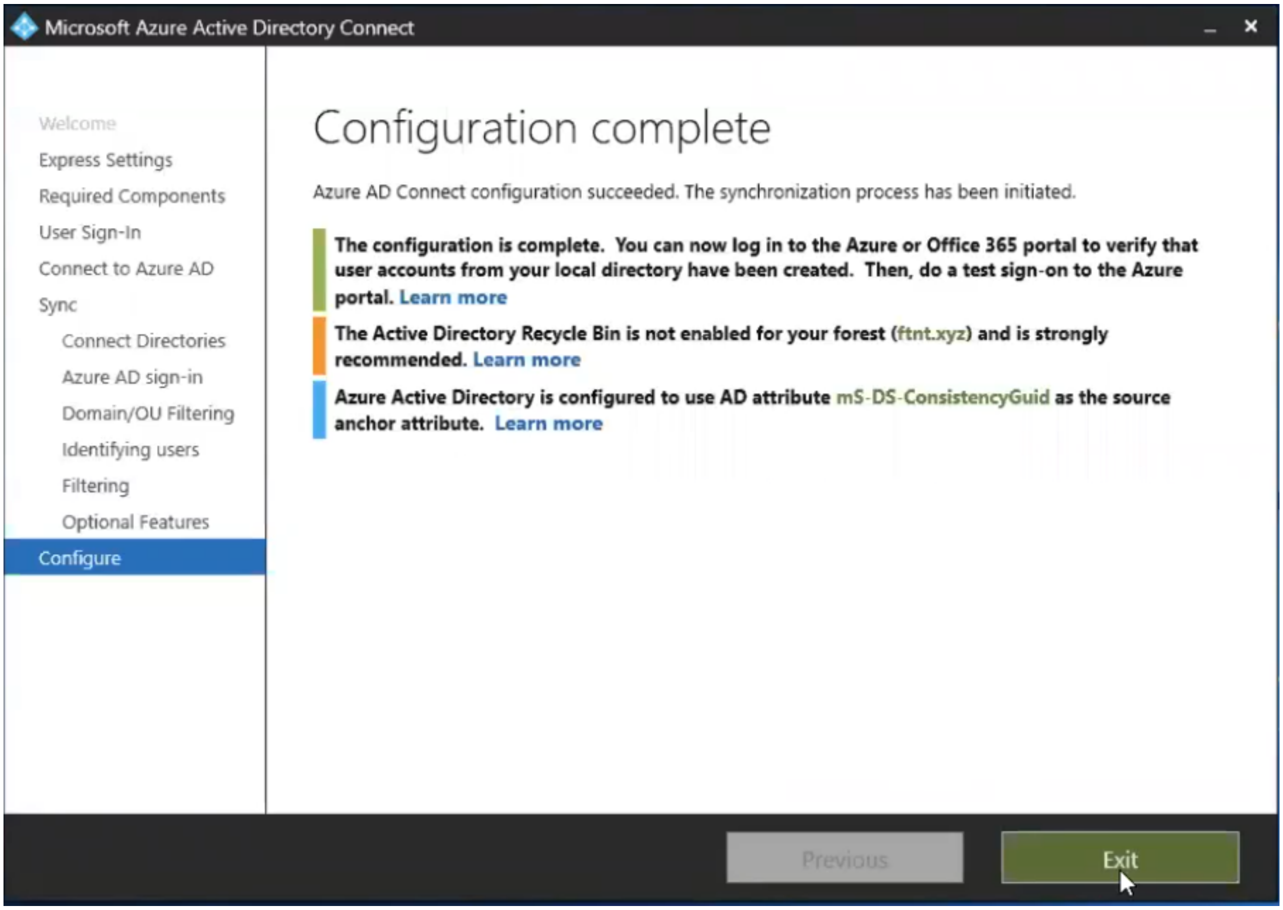
- Configure synchronization services on this computer
- Configure Source Anchor Attribute
- Configure rjremiengmailcom.onmicrosoft.com - AAD Connector
- Configure ftnt.xyz Connector
- Disable Password hash synchronization
- Enable Azure AD Export Deletion Threshold (500)

☑ 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

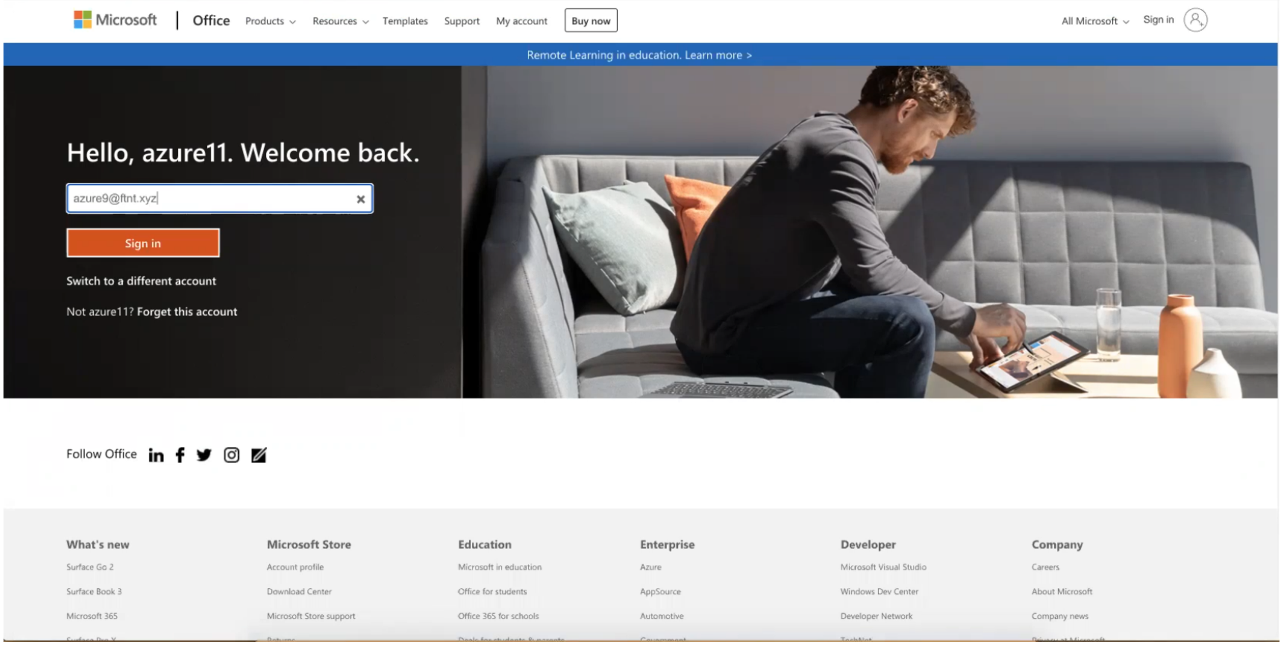
Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute. Learn more

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:

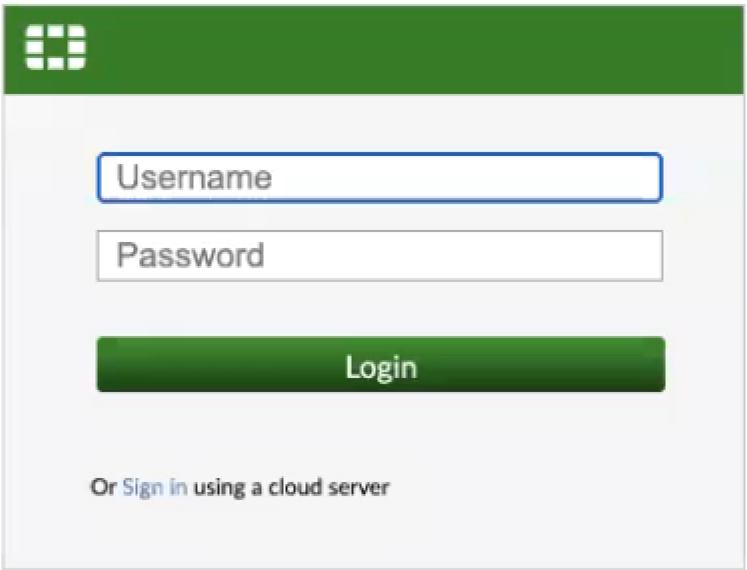
1. Navigate to Office 365 and click *Sign in* or *Switch to a different account*.
2. Enter a user account with domain and click *Sign in*.



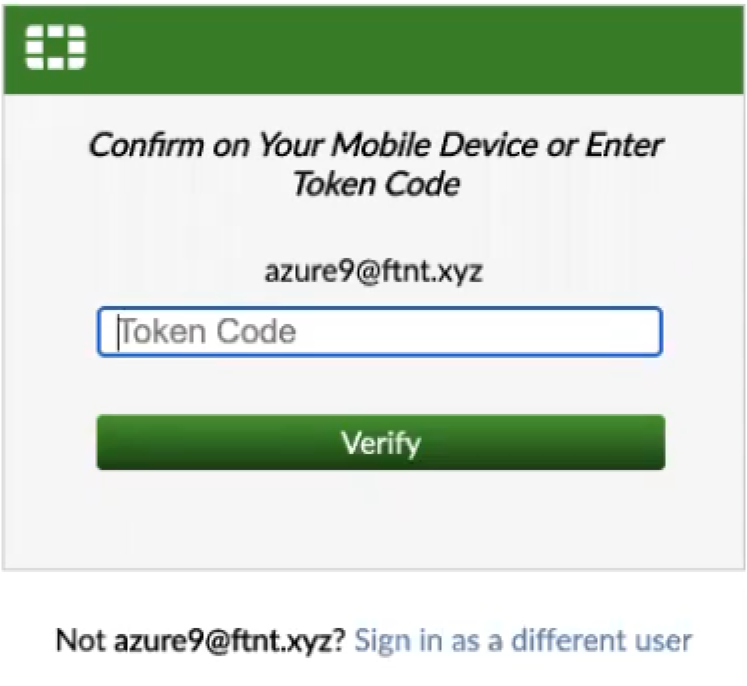
Hello, azure11. Welcome back.

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

Token Code

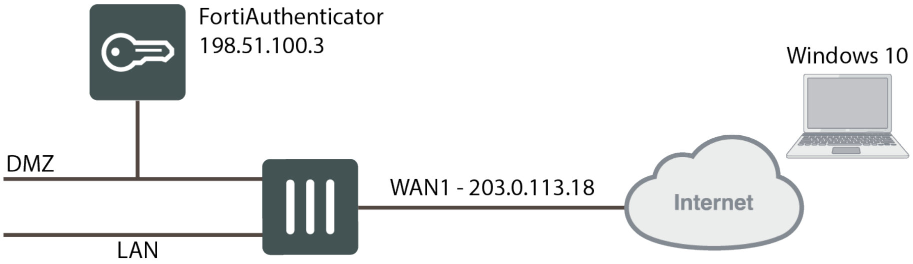
Not azure9@ftnt.xyz? Sign in as a different user

Once approved you are logged in to your Office 365 account.

FortiGate SSL VPN with FortiAuthenticator as the IdP proxy for Azure

This example configuration allows FortiAuthenticator to act as the IdP proxy for Azure authentication to a FortiGate SSL VPN connection. This allows authentication of SSL VPN users against an Azure IdP using two factor authentication with FortiToken by inserting FortiAuthenticator into the authentication flow.

This configuration uses the following topology:



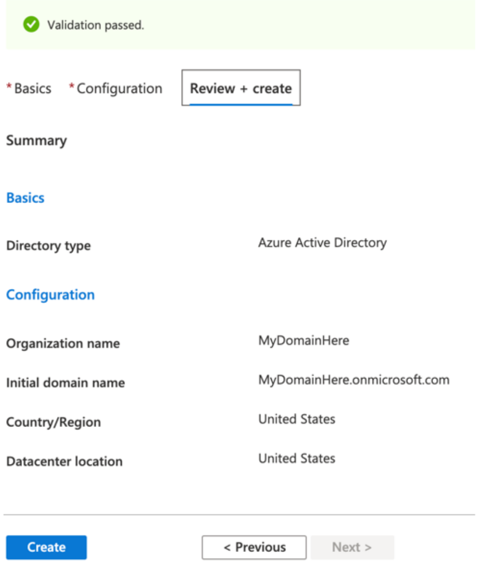
To configure FortiAuthenticator as the IdP proxy for Azure:

1. Configuring Azure on page 216
2. Configuring FortiAuthenticator on page 219
3. Configuring FortiGate on page 224
4. Results on page 226

You need Azure Active Directory Premium P1 or P2 to perform group-based assignments to an Enterprise App. Azure AD Free tier only supports user-based assignments.

Configuring Azure

1. Login to the Azure portal. If you do not yet have a directory or need to create a new one, go to *Azure AD* and click *Create a tenant*.
   Configure the directory with the following settings:
   a. **Select a directory type**: *Azure Active Directory*.
   b. **Organization name**: Enter a name for the organization.
   c. **Initial domain name**: Enter the domain name.
   d. **Country/Region**: Select the relevant country or region.
   e. Click *Create*. The directory will be created after a few minutes. When finished, select the directory in the top-right corner of Azure.



Validation passed.

Summary

Basics

Directory type: Azure Active Directory

Configuration

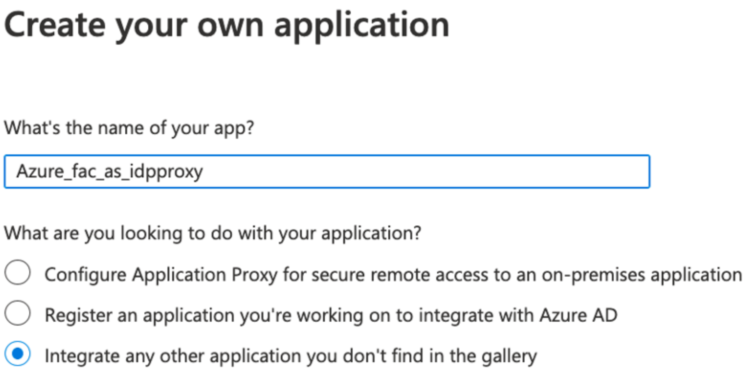
Organization name: MyDomainHere

Initial domain name: MyDomainHere.onmicrosoft.com

Country/Region: United States

Datacenter location: United States

2. Go to *Enterprise Applications*, and select *Create your own application*. Enter a name for your application, for example: `Azure_fac_as_idpproxy`.



Create your own application

What's the name of your app?

Azure_fac_as_idpproxy

What are you looking to do with your application?

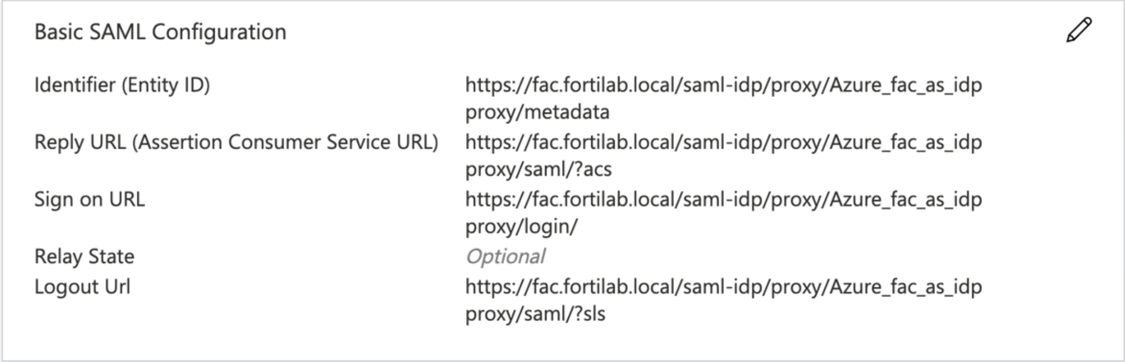
○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application you're working on to integrate with Azure AD

● Integrate any other application you don't find in the gallery

3. Go to the *Single Sign-on* section, select *SAML*, and edit the basic SAML configuration.
   Here you will include information obtained from FortiAuthenticator. In this example, the FortiAuthenticator FQDN is

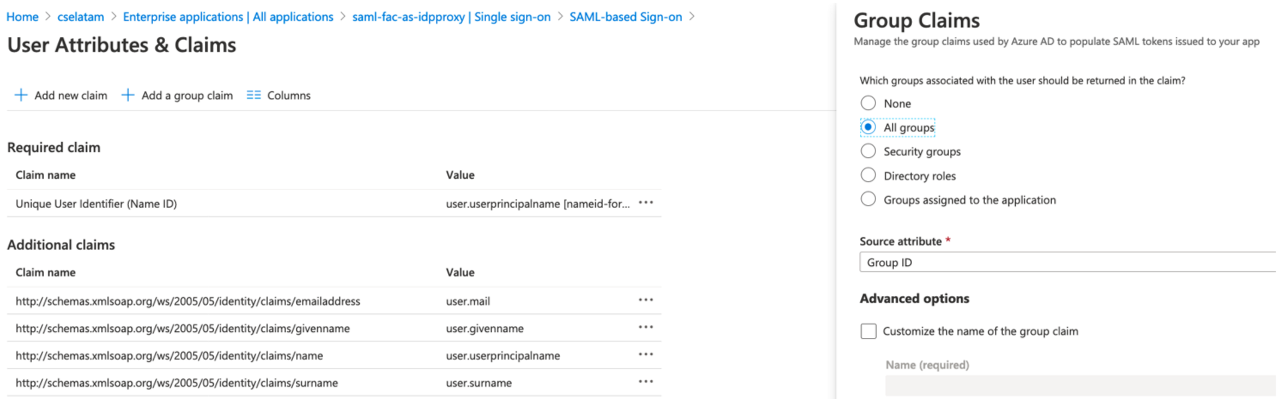
fac.fortilab.local, and the name of the server is defined as *Azure_fac_as_idpproxy*. You should adjust these settings to match your FortiAuthenticator's configuration.



Basic SAML Configuration

Identifier (Entity ID)	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/metadata
Reply URL (Assertion Consumer Service URL)	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/saml/?acs
Sign on URL	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/login/
Relay State	*Optional*
Logout Url	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/saml/?sls

4. Edit the *User Attributes & Claims* section to insert any attributes required for the SAML assertion. In this example, only user groups have been included.
   Click the edit icon, and then click *Add a group claim*. Select *All groups*.



Home > cselatam > Enterprise applications | All applications > saml-fac-as-idpproxy | Single sign-on > SAML-based Sign-on >

User Attributes & Claims

+ Add new claim
+ Add a group claim
Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
● All groups
○ Security groups
○ Directory roles
○ Groups assigned to the application

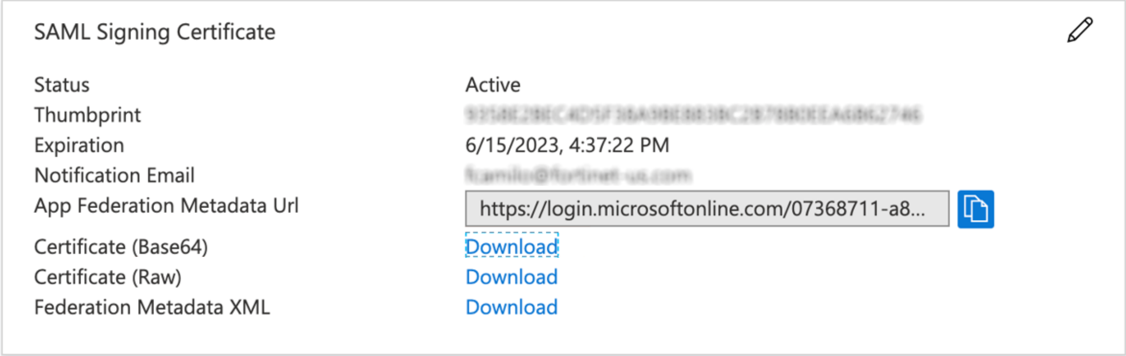
Source attribute *: Group ID

Advanced options

□ Customize the name of the group claim

Name (required)

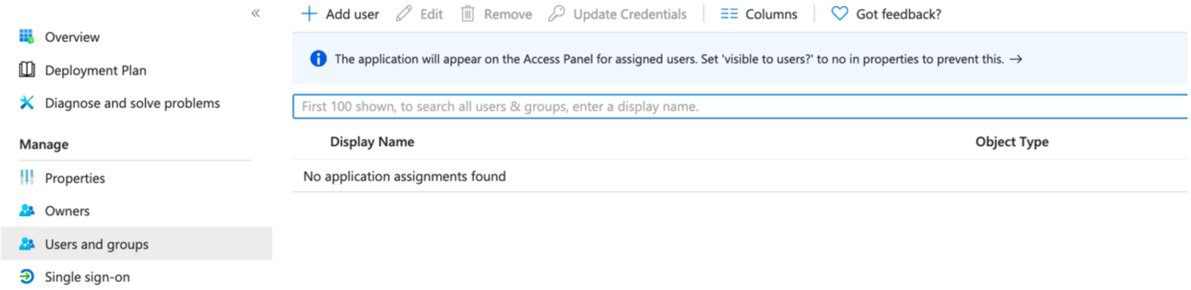
5. Download the certificate file. It will be used later when configuring FortiAuthenticator.



SAML Signing Certificate

Status	Active
Thumbprint	[redacted]
Expiration	6/15/2023, 4:37:22 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/07368711-a8...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

6. Go to *Users and Groups*, and click *Add user*. Include all users that will be able to authenticate using this application.

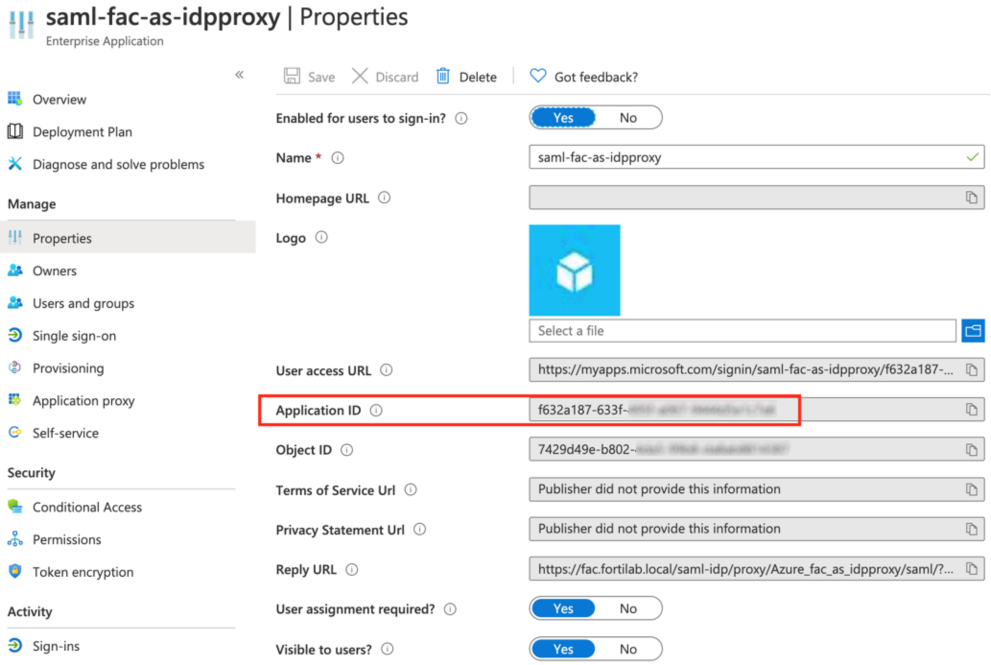


The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

Display Name	Object Type
No application assignments found	

7. Go to *Properties* and get the *Application ID*. This will be required later.



saml-fac-as-idpproxy | Properties

Enterprise Application

Enabled for users to sign-in? ● Yes ○ No

Name * saml-fac-as-idpproxy

Homepage URL

Logo

User access URL https://myapps.microsoft.com/signin/saml-fac-as-idpproxy/f632a187-...

Application ID f632a187-633f-[redacted]

Object ID 7429d49e-b802-[redacted]

Terms of Service Url Publisher did not provide this information

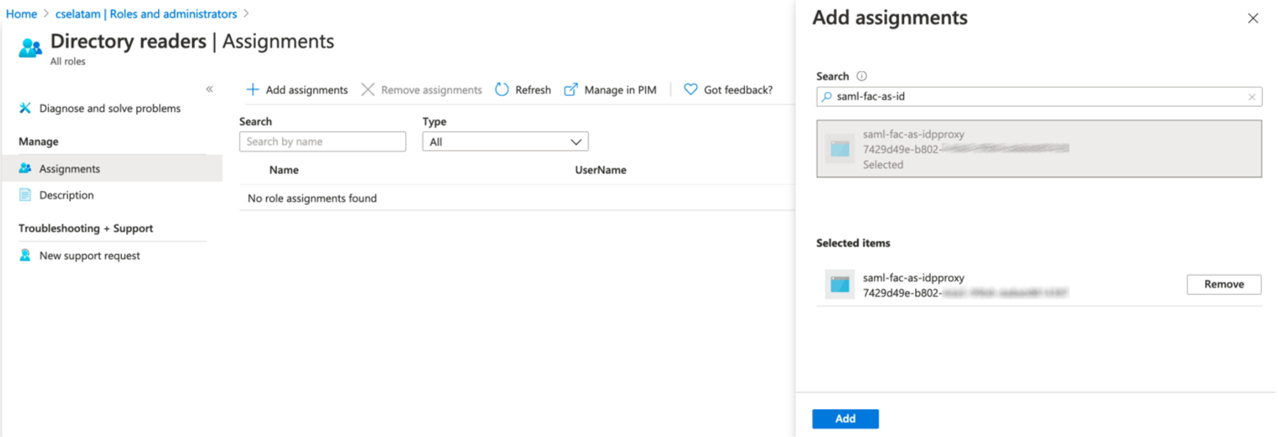
Privacy Statement Url Publisher did not provide this information

Reply URL https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/saml/?...

User assignment required? ● Yes ○ No

Visible to users? ● Yes ○ No

8. From the directory home, select *Roles and Administrators* > *Directory Readers*, and click *Add assignments*. Search for your application name, then select and add it.



Directory readers | Assignments

Search: Search by name

Type: All

Name	UserName
No role assignments found	

Add assignments

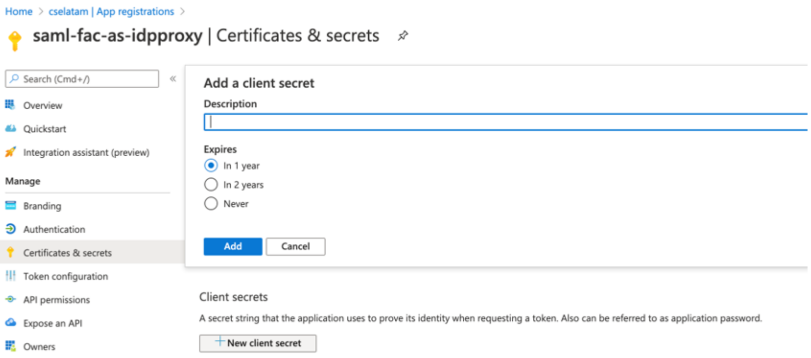
Search: saml-fac-as-id

saml-fac-as-idpproxy
7429d49e-b802-[redacted]
Selected

Selected items

saml-fac-as-idpproxy
7429d49e-b802-[redacted]

9. Finally, create your authentication key. Go to *App Registrations*, click *Certificates & Secrets*, and create a new key.



saml-fac-as-idpproxy | Certificates & secrets

Add a client secret

Description

Expires

● In 1 year

○ In 2 years

○ Never

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Before proceeding, make sure to copy the key value. The key is presented only after its creation, and you cannot get this information again later.

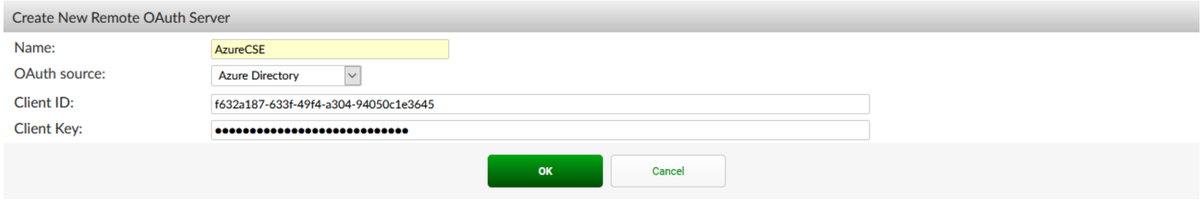
Configuring FortiAuthenticator

Configure the remote servers

A remote OAuth server is used to obtain group membership from Azure AD. Later, a FortiToken can be associated with those users.

To configure the remote OAuth server:

1. Go to *Authentication* > *Remote Auth. Servers* > *OAUTH*, and click *Create New*.
2. Configure the following information:
   - **Name**: Enter a name for your OAuth server, for example: *AzureCSE*.
   - **OAuth source**: *Azure Directory*.
   - **Client ID**: Enter your *Azure Application ID*.
   - **Client Key**: Enter your Azure key.



Create New Remote OAuth Server

Name:	AzureCSE
OAuth source:	Azure Directory
Client ID:	f632a187-633f-49f4-a304-94050c1e3645
Client Key:	●●●●●●●●●●●●●●●●●●●●●●●●●●●●

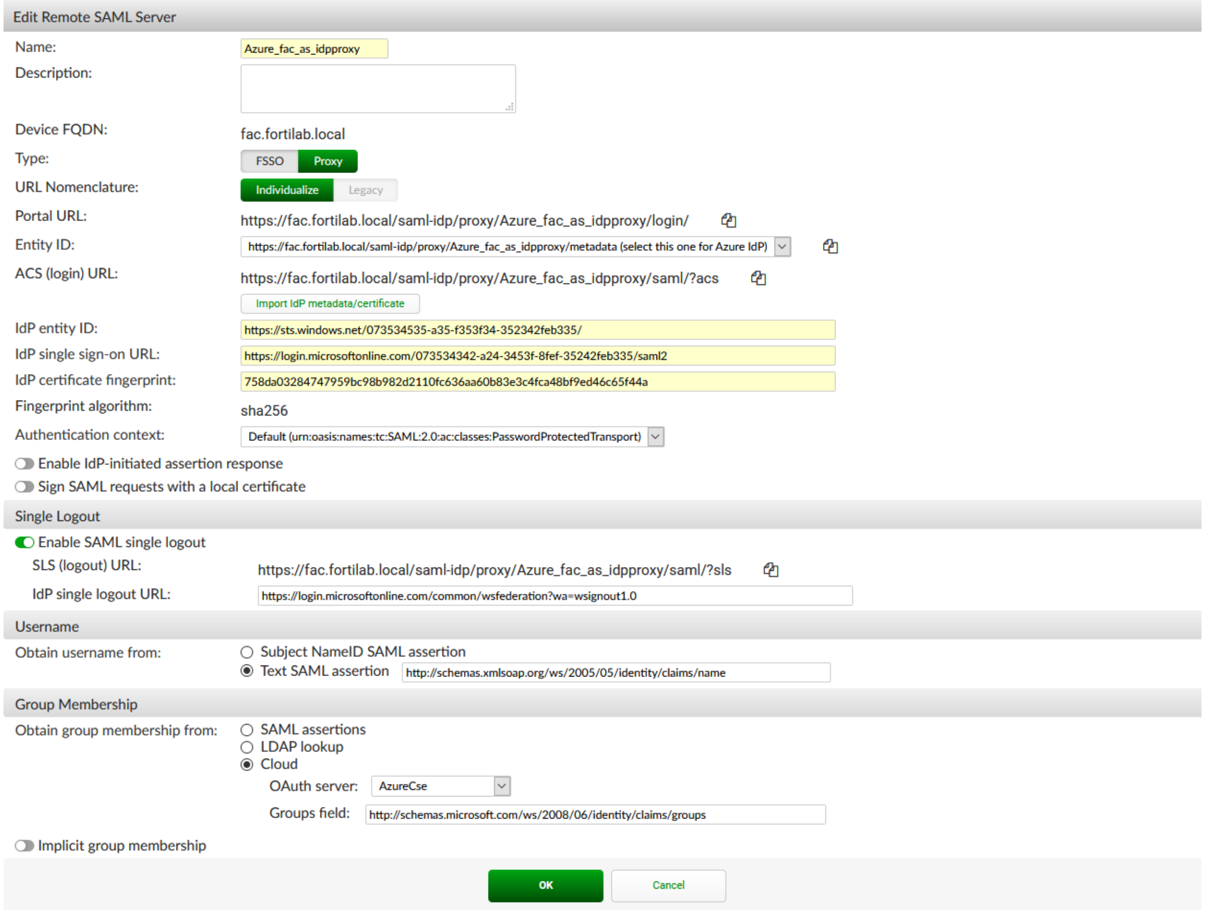
3. Click *OK*.

To configure the remote SAML server:

1. Go to *Authentication* > *Remote Auth. Servers* > *SAML*, and click *Create New*.
2. Under *Remote SAML Server*, configure the following:
   - **Name**: Enter a name for the server. This name must match the server name configured in Azure. In this example, the server name is *Azure_fac_as_idpproxy*.

- **Type**: *Proxy*.
- **Entity ID**: Select the Azure IdP option.
- **Import IdP metadata/certificate**: Import the certificate that you previously exported from Azure.
- **IdP entity ID**: Enter the *Azure AD Identifier* from your Azure configuration.
- **IdP single sign-on URL**: Enter the *Login URL* from your Azure configuration.

3. Under *Single Logout*, configure the following:
   - **Enable SAML single logout**: Optionally, you can enable this setting to enable SAML single logout.
   - **IdP single logout URL**: Enter the *Logout URL* from your Azure configuration.
4. Under *Username*, configure the following:
   - **Obtain username from**: Select *Text SAML assertion* and use the configured username claim URL from your Azure configuration.
5. In *Group Membership*, configure the following:
   - **Obtain group membership from**: Select *Cloud* and choose your remote OAuth server. Group membership of a particular user will be retrieved dynamically through OAuth upon authentication.



Edit Remote SAML Server

Name:	Azure_fac_as_idpproxy
Description:	
Device FQDN:	fac.fortilab.local
Type:	FSSO [✓ Proxy]
URL Nomenclature:	[✓ Individualize] Legacy
Portal URL:	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/login/
Entity ID:	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/metadata (select this one for Azure IdP)
ACS (login) URL:	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/saml/?acs
IdP entity ID:	https://sts.windows.net/073534535-a35-f353f34-352342feb335/
IdP single sign-on URL:	https://login.microsoftonline.com/073534342-a24-3453f-8fef-35242feb335/saml2
IdP certificate fingerprint:	758da03284747959bc98b982d2110fc636aa60b83e3c4fca48bf9ed46c65f44a
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

SLS (logout) URL:	https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idpproxy/saml/?sls
IdP single logout URL:	https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

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: AzureCse
Groups field: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

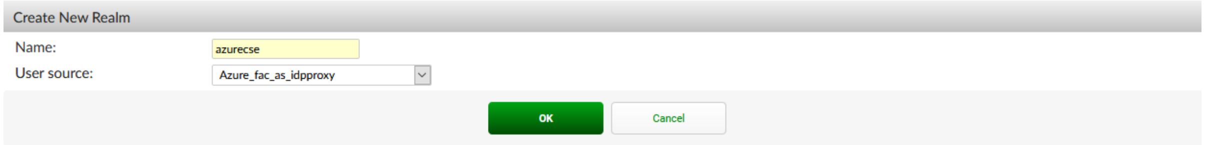
○ Implicit group membership

6. Click *OK*.

Configure the SAML IdP settings on FortiAuthenticator

To create the Azure realm:

1. Go to *Authentication > User Management > Realms*, and click *Create New*.
2. Configure the following information:
   a. **Name**: Enter a name for your user realm, for example: *azurecse*
   b. **User source**: Select your remote SAML server as the user source.



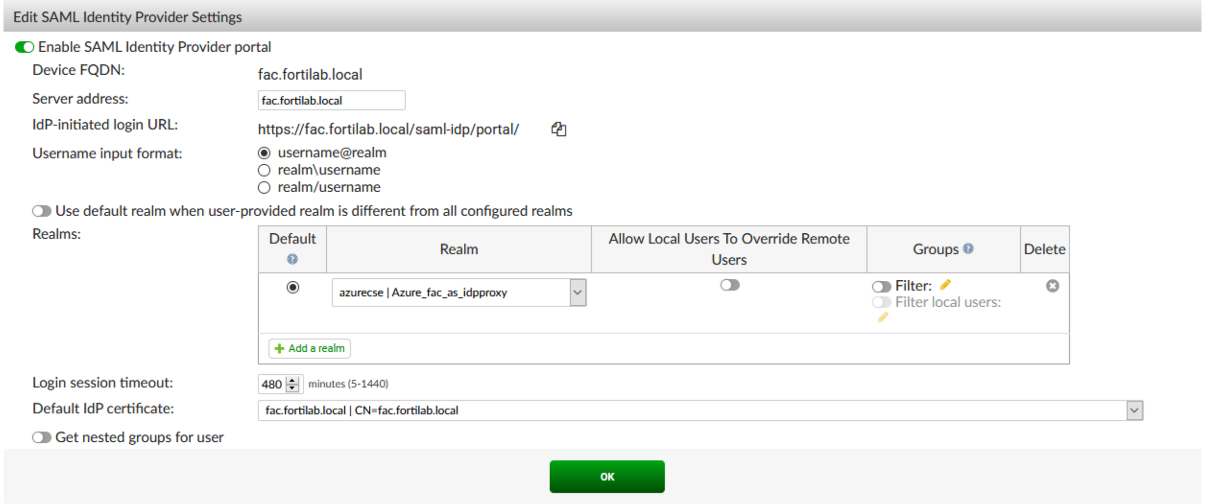
Create New Realm

Name:	azurecse
User source:	Azure_fac_as_idpproxy

3. Click *OK*.

To enable SAML IdP on FortiAuthenticator:

1. Go to *Authentication > SAML IdP > General*, click *Enable SAML Identity Provider portal*, and configure the following:
   a. **Server address**: Enter the IP or FQDN of your FortiAuthenticator.
   b. **Realms**: Select the SAML realm as the default.
   c. **Default IdP certificate**: Select a default IdP certificate.



Edit SAML Identity Provider Settings

Enable SAML Identity Provider portal

Device FQDN:	fac.fortilab.local
Server address:	fac.fortilab.local
IdP-initiated login URL:	https://fac.fortilab.local/saml-idp/portal/
Username input format:	● username@realm ○ realm\username ○ realm/username

Use default realm when user-provided realm is different from all configured realms

Realms:

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

Login session timeout:	480 minutes (5-1440)
Default IdP certificate:	fac.fortilab.local | CN=fac.fortilab.local

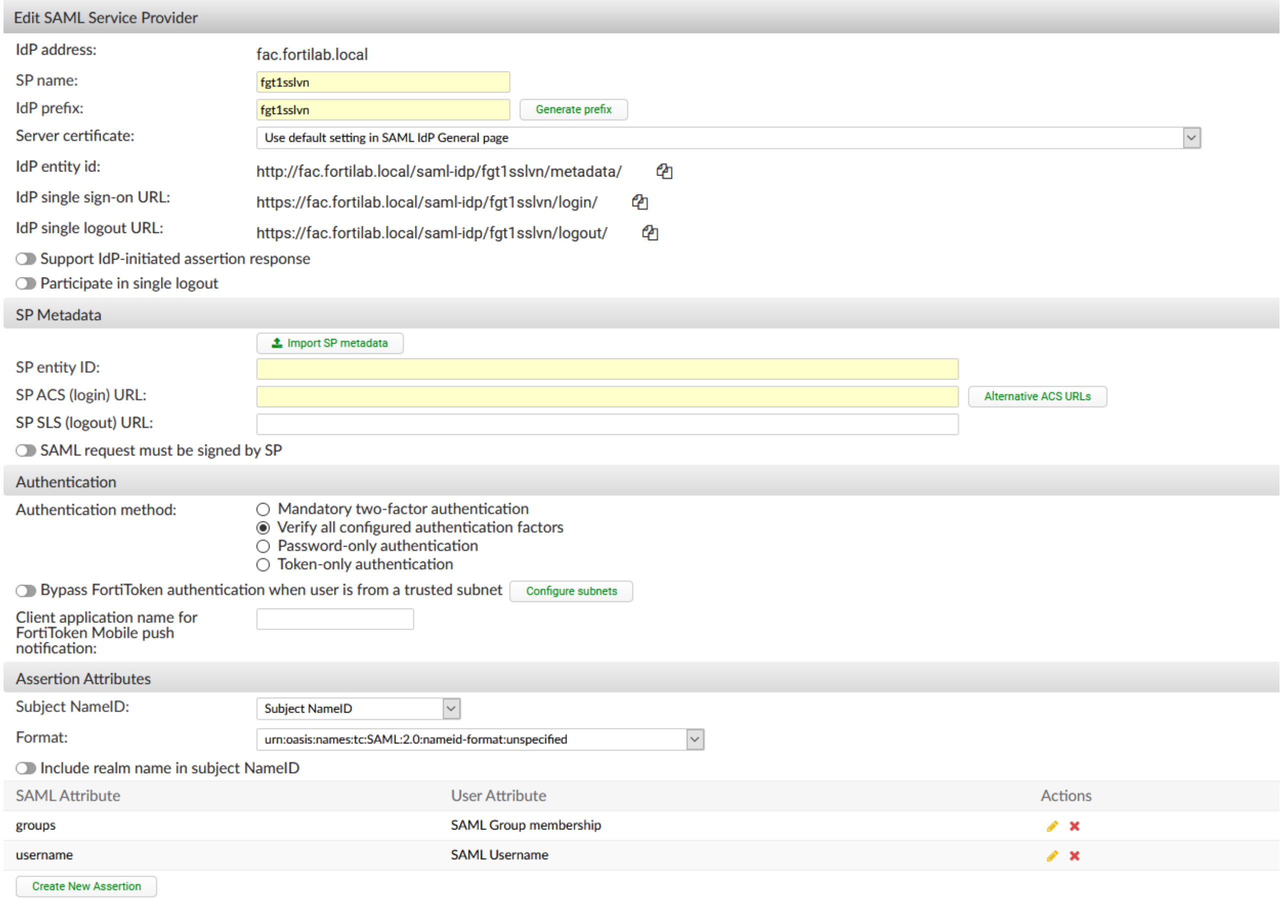
Get nested groups for user

2. Click *OK*.
   You will also need to download your IdP certificate for use later. It can be downloaded from *Certificate Management > End Entities*.

To add FortiGate as a SAML service provider:

1. Go to *Authentication > SAML IdP > Service Providers*, and click *Create New*.
2. Under *Edit SAML Service Provider*, configure the following:
   - **SP name**: Enter a name for this service provider, for example: *fgt1sslvpn*.
   - **IdP prefix**: Enter a custom IdP prefix or click *Generate prefix* to automatically populate this field.
3. Under *Assertion Attributes*, configure the following:
   - **Subject NameID**: *Remote SAML Server > Subject NameID*.
   - **Format**: *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified*.

4. Under *SAML Attributes*, add the following attributes. The user and group information will be propagated by the FortiAuthenticator IdP in SAML assertions to FortiGate. These must match with the *user-name* and *group-name* keywords defined for the SAML user. See Configure the SAML user on page 224.
   - Attribute 1: SAML attribute: *groups*, User attribute: *SAML Group membership*.
   - Attribute 2: SAML attribute: *username*, User attribute: *SAML Username*.
5. Click *Save*.



Edit SAML Service Provider

IdP address:	fac.fortilab.local
SP name:	fgt1sslvn
IdP prefix:	fgt1sslvn Generate prefix
Server certificate:	Use default setting in SAML IdP General page
IdP entity id:	http://fac.fortilab.local/saml-idp/fgt1sslvn/metadata/
IdP single sign-on URL:	https://fac.fortilab.local/saml-idp/fgt1sslvn/login/
IdP single logout URL:	https://fac.fortilab.local/saml-idp/fgt1sslvn/logout/

Support IdP-initiated assertion response

Participate in single logout

SP Metadata

Import SP metadata

SP entity ID:	
SP ACS (login) URL:	Alternative ACS URLs
SP SLS (logout) URL:	

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

Client application name for FortiToken Mobile push notification:

Assertion Attributes

Subject NameID:	Subject NameID
Format:	urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

Include realm name in subject NameID

SAML Attribute	User Attribute	Actions
groups	SAML Group membership	✎ ✖
username	SAML Username	✎ ✖

Create New Assertion

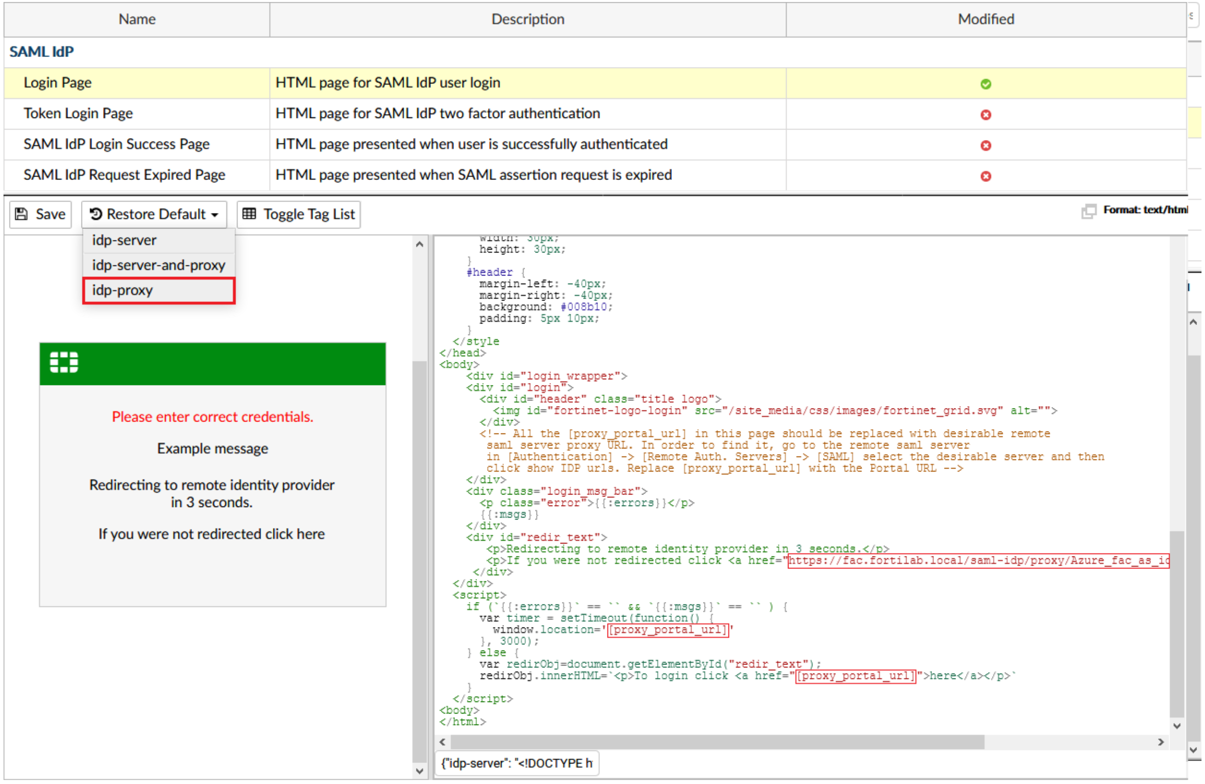
Once the settings have been saved, you will see that additional options are available.

You can return to complete the configuration of the SAML service provider settings on FortiAuthenticator once you have configured your FortiGate SAML user. You will need to enter the *SP entity ID*, *SP ACS (login) URL*, and *SP SLS (logout) URL* from the FortiGate configuration.

To update the SAML replacement message:

1. Go to *Authentication* > *SAML IdP* > *Replacement Messages*.
2. Select *SAML IdP* > *Login Page*, and then select *idp-proxy* in the *Restore Default* dropdown menu.
   You can now edit the content in the right pane to include the *Portal URL* obtained from your remote SAML server.

The URL must be replaced in three places as indicated by `[proxy_portal_url]` in the text.



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	✗

Please enter correct credentials.

Example message

Redirecting to remote identity provider in 3 seconds.

If you were not redirected click here

```
        width: 30px;
        height: 30px;
      }
      #header {
        margin-left: -40px;
        margin-right: -40px;
        background: #008b10;
        padding: 5px 10px;
      }
    </style
</head>
<body>
    <div id="login_wrapper">
    <div id="login">
      <div id="header" class="title logo">
        <img id="fortinet-logo-login" src="/site_media/css/images/fortinet_grid.svg" alt="">
      </div>
      <!-- All the [proxy_portal_url] in this page 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>
    <div class="login_msg_bar">
      <p class="error">{{:errors}}</p>
      {{:msgs}}
    </div>
    <div id="redir_text">
       <p>Redirecting to remote identity provider in 3 seconds.</p>
       <p>If you were not redirected click <a href="https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_id
     </div>
  </div>
  <script>
    if (`{{:errors}}` == `` && `{{:msgs}}` == `` ) {
      var timer = setTimeout(function() {
        window.location='[proxy_portal_url]'
      }, 3000);
    } else {
      var redirObj=document.getElementById("redir_text");
      redirObj.innerHTML=`<p>To login click <a href="[proxy_portal_url]">here</a></p>`
    }
  </script>
<body>
</html>
```

{"idp-server": "<!DOCTYPE h

3. Click *Save*.

Configure FortiToken

To include tokens in a user's authentication:

1. Go to *Authentication* > *User Management* > *Remote Users*, select *SAML*, and click *Import*.
2. Under *Import Remote SAML Users*, configure the following settings:
   a. **Remote SAML server**: Select your remote SAML server, for example: *Azure_fac_as_idpproxy*.
   b. **Group**: Select *All users* or choose a user group.
3. Click *OK*.
4. Edit an imported user to define the token. Enable *Token-based authentication*, and select your token type.
5. Click *OK*.

Configuring FortiGate

Import the certificate

To import the FortiAuthenticator IdP certificate:

1. Go to *System* > *Certificates*, and click *Import* > *Remote Certificate*.
2. Click *Upload* and select your FortiAuthenticator IdP certificate.
3. Click *OK*.
   FortiGate will choose a name by default. You can rename the certificate for easier management with the following CLI commands:

```
config vpn certificate remote
   rename <DEFAULT_CERT_NAME> to <NEW_CERT_NAME>
end
```

Configure the SAML user

You can now configure a FortiGate SAML user to point to FortiAuthenticator as the IdP.

In this example configuration, the FortiGate SSL VPN link is `https://203.0.113.18:10443`. This can be replaced with the SSL VPN link from your own configuration.

You will also need to adjust the FortiAuthenticator IdP entity ID, login URL, and logout URL to match those configured in your FortiAuthenticator. This information is available on FortiAuthenticator in *Authentication* > *SAML IdP* > *Service Providers*.

Configuring the SAML user must be done through the FortiGate CLI.

To configure a SAML user:

1. In the FortiGate CLI, enter the following commands:

```
config user saml
   edit "fac-samlproxy-sslvpn"
      set cert "Fortinet_Factory"
      set entity-id "https://203.0.113.18:10443/remote/saml/metadata"
      set single-sign-on-url "https://203.0.113.18:10443/remote/saml/login"
      set single-logout-url "https://203.0.113.18:10443/remote/saml/logout"
      set idp-entity-id "http://fac.fortilab.local/saml-idp/fgt1sslvpn/metadata/"
      set idp-single-sign-on-url "https://fac.fortilab.local/saml-
            idp/fgt1sslvpn/login/"
      set idp-single-logout-url "https://fac.fortilab.local/saml-
            idp/fgt1sslvpn/logout/"
      set idp-cert "FAC_IdP"
      set user-name "username"
      set group-name "groups"
   next
end
```

The entity ID, single sign on URL, and single logout URL configured in the FortiGate CLI must now be entered in the FortiAuthenticator service provider configuration.

See To add FortiGate as a SAML service provider: on page 221

The user-name and group-name configured must match what is being returned from FortiAuthenticator in the SAML assertions. See Configure the SAML IdP settings on FortiAuthenticator on page 221.

You can now create a SAML group which includes that user. You can also define the SAML groups that will be allowed to login as this group. In this example, only user that belong to "FGTGroup1" will be allowed to login to the SSL VPN. This can only be done through FortiGate CLI.

To configure a SAML group:

1. In the FortiGate CLI, enter the following commands:

```
config user group
   edit "samlproxy-sslvpn"
      set member "fac-samlproxy-sslvpn"
      config match
         edit 1
            set server-name fac-samlproxy-sslvpn
            set group-name “FGTGroup1”
         next
      end
   next
end
```

Next, increase the remote authentication timeout. This must be set to allow for enough time for the user to authenticate into Azure AD. This can only be done through the FortiGate CLI.

To increase the remote authentication timeout:

1. In the FortiGate CLI, enter the following commands:

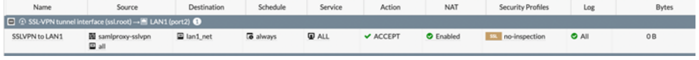
```
config system global
   set remoteauthtimeout 60
end
```

Configure the SSL VPN

You can define a portal for the SAML group in your SSL VPN settings.

To add a portal to your SSL VPN:

1. Go to *VPN > SSL-VPN Settings*, and edit your SSL VPN configuration.
2. Under *Authentication/Portal Mapping*, click *Create New*.
3. Configure the following information:
   a. **Users/Groups**: Select the configured user group.
   b. **Portal**: *full-access*.
4. Click *OK* and save your changes to the SSL VPN settings.
5. Configure your SSL VPN rules as required.



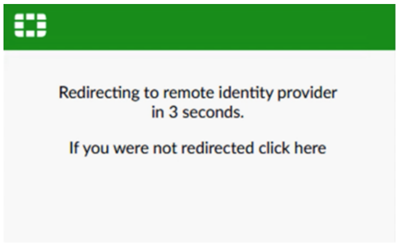
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
SSL-VPN tunnel interface (ssl.root) → LAN1 (port2) 1									
SSLVPN to LAN1	samlproxy-sslvpn all	lan1_net	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	✓ All	0 B

For more information on configuring SSL VPN on FortiGate, see the FortiGate Administration Guide.

Results

To sign in to your SSL VPN:

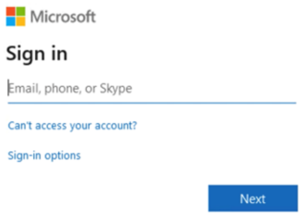
1. Once the user tries to connect to the SSL VPN web portal, FortiGate will redirect the user to FortiAuthenticator.



Redirecting to remote identity provider
in 3 seconds.

If you were not redirected click here

2. The FortiAuthenticator will act as a SAML proxy and forward the request to Azure for authentication.



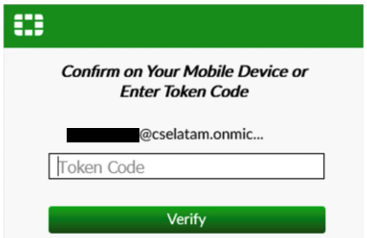
Sign in

Email, phone, or Skype

Can't access your account?

Sign-in options

3. After entering their credentials, if the user has a token assigned they will be requested to enter it for two factor authentication.



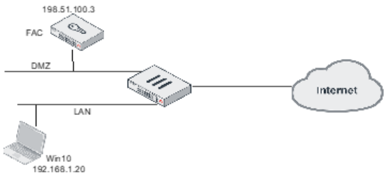
Confirm on Your Mobile Device or
Enter Token Code

[redacted]@cselatam.onmic...

Token Code

4. The user is now connected to the SSL VPN.

SAML FSSO with FortiAuthenticator and Microsoft Azure AD



In this example, you will provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator as the service provider (SP) and Microsoft Azure AD, as the identity provider (IdP).

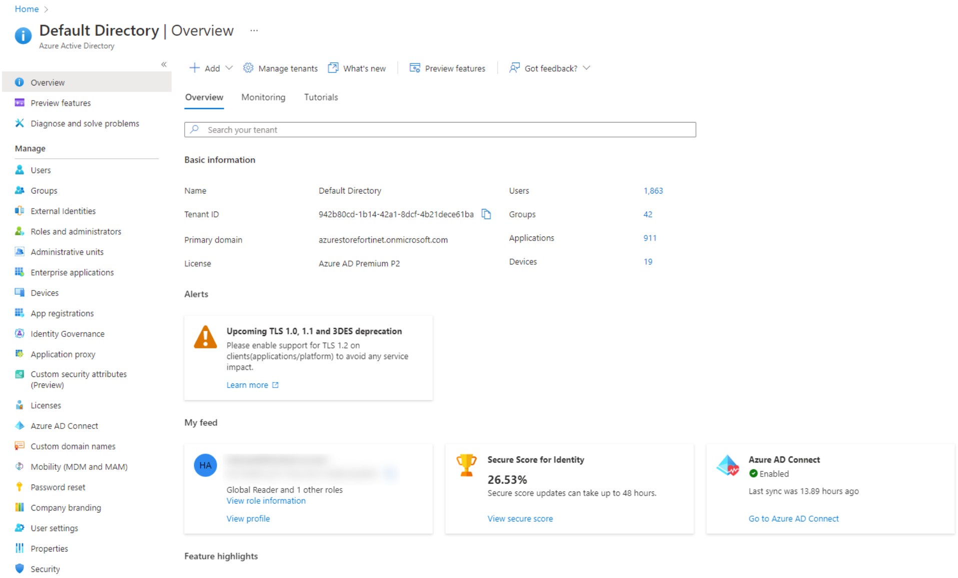
To configure SAML FSSO with FortiAuthenticator and Microsoft Azure AD:

1. Microsoft Azure related configurations:
   1. Creating a tenant in Azure Portal on page 227.
   2. Creating an enterprise application in Azure Portal on page 229.
   3. Setting up single sign-on for an enterprise application on page 230
      1. Adding a user group SAML attribute to the enterprise application on page 231.
      2. Adding users to an enterprise application on page 232.
   4. Adding the enterprise application as an assignment on page 232.
   5. Registering the enterprise application with Microsoft identity platform and generating authentication key on page 233.
2. FortiAuthenticator related configurations:
   1. Creating a remote OAuth server with Azure application ID and authentication key on page 233.
   2. Creating a remote SAML server on page 233.
   3. Setting up SAML SSO in FortiAuthenticator on page 235.
3. FortiGate related configurations:
   1. Adding an FSSO agent on page 235.
   2. Configuring an interface to use an external captive portal on page 236.
   3. Configuring a policy to allow a local network to access Microsoft Azure services on page 236.
   4. Creating an exempt policy to allow users to access the captive portal on page 237.
4. Results on page 238.

Creating a tenant in Azure Portal

To create a tenant:

1. Sign in to Microsoft Azure Portal.
2. In Azure portal, go to *Azure Active Directory*.
   The *Overview* page opens.



Home >

Default Directory | Overview

Azure Active Directory

Basic information

Name	Default Directory	Users	1,863
Tenant ID	942b80cd-1b14-42a1-8dcf-4b21dece61ba	Groups	42
Primary domain	azurestorefortinet.onmicrosoft.com	Applications	911
License	Azure AD Premium P2	Devices	19

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation

Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

Learn more

My feed

HA [redacted]

Global Reader and 1 other roles

View role information

View profile

Secure Score for Identity

26.53%

Secure score updates can take up to 48 hours.

View secure score

Azure AD Connect

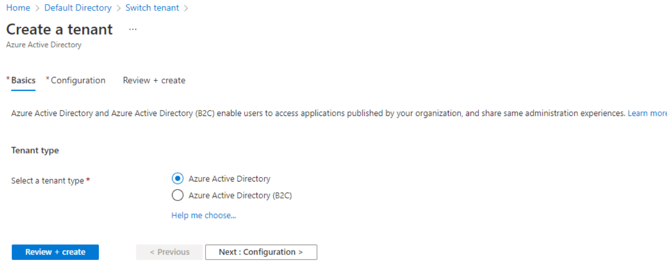
Enabled

Last sync was 13.89 hours ago

Go to Azure AD Connect

Feature highlights

3. In *Overview*, Select *Manage tenants*, and then select *Create*.
   Create a tenant window opens.
4. In the *Basics* tab, select *Azure Active Directory* as the tenant type, and select *Next: Configuration*.



Home > Default Directory > Switch tenant >

Create a tenant

Azure Active Directory

Azure Active Directory and Azure Active Directory (B2C) enable users to access applications published by your organization, and share same administration experiences. Learn more

Tenant type

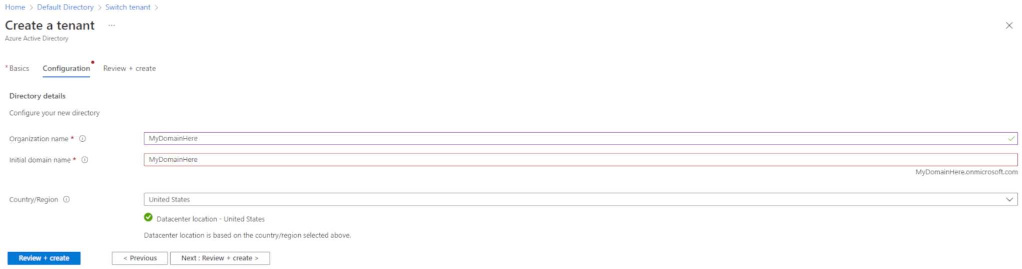
Select a tenant type *

● Azure Active Directory

○ Azure Active Directory (B2C)

Help me choose...

5. In *Configuration*, enter the *Organization name*, *Initial domain name*, and *Country/Region*.



Home > Default Directory > Switch tenant >

Create a tenant

Azure Active Directory

Directory details

Configure your new directory

Organization name * : MyDomainHere

Initial domain name * : MyDomainHere

MyDomainHere.onmicrosoft.com

Country/Region : United States

Datacenter location - United States

Datacenter location is based on the country/region selected above.

6. Select *Next: Review + create* to review the entries, and select *Create* to create the tenant.

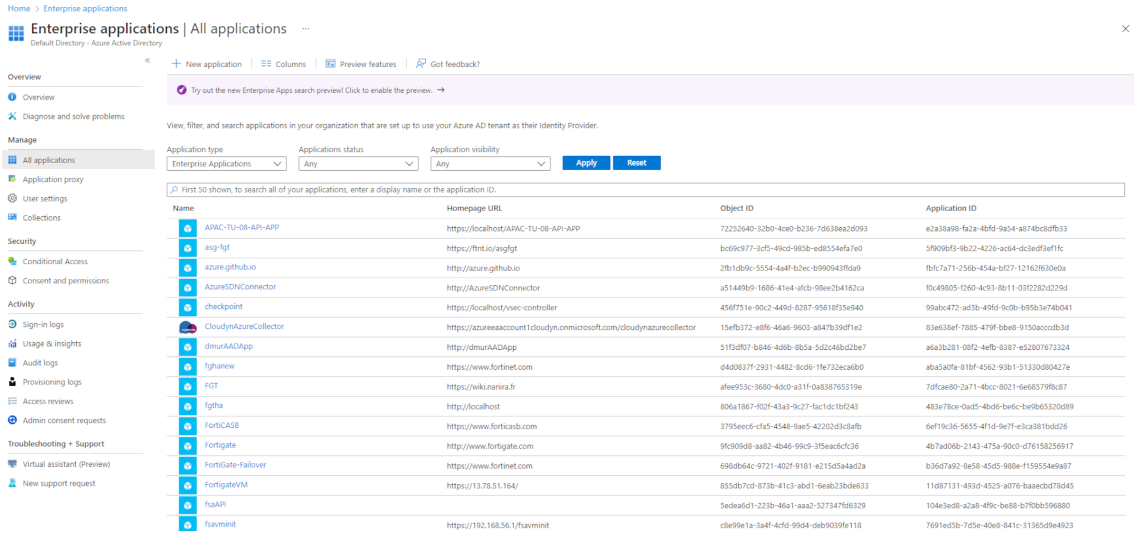
To switch to the correct directory:

1. Click the user icon on the top right.
2. Select *Switch directory*.
3. From the list, select *Switch* for the directory you intend to use.

Creating an enterprise application in Azure Portal

To create an enterprise application:

1. Go to *Azure Active Directory* > *Enterprise applications*.



Try out the new Enterprise Apps search preview! Click to enable the preview. →

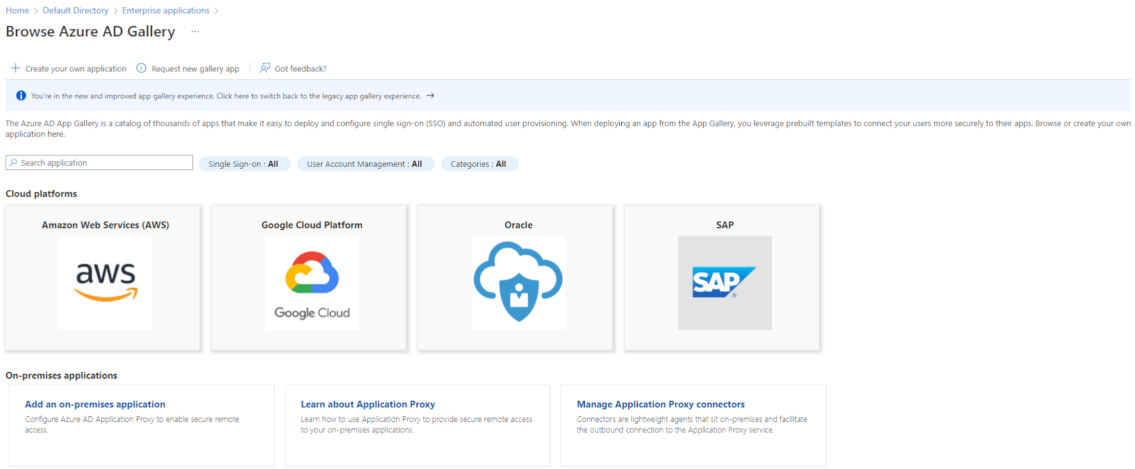
View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

Application type: Enterprise Applications
Applications status: Any
Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
APAC-TU-08-API-APP	https://localhost/APAC-TU-08-API-APP	72252640-32b0-4ce0-b236-7d638ea2d093	e2a38a98-fa2a-4bfd-9a54-a874bc8dfb33
asg-fgt	https://ftnt.io/asgfgt	bc69c977-3cf5-49cd-985b-ed8554efa7e0	5f909bf3-9b22-4226-ac64-dc3edf3ef1fc
azure.github.io	http://azure.github.io	2fb1db9c-5554-4a4f-b2ec-b990943ffda9	fbfc7a71-256b-454a-bf27-12162f630e0a
AzureSDNConnector	http://AzureSDNConnector	a51449b9-1686-41e4-afcb-98ee2b4162ca	f0c49805-f260-4c93-8b11-03f2282d229d
checkpoint	https://localhost/vsec-controller	456f751e-90c2-449d-8287-95618f35e940	99abc472-ad3b-49fd-9c0b-b95b3e74b041
CloudynAzureCollector	https://azureeaaccount1cloudyn.onmicrosoft.com/cloudynazurecollector	15efb372-e8f6-46a6-9603-a847b39df1e2	83e638ef-7885-479f-bbe8-9150acccdb3d
dmurAADApp	http://dmurAADApp	51f3df07-b846-4d6b-8b5a-5d2c46bd2be7	a6a3b281-08f2-4efb-8387-e52807673324
fghanew	https://www.fortinet.com	d4d0837f-2931-4482-8cd6-1fe732eca6b0	aba5a0fa-81bf-4562-93b1-51330d80427e
FGT	https://wiki.nanira.fr	afee953c-3680-4dc0-a31f-0a838765319e	7dfcae80-2a71-4bcc-8021-6e68579f8c87
fgtha	http://localhost	806a1867-f02f-43a3-9c27-fac1dc1bf243	483e78ce-0ad5-4bd6-be6c-be9b65320d89
FortiCASB	https://www.forticasb.com	3795eec6-cfa5-4548-9ae5-42202d3c8afb	6ef19c36-5655-4f1d-9e7f-e3ca381bdd26
Fortigate	http://www.fortigate.com	9fc909d8-aa82-4b46-99c9-3f5eac6cfc36	4b7ad06b-2143-475a-90c0-d76158256917
FortiGate-Failover	https://www.fortinet.com	698db64c-9721-402f-9181-e215d5a4ad2a	b36d7a92-8e58-45d5-988e-f159554e9a87
FortigateVM	https://13.78.51.164/	855db7cd-873b-41c3-abd1-6eab23bde633	11d87131-493d-4525-a076-baaecbd78d45
fsaAPI		5edea6d1-223b-46a1-aaa2-527347fd6329	104e3ed8-a2a8-4f9c-be88-b7f0bb596880
fsavminit	https://192.168.56.1/fsavminit	c8e99e1a-3a4f-4cfd-99d4-deb9039fe118	7691ed5b-7d5e-40e8-841c-31365d9e4923

2. In *Enterprise applications*, select *New application*.
   The *Browse Azure AD Gallery* page opens.



You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

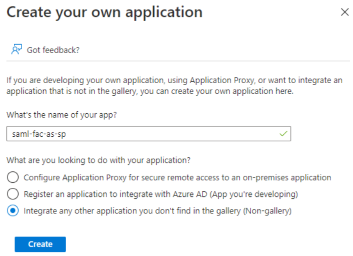
The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here.

Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

Manage Application Proxy connectors
Connectors are lightweight agents that sit on-premises and facilitate the outbound connection to the Application Proxy service.

3. In the *Browse Azure AD Gallery*, select *Create your own application*.
   The *Create your own application* window opens.
4. In the *Create your own application* window, enter a name for the application, and select *Create*.



If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?
saml-fac-as-sp

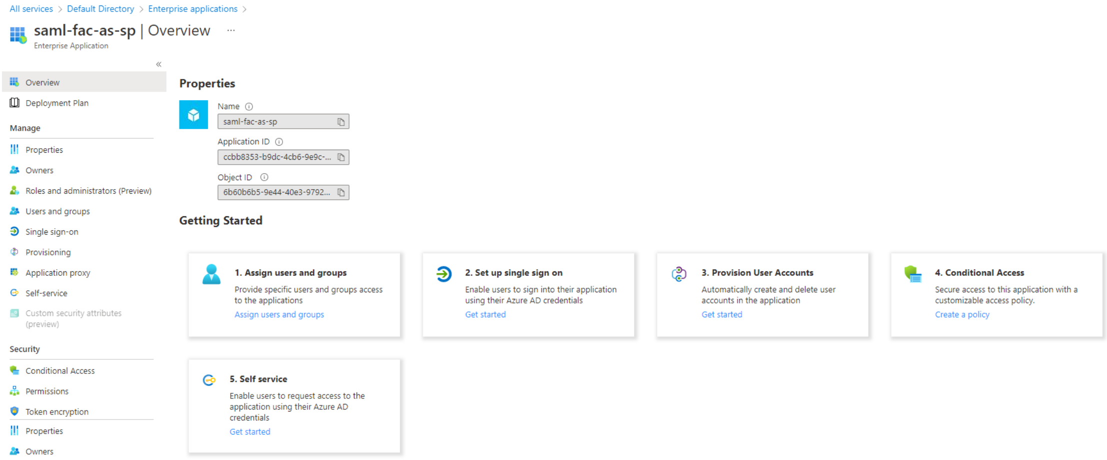
What are you looking to do with your application?
○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

Setting up single sign-on for an enterprise application

Once the application is created, you can set up single sign-on for your application.

To set up single sign-on:

1. Go to *Azure Active Directory* > *Enterprise applications*.
2. In *Enterprise applications*, enter the name of your enterprise application in the search bar, and click the application to open it.
   See Creating an enterprise application in Azure Portal on page 229.



Name: saml-fac-as-sp

Application ID: ccbb8353-b9dc-4cb6-9e9c-...

Object ID: 6b60b6b5-9e44-40e3-9792...

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

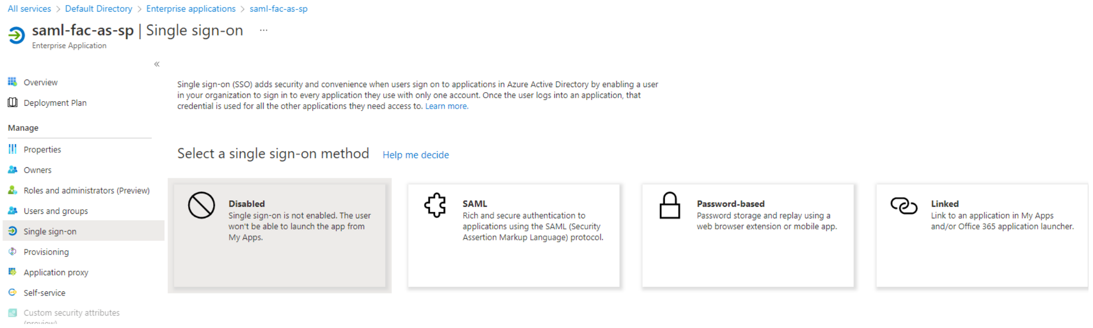
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

3. Select *Get Started* in *Set up single sign on*.
4. In *Single sign-on*, select *SAML*.


All services > Default Directory > Enterprise applications > saml-fac-as-sp
saml-fac-as-sp | Single sign-on ···
Enterprise Application
«
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes (preview)
Select a single sign-on method
Help me decide

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

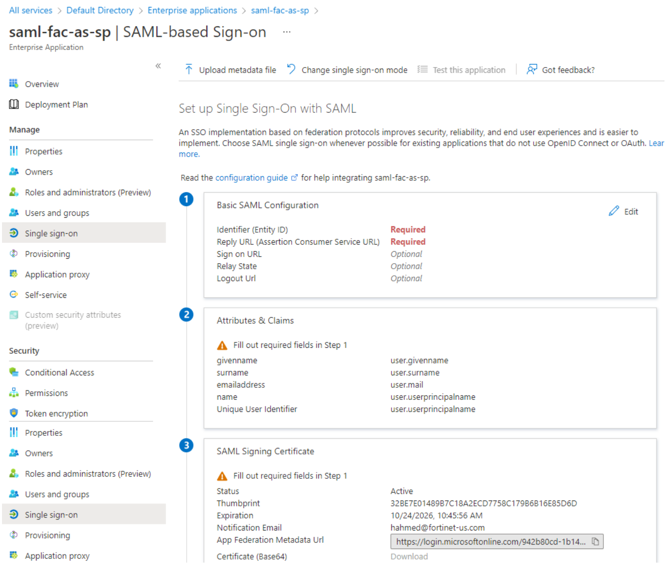
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

The *SAML-based Sign-on* window opens.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Lear more.

Read the configuration guide for help integrating saml-fac-as-sp.

Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

Attributes & Claims

⚠ Fill out required fields in Step 1

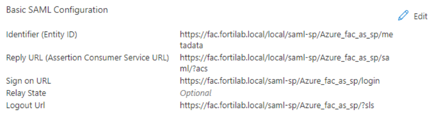
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

⚠ Fill out required fields in Step 1

Status	Active
Thumbprint	32BE7E01489B7C18A2ECD7758C179B6B16E85D6D
Expiration	10/24/2026, 10:45:56 AM
Notification Email	hahmed@fortinet-us.com
App Federation Metadata Url	https://login.microsoftonline.com/942b80cd-1b14...
Certificate (Base64)	Download

5. In the *SAML-based Sign-on* window, select *Edit* in the *Basic SAML Configuration* pane.
6. In the *Basic SAML Configuration* window, enter the following information from the FortiAuthenticator SP:
   a. In *Identifier (Entity ID)*, enter the SP entity ID.
   b. In *Reply URL (Assertion Consumer Service URL)*, enter the URL where the application receives the authentication token.
   c. In *Sign on URL*, enter the URL for the sign-in page for the application.
   d. In *Relay State*, enter the URL to which the user is redirected to by the SP after a successful assertion response.
   e. In *Logout Url*, enter the URL used to send the SAML logout response back to the application.
   f. Click *Save*.



Basic SAML Configuration

Identifier (Entity ID)	https://fac.fortilab.local/local/saml-sp/Azure_fac_as_sp/metadata
Reply URL (Assertion Consumer Service URL)	https://fac.fortilab.local/local/saml-sp/Azure_fac_as_sp/saml/?acs
Sign on URL	https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/login
Relay State	*Optional*
Logout Url	https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/?sls

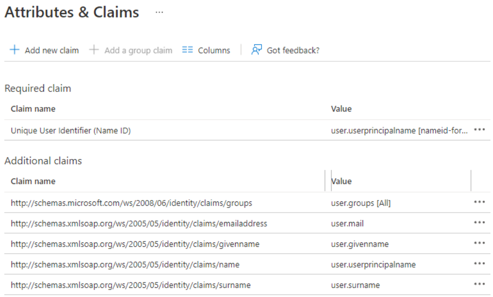
See Adding a user group SAML attribute to the enterprise application on page 231 and Adding users to an enterprise application on page 232.

Adding a user group SAML attribute to the enterprise application

To add a user group SAML attribute:

1. In the *SAML-based Sign-on* window that opens after step 4 in Setting up single sign-on for an enterprise application on page 230, go to the *Attributes & Claims* pane, and select *Edit*.
2. In the *Attributes & Claims* window, select *Add a group claim*.
   The *Group Claims* window opens.
3. In the *Group Claims* window, select *All groups* in *Which groups associated with the user should be returned in the claim?* and then click *Save*.

The *Attributes and Claims* window is updated to include a group claim.



Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... •••

Additional claims

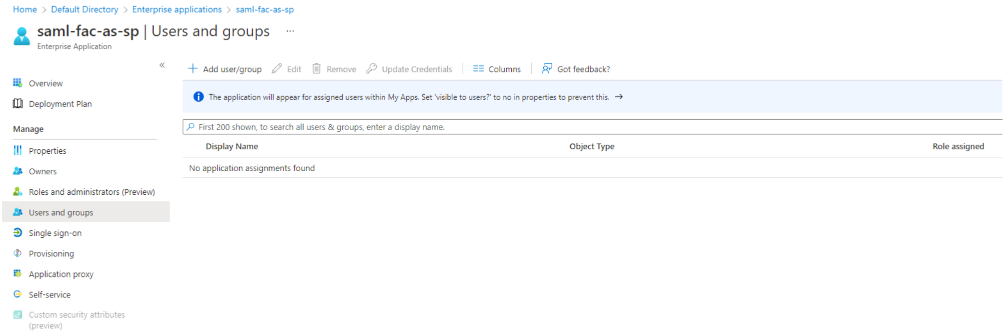
Claim name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups [All] •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname •••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname •••

In the *SAML Signing Certificate* pane, download the certificate file (base64) needed to configure the remote SAML server.

Adding users to an enterprise application

To add users:

1. In the *SAML-based Sign-on* window that opens after step 4 in Setting up single sign-on for an enterprise application on page 230, go to *Users and Groups*.



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
No application assignments found		

2. Select *Add user/group* and then select *None Selected* to open the *Users and groups* window.
3. In the *Users and groups* window, search the name of the user(s) and select *Select* to include all users able to authenticate using the enterprise application.
4. Select *Assign* to add the user(s).

Go to *Manage* > *Properties* and make note of the *Application ID* required when setting up an OAuth server.

Adding the enterprise application as an assignment

To add the enterprise application as an assignment:

1. Go to the directory home, and select *Roles and administrators*.
2. From the *Administrative roles* list, select *Directory readers*.

3. Select ellipsis for *Directory readers* and then select *Description*.
4. Go to *Assignments* and select *Add assignment*.
5. In the *Add assignments* window, search your application by name, and select *Add*.

Registering the enterprise application with Microsoft identity platform and generating authentication key

To register the enterprise application:

1. Go to the directory home, and select *App registrations*.
2. In the *App registrations* window, select *All applications*, and search your application by name.
3. In the list, select your application.
4. Go to *Manage* > *Certificates & secrets*, and select + *New client secret*.
5. In the *Add a client secret* window:
    a. In *Description*, enter a description for the client secret.
    b. From the *Expires* dropdown, select a time period after which the client secret expires.
    c. Select *Add*.

> In *Client secrets*, make note of the *Value*.
>
> Since this key is visible only once (immediately after creation), you will have to recreate the key if you do not copy and store it.
>
> The key is required when setting up an OAuth server.

Creating a remote OAuth server with Azure application ID and authentication key

To create a remote OAuth server:

1. Go to *Authentication* > *Remote Auth. Servers* > *OAUTH* and select *Create New*.
   The *Create New Remote OAuth Server* window appears.
2. Enter a name for the remote OAuth server.
3. In the *OAuth source* dropdown, select *Azure Directory*.
4. In *Client ID*, enter the application id that you saved when Adding users to an enterprise application on page 232.
5. In *Client Key*, enter the authentication key created in Registering the enterprise application with Microsoft identity platform and generating authentication key on page 233.
6. Enable *Include for SSO*, and in *Azure AD tenant ID*, enter your Microsoft Entra ID tenant ID.
7. Select *OK* to add the remote OAuth server.

Creating a remote SAML server

To create a remote SAML server:

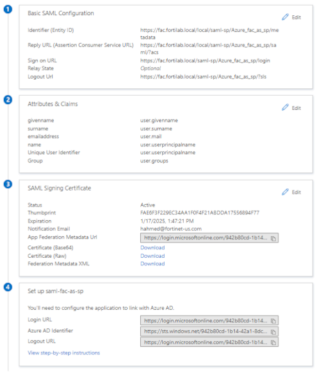
1. Go to *Authentication* > *Remote Auth. Servers* > *SAML* and select *Create New*.
   The *Create New Remote SAML Server* window opens.

2. Enter a name for the remote SAML server.
   The name of the remote SAML server is then used when configuring SAML single sign-on in Azure.
3. Select *Type* as *FSSO*.

> The *Portal URL* is the *Sign on URL* in the *SAML-based Sign-on* window in *Azure Active Directory > Enterprise applications* on the Azure portal.

4. In *Entity ID*, enter the SAML SP entity ID.
   The *Entity ID* is the *Identifier (Entity ID)* in the Azure portal.
5. In *IdP entity ID*, enter the unique name of the SAML IdP.
   The *IdP entity ID* is *Azure AD Identifier* in the Azure portal.
6. In *IdP single sign-on URL*, enter the identity provider portal URL you want to use for SSO.
   The *IdP single sign-on URL* is *Login URL* in the Azure portal.
7. In *IdP certificate fingerprint*:
   a. Select *Import Certificate*.
   b. In the *Import Certificate* dialog, select *Upload a file*, browse to the certificate file (base64) you saved earlier, click *Open*, and then click *OK*.
8. Select *Enable SAML single logout* and enter the URL used to send the SAML logout response back to the application in *IdP single logout URL*.
   The *IdP single logout URL* is the *Logout URL* in the Azure portal.
9. In the *Username* pane, select *Text SAML assertion*, enter the text-based SAML assertion that usernames are obtained from.
10. In the *Group Membership* pane:
    a. In *Obtain group membership from*, select *Cloud*.
    b. In the *OAuth server* dropdown, select the remote OAuth server created in Creating a remote OAuth server with Azure application ID and authentication key on page 233
11. Click *OK*.

The following shows the relation between the Microsoft Azure AD IdP and the remote SAML server.



1 Basic SAML Configuration — Edit

Identifier (Entity ID): https://fac.fortilab.local/local/saml-sp/Azure_fac_as_sp/metadata
Reply URL (Assertion Consumer Service URL): https://fac.fortilab.local/local/saml-sp/Azure_fac_as_sp/saml/?acs
Sign on URL: https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/login
Relay State: *Optional*
Logout Url: https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/?sls

2 Attributes & Claims — Edit

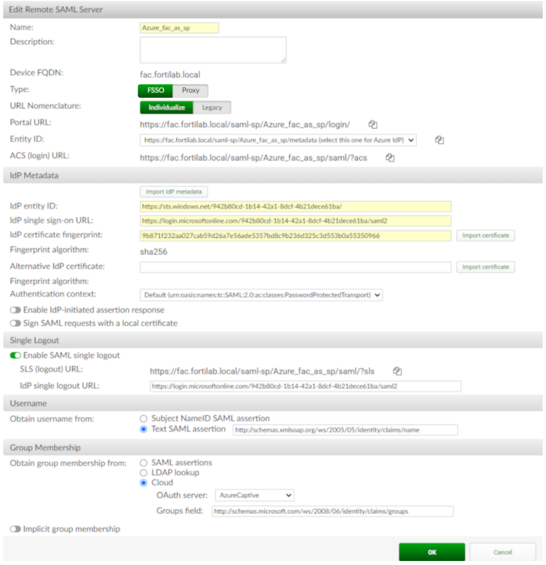
givenname: user.givenname
surname: user.surname
emailaddress: user.mail
name: user.userprincipalname
Unique User Identifier: user.userprincipalname
Group: user.groups

3 SAML Signing Certificate — Edit

Status: Active
Thumbprint: FAE6F3F229EC34AA1F0F4F21ABDDA17556894F77
Expiration: 1/17/2025, 1:47:21 PM
Notification Email: hahmed@fortinet-us.com
App Federation Metadata Url: https://login.microsoftonline.com/942b80cd-1b14...
Certificate (Base64): Download
Certificate (Raw): Download
Federation Metadata XML: Download

4 Set up saml-fac-as-sp

You'll need to configure the application to link with Azure AD.
Login URL: https://login.microsoftonline.com/942b80cd-1b14...
Azure AD Identifier: https://sts.windows.net/942b80cd-1b14-42a1-8dc...
Logout URL: https://login.microsoftonline.com/942b80cd-1b14...
View step-by-step instructions



Edit Remote SAML Server

Name: Azure_fac_as_sp
Description:
Device FQDN: fac.fortilab.local
Type: FSSO | Proxy
URL Nomenclature: Individualize | Legacy
Portal URL: https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/login/
Entity ID: https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/metadata (select this one for Azure IdP)
ACS (login) URL: https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/saml/?acs

IdP Metadata

Import IdP metadata
IdP entity ID: https://sts.windows.net/942b80cd-1b14-42a1-8dcf-4b21dece61ba/
IdP single sign-on URL: https://login.microsoftonline.com/942b80cd-1b14-42a1-8dcf-4b21dece61ba/saml2
IdP certificate fingerprint: 9b871f232aa027cab59d26a7e56ade5357bd8c9b236d325c3d553b0a55350966 — Import certificate
Fingerprint algorithm: sha256
Alternative IdP certificate: — Import certificate
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
SLS (logout) URL: https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/saml/?sls
IdP single logout URL: https://login.microsoftonline.com/942b80cd-1b14-42a1-8dcf-4b21dece61ba/saml2

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: AzureCaptive
Groups field: http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

Implicit group membership

Setting up SAML SSO in FortiAuthenticator

To enable SAML portal:

1. Go to *Fortinet SSO Methods* > *SSO* > *Portal Services*.
2. In the *Edit Portal Services Settings* window, select *Enable SAML portal* to enable SAML portal log in for SSO.
3. Click *OK*.

To configure SAML SSO authentication to use Azure SAML IdP:

1. Go to *Fortinet SSO Methods* > *SSO* > *SAML Authentication* and select *Create New*.
   The *Create New SAML Identity Provider* window opens.
2. In *Remote SAML server* dropdown, select the remote SAML server created in Creating a remote SAML server on page 233.
3. In the *Domain Membership* pane, enable *Get SSO domain name from*, and select *Username prefix/suffix* to obtain the domain name specified in the username.
4. Click *OK* to create the new SAML SP portal.

To enable FSSO for FortiGate and define a password:

1. Go to *Fortinet SSO Methods* > *SSO* > *General* to open the *Edit SSO Configuration* window.
2. In the *FortiGate* pane, select *Enable authentication*, then enter a secret key, or password, in the *Secret key* field.
3. Click *OK*.

To create a FortiGate filter and include the groups from Azure AD:

1. Go to *Fortinet SSO Methods* > *SSO* > *FortiGate Filtering* and select *Create New*.
   The *Create New FortiGate Filter* window opens.
2. Enter a name to identify the filter.
3. In *FortiGate name/IP*, enter FortiGate unit's FQDN or IP address.
4. In *Fortinet Single Sign-On (FSSO)* pane, enable *Forward FSSO information for users from the following subset of users/groups/containers only*, and include the groups from Azure AD you intend to send information to the FortiGate.
5. Click *OK*.

Adding an FSSO agent

To add an FSSO agent:

1. Go to *Security Fabric* > *External Connectors* and select *Create New*.
   The *New External Connector* window opens.
2. In the *Endpoint/Identity* pane, select *FSSO Agent on Windows AD*.

3. In the *Connector Settings* pane:
   a. Enter a name for the FSSO agent.
   b. In *Primary FSSO agent*, enter the FortiAuthenticator SP IP address, and enter a password.

   Select *View* next to *Users/Groups* to view the groups you previously added in FortiAuthenticator.

4. Click *Apply and Refresh* and then click *OK*.

Configuring an interface to use an external captive portal

To configure an interface:

1. Go to *Network* > *Interfaces*.
2. Select *Create New* > *Interface*.
   The *New Interface window* opens.
3. Enter a name for the interface. Optionally, enter an alias.
4. In *Type*, select *802.3ad Aggregate*.
5. In the *Role* dropdown, select *LAN*.
6. In the *Address* pane:
   a. In *Addressing mode*, select *Manual*.
   b. In *IP/Netmask*, enter an IP address/netmask for the interface.
   c. In *IPv6 addressing* mode, select *Manual*.
   d. Disable *Create address object matching subnet*.
7. In the *Network* pane:
   a. Enable *Device detection*.
   b. Enable *Security mode*, and from the dropdown, select *Captive Portal*.
   c. In *Authentication portal*, select *External*, and enter the captive portal URL.

   The captive portal URL points to `samlsp/[saml-sp-name]/login/` where `[saml-sp-name]` is the remote SAML server name in creating a remote SAML server.

   d. Optionally, in *User access*, select *Restricted to Groups*, and then select groups for *User Groups*.
8. Click *OK*.

Configuring a policy to allow a local network to access Microsoft Azure services

To configure a policy:

1. Go to *Policy & Objects* > *Firewall Policy* and select *Create New*.
2. Enter a name for the policy.
3. In *Incoming Interface*, select the interface created to use an external captive portal.
4. In *Outgoing Interface*, select the interface for virtual WAN.

5. In *Source*:
   a. Select + to open the *Select Entries* window.
   b. *In Address*, search and select *all*.
   c. Select *Close*.
6. In *Destination*:
   a. Select + to open the *Select Entries* window.
   b. In *Internet Service*, search and select *Microsoft-Azure*.
   c. Select *Close*.
7. In *Advanced* pane, enable *Exempt Captive Portal* to exempt this policy from the captive portal.

   To make the *Advanced* pane visible:
   - Go to *System* > *Feature Visibility*.
   - Enable *Policy Advanced Options*.
   - Click *Apply*.

8. Click *OK*.

Creating an exempt policy to allow users to access the captive portal

If the FortiAuthenticator is not in the local user's network, you need to create an exempt policy allowing users to access the FortiAuthenticator and reach the captive portal.

To create an exempt policy:

1. Go to *Policy & Objects* > *Firewall Policy* and select *Create New*.
2. Enter a policy name.
3. In *Incoming Interface*, select the interface created to use an external captive portal.
4. In *Outgoing Interface*, select the interface for DMZ.
5. In *Source*:
   a. Select + to open the *Select Entries* window.
   b. *In Address*, search and select *all*.
   c. Select *Close*.
6. In *Destination*:
   a. Select + to open the *Select Entries* window.
   b. In *Address*, select *Create* > *Address*, and in the *New Address* window, enter details related to the FortiAuthenticator SP. Click *OK*.
   c. Select *Close*.
7. In *Service*:
   a. Select + to open the *Select Entries* window.
   b. Search and select *HTTPS*.
   c. Select *Close*.
8. In the *Firewall/Network Options* pane, disable *NAT*.

9. In *Advanced* pane, enable *Exempt Captive Portal* to exempt this policy from the captive portal.

   To make the *Advanced* pane visible:

   - Go to *System* > *Feature Visibility*.
   - Enable *Policy Advanced Options*.
   - Click *Apply*.

10. Click *OK*.

Results

1. Once the user attempts to access the SP, they are redirected to Azure for authentication.
2. After entering the credentials, user receives the information that the login was successful.
   The SSO session is visible in both FortiAuthenticator and FortiGate:
   - In FortiAuthenticator: *Monitor* > *SSO* > *SSO Sessions*.
   - In FortiGate: *Dashboard* > *User & Devices*.

Office 365 SAML authentication using FortiAuthenticator with 2FA in Azure/ADFS hybrid environment

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, and that ADFS is set up as a SAML IdP.

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

1. Configure FortiAuthenticator as an SP in ADFS on page 238
2. Configure the remote SAML server on FortiAuthenticator on page 239
3. Configure SAML settings on FortiAuthenticator on page 240
4. Configure two-factor authentication on FortiAuthenticator on page 241
5. Configure FortiAuthenticator replacement messages on page 242
6. Results on page 242

Configure FortiAuthenticator as an SP in ADFS

On your ADFS IdP, configure FortiAuthenticator as a SAML SP and return the following SAML assertions:

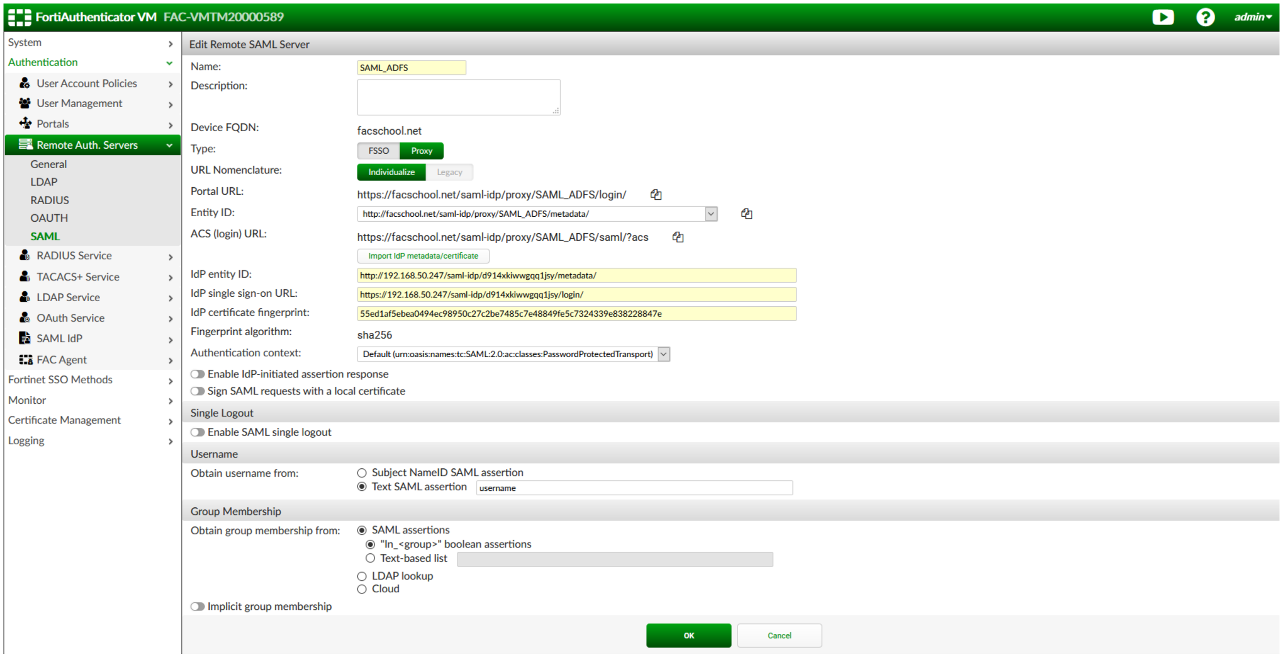
- **Type**: *Proxy*
- **Subject NameID**: *MS-DS-consistencyGUID*
- **IDPEmail**: *userPrincipalName*
- **username**: *sAMAccountName*

Configure the remote SAML server on FortiAuthenticator

Configure a remote SAML server connected to the ADFS IdP.

To configure the remote SAML server on FortiAuthenticator:

1. Go to *Authentication* > *Remote Auth. Servers* > *SAML* and click *Create New*.
2. Configure the remote SAML server:
    a. **Name**: Provide a name for the remote SAML server.
    b. **Type**: *Proxy*
    c. **IdP Settings**: Enter the *IdP entity ID*, *IdP Single sign-on URL*, and *IdP certificate fingerprint* obtained from your ADFS IdP.
    d. **Obtain username from**: Select *Text SAML Assertion* and enter `username`.
3. Click *OK* to save your changes.



Edit Remote SAML Server

Name:	SAML_ADFS
Description:	
Device FQDN:	facschool.net
Type:	FSSO [✓ Proxy]
URL Nomenclature:	[✓ Individualize] Legacy
Portal URL:	https://facschool.net/saml-idp/proxy/SAML_ADFS/login/
Entity ID:	http://facschool.net/saml-idp/proxy/SAML_ADFS/metadata/
ACS (login) URL:	https://facschool.net/saml-idp/proxy/SAML_ADFS/saml/?acs
IdP entity ID:	http://192.168.50.247/saml-idp/d914xkiwwgqq1jsy/metadata/
IdP single sign-on URL:	https://192.168.50.247/saml-idp/d914xkiwwgqq1jsy/login/
IdP certificate fingerprint:	55ed1af5ebea0494ec98950c27c2be7485c7e48849fe5c7324339e838228847e
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 username

Group Membership

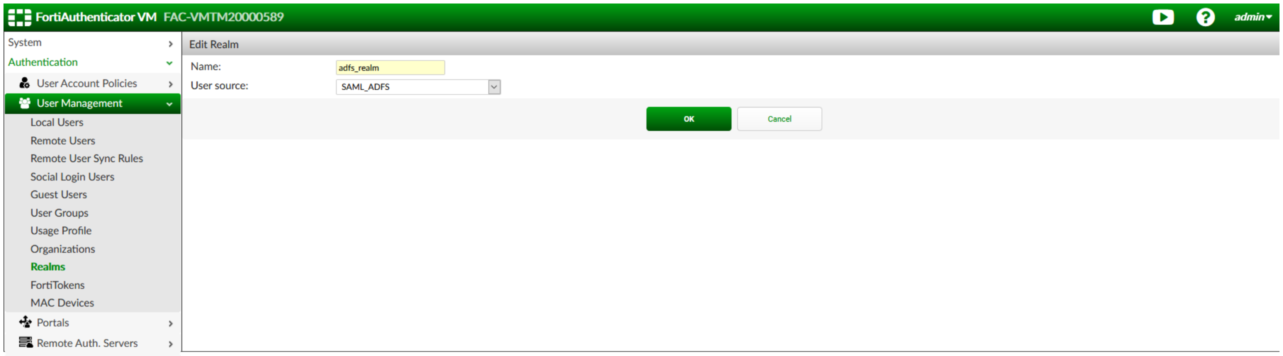
Obtain group membership from: ● SAML assertions
● "In_<group>" boolean assertions
○ Text-based list
○ LDAP lookup
○ Cloud

Implicit group membership

To configure the ADFS realm:

1. Go to *Authentication* > *User Management* > *Realms* and click *Create New*.
2. Configure a name for the realm and select your remote SAML server as the *User source*.

3. Click *OK* to save your changes.



Edit Realm

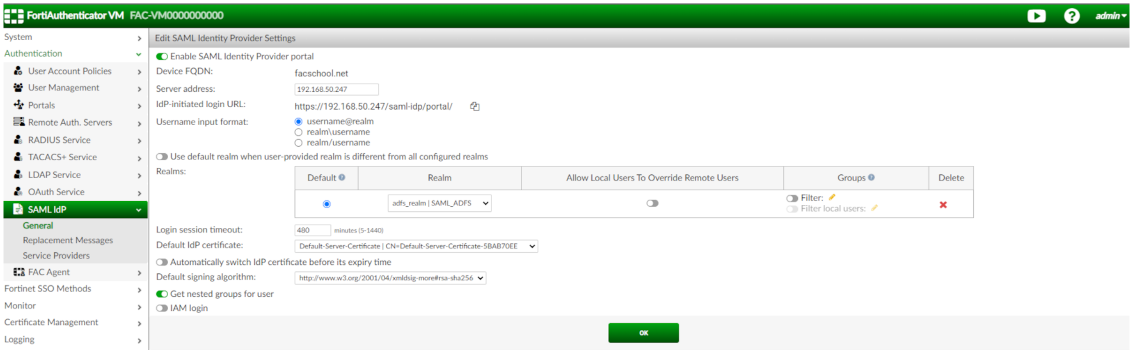
Name: adfs_realm

User source: SAML_ADFS

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 SAML 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.
3. Click *OK* to save your changes.



Edit SAML Identity Provider Settings

Enable SAML Identity Provider portal

Device FQDN: facschool.net

Server address: 192.168.50.247

IdP-initiated login URL: https://192.168.50.247/saml-idp/portal/

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

Use default realm when user-provided realm is different from all configured realms

Realms:

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

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: Default-Server-Certificate | CN=Default-Server-Certificate-5BAB70EE

Automatically switch IdP certificate before its expiry time

Default signing algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

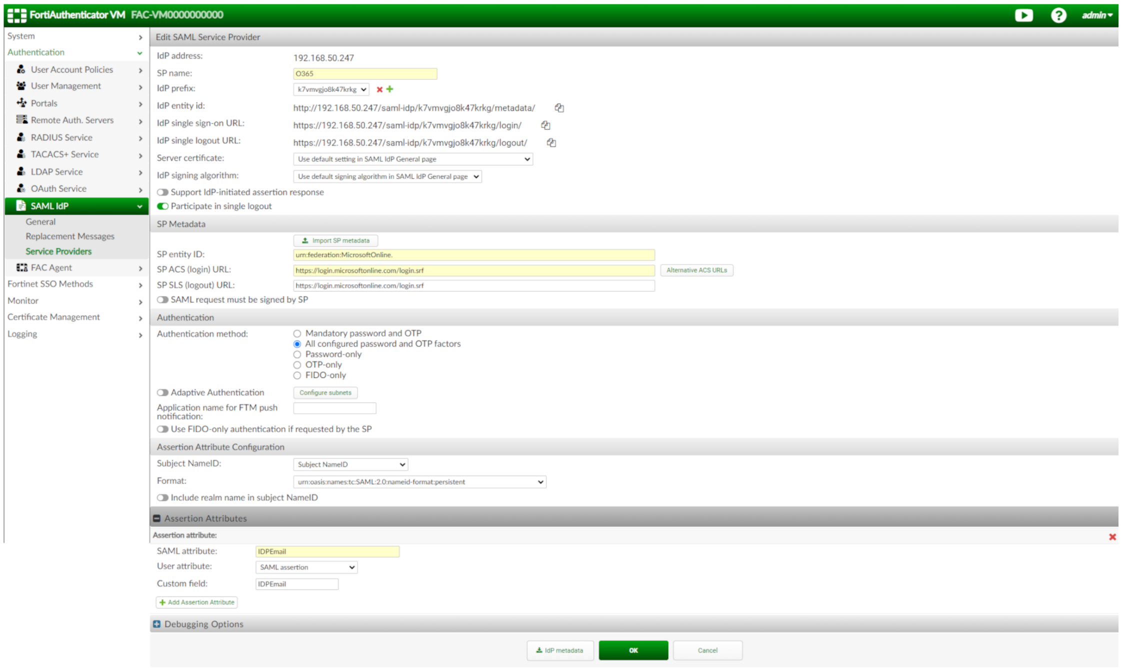
Get nested groups for user

IAM login

To configure the O365 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 O365 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. **IdP signing algorithm**: Select *Use default signing algorithm in SAML IdP General page*.
   e. **Participate in single logout**: Can be enabled if you wish this SP to participate in SAML single logout.
3. In the *Assertion Attribute Configuration* section, configure the following settings:
   a. **Subject NameID**: Select *Subject NameID*.
   b. **Format**: Select *urn:oasis:names:tc:SAML:2.0:nameid-format:persistent*.

4. Click *Save* and the *SP Metadata* and *Assertion Attribute* fields are displayed. Configure the following settings for the SP Metadata.
   a. **SP entity ID**: Enter `urn:federation:MicrosoftOnline`.
   b. **SP ACS (login) URL**: Enter `https://login.microsoftonline.com/login.srf`.
   c. **SP SLS (logout) URL**: Enter `https://login.microsoftonline.com/login.srf`.
5. In *Assertion Attributes* click *Create New* and configure the following assertion attribute:
   a. **SAML attribute**: *IDPEmail*
   b. **User attribute**: *SAML assertion*
   c. **Custom field**: *IDPEmail*
6. Save your changes to the SAML SP.



Edit SAML Service Provider

IdP address: 192.168.50.247
SP name: O365
IdP prefix: k7vmvgjo8k47krkg
IdP entity id: http://192.168.50.247/saml-idp/k7vmvgjo8k47krkg/metadata/
IdP single sign-on URL: https://192.168.50.247/saml-idp/k7vmvgjo8k47krkg/login/
IdP single logout URL: https://192.168.50.247/saml-idp/k7vmvgjo8k47krkg/logout/
Server certificate: Use default setting in SAML IdP General page
IdP signing algorithm: Use default signing algorithm in SAML IdP General page
Support IdP-initiated assertion response
Participate in single logout

SP Metadata

Import SP metadata
SP entity ID: urn:federation:MicrosoftOnline.
SP ACS (login) URL: https://login.microsoftonline.com/login.srf
Alternative ACS URLs
SP SLS (logout) URL: https://login.microsoftonline.com/login.srf
SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory password and OTP
● All configured password and OTP factors
○ Password-only
○ OTP-only
○ FIDO-only

Adaptive Authentication
Configure subnets
Application name for FTM push notification:
Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

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

Assertion Attributes

Assertion attribute:
SAML attribute: IDPEmail
User attribute: SAML assertion
Custom field: IDPEmail
Add Assertion Attribute

Debugging Options

IdP metadata
OK
Cancel

Configure two-factor authentication on FortiAuthenticator

To configure a remote user sync rule:

1. Go to *Authentication > User Management > Remote User Sync Rules*, choose *SAML* and then click *Create New*.
2. Configure the following settings:
   a. **Name**: Enter a name for the sync rule (e.g. SAML Users).
   b. **Remote SAML server**: Select the previously configured remote SAML 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)*.
4. Select or create a user group to associate users with from the dropdown menu.
5. In *SAML User Mapping Attributes*, set the *Username* field to `sAMAccountName`.
6. The remaining settings can be configured to your preference or left in their default state.
7. Click *OK* to save your changes when completed.

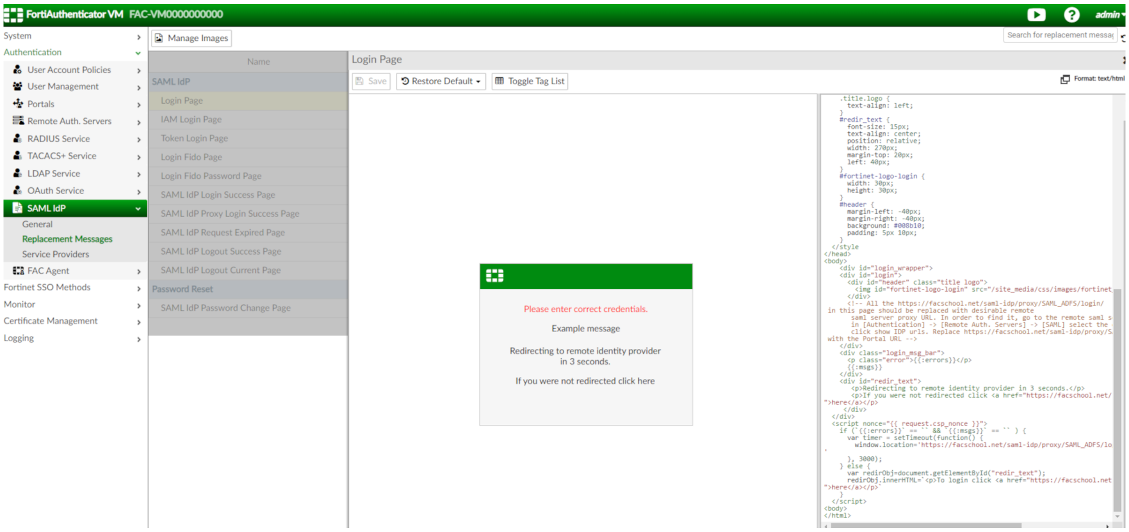
To configure remote users with two-factor authentication:

1. Go to *Authentication* > *User Management* > *Remote Users* and *Import* users from the remote SAML account.
2. Edit a user and enable *One-Time Password (OTP) authentication*, and select *FortiToken* > *Cloud* as the delivery method.
3. Click *OK* to save your changes.

Configure FortiAuthenticator replacement messages

To configure the FortiAuthenticator replacement messages:

1. Go to *Authentication* > *SAML IdP* > *Replacement Messages*, and click the *Login Page* replacement message.
2. Click Restore Default in the replacement message toolbar and select *idp-proxy*.
3. On the right side of the screen you can edit the replacement message's HTML. Follow the instructions included in the HTML to replace *[proxy_portal_url]* with the ADFS portal URL.
4. Click *Save*.



Please enter correct credentials.

Example message

Redirecting to remote identity provider in 3 seconds.

If you were not redirected click here

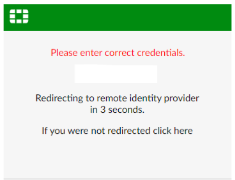
```
    .title.logo {
      text-align: left;
    }
    #redir_text {
      font-size: 15px;
      text-align: center;
      position: relative;
      width: 270px;
      margin-top: 20px;
      left: 40px;
    }
    #fortinet-logo-login {
      width: 30px;
      height: 30px;
    }
    #header {
      margin-left: -40px;
      margin-right: -40px;
      background: #008b10;
      padding: 5px 10px;
    }
  </style
</head>
<body>
    <div id="login_wrapper">
    <div id="login">
      <div id="header" class="title logo">
        <img id="fortinet-logo-login" src="/site_media/css/images/fortinet
      </div>
      <!-- All the https://facschool.net/saml-idp/proxy/SAML_ADFS/login/
 in this page should be replaced with desirable remote
       saml server proxy URL. In order to find it, go to the remote saml s
       in [Authentication] -> [Remote Auth. Servers] -> [SAML] select the
       click show IDP urls. Replace https://facschool.net/saml-idp/proxy/S
 with the Portal URL -->
    </div>
    <div class="login_msg_bar">
      <p class="error">{{:errors}}</p>
      {{:msgs}}
    </div>
    <div id="redir_text">
       <p>Redirecting to remote identity provider in 3 seconds.</p>
       <p>If you were not redirected click <a href="https://facschool.net/
">here</a></p>
     </div>
  </div>
  <script nonce="{{ request.csp_nonce }}">
    if (`{{:errors}}` == `` && `{{:msgs}}` == `` ) {
      var timer = setTimeout(function() {
        window.location='https://facschool.net/saml-idp/proxy/SAML_ADFS/lo
'
      }, 3000);
    } else {
      var redirObj=document.getElementById("redir_text");
      redirObj.innerHTML=`<p>To login click <a href="https://facschool.net
">here</a></p>`
    }
  </script>
<body>
</html>
```

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. When the user attempts to access the Office 365 SP, they are redirected to the ADFS SAML IdP.



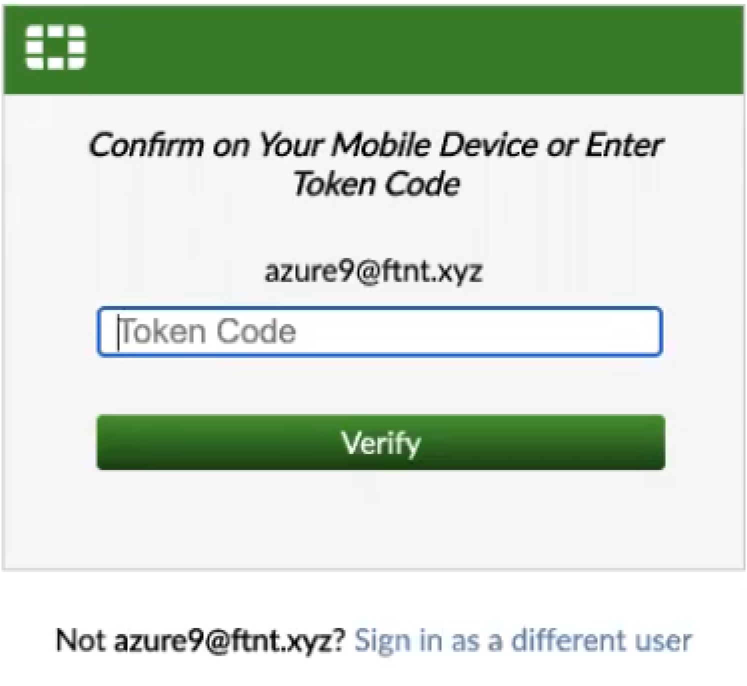
Please enter correct credentials.

Redirecting to remote identity provider in 3 seconds.

If you were not redirected click here

2. In the ADFS server login page, enter username and password.

3. 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.

SSL VPN SAML authentication using FortiAuthenticator with OneLogin as SAML IdP

Using this example, you can set up a SAML authentication based SSL VPN configuration with OneLogin as the IdP.

FortiAuthenticator and OneLogin configurations must be set up in parallel to generate the required SAML URL and certificate information.

Following the example you can connect to an SSL VPN configured FortiGate with your account validated by OneLogin using FortiAuthenticator as an IdP proxy.

In this example:

- FortiAuthenticator is as an IdP proxy to OneLogin, i.e., FortiAuthenticator IdP proxy receives SAML authentication requests to OneLogin and users are validated against the OneLogin user database.
- FortiAuthenticator is as an IdP to local resources. SAML clients act as SAML SP to FortiAuthenticator. FortiAuthenticator uses local or remote databases for user authentication.

User validation is done using OneLogin user database.

- FortiGate is an SSL VPN gateway and acts as an SP for FortiAuthenticator.

VPN user authentication requests are sent to FortiAuthenticator for validation.

- OneLogin is used to create an advanced SAML custom connector.
- OneLogin acts as an IdP for FortiAuthenticator.

Prerequisites and scope of the recipe

1. Access to a valid OneLogin account.
2. IP connectivity to FortiAuthenticator is already done.
3. FortiGate SSL VPN is already configured.
4. OneLogin MFA related configuration are beyond the scope of this recipe.

FortiGate 7.0.3 and OneLogin- SAML Custom Connector (Advanced)- SAML 2.0 are used in this recipe.

To configure SSL VPN SAML authentication with OneLogin as SAML IdP:

1. OneLogin related configurations:
   a. Creating an OneLogin application on page 245
   b. Configuring an application on OneLogin on page 245
      i. Configuring application parameters on OneLogin on page 247
      ii. Configuring SSO on OneLogin on page 248
   c. Granting user access to the application on page 249
2. FortiAuthenticator related configurations:
   a. Configuring a remote SAML server on page 250
   b. Configuring an OneLogin realm on page 252
   c. Creating remote SAML users on page 252
   d. Configuring SAML IdP settings on page 253
   e. Configuring FortiAuthenticator replacement message on page 254
   f. Configuring FortiGate SP settings on FortiAuthenticator on page 254
3. FortiGate related configurations:
   a. Uploading SAML IdP certificate to the FortiGate SP on page 256
   b. Creating SAML user and server on page 257
   c. Mapping SSL VPN authentication portal on page 259
   d. Increasing remote authentication timeout using FortiGate CLI on page 260
   e. Configuring a policy to allow users access to allowed network resources on page 260

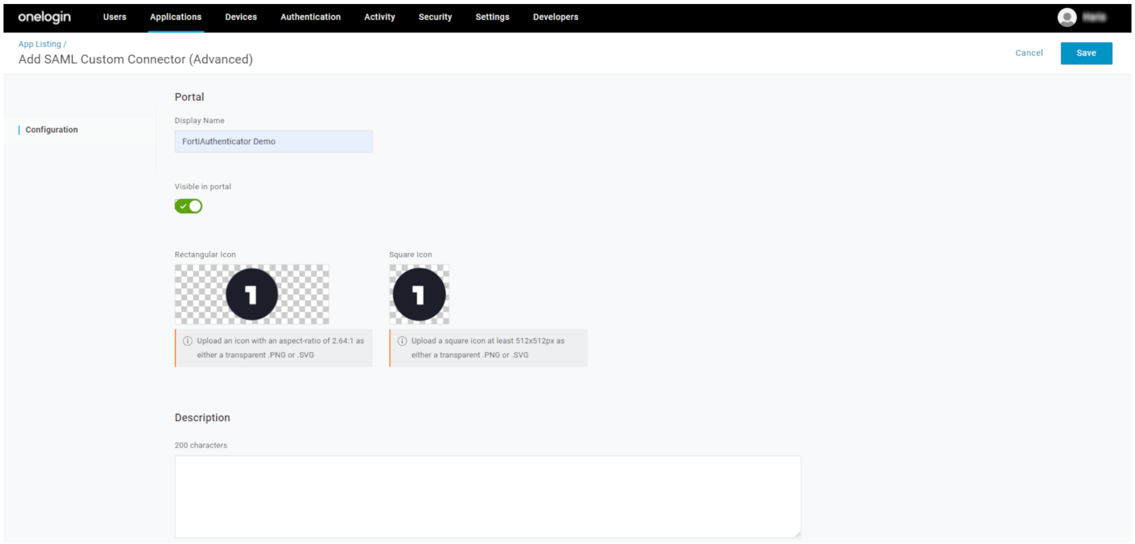
Creating an OneLogin application

To create an OneLogin application:

1. Log in to OneLogin with a Super user account.
2. Go to *Applications* > *Applications*.

> If you are unable to locate the *Applications* option, go to *Administration* > *Users and privileges* and ensure that *Permission* is set as *Super user*.

3. Select *Add App*.
4. In the *Find Applications* page, search and select *SAML Custom Connector (Advanced)*.
   The *Add SAML Custom Connector (Advanced)* window opens.
5. In *Display Name*, enter a name for the application.
6. Customize icons as required. Optionally, enter a description.
7. Click *Save*.



Add SAML Custom Connector (Advanced)

Portal

Display Name: FortiAuthenticator Demo

Visible in portal: ✓

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Description

200 characters

See Configuring an application on OneLogin on page 245, Configuring application parameters on OneLogin on page 247, and Configuring SSO on OneLogin on page 248.

Configuring an application on OneLogin

To configure an OneLogin application:

1. In the *SAML Custom Connector (Advanced)* window that opens after step 7 in Creating an OneLogin application on page 245, go to the *Configuration* tab.
   Alternatively, go to *Applications* > *Applications*, from the applications list select your application, and then go to the *Configuration* tab.
2. In *Audience (Entity ID)*, enter the *Entity ID* from the remote SAML server configuration on FortiAuthenticator.
3. In *ACS (Consumer) URL Validator*, enter the modified *ACS (login) URL* from the remote SAML server configuration on FortiAuthenticator.

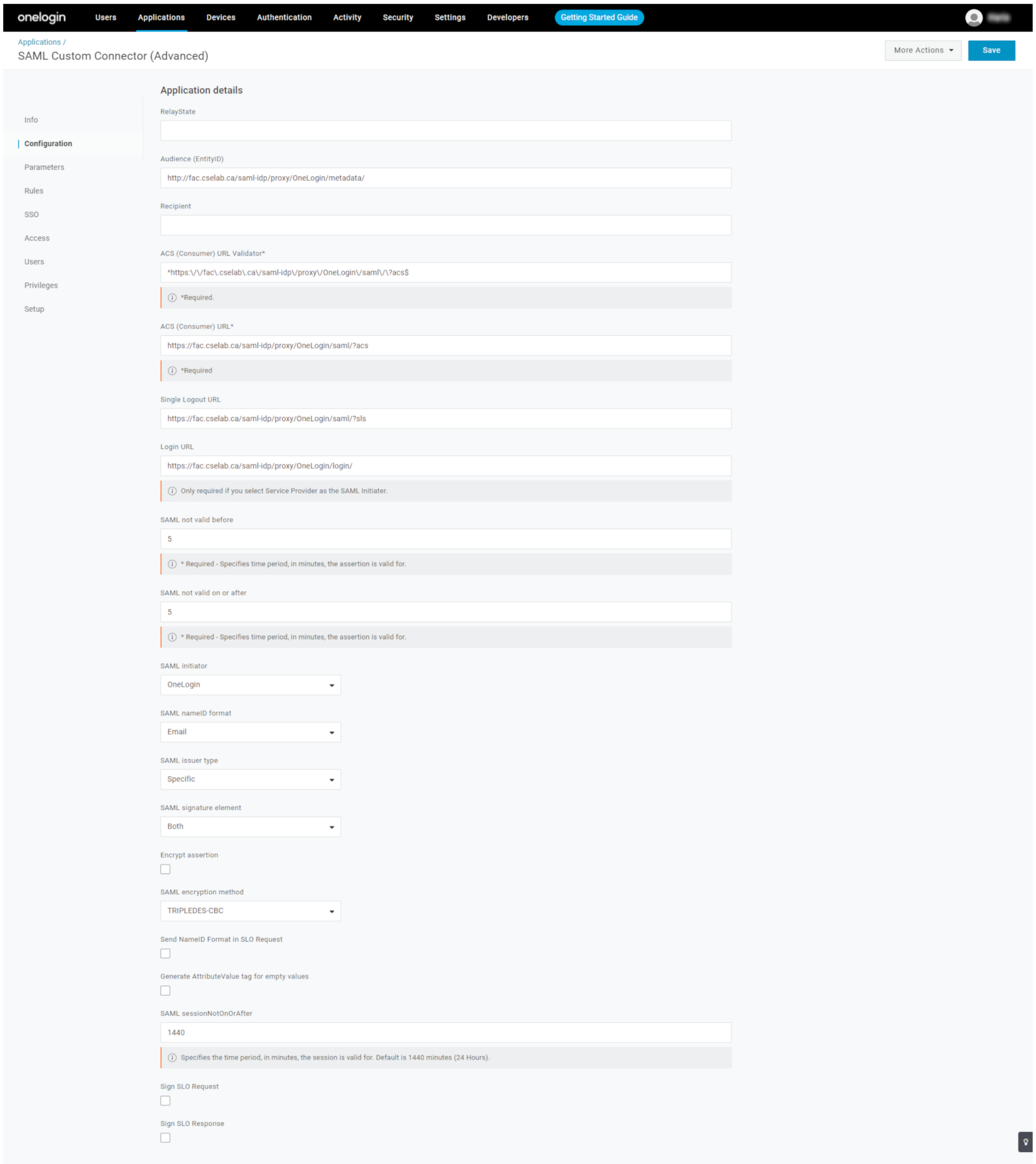
The *ACS (Consumer) URL Validator* must start with a "^", end with a "$", and have a "\" preceding every "/", "?" and ".".

See the screenshot below.

4. In *ACS (Consumer) URL*, enter the *ACS (login) URL* from the remote SAML server configuration on FortiAuthenticator.
5. In *Single Logout URL*, enter the *SLS (logout) URL* from the remote SAML server configuration on FortiAuthenticator.
6. In *Login URL*, enter the *Portal URL* from the remote SAML server configuration on FortiAuthenticator.
7. *SAML not valid before* and *SAML not valid on or after* may be changed as required.
8. Ensure that *SAML initiator* is set as *OneLogin*.
9. Ensure that *SAML nameID format* is as *Email*.
10. Ensure that *SAML issuer type* is set as *Specific*.
11. In the *SAML signature element* dropdown, select *Both*.
12. Click *Save*.

Parameters while configuring an application on OneLogin must match the remote SAML server configuration on FortiAuthenticator.

See Configuring a remote SAML server on page 250.



SAML Custom Connector (Advanced)

Application details

RelayState

Audience (EntityID)
http://fac.cselab.ca/saml-idp/proxy/OneLogin/metadata/

Recipient

ACS (Consumer) URL Validator*
^https:\/\/fac\.cselab\.ca\/saml-idp\/proxy\/OneLogin\/saml\/\?acs$
*Required.

ACS (Consumer) URL*
https://fac.cselab.ca/saml-idp/proxy/OneLogin/saml/?acs
*Required

Single Logout URL
https://fac.cselab.ca/saml-idp/proxy/OneLogin/saml/?sls

Login URL
https://fac.cselab.ca/saml-idp/proxy/OneLogin/login/
Only required if you select Service Provider as the SAML Initiater.

SAML not valid before
5
* Required - Specifies time period, in minutes, the assertion is valid for.

SAML not valid on or after
5
* Required - Specifies time period, in minutes, the assertion is valid for.

SAML initiator
OneLogin

SAML nameID format
Email

SAML issuer type
Specific

SAML signature element
Both

Encrypt assertion
☐

SAML encryption method
TRIPLEDES-CBC

Send NameID Format in SLO Request
☐

Generate AttributeValue tag for empty values
☐

SAML sessionNotOnOrAfter
1440
Specifies the time period, in minutes, the session is valid for. Default is 1440 minutes (24 Hours).

Sign SLO Request
☐

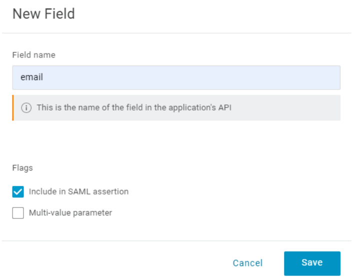
Sign SLO Response
☐

Configuring application parameters on OneLogin

To configure an email application parameters on OneLogin:

1. Go to *Applications* > *Applications*, from the applications list select your application.
2. Go to the *Parameters* tab and select +.
   The *New Field* dialog opens.
3. In the *New Field* dialog:
   a. In *Field* name, enter a name.
   b. Select the *Include in SAML assertion* checkbox
   c. Click *Save*.

4. Open the recently created field, and in the *Value* dropdown, select *Email*.
5. Click *Save*.



New Field

Field name: email

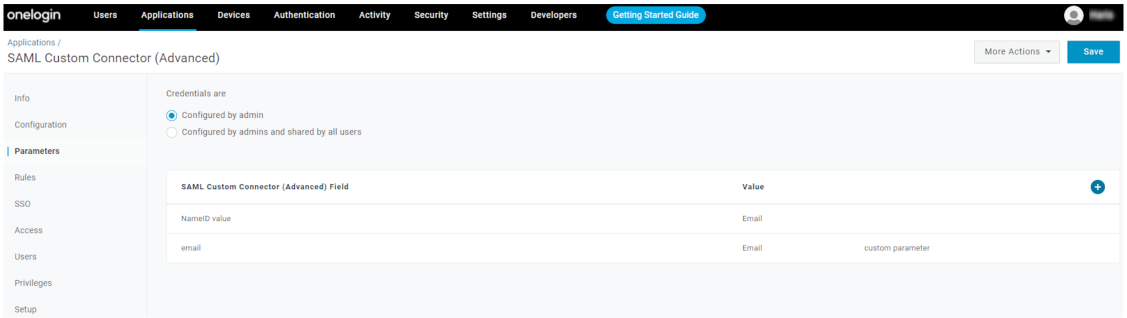
ⓘ This is the name of the field in the application's API

Flags

☑ Include in SAML assertion

□ Multi-value parameter

Once the field is configured, the window should appear as shown below.



SAML Custom Connector (Advanced)

Credentials are

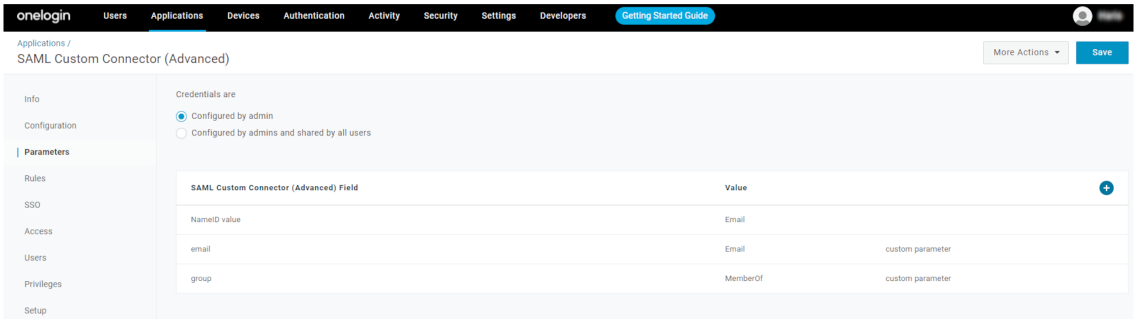
● Configured by admin

○ Configured by admins and shared by all users

SAML Custom Connector (Advanced) Field	Value	
NameID value	Email	
email	Email	custom parameter

To configure a Memberof application parameter on OneLogin:

1. Repeat steps 1 to 3 in Configuring an email application parameters on OneLogin.
2. Open the recently created field, and in the *Value* dropdown, select *MemberOf*.
3. Click *Save*.
4. Click *Save* from the top.



SAML Custom Connector (Advanced)

Credentials are

● Configured by admin

○ Configured by admins and shared by all users

SAML Custom Connector (Advanced) Field	Value	
NameID value	Email	
email	Email	custom parameter
group	MemberOf	custom parameter

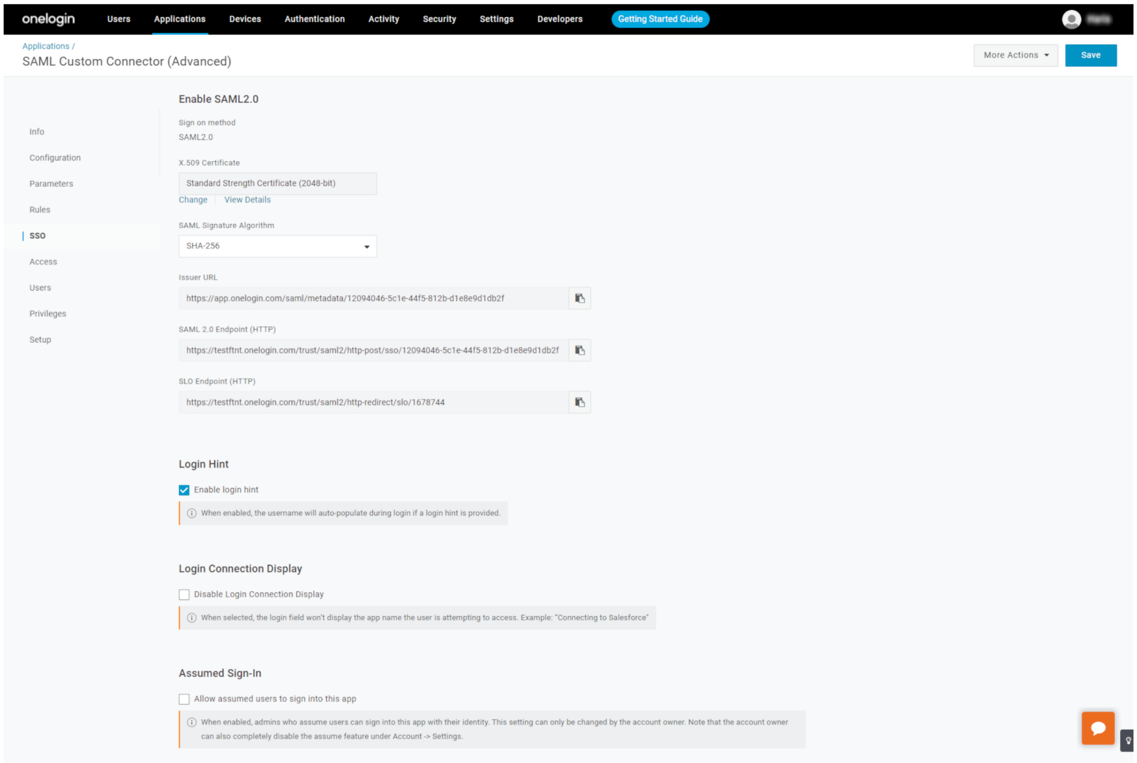
Configuring SSO on OneLogin

To configure SSO on OneLogin:

1. Go to *Applications* > *Applications*, from the applications list select your application.
2. Go to the *SSO* tab.
3. In the *SAML Signature Algorithm* dropdown, select *SHA-256*.

4. Click *Save*.

> Clicking *View Details* in *X.509 Certificate* shows the certificate assigned to the application by OneLogin that includes the fingerprint information. Ensure that *SHA fingerprint* is *SHA256*.
>
> Select a format from the dropdown and download the certificate.



SAML Custom Connector (Advanced)

Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)

SAML Signature Algorithm
SHA-256

Issuer URL
https://app.onelogin.com/saml/metadata/12094046-5c1e-44f5-812b-d1e8e9d1db2f

SAML 2.0 Endpoint (HTTP)
https://testftnt.onelogin.com/trust/saml2/http-post/sso/12094046-5c1e-44f5-812b-d1e8e9d1db2f

SLO Endpoint (HTTP)
https://testftnt.onelogin.com/trust/saml2/http-redirect/slo/1678744

Login Hint

☑ Enable login hint

ⓘ When enabled, the username will auto-populate during login if a login hint is provided.

Login Connection Display

☐ Disable Login Connection Display

ⓘ When selected, the login field won't display the app name the user is attempting to access. Example: "Connecting to Salesforce"

Assumed Sign-In

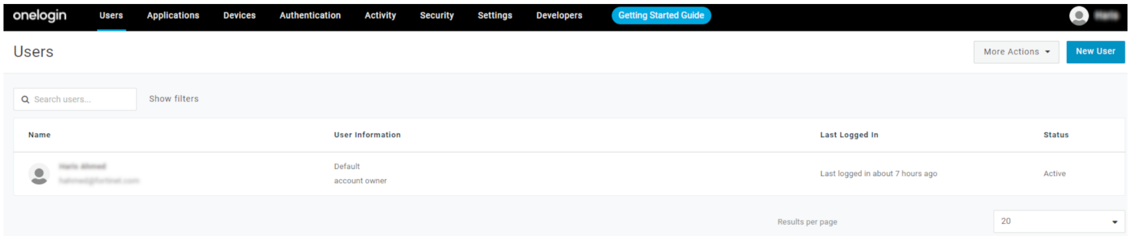
☐ Allow assumed users to sign into this app

ⓘ When enabled, admins who assume users can sign into this app with their identity. This setting can only be changed by the account owner. Note that the account owner can also completely disable the assume feature under Account -> Settings.

Granting user access to the application

To grant user access to the application:

1. Go to *Users* > *Users*.



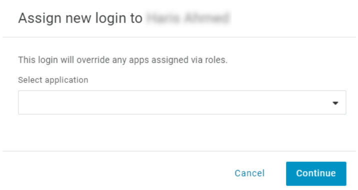
Users

Name	User Information	Last Logged In	Status
[redacted]	Default account owner	Last logged in about 7 hours ago	Active

2. Select the desired user from the list.
   The *Users* window opens.
3. Go to the *Applications* tab and select +.

4. In the *Assign new login to* window, select the previously created application, and select *Continue*.

If only one application exists or is unassigned to a user, it is automatically selected.



Assign new login to [redacted]

This login will override any apps assigned via roles.

Select application

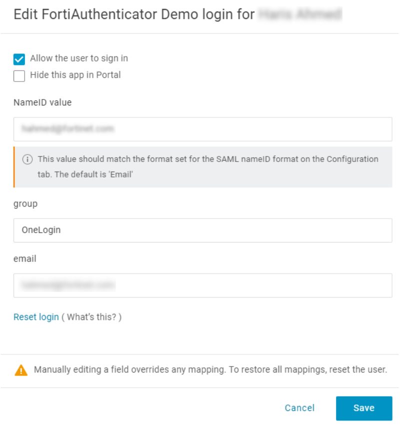
5. In the new dialog that appears:
   a. Ensure that *Allow the user to sign in* is selected.
   b. In *NameID value*, enter the user email address.
   c. In *group*, enter *OneLogin*.

      The *group* parameter has been manually overridden.

      The group value is contained in the SAML assertion and the FortiGate firewall policy configuration step uses it to match group information and grant users access based on the *OneLogin* group affiliation.

      See Configuring FortiGate SP settings on FortiAuthenticator on page 254 and Configuring a policy to allow users access to allowed network resources on page 260.

   d. Ensure that *email* is same as *NameID value*.
   e. Click *Save*.



Edit FortiAuthenticator Demo login for [redacted]

☑ Allow the user to sign in

□ Hide this app in Portal

NameID value: [redacted]

ⓘ This value should match the format set for the SAML nameID format on the Configuration tab. The default is 'Email'

group: OneLogin

email: [redacted]

Reset login (What's this?)

⚠ Manually editing a field overrides any mapping. To restore all mappings, reset the user.

Configuring a remote SAML server

Some fields, including *IdP entity ID*, *IdP single sign-on URL*, and *IdP certificate fingerprint*, are configured based on the corresponding OneLogin settings.

It is advised that you set up OneLogin and the SAML server simultaneously.

See Configuring SSO on OneLogin on page 248 and Configuring application parameters on OneLogin on page 247.

To configure a remote SAML server:

1. Go to *Authentication* > *Remote Auth. Servers* > *SAML* and select *Create New*.
   The *Create New Remote SAML Server window* opens.
2. Enter a name for the SAML server.
3. Select *Type* as *Proxy*.

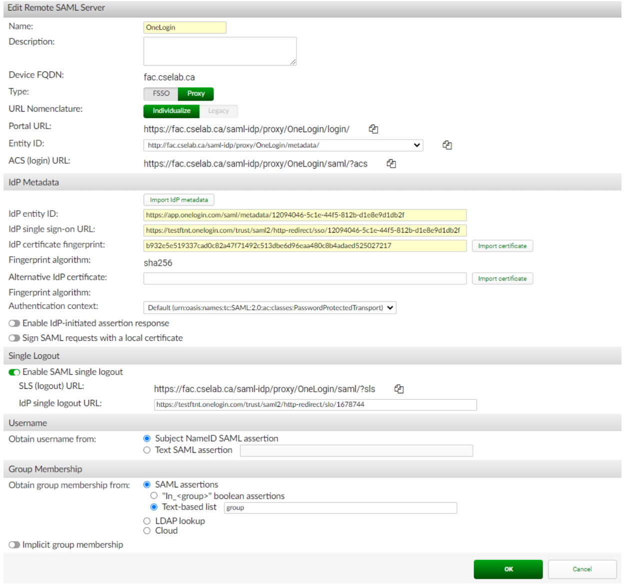
   The *Portal URL* is the SAML SP login URL.

4. In the *Entity ID* dropdown, select the non-Azure IdP entity ID.
5. In the *IdP Metadata* pane:
   - **a.** In *IdP entity ID*, enter *Issuer URL* from the *SSO* tab in OneLogin application configurtaion.
   - **b.** In *IdP single sign-on URL*, enter *SAML 2.0 Endpoint (HTTP)* from the *SSO* tab in OneLogin application configurtaion.
   - **c.** In *IdP certificate fingerprint*, select *Import certificate*, and upload the certificate fingerprint file that you saved while configuring the application on OneLogin. See Downloading the IdP certificate fingerprint on OneLogin.
     Alternatively, select *Import IdP metadata* to import the IdP related URL(s) you saved from OneLogin. See Importing IdP metadata.
6. Enable *SAML single logout* and in *IdP single logout URL* enter *SLO Endpoint (HTTP)* from the *SSO* tab in OneLogin application configuration. See View Details.
7. In the *Username* pane, ensure that *Obtain username from* is set to the default *Subject NameID SAML assertion*.
8. In the *Group Membership*:
   - **a.** In *Obtain group membership from*, select *SAML assertions*.
   - **b.** In *SAML assertions*, select *Text-based list*, and enter *group*.
     group is the application parameter with *Value* set as *Memberof*. See Configuring a Memberof application parameter on OneLogin.

     In the *Text-based list* field, any value can be used so long it is a parameter for the OneLogin application.

9. Optionally, enable *Implicit group membership* when only a single group exists.

10. Click *OK*.



Edit Remote SAML Server

Name: OneLogin

Description:

Device FQDN: fac.cselab.ca

Type: FSSO [✓ Proxy]

URL Nomenclature: [✓ Individualize] Legacy

Portal URL: https://fac.cselab.ca/saml-idp/proxy/OneLogin/login/

Entity ID: http://fac.cselab.ca/saml-idp/proxy/OneLogin/metadata/

ACS (login) URL: https://fac.cselab.ca/saml-idp/proxy/OneLogin/saml/?acs

IdP Metadata

Import IdP metadata

IdP entity ID: https://app.onelogin.com/saml/metadata/12094046-5c1e-44f5-812b-d1e8e9d1db2f

IdP single sign-on URL: https://testftnt.onelogin.com/trust/saml2/http-redirect/sso/12094046-5c1e-44f5-812b-d1e8e9d1db2f

IdP certificate fingerprint: b932e5e519337cad0c82a47f71492c513dbe6d96eaa480c8b4adaed525027217 Import certificate

Fingerprint algorithm: sha256

Alternative IdP certificate: Import certificate

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

SLS (logout) URL: https://fac.cselab.ca/saml-idp/proxy/OneLogin/saml/?sls

IdP single logout URL: https://testftnt.onelogin.com/trust/saml2/http-redirect/slo/1678744

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

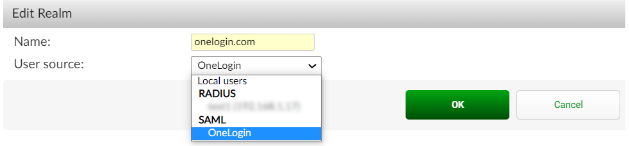
OK Cancel

Once the OneLogin application is set up and a certificate is associated with the application, you can download the IdP metadata by going to *More Actions* > *SAML Metadata* in one of the tabs when configuring the application.

Configuring an OneLogin realm

To create a realm:

1. Go to *Authentication* > *User Management* > *Realms*, and select *Create New*.
2. Enter an name for the realm.
3. In *User source*, select the remote SAML server created in Configuring a remote SAML server on page 250.
4. Click *OK*.



Edit Realm

Name: onelogin.com

User source: OneLogin

Local users
RADIUS
[redacted]
SAML
OneLogin

OK Cancel

Creating remote SAML users

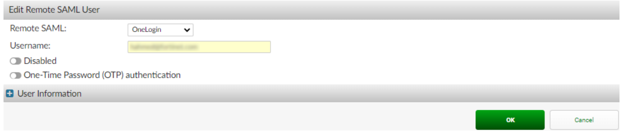
To create remote SAML users:

1. Go to *Authentication* > *User Management* > *Remote Users*, and select *SAML*.
2. Select *Create New*.
   The *Create New Remote SAML User* window opens.
3. In the *Remote SAML* dropdown, select the remote SAML server created in Configuring a remote SAML server on page 250.

4. In *Username*, enter a username in email format as set in OneLogin. Optionally, enter any useful information that you may need in the *User Information* pane.

> For successful authentication, the username must match with the email on OneLogin.

5. Click *OK*.



Edit Remote SAML User

Remote SAML: OneLogin

Username: [redacted]

○ Disabled

○ One-Time Password (OTP) authentication

User Information

Once saved, the newly created remote SAML user allows for FortiAuthenticator MFA, if required.

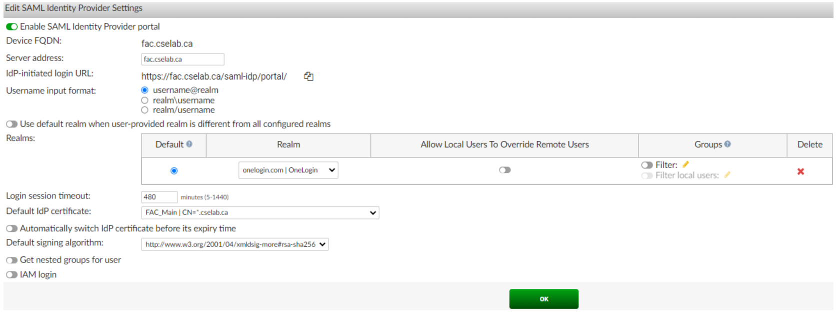
Configuring SAML IdP settings

To configure SAML IdP settings:

1. Go to *Authentication* > *SAML IdP* > *General*, and select *Enable SAML Identity Provider portal*.
2. In *Server address*, enter the FortiAuthenticator FQDN.

> *Device FQDN* can be configured from the *System Information* widget in System > *Dashboard* > *Status*.
>
> FQDN must be reachable via DNS for users using the service.

3. Ensure that *Username input format* is set as *username@realm*.
4. In the *Realms* dropdown, select the OneLogin realm configured in Configuring an OneLogin realm on page 252. Optionally, for group filtering, enable *Filter*, click the pen icon to edit, select groups from the *Available User Groups* search box, and click *OK*. This restricts access to a subset of users, e.g., restrict SAML authentication only to a group of 3rd party contractors even though all users may have been imported to FortiAuthenticator.
5. Optionally, in *login session timeout*, adjust the amount of time the user session is valid for, on successful authentication.
6. In the *Default IdP certificate* dropdown, select the local FortiAuthenticator certificate to use to sign SAML requests to SP clients. The certificate is uploaded to the FortiGate SP. See Uploading SAML IdP certificate to the FortiGate SP on page 256.
   To export the IdP certificate, see Exporting the IdP certificate.
7. Ensure that *Get nested groups for user* is disabled.
8. Click *OK*.



Edit SAML Identity Provider Settings

● Enable SAML Identity Provider portal

Device FQDN: fac.cselab.ca

Server address: fac.cselab.ca

IdP-initiated login URL: https://fac.cselab.ca/saml-idp/portal/

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

○ Use default realm when user-provided realm is different from all configured realms

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	onelogin.com | OneLogin	○	○ Filter: ○ Filter local users:	✗

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: FAC_Main | CN=*.cselab.ca

○ Automatically switch IdP certificate before its expiry time

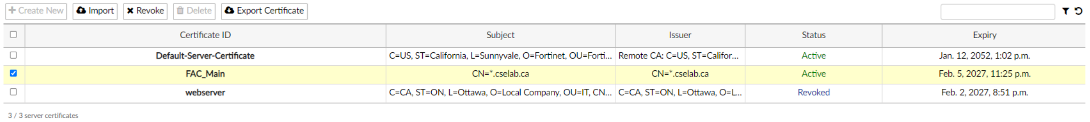
Default signing algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

○ Get nested groups for user

○ IAM login

To export the IdP certificate:

1. Go to *Certificate Management* > *End Entities* > *Local Services*.
2. Select the certificate used in the SAML IdP and click *Export Certificate*.



☐	Certificate ID	Subject	Issuer	Status	Expiry
☐	Default-Server-Certificate	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Forti...	Remote CA: C=US, ST=Califor...	Active	Jan. 12, 2052, 1:02 p.m.
☑	FAC_Main	CN=*.cselab.ca	CN=*.cselab.ca	Active	Feb. 5, 2027, 11:25 p.m.
☐	webserver	C=CA, ST=ON, L=Ottawa, O=Local Company, OU=IT, CN...	C=CA, ST=ON, L=Ottawa, O=L...	Revoked	Feb. 2, 2027, 8:51 p.m.

3 / 3 server certificates

As a best practice, the default certificate should not be used as it is less secure than a certificate issued by a trusted Certificate Authority (CA).

Configuring FortiAuthenticator replacement message

To configure a replacement message:

1. Go to *Authentication* > *SAML IdP* > *Replacement Messages*, and click the *Login Page* replacement message.
2. In *Restore Default* dropdown, select *idp-proxy* to automatically redirect users to the IdP proxy login page after 3 seconds.
   Alternatively, select *idp-server-and-proxy*, and then select *Or Sign in using a cloud server* to go to the IdP proxy login page.
3. On the right side of the screen, you can edit the replacement message in HTML. Replace all instances of *[proxy_portal_url]* with *Portal URL* in Configuring a remote SAML server on page 250.
4. Click *Save*.

In the *Restore Default* dropdown, *idp-server* option must not be selected as it does not redirect users to the IdP proxy, i.e., OneLogin for authentication.

For the configurations to work, the SAML IdP login page replacement message must be edited to include the portal URL.

Configuring FortiGate SP settings on FortiAuthenticator

FortiGate is configured as a SAML client ,i.e., SAML SP for FortiAuthenticator.

To complete the following configuration, you will need to configure the SAML settings on the ForiGate SP at the same time. This is because some fields including the *SP entity ID*, *SP ACS (login) URL*, and *SP SLS (logout) URL* are only available when configuring the SAML settings on the FortiGate SP.

To configure FortiGate service provider settings on FortiAuthenticator:

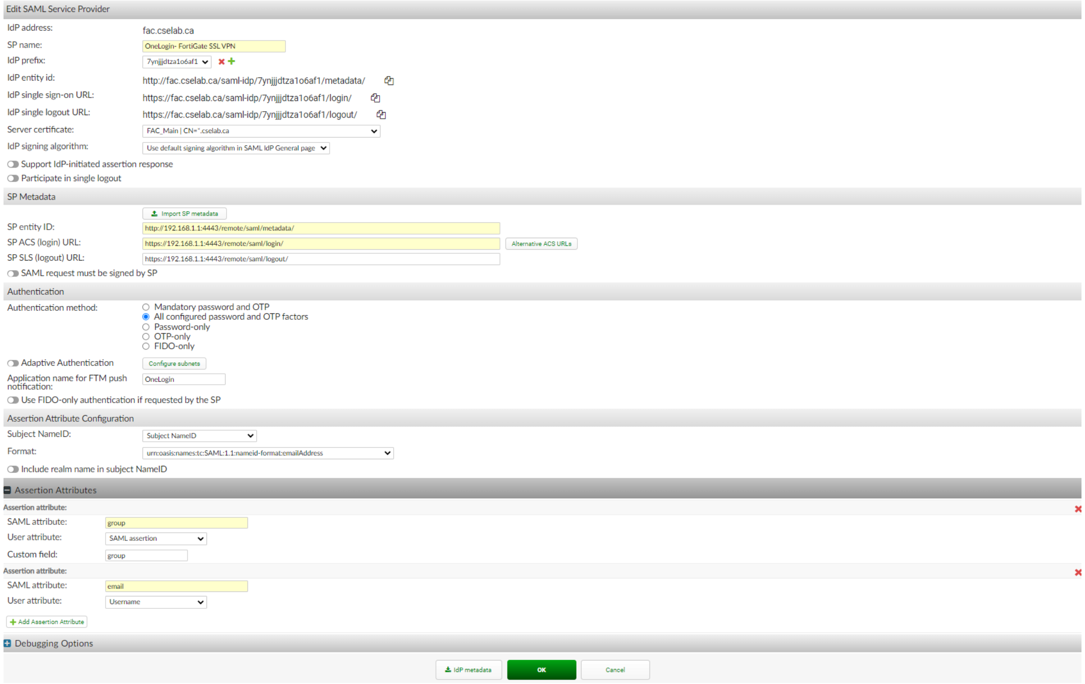
1. Go to *Authentication* > *SAML IdP* > *Service Providers*, and click *Create New*.
2. Enter the following information:
    - a. **SP name**: Enter a name for the FortiGate SP.
    - b. **IdP prefix**: Select +, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
    - c. **Server certificate**: Select the same certificate as the default IdP certificate used in *Authentication* > *SAML IdP* > *General*. See Configuring SAML IdP settings on page 253.
    - d. In *Application name for FTM push notification*, enter *OneLogin*.
3. Click *Save*.
4. In the *SP Metadata* pane, enter the following information:
    - a. **SP entity ID**: Enter the *SP entity ID* from Creating SAML user and server on page 257.
    - b. **SP ACS (login) URL**: Enter the *SP single sign-on URL* from Creating SAML user and server on page 257.
    - c. **SP SLS (logout) URL**: Enter the *SP single logout URL* from Creating SAML user and server on page 257.

    > *SP entity ID*, *SP ACS (login) URL*, and *SP SLS (logout) URL* must match their respective configurations on the FortiGate SP side.

5. Click *OK*.
6. Select and click *Edit* to edit the recently created FortiGate SP.
7. In *Assertion Attribute Configuration*:
    - a. Select *Subject NameID* in *Subject NameID*.
    - b. Select *urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress* in *Format*.
8. In *Assertion Attributes*, select *Add Assertion Attribute*:
    - a. Enter a name for the SAML attribute. Here, *group*.
    - b. Select *SAML assertion* in the *User attribute* dropdown.
    - c. Enter *group* in *Custom field*.
    - d. Select *Add Assertion Attribute* again to create a new SAML attribute named *email*, and from the *User attribute* dropdown select *SAML username*.

    > SAML assertion attribute names and values must match values configured in Creating SAML user and server on page 257.

9. Click *OK* to save changes.



Edit SAML Service Provider

IdP address: fac.cselab.ca
SP name: OneLogin- FortiGate SSL VPN
IdP prefix: 7ynjjjdtza1o6af1
IdP entity id: http://fac.cselab.ca/saml-idp/7ynjjjdtza1o6af1/metadata/
IdP single sign-on URL: https://fac.cselab.ca/saml-idp/7ynjjjdtza1o6af1/login/
IdP single logout URL: https://fac.cselab.ca/saml-idp/7ynjjjdtza1o6af1/logout/
Server certificate: FAC_Main | CN=*.cselab.ca
IdP signing algorithm: Use default signing algorithm in SAML IdP General page
Support IdP-initiated assertion response
Participate in single logout

SP Metadata

SP entity ID: http://192.168.1.1:4443/remote/saml/metadata/
SP ACS (login) URL: https://192.168.1.1:4443/remote/saml/login/
SP SLS (logout) URL: https://192.168.1.1:4443/remote/saml/logout/
SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory password and OTP
● All configured password and OTP factors
○ Password-only
○ OTP-only
○ FIDO-only

Adaptive Authentication
Application name for FTM push notification: OneLogin
Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

Subject NameID: Subject NameID
Format: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Include realm name in subject NameID

Assertion Attributes

Assertion attribute:
SAML attribute: group
User attribute: SAML assertion
Custom field: group

Assertion attribute:
SAML attribute: email
User attribute: Username

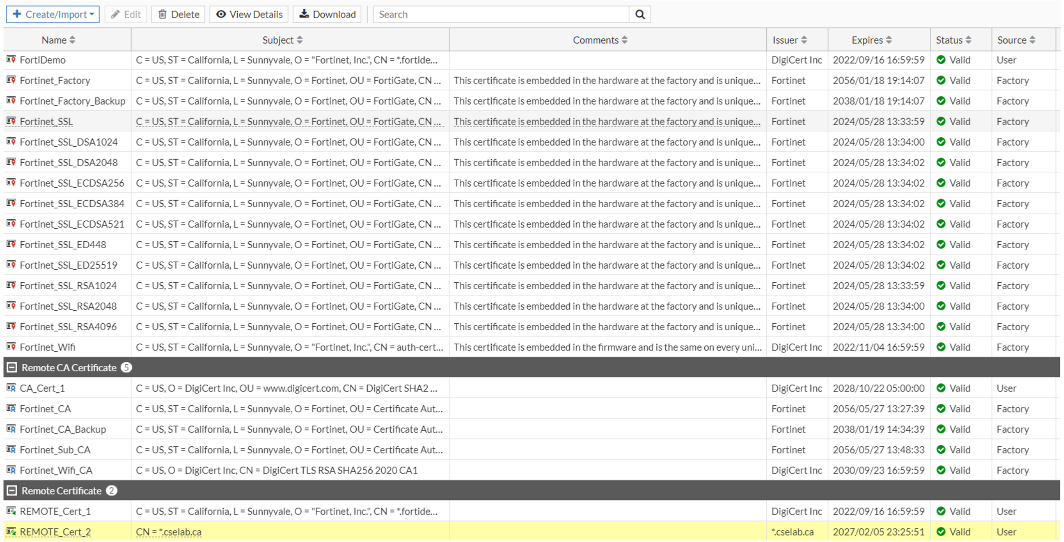
Debugging Options

Uploading SAML IdP certificate to the FortiGate SP

To upload SAML IdP certificate:

1. Go to *System* > *Certificates*.
2. From the *Create/Import* dropdown, select *Remote Certificate*.
   The *Upload Remote Certificate* window opens.
3. In the *Upload Remote Certificate* window, select *Upload*, and browse to the certificate that you saved in Exporting the IdP certificate.
4. Click *Open*.

5. Click *OK*.



Name	Subject	Comments	Issuer	Expires	Status	Source
FortiDemo	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = *.fortide...		DigiCert Inc	2022/09/16 16:59:59	✓ Valid	User
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2056/01/18 19:14:07	✓ Valid	Factory
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2038/01/18 19:14:07	✓ Valid	Factory
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:33:59	✓ Valid	Factory
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:00	✓ Valid	Factory
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:02	✓ Valid	Factory
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:02	✓ Valid	Factory
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:02	✓ Valid	Factory
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:02	✓ Valid	Factory
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:02	✓ Valid	Factory
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:02	✓ Valid	Factory
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:33:59	✓ Valid	Factory
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:00	✓ Valid	Factory
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2024/05/28 13:34:00	✓ Valid	Factory
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert...	This certificate is embedded in the firmware and is the same on every uni...	DigiCert Inc	2022/11/04 16:59:59	✓ Valid	Factory
⊟ Remote CA Certificate 5						
CA_Cert_1	C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 ...		DigiCert Inc	2028/10/22 05:00:00	✓ Valid	User
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:27:39	✓ Valid	Factory
Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2038/01/19 14:34:39	✓ Valid	Factory
Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:48:33	✓ Valid	Factory
Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1		DigiCert Inc	2030/09/23 16:59:59	✓ Valid	Factory
⊟ Remote Certificate 2						
REMOTE_Cert_1	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = *.fortide...		DigiCert Inc	2022/09/16 16:59:59	✓ Valid	User
REMOTE_Cert_2	CN = *.cselab.ca		*.cselab.ca	2027/02/05 23:25:51	✓ Valid	User

6. Make note of the name of the certificate used. Here, *REMOTE_Cert_2*.
   The certificate is then referenced in Creating SAML user and server on page 257.

Ensure that the correct certificate is uploaded to the FortiGate SP, else SAML authentication fails due to a mismatch in the certificate used by FortiAuthenticator to sign the SAML assertion.

The FortiGate SP only trusts SAML assertions signed by the certificate selected in Creating SAML user and server on page 257.

Creating SAML user and server

To create a new SAML server:

1. Go to *User & Authentication* > *Single Sign-On* and select *Create New*.
   The single-sign on wizard opens.
2. Enter a name for the SAML server.
3. In *SP address*, enter the local IP address and port in the format `<IP_ADDRESS>:<PORT>`.

SP address is the IP address of the interface users use to connect to the SSL VPN in *VPN > SSL-VPN Settings > Listen on Interface(s)*.

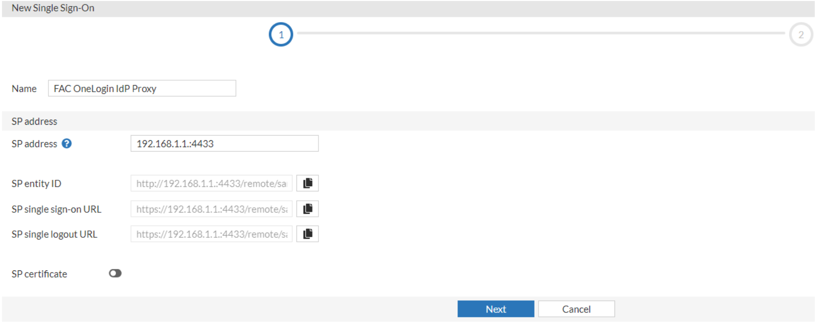
The port should be the same port configured in *VPN > SSL-VPN Settings > Listen on Port*.

Click the icon beside the *SP entity ID*, *SP single sign-on URL*, and *SP single logout URL* fields to copy the text.

SP entity ID, *SP single sign-on URL*, and *SP single logout URL* are then used when configuring SP settings on FortiAuthenticator.

See Configuring FortiGate SP settings on FortiAuthenticator on page 254.

4. Click *Next*.



New Single Sign-On

Name: FAC OneLogin IdP Proxy

SP address

SP address: 192.168.1.1.:4433

SP entity ID: http://192.168.1.1.:4433/remote/sa

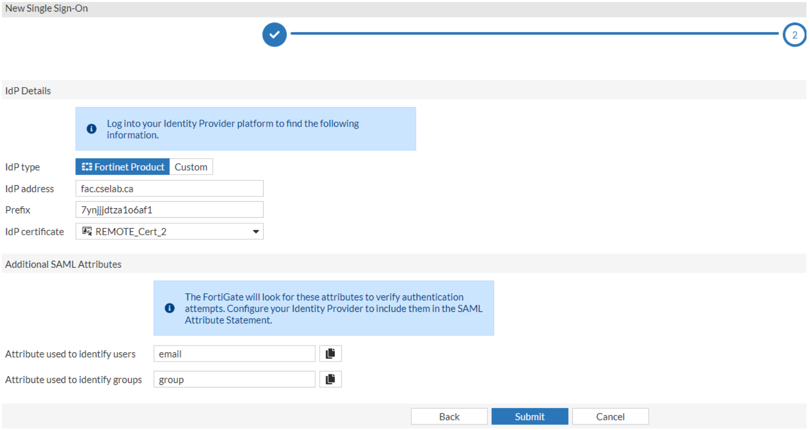
SP single sign-on URL: https://192.168.1.1.:4433/remote/s:

SP single logout URL: https://192.168.1.1.:4433/remote/s:

SP certificate

5. In *IdP Details*:
   - a. Ensure that *IdP type* is *Fortinet Product*.
   - b. In *IdP address*, enter the *Server address* from FortiAuthenticator. See Configuring SAML IdP settings on page 253.
   - c. In *Prefix*, enter the *IdP prefix* from Configuring FortiGate SP settings on FortiAuthenticator on page 254.
   - d. In the *IdP certificate* dropdown, select the certificate from Uploading SAML IdP certificate to the FortiGate SP on page 256.
6. In the *Additional SAML Attributes* pane:
   - a. In *Attribute used to identify users*, enter *email*.
   - b. In *Attribute used to identify groups*, enter *group*.

Attribute used to identify users and *Attribute used to identify groups* must match *Assertion Attributes* configured in Configuring FortiGate SP settings on FortiAuthenticator on page 254.



New Single Sign-On

IdP Details

Log into your Identity Provider platform to find the following information.

IdP type: Fortinet Product | Custom

IdP address: fac.cselab.ca

Prefix: 7ynjjjdtza1o6af1

IdP certificate: REMOTE_Cert_2

Additional SAML Attributes

The FortiGate will look for these attributes to verify authentication attempts. Configure your Identity Provider to include them in the SAML Attribute Statement.

Attribute used to identify users: email

Attribute used to identify groups: group

7. Click *Submit*.

To create the SAML group:

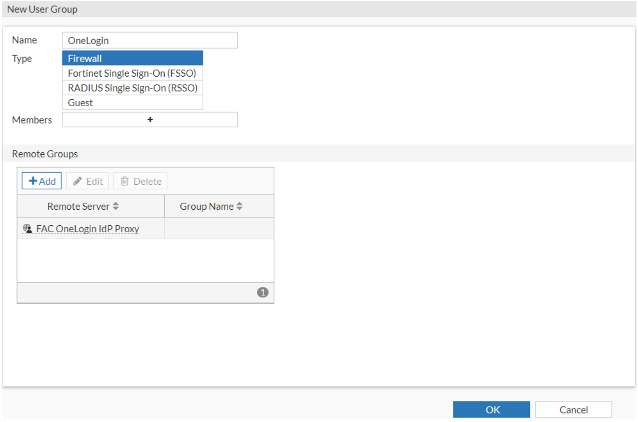
1. Go to *User & Authentication >User Groups* and click *Create New*.
2. Enter a name for the group.
3. In *Remote Groups*, select *Add*.
   The *Add Group Match* window opens.
4. In the *Remote Server* dropdown, select *FAC OneLogin IdP Proxy*.

FAC OneLogin IdP Proxy is the name of the SAML server set up in Creating a SAML server.

5. In *Groups*, select *Any*.

You may set *Groups* as *Specify* to filter specific groups from the FortiGate SP.

6. Click *OK*.
7. Click *OK*.



New User Group

Name: OneLogin

Type: Firewall

Remote Groups

Remote Server	Group Name
FAC OneLogin IdP Proxy	

Mapping SSL VPN authentication portal

To map SSL VPN authentication portal:

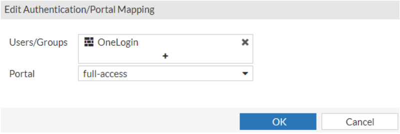
1. Go to *VPN > SSL-VPN Settings*.
2. In the *Authentication/Portal Mapping* pane:
   a. Select *Create New*.
      The *New Authentication/Portal Mapping* window opens.
   b. In *User/Groups*, select +, search and select the SAML user group configured in Creating the SAML group.

   c. In the *Portal* dropdown, select *full-access* or *tunnel-access*.

In the *Portal* dropdown, *web-access* can also be selected if the user connects to the network using the portal.

   d. Click *OK*.

3. Click *Apply*.



Edit Authentication/Portal Mapping

Users/Groups: OneLogin

Portal: full-access

Increasing remote authentication timeout using FortiGate CLI

To allow enough time for the remote authentication process to take place, the default value of the remote authentication timeout must be increased.

To increase remote authentication timeout:

1. In the FortiGate CLI console, enter the following commands:

```
config system global
   set remoteauthtimeout 60 #seconds that the FortiGate waits for response from remote
        authentication server.
end
```

Remote authentication timeout value should be adjusted according to the requirements of your environment. The value (60 seconds) set above may not work for you.

Configuring a policy to allow users access to allowed network resources

To configure a policy:

1. Go to *Policy & Objects* > *Firewall Policy* and select *Create New*.
2. Enter a name for the policy.
3. In *Incoming Interface*, select *SSL-VPN tunnel interface (ssl.root)*.
4. In *Outgoing Interface*, select a destination interface.
5. In *Source*:
   a. Select + to open the *Selected Entries* window.
   b. In *User*, search and select the SAML user group created in Creating a SAML group and the SSL VPN pool range object.
   c. Select *Close*.
6. In *Destination*:
   a. Select + to open the *Selected Entries* window.
   b. In *Address*, search and select the destination address.
   c. Select *Close*.

7. In the *Schedule* dropdown, select *always*.
8. In *Service*:
   a. Select + to open the *Selected Entries* window.
   b. Search and select *ALL*.
   c. Select *Close*.
9. Optionally, in the *Security Profiles* pane, select the required options.
10. Click *OK*.

If more policies are required, modify the above steps as needed.

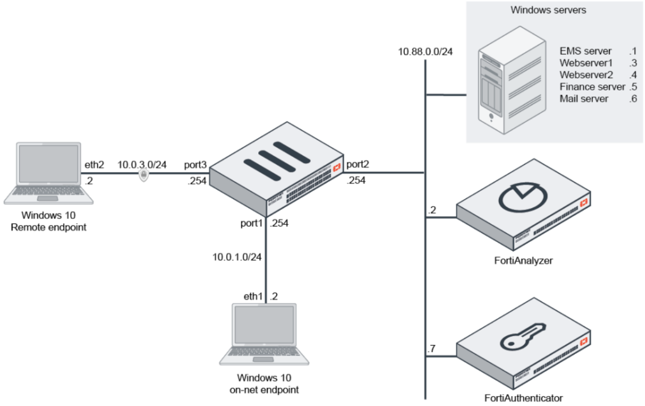
FortiGate SSL VPN with FortiAuthenticator as SAML IdP

In this configuration, the FortiGate acts as a SAML Service Provider (SP) requesting authentication from FortiAuthenticator, which acts as a SAML Identity Provider (IdP). It connects to the Windows AD via LDAP to authenticate user requests. The FortiAuthenticator also acts as a root CA to sign certificates for the SP, IdP and FortiGate SSL VPN portal.

Users are managed in Windows AD under the Security Groups **Finance** and **Sales**. The users are:

User name	sAMAccountName	Security Group	MemberOf
Tom Smith	tsmith	Sales	CN=Sales,CN=Users,DC=fortiad,DC=info
Dan Parker	dparker	Finance	CN=Finance,CN=Users,DC=fortiad,DC=info

The following shows topology for the configuration used in this example:



The authentication process is as follows in this deployment using SSL VPN web mode:

1. The user initiates an SSL VPN request to the FortiGate.
2. The FortiGate sends a POST redirect to browser.
3. Browser redirects the SAML authentication request to FortiAuthenticator.
4. The user authenticates with FortiAuthenticator using their LDAP credentials.
5. FortiAuthenticator sends a SAML assertion that contains the user and group authentication in a POST redirect to the SSL VPN login page.
6. Browser sends the redirected FortiAuthenticator request that contains the SAML assertion to the FortiGate.
7. The FortiGate consumes the assertion and provides the user with access to resources based on the defined firewall security policy.

In the case of SSL VPN tunnel mode, the communication on the user endpoint is done on the FortiClient rather than the browser.

Assumptions

1. A policy is configured on the FortiGate using VIP to allow external users access to the FortiAuthenticator for SAML authentication. The VIP maps `10.0.3.7->10.88.0.7` on `TCP/443`.
2. When using SSL VPN tunnel mode, the end user's FortiClient is registered to the EMS server in order to license the VPN remote access module.
3. A policy is configured on the FortiGate using VIP to allow external users access to EMS for Telemetry. The VIP maps `10.0.3.254->10.88.0.1` on `TCP/8013`.

Certificate management

During the authentication process, the SAML SP and IdP must verify each other. This means that they must verify certificates on both ends. Since the local CA manages the SAML certificates on the FortiAuthenticator, it has the certificates necessary for its configurations. To complete its configuration, the SAML SP certificate and SAML IdP certificate must be exported and loaded onto the FortiGate.

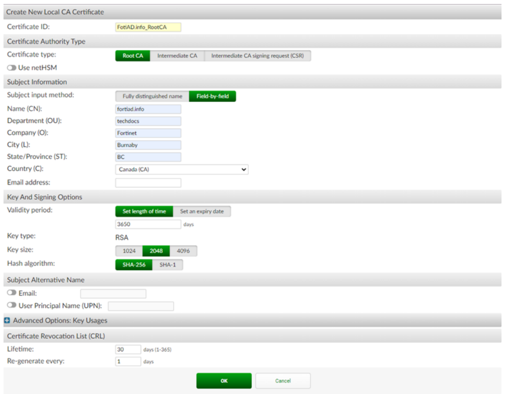
Furthermore, in this scenario, the CA on the FortiAuthenticator will also sign the SSL VPN certificate used by the FortiGate. This certificate must also be exported and loaded on the FortiGate.

Configuring the local CA on FortiAuthenticator

To configure a local CA on FortiAuthenticator:

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Create New*.
   The *Create New Local CA Certificate* window opens.
2. In *Certificate ID*, enter a unique ID for the CA.
3. In the *Subject Information* pane, enter the necessary subject information to identify the CA.

4. Click *OK*.



Create New Local CA Certificate

Certificate ID: FotiAD.info_RootCA

Certificate Authority Type

Certificate type: Root CA

Use netHSM

Subject Information

Subject input method: Field-by-field

Name (CN): fortiad.info

Department (OU): techdocs

Company (O): Fortinet

City (L): Burnaby

State/Province (ST): BC

Country (C): Canada (CA)

Email address:

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

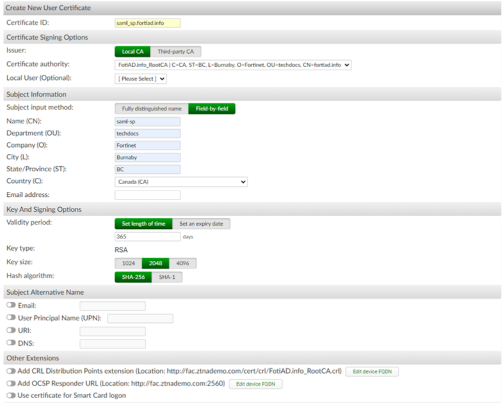
To export the created local CA:

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
2. From the local CA certificate list, select the local root CA created in Configuring a local root CA, and select *Export Certificate* to export the CA certificate in `.crt` format. This certificate is then imported on the client endpoint later.

Generating the certificates on FortiAuthenticator

To generate a user certificate for the FortiGate SAML SP on FortiAuthenticator:

1. Go to *Certificate Management* > *End Entities* > *Users* and select *Create New*.
2. In *Certificate ID*, enter a unique ID for the certificate.
3. Ensure that the *Issuer* is *Local CA*.
4. In *Certificate authority* dropdown, select the previously created local CA. See Configuring a local root CA.
5. In the *Subject Information* pane, enter the necessary subject information to identify the user certificate.
6. Click *OK*.



Create New User Certificate

Certificate ID: saml_sp.fortiad.info

Certificate Signing Options

Issuer: Local CA

Certificate authority: FotiAD.info_RootCA | C=CA, ST=BC, L=Burnaby, O=Fortinet, OU=techdocs, CN=fortiad.info

Local User (Optional): [Please Select]

Subject Information

Subject input method: Field-by-field

Name (CN): saml-sp

Department (OU): techdocs

Company (O): Fortinet

City (L): Burnaby

State/Province (ST): BC

Country (C): Canada (CA)

Email address:

Key And Signing Options

Validity period: Set length of time

365 days

Key type: RSA

Key size: 2048

Hash algorithm: SHA-256

Subject Alternative Name

Email:

User Principal Name (UPN):

URI:

DNS:

Other Extensions

Add CRL Distribution Points extension (Location: http://fac.ztnademo.com/cert/crl/FotiAD.info_RootCA.crl)

Add OCSP Responder URL (Location: http://fac.ztnademo.com:2560)

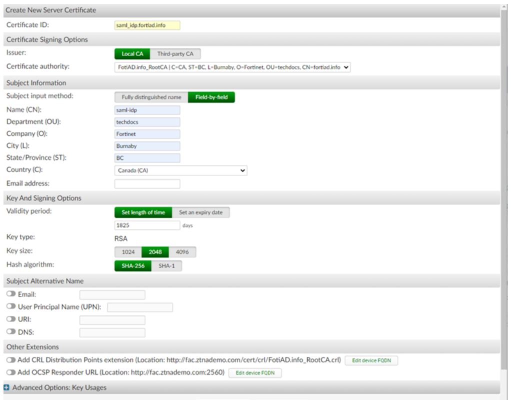
Use certificate for Smart Card logon

To export the user certificate:

1. Go to *Certificate Management* > *End Entities* > *Users*.
2. From the users list, select the user certificate created in Configuring a user certificate, and select *Export Key and Cert* to export the user certificate in `.p12` format.
3. Enter a password to secure the key.

To generate a server certificate for the SAML IdP on FortiAuthenticator:

1. Go to *Certificate Management* > *End Entities* > *Local Services* and select *Create New*.
2. In *Certificate ID*, enter a unique ID for the certificate.
3. In *Certificate authority* dropdown, select the previously created local CA.
   See Configuring a local root CA.
4. In the *Subject Information* pane, enter the necessary subject information to identify the server certificate.
5. Click *OK*.



Create New Server Certificate

Certificate ID: saml_idp.fortiad.info

Certificate Signing Options

Issuer: [✓ Local CA] Third-party CA

Certificate authority: FotiAD.info_RootCA | C=CA, ST=BC, L=Burnaby, O=Fortinet, OU=techdocs, CN=fortiad.info

Subject Information

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

Name (CN): saml-idp

Department (OU): techdocs

Company (O): Fortinet

City (L): Burnaby

State/Province (ST): BC

Country (C): Canada (CA)

Email address:

Key And Signing Options

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

1825 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.ztnademo.com/cert/crl/FotiAD.info_RootCA.crl) Edit device FQDN

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

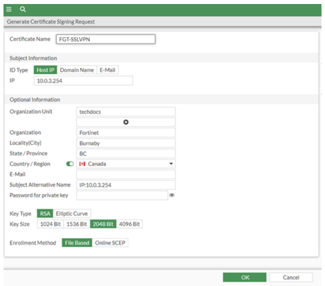
Advanced Options: Key Usages

To export the server certificate:

1. Go to *Certificate Management* > *End Entities* > *Local Services*.
2. From the local services list, select the server certificate created in Configuring a server certificate, and select Export Certificate to export the certificate in `.cer` format.

To create and sign a user certificate for FortiGate SSL VPN web portal:

1. On FortiGate, go to *System* > *Certificate*, and from the *Create/Import* dropdown, select *Generate CSR*.
2. 2. Enter the *Certificate Name*, *Subject Information* and any *Optional Information* such as a *Subject Alternative Name*.
3. Click *OK*.



Generate Certificate Signing Request

Certificate Name: FGT-SSLVPN

Subject Information

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

IP: 10.0.3.254

Optional Information

Organization Unit: techdocs

Organization: Fortinet

Locality(City): Burnaby

State / Province: BC

Country / Region: Canada

E-Mail:

Subject Alternative Name: IP:10.0.3.254

Password for private key:

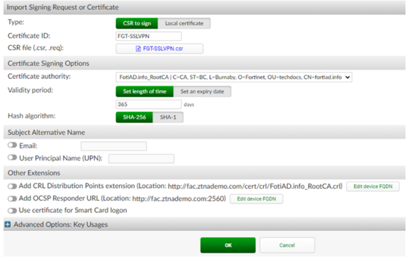
Key Type: [✓ RSA] Elliptic Curve

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

Enrollment Method: [✓ File Based] Online SCEP

4. On the *Certificates* list page, select the user certificate you have created under *Local Certificate*.
5. Click *Download* to download the CSR file.
6. On FortiAuthenticator, go to *Certificate Management* > *End Entities* > *Users*, and click *Import*.
7. Enter a certificate Id.
8. Select *Upload a file* to locate and upload the CSR file created from the FortiGate.
9. In the *Certificate authority* dropdown, select the certificate authority created earlier. See Configuring a local root CA.

10. Click *OK*.



Import Signing Request or Certificate

Type: CSR to sign | Local certificate

Certificate ID: FGT-SSLVPN

CSR file (.csr, .req): FGT-SSLVPN.csr

Certificate Signing Options

Certificate authority: FotiAD.info_RootCA | C=CA, ST=BC, L=Burnaby, O=Fortinet, OU=techdocs, CN=fortiad.info

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: http://fac.ztnademo.com/cert/crl/FotiAD.info_RootCA.crl) Edit device FQDN

Add OCSP Responder URL (Location: http://fac.ztnademo.com:2560) Edit device FQDN

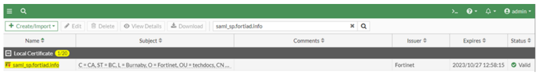
Use certificate for Smart Card logon

Advanced Options: Key Usages

11. In *Certificate Management* > *End Entities* > *Users*, select the above certificate.
12. Click *Export Certificate* to export a `.cer` file.

Importing certificates on FortiGate

1. On FortiGate, go to *System* > *Certificates*, and from the *Create/Import* dropdown, select *Certificate*.
2. In the *Create Certificate* window, select *Import Certificate* in the *Import Certificate* pane.
3. In *Type*, select *PKCS #12 Certificate*.
4. In *Certificate with key file*, select *Upload*, locate and then upload the `.p12` user certificate with key file from your computer, and enter the password.
   See Exporting user certificate.
5. Click *Create*.
   On the certificates list page, the new certificate is available in *Local Certificate*.

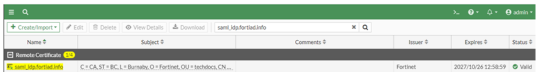


saml_sp.fortiad.info

Name	Subject	Comments	Issuer	Expires	Status
Local Certificate 1/20					
saml_sp.fortiad.info	C = CA, ST = BC, L = Burnaby, O = Fortinet, OU = techdocs, CN ...		Fortinet	2023/10/27 12:58:15	Valid

To import the SAML IdP remote certificate:

1. On FortiGate, go to *System* > *Certificates*, and from the *Create/Import* dropdown, select *Remote Certificate*.
2. Select *Upload* to locate and upload the `.cer` remote certificate from your computer.
3. Click *OK*.
   On the certificates list page, the new certificate is now available in *Remote Certificate*.

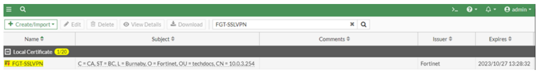


saml_idp.fortiad.info

Name	Subject	Comments	Issuer	Expires	Status
Remote Certificate 1/4					
saml_idp.fortiad.info	C = CA, ST = BC, L = Burnaby, O = Fortinet, OU = techdocs, CN ...		Fortinet	2027/10/26 12:58:59	Valid

To import the user certificate for the FortiGate SSL VPN portal

1. On FortiGate, go to *System* > *Certificates*, and from the *Create/Import* dropdown, select *Certificate*.
2. Select *Import Certificate* to locate the `.cer` user certificate file from your computer.
3. Click *Create*.
   On the certificates list page, the new certificate is now available in *Local Certificate*.



FGT-SSLVPN

Name	Subject	Comments	Issuer	Expires
Local Certificate 1/20				
FGT-SSLVPN	C = CA, ST = BC, L = Burnaby, O = Fortinet, OU = techdocs, CN = 10.0.3.254		Fortinet	2023/10/27 13:28:32

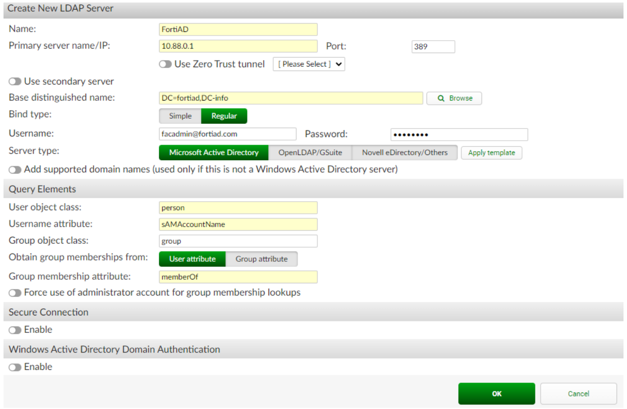
FortiAuthenticator user management

FortiAuthenticator acts as the SAML IdP, authenticating users against the Windows AD. To do this, the appropriate LDAP connection, user realm and user groups must be configured before it can be applied to the SAML IdP configurations.

Configuring multiple user groups is optional. In this example, multiple groups are used to ensure only users who are members of the **Sales** and **Finance** groups can pass authentication.

To configure an LDAP remote authentication server on FortiAuthenticator:

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and select *Create New*.
2. Configure the LDAP server settings to connect to the Windows AD as shown in the screenshot.



Create New LDAP Server

Name: FortiAD
Primary server name/IP: 10.88.0.1 Port: 389
○ Use Zero Trust tunnel [Please Select]
○ Use secondary server
Base distinguished name: DC=fortiad,DC-info Browse
Bind type: Simple [✓ Regular]
Username: facadmin@fortiad.com Password: ••••••••
Server type: [✓ Microsoft Active Directory] OpenLDAP/GSuite Novell eDirectory/Others Apply template
○ Add supported domain names (used only if this is not a Windows Active Directory server)

Query Elements

User object class: person
Username attribute: sAMAccountName
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

Windows Active Directory Domain Authentication

○ Enable

3. Click *OK*.

To configure a user realm on FortiAuthenticator:

1. Go to *Authentication* > *User Management* > *Realms* and select *Create New*.
2. Name the realm.
3. In *User source*, from the dropdown, select the recently created LDAP server.
4. Click *OK*.

To configure user groups on FortiAuthenticator:

1. Go to *Authentication* > *User Management* > *User Groups* and select *Create New*
2. To create a user group for **Sales**:
   a. In *Name*, enter `Sales`.
   b. Set the *Type* as *Remote LDAP*.
   c. From the *Remote LDAP* dropdown, select the recently created LDAP server.
   d. In *LDAP filter*, specify an LDAP filter using an LDAP query.
      To select users who are **memberOf** the **Sales** group, enter
      `(&(objectclass=user)(memberOf=CN=Sales,CN=Users,DC=fortiad,DC=info))`
3. Click *OK*.
4. To create a user group for **Finance**:
   a. In *Name*, enter `Finance`.
   b. Set the *Type* as *Remote LDAP*.

c. From the *Remote LDAP* dropdown, select the recently created LDAP server.

d. In *LDAP filter*, specify an LDAP filter using an LDAP query.
To select users who are **memberOf** the **Finance** group, enter

```
(&(objectclass=user)(memberOf=CN=Sales,CN=Users,DC=fortiad,DC=info))
```

e. Click *OK*.

The LDAP filter above will not match users whose group (**Sales** or **Finance**) is set as the primary group. This is because the primary group is returned by the **primaryGroupID** attribute by Windows AD and does not appear in the **memberOf** attribute.

SAML IdP and SP configurations

Before configuring the IdP and SP settings, quickly note down the IP addresses and ports that will be used by the client endpoint to connect to the IdP and SP.

In this topology, the IP addresses and ports used by the client endpoint are:

• **FortiAuthenticator (IdP)** – 10.0.3.7:443

• **FortiGate (SP)** – 10.0.3.254:10443 (10443 is used for access related to SSL VPN based on the default listening port for SSL VPN. Change this accordingly when listening on a different port)

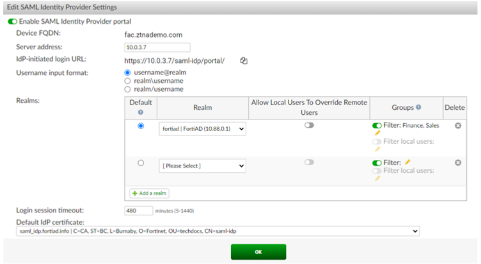
In general, the URLs used for the SP and IdP configurations in a SSL VPN scenario are in the following format:

Settings	FortiGate CLI setting	URL format
SP Entity ID	`entity-id`	http://<SP_IP>:<port>/remote/saml/metadata/
SP Assertion consumer service (login) URL	`single-sign-on-url`	https://<SP_IP>:<port>/remote/saml/login/
SP Single logout service URL	`single-logout-url`	https://<SP_IP>:<port>/remote/saml/logout/
IdP Entity ID	`idp-entity-id`	http://<IdP_IP>:<port>/saml-idp/<prefix>/metadata/
IdP Assertion consumer service URL (Single sign-on URL)	`idp-single-sign-on-url`	https://<IdP_IP>:<port>/saml-idp/<prefix>/login/
IdP Single logout service URL (single logout URL)	`idp-single-logout-url`	https://<IdP_IP>:<port>/saml-idp/<prefix>/logout/

To configure general SAML IdP settings on FortiAuthenticator:

1. Go to *Authentication > SAML IdP > General*.
2. Enable *SAML Identity Provider portal*.

3. Enter the server address. This address must be accessible by the client endpoint.
4. In *Realms*, select *Add a realm* and select the recently created realm from the dropdown.
5. In *Groups*, enable *Filter*, and choose the **Finance** and **Sales** user groups that you recently created.
6. In *Default IdP certificate* dropdown, select the IdP certificate created in *Certificate Management* > *End Entities* > *Local Services*. See Generating a server certificate.
7. Click *OK*.



Edit SAML Identity Provider Settings

Enable SAML Identity Provider portal

Device FQDN: fac.ztnademo.com

Server address: 10.0.3.7

IdP-initiated login URL: https://10.0.3.7/saml-idp/portal/

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

Realms:

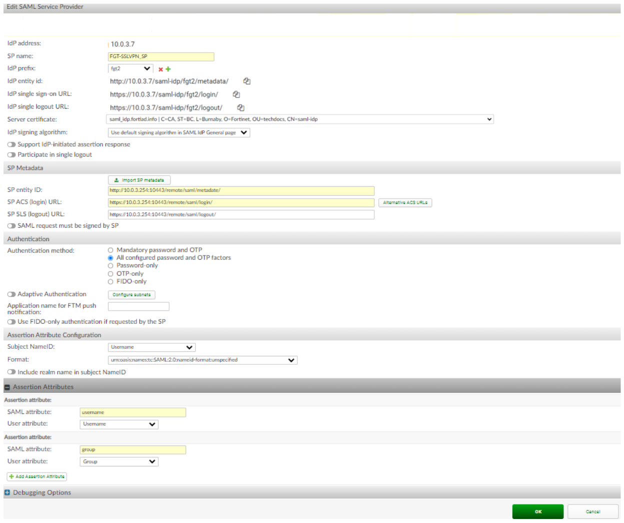
Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	fortiad | FortiAD (10.88.0.1)		Filter: Finance, Sales Filter local users:	
○	[Please Select]		Filter: Filter local users:	

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: saml_idp.fortiad.info | C=CA, ST=BC, L=Burnaby, O=Fortinet, OU=techdocs, CN=saml-idp

To configure service provider SAML settings on FortiAuthenticator

1. Go to *Authentication* > *SAML IdP* > *Service Providers* and select *Create New*.
2. Enter an SP name.
3. Enter an IdP prefix. This prefix will appear in the IdP URLs.
4. In *Server certificate*, choose the SAML IdP certificate created under *Certificate Management* > *End Entities* > *Local Services*. See Generating a server certificate.
5. Store the IdP URLs on Notepad as they are needed on FortiGate.
6. Enter the *SP entity ID*, *SP ACS (login) URL*, *SP SLS (logout) URL* as recommended in the table above.
7. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. In *SAML attribute*, enter `username`.
   b. In *User attribute* dropdown, select *FortiAuthenticator* > *Username*.
8. Select *Add Assertion Attribute*:
   a. In *SAML attribute*, enter `group`.
   b. In *User attribute* dropdown, select *Remote LDAP server* > *Group*.
   This is equivalent to returning the groups from the **memberOf** attribute.
   c. Click *OK*.



Edit SAML Service Provider

IdP address: 10.0.3.7

SP name: FGT-SSLVPN_SP

IdP prefix: fgt2

IdP entity id: http://10.0.3.7/saml-idp/fgt2/metadata/

IdP single sign-on URL: https://10.0.3.7/saml-idp/fgt2/login/

IdP single logout URL: https://10.0.3.7/saml-idp/fgt2/logout/

Server certificate: saml_idp.fortiad.info | C=CA, ST=BC, L=Burnaby, O=Fortinet, OU=techdocs, CN=saml-idp

IdP signing algorithm: Use default signing algorithm in SAML IdP General page

Support IdP-initiated assertion response

Participate in single logout

SP Metadata

SP entity ID: http://10.0.3.254:10443/remote/saml/metadate/

SP ACS (login) URL: https://10.0.3.254:10443/remote/saml/login/

SP SLS (logout) URL: https://10.0.3.254:10443/remote/saml/logout/

SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory password and OTP
● All configured password and OTP factors
○ Password-only
○ OTP-only
○ FIDO-only

Adaptive Authentication

Application name for FTM push notification:

Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

Subject NameID: Username

Format: urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

Include realm name in subject NameID

Assertion Attributes

Assertion attribute:

SAML attribute: username

User attribute: Username

Assertion attribute:

SAML attribute: group

User attribute: Group

Debugging Options

To configure SAML Single Sign-On settings on the FortiGate:

SAML settings can be configured from the GUI, but the default SP URLs must be changed after they are created. Therefore, the following instructions show how to configure the SAML settings from CLI instead.

1. In the CLI console, enter the following commands:

```
config user saml
   edit "fac_saml_idp-sslvpn"
      set cert "saml_sp.fortiad.info"
      set entity-id "http://10.0.3.254:10443/remote/saml/metadata/"
      set single-sign-on-url "https://10.0.3.254:10443/remote/saml/login/"
      set single-logout-url "https://10.0.3.254:10443/remote/saml/logout/"
      set idp-entity-id "http://10.0.3.7/saml-idp/fgt2/metadata/"
      set idp-single-sign-on-url "https://10.0.3.7/saml-idp/fgt2/login/"
      set idp-single-logout-url "https://10.0.3.7/saml-idp/fgt2/logout/"
      set idp-cert "saml_idp.fortiad.info"
      set user-name "username"
      set group-name "group"
      set digest-method sha1
   next
end
```

- The setting `set cert <certificate>` corresponds to the SP certificate imported to the FortiGate as a local certificate earlier in the example.
- The setting `set idp-cert <certificate>` corresponds to the IdP certificate imported to the FortiGate as a remote certificate earlier in the example.

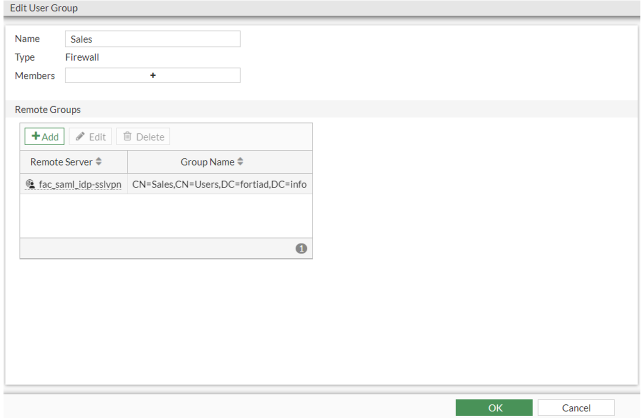
FortiGate user management

Once user authentication is successful on FortiAuthenticator, it sends a SAML assertion back to the client with the username and group information. When the client redirects this information to the FortiGate SAML SP, the FortiGate must process the assertion and match the correct user group for access control.

To configure user groups for Finance and Sales in FortiGate:

1. Go to *User & Authentication* > *User Groups* and select *Create New*.
2. To create a user group for **Sales**:
   a. In *Name*, enter *Sales*.
   b. In *Remote Groups*, click *Add*.
   c. Choose the SAML SSO settings as the *Remote Server*.
   d. Set *Groups* to *Specify* and enter the group name `CN=Sales,CN=Users,DC=fortiad,DC=info`.

e. Click *OK*.



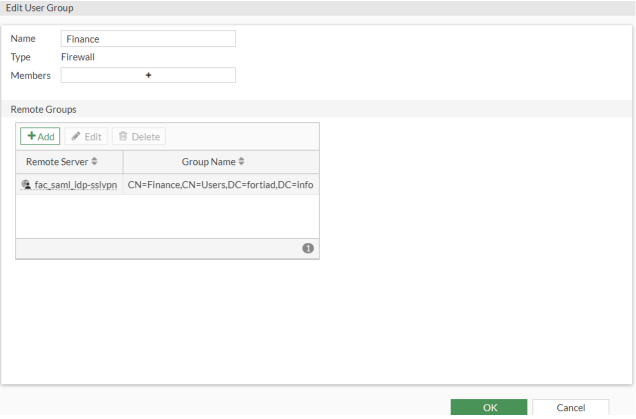
Edit User Group

Name: Sales
Type: Firewall
Members:

Remote Groups

Remote Server	Group Name
fac_saml_idp-sslvpn	CN=Sales,CN=Users,DC=fortiad,DC=info

3. To create a user group for **Finance**:
   a. In *Name*, enter *Finance*.
   b. In *Remote Groups*, click *Add*.
   c. Choose the SAML SSO settings as the *Remote Server*.
   d. Set *Groups* to *Specify*.
   The group name is the result of the output of the LDAP query for the **memberOf** attribute. In the example, this is `CN=Finance,CN=Users,DC=fortiad,DC=info`.
   e. Click *OK*.



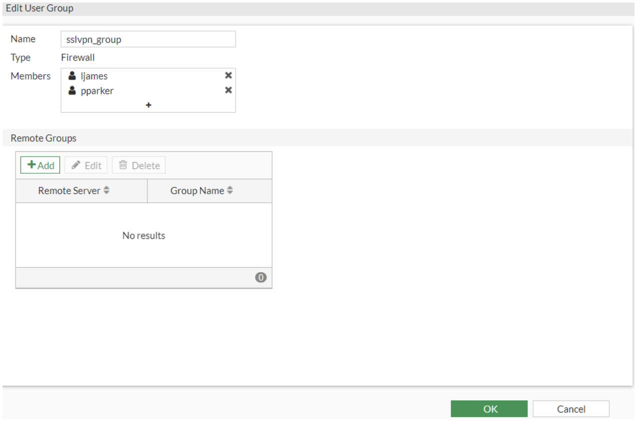
Edit User Group

Name: Finance
Type: Firewall
Members:

Remote Groups

Remote Server	Group Name
fac_saml_idp-sslvpn	CN=Finance,CN=Users,DC=fortiad,DC=info

Besides the groups for SAML users, a non-SAML placeholder group needs to be created in order for SSL VPN portal to be active. The following shows a placeholder group named `sslvpn_group` with 2 local users.



Edit User Group

Name: sslvpn_group
Type: Firewall
Members: ljames, pparker

Remote Groups

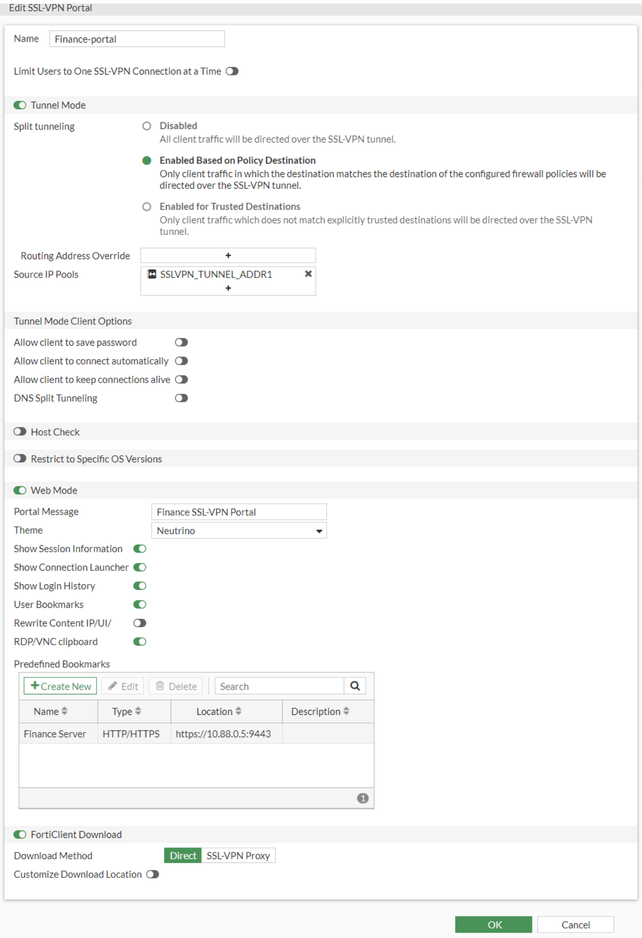
Remote Server	Group Name
No results	

FortiGate SSL VPN configurations

Configure SSL VPN portals and settings for **Finance** and **Sales** users to have remote network access. Firewall policies also need to be put into place for access control.

To configure SSL VPN portals for Finance and Sales users:

1. Go to *VPN* > *SSL-VPN Portals* and click *Create New*.
2. To create a profile named **Finance-portal**:
   a. In *Name*, enter *Finance-portal*.
   b. Enable *Tunnel Mode* with split tunneling set to *Enabled Based on Policy Destination*.
   c. Set *Source IP Pools* to a desired pool.
   d. Enable *Web Mode* and in *Portal Message*, enter *Finance SSL-VPN Portal*.
   e. In *Predefined Bookmarks*, select *Create New* to create a new bookmark called *Finance Server*. In our example, a *Finance server* is available on `https://10.88.0.5:9443`.
   f. Click *OK*.



Edit SSL-VPN Portal

Name: Finance-portal

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

● Tunnel Mode

Split tunneling
○ Disabled
All client traffic will be directed over the SSL-VPN tunnel.
● Enabled Based on Policy Destination
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.
○ Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override: +
Source IP Pools: SSLVPN_TUNNEL_ADDR1 ✖ +

Tunnel Mode Client Options
Allow client to save password ○
Allow client to connect automatically ○
Allow client to keep connections alive ○
DNS Split Tunneling ○

○ Host Check

○ Restrict to Specific OS Versions

● Web Mode

Portal Message: Finance SSL-VPN Portal
Theme: Neutrino
Show Session Information ●
Show Connection Launcher ●
Show Login History ●
User Bookmarks ●
Rewrite Content IP/UI/ ○
RDP/VNC clipboard ●

Predefined Bookmarks

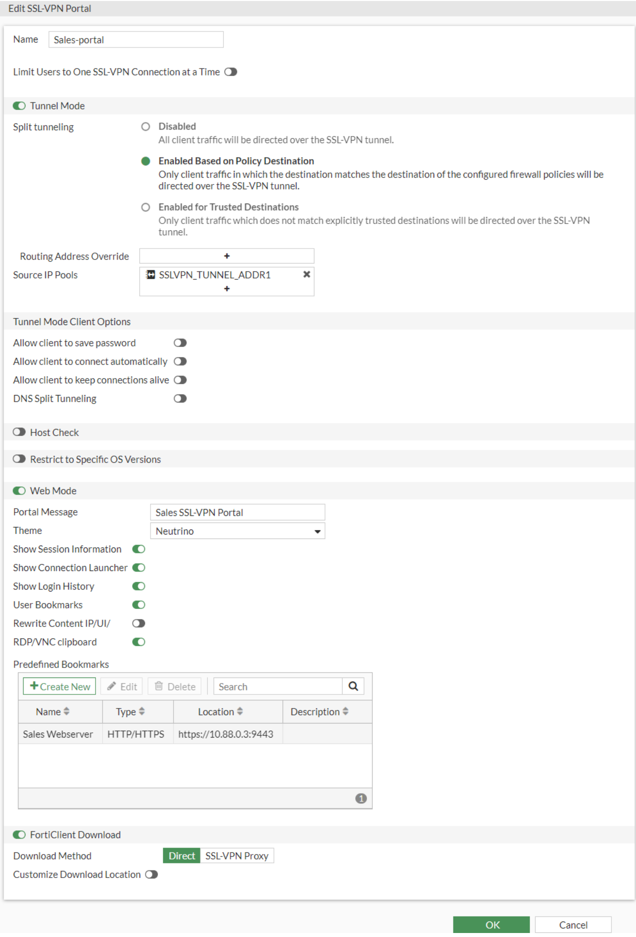
Name	Type	Location	Description
Finance Server	HTTP/HTTPS	https://10.88.0.5:9443	

● FortiClient Download

Download Method: [✓ Direct] SSL-VPN Proxy
Customize Download Location ○

3. To create a profile named **Sales-portal**:
   a. In *Name*, enter *Sales-portal*.
   b. Enable *Tunnel Mode* with split tunneling set to *Enabled Based on Policy Destination*.
   c. Set *Source IP Pools* to a desired pool.
   d. Enable *Web Mode* and in *Portal Message*, enter *Sales SSL-VPN Portal*.

e. In *Pre-defined Bookmarks*, create a new bookmark called *Sales Server*. In our example, a *Sales server* is available on `https://10.88.0.3:9443`.
f. Click *OK*.



Edit SSL-VPN Portal

Name: Sales-portal

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

● Tunnel Mode

Split tunneling
- ○ Disabled
  All client traffic will be directed over the SSL-VPN tunnel.
- ● Enabled Based on Policy Destination
  Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.
- ○ Enabled for Trusted Destinations
  Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override: +
Source IP Pools: SSLVPN_TUNNEL_ADDR1 ✖ +

Tunnel Mode Client Options

Allow client to save password ○
Allow client to connect automatically ○
Allow client to keep connections alive ○
DNS Split Tunneling ○

○ Host Check

○ Restrict to Specific OS Versions

● Web Mode

Portal Message: Sales SSL-VPN Portal
Theme: Neutrino
Show Session Information ●
Show Connection Launcher ●
Show Login History ●
User Bookmarks ●
Rewrite Content IP/UI/ ○
RDP/VNC clipboard ●

Predefined Bookmarks

+Create New | Edit | Delete | Search

Name	Type	Location	Description
Sales Webserver	HTTP/HTTPS	https://10.88.0.3:9443	

1

● FortiClient Download

Download Method: Direct | SSL-VPN Proxy
Customize Download Location ○

OK | Cancel

To configure SSL VPN settings:

1. Go to *VPN > SSL-VPN Settings* and enable SSL-VPN.
2. Set *Listen on Interface(s)* to *WAN (port3)*.
3. Set *Listen on Port* to *10443*.
4. Set the *Server Certificate* to *FGT-SSLVPN*.
5. In *Authentication/Portal Mapping*, configure user groups to portal mappings.
   a. Select *Create New* and create a new Finance mapping:
      i. Set *Users/Groups* to *Finance*.
      ii. Set *Portal* to *Finance-portal*.
      iii. Click *OK*.
   b. Select *Create New* and create a new Sales mapping:
      i. Set *Users/Groups* to *Sales*.
      ii. Set *Portal* to *Sales-portal*.
      iii. Click *OK*.

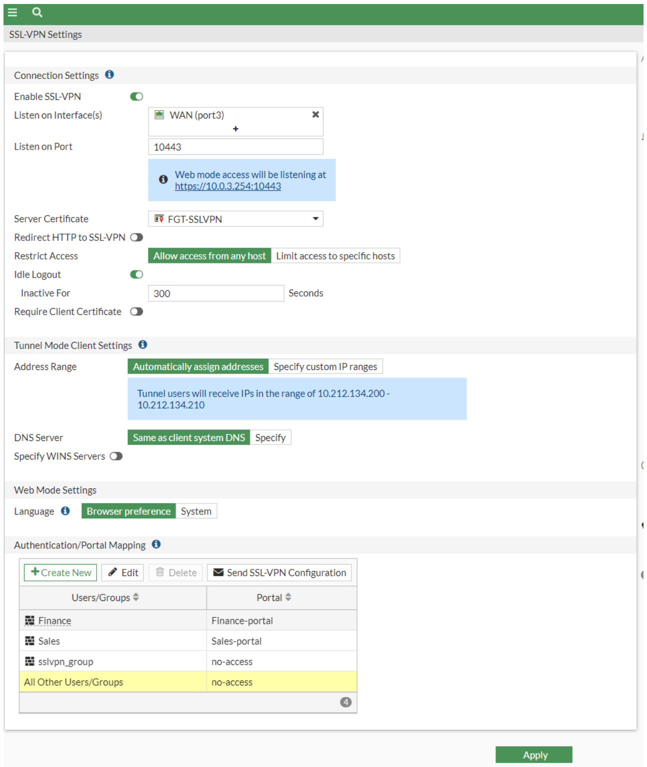
c. Select Create New and create a new placeholder mapping:

   i. Set *Users/Groups* to *sslvpn_group*.

   ii. Set *Portal* to *no-access*.

   iii. Click *OK*.

d. For *All other Users/Groups*, set *Portal* to *no-access*.



SSL-VPN Settings

Connection Settings

Enable SSL-VPN: on

Listen on Interface(s): WAN (port3)

Listen on Port: 10443

Web mode access will be listening at https://10.0.3.254:10443

Server Certificate: FGT-SSLVPN

Redirect HTTP to SSL-VPN: off

Restrict Access: Allow access from any host

Idle Logout: on

Inactive For: 300 Seconds

Require Client Certificate: off

Tunnel Mode Client Settings

Address Range: Automatically assign addresses

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: Same as client system DNS

Specify WINS Servers: off

Web Mode Settings

Language: Browser preference

Authentication/Portal Mapping

Users/Groups	Portal
Finance	Finance-portal
Sales	Sales-portal
sslvpn_group	no-access
All Other Users/Groups	no-access

To configure firewall policies for access control:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. Create a policy named *SSLVPN-Finance*.

   a. Set *Incoming Interface* to *SSL-VPN tunnel interface (ssl.root)*.

   b. Set *Outgoing Interface* to *port2*.

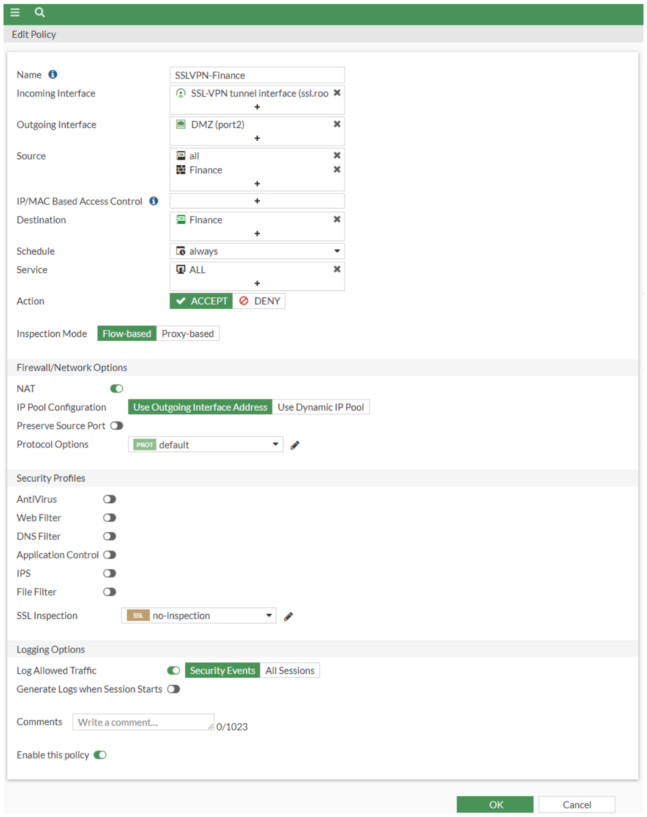
   c. Set *Source* to *all* and *User* to *Finance*.

   d. Set *Destination* to the Finance address object. If needed, create this object with the IP address `10.88.0.5/32`.

   e. Set *Service* to *ALL*.

   f. Configure other settings as needed.

g. Click *OK*.



Edit Policy

Name: SSLVPN-Finance

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

Outgoing Interface: DMZ (port2)

Source: all
Finance

IP/MAC Based Access Control

Destination: Finance

Schedule: always

Service: ALL

Action: [✓ ACCEPT] DENY

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: PROT default

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

IPS ○

File Filter ○

SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions

Generate Logs when Session Starts ○

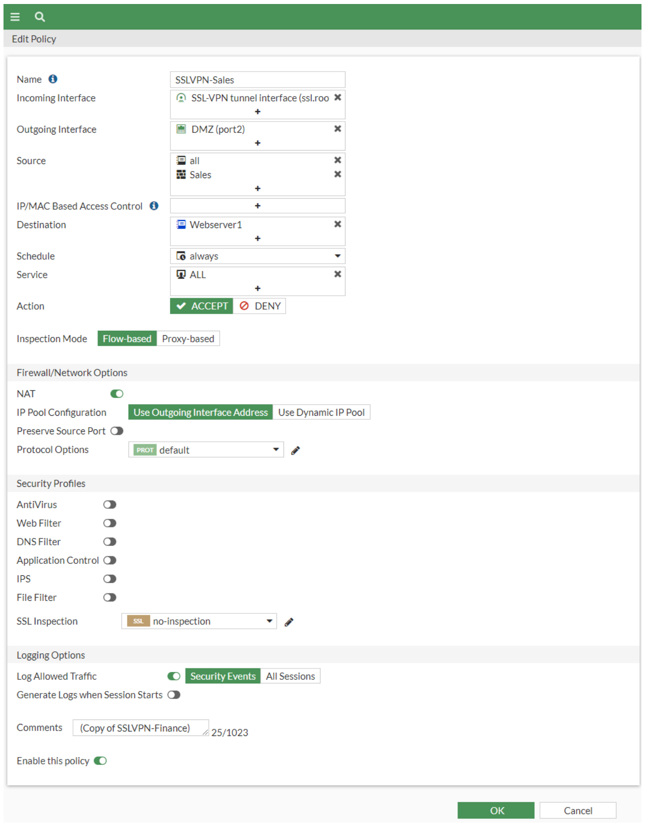
Comments: Write a comment... 0/1023

Enable this policy ●

OK Cancel

3. Create a policy named *SSLVPN-Sales*.
   a. Set *Incoming Interface* to *SSL-VPN tunnel interface (ssl.root)*.
   b. Set *Outgoing Interface* to *port2*.
   c. Set *Source* to *all* and *User* to *Sales*.
   d. Set *Destination* to the *Webserver1* address object. If needed, create this object with the IP address of `10.88.0.3/32`.
   e. Set *Service* to *ALL*.
   f. Configure other settings as needed.

g. Click *OK*.



Edit Policy

Name: SSLVPN-Sales
Incoming Interface: SSL-VPN tunnel interface (ssl.roo
Outgoing Interface: DMZ (port2)
Source: all, Sales
IP/MAC Based Access Control:
Destination: Webserver1
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY

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: PROT default

Security Profiles

AntiVirus ☐
Web Filter ☐
DNS Filter ☐
Application Control ☐
IPS ☐
File Filter ☐
SSL Inspection: SSL no-inspection

Logging Options

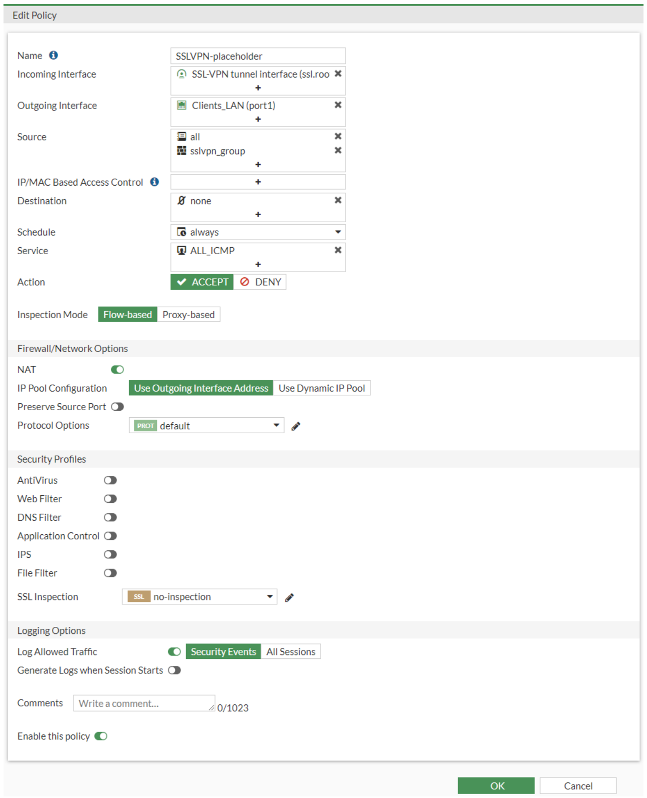
Log Allowed Traffic ☑ [✓ Security Events] All Sessions
Generate Logs when Session Starts ☐

Comments: (Copy of SSLVPN-Finance) 25/1023

Enable this policy ☑

4. Create a placeholder policy named *SSLVPN-placeholder*.
   a. Set *Incoming Interface* to *SSL-VPN tunnel interface (ssl.root)*.
   b. b. Set *Outgoing Interface* to *port1*.
   c. Set *Source* to *all* and *User* to *sslvpn_group*.
   d. Set *Destination* to *none*.
   e. Set *Service* to *ALL_ICMP*.

f. Click *OK*.



Edit Policy

Name	SSLVPN-placeholder
Incoming Interface	SSL-VPN tunnel interface (ssl.roo
Outgoing Interface	Clients_LAN (port1)
Source	all sslvpn_group
IP/MAC Based Access Control	
Destination	none
Schedule	always
Service	ALL_ICMP
Action	[✓ ACCEPT] DENY
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	PROT default

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL no-inspection

Logging Options

Log Allowed Traffic	● [✓ Security Events] All Sessions
Generate Logs when Session Starts	○
Comments	Write a comment... 0/1023
Enable this policy	●

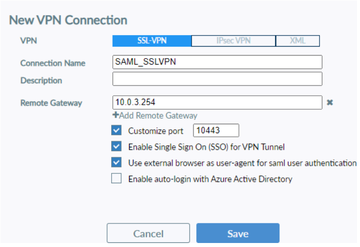
FortiClient configurations

In SSL-VPN tunnel mode, the FortiClient will initiate the connection. Below are two ways of configuring the SSL VPN connection profile.

To configure an SSL VPN remote access profile on FortiClient:

1. Go to the *Remote Access* tab.
2. Click the hamburger icon beside the *VPN Name* dropdown and select *Add a new connection*.
3. Set the *VPN* to *SSL-VPN*.
4. Set the *Connection Name* to *SAML_SSLVPN*.
5. Set *Remote Gateway* to `10.0.3.254`.
6. Select *Customize port* and set it to *10443*.
7. Select *Enable Single Sign On (SSO) for VPN Tunnel*.
8. Optionally, select *Use external browser as user-agent for saml user authentication* if you wish to use an external browser instead of the embedded module for authentication.

9. Click *Save*.



New VPN Connection

VPN: SSL-VPN | IPsec VPN | XML

Connection Name: SAML_SSLVPN

Description:

Remote Gateway: 10.0.3.254

☑ Customize port 10443

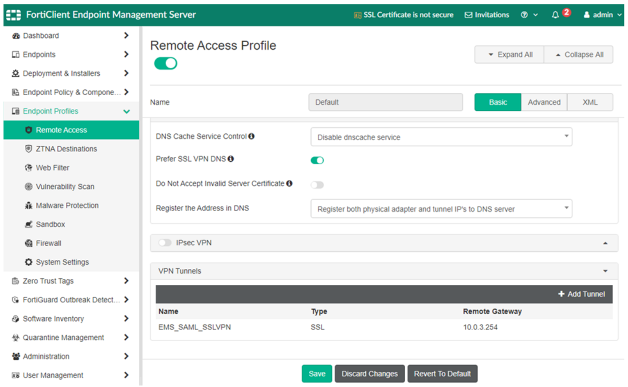
☑ Enable Single Sign On (SSO) for VPN Tunnel

☑ Use external browser as user-agent for saml user authentication

□ Enable auto-login with Azure Active Directory

To configure an SSL VPN remote access profile on FortiClient EMS:

1. Go to *Endpoint Profiles* > *Remote Access*.
2. Select an existing profile such as *Default* and click *Edit*.
3. In *VPN Tunnels*, add *Add Tunnel*.
4. In *VPN Type*, select *Manual* and click *Next*.
5. In *Basic Settings*:
   a. Set *Name* to *EMS_SAML_SSLVPN*.
   b. Set *Remote Gateway* to `10.0.3.254`.
   c. Set *Port* to *10443*.
6. In *Advanced Settings*:
   a. Enable *SAML Login*.
   b. b. Optionally, enable *Use external browser as user-agent for saml user authentication* if you wish to use an external browser instead of the embedded module for authentication.
7. Click *Save* to save the VPN profile.
8. Click *Save* again to save the changes to the *Remote Access Profile*.



Remote Access Profile

Name: Default

DNS Cache Service Control: Disable dnscache service

Prefer SSL VPN DNS: on

Do Not Accept Invalid Server Certificate: off

Register the Address in DNS: Register both physical adapter and tunnel IP's to DNS server

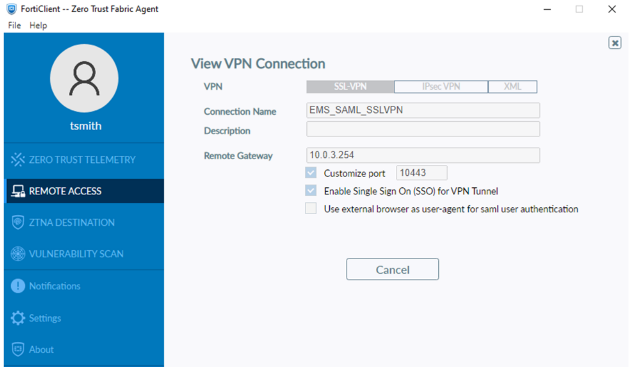
IPsec VPN: off

VPN Tunnels

Name	Type	Remote Gateway
EMS_SAML_SSLVPN	SSL	10.0.3.254

9. Shortly after, the FortiClient endpoint should receive the newly synced *EMS_SAML_SSLVPN* profile.

10. View the settings on FortiClient.



View VPN Connection

VPN: SSL-VPN | IPsec VPN | XML

Connection Name: EMS_SAML_SSLVPN

Description:

Remote Gateway: 10.0.3.254

☑ Customize port 10443

☑ Enable Single Sign On (SSO) for VPN Tunnel

□ Use external browser as user-agent for saml user authentication

Testing and verification

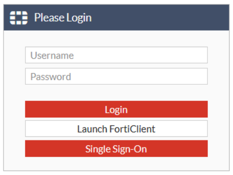
The following demonstrates connection via Web mode and Tunnel mode using SAML authentication. Review the authentication process at the beginning of this deployment scenario to understand how the process works.

For Web mode, import the CA certificate of the FortiAuthenticator Local CA into the trusted certificate store used by your browser. This will prevent warnings from appearing when accessing the SSL VPN web portal.

Web mode SSL VPN

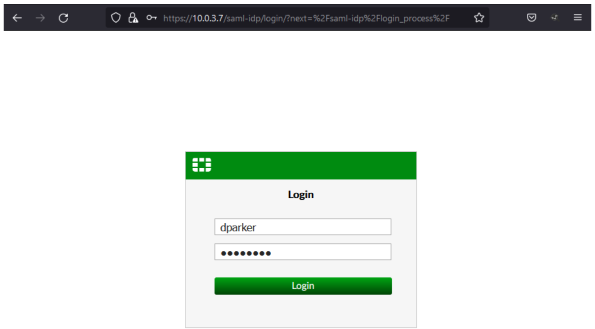
To verify a Web mode SSL VPN connection with the Finance user Dan Parker (dparker):

1. Open a browser, and enter `https://10.0.3.254:10443`.
2. Click *Single Sign-On* to sign in.



Your sign-on request will be redirected by the FortiGate SAML SP to the FortiAuthenticator SAML IdP.

3. Enter the user credentials for the user and click *Login*.



https://10.0.3.7/saml-idp/login/?next=%2Fsaml-idp%2Flogin_process%2F

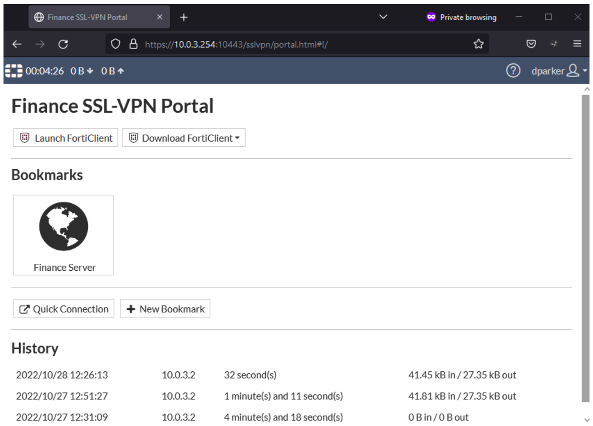
dparker

••••••••

In the background, the FortiAuthenticator authenticates this user over the LDAP connection to the Windows AD. If the authentication succeeds and matches a user group on FortiAuthenticator, FortiAuthenticator sends a SAML assertion back to the browser containing the username and group information.

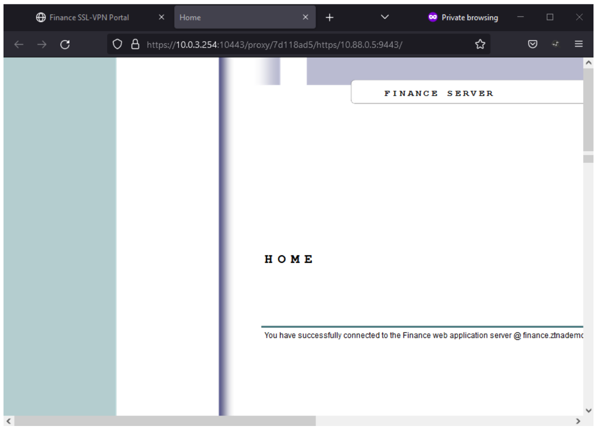
The browser redirects the SAML assertion to the FortiGate SAML SP, which matches the username and group information to a user group. Based on this user group, access is granted.

The Finance user can now see the Finance SSL-VPN Portal.



2022/10/28 12:26:13	10.0.3.2	32 second(s)	41.45 kB in / 27.35 kB out
2022/10/27 12:51:27	10.0.3.2	1 minute(s) and 11 second(s)	41.81 kB in / 27.35 kB out
2022/10/27 12:31:09	10.0.3.2	4 minute(s) and 18 second(s)	0 B in / 0 B out

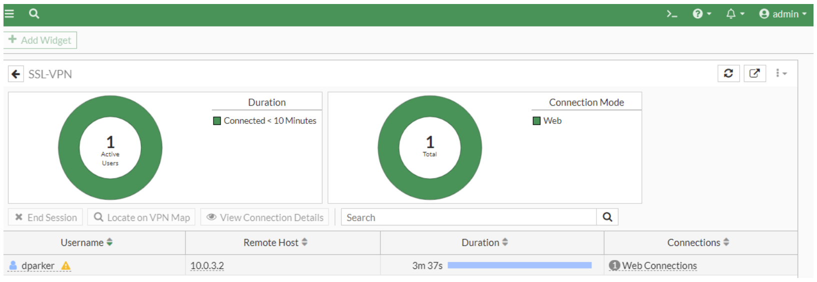
4. Clicking on the Finance Server bookmark, the user can access the Finance server.


Finance SSL-VPN Portal
Home
Private browsing
https://10.0.3.254:10443/proxy/7d118ad5/https/10.88.0.5:9443/
FINANCE SERVER
HOME

You have successfully connected to the Finance web application server @ finance.ztnademo

To verify the login status on the FortiGate and FortiAuthenticator:

1. On FortiGate, go to *Dashboard* > *Network* and expand the *SSL-VPN* widget.



Username	Remote Host	Duration	Connections
dparker	10.0.3.2	3m 37s	Web Connections

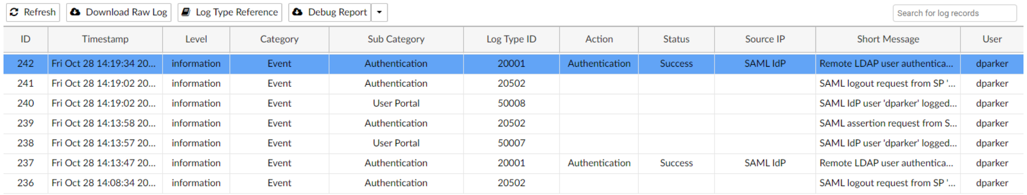
2. From *Log & Report* > *System Events*, switch to *VPN Events* log.

Alternatively, in the CLI console, enter the following commands:

```
   execute log filter category 1
   execute log filter field subtype vpn
   execute log display
1974 logs found.
10 logs returned.
```

```
38: date=2022-10-28 time=14:20:00 eventtime=1666992000214198069 tz="-0700"
logid="0101039938" type="event" subtype="vpn" level="warning" vd="root"
logdesc="SSL VPN pass" action="ssl-web-pass" tunneltype="ssl-web"
tunnelid=165774014 remip=10.0.3.2 user="dparker" group="Finance" dst_
host="10.88.0.5" reason="https" msg="SSL web application activated
```

3. On FortiAuthenticator, go to *Logging* > *Log Access* > *Logs*.
   The SAML IdP authentication for dparker will be displayed.

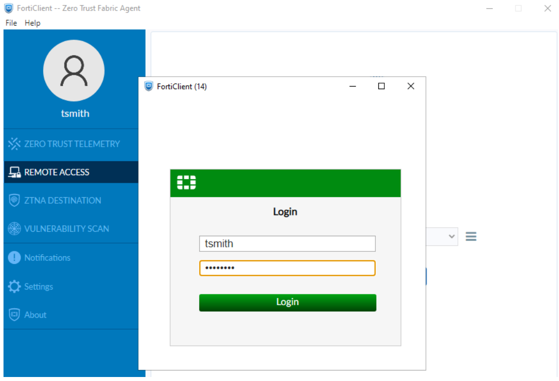


ID	Timestamp	Level	Category	Sub Category	Log Type ID	Action	Status	Source IP	Short Message	User
242	Fri Oct 28 14:19:34 20...	information	Event	Authentication	20001	Authentication	Success	SAML IdP	Remote LDAP user authentica...	dparker
241	Fri Oct 28 14:19:02 20...	information	Event	Authentication	20502				SAML logout request from SP '...	dparker
240	Fri Oct 28 14:19:02 20...	information	Event	User Portal	50008				SAML IdP user 'dparker' logged...	dparker
239	Fri Oct 28 14:13:58 20...	information	Event	Authentication	20502				SAML assertion request from S...	dparker
238	Fri Oct 28 14:13:57 20...	information	Event	User Portal	50007				SAML IdP user 'dparker' logged...	dparker
237	Fri Oct 28 14:13:47 20...	information	Event	Authentication	20001	Authentication	Success	SAML IdP	Remote LDAP user authentica...	dparker
236	Fri Oct 28 14:08:34 20...	information	Event	Authentication	20502				SAML logout request from SP '...	dparker

Tunnel mode SSL VPN

To verify a Tunnel mode SSL VPN connection with the Sales user Tom Smith (tsmith):

1. On the client desktop, open FortiClient and go to the *Remote Access* tab.
2. Select the VPN tunnel created earlier and click *SAML Login*.
3. When prompted for the login credentials, enter the username and password and click *Login*.



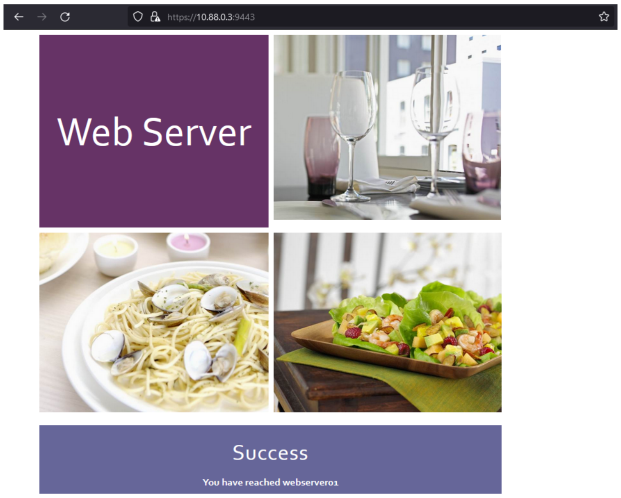
tsmith

••••••••

   Again, in the background, the SAML login request gets processed by FortiAuthenticator. Upon a successful match, it sends a SAML assertion back to the FortiClient. The FortiClient forwards this to the FortiGate which matches a corresponding user group.

4. Once connected, the user can open a browser and browse to `https://10.88.0.3:9443` to access the Sales

webserver.



https://10.88.0.3:9443

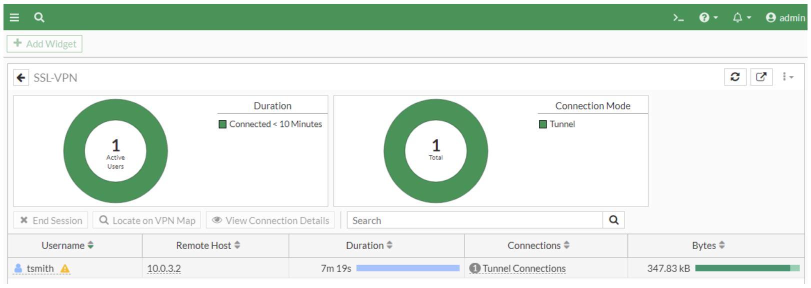
Web Server

Success

You have reached webserver01

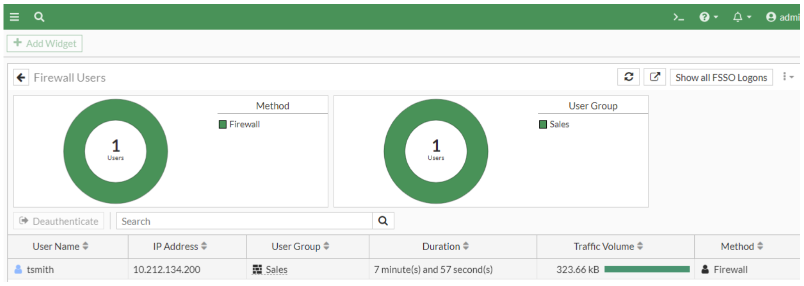
To verify the login status on the FortiGate and FortiAuthenticator:

1. On FortiGate, go to *Dashboard* > *Network* and expand the *SSL-VPN* widget.



Username	Remote Host	Duration	Connections	Bytes
tsmith ⚠	10.0.3.2	7m 19s	1 Tunnel Connections	347.83 kB

2. Go to *Dashboard* > *User & Devices* and expand the *Firewall Users* widget.



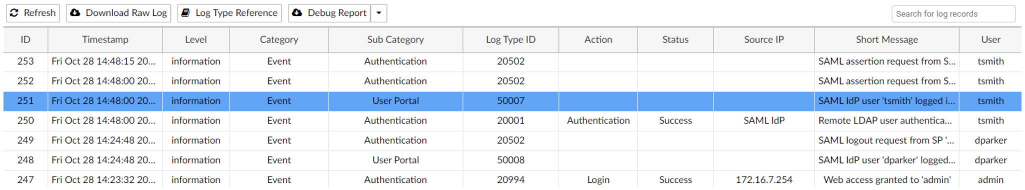
User Name	IP Address	User Group	Duration	Traffic Volume	Method
tsmith	10.212.134.200	Sales	7 minute(s) and 57 second(s)	323.66 kB	Firewall

3. From *Log & Report* > *System Events*, switch to *VPN Events* log.
   Alternatively, in the CLI console, enter the following commands:

```
   execute log filter category 1
   execute log filter field subtype vpn
   execute log display
2063 logs found.
10 logs returned.
10: date=2022-10-28 time=14:48:24 eventtime=1666993704610253079 tz="-0700"
logid="0101039947" type="event" subtype="vpn" level="information" vd="root"
logdesc="SSL VPN tunnel up" action="tunnel-up" tunneltype="ssl-tunnel"
```

```
tunnelid=165774015 remip=10.0.3.2 tunnelip=10.212.134.200 user="tsmith"
group="Sales" dst_host="N/A" reason="tunnel established" msg="SSL tunnel
established"
```

4. On FortiAuthenticator, go to *Logging* > *Log Access* > *Logs*.
   The SAML IdP authentication for tsmith will be displayed.



ID	Timestamp	Level	Category	Sub Category	Log Type ID	Action	Status	Source IP	Short Message	User
253	Fri Oct 28 14:48:15 20...	information	Event	Authentication	20502				SAML assertion request from S...	tsmith
252	Fri Oct 28 14:48:00 20...	information	Event	Authentication	20502				SAML assertion request from S...	tsmith
251	Fri Oct 28 14:48:00 20...	information	Event	User Portal	50007				SAML IdP user 'tsmith' logged i...	tsmith
250	Fri Oct 28 14:48:00 20...	information	Event	Authentication	20001	Authentication	Success	SAML IdP	Remote LDAP user authentica...	tsmith
249	Fri Oct 28 14:24:48 20...	information	Event	Authentication	20502				SAML logout request from SP '...	dparker
248	Fri Oct 28 14:24:48 20...	information	Event	User Portal	50008				SAML IdP user 'dparker' logged...	dparker
247	Fri Oct 28 14:23:32 20...	information	Event	Authentication	20994	Login	Success	172.16.7.254	Web access granted to 'admin'	admin

Computer Authentication

This section describes configuring computer authentication.

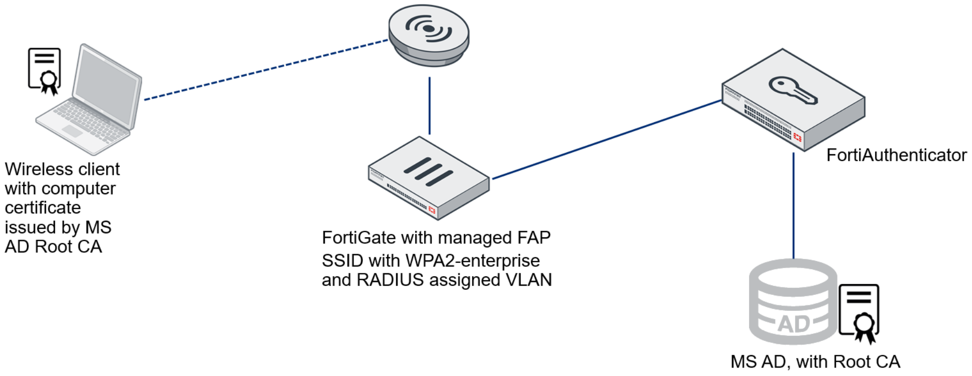
- Computer authentication using FortiAuthenticator with MS AD Root CA on page 283

Computer authentication using FortiAuthenticator with MS AD Root CA

This example includes the configuration required for computer authentication using FortiAuthenticator with a Microsoft Active Directory Root CA.

This configuration uses the following topology:

- Microsoft Active Directory configured with a Root CA.
- A wireless client with a computer certificate issued by the MS AD Root CA.
- A FortiGate and a managed FortiAP SSID with a WPA2-enterprise and RADIUS assigned VLAN.
- A FortiAuthenticator.


Wireless client with computer certificate issued by MS AD Root CA
FortiGate with managed FAP SSID with WPA2-enterprise and RADIUS assigned VLAN
FortiAuthenticator
AD
MS AD, with Root CA

To configure computer authentication using FortiAuthenticator with a Microsoft AD Root CA:

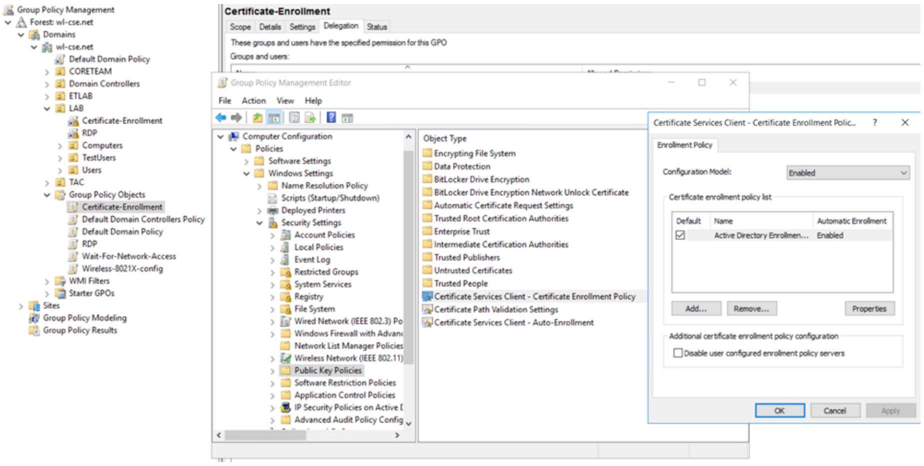
1. Configure the certificates and Root CA on page 283
2. Configure LDAP users on FortiAuthenticator on page 285
3. Configure RADIUS authentication on page 288
4. Configure the SSID and interface objects on page 293
5. Results on page 295

Configure the certificates and Root CA

With Microsoft Active Directory as the Root CA, use Group Policy Management to deploy client certificates to domain computers. This is the certificate that will be used to validate RADIUS requests.

To create a computer client certificate:

1. In *Active Directory* > *Group Policy Management*, create a new Group Policy Object (GPO) with settings configured for auto-enrollment.



Configuration Model: Enabled

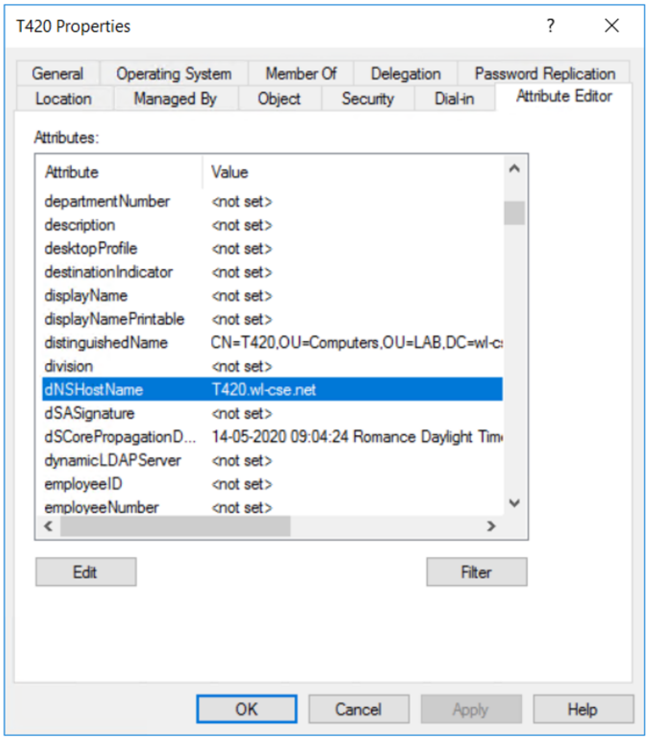
Certificate enrollment policy list

Default	Name	Automatic Enrollment
☑	Active Directory Enrollmen...	Enabled

Additional certificate enrollment policy configuration

☐ Disable user configured enrollment policy servers

2. Link the GPO to the OU where the client computers are located.
   The computer account in Active Directory must use the attribute `dNSHostName` with the value of the computer's name. This attribute is used later on FortiAuthenticator when creating the user remote sync rule.



Attributes:

Attribute	Value
departmentNumber	<not set>
description	<not set>
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	CN=T420,OU=Computers,OU=LAB,DC=wl-c:
division	<not set>
dNSHostName	T420.wl-cse.net
dSASignature	<not set>
dSCorePropagationD...	14-05-2020 09:04:24 Romance Daylight Tim
dynamicLDAPServer	<not set>
employeeID	<not set>
employeeNumber	<not set>

To import the Microsoft AD Root CA as a trusted CA:

1. On the FortiGate, go to *System* > *Certificates*, and click *Import* > *CA Certificate*. Configure the following settings, and click *OK* when complete.
   a. **Type**: *File*.
   b. **Upload**: Click *Upload* and browse to the location of your certificate.

2. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs*, and click *Import*. Configure the following settings, and click *OK* when complete.
   a. **Certificate ID**: Enter the certificate ID.
   b. **Certificate**: Click *Upload a file* and browse to the location of your certificate.

Once the Root CA is configured, you can issue certificates from AD to both the FortiGate and the FortiAuthenticator.

Configure LDAP users on FortiAuthenticator

You can now configure the remote LDAP server on FortiAuthenticator to connect to Active Directory, create a user realm and user group, and import the AD users into FortiAuthenticator using a remote user sync rule.

To configure LDAP users on FortiAuthenticator:

1. Configuring the LDAP server on page 285
2. Creating a user realm on page 286
3. Creating a user group on page 287
4. Importing users with a remote user sync rule on page 287

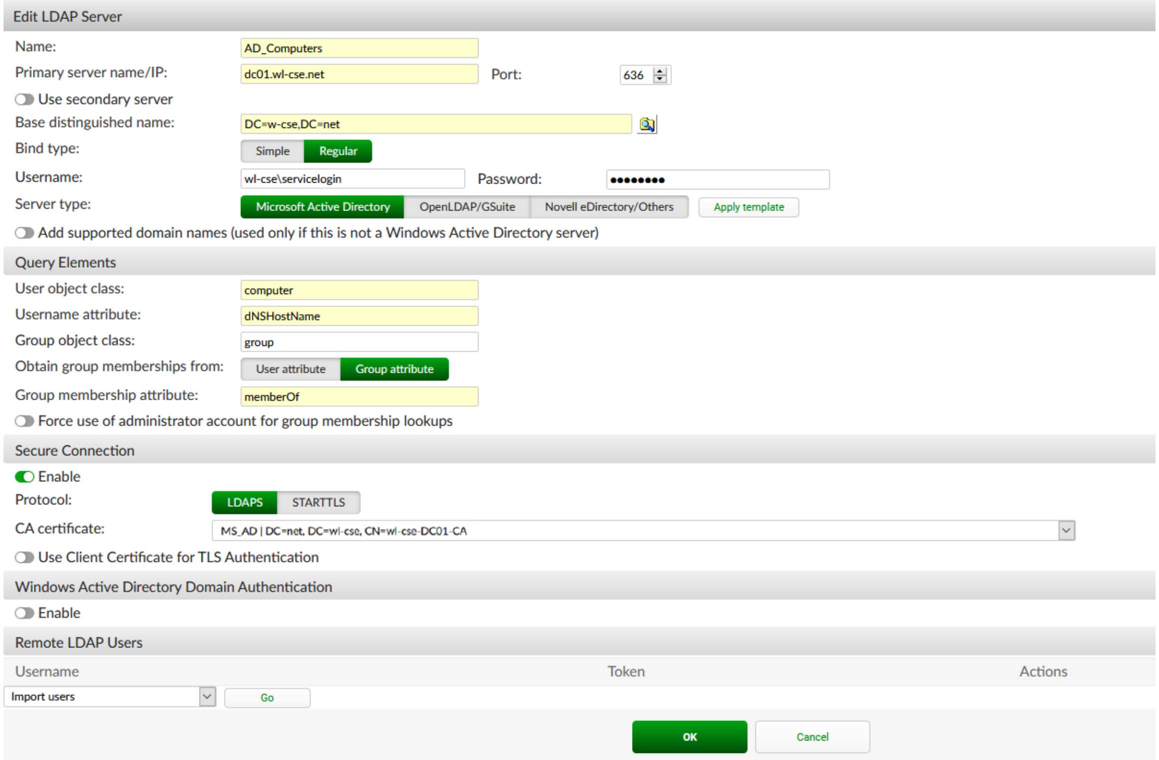
Configuring the LDAP server

Create an LDAP entry for remote lookup of computers with the username attribute as `dNSHostName`.

To configure remote LDAP server on FortiAuthenticator:

1. In FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and click *Create New*.
2. Under *Create New LDAP Server*, set the following:
   a. **Name**: Enter the server name, for example: `AD_Computers`.
   b. **Primary server name/IP**: Enter the LDAP server name, for example: `dc01.wl-cse.net` using *Port* 636.
   c. **Base distinguished name**: Enter the base distinguished name, for example: `DC=wl-cse,DC=net`.
   d. **Bind type**: *Regular*.
      Enter the username and password for your LDAP user.
3. Under *Query Elements*, set the following:
   a. **User object class**: `computer`.
   b. **Username attribute**: `dNShostName`.
   c. **Group object class**: `group`.
   d. **Obtain group memberships from**: *Group attribute*.
   e. **Group membership attribute**: `memberOf`.

4. Enable *Secure Connection*, and set the following:
   a. **Protocol**: *LDAPS*.
   b. **CA certificate**: Select the CA certificate you previously configured.



Edit LDAP Server

Name:	AD_Computers		
Primary server name/IP:	dc01.wl-cse.net	Port:	636
○ Use secondary server			
Base distinguished name:	DC=w-cse,DC=net		
Bind type:	Simple / **Regular**		
Username:	wl-cse\servicelogin	Password:	••••••••
Server type:	**Microsoft Active Directory** / OpenLDAP/GSuite / Novell eDirectory/Others	Apply template	

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

Query Elements

User object class:	computer
Username attribute:	dNSHostName
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:	MS_AD | DC=net, DC=wl-cse, CN=wl-cse-DC01-CA

○ Use Client Certificate for TLS Authentication

Windows Active Directory Domain Authentication

○ Enable

Remote LDAP Users

Username	Token	Actions
Import users	Go	

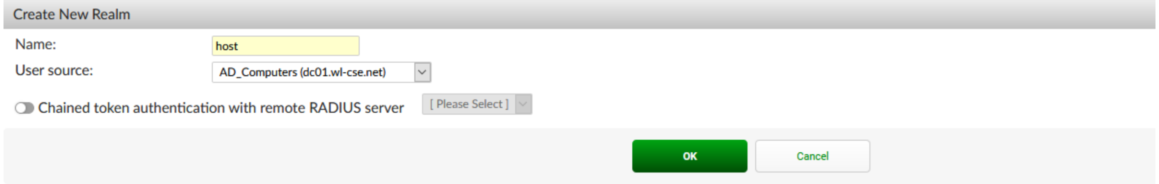
5. Click *OK*.

Creating a user realm

Create a user realm for the users (computers) from your remote LDAP. This realm is used later when configuring RADIUS authentication.

To create a user realm:

1. Go to *Authentication* > *User Management* > *Realms*, and click *Create New*.
2. Set the following:
   a. **Name**: Enter a name for the realm, for example: `host`.
   b. **User source**: Select the previously configured remote LDAP server.



Create New Realm

Name:	host
User source:	AD_Computers (dc01.wl-cse.net)

○ Chained token authentication with remote RADIUS server [Please Select]

3. Click *OK*.

Creating a user group

Create a user group for the users (computers) from your remote LDAP.

To create a remote LDAP user group:

1. Go to *Authentication* > *User Management* > *User Groups*, and click *Create New*.
2. Set the following:
   a. **Name**: Enter a name for the LDAP group, for example: `AD_LAB_PC`.
   b. **Type**: *Remote LDAP*.
   c. **User retrieval**: Set a list of imported remote LDAP users.
   d. **Remote LDAP**: Select the previously configured remote LDAP server, for example *AD_Computers*.
   e. **LDAP users**: Add your chosen LDAP users to the *Selected LDAP Users* pane.
3. Click *OK*.

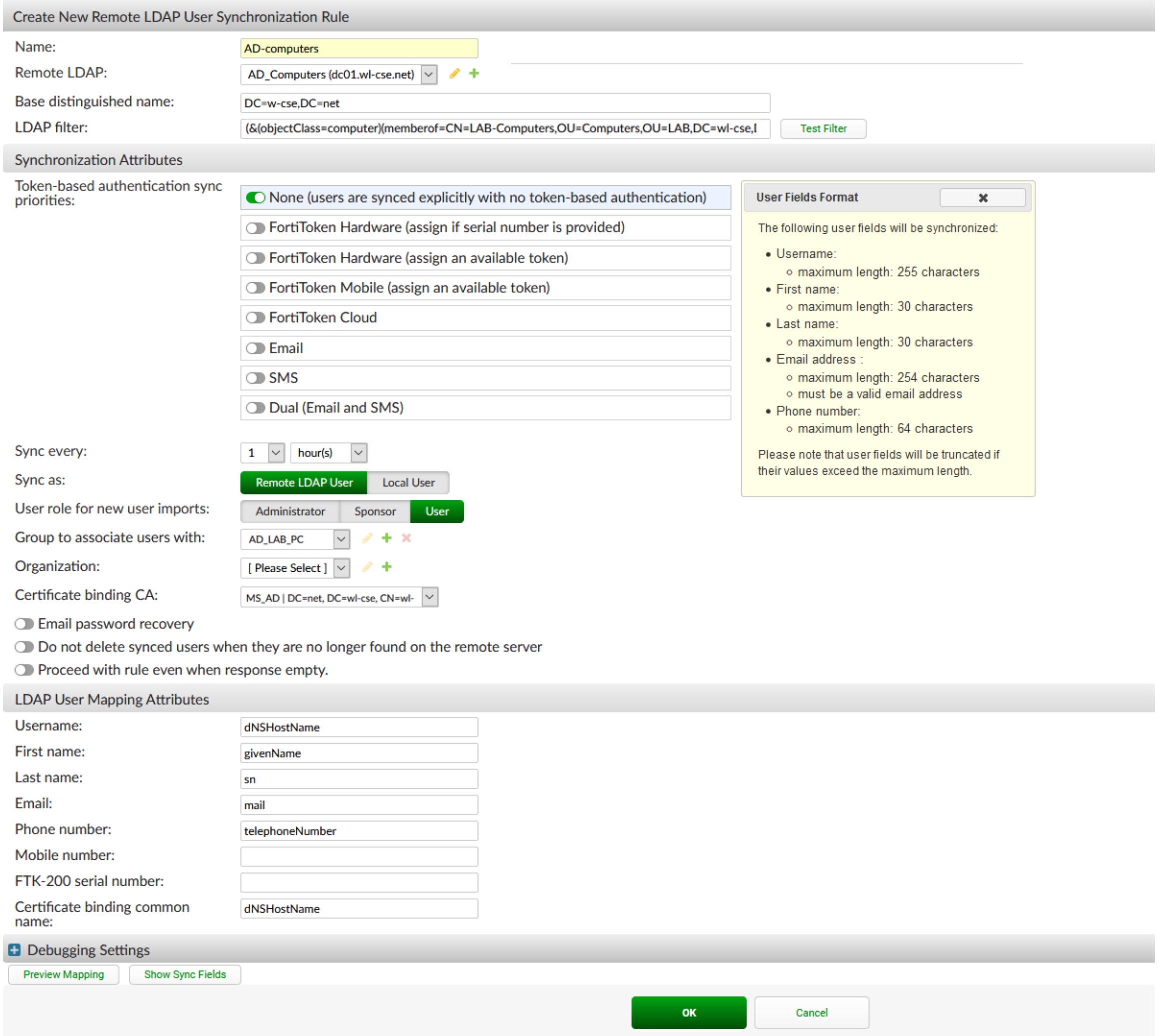
Importing users with a remote user sync rule

Create the user sync rule to import your users (computers) into FortiAuthenticator. You can configure this rule with an LDAP filter to match specific groups in Active Directory. For the LDAP *username* and *certificate binding common name*, use `dNSHostName`. This must match the CN of the actual issued certificate.

To configure a remote user sync rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rules*, and click *Create New*.
2. Under *Edit Remote LDAP User Synchronization Rule*, set the following:
   a. **Name**: Enter a name for the rule, for example: `AD-computers`.
   b. **Remote LDAP**: Select the remote LDAP server you previously configured.
   c. **Base distinguished name**: Enter your base distinguished name, for example: `DC=wl-cse,DC=net`.
   d. **LDAP filter**: Select the LDAP filter which matches your specific group in Active Directory, for example: `(&(objectClass=computer)(memberof=CN=LAB-Computers,OU=Computers,OU=LAB,DC=wl-cse,DC=net))`.
3. Under *Synchronization Attributes*, set the following:
   a. **Token-based authentication sync priorities**: Select *None*.
   b. **Sync every**: Select the sync frequency based on your preferences, for example: *1 hour(s).*
   c. **Sync as**: *Remote LDAP User*.
   d. **User role for new user imports**: *User*.
   e. **Group to associate users with**: Select your remote LDAP user group.
   f. **Certificate binding CA**: Select your CA for certificate binding.

4. Under *LDAP User Mapping Attributes*, set the following:
   a. **Username**: `dNSHostName`.
   b. **Certificate binding common name**: `dNSHostName`.



Create New Remote LDAP User Synchronization Rule

Name:	AD-computers
Remote LDAP:	AD_Computers (dc01.wl-cse.net)
Base distinguished name:	DC=w-cse,DC=net
LDAP filter:	(&(objectClass=computer)(memberof=CN=LAB-Computers,OU=Computers,OU=LAB,DC=wl-cse,I

Synchronization Attributes

Token-based authentication sync priorities:

- ● 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)
- ○ FortiToken Cloud
- ○ Email
- ○ SMS
- ○ Dual (Email and SMS)

User Fields Format

The following user fields will be synchronized:

- Username:
  - maximum length: 255 characters
- First name:
  - maximum length: 30 characters
- Last name:
  - maximum length: 30 characters
- Email address :
  - maximum length: 254 characters
  - must be a valid email address
- Phone number:
  - maximum length: 64 characters

Please note that user fields will be truncated if their values exceed the maximum length.

Sync every:	1 hour(s)
Sync as:	[✓ Remote LDAP User] Local User
User role for new user imports:	Administrator Sponsor [✓ User]
Group to associate users with:	AD_LAB_PC
Organization:	[Please Select]
Certificate binding CA:	MS_AD | DC=net, DC=wl-cse, CN=wl-

- ○ Email password recovery
- ○ 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:	dNSHostName
First name:	givenName
Last name:	sn
Email:	mail
Phone number:	telephoneNumber
Mobile number:	
FTK-200 serial number:	
Certificate binding common name:	dNSHostName

5. Click *OK*.

Once the user sync rule has been created, run it to import your user (computer) account, and then verify the user was successfully created in *Authentication* > *User Management* > *Remote Users* and that the certificate binding is in place.

Configure RADIUS authentication

You can now configure RADIUS authentication between the FortiAuthenticator and FortiGate.

To configure RADIUS authentication:

1. Adding RADIUS attributes on page 289
2. Configuring the RADIUS client on page 289
3. Configuring the EAP server certificate on page 290

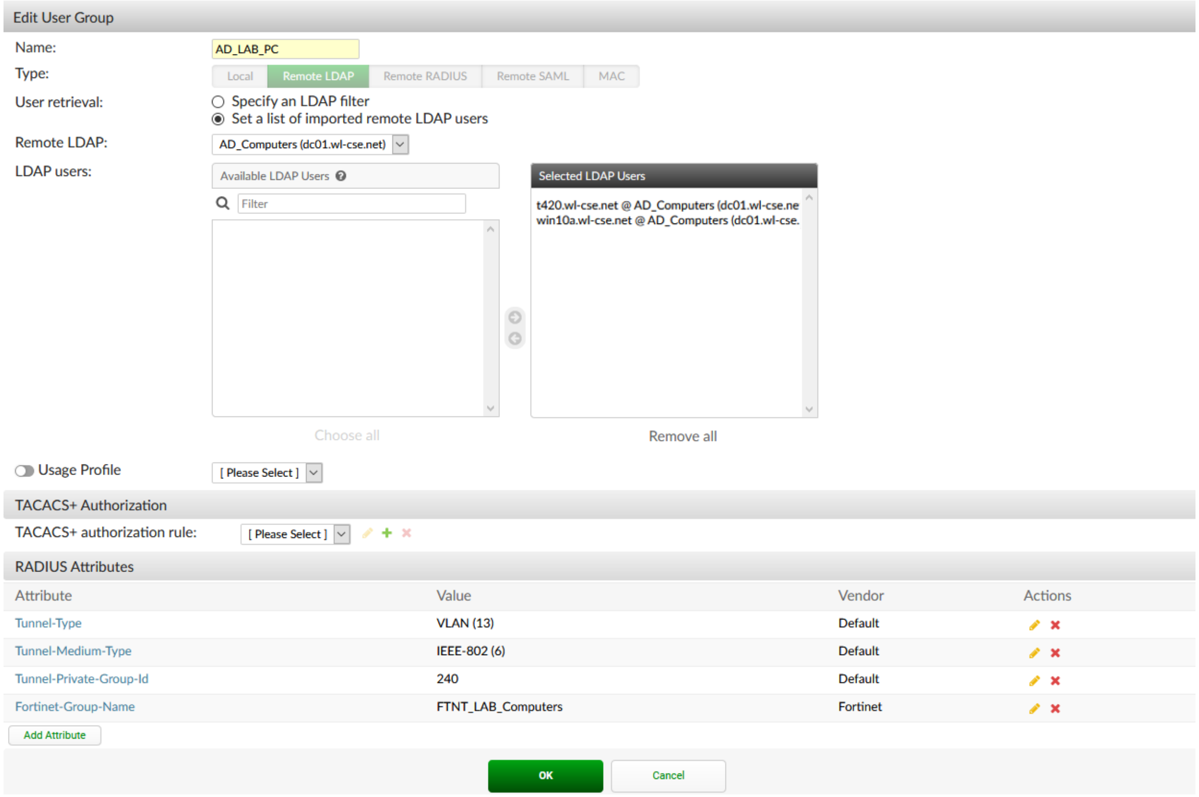
4. Creating a RADIUS policy on page 290
5. Configuring the RADIUS server on FortiGate on page 292

Adding RADIUS attributes

RADIUS attributes can be added to the previously configured LDAP user group.

To add RADIUS attributes to the LDAP user group:

1. Go to *Authentication* > *User Management* > *User Groups*, and edit the user group associated with the remote LDAP users.
2. Under *RADIUS Attributes*, add the RADIUS attributes required by your configuration. In this example, the following attributes are required:
   - Tunnel-Type: VLAN.
   - Tunnel-Medium-Type: IEEE-802.
   - Tunnel-Private-Group-Id: 240.
   - Fortinet-Group-Name: FTNT_LAB_Computers.



Edit User Group

Name: AD_LAB_PC

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

User retrieval: ○ Specify an LDAP filter ● Set a list of imported remote LDAP users

Remote LDAP: AD_Computers (dc01.wl-cse.net)

LDAP users: Available LDAP Users

Selected LDAP Users:
t420.wl-cse.net @ AD_Computers (dc01.wl-cse.ne
win10a.wl-cse.net @ AD_Computers (dc01.wl-cse.

Usage Profile: [Please Select]

TACACS+ Authorization

TACACS+ authorization rule: [Please Select]

RADIUS Attributes

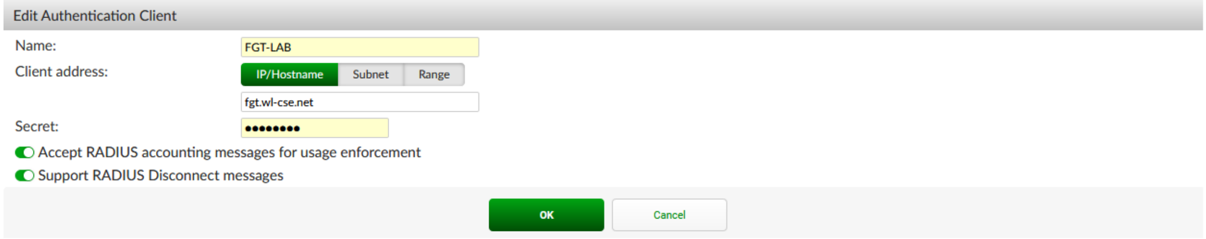
Attribute	Value	Vendor	Actions
Tunnel-Type	VLAN (13)	Default	✎ ✖
Tunnel-Medium-Type	IEEE-802 (6)	Default	✎ ✖
Tunnel-Private-Group-Id	240	Default	✎ ✖
Fortinet-Group-Name	FTNT_LAB_Computers	Fortinet	✎ ✖

Configuring the RADIUS client

To configure RADIUS authentication using FortiAuthenticator, the FortiGate must be configured as a RADIUS client.

To configure the RADIUS client settings:

1. Go to *Authentication* > *RADIUS Service* > *Clients*, and click *Create New*.
2. Set the following:
   a. **Name**: Enter a name for the RADIUS client, for example: `FGT-LAB`.
   b. **Client address**: Select IP/Hostname, and enter your RADIUS client's IP or hostname, for example: `fgt.wl-cse.net`.
   c. **Secret**: Enter a shared secret. This will also be used to configure RADIUS settings on FortiGate.
   d. **(Optional) Accept RADIUS accounting messages for usage enforcement**: *Enabled*.
   e. **(Optional) Support RADIUS Disconnect messages**: *Enabled.*



Edit Authentication Client

Name: FGT-LAB

Client address: IP/Hostname

fgt.wl-cse.net

Secret: ••••••••

● Accept RADIUS accounting messages for usage enforcement

● Support RADIUS Disconnect messages

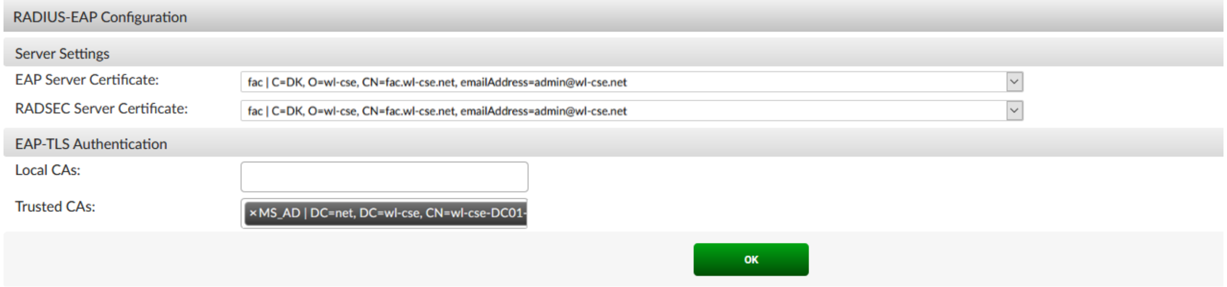
3. Click *OK*.

Configuring the EAP server certificate

In order to use EAP, you must specify the certificate used for FortiAuthenticator in the RADIUS-EAP configuration settings.

To configure the RADIUS certificate for EAP-TLS:

1. Go to *Authentication* > *RADIUS Service* > *Certificates*.
2. Specify the *EAP Server Certificate* and the *Trusted CA* from Active Directory that you previously configured.



RADIUS-EAP Configuration

Server Settings

EAP Server Certificate: fac | C=DK, O=wl-cse, CN=fac.wl-cse.net, emailAddress=admin@wl-cse.net

RADSEC Server Certificate: fac | C=DK, O=wl-cse, CN=fac.wl-cse.net, emailAddress=admin@wl-cse.net

EAP-TLS Authentication

Local CAs:

Trusted CAs: ×MS_AD | DC=net, DC=wl-cse, CN=wl-cse-DC01-

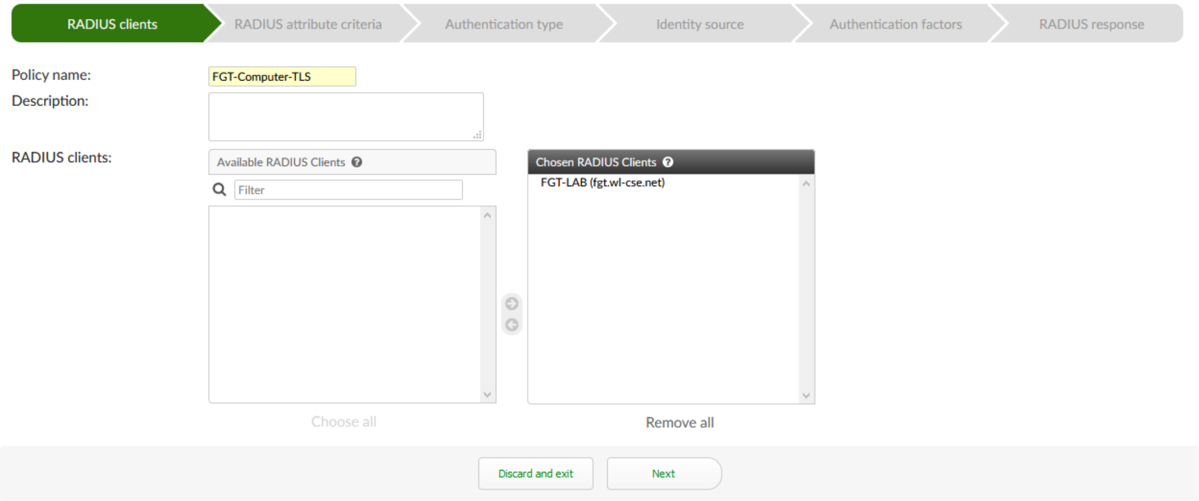
3. Click *OK*.

Creating a RADIUS policy

A RADIUS policy must be configured in order to allow RADIUS authentication for the selected client.

To create a RADIUS policy:

1. Go to *Authentication > RADIUS Service > Policies*, and click *Create New*.
2. Under RADIUS clients, configure the following, and click *Next*.
   a. **Policy name**: Enter a name for this policy, for example: *FGT-Computer-TLS*.
   b. **RADIUS clients**: Add the previously configured FortiGate RADIUS client to the *Chosen RADIUS Clients* section.



Policy name: FGT-Computer-TLS

Description:

RADIUS clients:

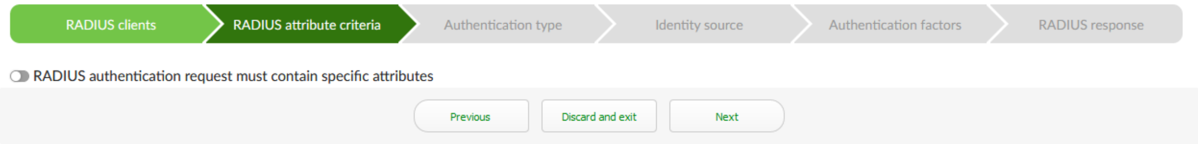
Available RADIUS Clients

Filter

Chosen RADIUS Clients

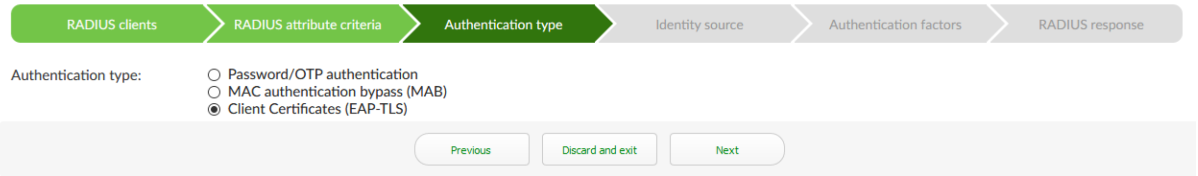
FGT-LAB (fgt.wl-cse.net)

3. Under *RADIUS attribute criteria*, click *Next*.



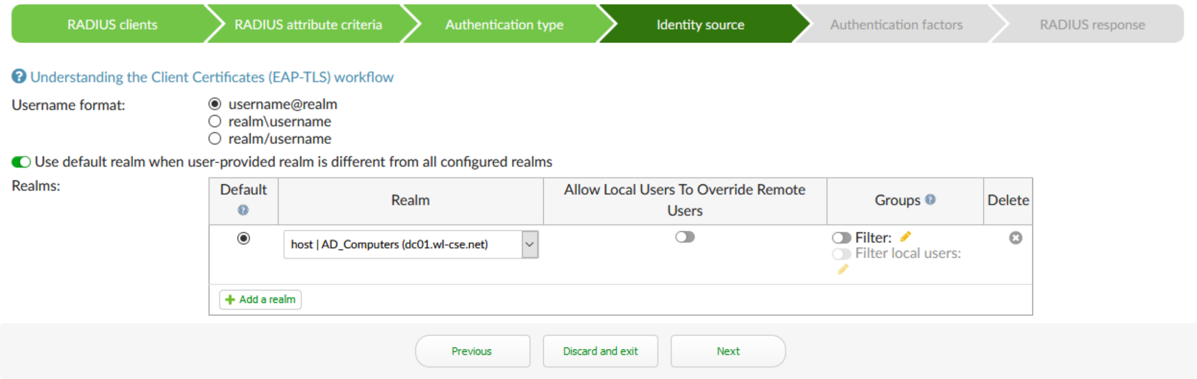
RADIUS authentication request must contain specific attributes

4. Under *Authentication type*, choose *Client Certificates (EAP-TLS)*, and click *Next*.



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

5. Under *Identity source*, configure the following, and click *Next*.
   a. **Username format**: Select your preferred username format, for example: *realm\username*.
   b. **Realms**: In the *Realms* table, select your AD realm.
   You can additionally apply a group filter if required.



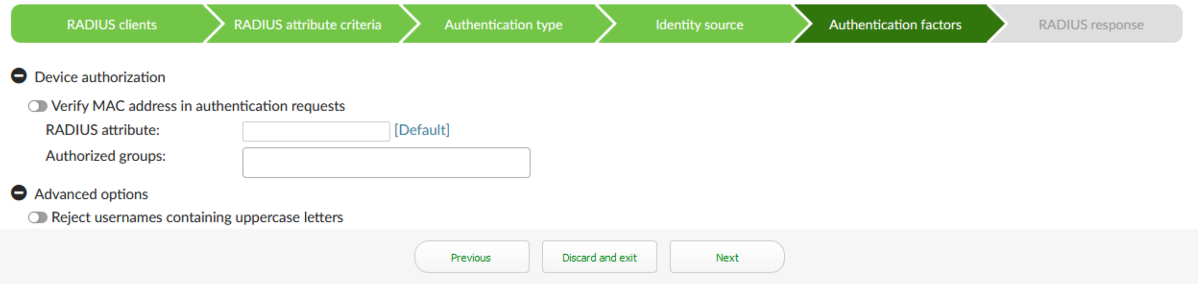
Username format:
● username@realm
○ realm\username
○ realm/username

Use default realm when user-provided realm is different from all configured realms

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	host | AD_Computers (dc01.wl-cse.net)		Filter: Filter local users:	

6. Under *Authentication factors*, click *Next*.



● Device authorization

○ Verify MAC address in authentication requests

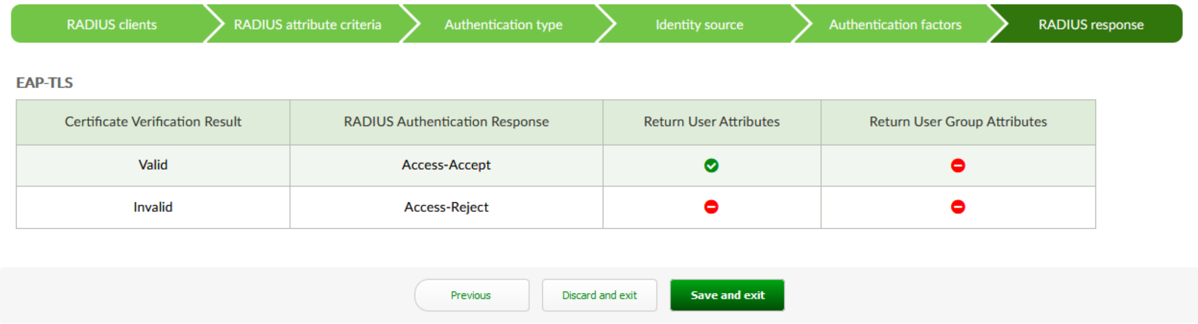
RADIUS attribute: [Default]

Authorized groups:

● Advanced options

○ Reject usernames containing uppercase letters

7. Under *RADIUS response*, click *Save and exit*.



EAP-TLS

Certificate Verification Result	RADIUS Authentication Response	Return User Attributes	Return User Group Attributes
Valid	Access-Accept	✓	⛔
Invalid	Access-Reject	⛔	⛔

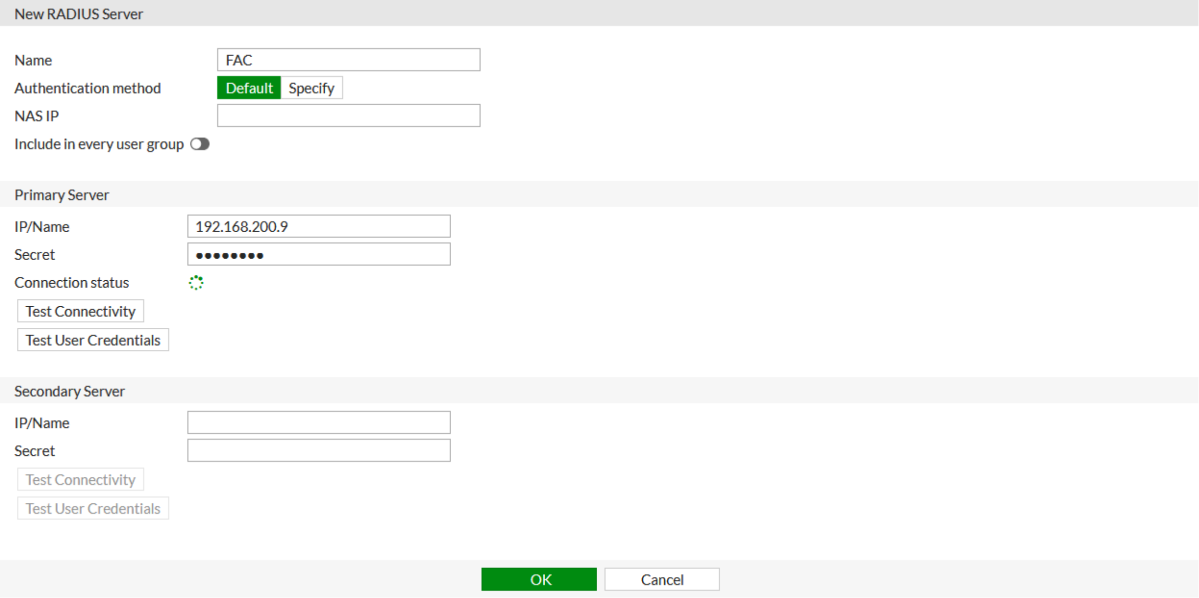
Configuring the RADIUS server on FortiGate

Finally, you can configure the RADIUS server settings (FortiAuthenticator) on FortiGate.

To configure the RADIUS server on FortiGate:

1. On FortiGate, go to *User & Authentication > RADIUS Servers*, and click *Create New*.
2. Under *New RADIUS Server*, set the following:
   a. **Name**: Enter a name for the RADIUS server, for example: *FAC*.
   b. **Authentication method**: *Default*.

3. Under *Primary Server*, set the following:
   a. **IP/Name**: Enter the IP address of the FortiAuthenticator.
   b. **Secret**: Enter the RADIUS server secret created on FortiAuthenticator.



New RADIUS Server

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

Primary Server

IP/Name: 192.168.200.9
Secret: ••••••••
Connection status

Secondary Server

IP/Name:
Secret:

4. Click *OK*.

Configure the SSID and interface objects

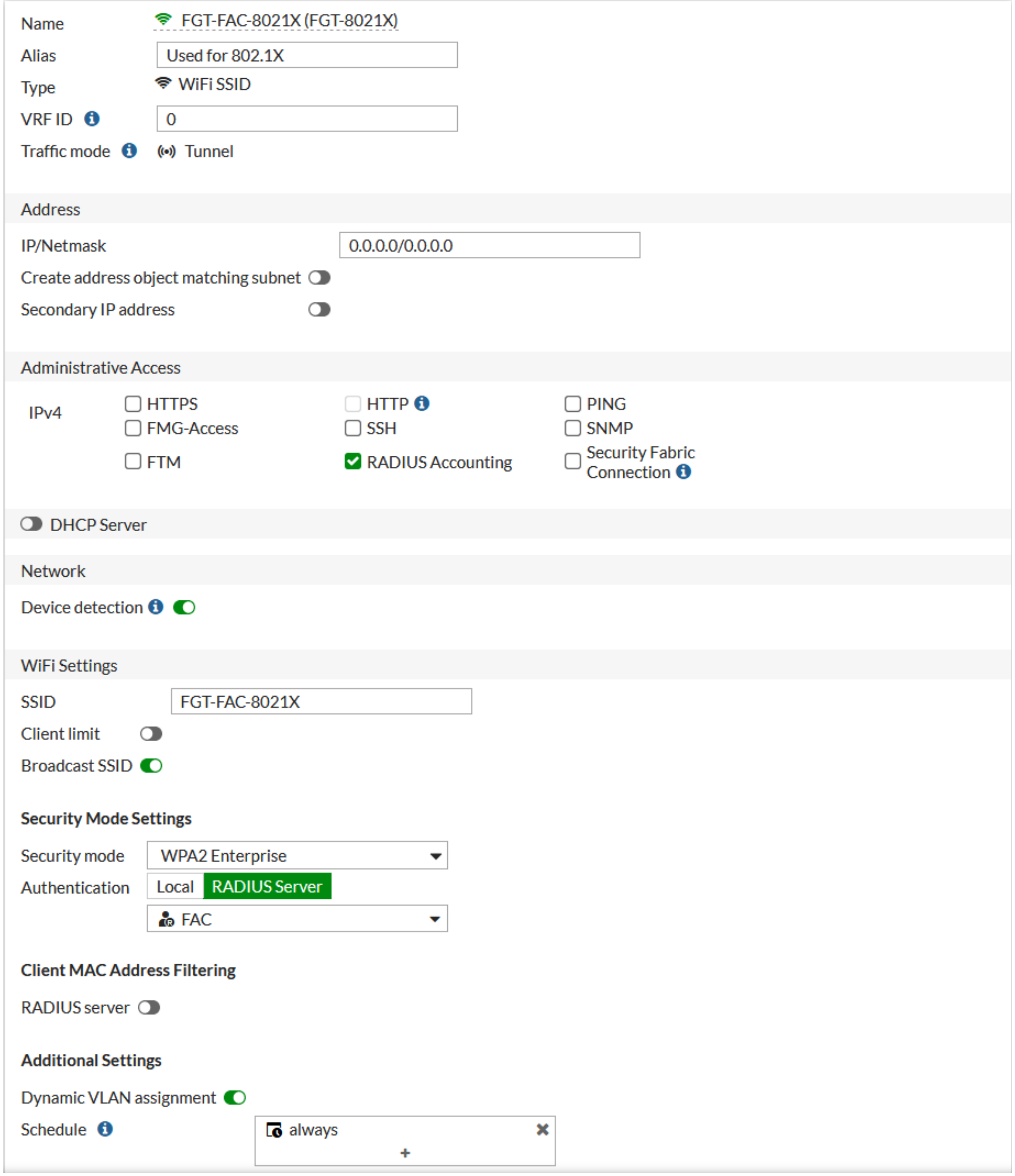
To configure the SSID and interface objects:

1. Creating the SSID on page 294
2. Creating interfaces on page 295

Creating the SSID

To create an SSID with dynamic VLAN assignment:

1. On FortiGate, go to *WiFi & Switch Controller > SSID*, and click *Create New > SSID*.
2. Create a new SSID with *Dynamic VLAN assignment* enabled under *Additional Settings*.



Name FGT-FAC-8021X (FGT-8021X)

Alias Used for 802.1X

Type WiFi SSID

VRF ID 0

Traffic mode Tunnel

Address

IP/Netmask 0.0.0.0/0.0.0.0

Create address object matching subnet ○

Secondary IP address ○

Administrative Access

IPv4 ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ FTM ☑ RADIUS Accounting ☐ Security Fabric Connection

○ DHCP Server

Network

Device detection ●

WiFi Settings

SSID FGT-FAC-8021X

Client limit ○

Broadcast SSID ●

Security Mode Settings

Security mode WPA2 Enterprise

Authentication Local [✓ RADIUS Server]

FAC

Client MAC Address Filtering

RADIUS server ○

Additional Settings

Dynamic VLAN assignment ●

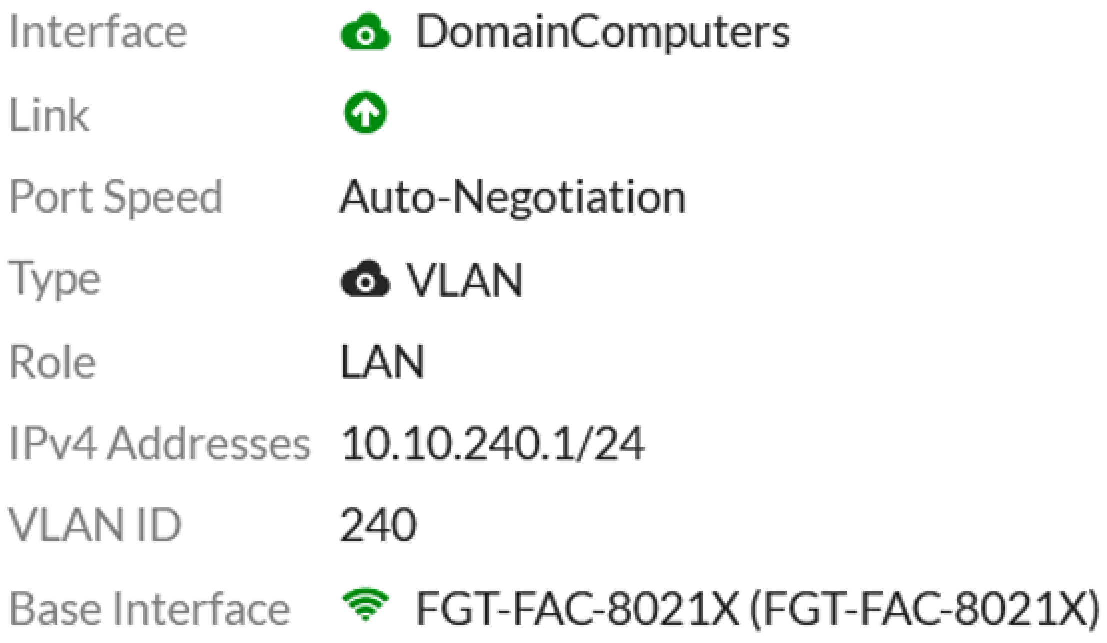
Schedule always

Creating interfaces

You can now create interfaces as required.

To create additional interfaces:

1. Go to *Network* > *Interfaces*, and click *Create New* > *Interface*.
2. Configure your VLAN interface. In this example, the DomainComputers VLAN is created with the following settings:
   a. **Name**: DomainComputers.
   b. **Type**: *VLAN*.
   c. **Interface**: The configured SSID, FGT-FAC-8021X (FGT-FAC-8032X).
   d. **VLAN ID**: 240
   e. **Role**: LAN.



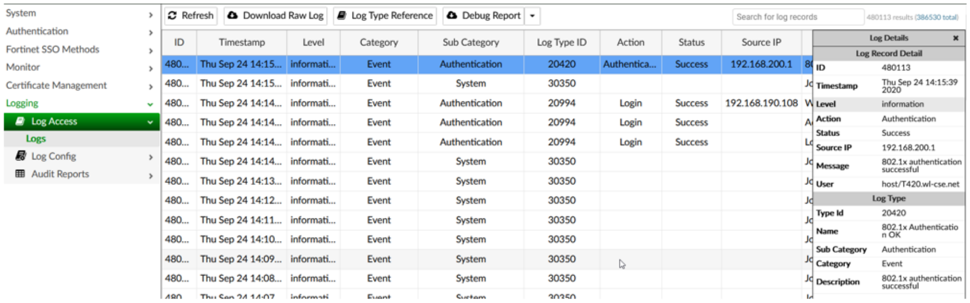
Interface	DomainComputers
Link	⬆
Port Speed	Auto-Negotiation
Type	VLAN
Role	LAN
IPv4 Addresses	10.10.240.1/24
VLAN ID	240
Base Interface	FGT-FAC-8021X (FGT-FAC-8021X)

Results

Once the configuration is complete, you should now be able to authenticate your computer using FortiAuthenticator with a Microsoft AD Root CA.

To confirm computer authentication is working as intended:

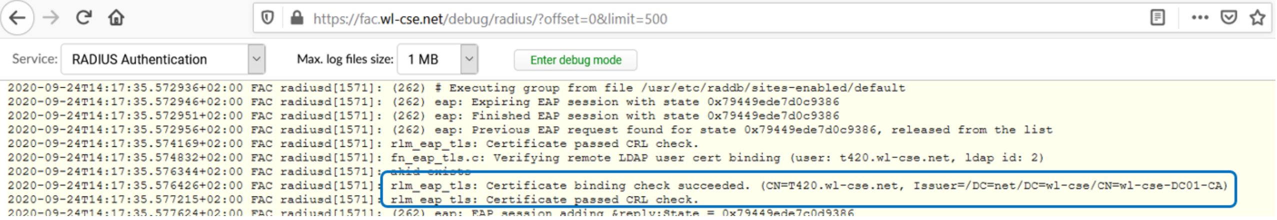
1. When connecting to the client, you can see *Authentication Success* in the FortiAuthenticator logs.



ID	Timestamp	Level	Category	Sub Category	Log Type ID	Action	Status	Source IP
480...	Thu Sep 24 14:15...	informati...	Event	Authentication	20420	Authentica...	Success	192.168.200.1
480...	Thu Sep 24 14:15...	informati...	Event	System	30350			
480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success	192.168.190.108
480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success	
480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success	
480...	Thu Sep 24 14:14...	informati...	Event	System	30350			
480...	Thu Sep 24 14:13...	informati...	Event	System	30350			
480...	Thu Sep 24 14:12...	informati...	Event	System	30350			
480...	Thu Sep 24 14:11...	informati...	Event	System	30350			
480...	Thu Sep 24 14:10...	informati...	Event	System	30350			
480...	Thu Sep 24 14:09...	informati...	Event	System	30350			
480...	Thu Sep 24 14:08...	informati...	Event	System	30350			
480...	Thu Sep 24 14:07	informati	Event	System	30350			

Log Details	
Log Record Detail	
ID	480113
Timestamp	Thu Sep 24 14:15:39 2020
Level	information
Action	Authentication
Status	Success
Source IP	192.168.200.1
Message	802.1x authentication successful
User	host/T420.wl-cse.net
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

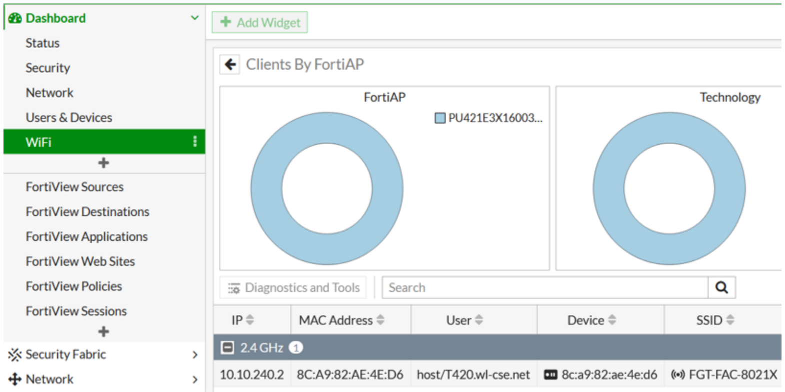
2. When reviewing the debug logs, you can see that certificate binding check has passed.



Service: RADIUS Authentication Max. log files size: 1 MB

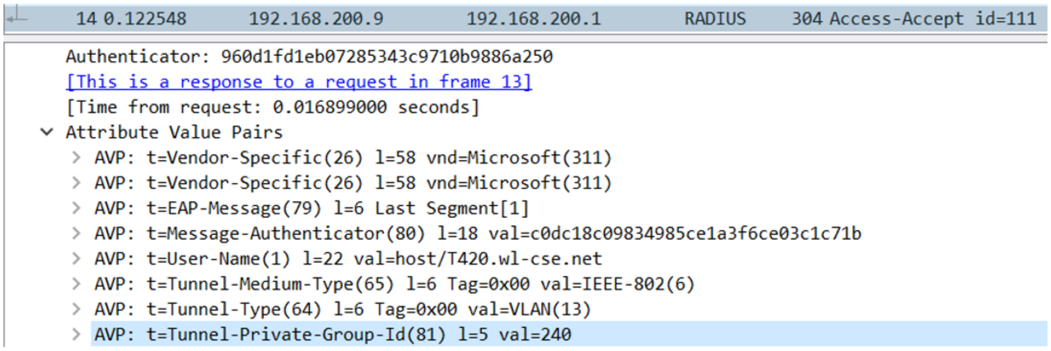
```
2020-09-24T14:17:35.572936+02:00 FAC radiusd[1571]: (262) # Executing group from file /usr/etc/raddb/sites-enabled/default
2020-09-24T14:17:35.572946+02:00 FAC radiusd[1571]: (262) eap: Expiring EAP session with state 0x79449ede7d0c9386
2020-09-24T14:17:35.572951+02:00 FAC radiusd[1571]: (262) eap: Finished EAP session with state 0x79449ede7d0c9386
2020-09-24T14:17:35.572956+02:00 FAC radiusd[1571]: (262) eap: Previous EAP request found for state 0x79449ede7d0c9386, released from the list
2020-09-24T14:17:35.574169+02:00 FAC radiusd[1571]: rlm_eap_tls: Certificate passed CRL check.
2020-09-24T14:17:35.574832+02:00 FAC radiusd[1571]: fn_eap_tls.c: Verifying remote LDAP user cert binding (user: t420.wl-cse.net, ldap id: 2)
2020-09-24T14:17:35.576344+02:00 FAC radiusd[1571]: akid exists
2020-09-24T14:17:35.576426+02:00 FAC radiusd[1571]: rlm_eap_tls: Certificate binding check succeeded. (CN=T420.wl-cse.net, Issuer=/DC=net/DC=wl-cse/CN=wl-cse-DC01-CA)
2020-09-24T14:17:35.577215+02:00 FAC radiusd[1571]: rlm_eap_tls: Certificate passed CRL check.
2020-09-24T14:17:35.577624+02:00 FAC radiusd[1571]: (262) eap: EAP session adding &reply:State = 0x79449ede7c0d9386
```

3. On FortiGate, you can see that the client successfully connected:



IP	MAC Address	User	Device	SSID
2.4 GHz				
10.10.240.2	8C:A9:82:AE:4E:D6	host/T420.wl-cse.net	8c:a9:82:ae:4e:d6	FGT-FAC-8021X

4. Packet capture shows the RADIUS-Accept message, including the VLAN 240.



```
   14 0.122548      192.168.200.9        192.168.200.1        RADIUS    304 Access-Accept id=111

      Authenticator: 960d1fd1eb07285343c9710b9886a250
      [This is a response to a request in frame 13]
      [Time from request: 0.016899000 seconds]
    ⌄ Attribute Value Pairs
      › AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
      › AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
      › AVP: t=EAP-Message(79) l=6 Last Segment[1]
      › AVP: t=Message-Authenticator(80) l=18 val=c0dc18c09834985ce1a3f6ce03c1c71b
      › AVP: t=User-Name(1) l=22 val=host/T420.wl-cse.net
      › AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x00 val=IEEE-802(6)
      › AVP: t=Tunnel-Type(64) l=6 Tag=0x00 val=VLAN(13)
      › AVP: t=Tunnel-Private-Group-Id(81) l=5 val=240
```

WiFi onboarding using FortiAuthenticator Smart Connect

This example demonstrates how to configure WiFi onboarding using FortiAuthenticator Smart Connect with either Google Workspace or Microsoft Azure.

This configuration assumes that you have already configured your FortiAuthenticator following the initial configuration steps available within the FortiAuthenticator Administration Guide. FortiAuthenticator must be version 6.1.1 or higher.

Before starting, you should already have the following available:

- A registered domain name and functional DNS. This example uses fortixpert.com.
- A publicly signed wildcard certificate for your domain (for example *.fortixpert.com used to sign MS Azure DS Secure LDAP Connector).
- A publicly signed host/server certificate for FortiAuthenticator.
- An active Google Workspace Enterprise or MS Azure subscription, depending on your chosen configuration.
  - Please note: Secure LDAP is not supported using Google Workspace Business or Google Workspace Basic subscriptions.
  - An active MS Azure subscription requires AD Directory Services to be provisioned in order to support Secure LDAP.
- Have the appropriate Fortinet infrastructure in place, for example, Fortigate running FOS 6.2.4GA+, FortiSwitch running 6.2.4GA+, FortiAP/FortiAP-U running latest GA and FortiAuthenticator 6.1.1 and above.

To configure WiFi onboarding using Smart Connect:

1. Initial settings on FortiAuthenticator on page 297
2. Select either the Google Workspace or Azure configuration:
   a. Option A - WiFi onboarding with Smart Connect and Google Workspace on page 301
   b. Option B - WiFi onboarding with Smart Connect and Azure on page 311
3. FortiGate configuration on page 319
4. Results on page 330

Initial settings on FortiAuthenticator

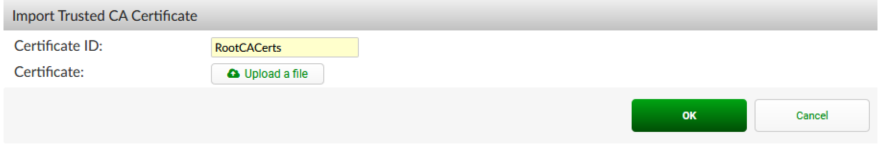
To set up the initial configuration on FortiAuthenticator:

1. Install certificates on page 298
2. Configure the RADIUS client settings on page 299
3. Configure the local root CA on page 300
4. Configure the EAP server certificate and CA for EAP-TLS on page 301

Install certificates

To install a wildcard certificate on FortiAuthenticator:

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CA*.
   Import a trusted root/intermediate public CA certificate in order to support your wildcard certificate.

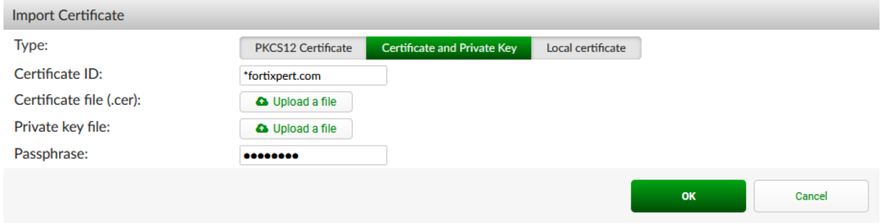


Import Trusted CA Certificate

Certificate ID: RootCACerts

Certificate: Upload a file

2. In *Certificate Management* > *End Entities* > *Local Services*, click *Import*, select *Certificate and Private Key*, and import your domain wildcard certificate as *domainname. For example, `*fortixpert.com`.



Import Certificate

Type: PKCS12 Certificate | Certificate and Private Key | Local certificate

Certificate ID: *fortixpert.com

Certificate file (.cer): Upload a file

Private key file: Upload a file

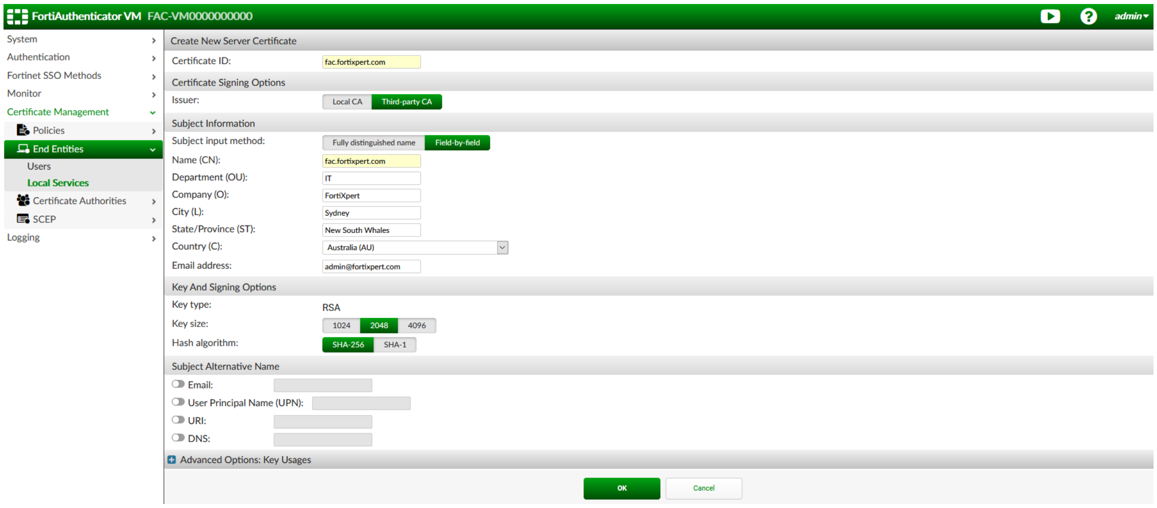
Passphrase: ••••••••

To generate a Certificate Signing Request (optional):

The following steps are optional and can be done if the server certificate matching the FortiAuthenticator FQDN is not yet available.

1. In *Certificate Management* > *End Entities* > *Local Services*, select the *Create New* button.
   Configure the following settings:
   a. Under *Create New Server Certificate*, set the *Certificate ID* to your certificate name, for example, fac.fortixpert.com.
   b. Under *Subject Information*, configure the *Name*, *Department*, *Company*, *City*, *State/Province*, *Country* and *Email Address* for your certificate.
   c. (Optional) If you are using a self-signed certificate on FortiAuthenticator, add a Subject Alternative Name (SAN) matching the FQDN under *Subject Alternative Name*.
   d. (Optional) Under *Advanced Options: Key Usages*, choose all *Key Usages* and *Extended Key Usages*.

e. All other fields can be left in their default state. Click *OK* to save your changes.



Create New Server Certificate

Certificate ID: fac.fortixpert.com

Certificate Signing Options

Issuer: Local CA [✓ Third-party CA]

Subject Information

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

Name (CN): fac.fortixpert.com

Department (OU): IT

Company (O): FortiXpert

City (L): Sydney

State/Province (ST): New South Whales

Country (C): Australia (AU)

Email address: admin@fortixpert.com

Key And Signing Options

Key type: RSA

Key size: 1024 [✓ 2048] 4096

Hash algorithm: [✓ SHA-256] SHA-1

Subject Alternative Name

○ Email:

○ User Principal Name (UPN):

○ URI:

○ DNS:

Advanced Options: Key Usages

2. Export the pending CSR by selecting the pending entry and then clicking *Export Certificate*. Use the downloaded `certificate-name.csr` file to obtain a certificate from a public CA.
3. Import the signed certificate file from the public CA by selecting *Import* and uploading the `certificatename.cer` file.

To install local service certificates:

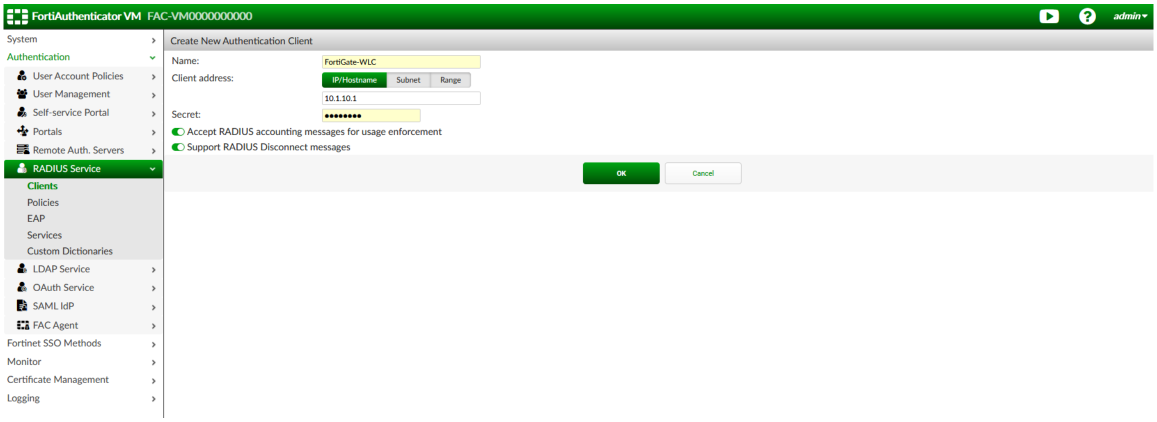
1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CA*.
   Upload the trusted root/intermediate public CA certificates in order to support your host/server certificate.
2. Under *Certificate Management* > *End Entities* > *Local Services*, *Import* your publicly signed host/server certificate matching the FQDN (i.e. fac.fortixpert.com) along with the matching private key.
3. Under *System* > *Administration* > *System Access* > *GUI Access*, configure the following:
   a. For *HTTPS Certificate*, select the server certificate matching the device FQDN from the dropdown box.
   b. For *CA Certificate*, select the Root CA certificate that was used to sign the host/server certificate selected above.
4. Select *OK*.

Configure the RADIUS client settings

To configure the RADIUS client:

1. Add the FortiAuthenticator host record to your local DNS server.
   If you are using FortiGate as the DNS server, this can be set under *Network* > *DNS Servers* on FortiGate.
2. Under *System* > *Dashboard* > *Status*, edit and set the hostname and FQDN for FortiAuthenticator so that it matches the DNS host record.
3. In *Authentication* > *RADIUS Service* > *Clients*, add the wireless controller, in this example FortiGate, as a new RADIUS client.
   Enter the *Name* and *IP/Hostname* of the wireless controller, and create a *Secret*.

4. Click *OK*.



Create New Authentication Client

Name: FortiGate-WLC

Client address: IP/Hostname | Subnet | Range

10.1.10.1

Secret: ••••••••

Accept RADIUS accounting messages for usage enforcement

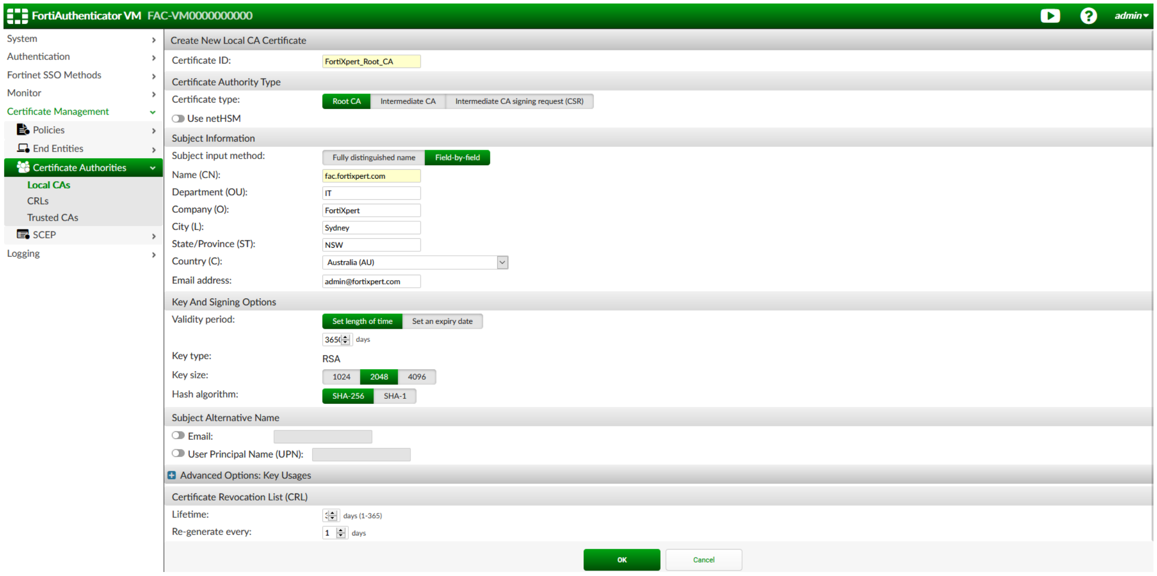
Support RADIUS Disconnect messages

Configure the local root CA

You can now configure a local CA on FortiAuthenticator. This will be used to generate client certificates for authentication via EAP-TLS.

To configure the Local Root CA:

1. In *Certificate Management > Certificate Authorities > Local CAs*, select *Create New*.
2. Configure the following settings:
   - **a.** Set the *Certificate ID* to the Local_Root_CA_Name.
   - **b.** In *Certificate Authority Type*, set the *Certificate Type* to *Root CA*.
   - **c.** In *Subject Information*, configure the *Name*, *Department*, *Company*, *City*, *State/Province*, *Country*, and *Email address* for your certificate.
   - **d.** In *Advanced Options > Key Usages*, choose *all* Key Usages and Extended Key Usages.
3. Leave all other settings as their default, and click *OK*.



Create New Local CA Certificate

Certificate ID: FortiXpert_Root_CA

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): fac.fortixpert.com

Department (OU): IT

Company (O): FortiXpert

City (L): Sydney

State/Province (ST): NSW

Country (C): Australia (AU)

Email address: admin@fortixpert.com

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)

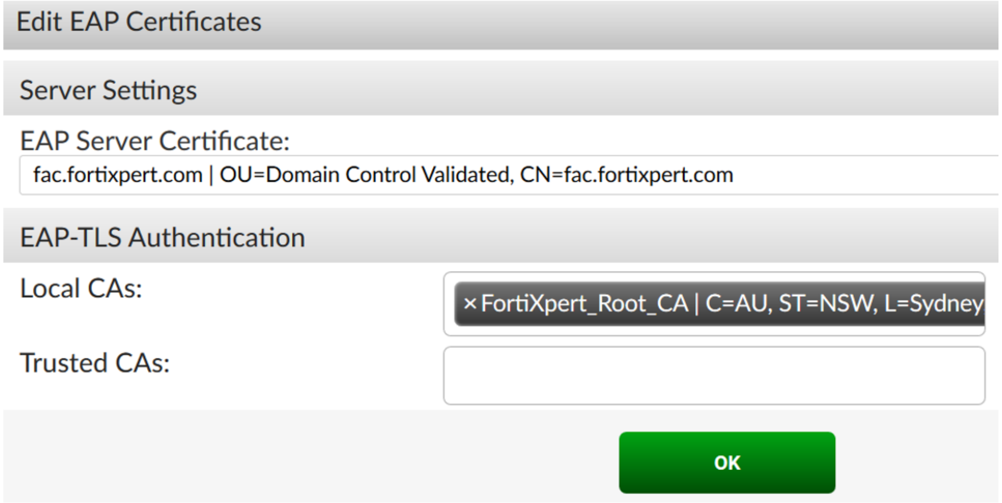
Lifetime: days (1-365)

Re-generate every: 1 days

Configure the EAP server certificate and CA for EAP-TLS

To set an EAP Server Certificate and CA for EAP-TLS:

1. Go to *Authentication* > *RADIUS Service* > *Certificates*.
2. In *Server Settings* > *EAP Server Certificate*, select the publicly signed certificate matching the FortiAuthenticator FQDN (e.g. fac.fortixpert.com).
3. In *EAP-TLS Authentication* > *Local CAs*, select the local CA (e.g. FortiXpert_Root_CA).



Edit EAP Certificates

Server Settings

EAP Server Certificate: fac.fortixpert.com | OU=Domain Control Validated, CN=fac.fortixpert.com

EAP-TLS Authentication

Local CAs: ×FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney

Trusted CAs:

4. Click *OK*.

Option A - WiFi onboarding with Smart Connect and Google Workspace

This section outlines how to configure the FortiAuthenticator to communicate with Google Workspace via Secure Lightweight Directory Access Protocol.

To configure WiFi Onboarding with Google Workspace:

1. Configure Google Workspace LDAPS Integration on page 301
2. Configure Smart Connect and the captive portal on page 307
3. Configure RADIUS settings on FortiAuthenticator on page 310

Configure Google Workspace LDAPS Integration

Here you will configure FortiAuthenticator to communicate with Google Workspace via Secure Lightweight Directory Access Protocol.

To configure FortiAuthenticator and Google Workspace LDAPS integration:

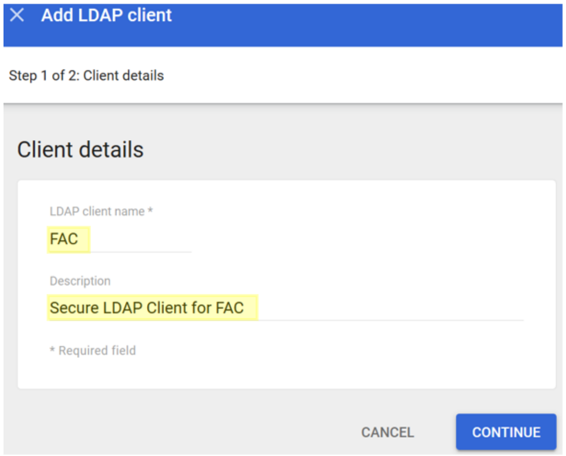
1. Provision the LDAP connector in Google Workspace on page 302
2. Configure certificates on FortiAuthenticator on page 304
3. Configure the remote LDAP server and users on page 305

Provision the LDAP connector in Google Workspace

To provision the LDAP connector in Google Workspace:

Configure FortiAuthenticator to communicate with Google Workspace via Secure Lightweight Directory Access Protocol (LDAPS).

1. Login to the Google Workspace admin console using a Google Workspace admin account.
2. Click the Apps icon, then select *LDAP* and *Add Client*.
3. In *Add LDAP Client Step 1*, configure the following settings:
   a. **Name**:Enter a name, for example *FAC*.
   b. **Description**: Enter a description, for example *Secure LDAP Client for FAC*.



Add LDAP client

Step 1 of 2: Client details

Client details

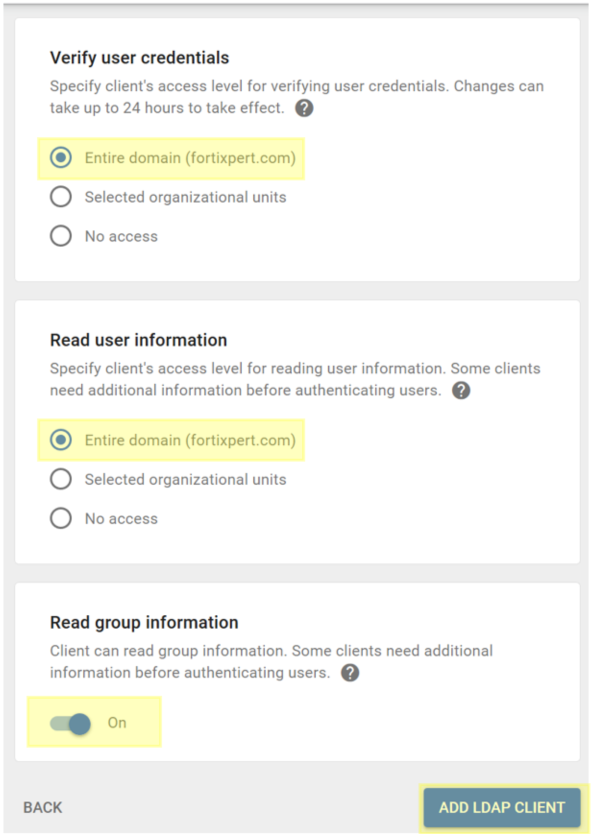
LDAP client name *: FAC

Description: Secure LDAP Client for FAC

* Required field

4. Under Add LDAP Client Step 2, configure the following settings:
   a. **Verify User Credentials**: *Entire domain*.
   b. **Read user information**: *Entire domain*.
   c. **Read Group Information**: *On*.

5. Click *Add LDAP Client*.



Verify user credentials

Specify client's access level for verifying user credentials. Changes can take up to 24 hours to take effect.

- ● Entire domain (fortixpert.com)
- ○ Selected organizational units
- ○ No access

Read user information

Specify client's access level for reading user information. Some clients need additional information before authenticating users.

- ● Entire domain (fortixpert.com)
- ○ Selected organizational units
- ○ No access

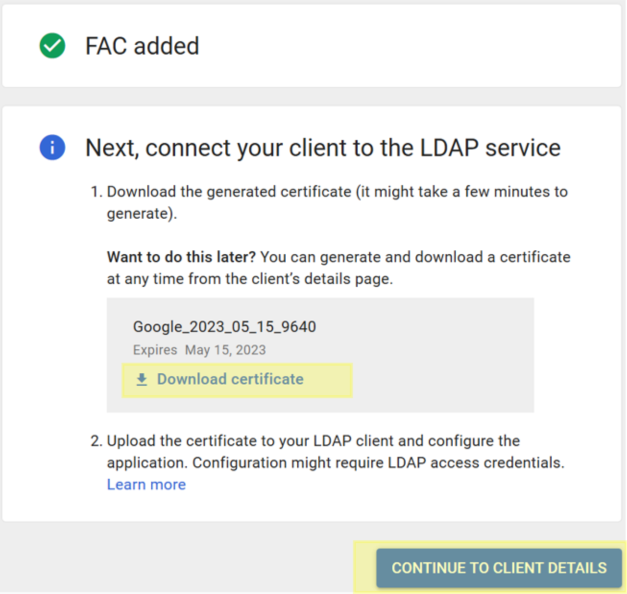
Read group information

Client can read group information. Some clients need additional information before authenticating users.

On

You will now be prompted to connect your client to the LDAP service.

6. Click *Download Certificate* and save the ZIP file.



FAC added

Next, connect your client to the LDAP service

1. Download the generated certificate (it might take a few minutes to generate).

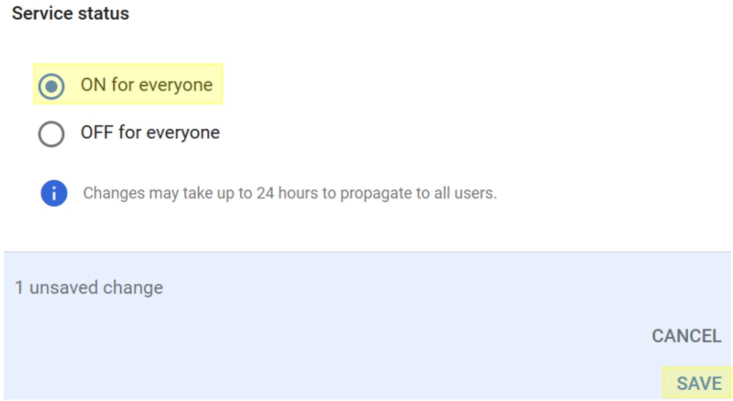
   Want to do this later? You can generate and download a certificate at any time from the client's details page.

   Google_2023_05_15_9640
   Expires May 15, 2023

2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more

Unzip the certificate file to a local folder. Contained within will be a public certificate along with a private key.

7. Select *Continue to Client Details*. Select Service status and change the status to *On*.



Service status

● ON for everyone

○ OFF for everyone

Changes may take up to 24 hours to propagate to all users.

1 unsaved change

8. Click *Save*.

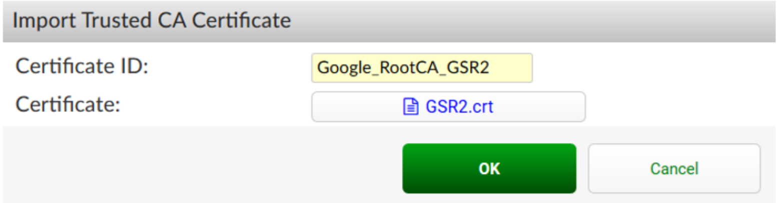
Configure certificates on FortiAuthenticator

To download Google Root CA Certificate:

1. Open a new Internet browser and navigate to https://pki.goog.
2. Under *Root CAs* in the *Repository* tab, download the *GS Root R2* certificate in the DER format. The file will be called *GSR2.crt*.

To import the Google Certificates into FortiAuthenticator:

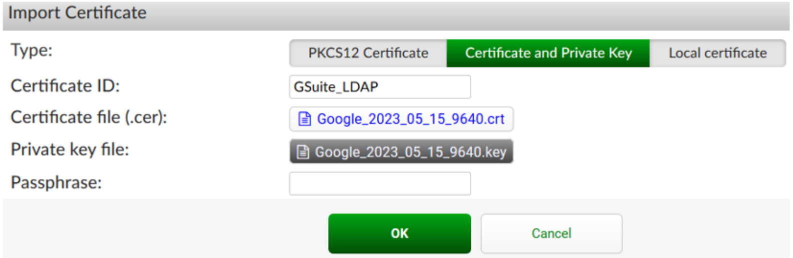
1. In FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs*, and click *Import*.
2. Enter a *Certificate ID* and then upload the Google Root CA certificate previously downloaded.



Import Trusted CA Certificate

Certificate ID:	Google_RootCA_GSR2
Certificate:	GSR2.crt

3. Go to *Certificate Management* > *End Entities* > *Local Services*, and click *Import*.
4. Under *Import Certificate* , select *Certificate and Private Key* as the *Type*.
Enter a *Certificate ID*, and select the *Certificate file* and *Private key file* from the file you unzipped previously. A *Passphrase* is not required. Click *OK*.



Import Certificate

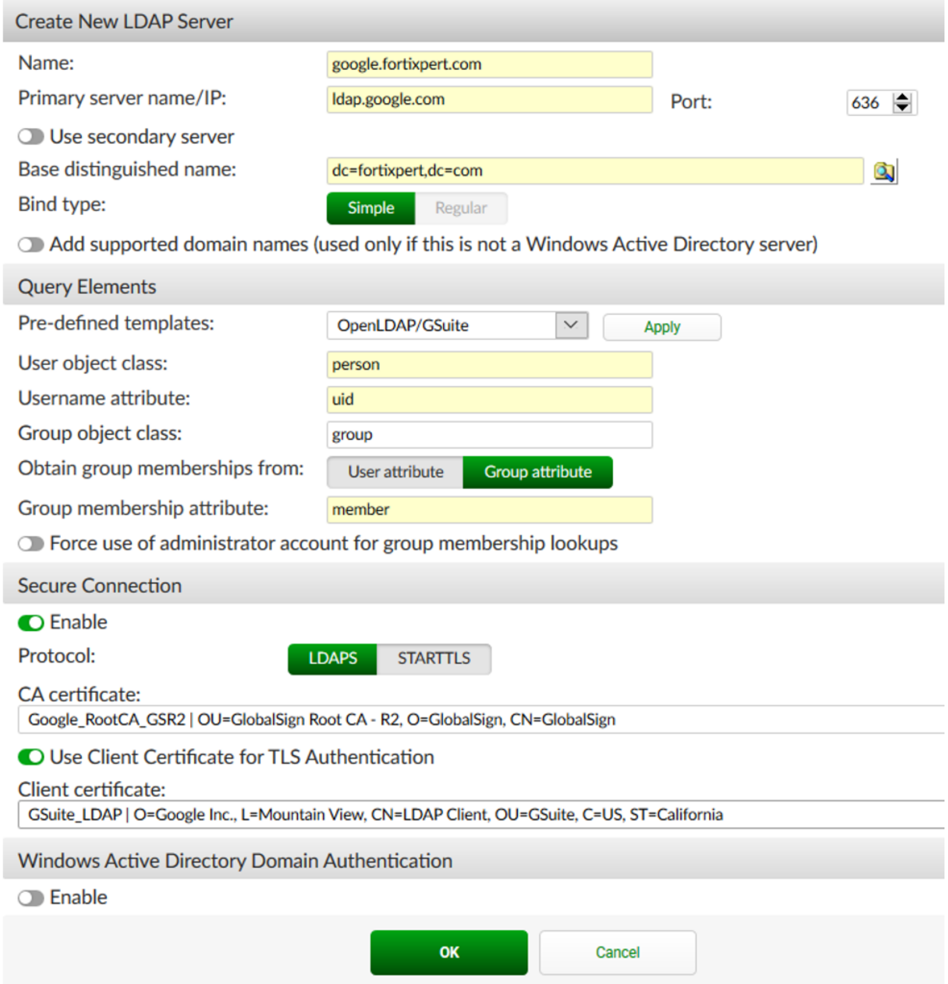
Type:	PKCS12 Certificate / **Certificate and Private Key** / Local certificate
Certificate ID:	GSuite_LDAP
Certificate file (.cer):	Google_2023_05_15_9640.crt
Private key file:	Google_2023_05_15_9640.key
Passphrase:	

Configure the remote LDAP server and users

To provision the remote LDAP server:

1. In FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and click *Create New*.
2. Under *Create New LDAP Server*, set the following:
   a. **Name**: Enter a name for the remote LDAP server, for example *google.fortixpert.com*.
   b. **Primary server name/IP**: *ldap.google.com*.
   c. **Base distinguished name**: Enter the base LDAP search directory, for example the Google Workspace domain: *dc=fortixpert,dc=com*.
   d. **Bind type**: *Simple*.
3. Under *Query Elements*, set the following:
   a. **Pre-defined templates**: Select *OpenLDAP/G Suite* from the dropdown box, and click *Apply*.
4. Under *Secure Connection*, enable the secure connection function, and set the following:
   a. **Protocol**: *LDAPS*.
   b. **CA Certificate**: Select the *Google_RootCA_GSR2* certificate from the dropdown box.
   c. **Use Client Certificate for TLS Authentication**: *Enabled*.
   d. **Client certificate**: Select the *G Suite_LDAP* client certificate from the dropdown box.
5. At the top of the page under Base distinguished name, select the directory lookup icon.
   Once the LDAPS connection is established you'll see the Directory of Groups and Users within Google Workspace.

Select *OK*.



Create New LDAP Server

Name: google.fortixpert.com

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

○ Use secondary server

Base distinguished name: dc=fortixpert,dc=com

Bind type: Simple | Regular

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

Query Elements

Pre-defined templates: OpenLDAP/GSuite Apply

User object class: person

Username attribute: uid

Group object class: group

Obtain group memberships from: User attribute | Group attribute

Group membership attribute: member

○ Force use of administrator account for group membership lookups

Secure Connection

● Enable

Protocol: LDAPS | STARTTLS

CA certificate:
Google_RootCA_GSR2 | 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

OK Cancel

6. Select *OK* again to save the LDAP server settings.

To import remote user accounts:

1. Go to *Authentication* > *User Management* > *Remote Users*, and confirm that *LDAP* is selected at the top right of the page.
2. Click *Import*.
3. Under *Import Remote LDAP Users*, set the following:
   a. **Remote** LDAP server: Select your connector bound to ldap.google.com from the dropdown box.
   b. **Action**: *Import Users*.
4. Click *Go*. A list of all the users within your Google Workspace directory will be displayed.
5. Select the users you want to be able to connect to the wireless network using their Google Workspace account, and select *OK* to import the relevant user accounts.
6. Under *Synchronization Attributes*, set the following:
   a. **Token-based authentication sync priorities**: *None*.
   b. **Sync every**: Select the sync frequency. In production environments, this should be set to 30 minutes or more depending on the number of users being synchronized.
   c. **Sync as**: *Remote LDAP User*.
   d. **User role for new user imports**: *User*.

7. Leave all other settings in their default state, and click *OK*.

To create a new realm:

1. Go to *Authentication* > *User Management* > *Realms*, and click *Create New*.
2. Configure the following settings:
   a. **Name**: Enter a name for your realm, for example fortixpert.com.
   b. **User source**: Select the remote LDAP service from the dropdown box.
3. Click *OK*.

Configure Smart Connect and the captive portal

This section outlines the configuration required on FortiAuthenticator to provision a captive portal using Smart Connect authenticating against Google Workspace.

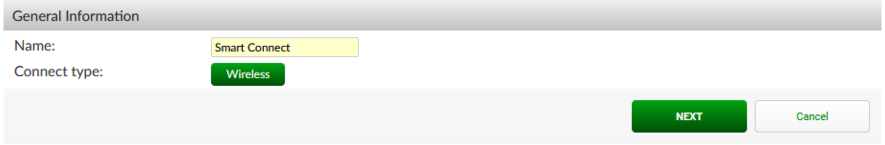
To configure Smart Connect and portals on FortiAuthenticator:

1. Create the Smart Connect profile on page 307
2. Create the captive portal on page 308
3. Create the self-service portal policy on page 309

Create the Smart Connect profile

To create Smart Connect profiles:

1. Go to *Authentication* > *Portals* > *Smart Connect Profiles*, and click *Create New*.
2. Under *General Information*, enter a name for the profile, and click *Next*.

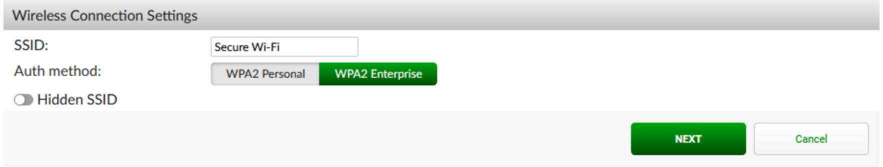


General Information

Name: Smart Connect

Connect type: Wireless

3. Under *Wireless Connection Settings*, set the following and then click *Next*.
   a. **SSID**: Enter your SSID name, for example Secure Wi-Fi.
   b. **Auth method**: *WPA2 Enterprise*.
   c. **Hidden SSID**: *Disabled*.



Wireless Connection Settings

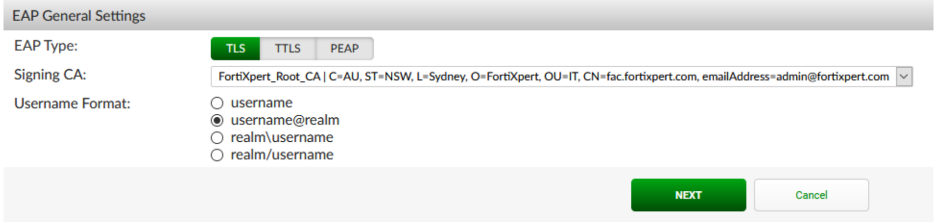
SSID: Secure Wi-Fi

Auth method: WPA2 Personal | WPA2 Enterprise

Hidden SSID

4. Under *EAP General Settings*, set the following and then click *Next*.
   a. **EAP Type**: *TLS*.
   b. **Signing CA**: Select the local Root CA configured earlier.

c. **Username Format**: Select your preference, for example *username@realm*.



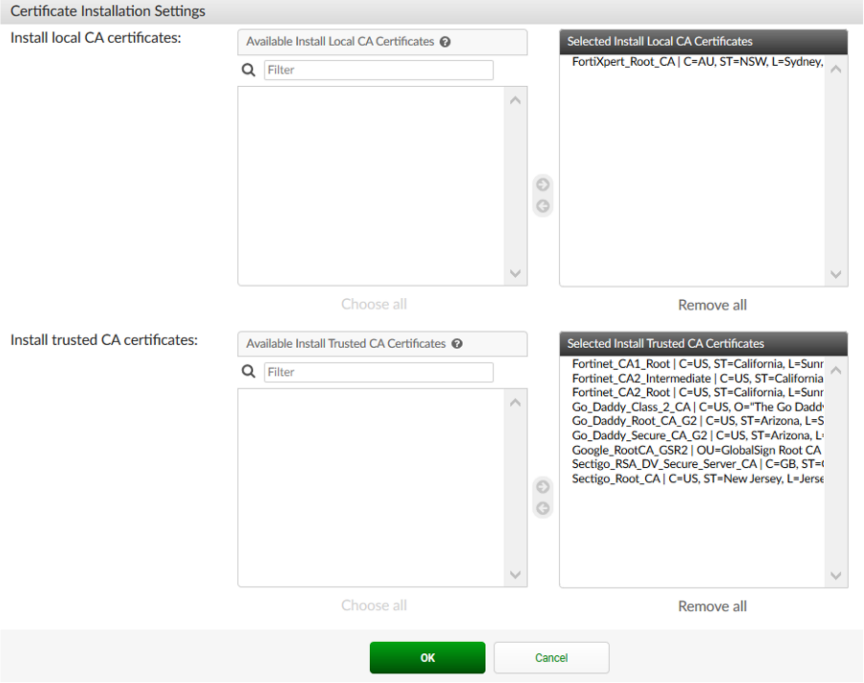
EAP General Settings

EAP Type: TLS | TTLS | PEAP

Signing CA: FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney, O=FortiXpert, OU=IT, CN=fac.fortixpert.com, emailAddress=admin@fortixpert.com

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

5. Under *Certificate Installation Settings*, set the following and then click *OK*.
   a. **Install local CA certificates**: Choose to install the local Root_CA certificate.
   b. **Install trusted CA certificates**: Choose to install any certificate that is required for all relevant certificate chains to be fully trusted.



Certificate Installation Settings

Install local CA certificates:

Available Install Local CA Certificates

Selected Install Local CA Certificates
FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney,

Install trusted CA certificates:

Available Install Trusted CA Certificates

Selected Install Trusted CA Certificates
Fortinet_CA1_Root | C=US, ST=California, L=Sunr
Fortinet_CA2_Intermediate | C=US, ST=California
Fortinet_CA2_Root | C=US, ST=California, L=Sunr
Go_Daddy_Class_2_CA | C=US, O="The Go Dadd
Go_Daddy_Root_CA_G2 | C=US, ST=Arizona, L=S
Go_Daddy_Secure_CA_G2 | C=US, ST=Arizona, L
Google_RootCA_GSR2 | OU=GlobalSign Root CA
Sectigo_RSA_DV_Secure_Server_CA | C=GB, ST=
Sectigo_Root_CA | C=US, ST=New Jersey, L=Jerse

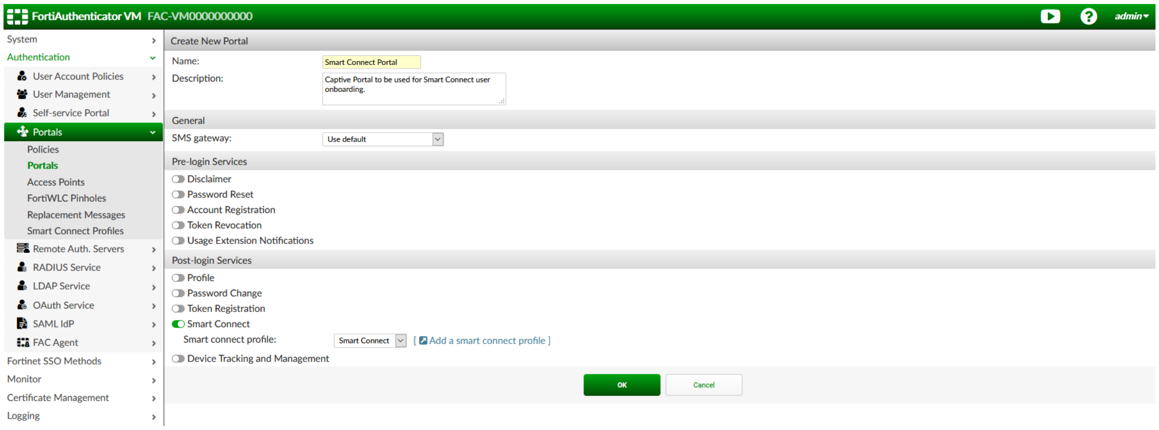
6. Select *OK* to complete the setup of the Smart Connect profile.

Create the captive portal

To create a captive portal:

1. Go to *Authentication* > *Portals* > *Portals*, and click *Create New*.
2. Under *Create New Portal*, enter a name and optional description for the portal.
3. Under *Post-login services*, enable *Smart Connect* and select the previously configured Smart Connect profile from the dropdown.

4. Select *OK*.



Create New Portal

Name: Smart Connect Portal

Description: Captive Portal to be used for Smart Connect user onboarding.

General

SMS gateway: Use default

Pre-login Services

- ○ Disclaimer
- ○ Password Reset
- ○ Account Registration
- ○ Token Revocation
- ○ Usage Extension Notifications

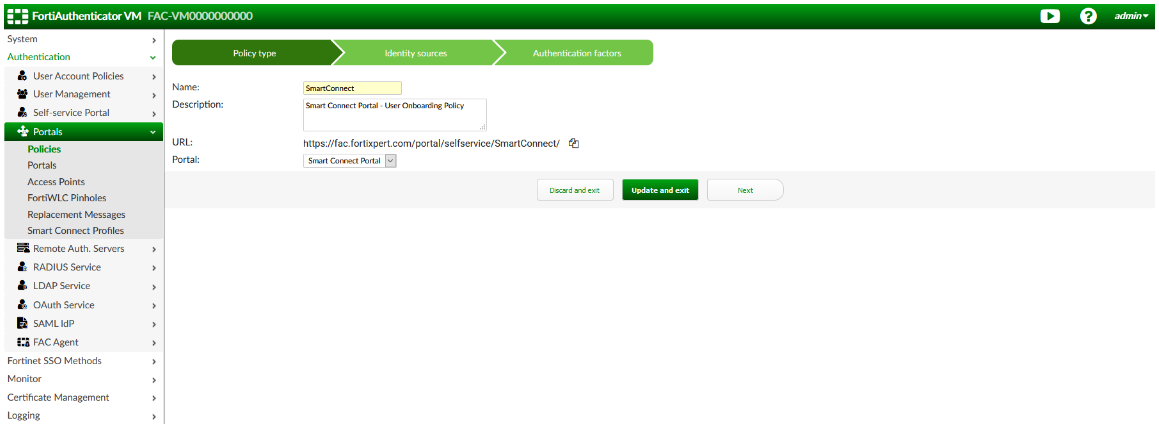
Post-login Services

- ○ Profile
- ○ Password Change
- ○ Token Registration
- ● Smart Connect
  - Smart connect profile: Smart Connect [Add a smart connect profile]
- ○ Device Tracking and Management

Create the self-service portal policy

To create a self-service portal policy:

1. Go to *Authentication* > *Portals* > *Policies*. Select the *Self-Service Portal* option, and click *Create New*.
2. Under *Policy Type*, set the following and then click *Next*.
   a. **Name**: Enter a policy name, for example *SmartConnect*.
   b. **Description**: Enter an optional description for the policy.
   c. **URL**: Note this URL. This is the external captive portal redirection URL which must be added to the Onboarding SSID configured on the FortiGate/WLC later.
   d. **Portal**: Select the previously configured Smart Connect portal.



Name: SmartConnect

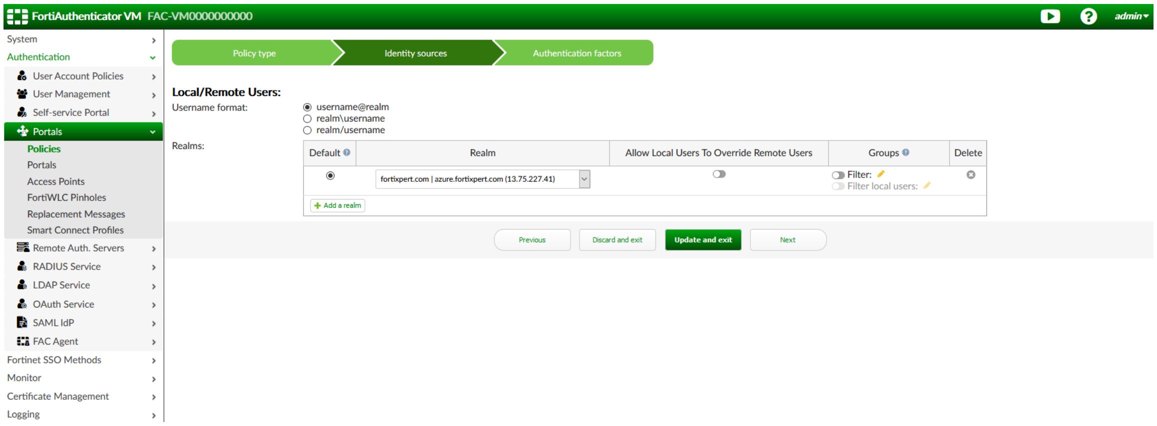
Description: Smart Connect Portal - User Onboarding Policy

URL: https://fac.fortixpert.com/portal/selfservice/SmartConnect/

Portal: Smart Connect Portal

3. Under *Identity sources*, set the following and then click *Next*:
   a. **Username format**: username@realm.

b. **Realms**: In the dropdown box, select the LDAP realm associated with ldap.google.com, for example fortixpert.com.



Local/Remote Users:

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

Realms:

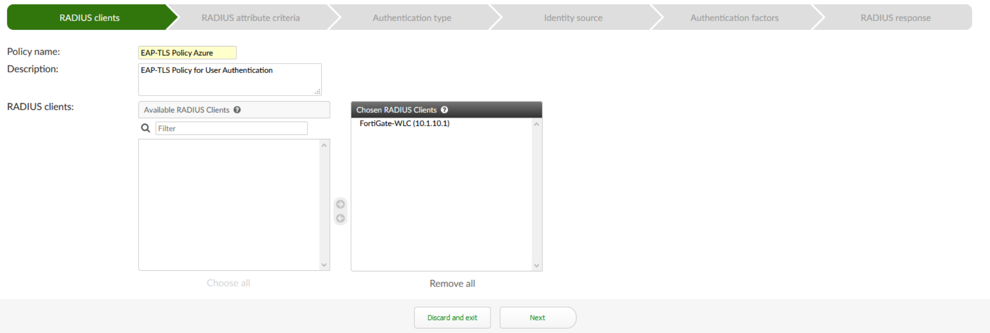
Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	fortixpert.com | azure.fortixpert.com (13.75.227.41)	○	Filter: Filter local users:	⊗

4. Under *Authentication factors*, leave the default options in place, and click *Save and exit*.

Configure RADIUS settings on FortiAuthenticator

To create a RADIUS service policy:

1. Go to *Authentication > RADIUS Service > Policies*, and click *Create New*.
2. Under *RADIUS clients*, set the following and then click *Next*:
   a. **Policy Name**: Enter a name for the policy, for example EAP-TLS Policy Google Workspace.
   b. **Description**: Enter an optional description, for example EAP-TLS Policy for User Authentication.
   c. **RADIUS Clients**: Add the FortiGate to the *Chosen RADIUS Clients* section.

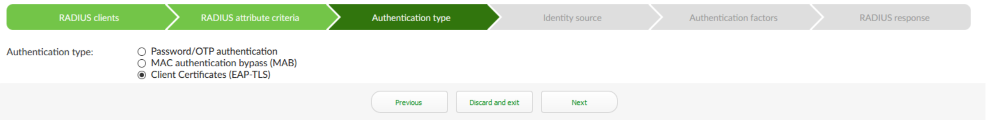


Policy name: EAP-TLS Policy Azure

Description: EAP-TLS Policy for User Authentication

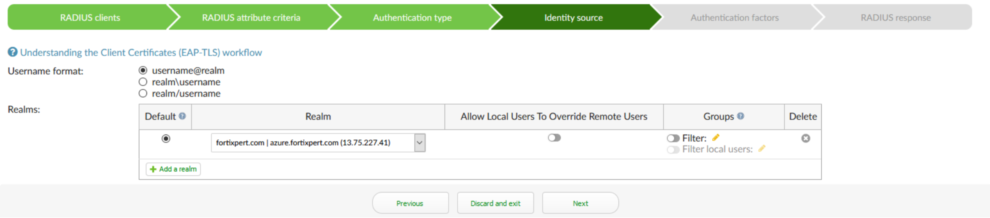
RADIUS clients: Chosen RADIUS Clients: FortiGate-WLC (10.1.10.1)

3. Under *RADIUS attribute criteria*, click *Next* without making changes.
4. Under *Authentication type*, select *Client Certificates (EAP-TLS)*, and click *Next*.



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

5. Under *Identity source*, set the following and then click *Next*:
   a. **Username format**: Select your preferred format, for example username@realm.
   b. **Realms**: Select the realm that you set up to communicate with ldap.google.com, for example fortixpert.com.



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

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	fortixpert.com | azure.fortixpert.com (13.75.227.41)	○	Filter: Filter local users:	⊗

+ Add a realm

6. Under *Authentication factors*, click *Next* without making changes.
7. Under *RADIUS response*, validate that the EAP-TLS response is as expected, and click *Save and exit*.

Option B - WiFi onboarding with Smart Connect and Azure

This section outlines how to configure the FortiAuthenticator to communicate with Microsoft Azure AD Directory Services via Secure Lightweight Directory Access Protocol

To configure WiFi Onboarding with Azure:

1. Configure Azure AD DS LDAPS integration on page 311
2. Configure Smart Connect and the captive portal on page 316
3. Configure RADIUS settings on FortiAuthenticator on page 319

Configure Azure AD DS LDAPS integration

This guide does not include information on how to provision Azure AD DS. Please refer to Microsoft's support site for instructions on how to do this.

To configure Azure AD DS LDAPS integration:

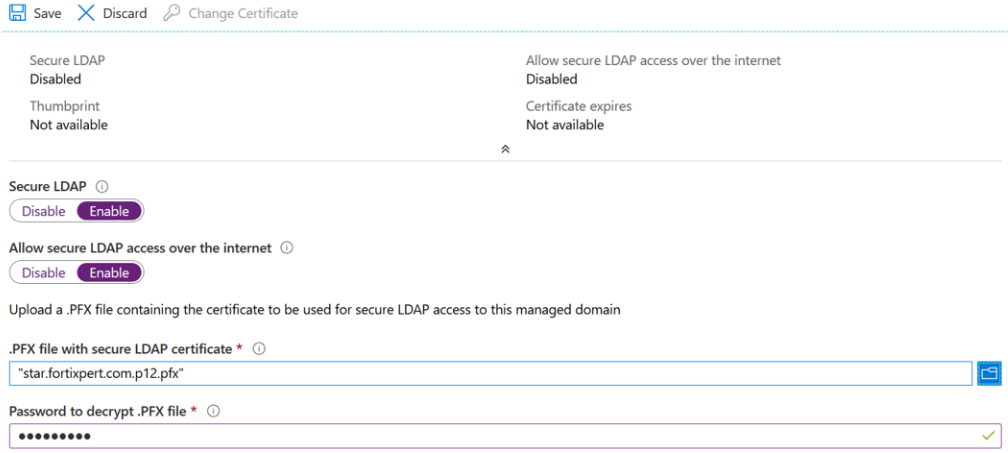
1. Provision the LDAPS connector in Azure AD DS on page 311
2. Provision the remote LDAP server on FortiAuthenticator on page 313

Provision the LDAPS connector in Azure AD DS

To provision the LDAP connector in Azure AD DS:

1. Login to the Azure admin portal using an Azure admin account.
2. Select *Active Directory Domain Services*.
3. Select *View*.
4. Select your AD DS instance, for example fortixpert.com.
5. Within the AD DS menu for your domain, select *Secure LDAP* under *Settings*.

6. In the Secure LDAP window, perform the following:
   a. Set *Secure LDAP* to *Enable*.
   b. Set *Allow secure LDAP access over the internet* to *Enable*.
   c. Upload your domain wildcard certificate, for example *.fortixpert.com, in .PFX format.
   d. Enter the password to decrypt the PFX file.



Secure LDAP
Disabled

Allow secure LDAP access over the internet
Disabled

Thumbprint
Not available

Certificate expires
Not available

Secure LDAP: Disable [✓ Enable]

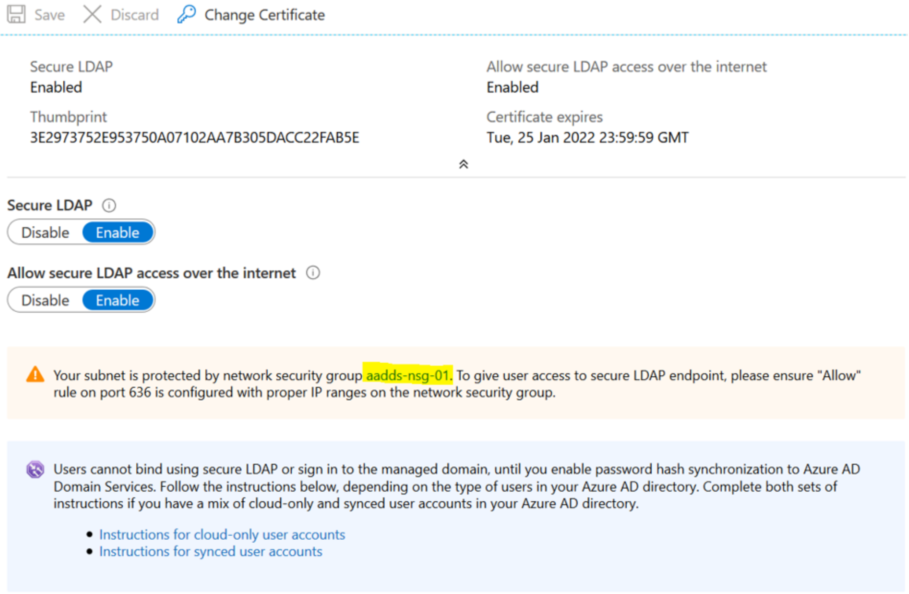
Allow secure LDAP access over the internet: Disable [✓ Enable]

Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain

.PFX file with secure LDAP certificate *
"star.fortixpert.com.p12.pfx"

Password to decrypt .PFX file *
●●●●●●●●● ✓

7. Select the *Save* button at the top of the page, and wait for Azure to configure Secure LDAP.
   This process takes approximately five minutes.
8. Once provisioning is complete, you must now allow inbound access for the secure LDAP protocol (port 636 to your AD DS instance.
9. Browse to the network security group linked in your Secure LDAP connector.
10. Select the network secure group link to access the network security group settings.
   You can follow the steps found on Microsoft's support website to enable user accounts for Azure AD DS. This is required for users to authenticate through Secure LDAP.



Secure LDAP
Enabled

Allow secure LDAP access over the internet
Enabled

Thumbprint
3E2973752E953750A07102AA7B305DACC22FAB5E

Certificate expires
Tue, 25 Jan 2022 23:59:59 GMT

Secure LDAP: Disable [✓ Enable]

Allow secure LDAP access over the internet: Disable [✓ Enable]

⚠ Your subnet is protected by network security group aadds-nsg-01. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.

Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory.

- Instructions for cloud-only user accounts
- Instructions for synced user accounts

To create an Azure inbound firewall policy:

1. Within the network security group, go to *Settings* > *Inbound Security Rules*, and click *Add*.
2. In *Add inbound security rule*, set the following:
   a. **Source**: IP Address.
   b. **Source IP address/CIDR ranges**: Set as the IP address/range that the inbound request will be originating from.
   c. **Destination port ranges**: 636.
   d. **Name**: Enter the name, for example AllowSecureLDAP.
   e. **Description**: Add an optional description.
3. Leave all other settings as their default values, and click *Add*.

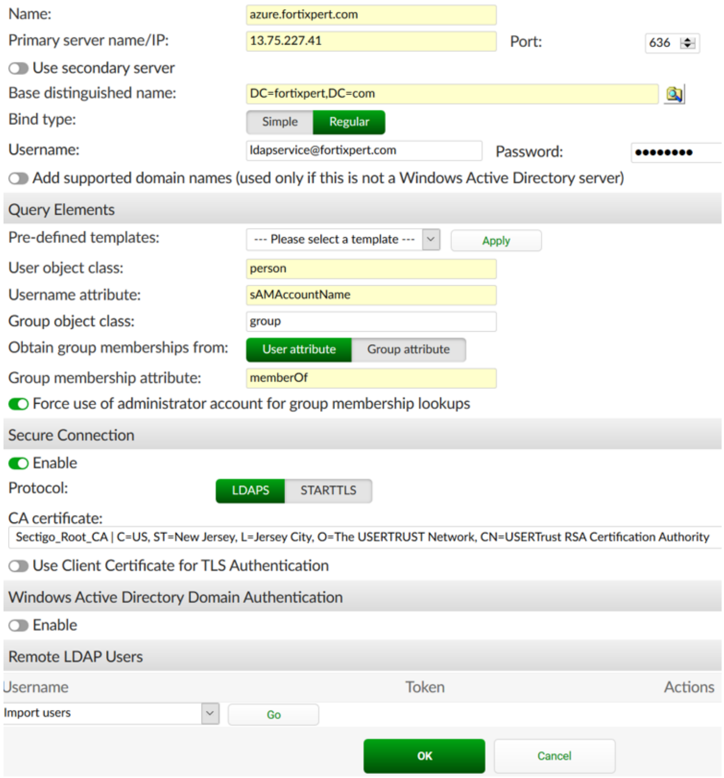
To obtain the LDAPS IP address:

1. Go to Azure AD Directory Services, and select the Azure domain.
2. Go to *Settings* > *Properties*. Note down the Secure LDAP external IP address.

Provision the remote LDAP server on FortiAuthenticator

To provision the remote LDAP server:

1. In FortiAuthenticator, go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and click *Create New*.
2. In the *Create New LDAP Server* window, set the following:
   a. **Name**: Enter a name, for example azure.fortixpert.com.
   b. **Primary server name/IP**: Enter the Secure LDAP IP.
   c. **Bind type**: *Regular*.
   d. **Username/Password**: Enter a username and password that can access MS Azure DS to perform directory lookups.
   e. **Base distinguished name**: Leave blank.
3. In the *Query Elements* section, set the following:
   a. **Pre-defined templates**: Select *Microsoft Active Directory* and click *Apply*.
   b. **Force use of administrator account for group membership lookups**: Enabled.
4. In the *Secure Connection* section, set the following
   a. **Secure Connection**: Enabled.
   b. **Protocol**: *LDAPS*.
   c. **CA Certificate**: Select the Root CA certificate for the wildcard certificate that was uploaded to MS Azure to use with the Secure LDAP connector.
5. Select the lookup icon next to *Base distinguished name*. Choose the base DN for your user accounts, for example DC=fortixpert,DC=com. Click *OK*.



Name: azure.fortixpert.com
Primary server name/IP: 13.75.227.41 Port: 636
○ Use secondary server
Base distinguished name: DC=fortixpert,DC=com
Bind type: Simple [✓ Regular]
Username: ldapservice@fortixpert.com Password: ••••••••
○ 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: sAMAccountName
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:
Sectigo_Root_CA | C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
○ Use Client Certificate for TLS Authentication

Windows Active Directory Domain Authentication

○ Enable

Remote LDAP Users

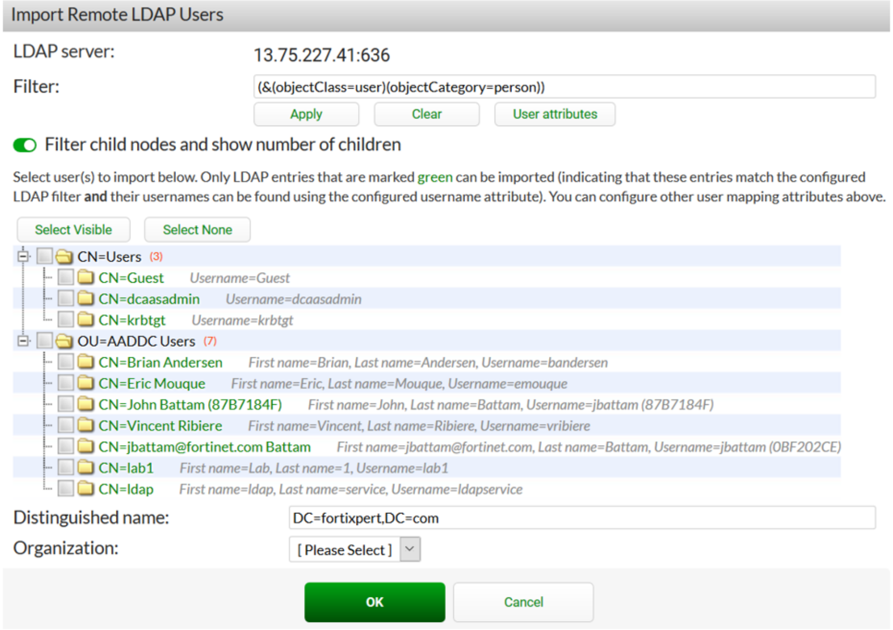
Username	Token	Actions
Import users		

6. Click *OK* to save the remote LDAP server configuration.

To import remote user accounts:

1. Go to *Authentication* > *User Management* > *Remote Users*. Confirm *LDAP* is selected at the top of the page, and click *Import*.
2. Under *Import Remote LDAP User*, complete the following:
   a. **Remote LDAP Server**: Select the Azure remote LDAP server.
   b. **Action**: Select *Import users*, and click *Go* to view a list of users within your Azure directory.

c. Select the users you wish to be able to connect to the wireless network using their Azure based account.



Import Remote LDAP Users

LDAP server: 13.75.227.41:636

Filter: (&(objectClass=user)(objectCategory=person))

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.

- □ CN=Users (3)
  - □ CN=Guest *Username=Guest*
  - □ CN=dcaasadmin *Username=dcaasadmin*
  - □ CN=krbtgt *Username=krbtgt*
- □ OU=AADDC Users (7)
  - □ CN=Brian Andersen *First name=Brian, Last name=Andersen, Username=bandersen*
  - □ CN=Eric Mouque *First name=Eric, Last name=Mouque, Username=emouque*
  - □ CN=John Battam (87B7184F) *First name=John, Last name=Battam, Username=jbattam (87B7184F)*
  - □ CN=Vincent Ribiere *First name=Vincent, Last name=Ribiere, Username=vribiere*
  - □ CN=jbattam@fortinet.com Battam *First name=jbattam@fortinet.com, Last name=Battam, Username=jbattam (0BF202CE)*
  - □ CN=lab1 *First name=Lab, Last name=1, Username=lab1*
  - □ CN=ldap *First name=ldap, Last name=service, Username=ldapservice*

Distinguished name: DC=fortixpert,DC=com

Organization: [Please Select]

3. Click *OK*.

To set up a remote user sync rule:

1. Go to *Authentication* > *User Management* > *Remote User Sync Rule*, and click *Create New*.
2. Under *Create New Remote LDAP User Synchronization Rule*, set the following:
   a. **Name**: Enter a name, for example Azure_Remote_Sync.
   b. **Remote LDAP**: Select your Azure remote LDAP server.
   c. **Base distinguished name**: This setting can be left as the default, for example DC=fortixpert,DC=com.
3. Under *Synchronization Attributes*, set the following:
   a. **Token-based authentication sync priorities**: Enable *None*.
   b. **Sync every**: Select the sync frequency. In production environments, this should be set to 30 minutes or more depending on the number of users being synchronized.
   c. **Sync as**: *Remote LDAP User*.
   d. **User role for new user imports**: *User*.
4. Leave all other settings in their default states, and click *OK*.

To create a new realm:

1. Go to *Authentication* > *User Management* > *Realms*, and click *Create New*.
2. Under *Create New Realm*, set the following:
   a. **Name**: Enter the realm name, for example fortixpert.com.
   b. **User source**: Select the remote LDAP service from the dropdown box.
3. Click *OK*.

Configure Smart Connect and the captive portal

This section outlines the configuration required on FortiAuthenticator to provision a Captive Portal using Smart Connect authenticating against MS Azure AD DS.

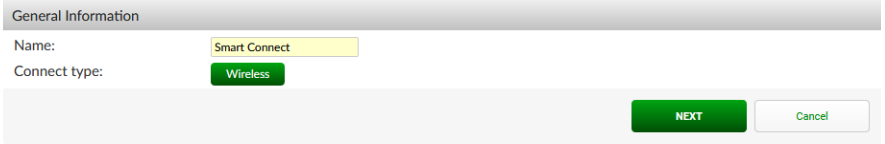
To configure Smart Connect and portals on FortiAuthenticator:

1. Create the Smart Connect profile on page 316
2. Create the captive portal on page 317
3. Create the self-service portal policy on page 318

Create the Smart Connect profile

To create Smart Connect profiles:

1. Go to *Authentication* > *Portals* > *Smart Connect Profiles*, and click *Create New*.
2. Under *General Information*, enter a name for the profile, and click *Next*.

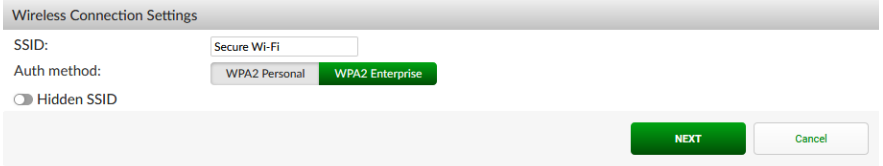


General Information

Name: Smart Connect

Connect type: Wireless

3. Under *Wireless Connection Settings*, set the following and then click *Next*.
   a. **SSID**: Enter your SSID name, for example Secure Wi-Fi.
   b. **Auth method**: *WPA2 Enterprise*.
   c. **Hidden SSID**: *Disabled*.



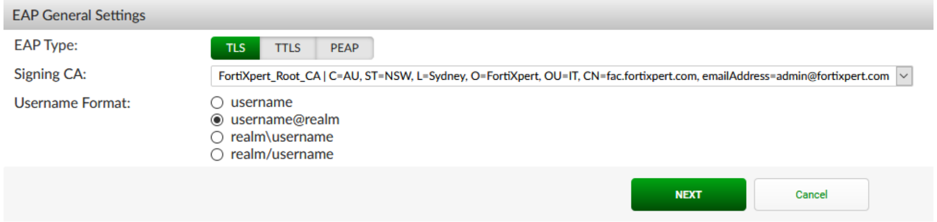
Wireless Connection Settings

SSID: Secure Wi-Fi

Auth method: WPA2 Personal [✓ WPA2 Enterprise]

Hidden SSID

4. Under *EAP General Settings*, set the following and then click *Next*.
   a. **EAP Type**: *TLS*.
   b. **Signing CA**: Select the local Root CA configured earlier.
   c. **Username Format**: Select your preference, for example *username@realm*.



EAP General Settings

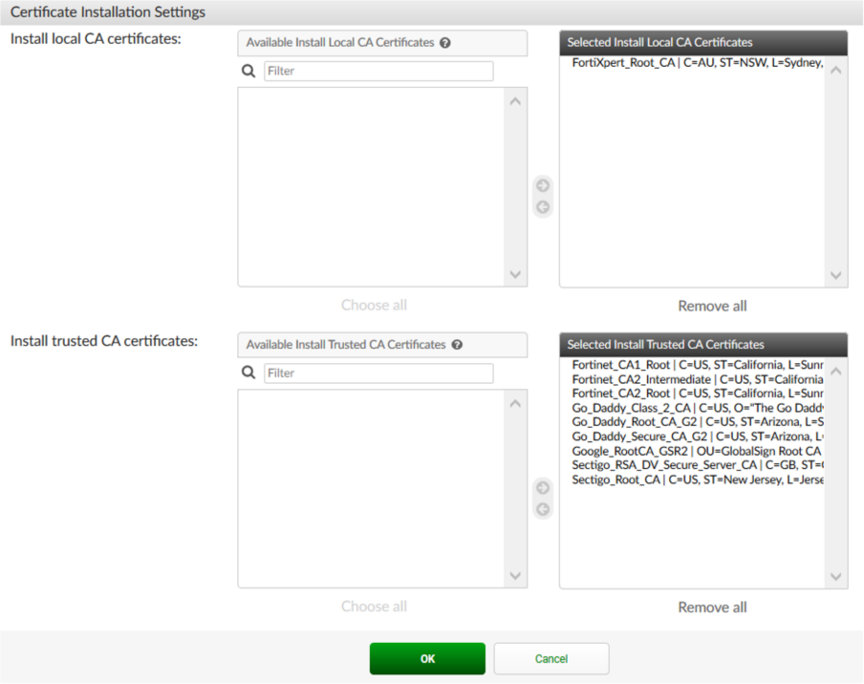
EAP Type: [✓ TLS] TTLS PEAP

Signing CA: FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney, O=FortiXpert, OU=IT, CN=fac.fortixpert.com, emailAddress=admin@fortixpert.com

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

5. Under *Certificate Installation Settings*, set the following and then click *OK*.
   a. **Install local CA certificates**: Choose to install the local Root_CA certificate.
   b. **Install trusted CA certificates**: Choose to install any certificate that is required for all relevant certificate

chains to be fully trusted.



Certificate Installation Settings

Install local CA certificates:

Selected Install Local CA Certificates:
FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney,

Install trusted CA certificates:

Selected Install Trusted CA Certificates:
Fortinet_CA1_Root | C=US, ST=California, L=Sunr
Fortinet_CA2_Intermediate | C=US, ST=California
Fortinet_CA2_Root | C=US, ST=California, L=Sunr
Go_Daddy_Class_2_CA | C=US, O="The Go Dadd
Go_Daddy_Root_CA_G2 | C=US, ST=Arizona, L=S
Go_Daddy_Secure_CA_G2 | C=US, ST=Arizona, L
Google_RootCA_GSR2 | OU=GlobalSign Root CA
Sectigo_RSA_DV_Secure_Server_CA | C=GB, ST=
Sectigo_Root_CA | C=US, ST=New Jersey, L=Jerse

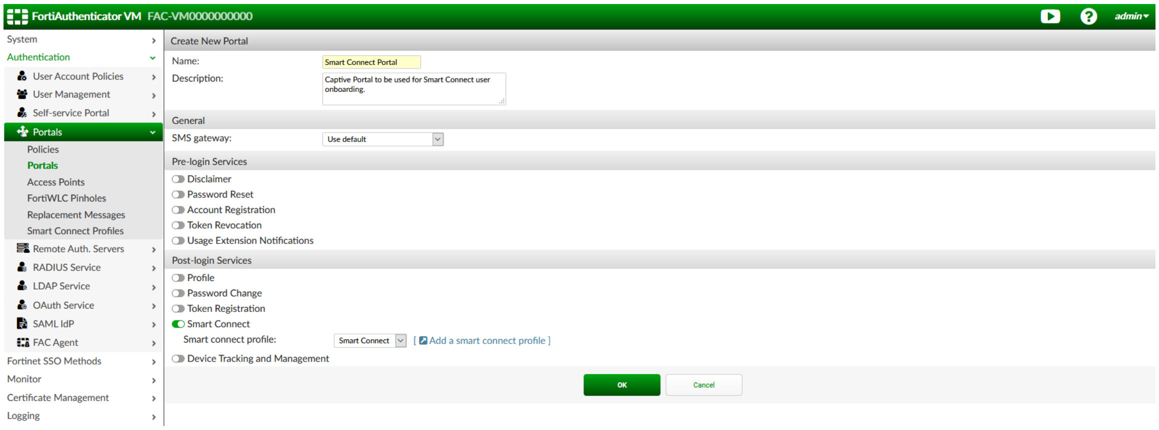
Available Install Local CA Certificates
Filter
Choose all
Remove all
Available Install Trusted CA Certificates
Filter
Choose all
Remove all
OK
Cancel

6. Select *OK* to complete the setup of the Smart Connect profile.

Create the captive portal

To create a captive portal:

1. Go to *Authentication* > *Portals* > *Portals*, and click *Create New*.
2. Under *Create New Portal*, enter a name and optional description for the portal.
3. Under *Post-login services*, enable *Smart Connect* and select the previously configured Smart Connect profile from the dropdown.
4. Select *OK*.



Create New Portal

Name: Smart Connect Portal

Description: Captive Portal to be used for Smart Connect user onboarding.

General

SMS gateway: Use default

Pre-login Services

○ Disclaimer
○ Password Reset
○ Account Registration
○ Token Revocation
○ Usage Extension Notifications

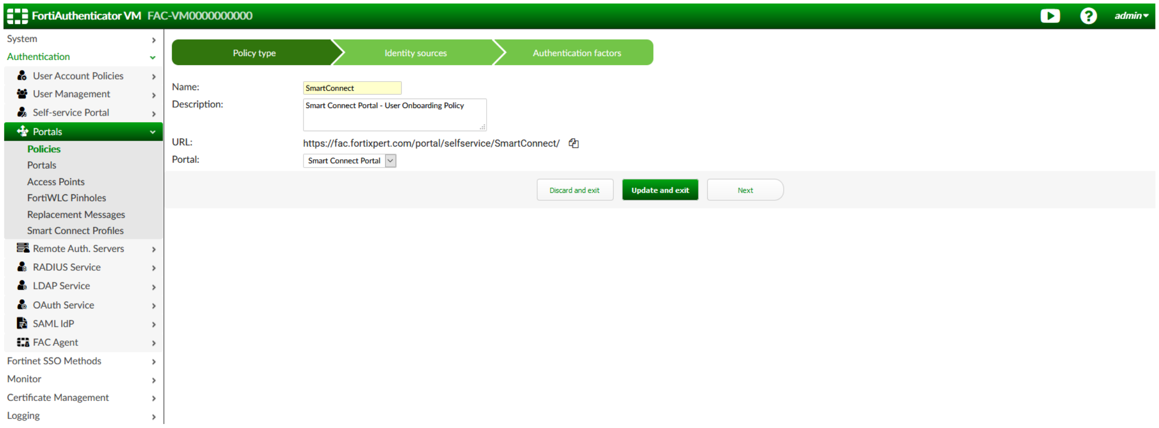
Post-login Services

○ Profile
○ Password Change
○ Token Registration
● Smart Connect
Smart connect profile: Smart Connect [Add a smart connect profile]
○ Device Tracking and Management

Create the self-service portal policy

To create a self-service portal policy:

1. Go to *Authentication > Portals > Policies*. Select the *Self-Service Portal* option, and click *Create New*.
2. Under *Policy Type*, set the following and then click *Next*.
   a. **Name**: Enter a policy name, for example *SmartConnect*.
   b. **Description**: Enter an optional description for the policy.
   c. **URL**: Note this URL. This is the external captive portal redirection URL which must be added to the Onboarding SSID configured on the FortiGate/WLC later.
   d. **Portal**: Select the previously configured Smart Connect portal.



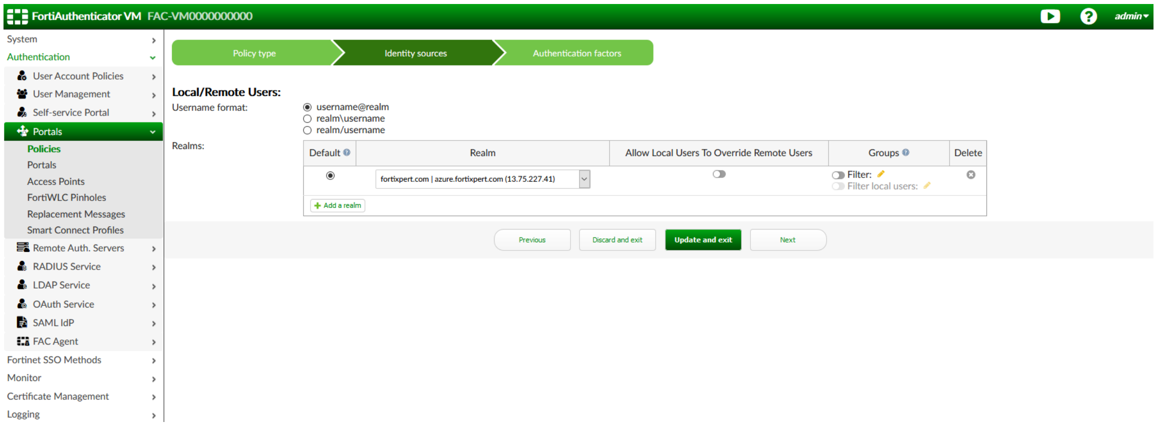
Name: SmartConnect

Description: Smart Connect Portal - User Onboarding Policy

URL: https://fac.fortixpert.com/portal/selfservice/SmartConnect/

Portal: Smart Connect Portal

3. Under *Identity sources*, set the following and then click *Next*:
   a. **Username format**: username@realm.
   b. **Realms**: In the dropdown box, select the LDAP realm associated with Azure, for example fortixpert.com.



Local/Remote Users:

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

Realms:

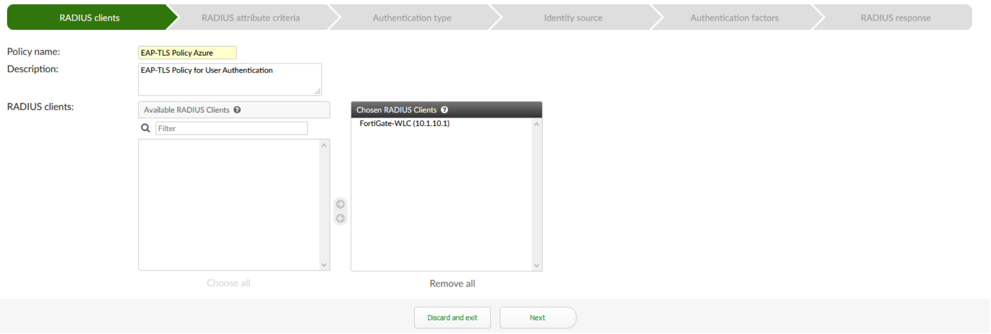
Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	fortixpert.com | azure.fortixpert.com (13.75.227.41)		Filter: Filter local users:	

4. Under *Authentication factors*, leave the default options in place, and click *Save and exit*.

Configure RADIUS settings on FortiAuthenticator

To create a RADIUS service policy:

1. Go to *Authentication* > *RADIUS Service* > *Policies*, and click *Create New*.
2. Under *RADIUS clients*, set the following and then click *Next*:
   a. **Policy Name**: Enter a name for the policy, for example EAP-TLS Policy Azure.
   b. **Description**: Enter an optional description, for example EAP-TLS Policy for User Authentication.
   c. **RADIUS Clients**: Add the FortiGate to the *Chosen RADIUS Clients* section.

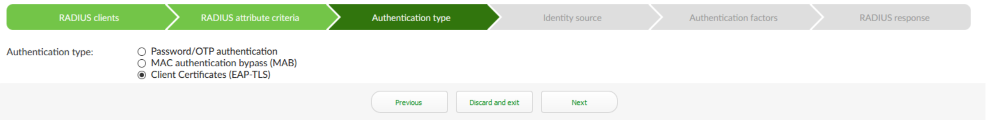


Policy name: EAP-TLS Policy Azure

Description: EAP-TLS Policy for User Authentication

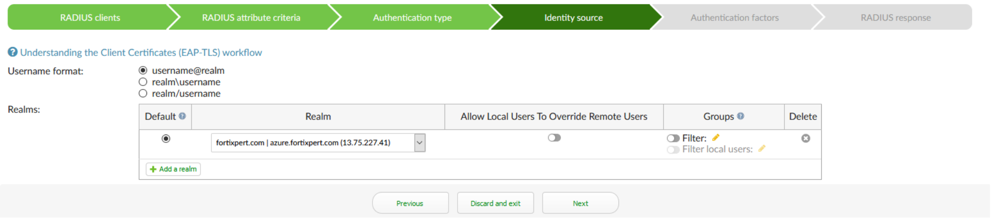
RADIUS clients: Chosen RADIUS Clients: FortiGate-WLC (10.1.10.1)

3. Under *RADIUS attribute criteria*, click *Next* without making changes.
4. Under *Authentication type*, select *Client Certificates (EAP-TLS)*, and click *Next*.



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

5. Under *Identity source*, set the following and then click *Next*:
   a. **Username format**: Select your preferred format, for example username@realm.
   b. **Realms**: Select the realm that you set up to communicate with Azure, for example fortixpert.com.



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

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	fortixpert.com | azure.fortixpert.com (13.75.227.41)		Filter: Filter local users:	

6. Under *Authentication factors*, click *Next* without making changes.
7. Under *RADIUS response*, validate that the EAP-TLS response is as expected, and click *Save and exit*.

FortiGate configuration

This section outlines the configuration required on FortiGate WLAC to provision an onboarding (Smart Connect enabled) WiFi network and a secure (WPA2 + EAP-TLS enabled) Wi-Fi network.

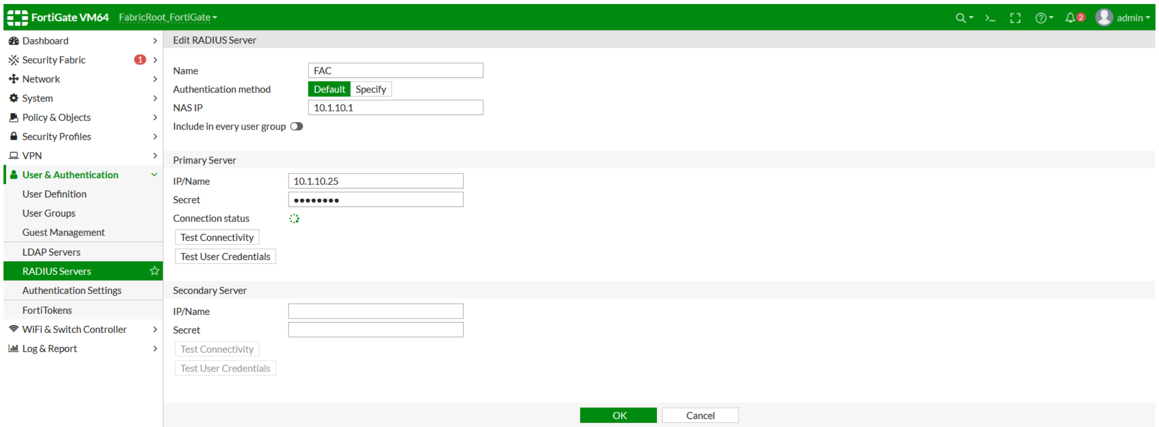
To configure the FortiGate:

1. Configure the RADIUS server on FortiGate on page 320
2. Create the user group for cloud-based directory user accounts on page 320
3. Provision the Onboarding and Secure WiFi networks on page 321

Configure the RADIUS server on FortiGate

To configure the RADIUS server:

1. In FortiGate, go to *User & Authentication* > *RADIUS Servers*, and click *Create New*.
2. Under *New RADIUS Server*, set the following:
   a. **Name**: Enter a name for the RADIUS server, for example FAC.
   b. **NAS IP**: Enter the Network Access Server (NAS) IP. This should ideally be the IP from the interface/VLAN FortiAuthenticator is on.
3. Under *Primary Server*, set the following:
   a. **IP/Name**: Enter the FortiAuthenticator IP address.
   b. **Secret**: Enter the secret matching the one configured on FortiAuthenticator.
4. Click *Test Connectivity* to test if the connection is correctly configured, and click *OK*.



Edit RADIUS Server

Name: FAC
Authentication method: Default Specify
NAS IP: 10.1.10.1
Include in every user group

Primary Server

IP/Name: 10.1.10.25
Secret: ••••••••
Connection status

Secondary Server

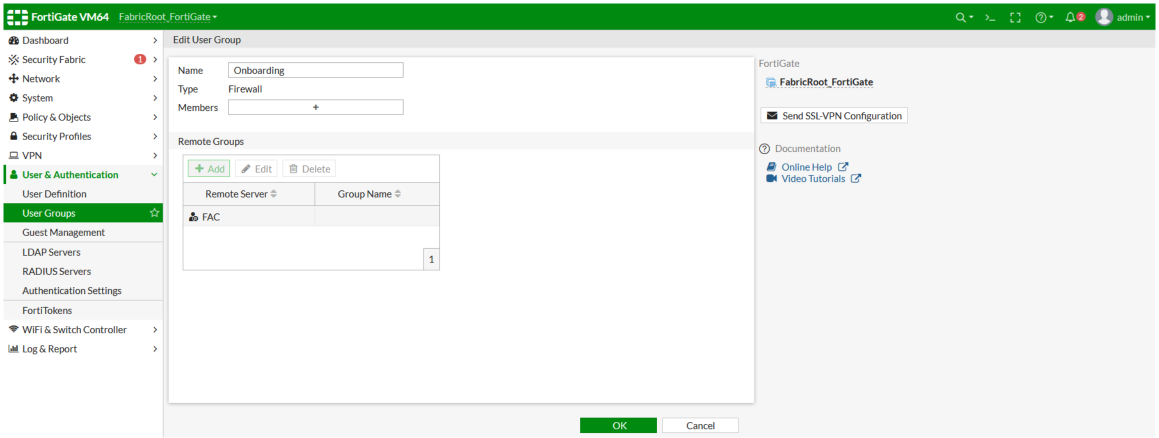
IP/Name:
Secret:

Create the user group for cloud-based directory user accounts

To create user groups:

1. Go to *User & Authentication* > *User Groups*, and click *Create New*.
2. Configure the following settings:
   a. **Name**: Configure a name, for example Onboarding.
   b. **Type**: Firewall.
   c. **Remote Groups**: Select *Add*. Within the Add Group Match window, select FortiAuthenticator as the remote server from the dropdown box.
   d. **Groups**: Any.

3. Select *OK* on the *Add Group Match* window. The Onboarding group is now created.



Edit User Group

Name: Onboarding
Type: Firewall
Members: +

Remote Groups

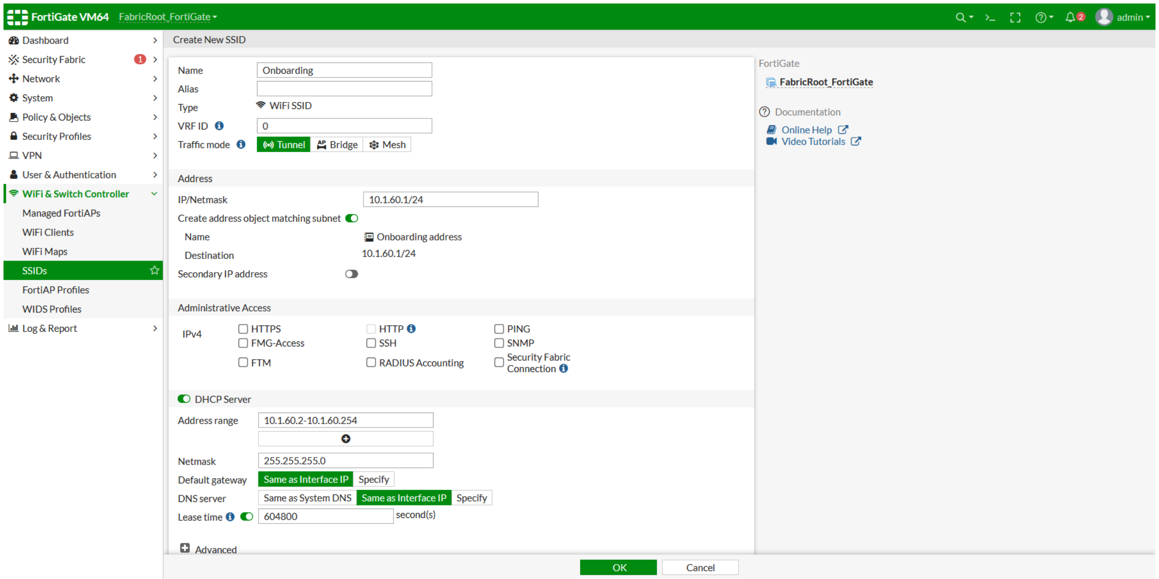
Remote Server	Group Name
FAC	

1

Provision the Onboarding and Secure WiFi networks

To provision the Smart Connect enabled "Onboarding" SSID:

1. Go to *Wi-Fi & Switch Controller > SSID*, and click *Create New*.
2. Under *Create New SSID*, set the following:
   a. **Profile name**: Enter a name for the profile, for example Onboarding.
   b. **Traffic mode**: *Tunnel*.
3. Under *Address*, set the following:
   a. **IP/Netmask**: Enter the interface IP address for the Onboarding SSID.
4. Under *DHCP Server*, enable the DHCP Server setting and set the following:
   a. Leave *Address range*, *Netmask*, *Gateway*, and *Lease time* in their default states.
   b. **DNS server**: Select *Same as Interface IP* or specify a local DNS server that can resolve your FortiAuthenticator FQDN. If you are using the DNS database on FortiGate, select *Same as Interface IP*.



Create New SSID

Name: Onboarding
Alias:
Type: WiFi SSID
VRF ID: 0
Traffic mode: [✓ Tunnel] Bridge Mesh

Address

IP/Netmask: 10.1.60.1/24
Create address object matching subnet: ●
Name: Onboarding address
Destination: 10.1.60.1/24
Secondary IP address: ○

Administrative Access

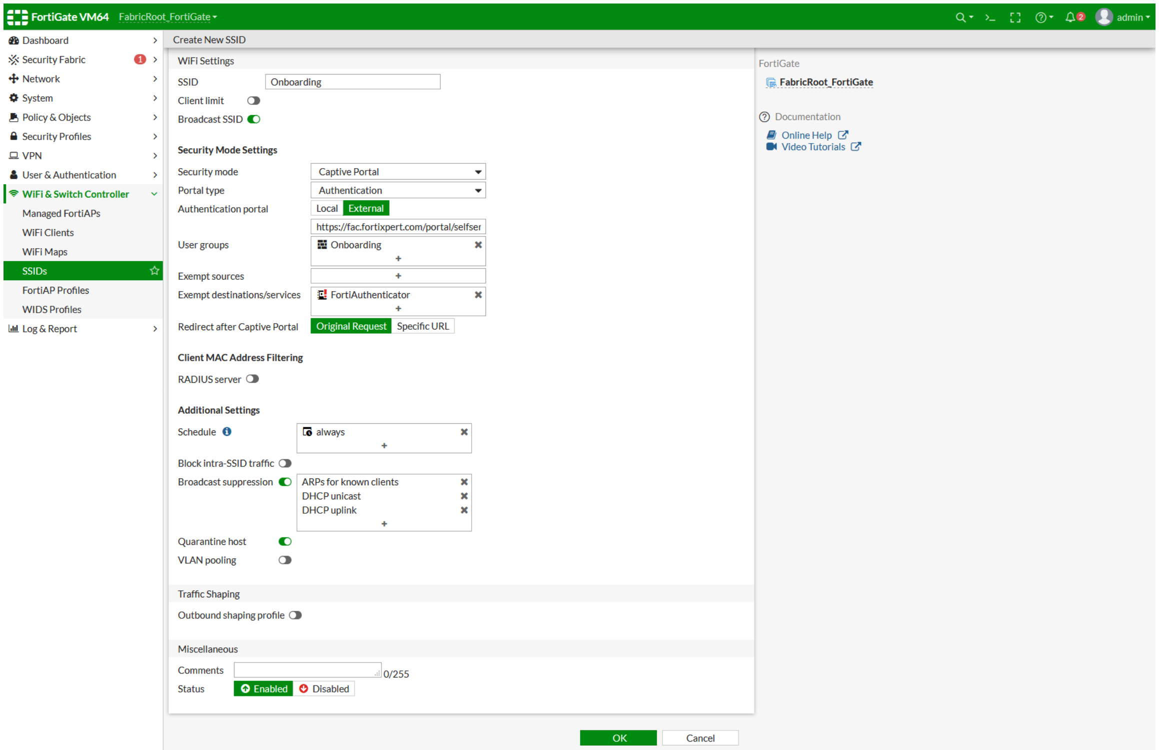
IPv4: □ HTTPS □ FMG-Access □ FTM □ HTTP □ SSH □ RADIUS Accounting □ PING □ SNMP □ Security Fabric Connection

● DHCP Server

Address range: 10.1.60.2-10.1.60.254
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: Same as System DNS [✓ Same as Interface IP] Specify
Lease time ●: 604800 second(s)

5. Under *Network*, leave the *Decide detection* setting enabled.

6. Under *WiFi Settings*, set the following:
   a. **SSID**: Enter the SSID, for example Onboarding.
   b. **Security mode**: *Captive Portal*.
   c. **Portal type**: *Authentication*.
   d. **Authentication portal**: Select *External*, and enter the FortiAuthenticator Smart Connect portal redirection URL obtained when configuring Smart Connect on FortiAuthenticator.
   e. **User groups**: Select the previously configured user group, for example Onboarding.
   f. **Exempt destinations/services**: Select FortiAuthenticator.
   g. Leave all other settings as their default state.



Create New SSID

WiFi Settings

SSID: Onboarding
Client limit: off
Broadcast SSID: on

Security Mode Settings

Security mode: Captive Portal
Portal type: Authentication
Authentication portal: Local [✓ External]
https://fac.fortixpert.com/portal/selfser
User groups: Onboarding
Exempt sources:
Exempt destinations/services: FortiAuthenticator
Redirect after Captive Portal: [✓ Original Request] Specific URL

Client MAC Address Filtering

RADIUS server: off

Additional Settings

Schedule: always
Block intra-SSID traffic: off
Broadcast suppression: on
ARPs for known clients
DHCP unicast
DHCP uplink
Quarantine host: on
VLAN pooling: off

Traffic Shaping

Outbound shaping profile: off

Miscellaneous

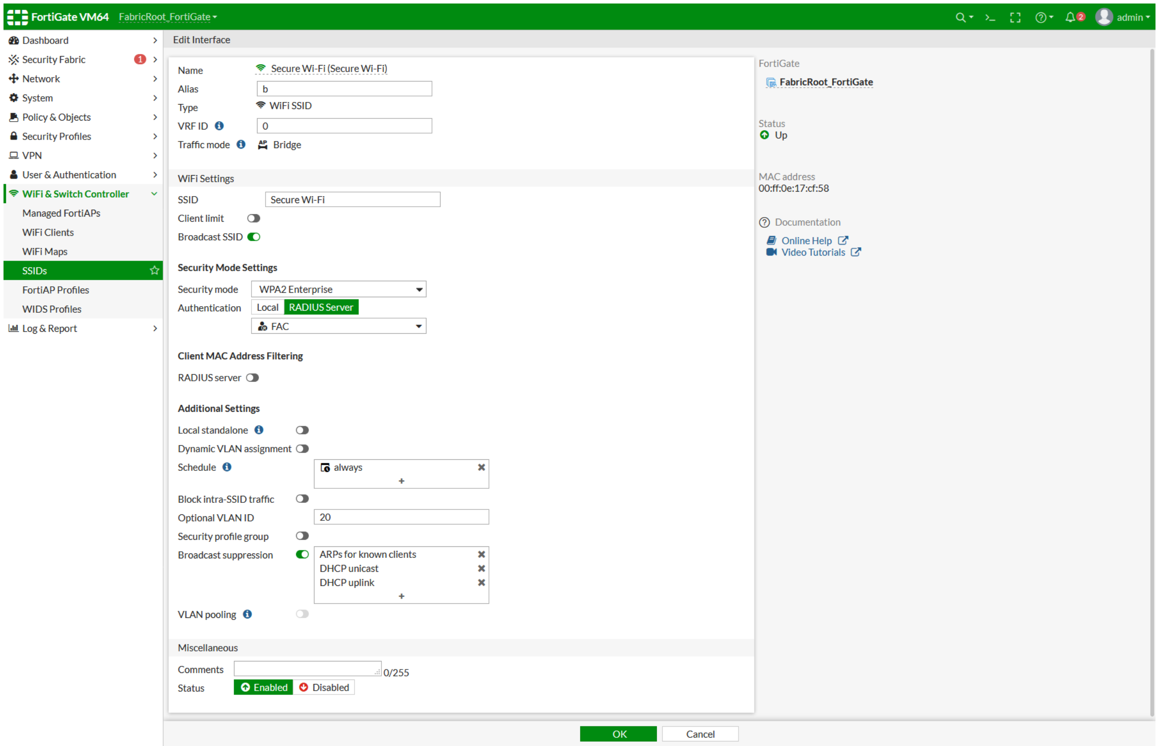
Comments: 0/255
Status: [✓ Enabled] Disabled

7. Click *OK*.

To provision the "Secure Wi-Fi" network:

1. Go to *WiFi & Switch Controller > SSID*, and click *Create New*.
2. Configure the following settings:
   a. **Profile name**: Enter a profile name, for example Secure Wi-Fi.
   b. **Traffic mode**: *Bridge*.
   c. **SSID**: Enter the SSID name, for example Secure Wi-Fi.
   d. **Security mode**: *WPA2 Enterprise*.
   e. **Authentication**: Choose *RADIUS Server*, and select the FortiAuthenticator.

f. **Optional VLAN ID**: This setting is optional and can be configured if WiFi traffic needs to be tagged by the AP to a VLAN configured on your local switch. Dynamic VLAN assignment is also supported.



Edit Interface

Name: Secure Wi-Fi (Secure Wi-Fi)
Alias: b
Type: WiFi SSID
VRF ID: 0
Traffic mode: Bridge

WiFi Settings

SSID: Secure Wi-Fi
Client limit: off
Broadcast SSID: on

Security Mode Settings

Security mode: WPA2 Enterprise
Authentication: Local [✓ RADIUS Server]
FAC

Client MAC Address Filtering

RADIUS server: off

Additional Settings

Local standalone: off
Dynamic VLAN assignment: off
Schedule: always
Block intra-SSID traffic: off
Optional VLAN ID: 20
Security profile group: off
Broadcast suppression: on
ARPs for known clients
DHCP unicast
DHCP uplink
VLAN pooling: off

Miscellaneous

Comments: 0/255
Status: [✓ Enabled] Disabled

Status: Up
MAC address: 00:ff:0e:17:cf:58

OK Cancel

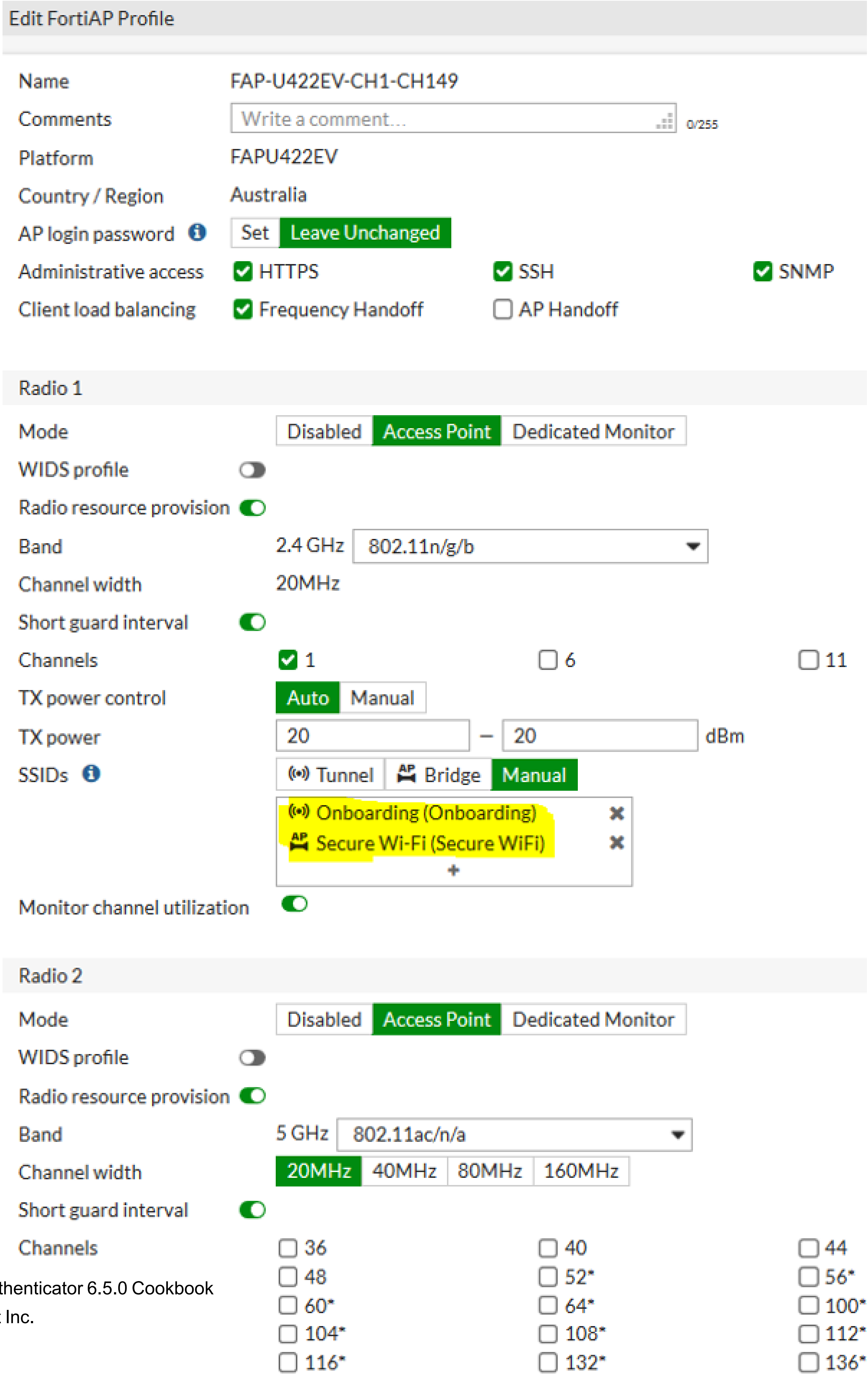
3. Click *OK*.

To assign SSIDs to FortiAP profiles:

1. Go to *WiFi & Switch Controller > FortiAP Profiles*.
2. Select the relevant AP profile(s) and assign the previously created SSIDs (Onboarding and Secure Wi-Fi) to the

AP radio interfaces.

3. Confirm the SSIDs are broadcasting and can be seen by WiFi enabled devices.



Edit FortiAP Profile

Name	FAP-U422EV-CH1-CH149		
Comments	Write a comment... 0/255		
Platform	FAPU422EV		
Country / Region	Australia		
AP login password	Set [✓ Leave Unchanged]		
Administrative access	☑ HTTPS	☑ SSH	☑ SNMP
Client load balancing	☑ Frequency Handoff	□ AP Handoff	

Radio 1

Mode	Disabled [✓ Access Point] Dedicated Monitor		
WIDS profile	○		
Radio resource provision	●		
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	20 – 20 dBm		
SSIDs	Tunnel Bridge [✓ Manual]		
	Onboarding (Onboarding) ✖ Secure Wi-Fi (Secure WiFi) ✖ +		
Monitor channel utilization	●		

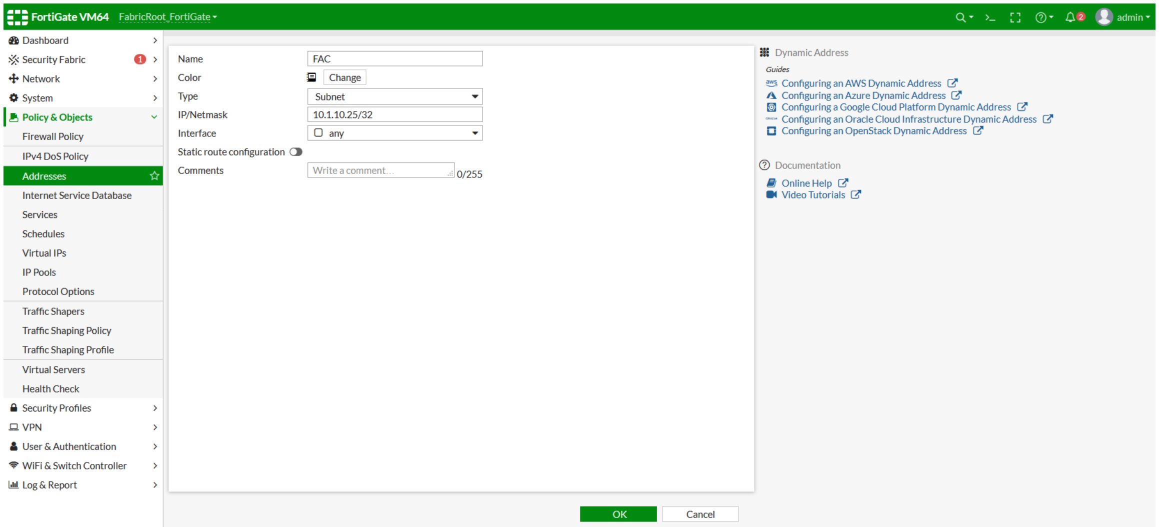
Radio 2

Mode	Disabled [✓ Access Point] Dedicated Monitor		
WIDS profile	○		
Radio resource provision	●		
Band	5 GHz 802.11ac/n/a		
Channel width	[✓ 20MHz] 40MHz 80MHz 160MHz		
Short guard interval	●		
Channels	□ 36	□ 40	□ 44
	□ 48	□ 52*	□ 56*
	□ 60*	□ 64*	□ 100*
	□ 104*	□ 108*	□ 112*
	□ 116*	□ 132*	□ 136*

4. Click *OK*.

To create a new FortiAuthenticator object to use with firewall policies:

1. Go to *Policy & Objects* > *Addresses*, and click *Create New* > *Address*.
2. Configure the following settings:
   a. **Name**: Enter a name, for example FAC.
   b. **Type**: *Subnet*.
   c. **IP/Netmask**: The FortiAuthenticator IP address.
   d. **Interface**: *any*.



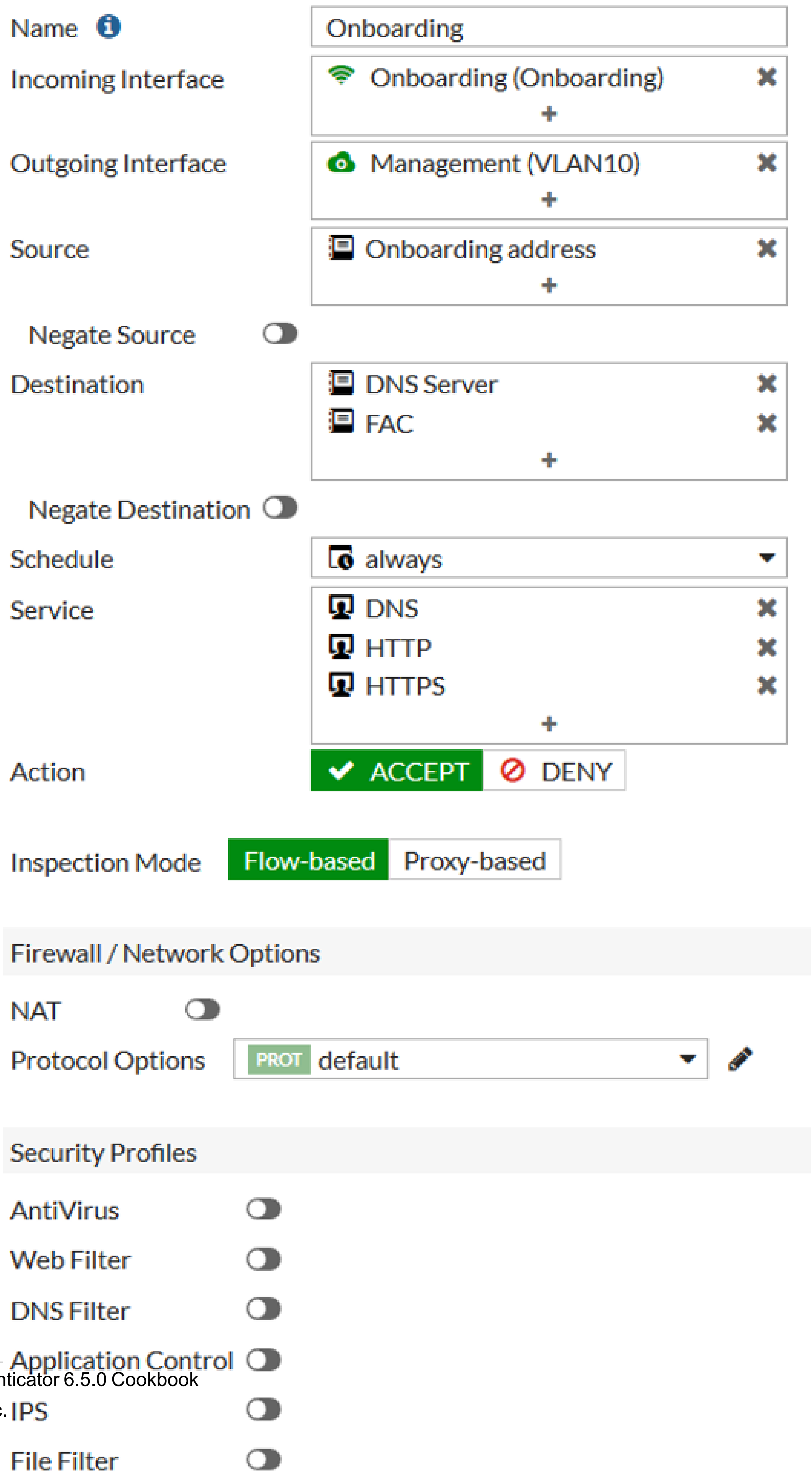
Name: FAC
Color: Change
Type: Subnet
IP/Netmask: 10.1.10.25/32
Interface: □ any
Static route configuration
Comments: Write a comment... 0/255

3. Click *OK*.

To create a firewall policy for the Onboarding SSID:

1. Go to *Policy & Objects* > *Firewall Policy*, and click *Create New*.
2. On the *New Policy* page, set the following:
   a. **Name**: Enter a name, for example Onboarding Policy.
   b. **Incoming Interface**: Select the Onboarding SSID.
   c. **Outgoing Interface**: Select the Management VLAN.
   d. **Source**: Select *all* or the Onboarding address subnet range.
   e. **Destination**: Select FortiAuthenticator and the DNS server if you are using a third party DNS server.
   f. **Service**: *DNS*, *HTTP*, and *HTTPS*.
   g. Under *Advanced*, enable the *Exempt from Captive Portal* option.
   When using a FortiOS version earlier than 6.4.1, you can enable this setting in the CLI with the command `set`

```
captive-portal-exempt enable.
```



Name	Onboarding
Incoming Interface	Onboarding (Onboarding)
Outgoing Interface	Management (VLAN10)
Source	Onboarding address
Negate Source	○
Destination	DNS Server FAC
Negate Destination	○
Schedule	always
Service	DNS HTTP HTTPS
Action	[✓ ACCEPT] DENY
Inspection Mode	[✓ Flow-based] Proxy-based

Firewall / Network Options

NAT	○
Protocol Options	PROT default

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○
File Filter	○

3. Click *OK*.

Results

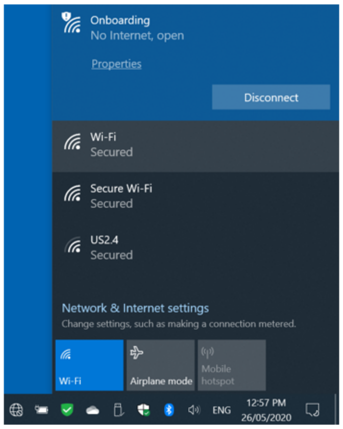
You can now connect your device to the Onboarding SSID and proceed with the Smart Connect onboarding process:

- Smart Connect Windows device onboarding process on page 330
- Smart Connect iOS device onboarding process on page 332

Smart Connect Windows device onboarding process

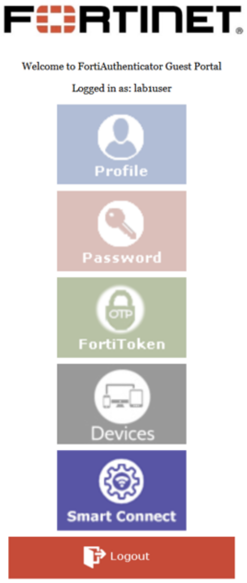
To onboard a Windows device:

1. On your Windows device, connect to the Onboarding WiFi network.

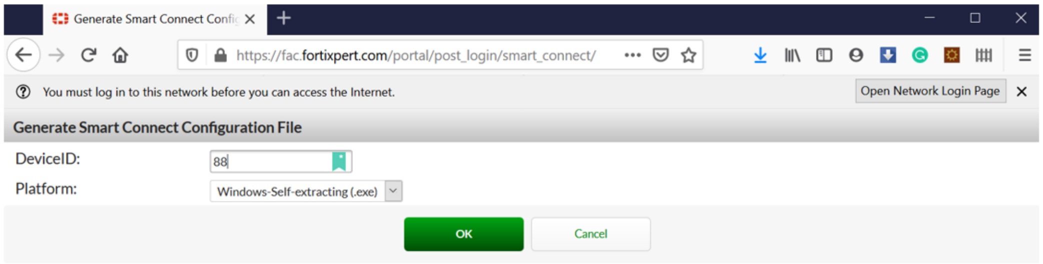


The FortiAuthenticator login screen is displayed.

2. Enter either your Google Workspace or Azure login credentials, and select *Login*. Once logged in, select *Smart Connect*.



3. Enter a unique *Device ID* and choose your operating system from the *Platform* dropdown. Click *OK*.


Generate Smart Connect Confi
https://fac.fortixpert.com/portal/post_login/smart_connect/
Open Network Login Page
OK
Cancel

You must log in to this network before you can access the Internet.

Generate Smart Connect Configuration File

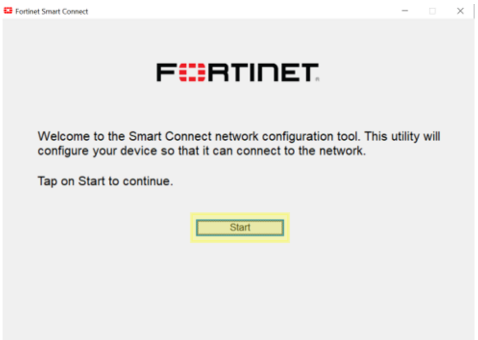
DeviceID: 88

Platform: Windows-Self-extracting (.exe)

A *SmartConnect_UserName.exe* file will be made available. Save this file.

4. Run the *SmartConnect_UserName.exe* file.
If the Microsoft Defender warning message appears, click *More info* > *Run anyway*. If the User Account Control warning appears, click *Yes*.
The Fortinet Smart Connect network configuration tool will now run.

5. Select *Start*.



Welcome to the Smart Connect network configuration tool. This utility will configure your device so that it can connect to the network.

Tap on Start to continue.

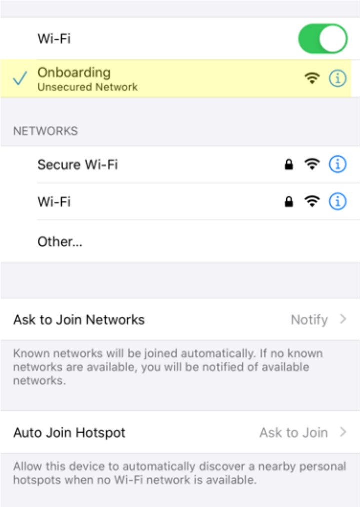
Your device will now be provisioned with the wireless network information and certificates in order to connect to the Secure Wi-Fi SSID.

6. Once provisioning is complete, click *Connect*. Your device will now connect to the Secure Wi-Fi network using WPA2 and EAP-TLS.
You may wish to forget the Onboarding network to prevent your device from automatically connecting to it in the future.

Smart Connect iOS device onboarding process

To onboard an iOS device:

1. On the iOS device, connect to the Onboarding WiFi network.



Wi-Fi

✓ Onboarding
Unsecured Network

NETWORKS

Secure Wi-Fi

Wi-Fi

Other...

Ask to Join Networks: Notify

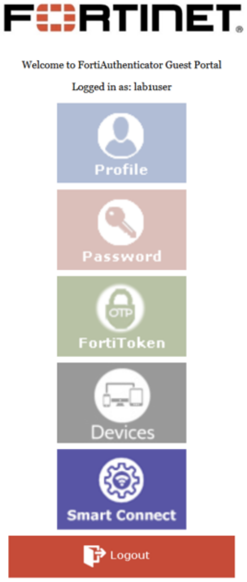
Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.

Auto Join Hotspot: Ask to Join

Allow this device to automatically discover a nearby personal hotspots when no Wi-Fi network is available.

The FortiAuthenticator login screen is displayed.

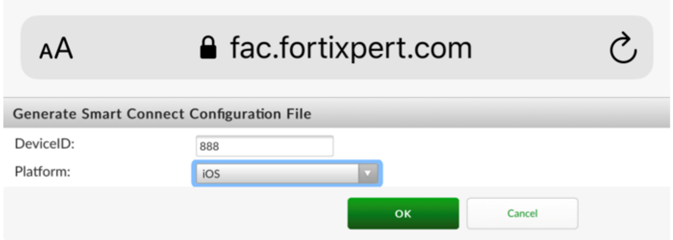
2. Enter either your Google Workspace or Azure login credentials, and select *Login*.
Once logged in, select *Smart Connect*.



Welcome to FortiAuthenticator Guest Portal

Logged in as: lab1user

3. Enter a unique *Device ID* and choose your operating system from the *Platform* dropdown. Click *OK*.



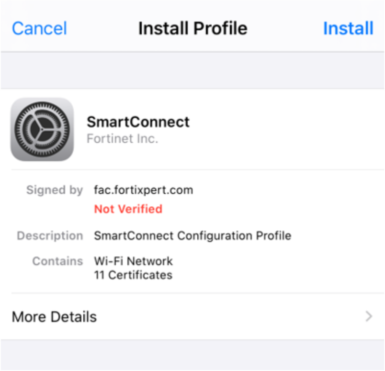
AA fac.fortixpert.com

Generate Smart Connect Configuration File

DeviceID: 888

Platform: iOS

4. When prompted, download the configuration profile.
5. In *Settings*, select *Profile Downloaded*.
6. Select *Install* within the SmartConnect Install Profile. Depending on your device setup, you may be prompted to enter your device passcode/password.



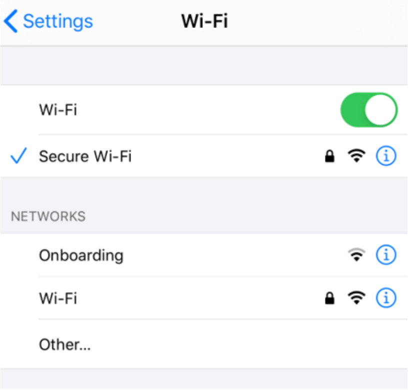
SmartConnect
Fortinet Inc.

Signed by fac.fortixpert.com
Not Verified

Description SmartConnect Configuration Profile

Contains Wi-Fi Network
11 Certificates

7. On the warning screen, select *Install* to install any root certificates included within the profile. Once the installation is finished, click *Done*.
8. In *Settings*, select the information icon next to the Onboarding WiFi network and select *Forget this Network*. Once the network has been forgotten, the device will automatically connect to the Secure Wi-Fi network.



Wi-Fi

✓ Secure Wi-Fi

NETWORKS

Onboarding

Wi-Fi

Other...

ZTNA

This section describes configuring ZTNA using FortiAuthenticator.

Setting up a zero trust tunnel

A zero trust tunnel allows FortiAuthenticator to securely access TCP-based-on-premise services from the public internet. Further, using zero trust tunnels, you can access an on-premise LDAP/AD server.

In this example, FortiAuthenticator forms a zero trust tunnel to a remote ZTNA server, i.e., a FortiGate device.

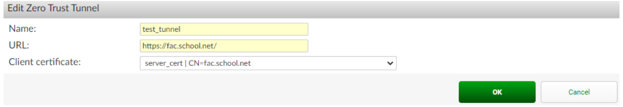
To set up a zero trust tunnel:

1. Configuring a zero trust tunnel on FortiAuthenticator on page 334
2. Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator on page 335
3. Configuring certificate authentication for FortiAuthenticator on page 335
4. Configuring a ZTNA server on page 338
5. Configuring a ZTNA rule on page 339
6. Debugging on page 340

Configuring a zero trust tunnel on FortiAuthenticator

To configure a zero trust tunnel:

1. Go to *System* > *Network* > *Zero Trust Tunnels*.
2. Select *Create New*.
   The *Create New Zero Trust Tunnel* window opens.
3. In *Name*, enter a name for the zero trust tunnel.
4. In *URL*, enter a URL specifying the IP/FQDN and port for the ZTNA server, e.g., `https://fac.school.net:8443/`.
5. In the *Client certificate* dropdown, select a certificate.
   This certificate is used to authenticate to the ZTNA server. In this example, it is generated by the FortiAuthenticator CA. See Server Certificate.
6. Click *OK*.



Edit Zero Trust Tunnel

Name: test_tunnel

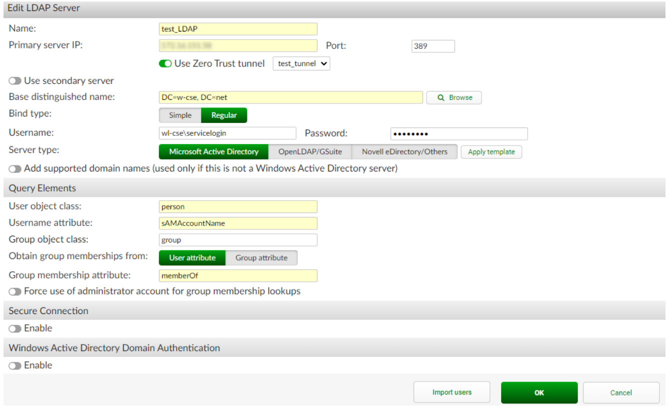
URL: https://fac.school.net/

Client certificate: server_cert | CN=fac.school.net

Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator

To configure an LDAP server:

1. Go to *Authentication* > *Remote Auth. Servers* > *LDAP*, and select *Create New*.
2. In *Create New LDAP server*:
   a. In *Name*, enter a name.
   b. Enable *Use Zero Trust tunnel* and from the dropdown select the zero trust tunnel configured in Configuring a zero trust tunnel on FortiAuthenticator on page 334.
   c. In *Primary Server IP*, enter the IP address/FQDN of the LDAP server.
   d. In *Port*, enter the port number of the LDAP server.
   e. In *Base distinguished name*, enter a base distinguished name.
   f. In *Bind Type*, select *Regular*.
   Enter the username and password for the LDAP server administrator account.
3. Click *OK*.



Edit LDAP Server

Name: test_LDAP

Primary server IP: [redacted] Port: 389

Use Zero Trust tunnel: test_tunnel

Use secondary server

Base distinguished name: DC=w-cse, DC=net

Bind type: Simple [✓ Regular]

Username: wl-cse\servicelogin Password: ••••••••

Server type: [✓ Microsoft Active Directory] OpenLDAP/GSuite Novell eDirectory/Others

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

Query Elements

User object class: person

Username attribute: sAMAccountName

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

Windows Active Directory Domain Authentication

Enable

Configuring certificate authentication for FortiAuthenticator

To configure a local root CA:

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*, and select *Create New*.
   The *Create New Local CA Certificate* window opens.
2. In *Certificate ID*, enter a unique ID for the CA.
3. Ensure that the *Certificate type* is *Root CA*.
4. In *Name(CN)*, enter the subject name, e.g., a domain name.
5. Click *OK*.

To export the local root CA:

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
2. From the local CA certificate list, select the local root CA created in Configuring a local root CA, and select *Export Certificate*.
   The public certificate for the CA is downloaded to your computer, and the certificate is later imported to FortiGate. See Importing local root CA.

To create a server certificate for FortiAuthenticator signed by the CA:

1. Go *Certificate Management* > *End Entities* > *Local Services*, and select *Create New*.
   The *Create New Server Certificate* window opens.
2. In *Certificate ID*, enter a unique ID for the certificate.
3. In the *Certificate Signing Options* pane, ensure that the *Issuer* is *Local CA* and the *Certificate authority* is the local CA created in Configuring a local root CA.
4. In the *Subject Information* pane, for *Name(CN)*, enter the FQDN of the FortiAuthenticator.
   The certificate is used when configuring the zero trust tunnel. See Configuring a zero trust tunnel on FortiAuthenticator on page 334.

To import the local root CA to FortiGate:

1. Go to *System* > *Certificates*, and from the *Create/Import* dropdown, select *CA Certificate*.
   The *Import CA Certificate* window opens.
2. In *Type*, select *File*.
3. Select *Upload*, and locate the local root certificate created in Configuring a local root CA on your computer.
4. Click *OK*.

The imported root CA is available with the name `CA_Cert_X` where `X` denotes the number of certificates imported.

The *Issuer* field for the imported root CA is the *Name(CN)* you gave it.

To rename the root CA on FortiGate:

In the CLI console, enter the following commands:

```
config vpn certificate ca
   rename <cert> to <new name>
```

To create an address object on FortiGate for FortiAuthenticator and the LDAP server:

1. Go to *Policy & Objects* > *Addresses*, and from the *Create New* dropdown, select *Address*.
   The *New Address* window opens.
2. In *Name*, enter a name for the address, e.g., `FAC`.
3. In *IP/Netmask*, enter the public IP address of the FortiAuthenticator with its subnet mask.

For FortiTrust Identity, `154.52.4.227` is the fixed WAN IP address for FortiAuthenticator Cloud to build zero trust tunnels into an on-prem environment.

Use the IP address with its subnet mask.

4. Click *OK*.
   The address is used when Configuring an authentication rule.
5. Go to *Policy & Objects* > *Addresses*, and from the *Create New* dropdown, select *Address*.
   The *New Address* window opens.
6. In *Name*, enter a name for the address, e.g., `lab-ad-address`.
7. In *IP/Netmask*, enter the private IP address of the LDAP server with its subnet mask.
8. Click *OK*.

To configure an authentication scheme with `user-cert` enabled:

1. Go to *Policy & Objects* > *Authentication Rules*.
2. From the *Create New* dropdown, select *Authentication Schemes*.
   The *New Authentication Scheme* window opens.
3. In *Name*, enter a name for the authentication scheme.
4. In *Method*:
   a. Select + to open the *Select Entries* window.
   b. Select *Certificate*.
   c. Select *Close*.
5. Click *OK*.

Alternatively, in the CLI console, enter the following commands:

```
config authentication scheme
   edit "test_scheme" #The authentication scheme name
      set method cert
      set user-cert enable
   next
end
```

To configure an authentication rule that uses the authentication scheme:

1. Go to *Policy & Objects* > *Authentication Rules*.
2. From the *Create New* dropdown, select *Authentication Rules*.
   The *Add New Rule* window opens.
3. In *Name*, enter a name for the authentication rule.
4. In *Source Address*:
   a. Select + to open the *Select Entries* window.
   b. Search and select the address object for FortiAuthenticator. See Address object for FortiAuthenticator.
   c. Select *Close*.
5. In *Incoming interface*:
   a. From the dropdown, select the external interface used in Configuring a ZTNA server on page 338.
6. Enable *Authentication Scheme* and from the dropdown select the authentication scheme created in Creating an authentication scheme.
7. Set *IP-based Authentication* as *Disable*.
8. Click *OK*.

Alternatively, in the CLI console, enter the following commands:

```
config authentication rule
   edit "Cert-Auth-Rule" #The authentication rule name
      set srcintf "port1"
      set srcaddr "fac"
      set ip-based disable
      set active-auth-method "test_scheme" #The authentication scheme
   next
end
```

To configure authentication setting to use the CA that issued the client certificate as the `user-cert-ca`:

1. In the CLI console, enter the following commands:
   ```
   config authentication setting
     set user-cert-ca "FAC_Cloud" #The CA certificate being used for client certificate
          verification
   end
   ```

Configuring a ZTNA server

To configure a ZTNA server:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Servers* tab.
2. Select *Create New*.
   The *New ZTNA Server* window opens.
3. In *Type* select *IPv4*.

   Once set up, *Type* cannot be changed when editing the ZTNA server.

4. In *Name*, enter a name for the server.
5. In the *Network* pane:
   a. In *External interface* dropdown, select an external interface.
      Select *Create* to create a new interface.
   b. In *External IP*, enter the external IP address that the ZTNA clients, e.g., FortiAuthenticator, connect to.
   c. In *External port*, enter the port number that the ZTNA clients, e.g., FortiAuthenticator, connect to, e.g., `8443`.
6. In *Services and Servers* pane:
   a. In *Default certificate* dropdown, select *Fortinet_Factory*.
      Clients are presented with this certificate when they connect to the access proxy VIP.
   b. In *Service/server mapping*, select *Create new*.
      The *New Service/Server Mapping* window opens.
      i. In *Type*, select *IPv4*.

         All hosted servers must be the same address type. The address type cannot be changed after the mapping is created.

      ii. In *Service*, select *TCP Forwarding*.
      iii. In the *Servers* pane, add a server by selecting *Create new*.
         Select an address and enter a port number for the LDAP server, e.g., `lab-ad-address` and `389`.

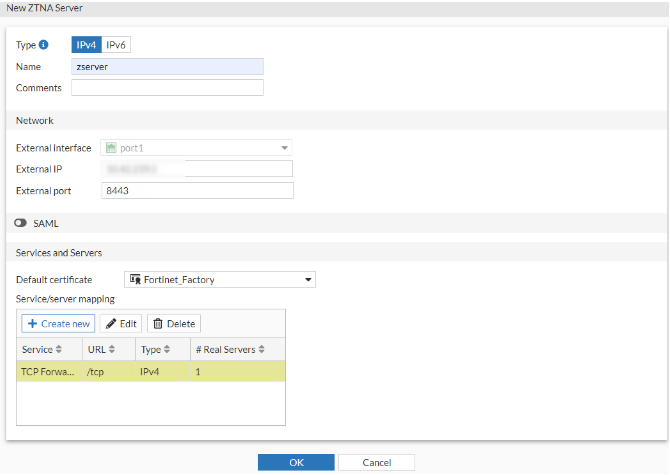
         The address and the port number must match the *Primary Server IP* and *Port* when Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator on page 335.

By default, LDAP uses port `389`.

Click *OK*.

iv. Click *OK*.

7. Click *OK*.



New ZTNA Server

Type: IPv4 | IPv6

Name: zserver

Comments:

Network

External interface: port1

External IP: [redacted]

External port: 8443

SAML

Services and Servers

Default certificate: Fortinet_Factory

Service/server mapping

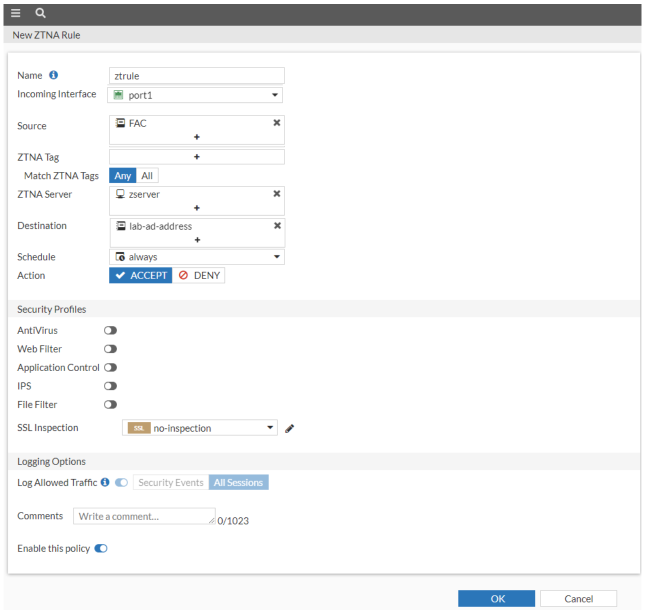
Service	URL	Type	# Real Servers
TCP Forwa...	/tcp	IPv4	1

Configuring a ZTNA rule

To configure a ZTNA rule:

1. Go to *Policy & Objects* > *ZTNA* and select *ZTNA Rules* tab.
2. Select *Create New*.
   The *New ZTNA Rule* window opens.
3. In *Name*, enter a name for the ZTNA rule.
4. In *Incoming Interface*, select the same interface as selected in Configuring a ZTNA server on page 338.
5. In *Source*, select +, and from the *Select Entries* list, select the address object for FortiAuthenticator. See Address object for FortiAuthenticator, and select *Close*.
6. In *ZTNA Server*, select the server created in Configuring a ZTNA server on page 338.
7. In *Destination*, select +, and from the *Select Entries* list, either select or create a destination.

8. Click *OK*.



Name	ztrule
Incoming Interface	port1
Source	FAC
ZTNA Tag	
Match ZTNA Tags	Any All
ZTNA Server	zserver
Destination	lab-ad-address
Schedule	always
Action	✓ ACCEPT ⊘ DENY

Security Profiles

AntiVirus	○
Web Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	no-inspection

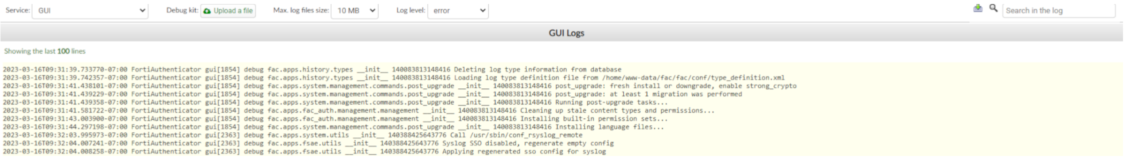
Logging Options

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

Debugging

Go to `https://<FortiAuthenticator-IP-Address>/debug` and select *GUI* from the *Service* dropdown to see extended FortiAuthenticator debug logs.

You can change the *Log level* to increase or decrease the depth of details.



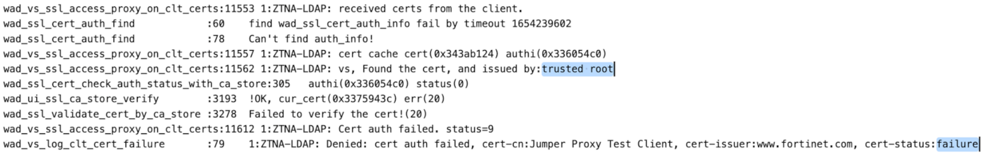
Service: GUI Debug kit: Upload a file Max. log files size: 10 MB Log level: error

Showing the last 100 lines

```
2023-03-16T09:31:39.733770-07:00 FortiAuthenticator gui[1854] debug fac.apps.history.types __init__ 140083813148416 Deleting log type information from database
2023-03-16T09:31:39.742357-07:00 FortiAuthenticator gui[1854] debug fac.apps.history.types __init__ 140083813148416 Loading log type definition file from /home/www-data/fac/fac/conf/type_definition.xml
2023-03-16T09:31:41.438101-07:00 FortiAuthenticator gui[1854] debug fac.apps.system.management.commands.post_upgrade __init__ 140083813148416 post_upgrade: fresh install or downgrade, enable strong_crypto
2023-03-16T09:31:41.439229-07:00 FortiAuthenticator gui[1854] debug fac.apps.system.management.commands.post_upgrade __init__ 140083813148416 post_upgrade: at least 1 migration was performed
2023-03-16T09:31:41.439358-07:00 FortiAuthenticator gui[1854] debug fac.apps.system.management.commands.post_upgrade __init__ 140083813148416 Running post-upgrade tasks...
2023-03-16T09:31:41.581722-07:00 FortiAuthenticator gui[1854] debug fac.apps.fac_auth.management.management __init__ 140083813148416 Cleaning up stale content types and permissions...
2023-03-16T09:31:43.003900-07:00 FortiAuthenticator gui[1854] debug fac.apps.fac_auth.management.management __init__ 140083813148416 Installing built-in permission sets...
2023-03-16T09:31:44.297198-07:00 FortiAuthenticator gui[1854] debug fac.apps.system.management.commands.post_upgrade __init__ 140083813148416 Installing language files...
2023-03-16T09:32:03.995973-07:00 FortiAuthenticator gui[2363] debug fac.apps.system.utils __init__ 140388425643776 Call /usr/sbin/conf_rsyslog_remote
2023-03-16T09:32:04.007241-07:00 FortiAuthenticator gui[2363] debug fac.apps.fsae.utils __init__ 140388425643776 Syslog SSO disabled, regenerate empty config
2023-03-16T09:32:04.008258-07:00 FortiAuthenticator gui[2363] debug fac.apps.fsae.utils __init__ 140388425643776 Applying regenerated sso config for syslog
```

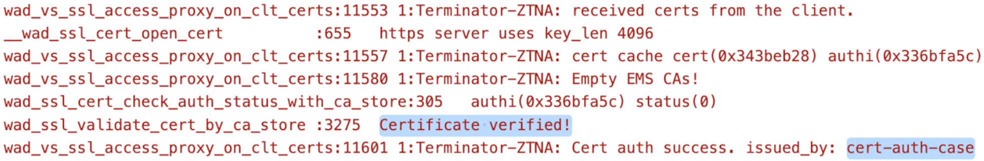
To access WAD debug categories and set them to the maximum level in a FortiGate ZTNA server, use `diagnose wad debug enable all` CLI command.

- cert-status: failure



```
wad_vs_ssl_access_proxy_on_clt_certs:11553 1:ZTNA-LDAP: received certs from the client.
wad_ssl_cert_auth_find            :60    find wad_ssl_cert_auth_info fail by timeout 1654239602
wad_ssl_cert_auth_find            :78    Can't find auth_info!
wad_vs_ssl_access_proxy_on_clt_certs:11557 1:ZTNA-LDAP: cert cache cert(0x343ab124) authi(0x336054c0)
wad_vs_ssl_access_proxy_on_clt_certs:11562 1:ZTNA-LDAP: vs, Found the cert, and issued by:trusted root
wad_ssl_cert_check_auth_status_with_ca_store:305   authi(0x336054c0) status(0)
wad_ui_ssl_ca_store_verify        :3193  !OK, cur_cert(0x3375943c) err(20)
wad_ssl_validate_cert_by_ca_store :3278  Failed to verify the cert!(20)
wad_vs_ssl_access_proxy_on_clt_certs:11612 1:ZTNA-LDAP: Cert auth failed. status=9
wad_vs_log_clt_cert_failure       :79    1:ZTNA-LDAP: Denied: cert auth failed, cert-cn:Jumper Proxy Test Client, cert-issuer:www.fortinet.com, cert-status:failure
```

- cert-status: success



```
wad_vs_ssl_access_proxy_on_clt_certs:11553 1:Terminator-ZTNA: received certs from the client.
__wad_ssl_cert_open_cert          :655   https server uses key_len 4096
wad_vs_ssl_access_proxy_on_clt_certs:11557 1:Terminator-ZTNA: cert cache cert(0x343beb28) authi(0x336bfa5c)
wad_vs_ssl_access_proxy_on_clt_certs:11580 1:Terminator-ZTNA: Empty EMS CAs!
wad_ssl_cert_check_auth_status_with_ca_store:305   authi(0x336bfa5c) status(0)
wad_ssl_validate_cert_by_ca_store :3275  Certificate verified!
wad_vs_ssl_access_proxy_on_clt_certs:11601 1:Terminator-ZTNA: Cert auth success. issued_by: cert-auth-case
```

www.fortinet.com