Examples

FortiAuthenticator 8.0.0

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

March 5, 2026
FortiAuthenticator 8.0.0 Examples
23-800-1084124-20260305

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-02	Initial release.
2025-10-21	Added FortiAuthenticator and FortiGate SCEP automatic enrollment on page 32.
2025-10-29	Updated Configuring RADIUS EAP on FortiAuthenticator on page 335.
2025-11-12	Updated Configuring SAML IdP settings on page 192 and Configuring IdP settings on page 198.
2025-11-18	Added Intune Certificate Provisioning with FortiAuthenticator CA on page 41.
2025-11-25	Updated Intune Certificate Provisioning with FortiAuthenticator CA on page 41.
2025-12-04	Added video for Intune Certificate Provisioning with FortiAuthenticator CA on page 41.
2025-12-09	Added SAML IdP custom multi-value attributes for FortiManager and FortiAnalyzer on page 394.
2026-01-19	Added Configuring RADSec between FortiAuthenticator and FortiSwitch on page 405.
2026-02-06	Added FortiAnalyzer- Event handlers for FortiAuthenticator on page 401.
2026-02-13	Updated FortiAuthenticator user self-registration on page 69 and Configuring a self-registration portal on page 70. Added Creating a portal policy on page 71.
2026-03-05	Added topology diagram for Configuring RADSec between FortiAuthenticator and FortiSwitch on page 405.

FortiAuthenticator standalone IAM

This chapter contains FortiAuthenticator related examples.

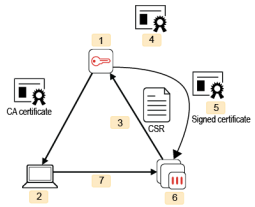
Certificate management

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

For this example, 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.



1. Create CA certificate on FortiAuthenticator.
2. Download the CA certificate to browser.
3. Create CSR on the FortiGate device.
4. Import and sign CSR on FortiAuthenticator.
5. Download the signed certificate.
6. Import the signed certificate and apply to admin GUI access.
7. The management connection is now trusted.

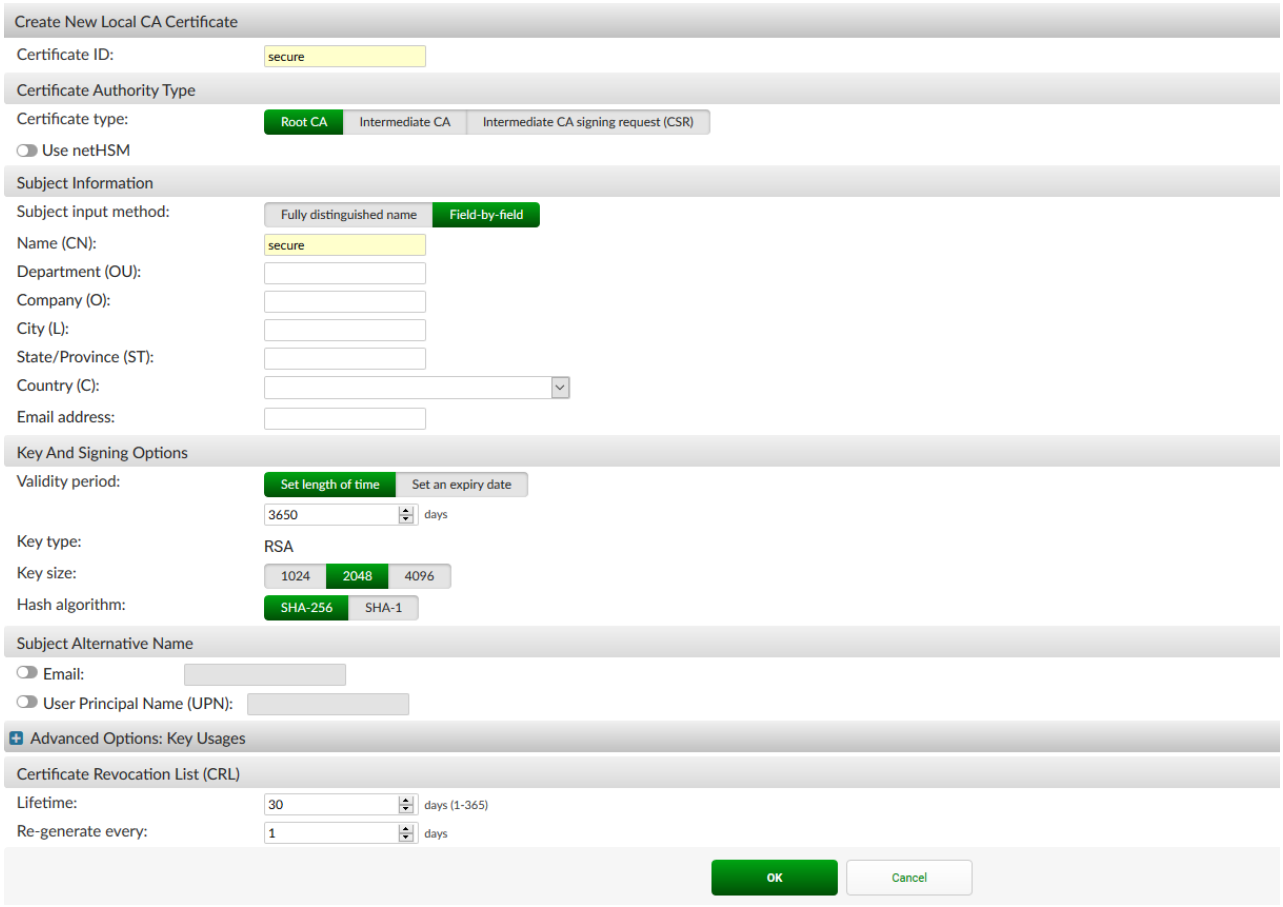
This scenario includes creating a certificate request on the FortiGate, downloading the certificate to the network's computers, and then importing it to the FortiAuthenticator. You will sign the certificate with the FortiAuthenticator's own certificate, then download and import the signed certificate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

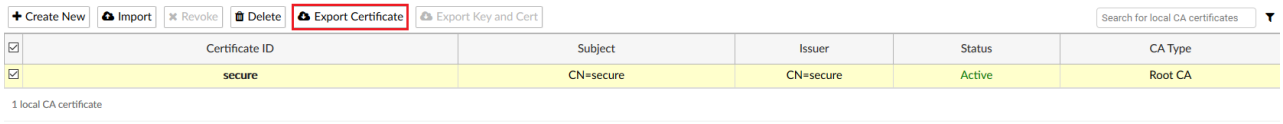
Creating a new CA on the FortiAuthenticator

To create a new CA:

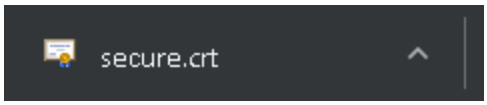
1. On the FortiAuthenticator, go to *Certificate Management > Certificate Authorities > Local CAs* and create a new CA. Enter a *Certificate ID*, select *Root CA certificate*, and configure the key options as shown in the example.



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



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

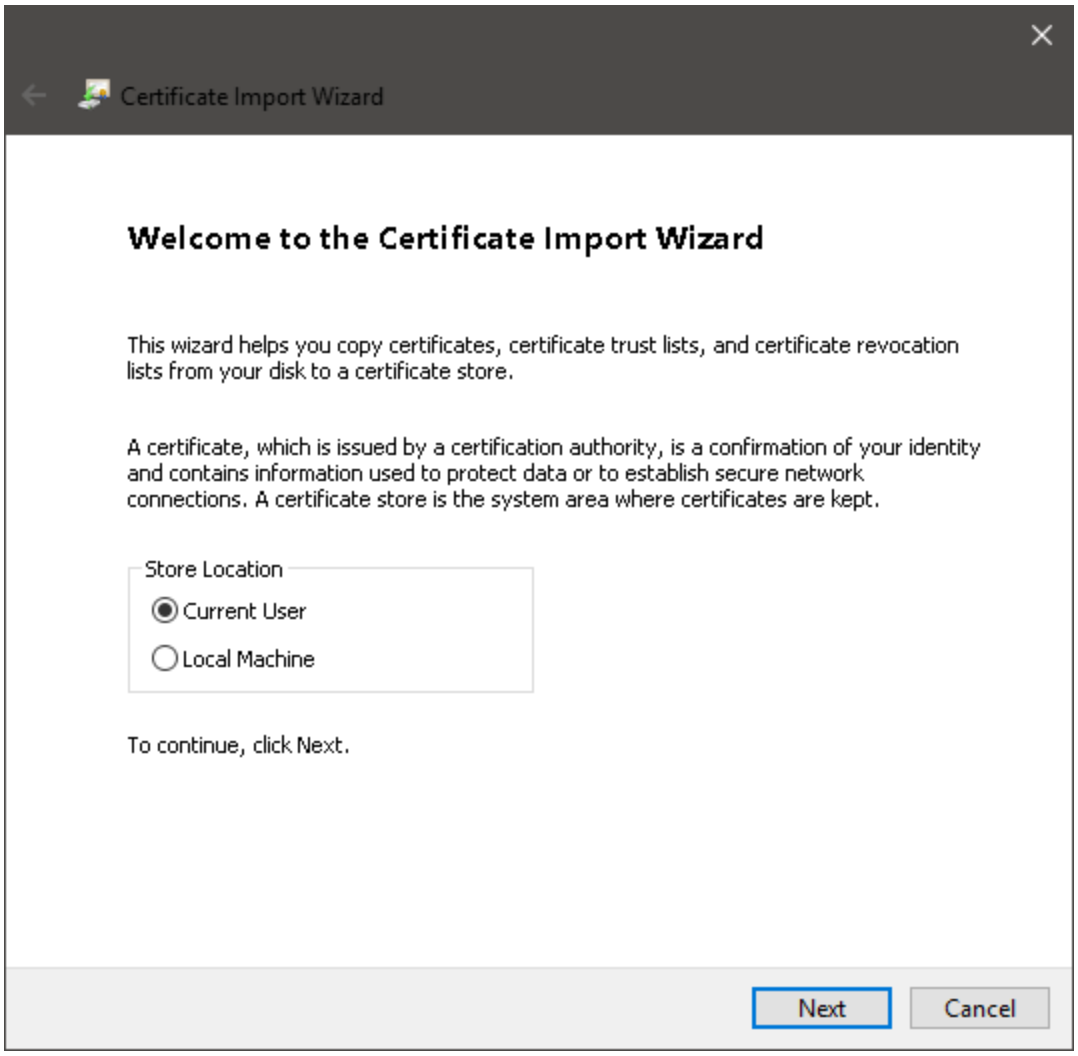


Installing the CA on the network

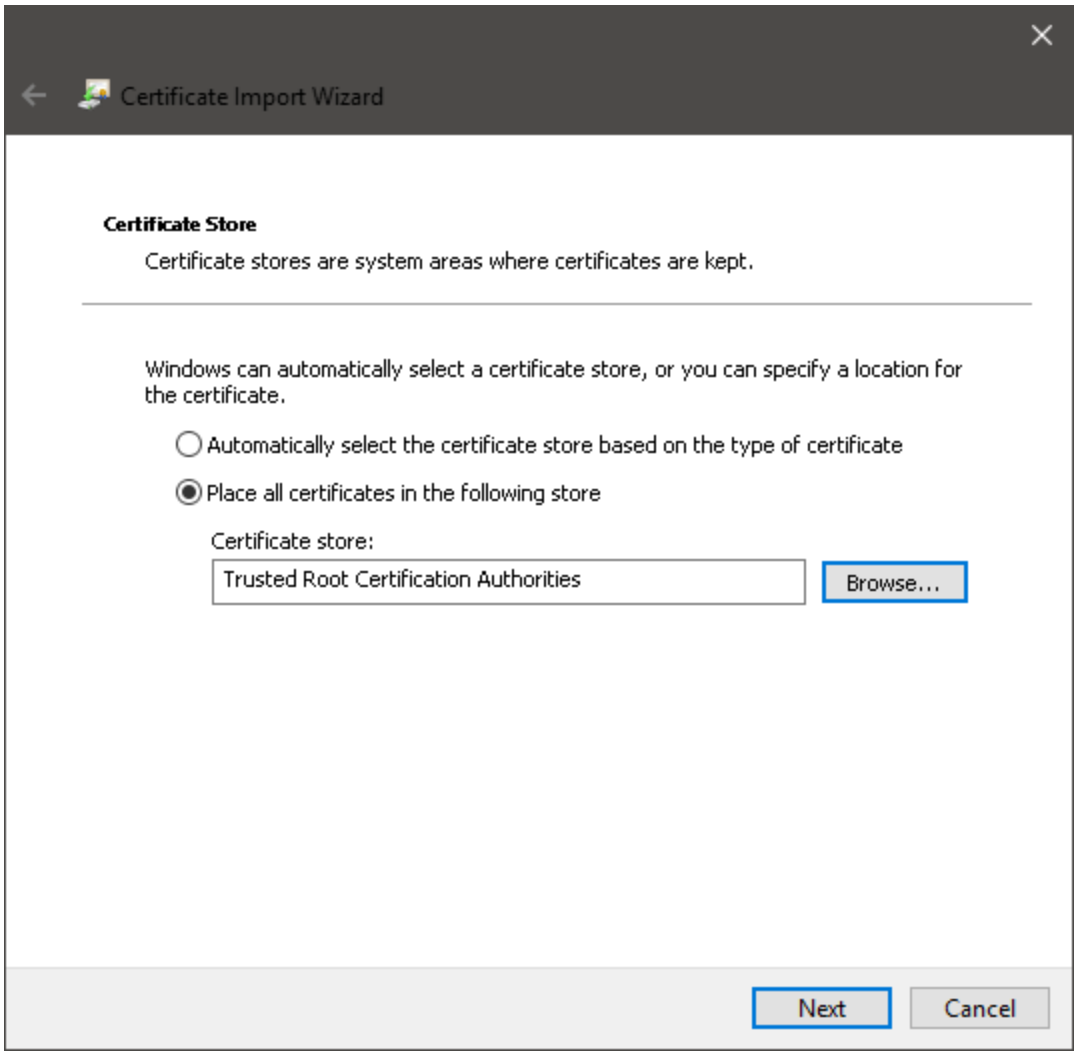
The certificate must now be installed on the computers in your network as a trusted root CA. The steps below show different methods of installing the certificate, depending on your browser.

Internet Explorer and Chrome

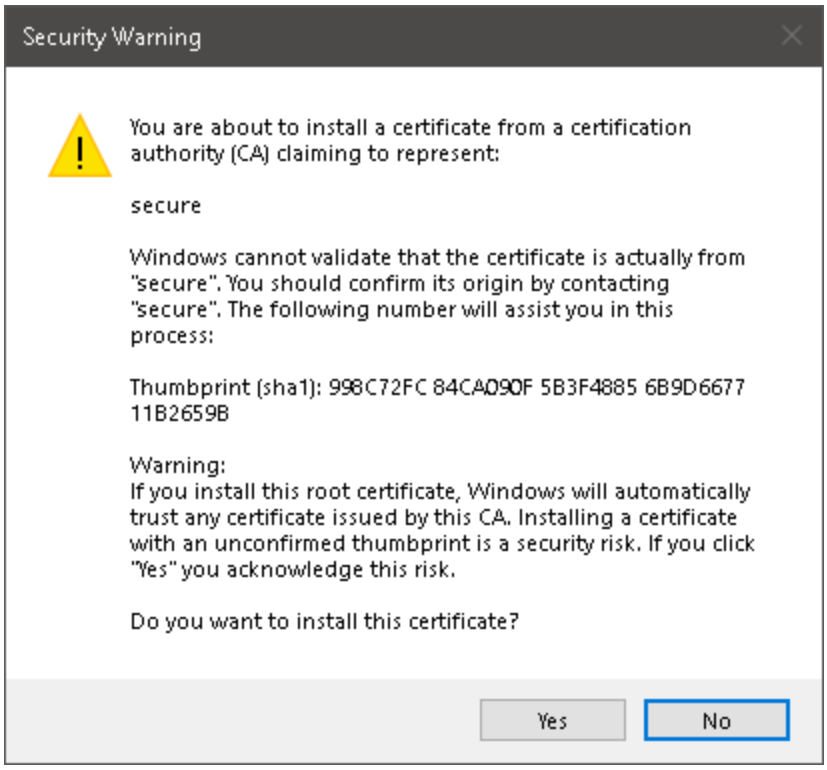
1. In Windows Explorer, right-click on the certificate and select *Install Certificate*. Open the certificate and follow the *Certificate Import Wizard*.



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

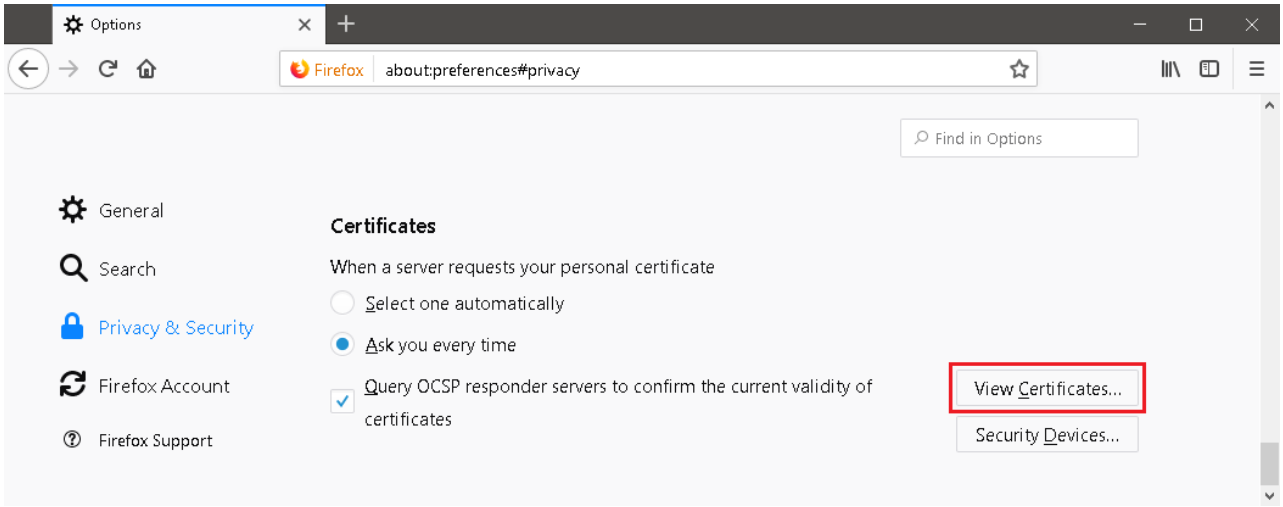


3. Finish the Wizard and select *Yes* to confirm and install the certificate.

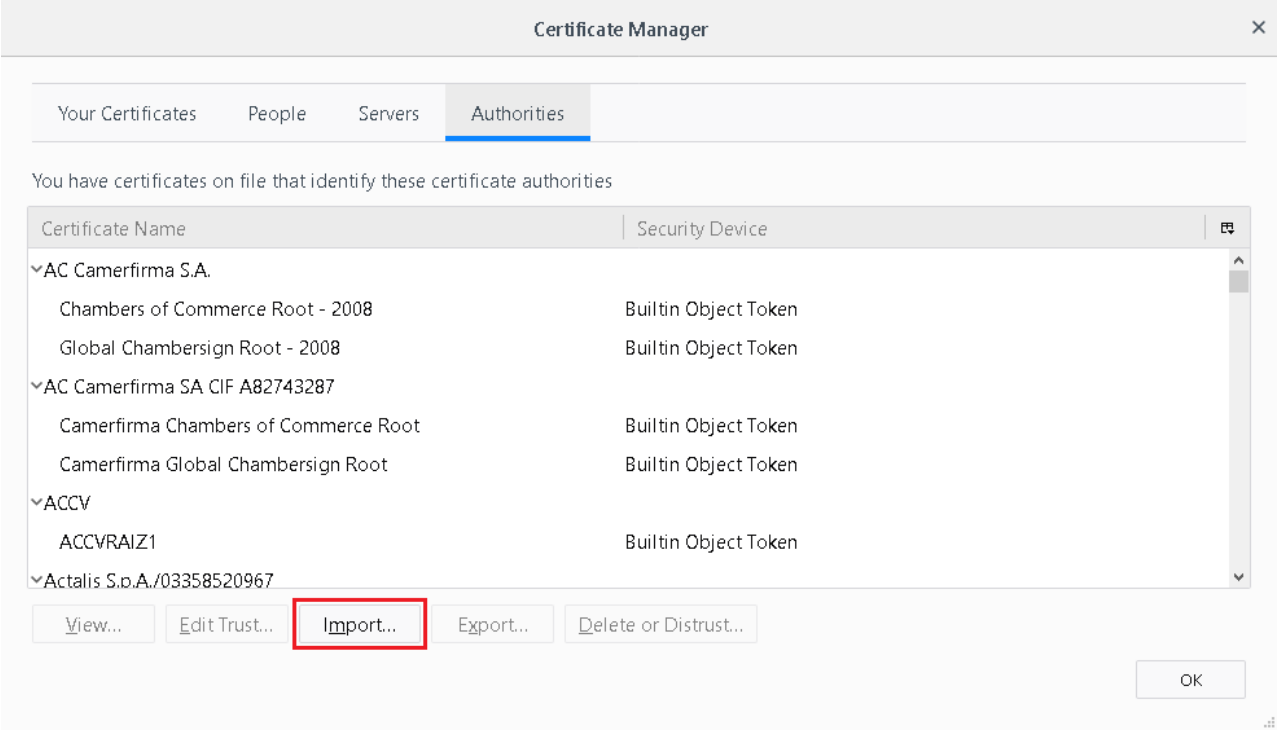


Firefox

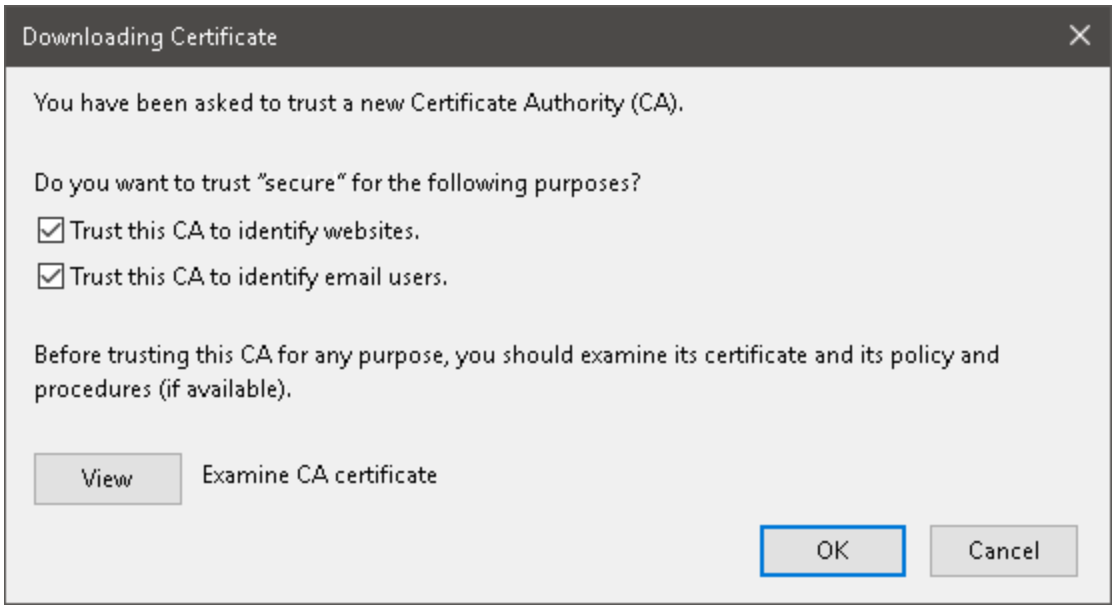
1. In the web browser, go to *Options* > *Privacy & Security* > *Certificates*, and select *View Certificates*.



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



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*.



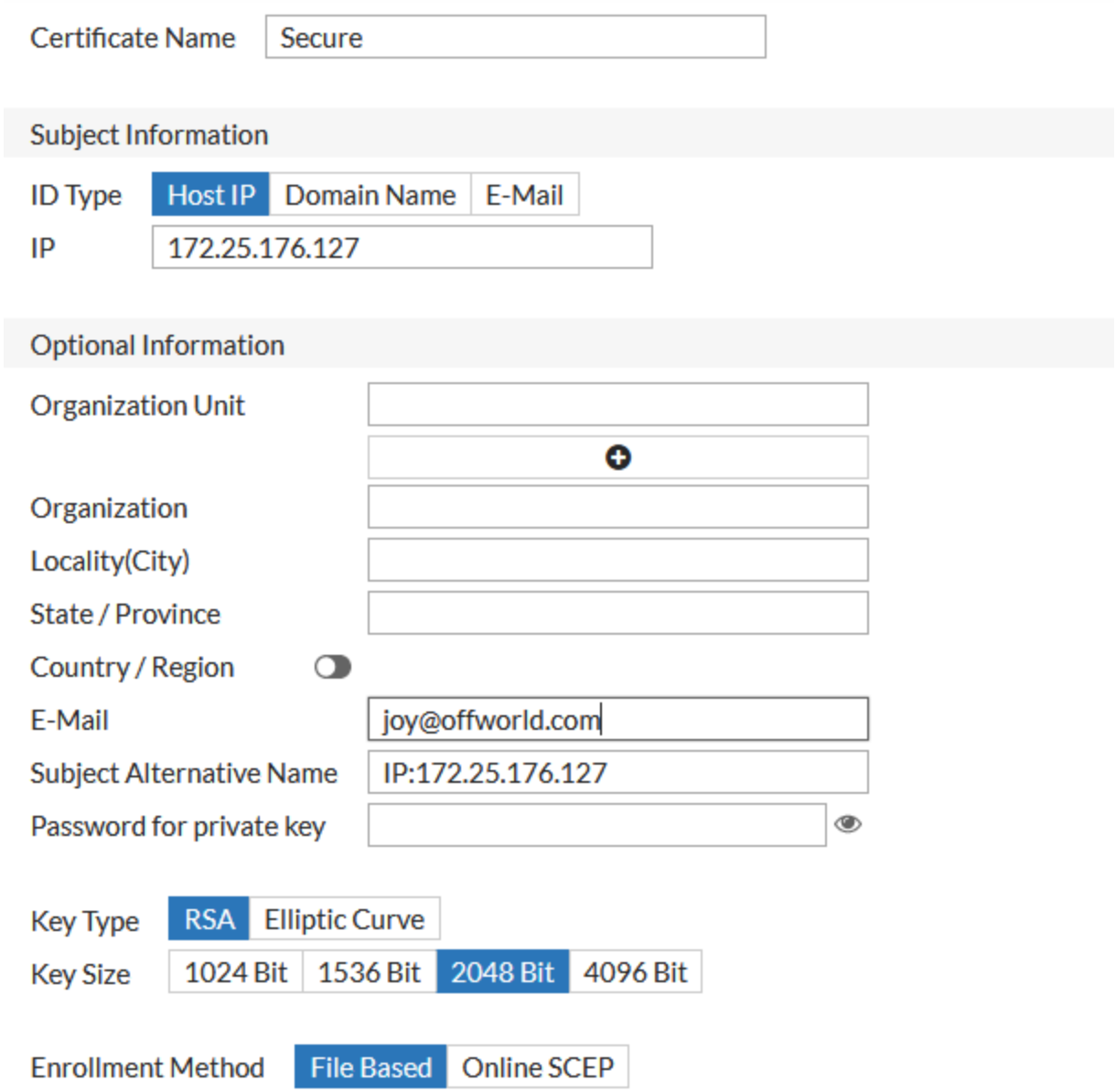
Creating a CSR on the FortiGate

To create a CSR:

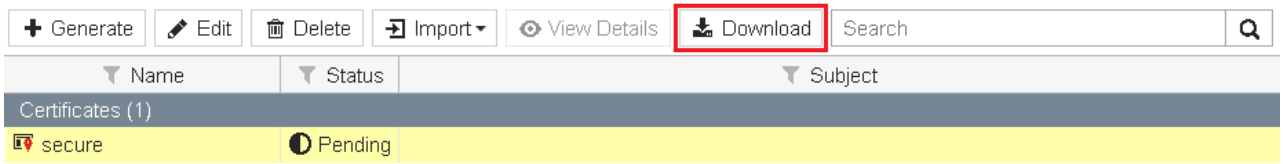
1. On the FortiGate, go to *System > Certificates* and select *Generate* to create a new certificate signing request (CSR).

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.

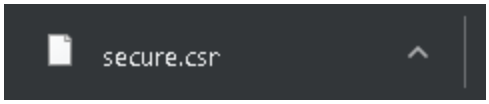
The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



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



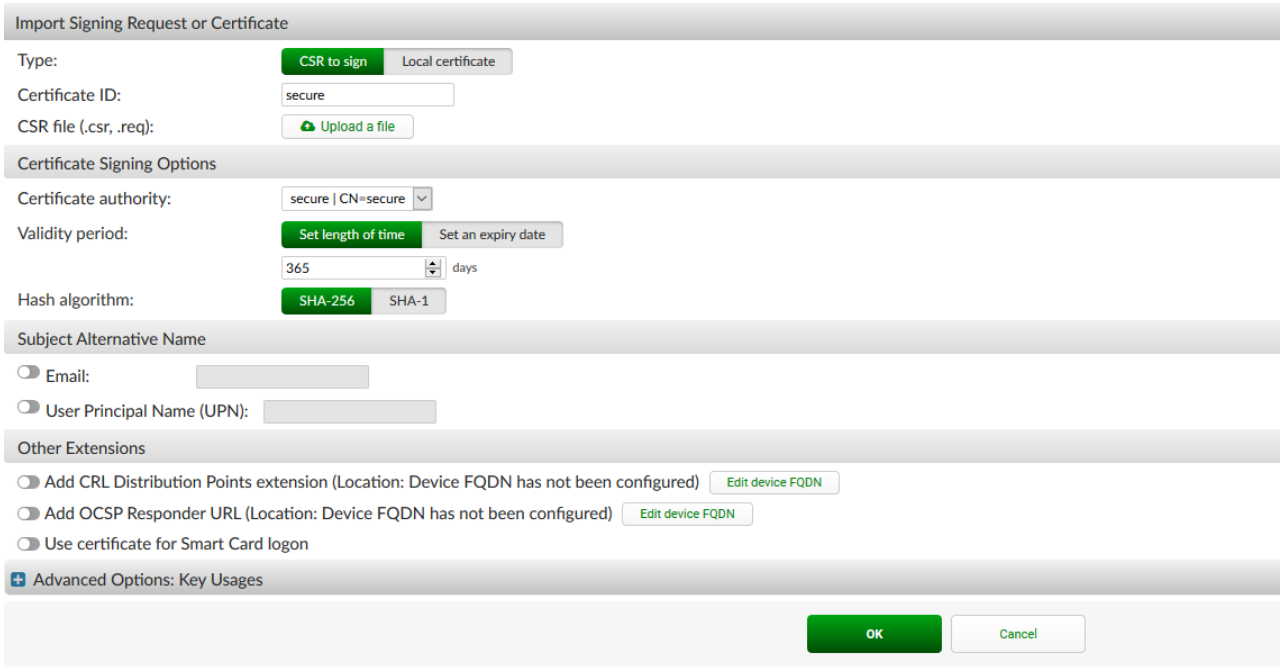
This will save a **.csr** file to your local drive.



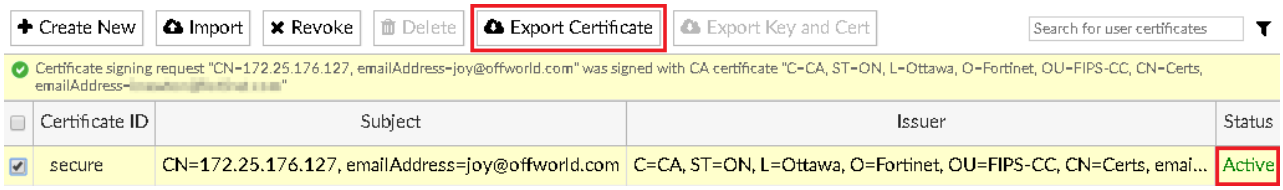
Importing and signing the CSR on the FortiAuthenticator

To import and sign the CSR:

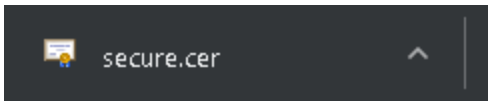
1. Back on the FortiAuthenticator, go to *Certificate Management > End Entities > Users* and import the *.csr* certificate created earlier.
   Make sure to select the *Certificate authority* from the dropdown menu, and set the *Hash algorithm* to *SHA-256*, as configured earlier.



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*.



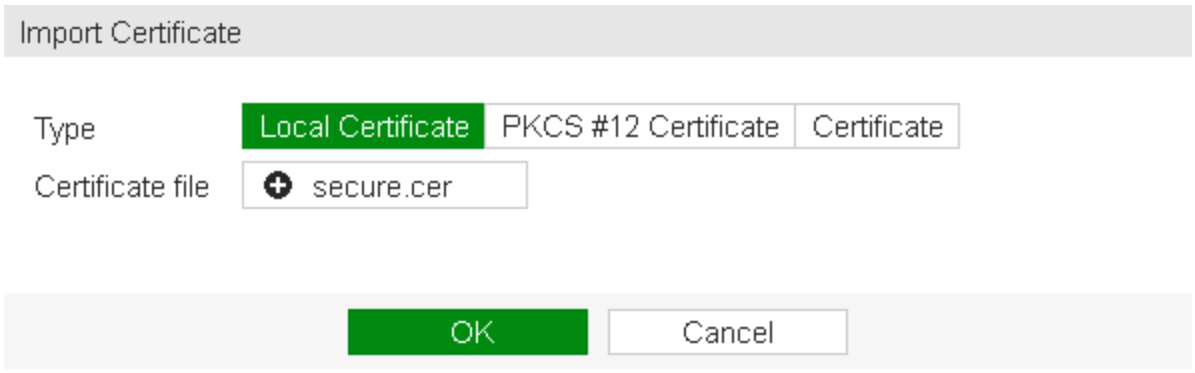
This will save a **.cer** file to your local drive.



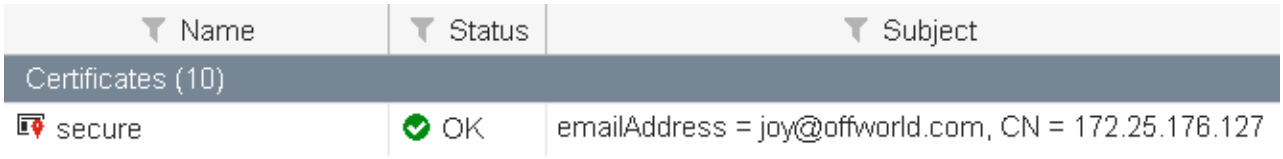
Importing the local certificate to the FortiGate

To import the local certificate:

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



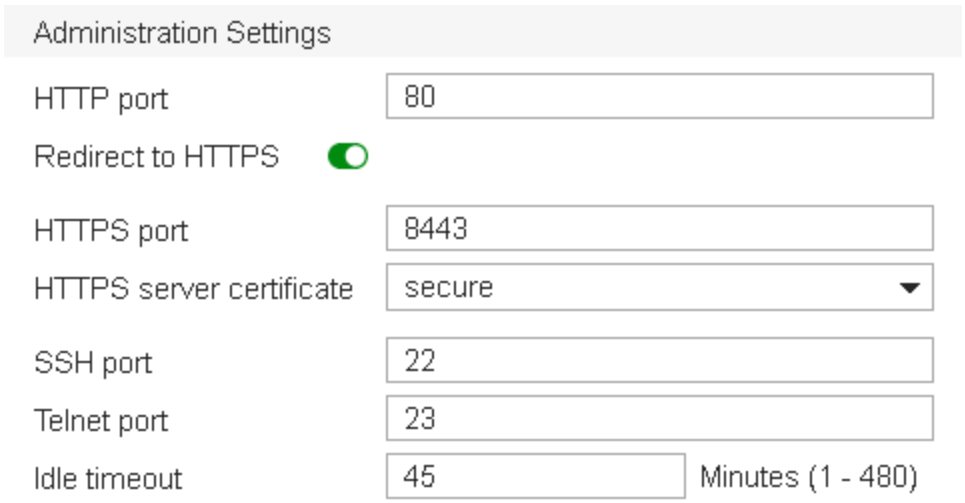
You should now see that the certificate's *Status* has changed from *Pending* to *OK*. You may have to refresh your page to see the status change.



Configuring the certificate for the GUI

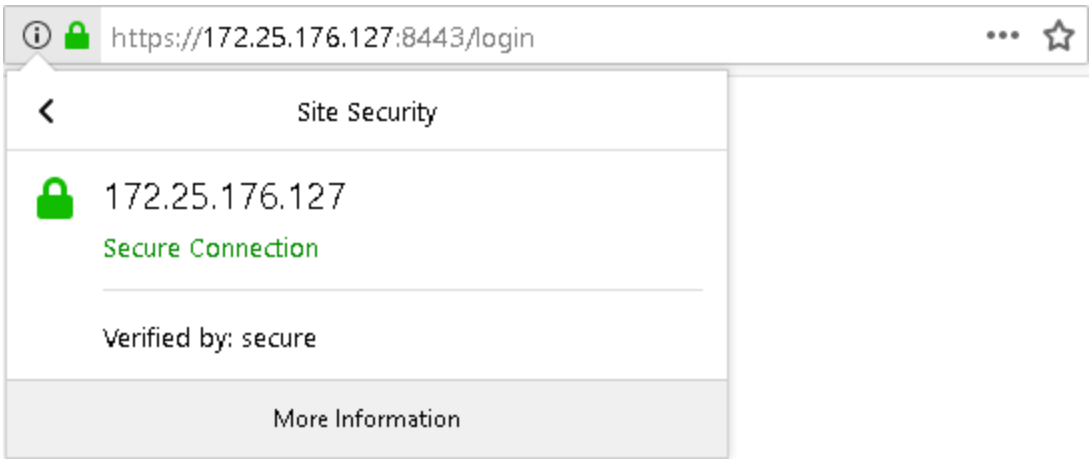
To configure the certificate:

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



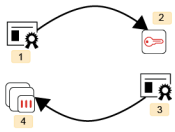
Results

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.



FortiAuthenticator certificate with SSL inspection

For this example, 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.



1. Create CSR on the FortiGate device.
2. Import and sign CSR on FortiAuthenticator.
3. Download the signed intermediate CA.
4. Import signed certificate and apply deep inspection of cloud applications.

Note that, for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this example 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.

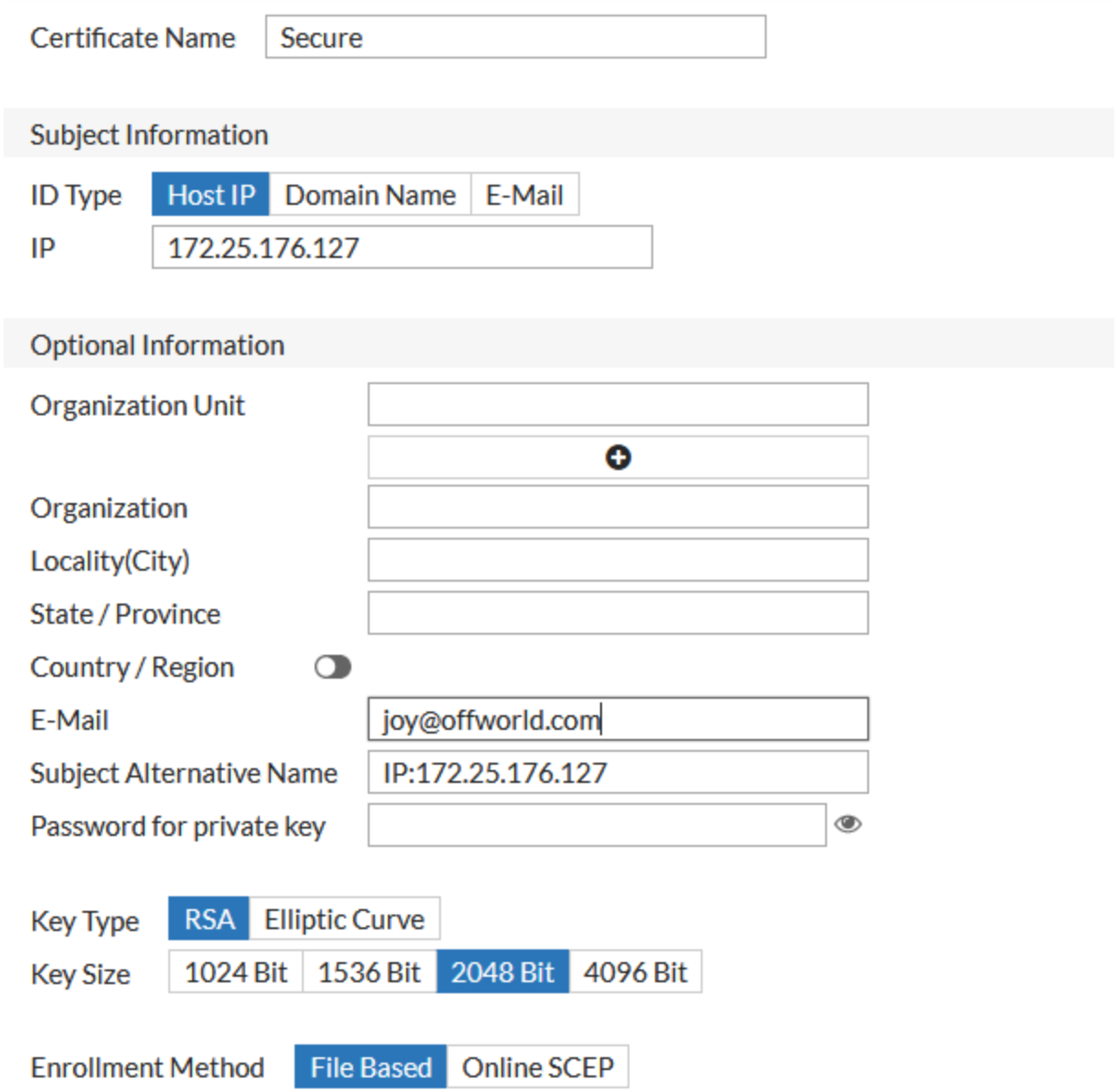
As an example, you will also have *Application Control* with *Deep Inspection of Cloud Applications* enabled. This will apply inspection to HTTPS traffic. Note that you may use another security profile instead of *Application Control*.

Creating a CSR on the FortiGate

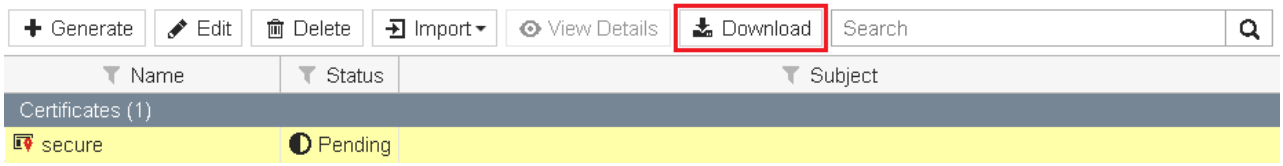
To create a CSR:

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.

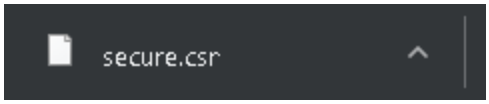
The *Subject Alternative Name* field must be configured with the internet facing IP address or FQDN in the following format: `IP:x.x.x.x` or `DNS:hostname.example.com`.



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



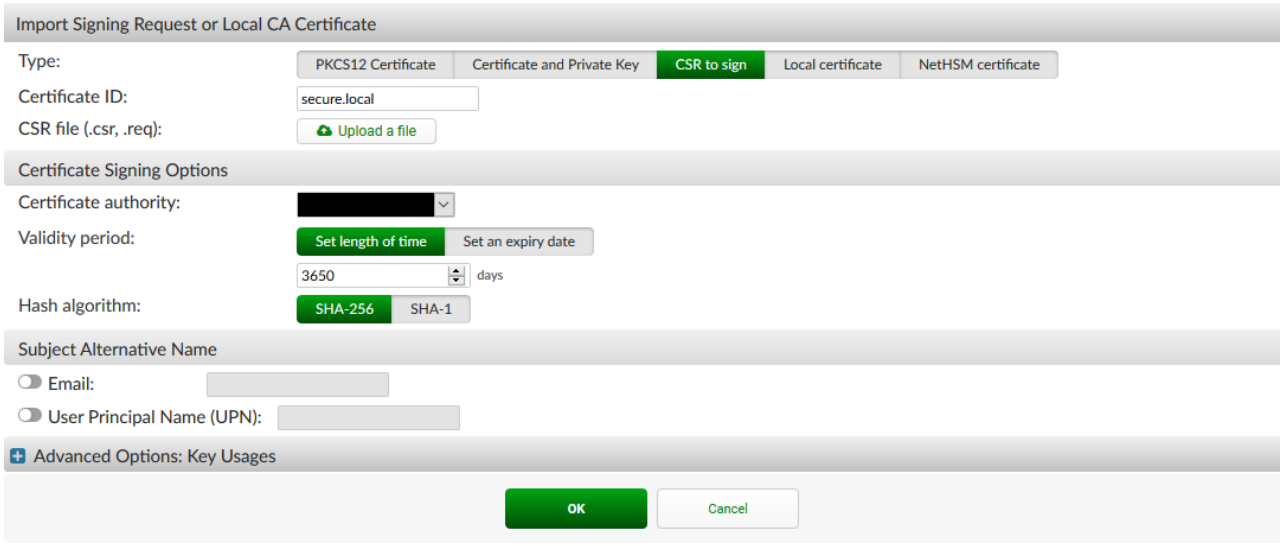
This will save a **.csr** file to your local drive.



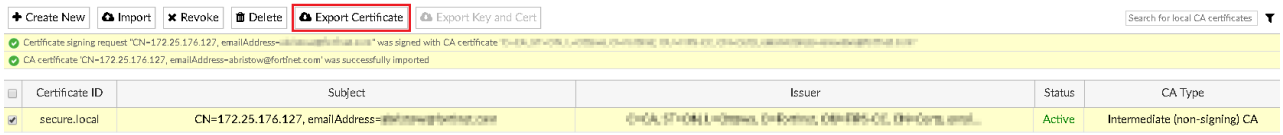
Creating an Intermediate CA on the FortiAuthenticator

To create an Intermediate CA:

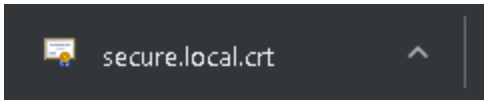
1. On the FortiAuthenticator, go to *Certificate Management > Certificate Authorities > Local CAs* and select *Import*. Set *Type* to *CSR to sign*, enter a *Certificate ID*, and import the CSR file. Make sure to select the *Certificate authority* from the dropdown menu, and set the *Hash algorithm*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



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*.



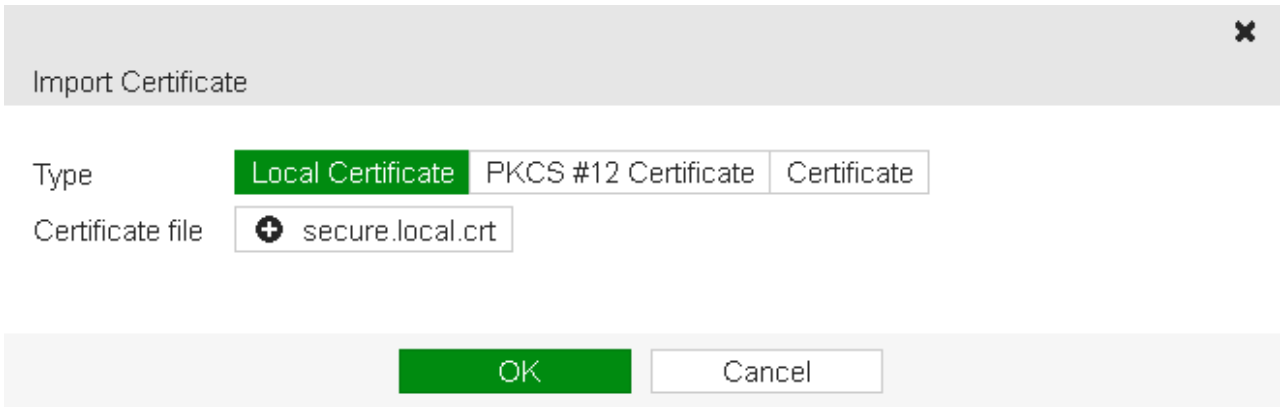
This will save a *.crt* file to your local drive.



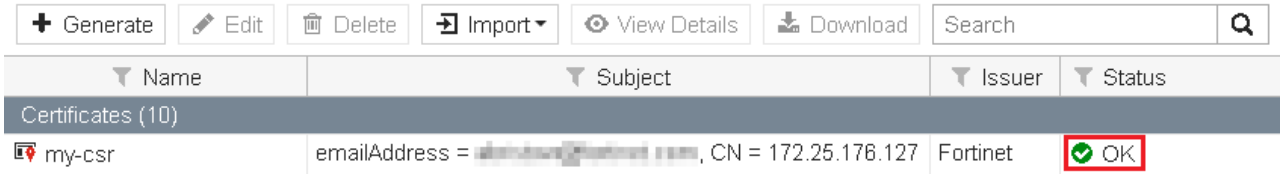
Importing the signed certificate on the FortiGate

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*.



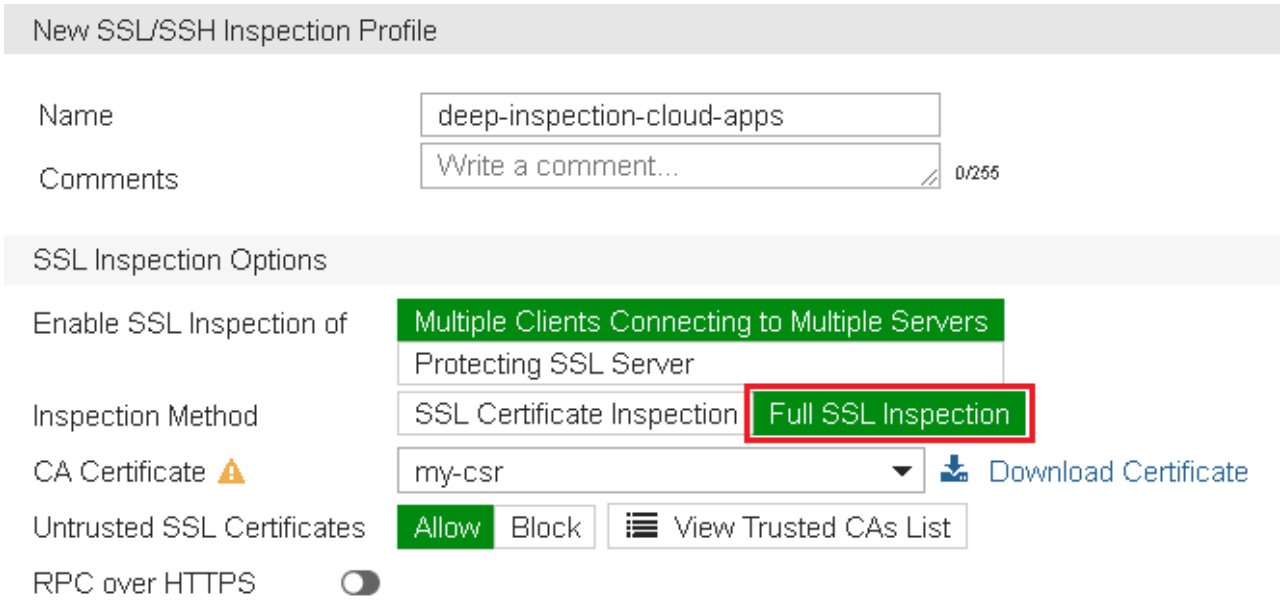
2. You should now see that the certificate has a *Status* of *OK*.



Configuring full SSL inspection

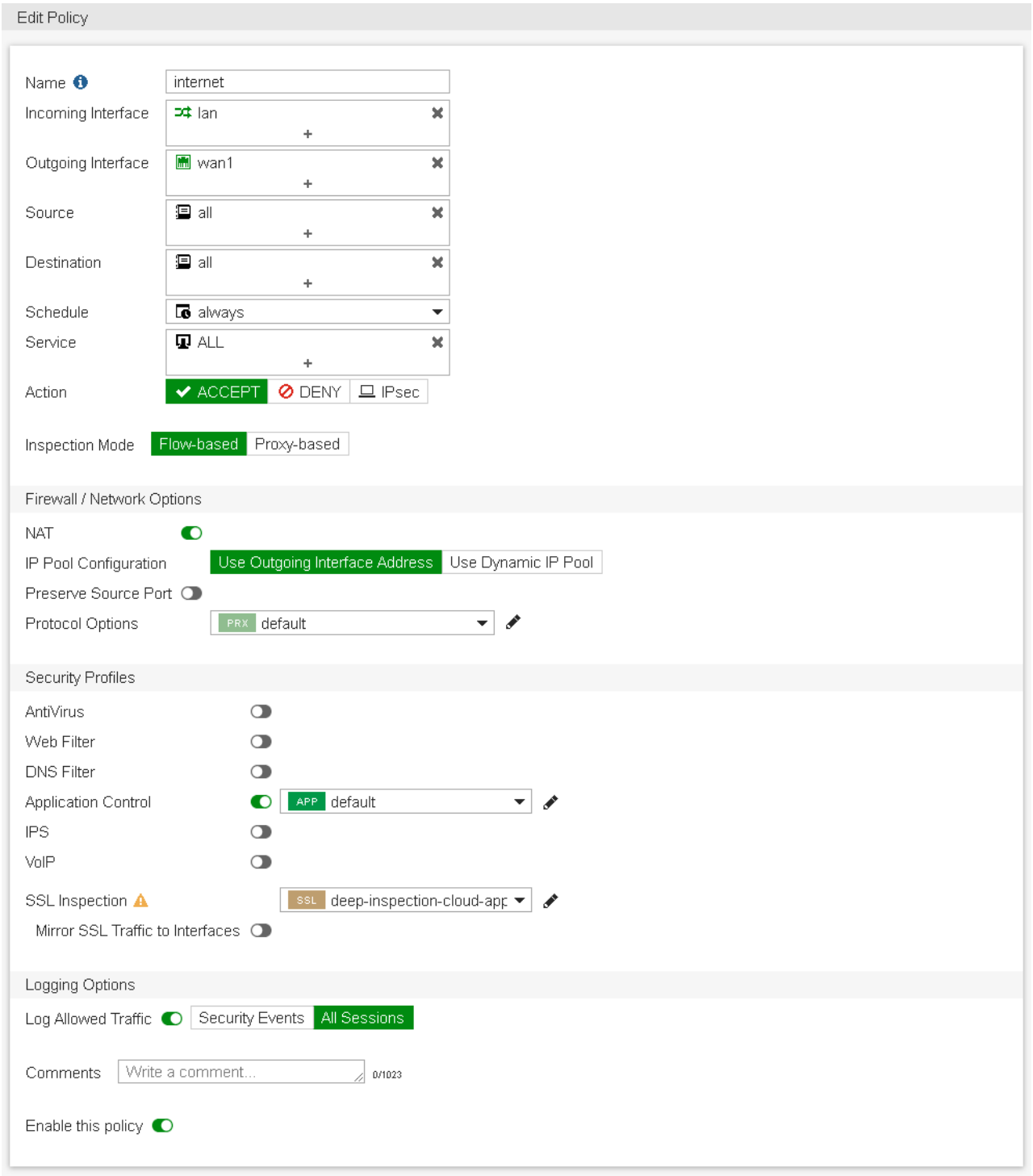
To configure full SSL inspection:

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*.



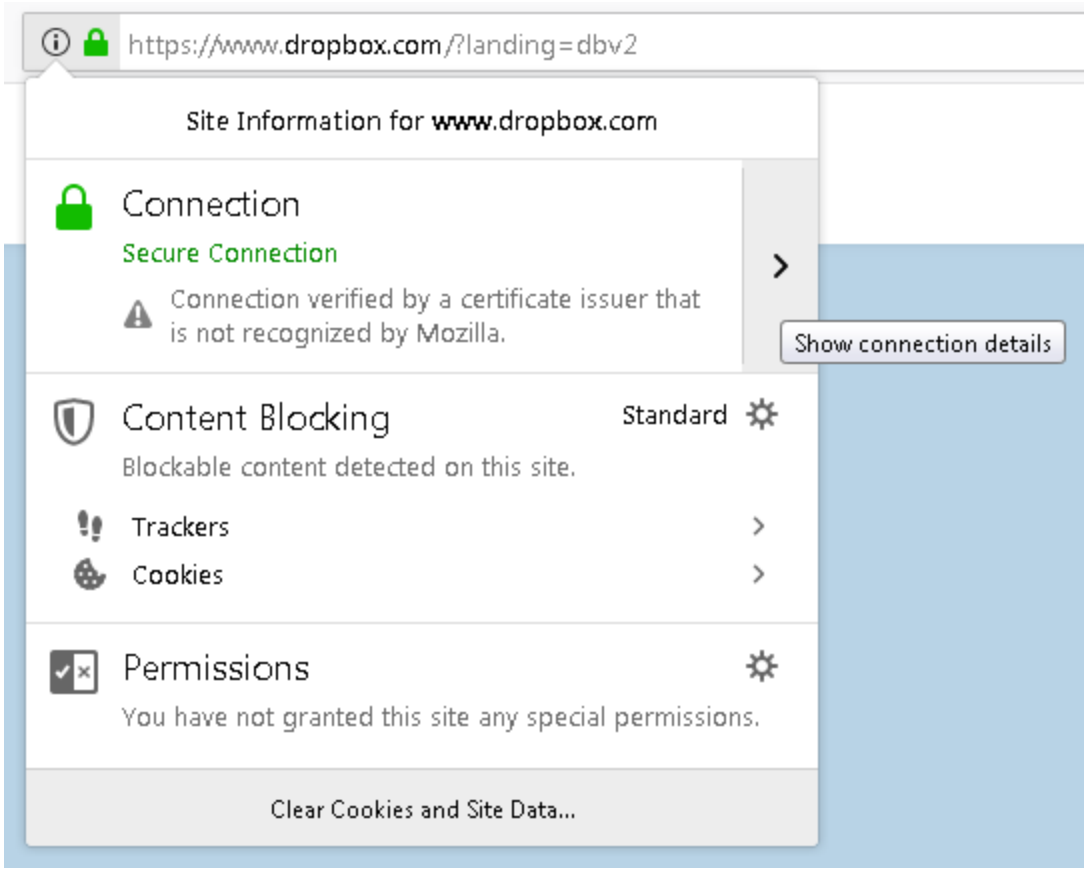
2. Add the certificate to your web browser's list of trusted certificates. End users will likely see certificate warnings unless the certificate is installed in their browser.

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*.

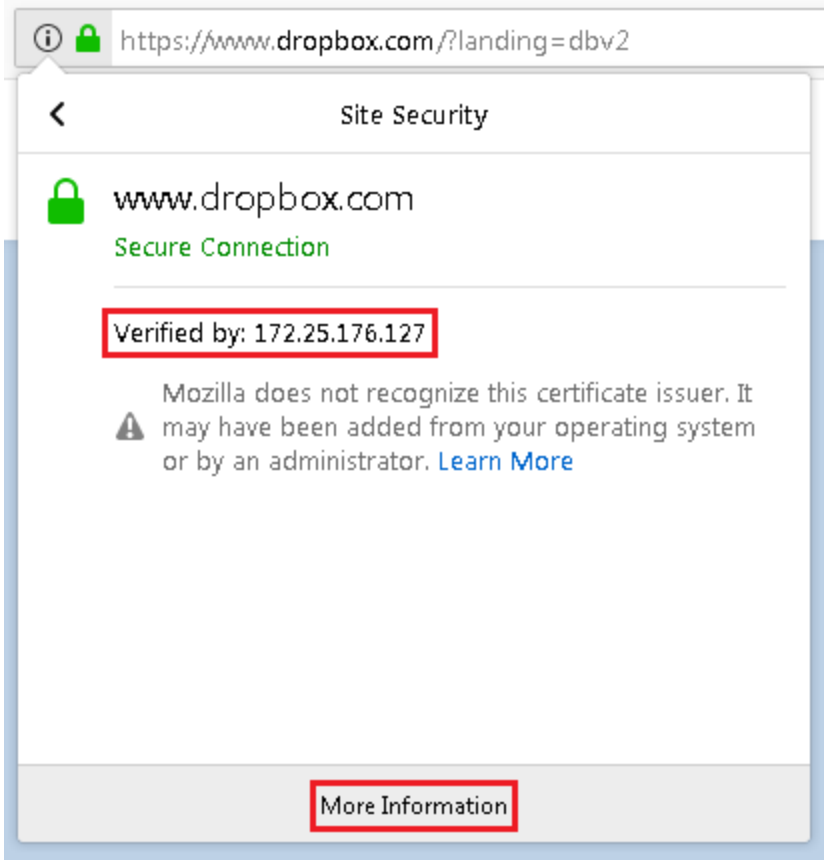


Results

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*.

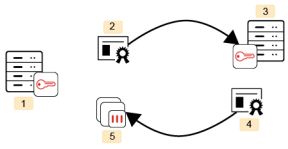


2. You should now see that the certificate from the FortiGate (`172.25.176.127`) has signed and verified access to the site. As a result, no certificate errors will appear.
   Optionally select *More Information*.



FortiAuthenticator certificate with SSL inspection using an HSM

For this example, 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.



1. Configure FortiAuthenticator with NetHSM.
2. Create CSR on the FortiGate device.
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.

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

1. Configuring the NetHSM profile on FortiAuthenticator on page 24
2. Creating a local CA certificate using an HSM server on page 25
3. Creating a CSR on the FortiGate on page 26
4. Creating an Intermediate CA on the FortiAuthenticator on page 27
5. Importing the signed certificate on the FortiGate on page 28
6. Configuring full SSL inspection on page 28
7. Results on page 31

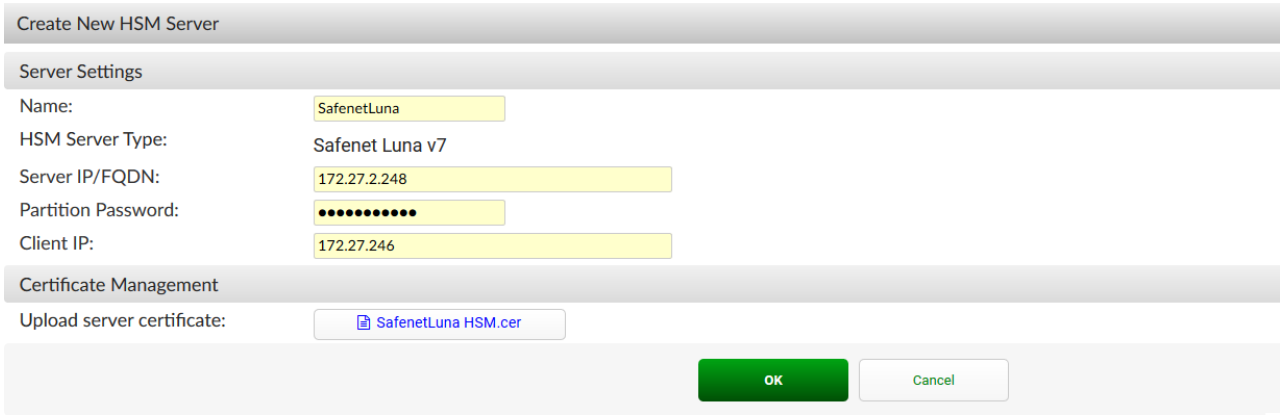
In order for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this example will not be trusted. For more information on how to do this, see Creating a local CA certificate using an HSM server on page 25 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:



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

3. Click *OK* to complete the setup.

To authorize FortiAuthenticator as a Safenet Luna HSM client:

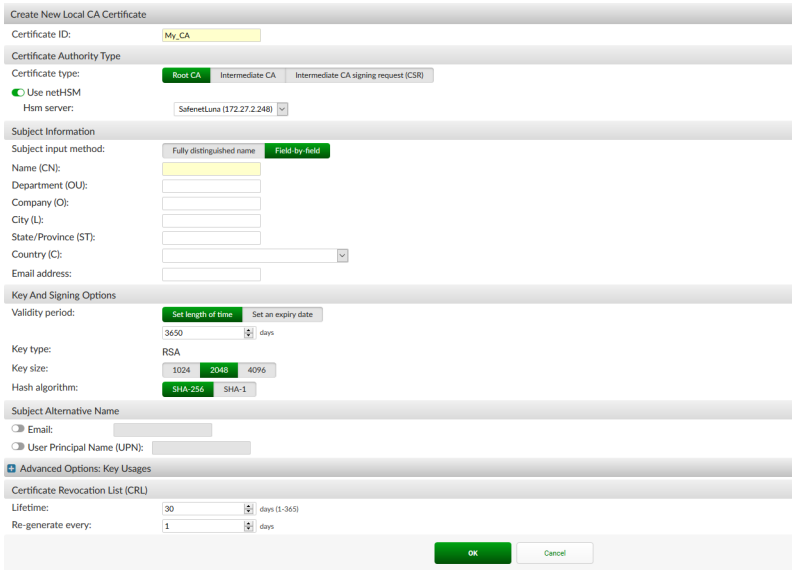
1. Make sure the FortiAuthenticator client certificate uses the `<FAC IP>.pem` naming convention. For example: `172.16.68.47.pem`
2. Upload the FortiAuthenticator client certificate to Safenet Luna HSM using SCP transfer.
   ```
   scp [certificate filename] admin@[HSM address]:
   ```
3. Use SSH to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

Creating a local CA certificate using an HSM server

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

To create a new local CA certificate using HSM:

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

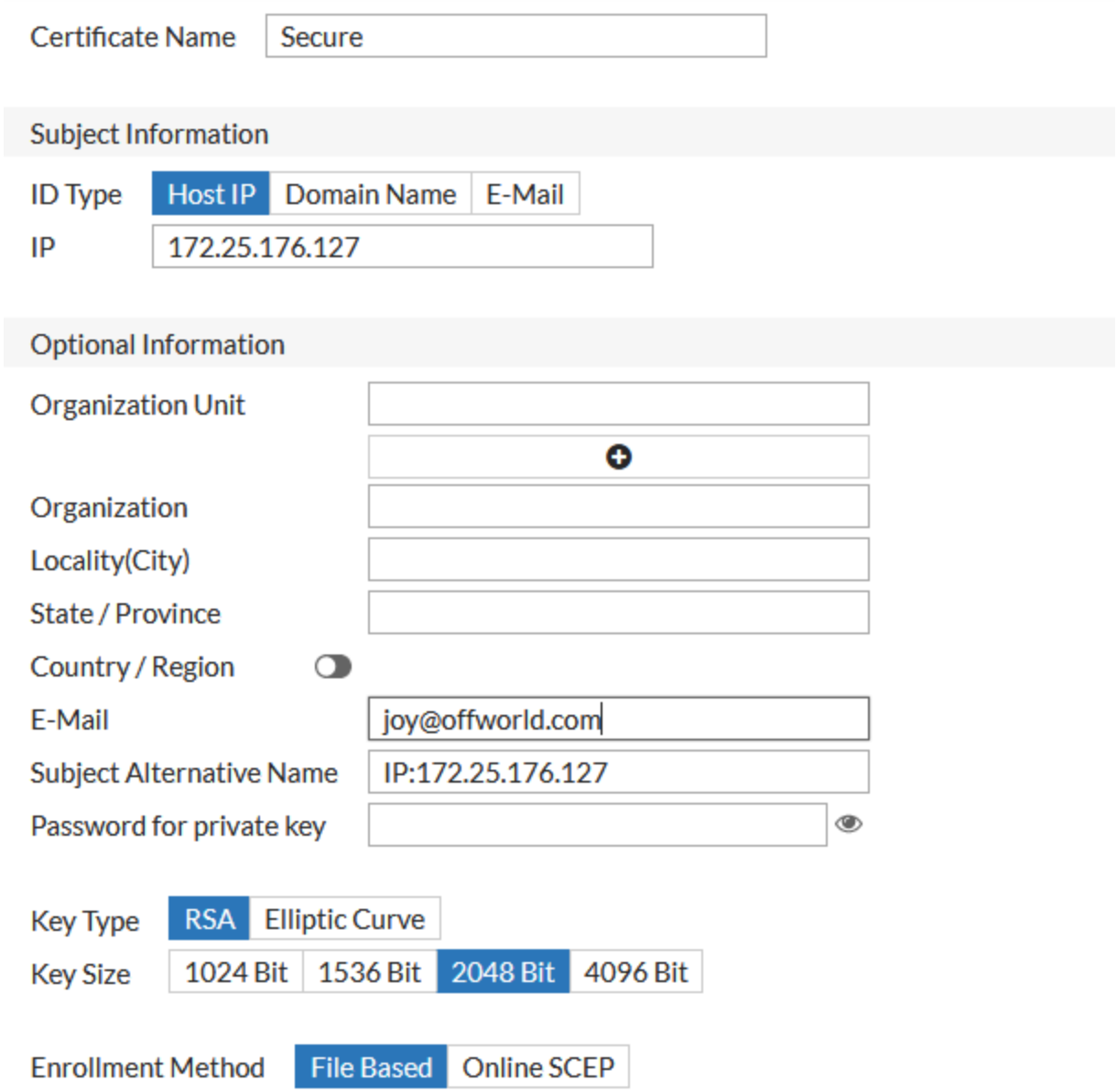


2. Enter a name for the CA certificate, for example *My_CA*.
3. Select *Root CA* as the *Certificate type*.
4. Enable *Use NetHSM*, and choose an HSM server from the dropdown menu.
5. Configure the remaining settings as desired, and click *OK* to save your changes.
   Once your CA certificate has been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

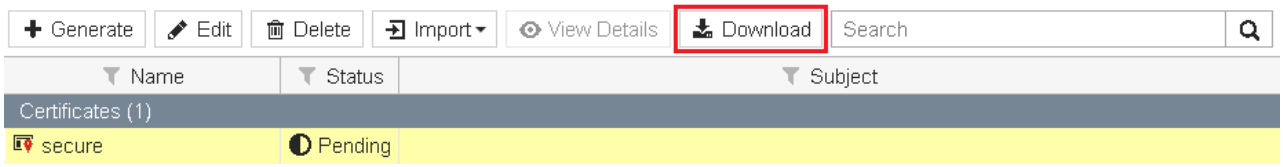
Creating a CSR on the FortiGate

To create a CSR:

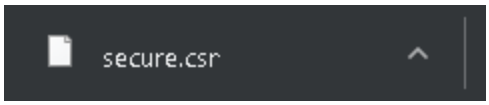
1. On the FortiGate, go to *System* > *Certificates* and select *Generate* to create a new certificate signing request (CSR).
   Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.
   The *Subject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



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



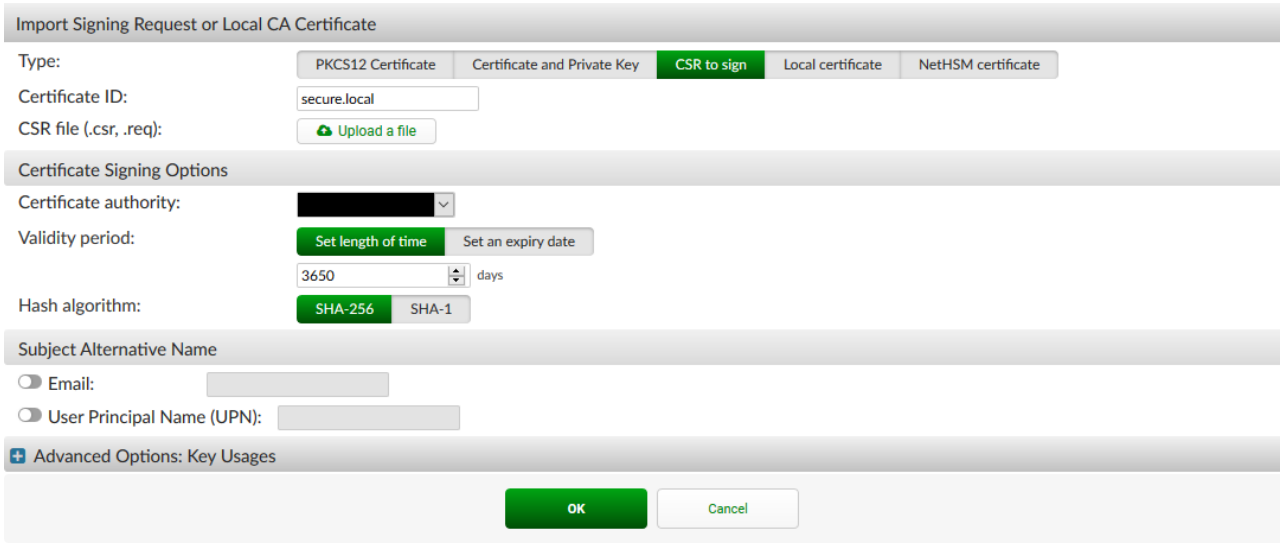
This will save a **.csr** file to your local drive.



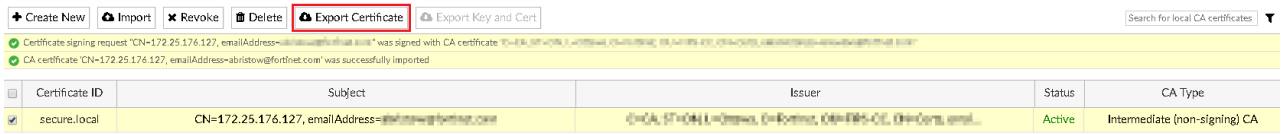
Creating an Intermediate CA on the FortiAuthenticator

To create an Intermediate CA:

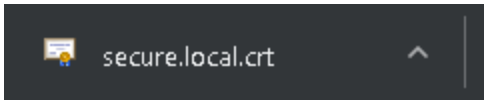
1. On the FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Import*. Set *Type* to *CSR to sign*, enter a *Certificate ID*, and import the CSR file.
2. Select the *Certificate authority* configured with the HSM from the dropdown menu, and set the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



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*.



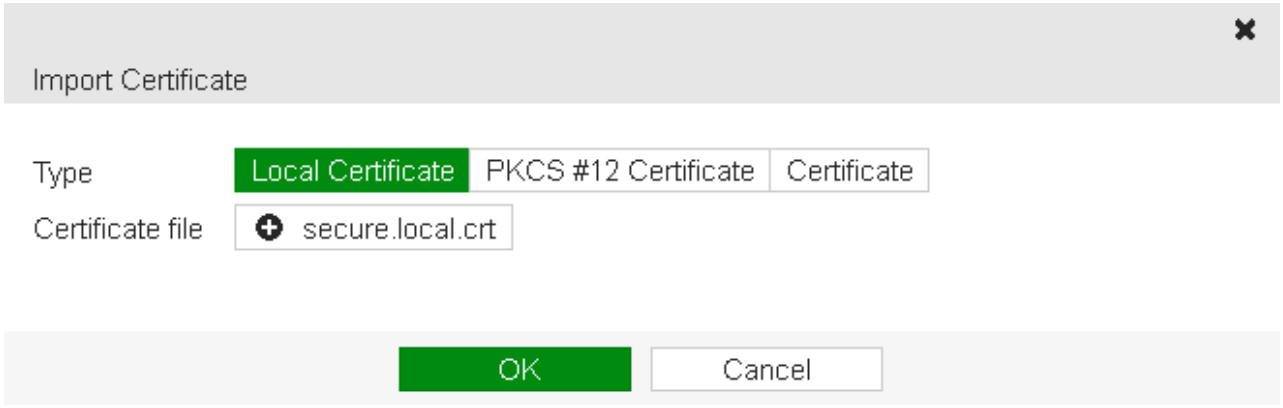
This will save a *.crt* file to your local drive.



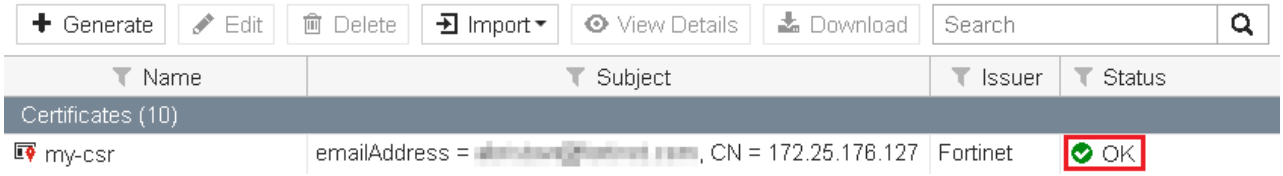
Importing the signed certificate on the FortiGate

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*.



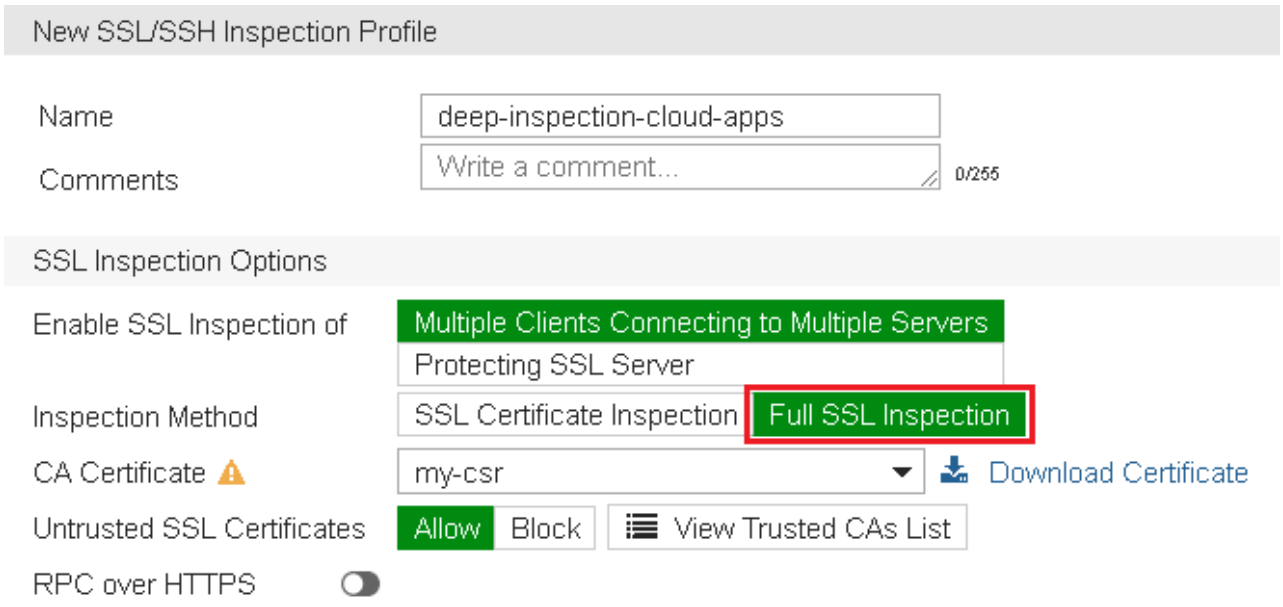
2. You should now see that the certificate has a *Status* of *OK*.



Configuring full SSL inspection

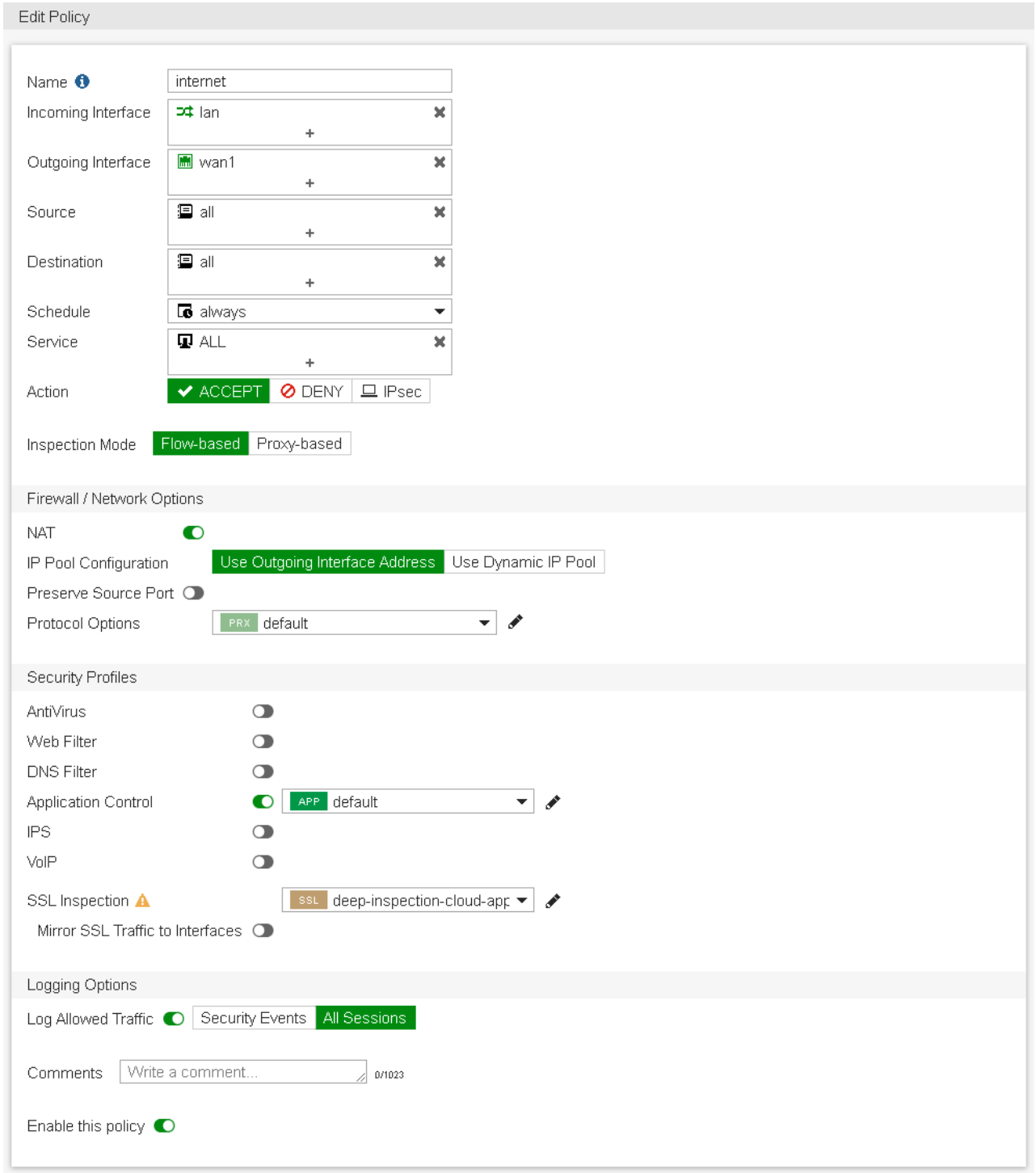
To configure full SSL inspection:

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*.



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.

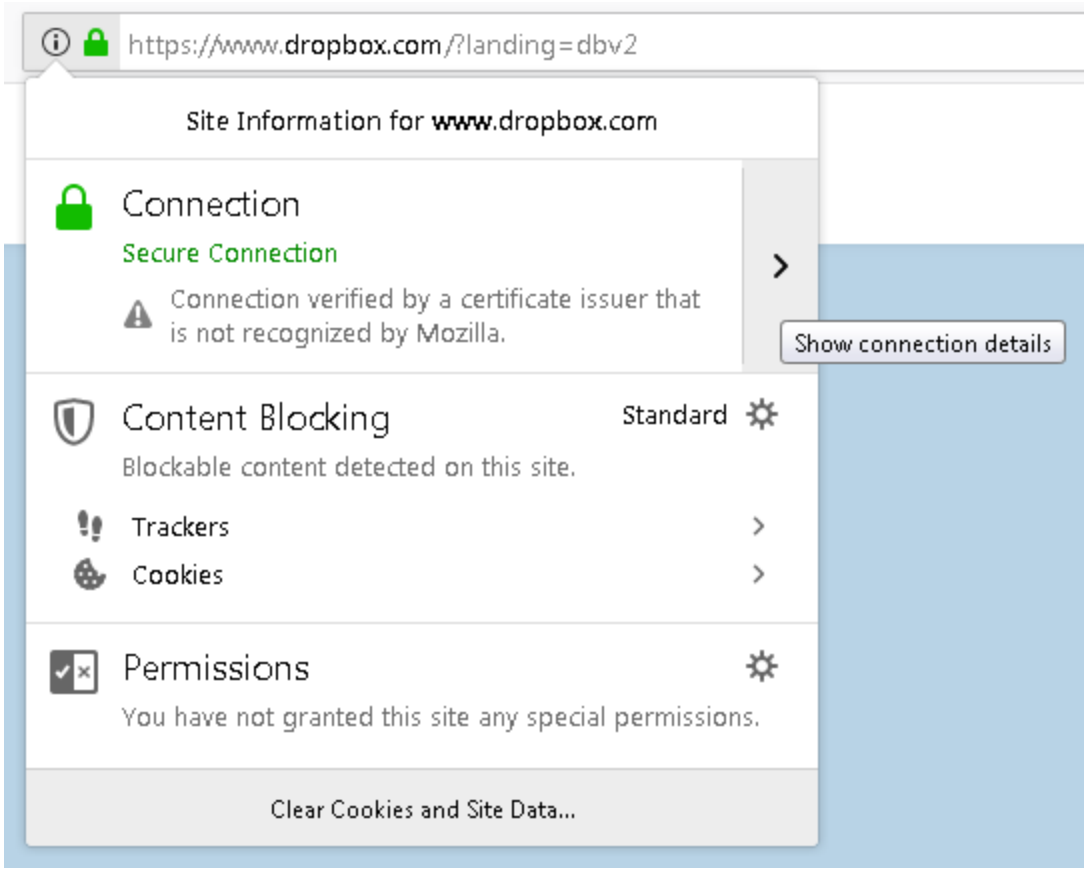
3. Next go to *Policy & Objects > IPv4 Policy* and edit the policy that allows Internet access.



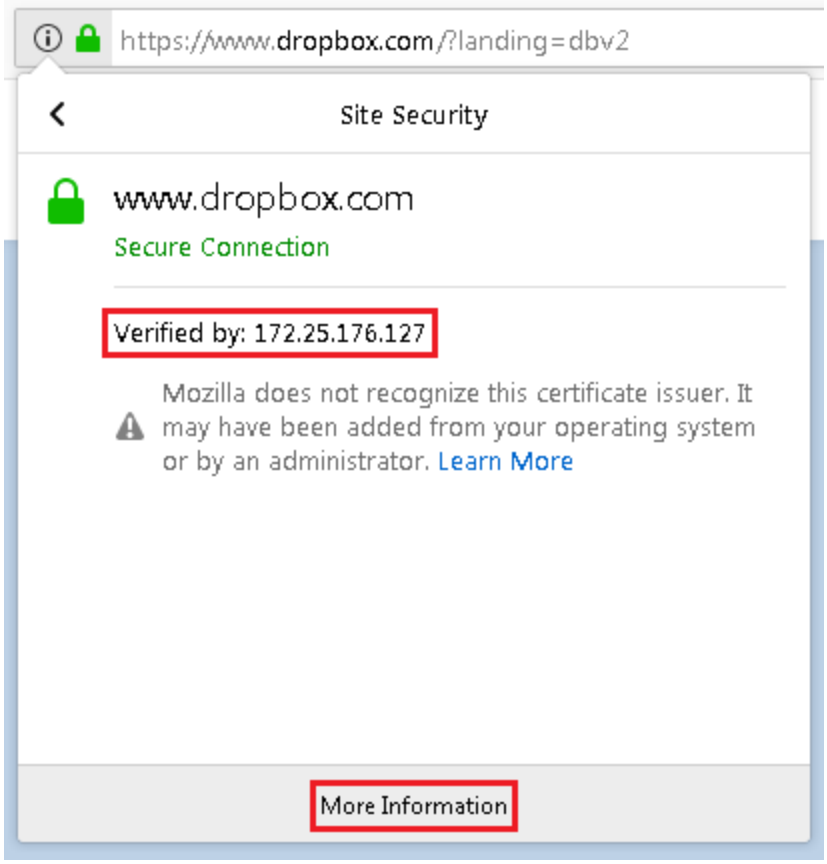
4. Under *Security Profiles*, enable *SSL/SSH Inspection* and select the custom profile created earlier.
5. Enable *Application Control* and set it to *default*.

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*.



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*.



FortiAuthenticator and FortiGate SCEP automatic enrollment

In this example, you will enable SCEP (Simple Certificate Enrollment Protocol) on FortiAuthenticator (acting as a private CA) and use it to automatically issue a device certificate to a FortiGate.

Having a FortiAuthenticator signing certificate for FortiGate as a CA can be used in the following scenarios:

- Automatically renew/rotate for FortiGate VPN tunnels
- EAP-TLS for WiFi authentication
- Issue a certificate for FortiGate administration GUI

1. Configure FortiAuthenticator as a local CA and enable its SCEP service.
2. Expose the SCEP service on a FortiAuthenticator interface.
3. From FortiGate, pull the CA/CRL over the SCEP URL, submit a SCEP CSR, and auto receive the signed certificate.

Prerequisites

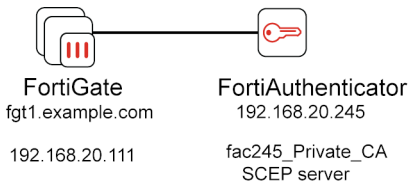
- FortiOS 7.4.2
- FortiAuthenticator 8.0.0

SCEP path:

```
/app/cert/scep/
```

- FortiAuthenticator is reachable from FortiGate (HTTPS to the SCEP URL).
- FortiAuthenticator operating as a local/private CA.
- Administrative access to both the devices.

Topology



- **FortiGate**: `fg1.example.com - 192.168.20.111`
- **FortiAuthenticator** (Private CA + SCEP): `fac245.example.com - 192.168.20.245`
- **SCEP URL**:

```
https://fac245.example.com/app/cert/scep/
```

FortiAuthenticator and FortiGate SCEP automatic enrollment

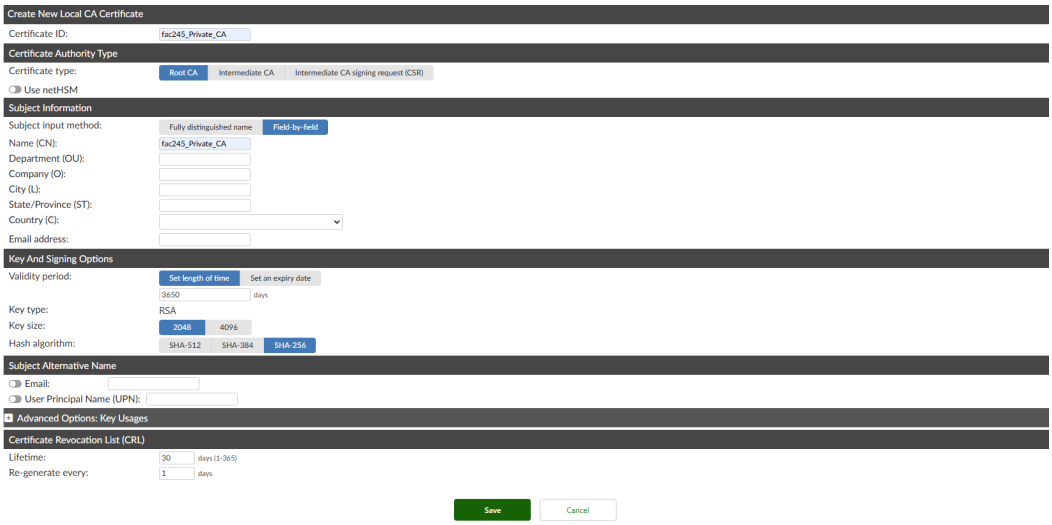
1. Configuring FortiAuthenticator as a private CA on page 33
2. Enable the SCEP service on FortiAuthenticator on page 34
3. FortiGate: Trust CA and CRL via SCEP on page 35
4. SCEP enrollment method: Automatic on page 37
5. FortiGate: Request and install a certificate via SCEP (automatic approval) on page 38
6. Results on page 40
7. Troubleshooting on page 40

Configuring FortiAuthenticator as a private CA

To configure FortiAuthenticator as a private CA:

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*, and select *Create*.
   The *Create New Local CA Certificate* window opens.
2. Enter a *Certificate ID*.
3. In *Certificate type*, select *Root CA* to create a local root CA to sign device certificates.
4. In *Subject input method*, ensure that *Field-by-field* is selected.
5. Enter a *Name (CN)*.

6. Click *Save*.



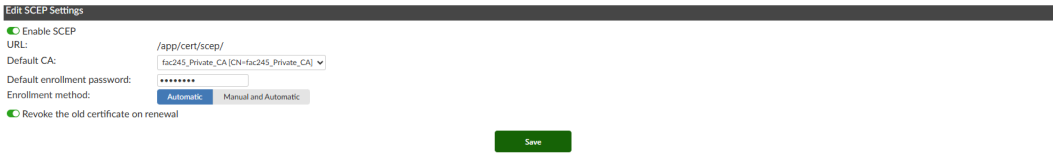
Enable the SCEP service on FortiAuthenticator

To enable the SCEP service on FortiAuthenticator:

1. Go to *Certificate Management > Certificate Authorities > SCEP > General*.
2. Select *Enable SCEP*.
   Note: The default SCEP URL path:

   ```
   /app/cert/scep/
   ```

3. Ensure that the *Default CA* is the CA configured in Configuring FortiAuthenticator as a private CA on page 33.
4. Enter the default enrollment password that is used when not setting a random password.
5. Ensure that the *Enrollment method* is *Automatic*.
6. Enable *Revoke the old certificate on renewal*.
7. Click *Save*.



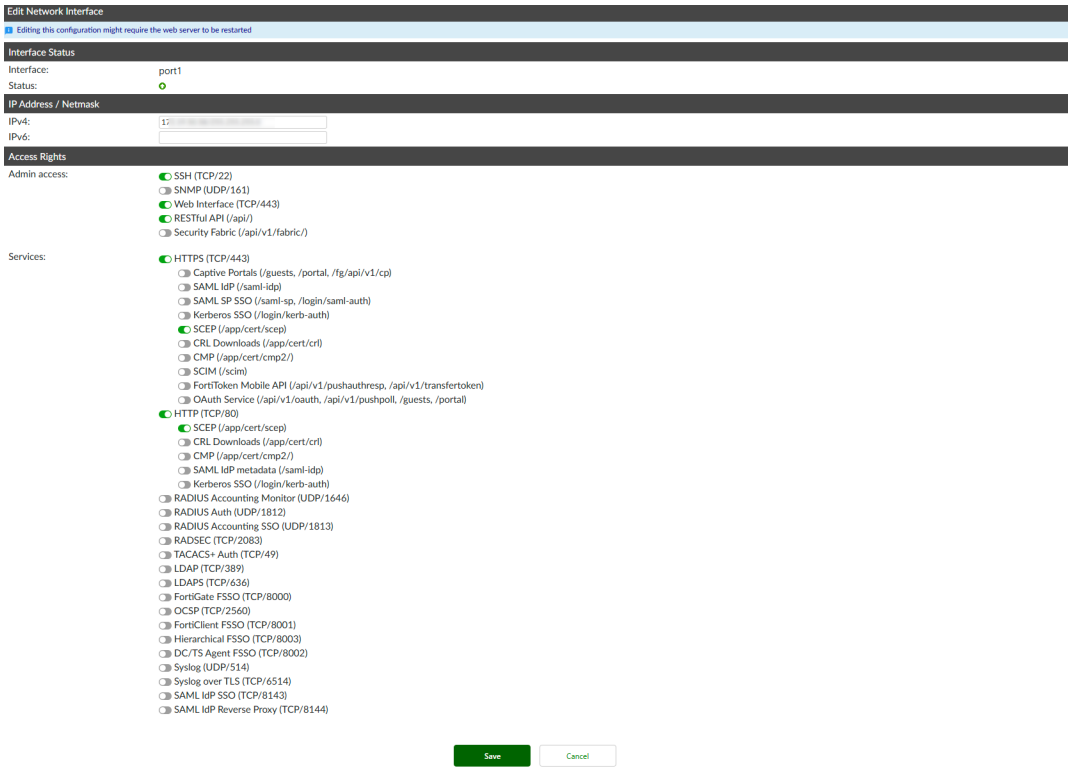
Enabling SCEP service on the interface

We now bind SCEP to an interface so clients can reach it.

To enable SCEP service on the interface:

1. Go to *System > Network > Interfaces*.
2. Select an interface to open it.
3. Enable *HTTPS (TCP/443)*.
   a. Enable *SCEP (/app/cert/scep)*.

4. Enable *HTTP (TCP/80)*.
   a. Enable *SCEP (/app/cert/scep)*.
5. Click *Save*.



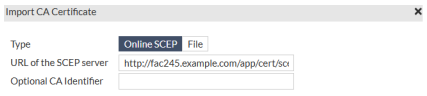
FortiGate: Trust CA and CRL via SCEP

Importing the CA:

1. Go to *System > Certificates*.
2. From the *Create/Import* dropdown, select *CA Certificate*.
   The *Import CA Certificate* window opens.
3. Ensure that the *Type* is *Online SCEP*.
4. In *URL of the SCEP server*, enter:

```
http://fac245.example.com/app/cert/scep/
```

5. Click *OK*.



Alternatively:

a. In FortiAuthenticator, export the private CA by selecting the CA in *Certificate Management > Certificate Authorities > Local CAs*, and selecting *Export Certificate*.
   The CA certificate is downloaded to your management computer.
b. In FortiGate, go to *System > Certificates*.

c. In *Create/Import*, select *CA Certificate*.
The *Import CA Certificate* window opens.
d. In *Type*, select *File*.
e. Select *Upload*.
f. On the management computer, locate the exported CA certificate, and select *Open*.
g. Click *OK*.

6. Confirm that the CA import is successful.

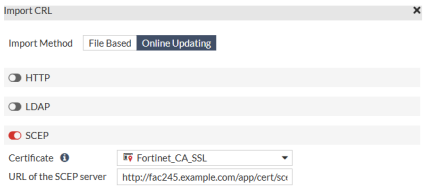
Importing the CRL:

Import CRL the same way as Importing the CA, pointing to the same SCEP URL (FortiGate fetches the CA's CRL distribution).

1. Go to *System > Certificates*.
2. From the *Create/Import* dropdown, select *CRL*.
The *Import CRL* window opens.
3. Ensure that the *Import Method* is *Online Updating*.
4. Enable *SCEP*.
5. In *URL of the SCEP server*, enter:

```
http://fac245.example.com/app/cert/scep/
```

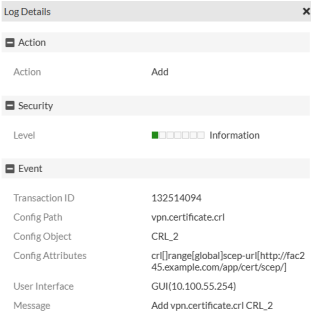
6. Click *OK*.

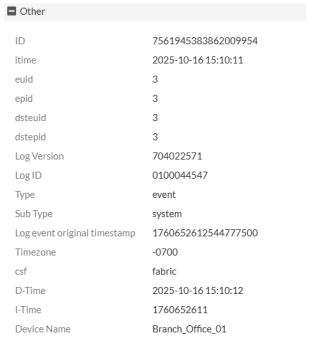


Verify import success in logs

1. Go to *Log & Report > System Events*, and select the *Logs* tab.
2. In the *Logs* tab, locate the CRL related log.

3. Double-click the log entry to open it.





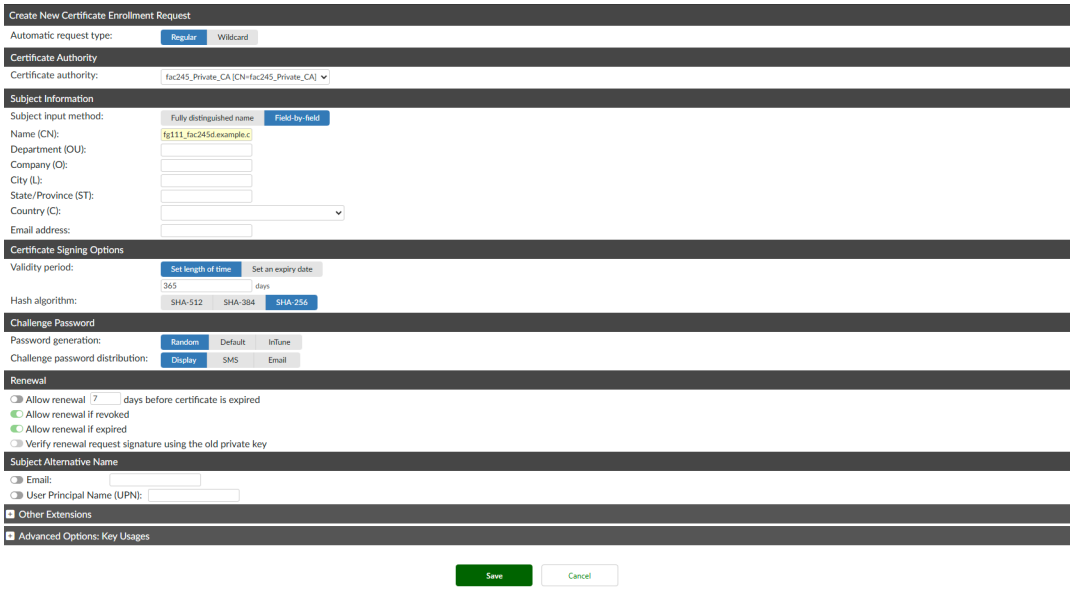
SCEP enrollment method: Automatic

To configure an automatic SCEP enrollment method:

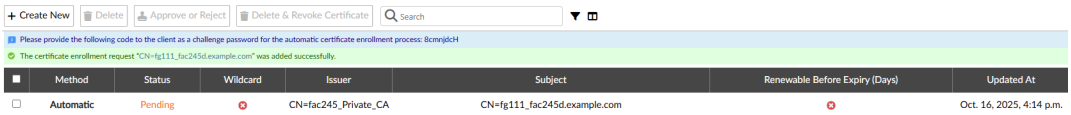
1. Go to *Certificate Management > SCEP > Enrollment Requests*, and select *Create New*.
   The *Create New Certificate Enrollment Request* window opens.
2. Ensure that the *Automatic request type* is *Regular*.
3. Ensure that the *Certificate authority* is set to the CA configured in Configuring FortiAuthenticator as a private CA on page 33.
4. Ensure that the *Subject input method* is *Field-by-field*.
5. In *Name (CN)*, enter:

```
fg111_fac245d.example.com
```

6. Ensure that the *Challenge password distribution* is set to *Display*.
7. Keep the default settings in the *Renewal* pane.
8. Click *Save*.



The new enrollment request is now listed.



Verify the enrollment log

1. Go to *Logging* > *Log Access* > *Logs*, and look for the SCEP enrollment request log entry.

FortiGate: Request and install a certificate via SCEP (automatic approval)

With FortiAuthenticator SCEP enrollment method set to *Automatic*, the request is approved without manual intervention.

See SCEP enrollment method: Automatic on page 37.

To create a CSR using SCEP:

1. Go to *System* > *Certificates*.
2. From the *Create/Import* dropdown, select *Generate CSR*.
   The *Generate Certificate Signing Request* window opens.
3. Enter a *Certificate Name*.
4. In *ID Type*, select *Domain Name*.
5. In *Domain Name*, enter:

```
fg111_fac245d.example.com
```

   Note: The domain name is same as the name used in SCEP enrollment method: Automatic on page 37.
6. In *Subject Alternative Name*, enter:

```
fg111_fac245d.example.com
```

7. Enter the *Password for private key*.

When prompted for a password in the CSR workflow, note that this is the private key protection password, not an SCEP challenge password.

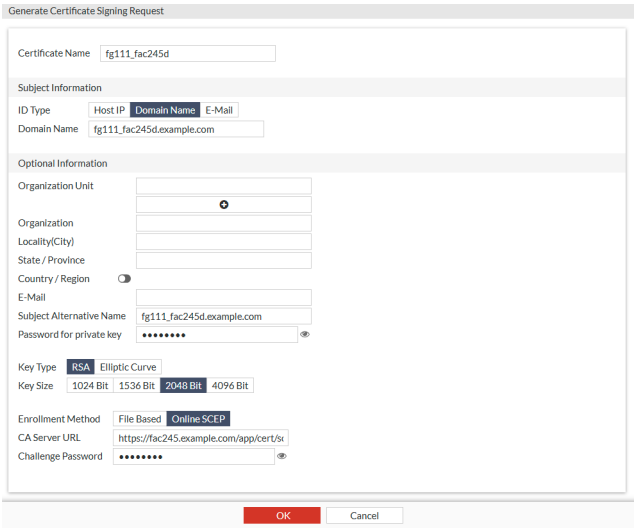
You may set any value; it is not used by FortiAuthenticator for automatic SCEP approval.

8. In *Enrollment Method*, select *Online SCEP*.

9. In *CA Server URL*, enter the SCEP URL:

```
https://fac245.example.com/app/cert/scep/
```

10. In *Challenge Password*, enter the password created on FortiAuthenticator for SCEP enrollment.
11. Click *OK*.



Once the SCEP request is submitted, with automatic approval, the certificate is returned and the local certificate *Status* changes to *Valid*.

SCEP "Challenge" vs. Key Password:

Automatic enrollment is used on FortiAuthenticator, so no server-side SCEP challenge is required.

The *Challenge Password* field shown during FortiGate CSR creation protects the local private key and is not the SCEP enrollment password.

This distinction prevents confusion when reviewing logs.

Verify success log

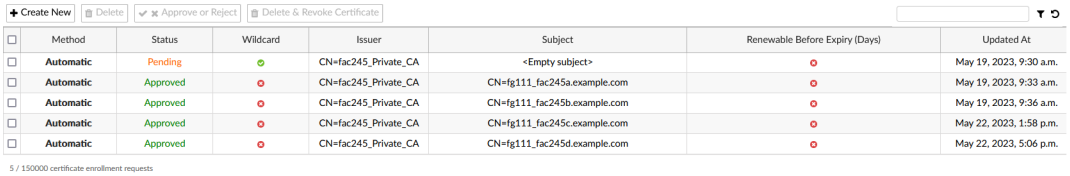
FortiGate and FortiAuthenticator logs reflect successful issuance.

On FortiGate:

1. Go to *Log & Report > System Events*.
2. Select the *Logs* tab.
3. In the *Logs* tab, locate the SCEP enrollment logs.

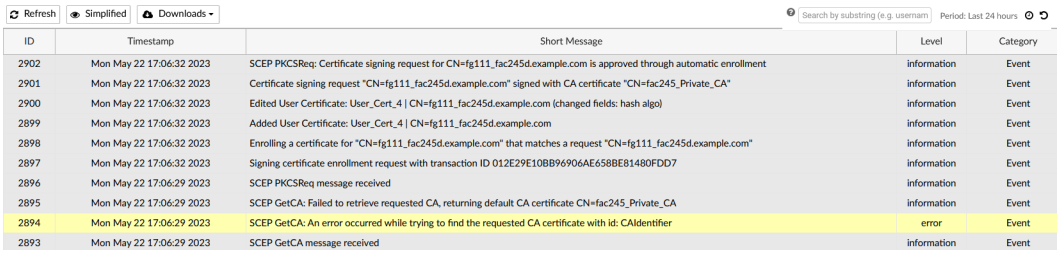
On FortiAuthenticator:

1. Go to *Certificate Management > SCEP > Enrollment Requests*.
   In the *Enrollment Requests* lists, the SCEP enrollment request is *Approved*.



Method	Status	Wildcard	Issuer	Subject	Renewable Before Expiry (Days)	Updated At
Automatic	Pending	✓	CN=fac245_Private_CA	<Empty subject>	✗	May 19, 2023, 9:30 a.m.
Automatic	Approved	✗	CN=fac245_Private_CA	CN=fg111_fac245a.example.com	✗	May 19, 2023, 9:33 a.m.
Automatic	Approved	✗	CN=fac245_Private_CA	CN=fg111_fac245b.example.com	✗	May 19, 2023, 9:36 a.m.
Automatic	Approved	✗	CN=fac245_Private_CA	CN=fg111_fac245c.example.com	✗	May 22, 2023, 1:58 p.m.
Automatic	Approved	✗	CN=fac245_Private_CA	CN=fg111_fac245d.example.com	✗	May 22, 2023, 5:06 p.m.

2. Go to *Logging > Log Access > Logs*.
   In the *Logs* list, locate the SCEP enrollment log.



ID	Timestamp	Short Message	Level	Category
2902	Mon May 22 17:06:32 2023	SCEP PKCSReq: Certificate signing request for CN=fg111_fac245d.example.com is approved through automatic enrollment	information	Event
2901	Mon May 22 17:06:32 2023	Certificate signing request "CN=fg111_fac245d.example.com" signed with CA certificate "CN=fac245_Private_CA"	information	Event
2900	Mon May 22 17:06:32 2023	Edited User Certificate: User_Cert_4 | CN=fg111_fac245d.example.com (changed fields: hash algo)	information	Event
2899	Mon May 22 17:06:32 2023	Added User Certificate: User_Cert_4 | CN=fg111_fac245d.example.com	information	Event
2898	Mon May 22 17:06:32 2023	Enrolling a certificate for "CN=fg111_fac245d.example.com" that matches a request "CN=fg111_fac245d.example.com"	information	Event
2897	Mon May 22 17:06:32 2023	Signing certificate enrollment request with transaction ID 012E29E10BB96906AE658BE81480FDD7	information	Event
2896	Mon May 22 17:06:29 2023	SCEP PKCSReq message received	information	Event
2895	Mon May 22 17:06:29 2023	SCEP GetCA: Failed to retrieve requested CA, returning default CA certificate CN=fac245_Private_CA	information	Event
2894	Mon May 22 17:06:29 2023	SCEP GetCA: An error occurred while trying to find the requested CA certificate with id: CAIdentifier	error	Event
2893	Mon May 22 17:06:29 2023	SCEP GetCA message received	information	Event

Results

1. The FortiGate now trusts the FortiAuthenticator CA and has a device certificate issued via SCEP.
   GUI status shows *Valid* for the local certificate.
2. On FortiAuthenticator, the SCEP *Enrollment Request* appears in logs, and the request shows *Automatic/Approved*.
   You can now reference this certificate, e.g., for the FortiGate HTTPS admin GUI or other TLS functions.

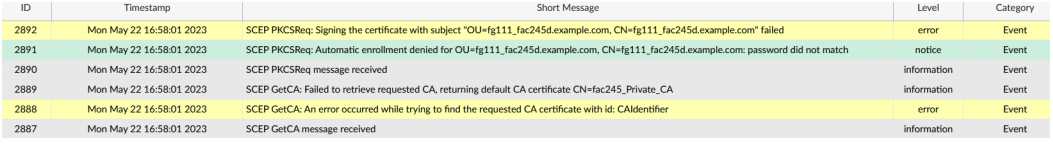
Troubleshooting

1. **Password mismatch during SCEP/CSR submission**:
   FortiGate and FortiAuthenticator logs will show a clear failure entry.
   Recheck the key password you set when generating the CSR on FortiGate.
   Note: This is not the SCEP challenge in the automatic flow.
   In case of password mismatch:

FortiGate

Name	Subject	Comments	Issuer	Expires	Status	Source
fg111_fac245d					Unknown	User

FortiAuthenticator



ID	Timestamp	Short Message	Level	Category
2892	Mon May 22 16:58:01 2023	SCEP PKCSReq: Signing the certificate with subject "OU=fg111_fac245d.example.com, CN=fg111_fac245d.example.com" failed	error	Event
2891	Mon May 22 16:58:01 2023	SCEP PKCSReq: Automatic enrollment denied for OU=fg111_fac245d.example.com, CN=fg111_fac245d.example.com: password did not match	notice	Event
2890	Mon May 22 16:58:01 2023	SCEP PKCSReq message received	information	Event
2889	Mon May 22 16:58:01 2023	SCEP GetCA: Failed to retrieve requested CA, returning default CA certificate CN=fac245_Private_CA	information	Event
2888	Mon May 22 16:58:01 2023	SCEP GetCA: An error occurred while trying to find the requested CA certificate with id: CAIdentifier	error	Event
2887	Mon May 22 16:58:01 2023	SCEP GetCA message received	information	Event

2. **Unable to fetch CA/CRL over URL**:
   Verify the SCEP service is enabled on the correct FAC interface and that `https://<fac-fqdn>/app/cert/scep/` is reachable from FortiGate.

Intune Certificate Provisioning with FortiAuthenticator CA

This example demonstrates how to integrate Microsoft Intune with FortiAuthenticator to provision certificates to Windows endpoints using SCEP.

Microsoft Intune is a cloud-based **unified management (UEM)** and **mobile device management (MDM)** solution. It helps manage and secure devices, applications, and data from a central cloud console.

FortiAuthenticator works with Microsoft Intune to issue and manage certificates for device authentication, WiFi, VPN, and other secure access scenarios. This is performed using the **Intune Certificate Connector** and FortiAuthenticator SCEP.

In this example, FortiAuthenticator acts as the Certificate Authority (CA), and Intune handles device enrollment and certificate deployment.

The integration enables secure, automated certificate issuance for Intune-managed Windows devices.

It uses:

- FortiAuthenticator for CA and SCEP services.
- Microsoft Intune for device management and profile deployment.
- Microsoft EntraID (formerly Azure AD) for identity and access control.

Use case:

Certificate distribution in Azure Cloud with Intune to Windows endpoints, using FortiAuthenticator as a cost effective CA.

Benefits:

- **Automated Certificate Provisioning**: No manual intervention required for certificate issuance.
  This reduces login issues and ensures more reliable and stable network connections.
  Certificates give stronger security than passwords or SMS codes.
- **Secure Identity Integration**: Leverages Microsoft EntraID and OAuth/SAML for authentication and group-based access.
- **Scalable Deployment**: Supports large-scale enterprise environments with centralized certificate management.
- **Improved BYOD experience**: On personal devices, users do not need to give the IT full control. Only organization applications get certificates. The device privacy is preserved.
- **Faster onboarding for new or replacement devices**: New laptops/phones receive certificates automatically once enrolled in Intune.
- **Consistent Experience Across All Devices**: On Windows, macOS, iOS, and Android, certificate deployment works the same.
- **Automatic setup and zero-touch enrollment**: When a device enrolls into Intune:
  - Root CA certificates are automatically pushed.
  - Client certificate is automatically issued.
  - WiFi and VPN profiles are delivered automatically.

Intune Certificate Provisioning with FortiAuthenticator CA

1. Creating a local certificate authority on page 42
   Set up a root CA in FortiAuthenticator for issuing certificates.
2. Creating a local services certificate on page 43
   Generate a server certificate from the CA for GUI management and SAML/OAuth IdP configuration.
3. Creating remote OAuth/SAML server on page 44
   Integrate with Microsoft Entra ID for identity and access control, enabling group-based authentication.
4. Enabling and configuring SCEP on page 45
   Activate SCEP on FortiAuthenticator, set enrollment methods, and create a wildcard enrollment request tied to OAuth.
5. Configuring Intune on page 46
   Assign Intune licenses to users and enable automatic device enrollment for Entra ID-joined devices.
6. Create configuration profiles on page 47
   a. Deploy the CA certificate to endpoints using a Trusted Certificate profile.
   b. Create a SCEP certificate profile for automated certificate issuance.
7. Join Windows endpoints to Microsoft EntraID on page 50
   Connect devices to Entra ID to trigger Intune enrollment and certificate provisioning.

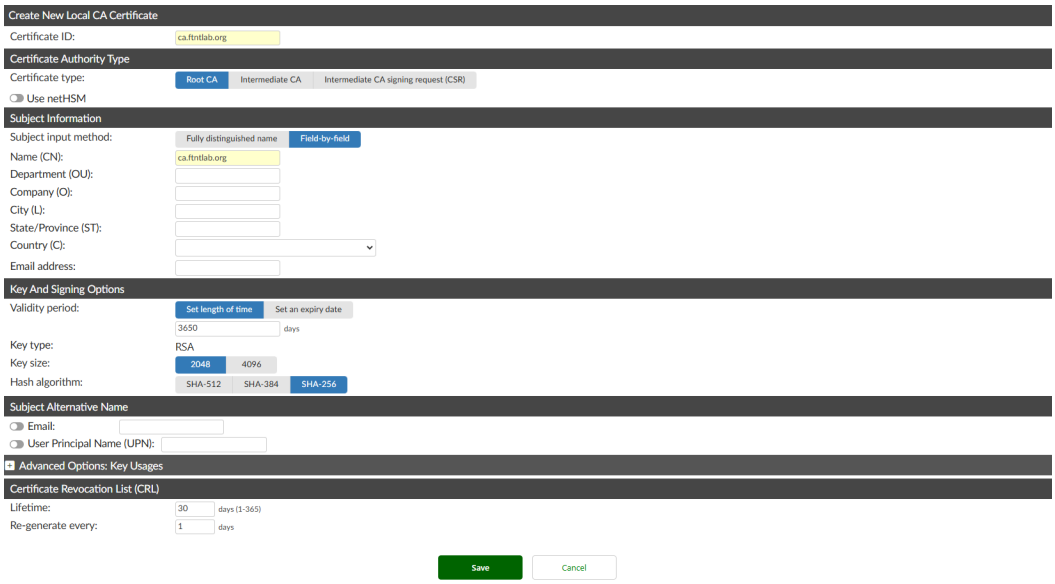
Creating a local certificate authority

You will deploy this CA certificate to Intune managed endpoints using a Configuration Profile in Intune.

To create a local CA:

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
2. Select *Create New*.
   The *Create New Local CA Certificate* window opens.
3. Ensure that the certificate type is *Root CA*.
4. Enter a certificate ID.
5. In *Name (CN)*, enter the common name.

6. Click *Save*.



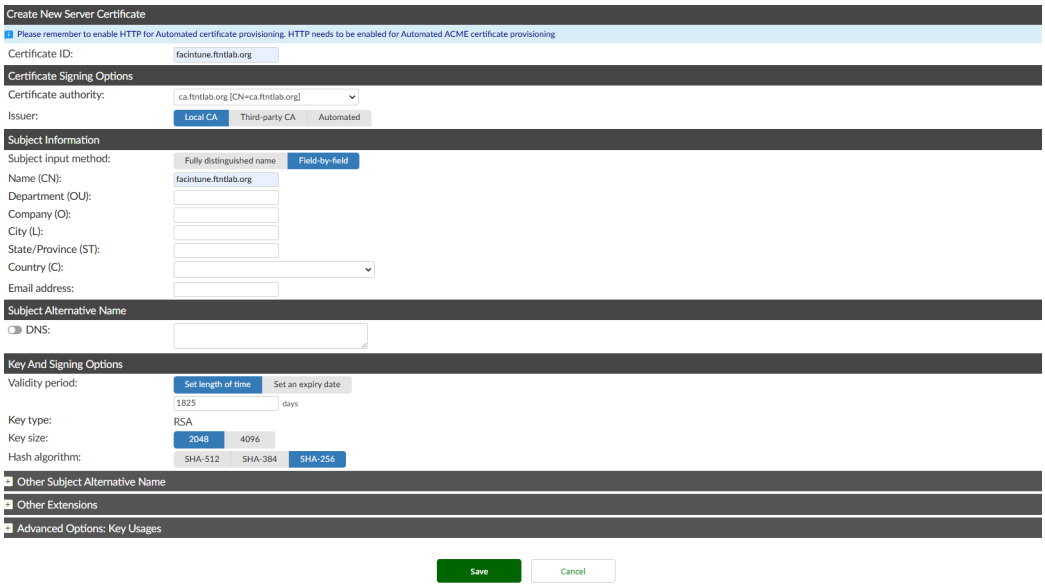
Creating a local services certificate

Issue a server certificate from the newly created CA.

To create a local services certificate:

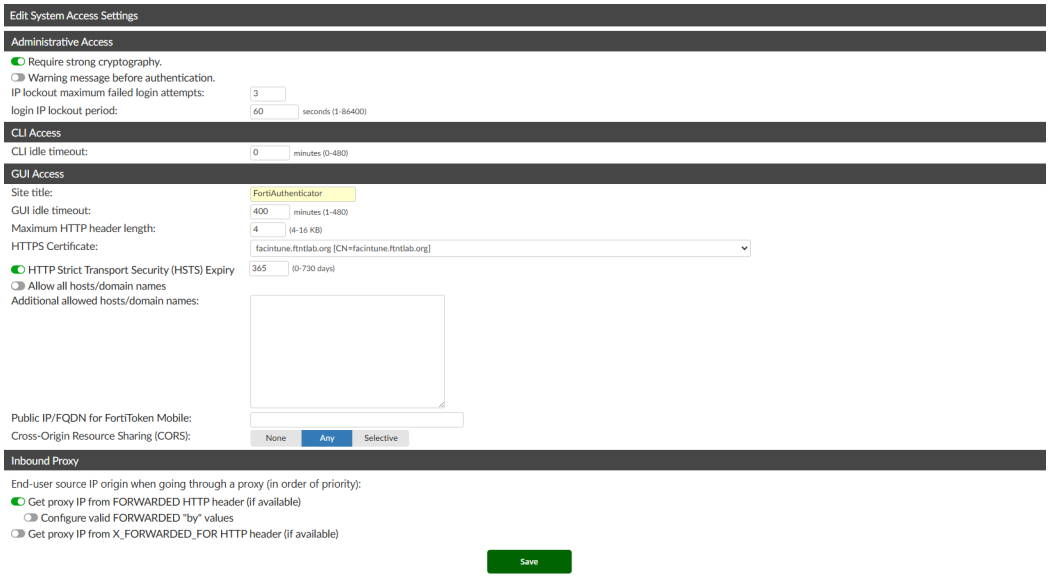
1. Go to *Certificate Management > End Entities > Local Services*.
2. Select *Create New*.
   The *Create New Server Certificate* window opens.
3. Enter a certificate ID.
4. Ensure that the *Certificate authority* is the one created in Creating a local certificate authority on page 42.
5. In *Name (CN)*, enter the common name.

6. Click *Save*.



Use this certificate for GUI management and SAML/OAuth IdP configuration.

1. Go to *System > Administration > System Access*.
2. In *HTTPS Certificate*, select the certificate created in Creating a local services certificate on page 43.
3. Click *Save*.



Creating remote OAuth/SAML server

Configure a remote SAML server, OAUTH server and EntraID Enterprise Application as shown in SAML IdP proxy for Azure on page 189.

The above example uses a remote user sync rule to import SAML users to FortiAuthenticator.

SCIM may also be used, however, a public certificate is required on FortiAuthenticator if using SCIM.

Make sure the relevant users in EntraID are given access to the Enterprise Application.

You must configure the SAML remote server to use the OAuth configuration to retrieve the group names.

Setup a SAML SP, e.g., FortiGate admin authentication, and use SAML tracer to validate the configuration.

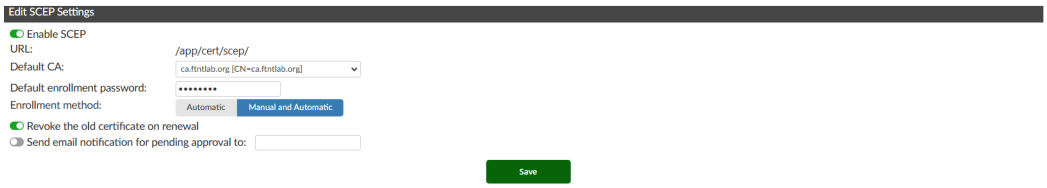
If you are receiving group names in the SAML response from FortiAuthenticator to the FortiGate your SAML and OAuth configuration is working properly.

Enabling and configuring SCEP

- Enable SCEP globally and on the interface.
- Allow both *Manual* and *Automatic* enrollment.
- Create a *Wildcard Enrollment Request* with a challenge password tied to the OAuth configuration.

To enable and configure SCEP:

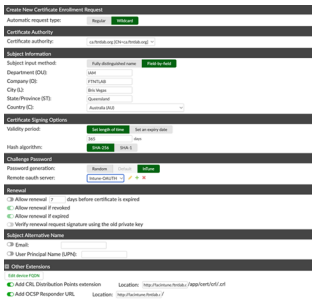
1. Go to *Certificate Management > SCEP > General*, and *select Enable SCEP*.
2. In *Default CA,* select the local CA created in Creating a local certificate authority on page 42.
3. In *Enrollment method*, select *Manual and Automatic*.
4. Ensure that *Revoke the old certificate on renewal* is enabled.
5. Click *Save*.



To create a wildcard certificate enrollment request:

1. Go to *Certificate Management > SCEP > Enrollement Requests*, and select *Create New*.
   The *Create New Certificate Enrollment Request* window opens.
2. In *Automatic request type*, select *Wildcard*.
3. In *Certificate authority*, select the local CA created in Creating a local certificate authority on page 42.
4. Enter the *Subject Information*.
5. In *Password generation*, select *InTune*.
6. In *Remote oauth server*, select the remote OAuth server created in Creating remote OAuth/SAML server on page 44.
7. In *Other Extensions*:
   a. Select to add a CRL Distribution Points extension.
      In this example, the location is `http://facintune.ftntlab.com/app/cert/crl/.crl`
   b. Select to add a CRL Distribution Points extension.
      In this example, the location is `https://facintune.ftntlab.com`.

8. Click *Save*.



Configuring Intune

Assign licenses

Allocate Intune licenses to users.

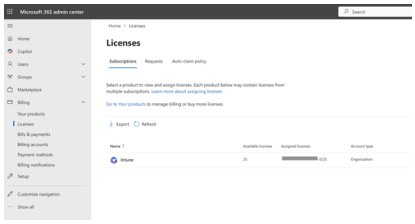
Create all users first so you do not have to separately assign licenses to users each time a new user is created.

If you create a new user, you must assign an Intune license to that user if the user requires a certificate provisioned by Intune/FortiAuthenticator.

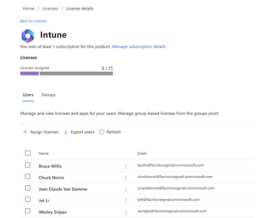
To assign Intune license:

In Microsoft 365 Admin Center, assign Intune licenses to all users requiring certificates:

1. Open https://admin.microsoft.com/.
2. Go to *Billing* > *Licenses* > *Intune*.



3. Select *Intune* to open the Intune license.

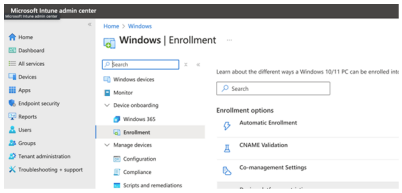


4. From the list of users, select the users you want to allocate Intune licenses to, and select *Assign licenses*.

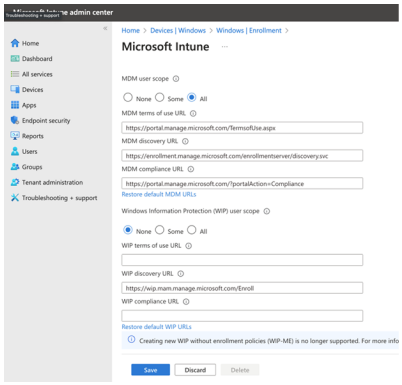
Configuring device enrollment

To configure device enrollment:

1. Go to *Devices* > *Windows* > *Enrollment*.
2. Enable *Automatic Enrollment* for devices joined to EntraID.



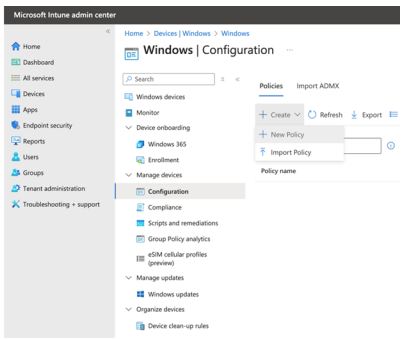
This automatically enrolls Windows devices with Intune when they are joined to EntraID.



Create configuration profiles

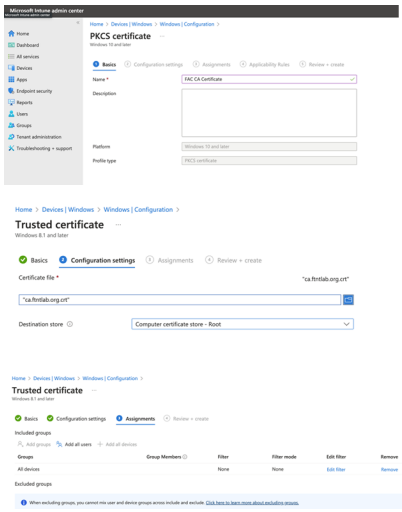
To create a CA certificate profile:

1. In Intune Admin Center, go to *Devices* > *Windows* > *Configuration*.
2. In the *Policies* tab, from the *Create* dropdown, select *New Policy*.



3. Configure the profile:
   a. *Platform*: *Windows 8.1 and later*.
   b. *Profile type*: *Trusted certificate*.

4. We create a profile to deploy FortiAuthenticator CA certificate to endpoints:
   a. *Name*: Enter a name for the profile.
   b. *Certificate file*: Upload the FortiAuthenticator CA certificate created in Creating a local certificate authority on page 42.
   c. *Destination store*: *Computer certificate store - Root*.
   d. *Assignments*: *All devices*.



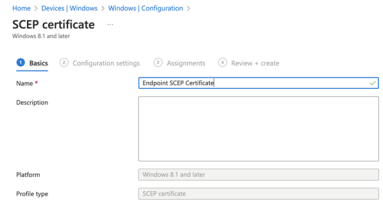
5. Save the configuration profile.

Create a *SCEP certificate* type configuration profile.

To create a SCEP certificate profile:

1. Repeat steps 1 and 2 from To create a CA certificate profile.
2. Configure the profile:
   a. *Platform*: *Windows 8.1 and later*.
   b. *Profile type*: *SCEP Certificate*.

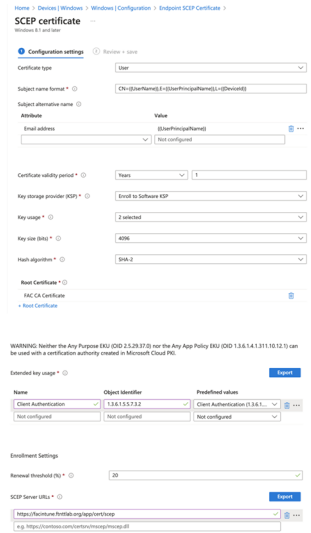
   c. *Name*: Enter a name for the profile.



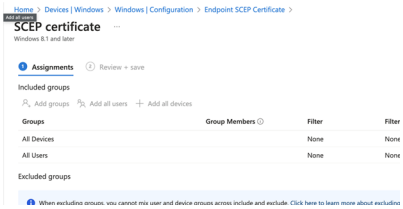
   d. *Subject name format*: `CN={{UserName}},E={{EmailAddress}},L={{DeviceId}}`.
   Note:
   The *DeviceId* is used to create a unique certificate CN for each device that the user logs in to.
   This is required since FortiAuthenticator will not provision multiple certificates with the same CN.
   e. *Subject alternative name*: The email address.
   f. *Key storage provider (KSP)*: *Enroll to Software KSP*.

g. *Key usage*: *Digital Signature* and *Key Encipherment*.
h. *Key size (bits)*: `4096`.
i. *Hash algorithm*: `SHA-2`.
j. *Root Certificate*: The certificate from To create a CA certificate profile.
k. *Extended key usage*: *Client Authentication*.
l. *SCEP Server URLs*: The FortiAuthenticator SCEP server URL:

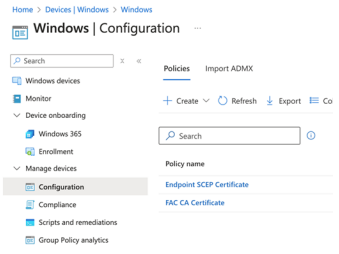
```
https://facintune.ftntlab.org/app/cert/scep
```



m. *Assignments*: *All Devices*, *All Users*.



3. Save the configuration profile.
4. Refresh the view and you should now have two Configuration Profiles - one to deploy the CA certificate and one to provision an endpoint user certificate using SCEP.

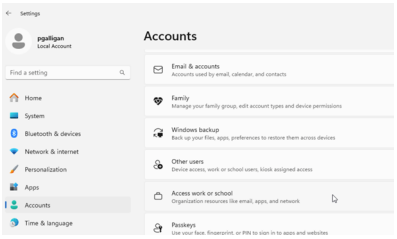


If you have other devices, e.g., macOS, phones/tablets, you must create new configuration profiles. These are not covered in this example.

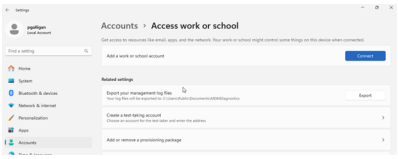
Join Windows endpoints to Microsoft EntraID

On each Windows device:

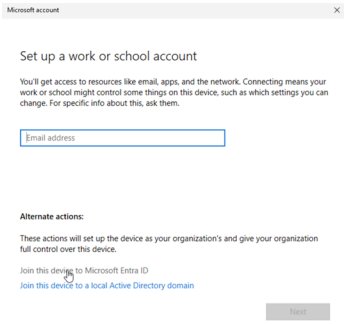
1. Go to *Settings* > *Accounts* > *Access work or school*.



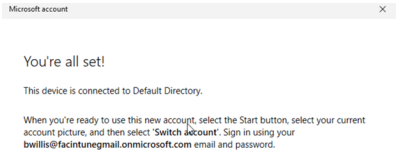
2. Select *Connect* to add a work or school account.



3. Enter the email address, select *Join this device to Microsoft EntraID*.



4. Authenticate and complete the join process.

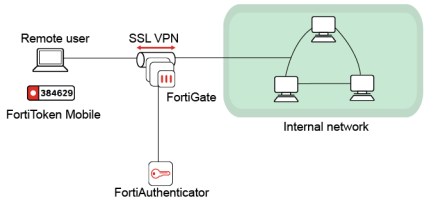


Once joined, devices will automatically enroll with Intune and receive the CA and SCEP certificates provisioned by FortiAuthenticator.

Authentication and User management

The section describes authentication and user management examples for FortiAuthenticator.

FortiToken Mobile Push for Agentless VPN



In this example, you set up FortiAuthenticator to function as a RADIUS server to authenticate Agentless 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 Agentless 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
- Agentless VPN user group: SSLVPNGroup
- FortiAuthenticator: 172.25.176.141
- FortiGate: 172.25.176.92

For the purposes of this example, a FortiToken Mobile free trial token is used. This example 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.

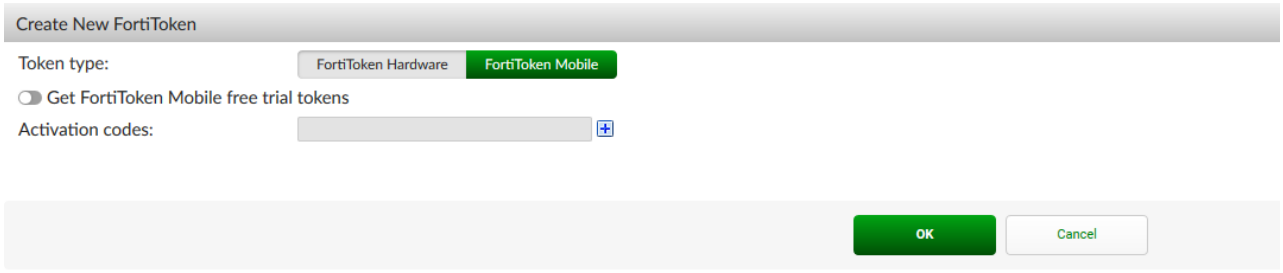
The interface that receives the approve/deny FTM push responses must have the *FortiToken Mobile API* service enabled.

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:

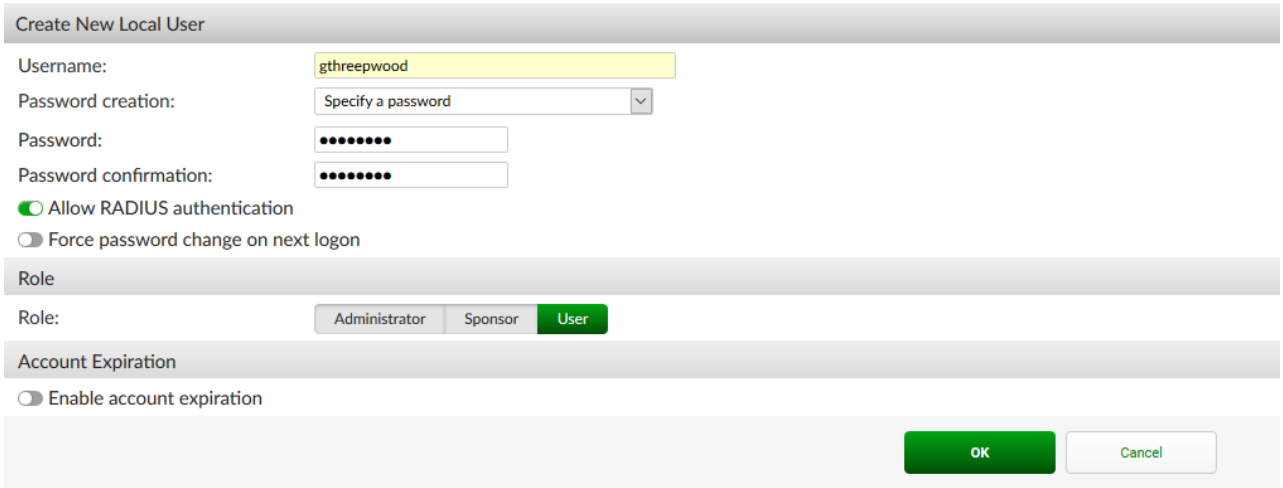
1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *FortiTokens*, and select *Create New*.
2. Set *Token type* to *FortiToken Mobile*, and enter the FortiToken *Activation codes* in the field provided.



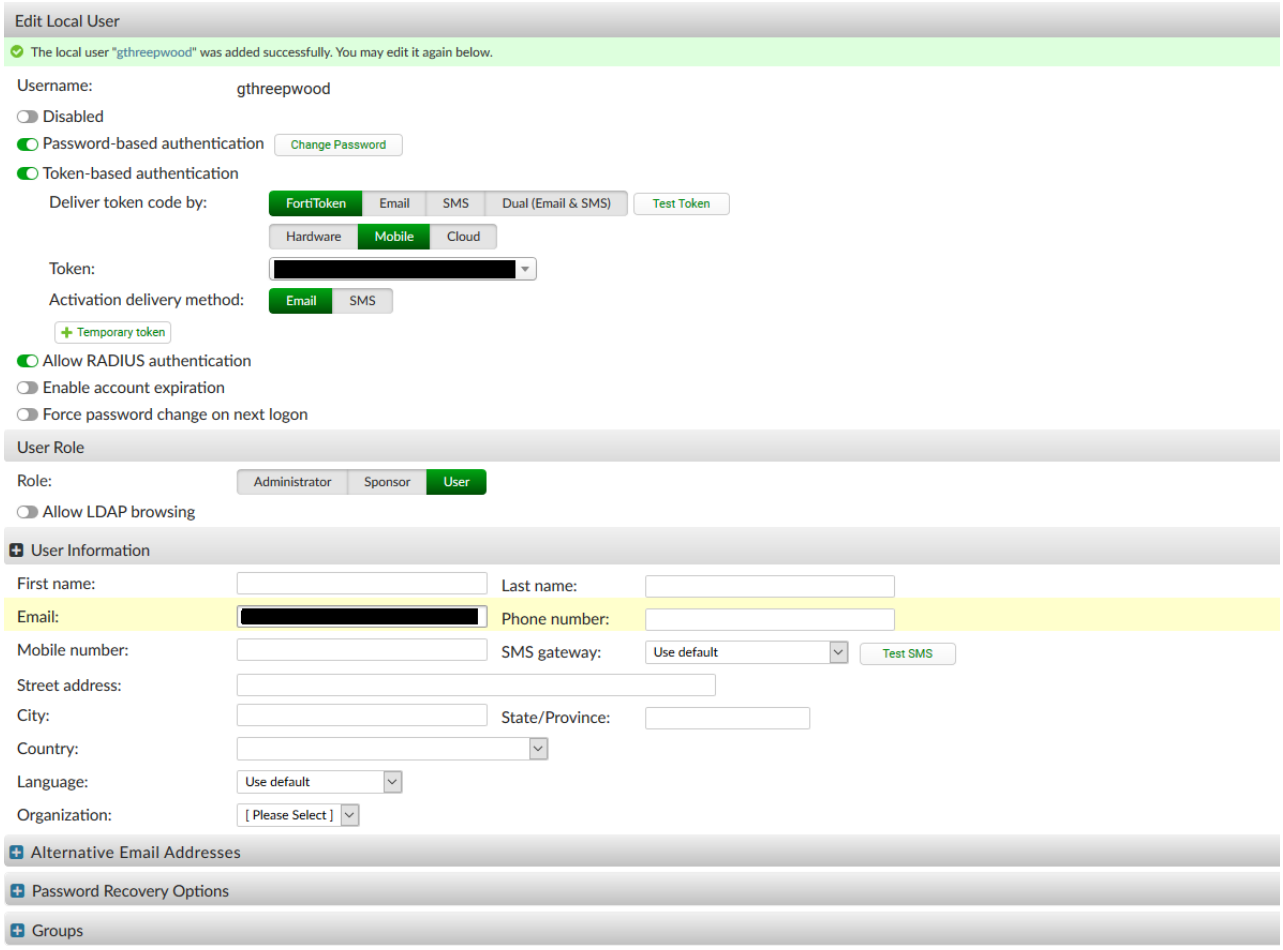
Adding the user to the FortiAuthenticator

To add a user to FortiAuthenticator:

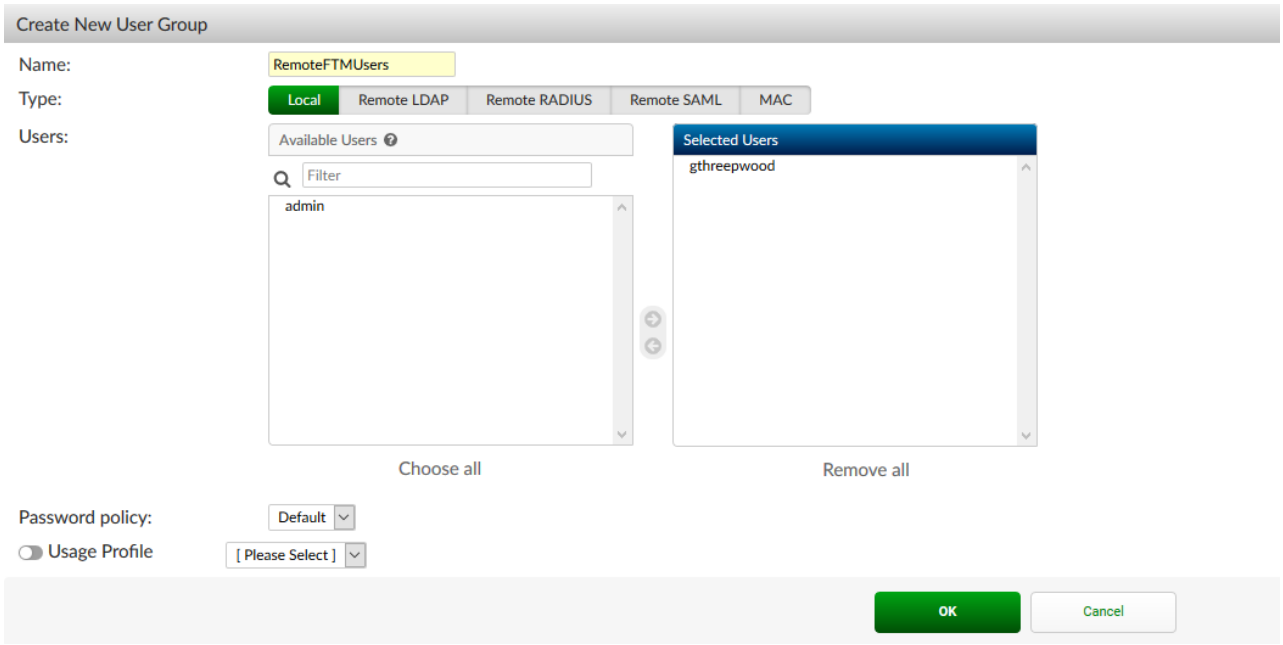
1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users*, and select *Create New*.
   Enter a *Username* (`gthreepwood`) and enter and confirm the user password.
   Enable *Allow RADIUS authentication*, and select *OK* to access additional settings.



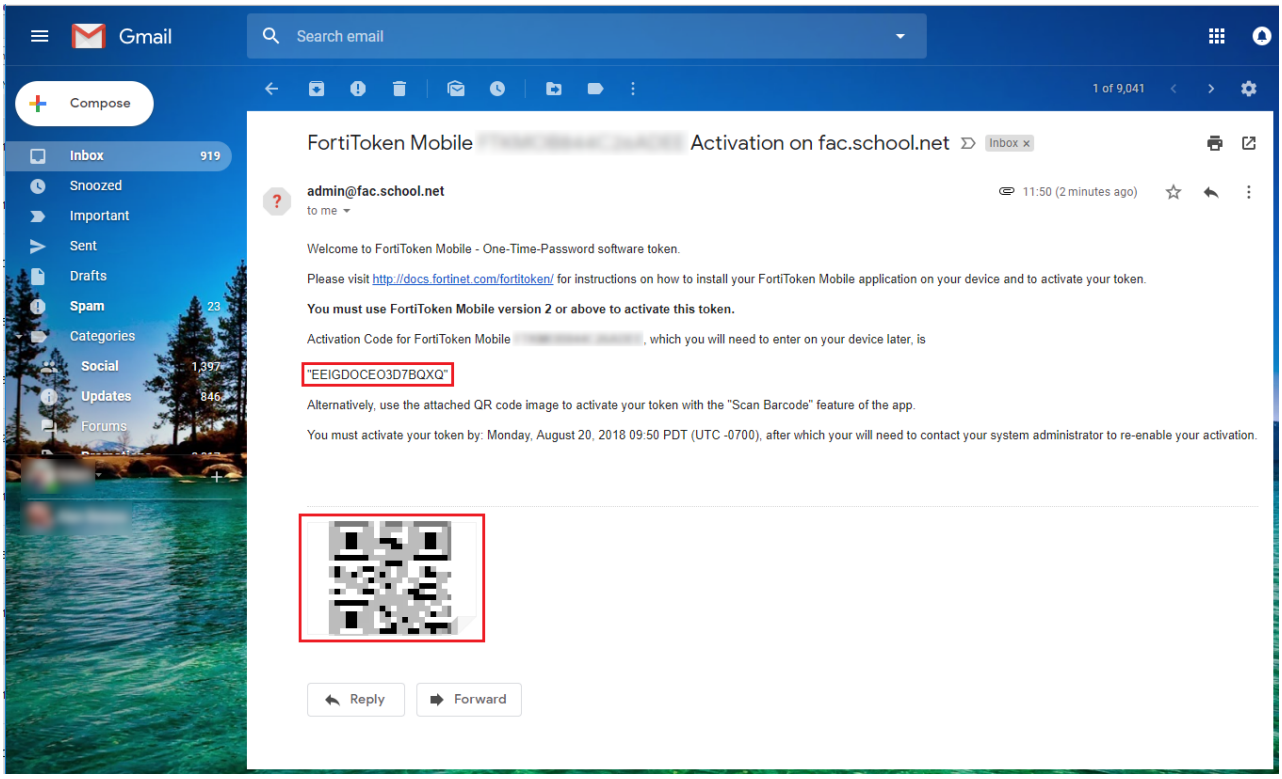
2. Enable *Token-based authentication* and select to deliver the token code by *FortiToken*. Select the FortiToken added earlier from the *FortiToken Mobile* drop-down menu.
   Set *Delivery method* to *Email*. This will automatically open the *User Information* section where you can enter the user email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



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



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



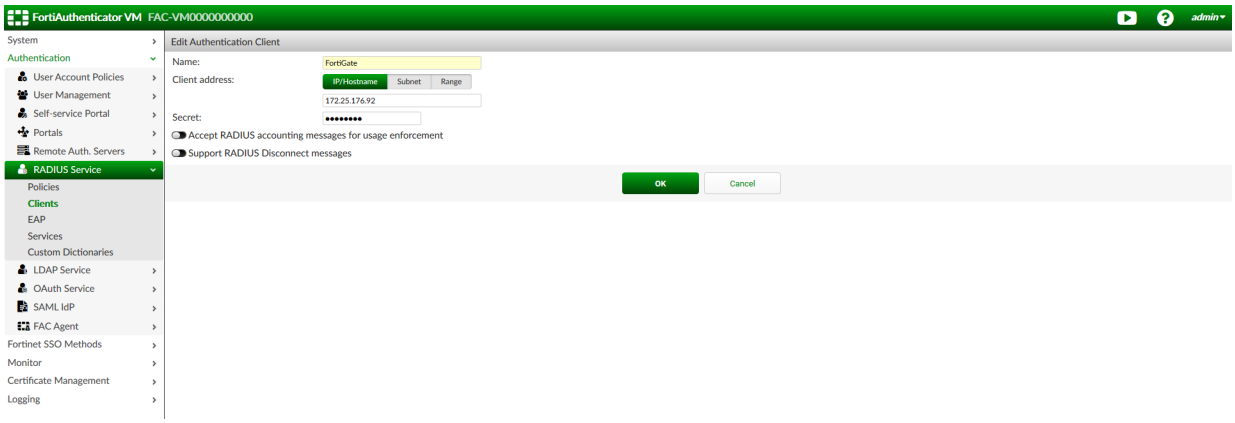
   For more information, see the FortiToken Mobile user instructions.

Creating the RADIUS client and policy on the FortiAuthenticator

To create the RADIUS client:

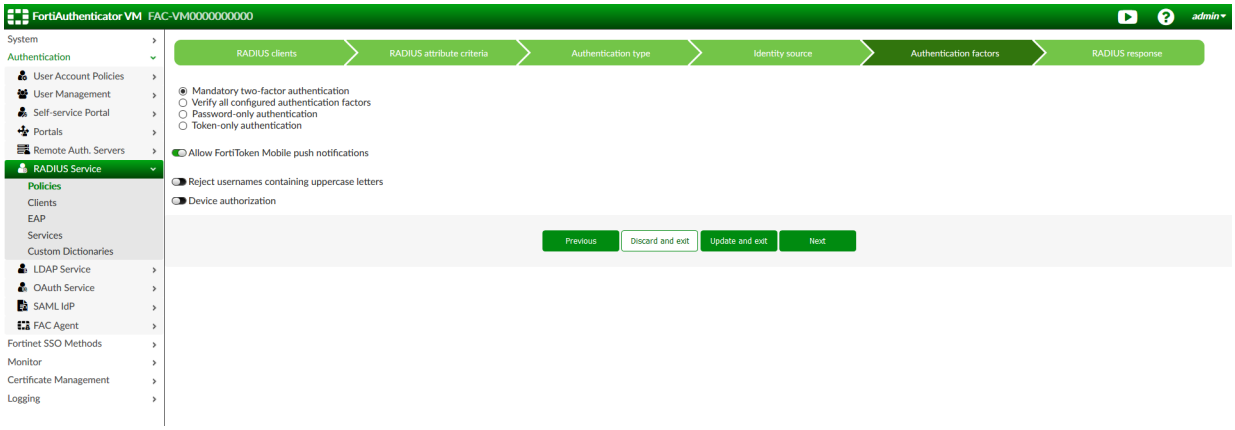
1. On the FortiAuthenticator, go to *Authentication* > *RADIUS Service* > *Clients*, and select *Create New* to add the FortiGate as a RADIUS client.
2. Enter a *Name* (*OfficeServer*), the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.

3. Click *OK*.



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*.



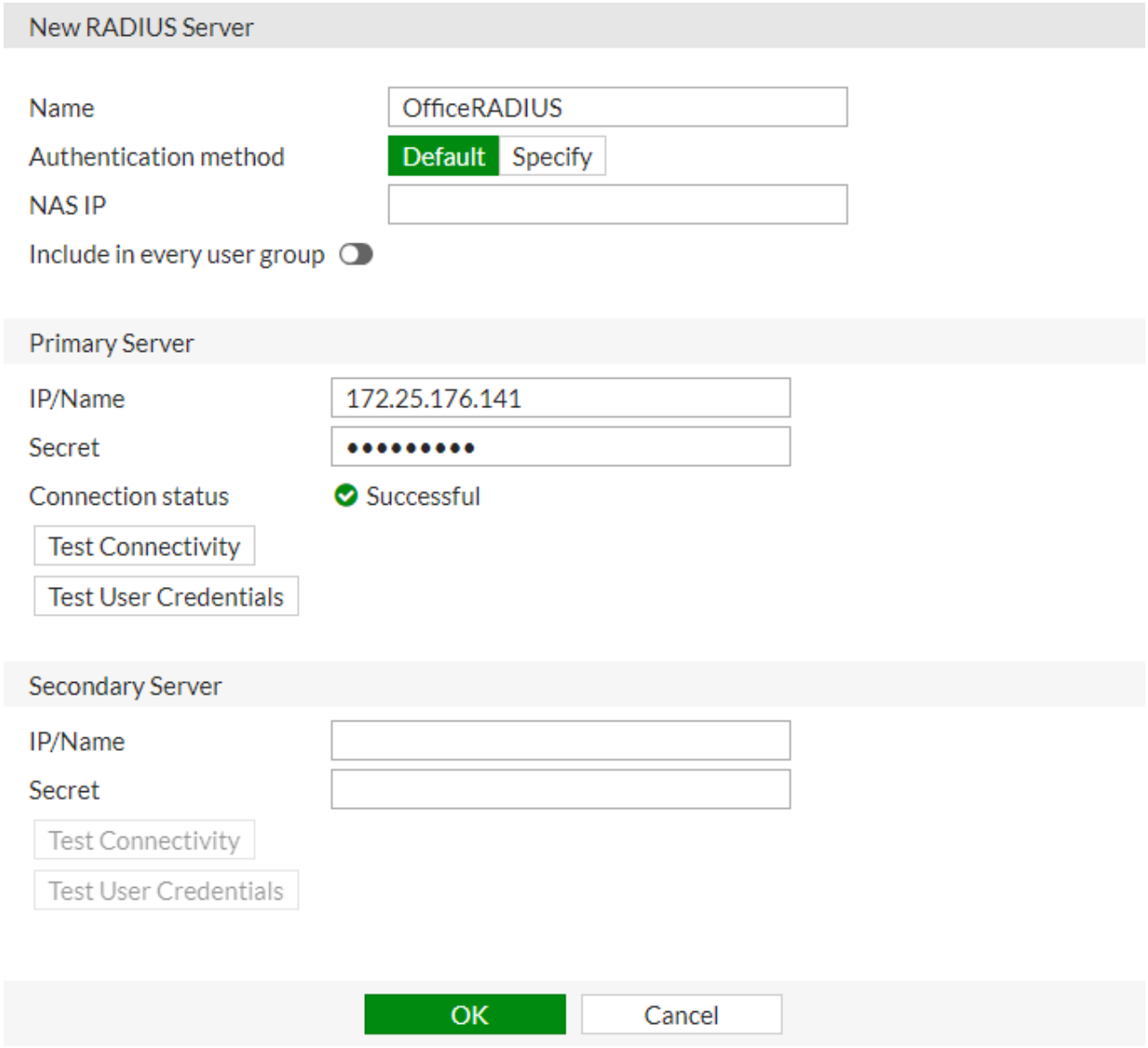
Note the *Username input format*. This is the format that the user must use to enter their username in the web portal, made up of their username and realm. In this example, the full username for gthreepwood is `gthreepwood@local`.

Connecting the FortiGate to the RADIUS server

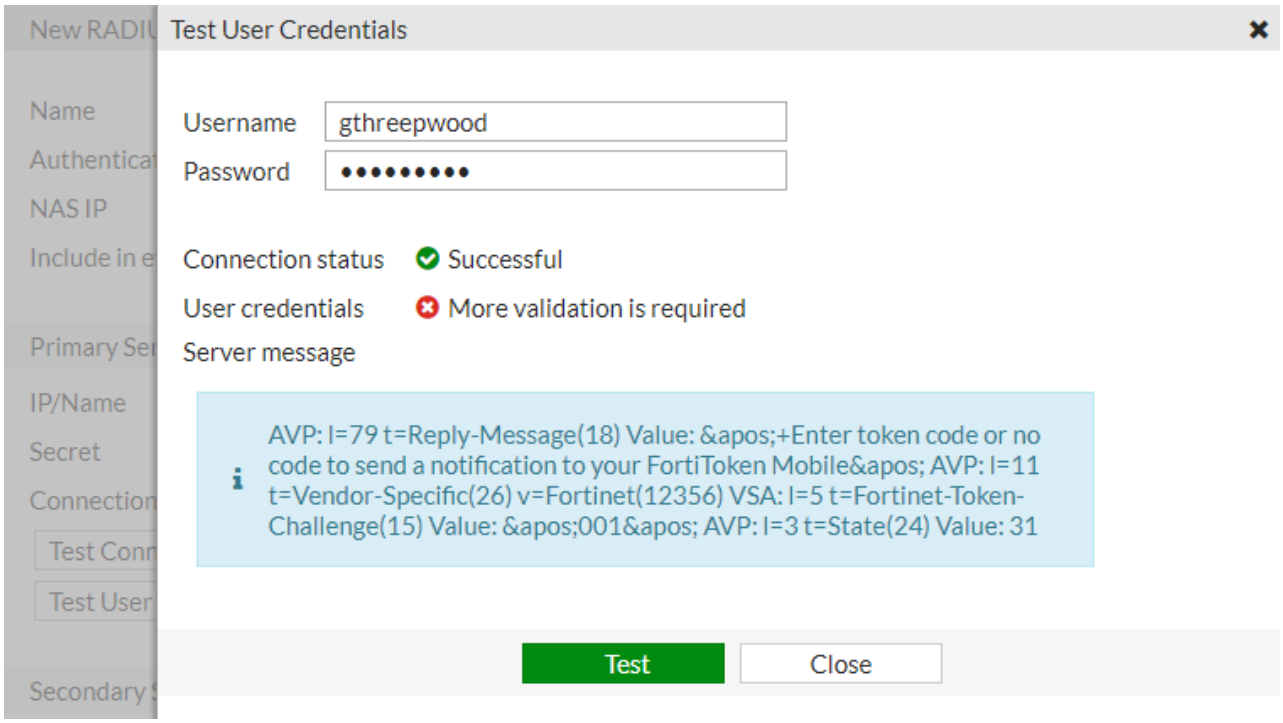
To connect the FortiGate to the RADIUS server:

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*.

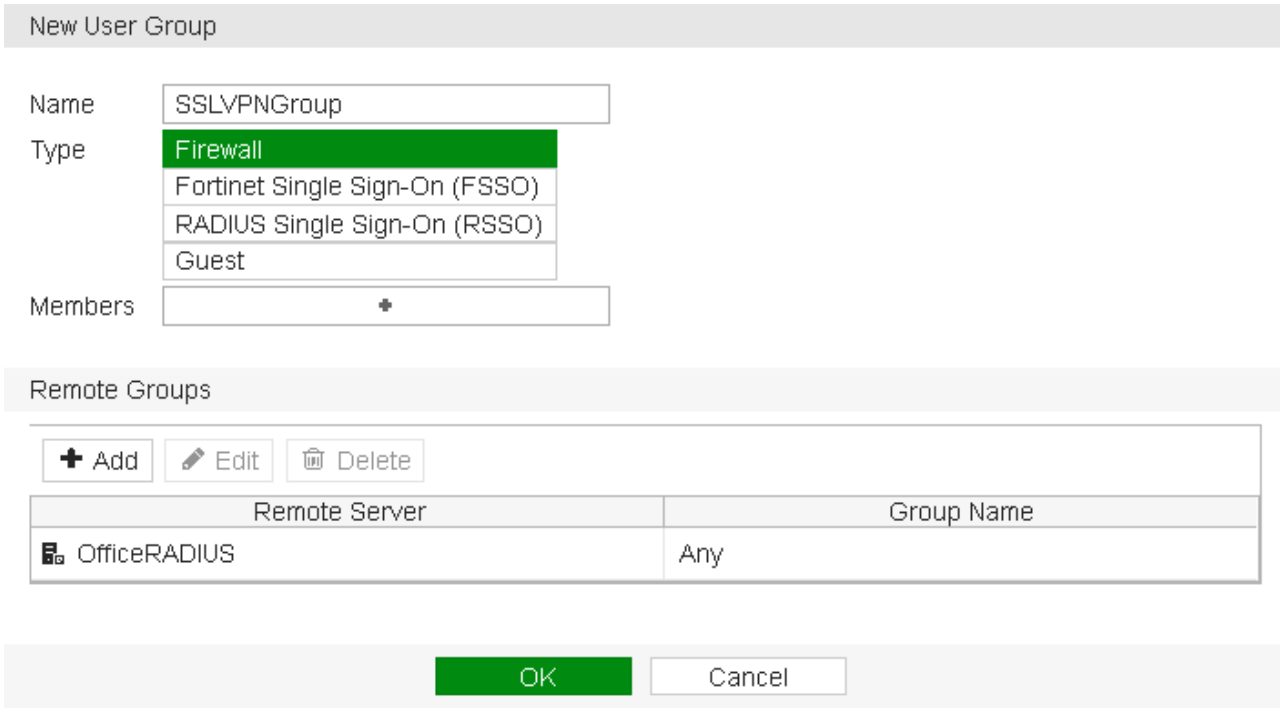


Because the user has been assigned a FortiToken, the test should return stating that *More validation is required*.



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

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



3. In the FortiGate CLI, increase the remote authentication timeout to 60 seconds.
   `#config system global`

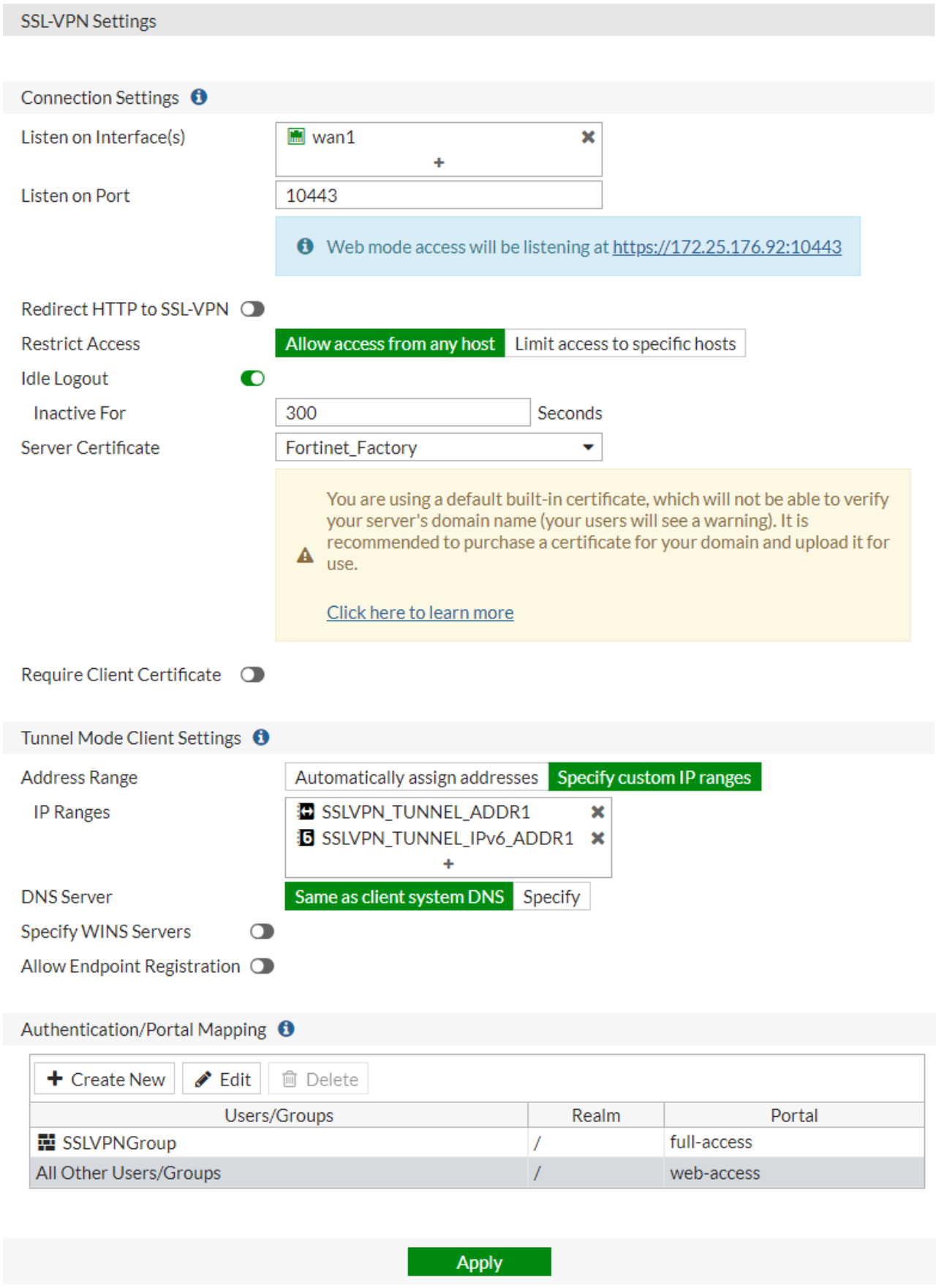
```
    #set remoteauthtimeout 60
#end
```

Configuring the Agentless VPN

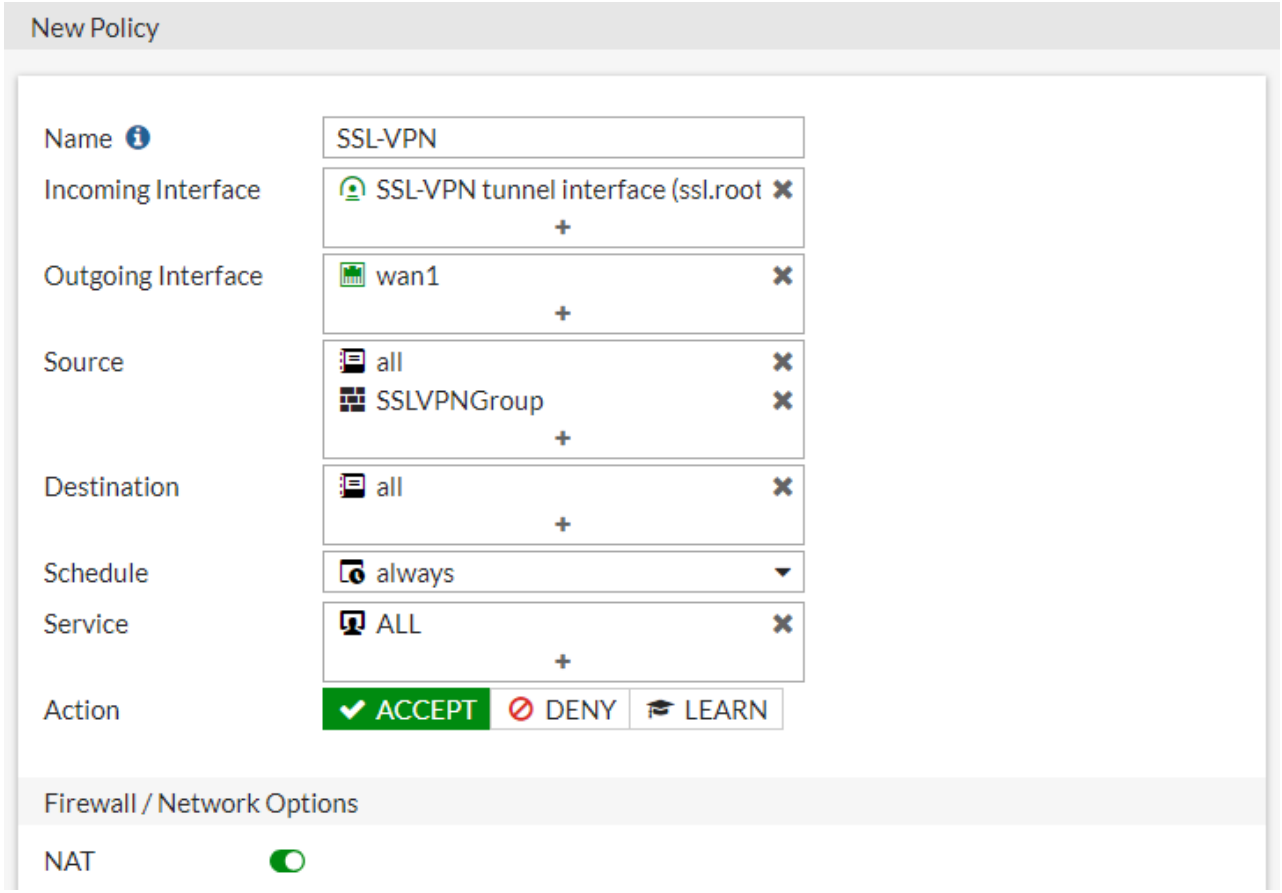
To configure the Agentless VPN:

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

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

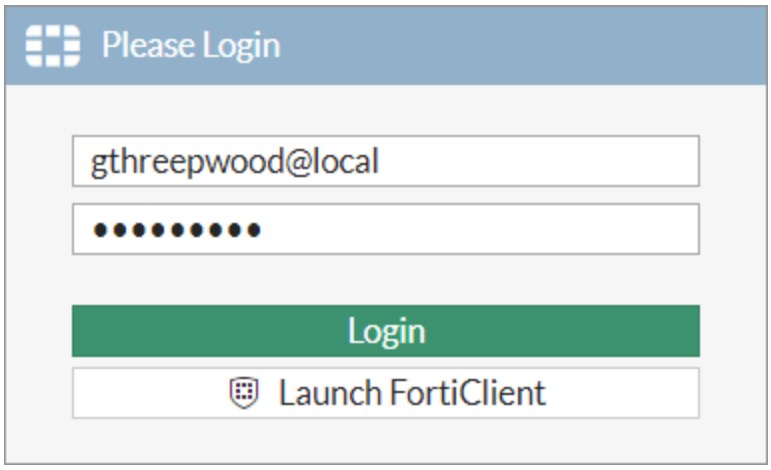

SSL-VPN Settings
Connection Settings
Listen on Interface(s)
wan1
Listen on Port
10443
Web mode access will be listening at https://172.25.176.92:10443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate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

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

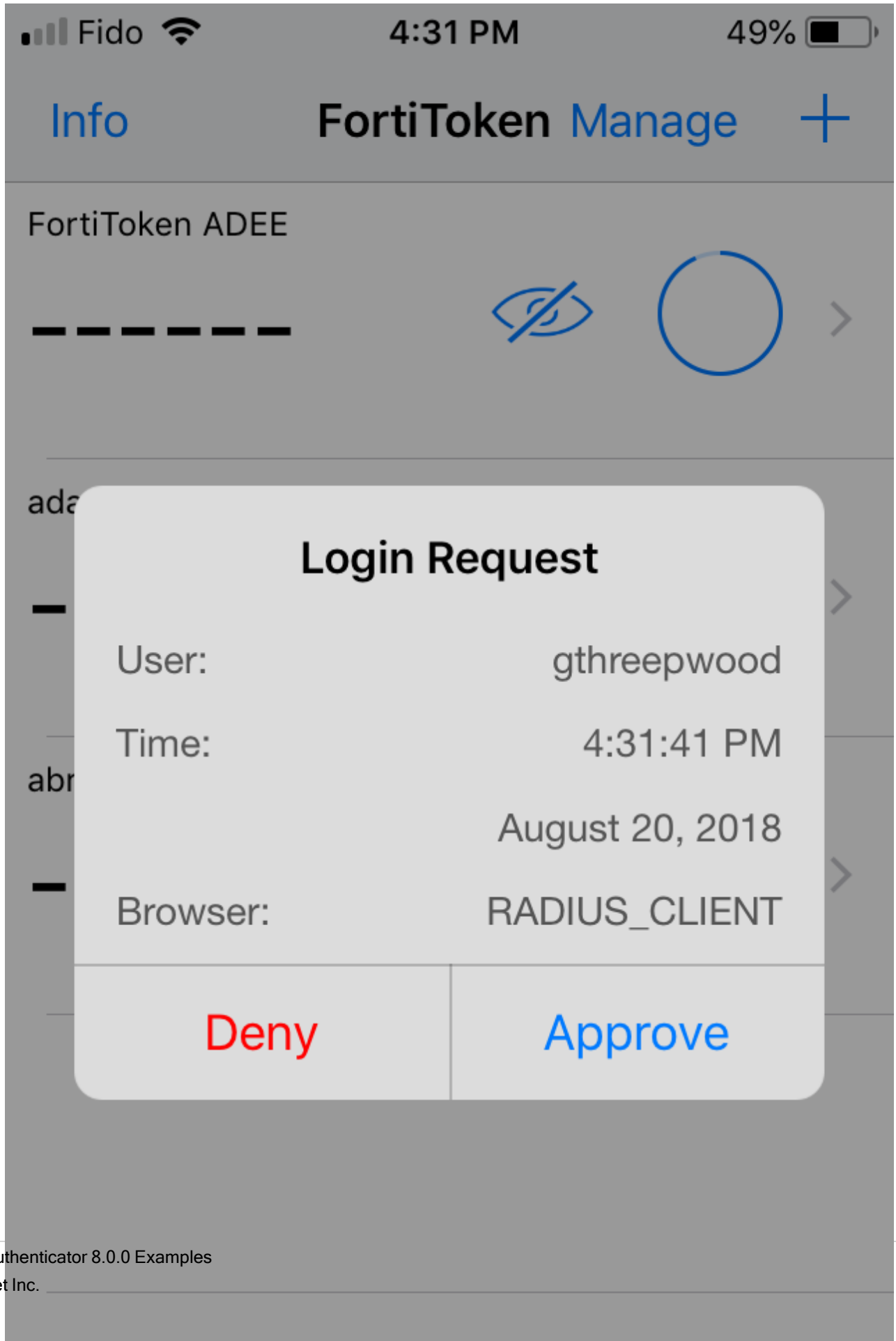


Results

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

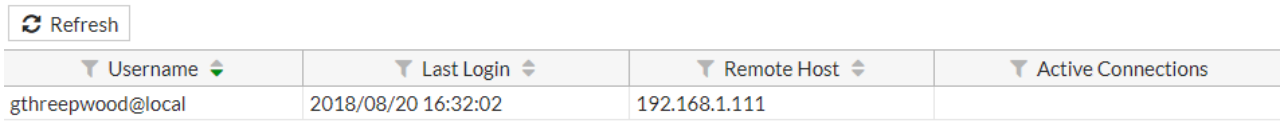


3. The FortiAuthenticator will then push a login request notification through the FortiToken Mobile application. Select *Approve*.


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

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

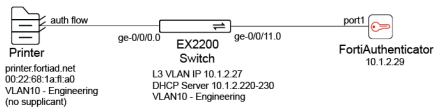
4. On the FortiGate, go to *Monitor > Agentless VPN Monitor* to confirm the user's connection.



MAC authentication bypass with dynamic VLAN assignment

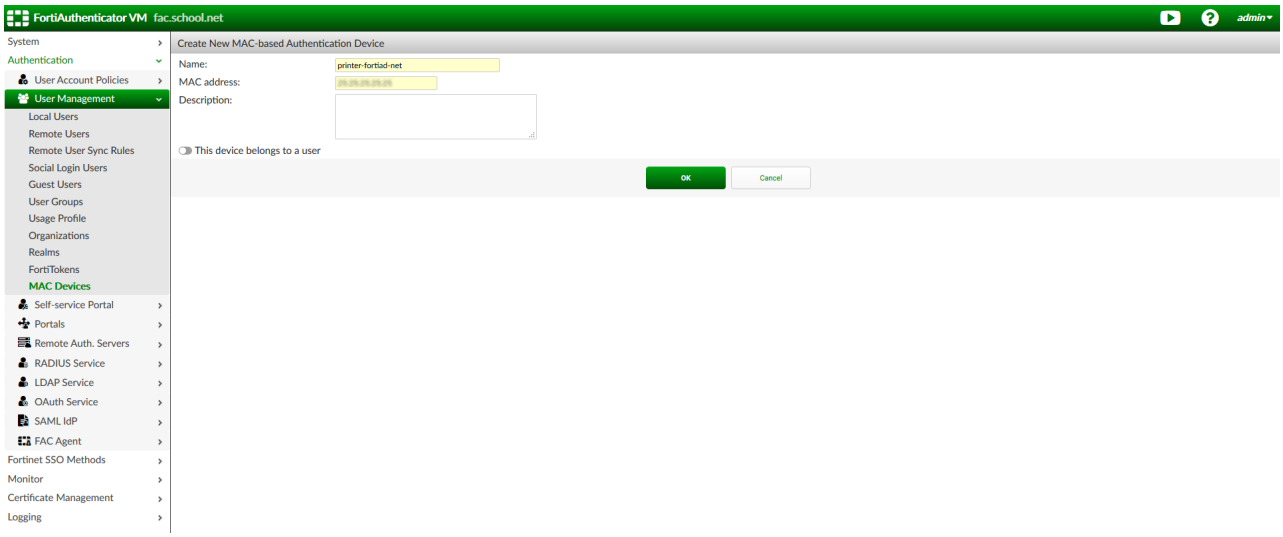
In this example, you will configure MAC authentication bypass (MAB) in a wired network with dynamic VLAN assignment.

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



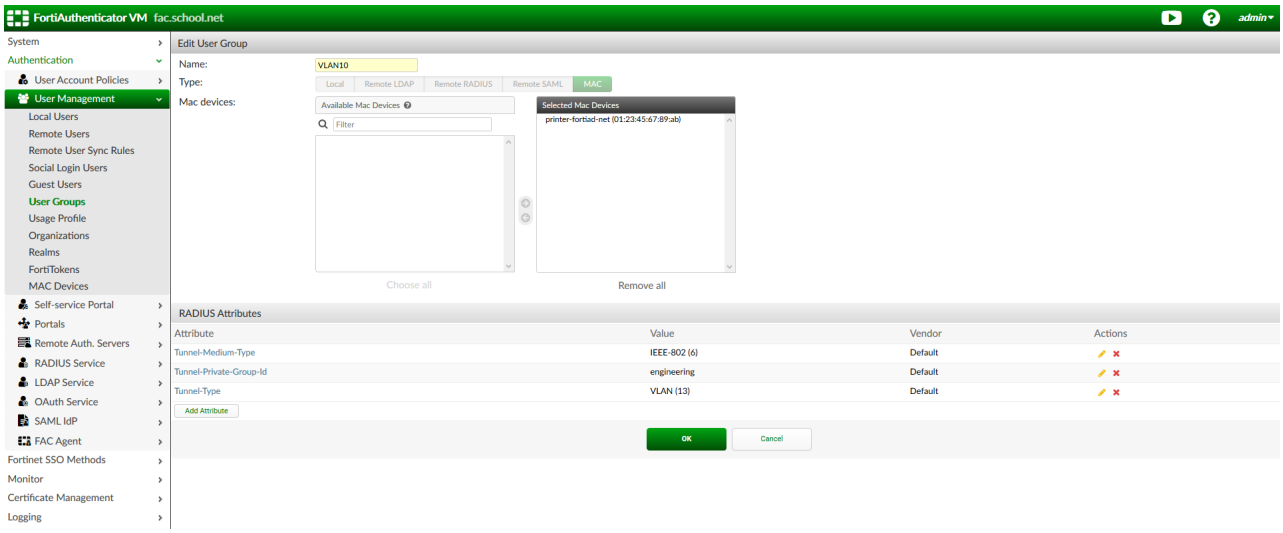
Configuring MAC authentication bypass on the FortiAuthenticator

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.



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.

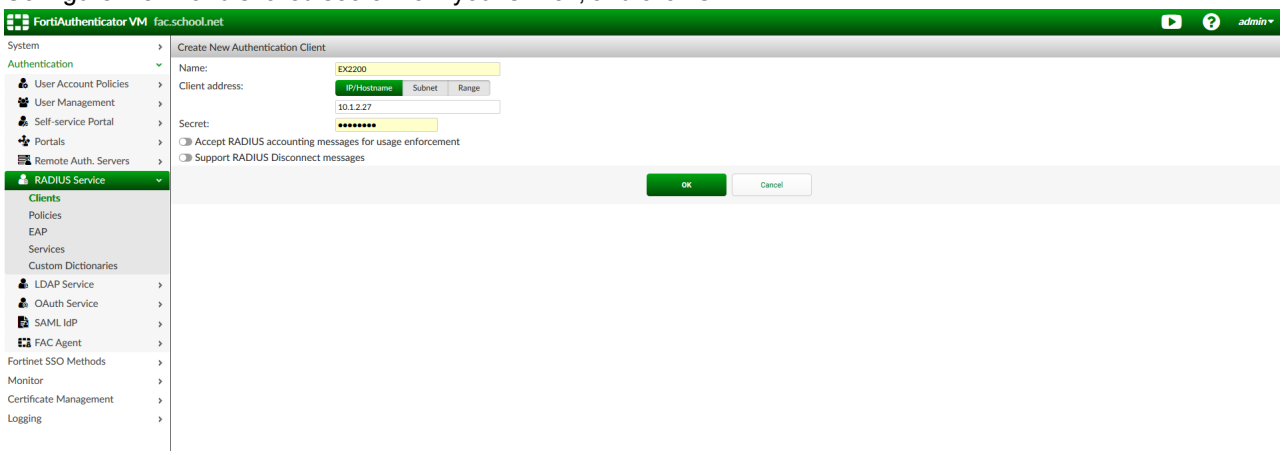


RADIUS attributes can only be added after the group has been created.

Configuring RADIUS settings on FortiAuthenticator

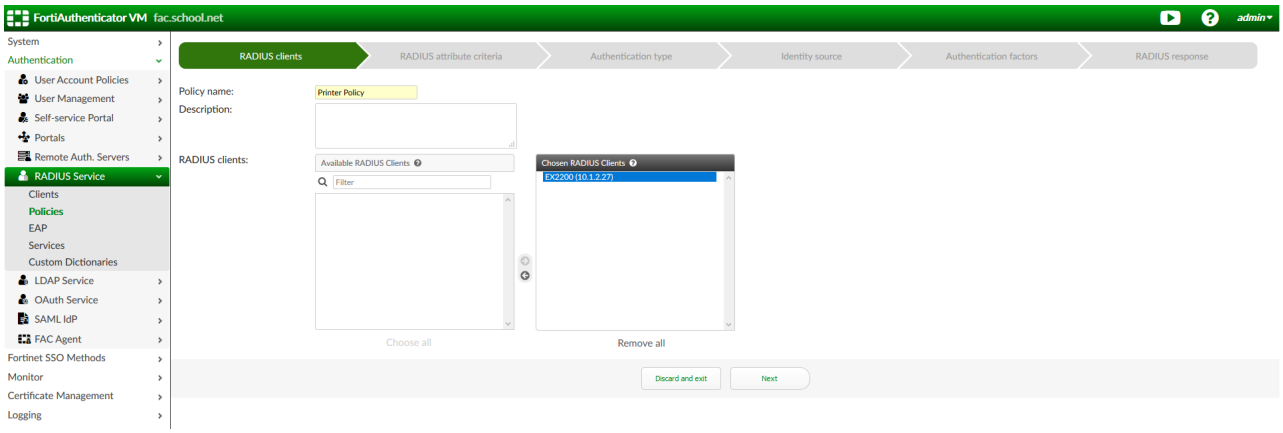
To create the RADIUS client:

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*.



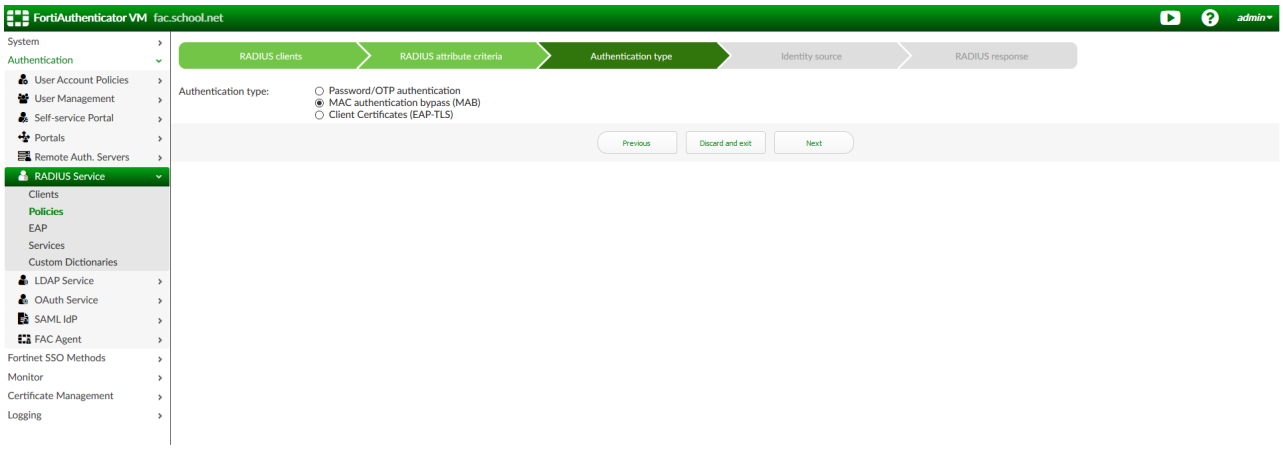
To create the RADIUS policy:

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.

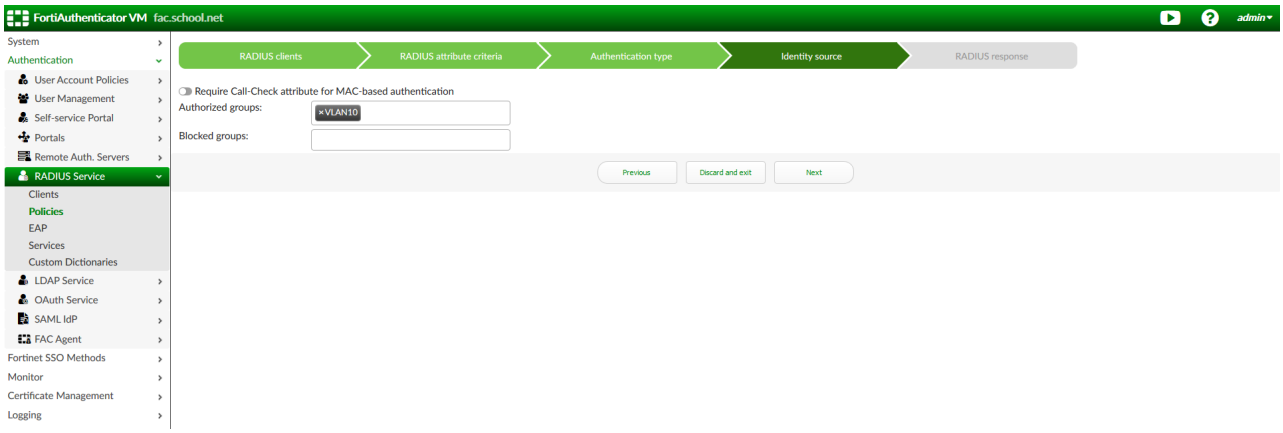


RADIUS attribute criteria can be left blank.

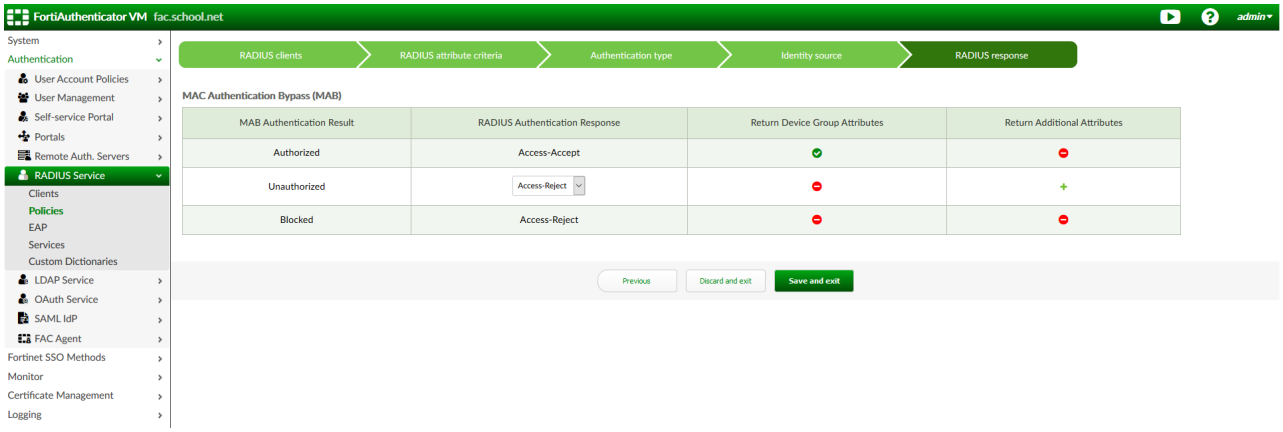
2. In *Authentication type*, select *MAC authentication bypass (MAB)*.



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



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



Configuring the 3rd-party switch

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

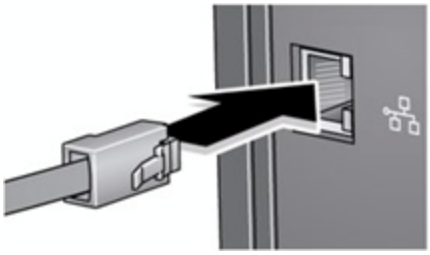
```
set system services dhcp pool 10.1.2.0/24 address-range low 10.1.2.220
set system services dhcp pool 10.1.2.0/24 address-range high 10.1.2.230
```

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

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

FortiAuthenticator user self-registration

This example enables end-users (guests/BYOD) to create their own local accounts on FortiAuthenticator using a portal.

It supports:

1. Email and/or SMS verification before the account becomes usable.
2. Optional administrator approval or endorser approval by email.
3. Automatic group placement for self-registered users.
4. Password choice (user-defined) or random password with delivery by email/SMS or on-page (if approval is not required).
5. Optional device registration/tracking for BYOD (MAC based).

Topology

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

Since administrators will approve requests by email, this example describes how to add an email server to your FortiAuthenticator. You will create and use a new server instead of the unit default server.

Prerequisites

1. Set device identity and time:
   a. In the *System Information* widget in *Dashboard > Status*, set the device FQDN and enable NTP (accurate time is required for token/OTP and link validity).
2. Configure outbound email (SMTP):
   See Creating a new SMTP server on page 69.
   a. Go to *System > Messaging > Email Services*, and from the *User* dropdown, select the recently created SMTP server.
   Optionally, set the public address.
3. Optionally, configure SMS:
   a. Go to *System > Messaging > SMS Gateways*, and configure a new SMS gateway (including CA certificates for HTTPS APIs if needed).

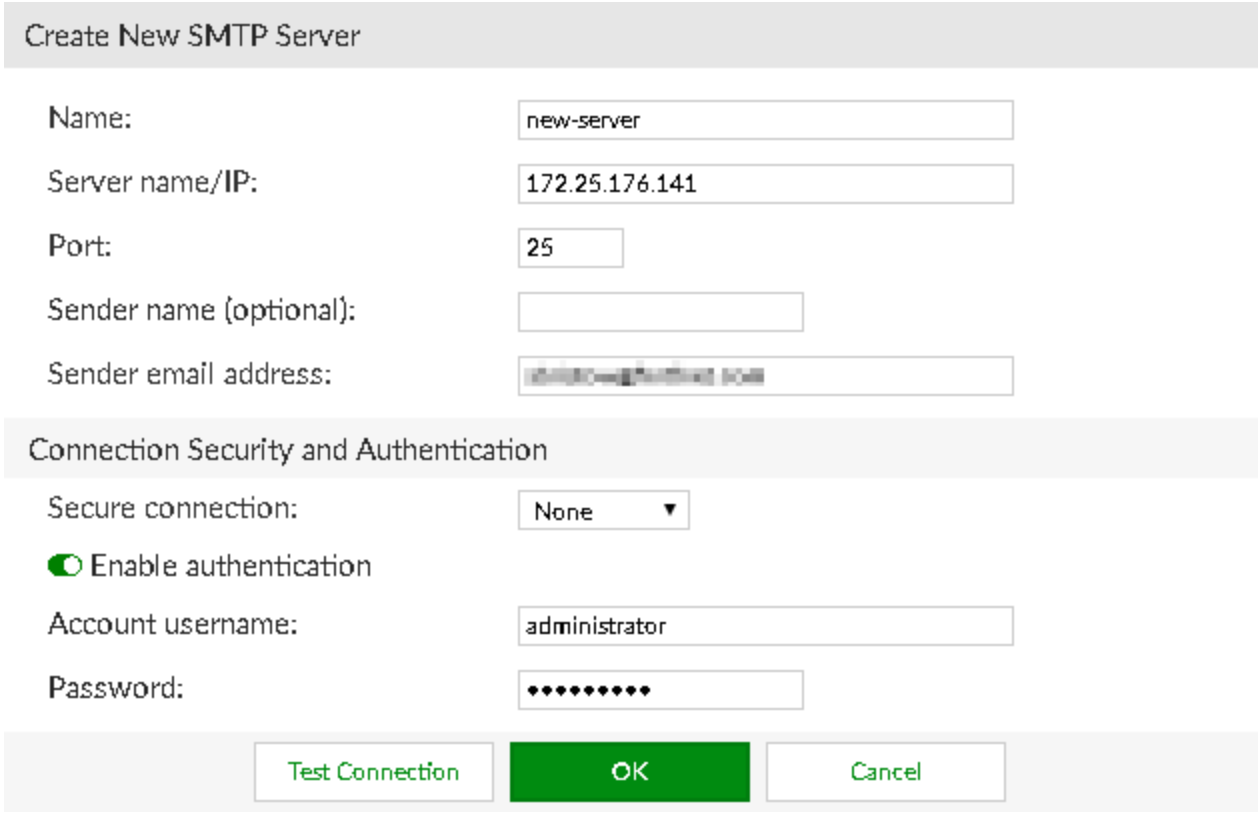
Creating a new SMTP server

To create a new SMTP server:

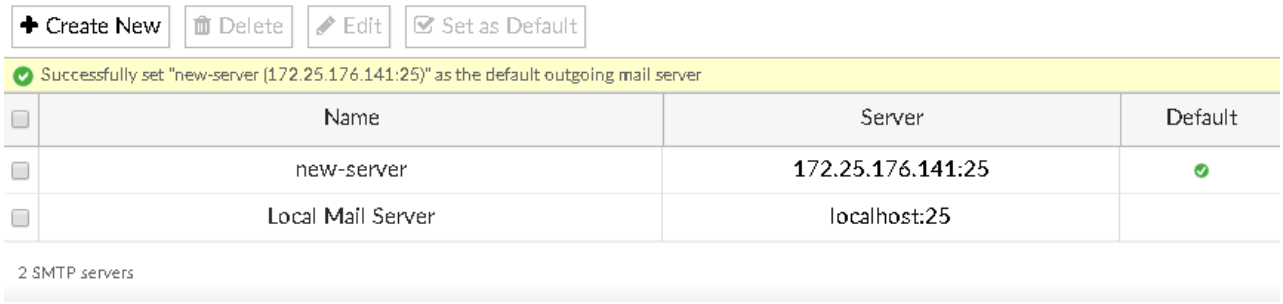
1. Go to *System > Messaging > SMTP Servers* and create a new email server for your users.
   Enter a *Name*, the IP address of the FortiAuthenticator, and leave the default port value (25).

Enter the administrator's email address, *Account username*, and *Password*.

Note that, for the purpose of this example, *Secure connection* will not be set to *STARTTLS* as a signed CA certificate would be required.



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



Configuring a self-registration portal

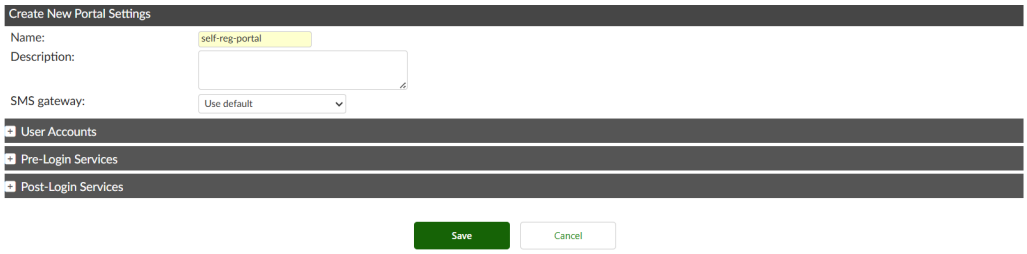
You create a portal and enable *User Account Self-Registration*.

This adds the *Create account* link on the login page.

Creating a portal

To create a portal:

1. Go to *Authentication > Portals > Portals*, and select *Create New*.
2. In *Name*, enter a name for the portal.
3. Click *Save*.



4. In the portal, under *User Accounts*, enable *User Account Self-Registration*.
   Enabling *User Account Self-Registration* displays the *Create account* link on the portal.
5. Enable *Require administrator approval*, select *Forward all approvals to the following email addresses*, specify administrator email addresses where the registration approval link for new users is sent.
6. Enable *Place registered users into a group* and select a user group.
7. Enable *Enforce contact verification* and select from the given options.
8. In *Password creation*, select *Randomly generated*.
9. In *Account delivery options available to the user*, select *Email*.
10. By default, *First name*, *Last name*, *Email*, *Mobile number* are required.
    You can add address/phone/custom fields as needed.
11. Optionally, set up *Pre-Login Services* and *Post-Login Services*.
12. Optionally, if you want new devices to be explicitly registered by the user at first login, enable *Devices* in *Post-login Services*.
    a. Choose *Tracking and Management* mode, set max devices per user (default 3, up to 20). Optionally, place registered devices into the MAC group, and set the device expiration (default 7 days, range 1-365).
       On first login from an unknown MAC, the user is prompted to register the device.
       After registration, network access proceeds per policy.
13. Click *Save*.

Creating a portal policy

Self-registration works when the portal is reachable and mapped by a portal policy.

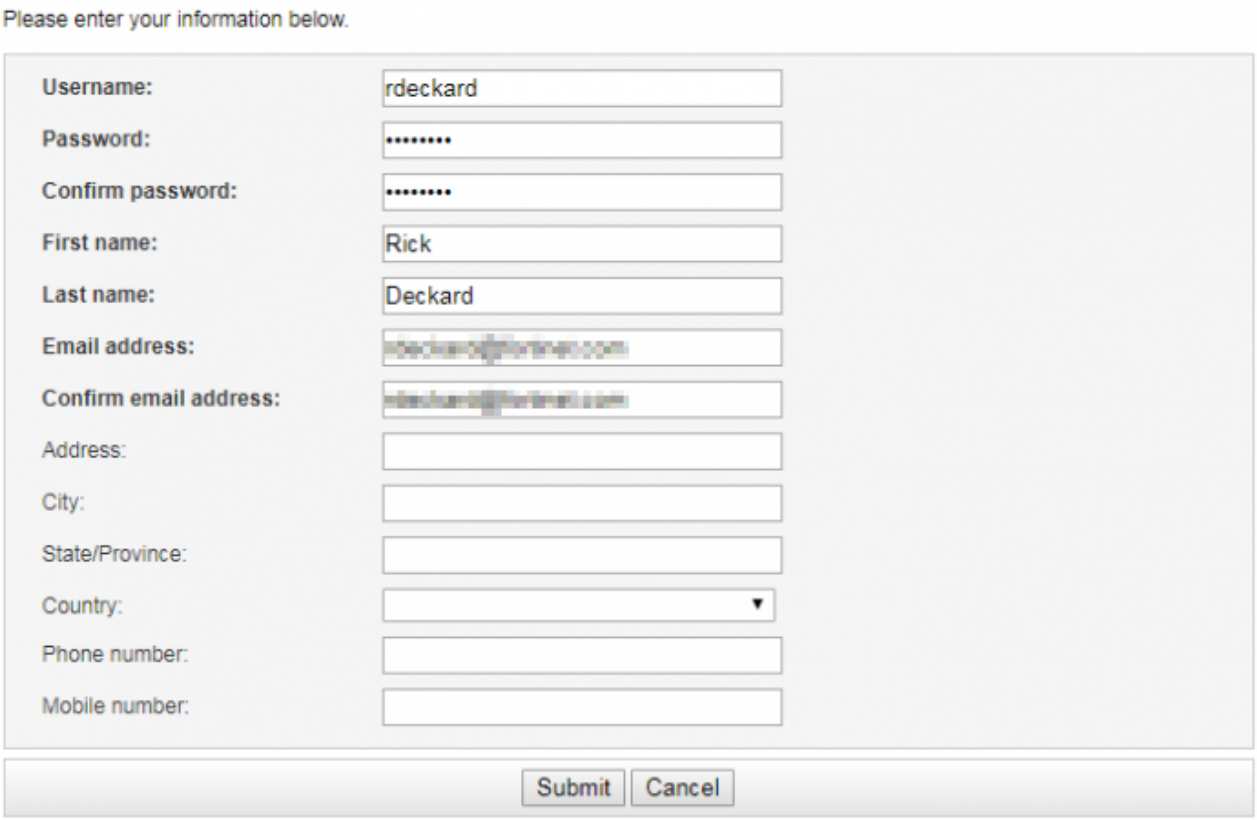
To create a portal policy:

1. Go to *Authentication > Portals > Policies*.
2. In the *Self-Service Portal* tab, select *Create New*.
3. Enter a name for the policy.
4. In *Portal*, select the portal created in Creating a portal on page 71, and click *Next*.
5. Ensure that the *Username* format is *username@realm*.
6. Enable *Use the default realm if the user-provided realm does not match any of the configured realms*.
7. Click *Next*.

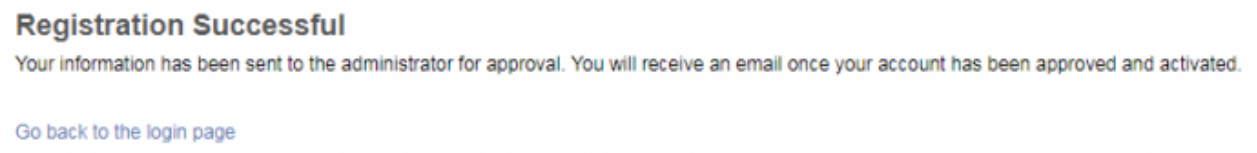
8. Click *Save and exit*.

Results - Self-registration

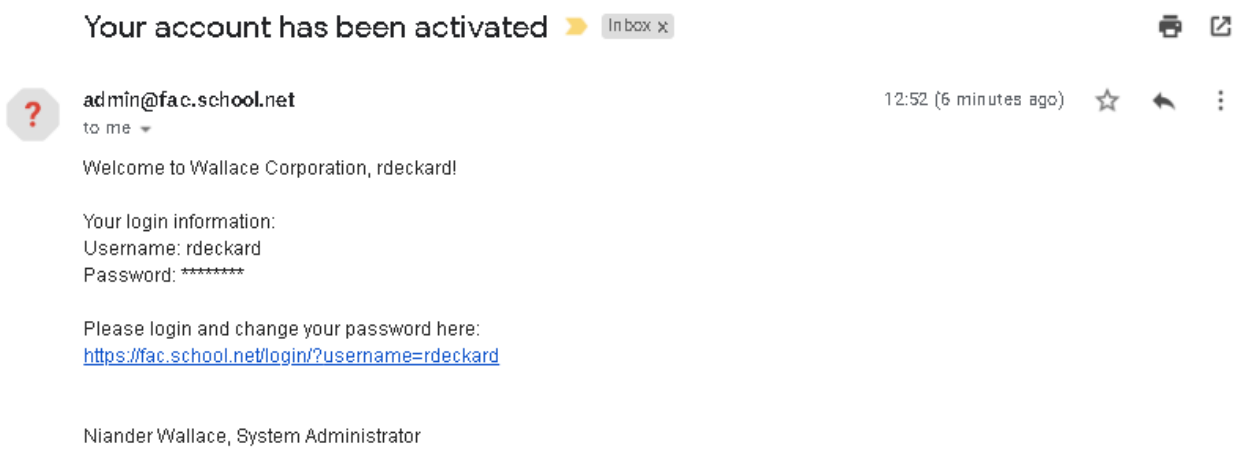
1. When the user visits the login page, *https://<FortiAuthenticator-IP>/auth/register/*, they can click the *Register* button, where they will be prompted to enter their information.
   They will need to enter and confirm a *Username*, *Password*, *First name*, *Last name*, and *Email address*. These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



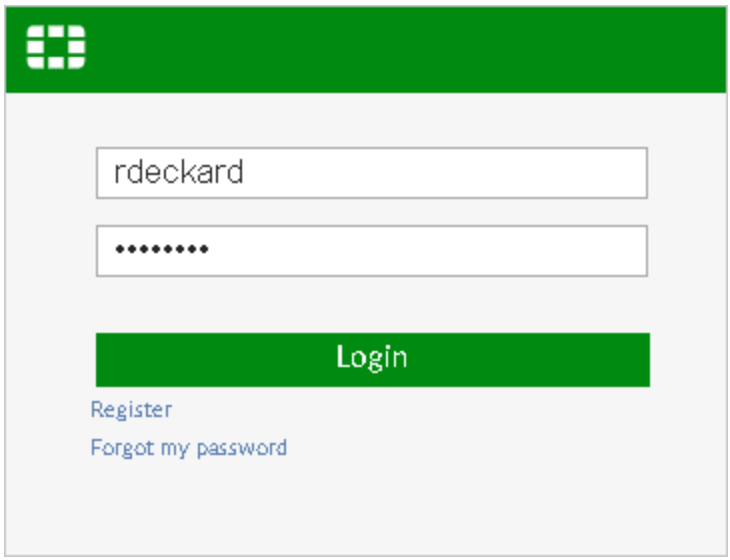
2. The user's registration is successful, and their information has been sent to the administrator for approval.



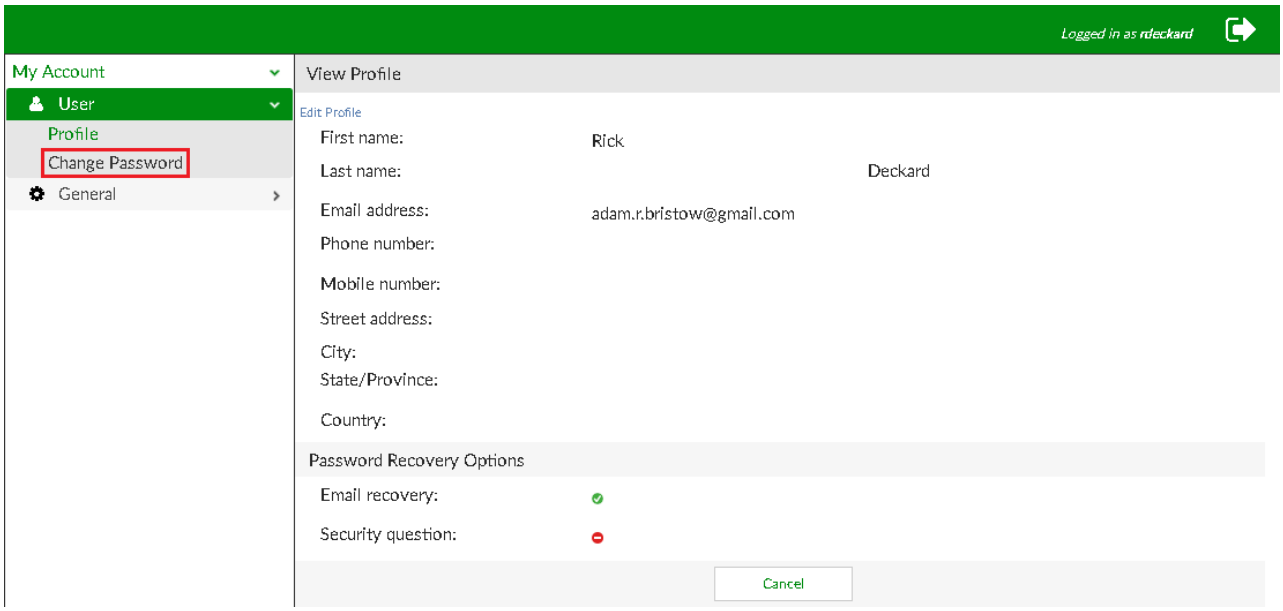
3. When the administrator has enabled the user's account, the user will receive an activation welcome email.
   The user's login information will be listed.



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

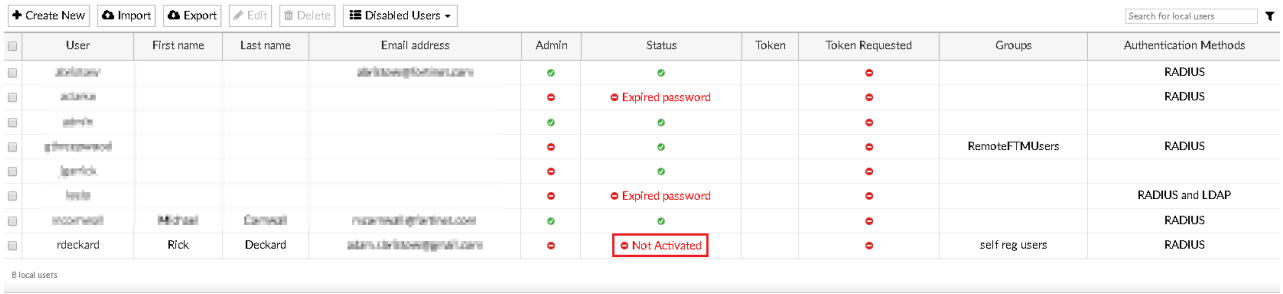


5. The user is now logged into their account where they can review their information.
As recommended in the user's welcome email, the user may change their password. However, this is optional.

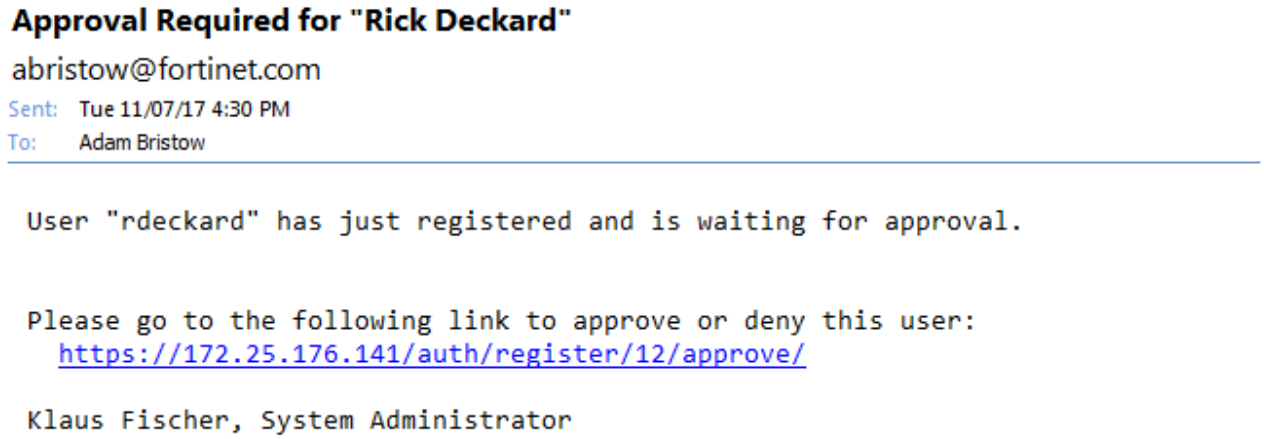


Results - Administrator approval

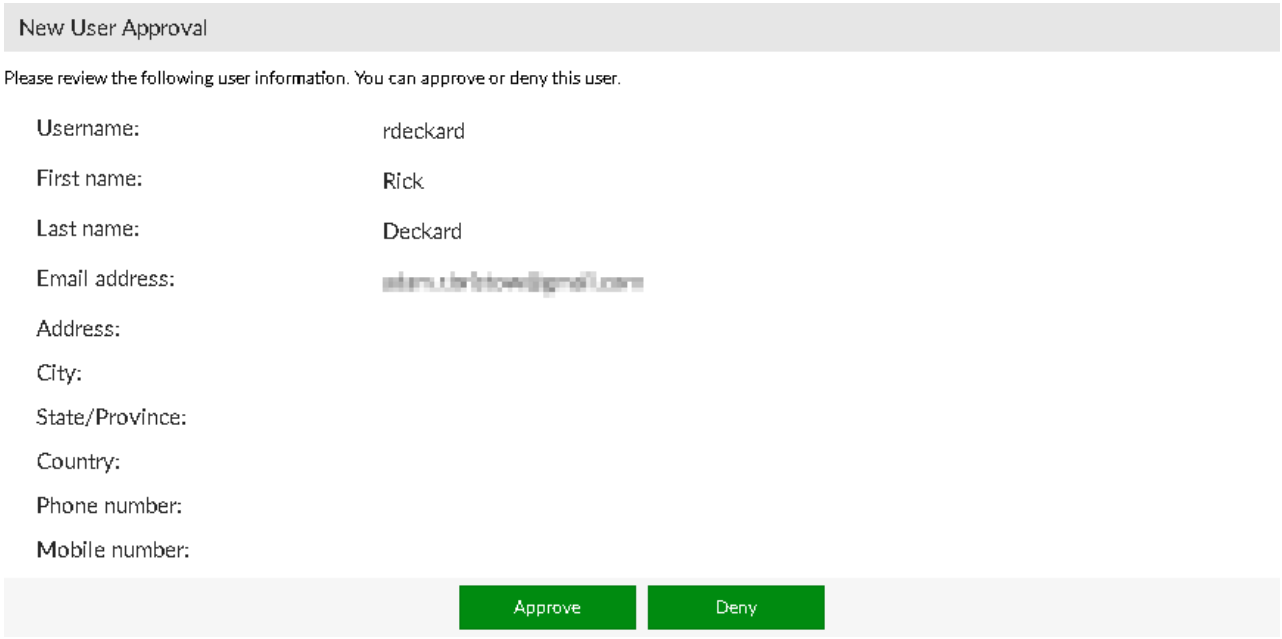
1. After receiving the user's registration request, in the FortiAuthenticator as the administrator, go to *Authentication > User Management > Local Users*. The user has been added, but their *Status* is listed as *Not Activated*.



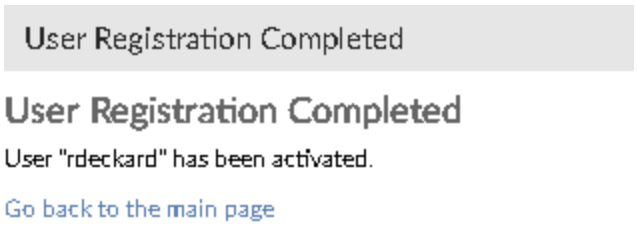
2. In the administrator's email account, open the user's *Approval Required* email. The user's full name will appear in the email's subject, along with their username in the email's body.
Select the link to approve or deny the user.



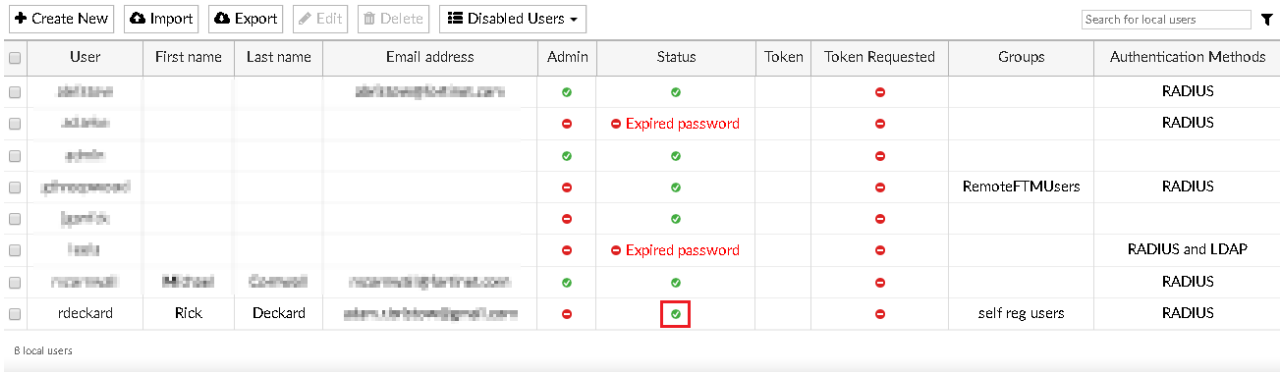
3. The link will take you to the *New User Approval* page, where you can review the user's information and either approve or deny the user's full registration.
Select *Approve*.



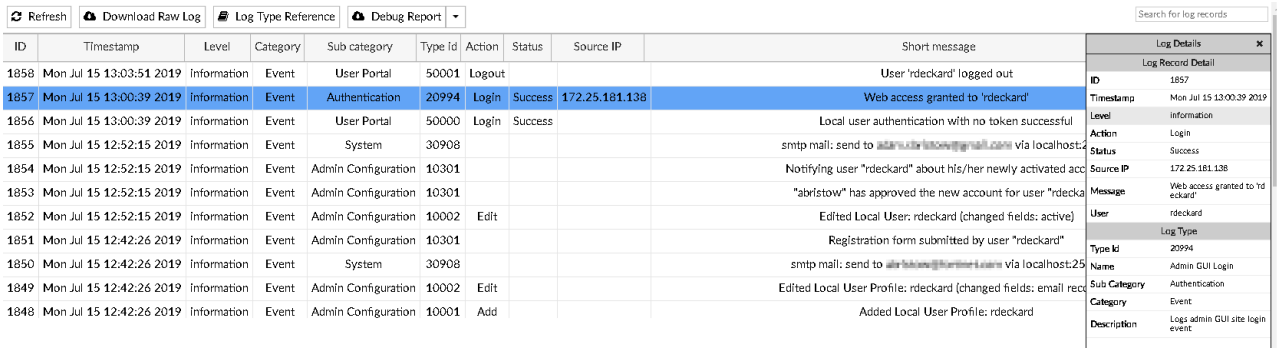
4. The user has now been approved and activated by the administrator.



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



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



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.

To configure computer authentication using FortiAuthenticator with a Microsoft AD Root CA:

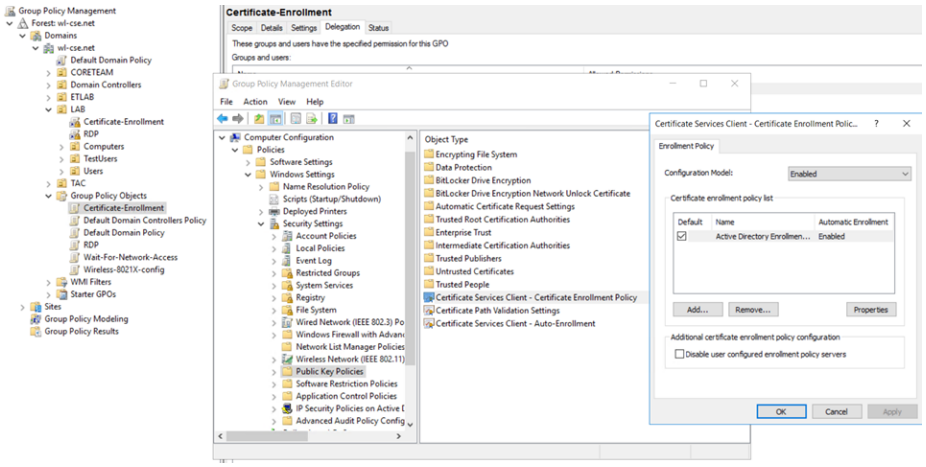
1. Configure the certificates and Root CA on page 76
2. Configure LDAP users on FortiAuthenticator on page 78
3. Configure RADIUS authentication on page 81
4. Creating the SSID on page 87
5. Results on page 88

Configure the certificates and Root CA

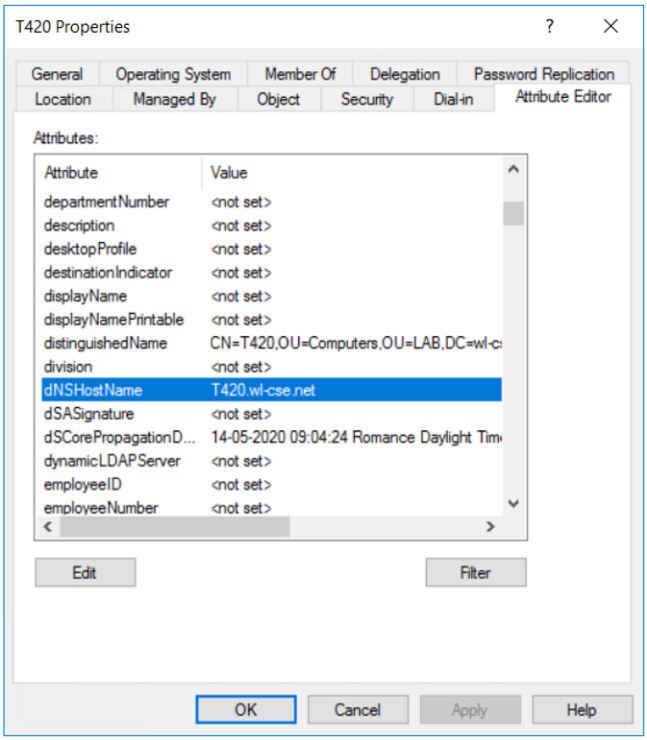
With Microsoft Active Directory as the Root CA, use Group Policy Management to deploy client certificates to domain computers. This is the certificate that will be used to validate RADIUS requests.

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.



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.



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 78
2. Creating a user realm on page 79
3. Creating a user group on page 79
4. Importing users with a remote user sync rule on page 80

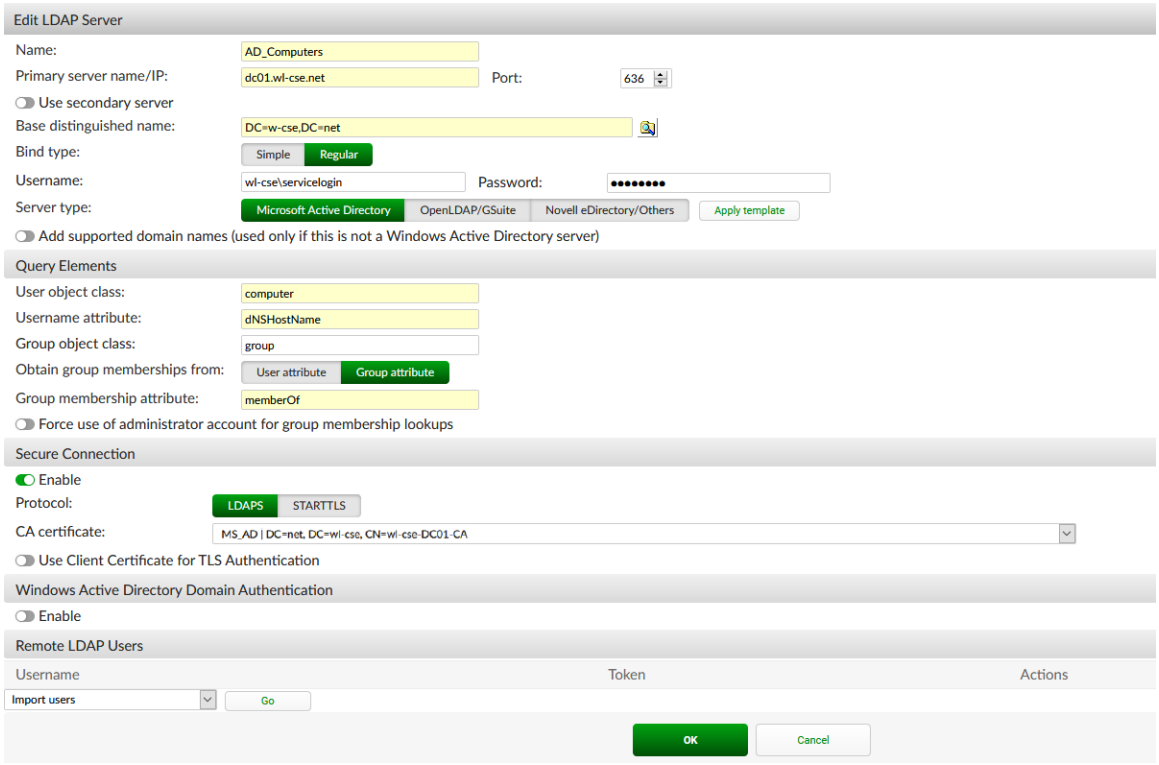
Configuring the LDAP server

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.



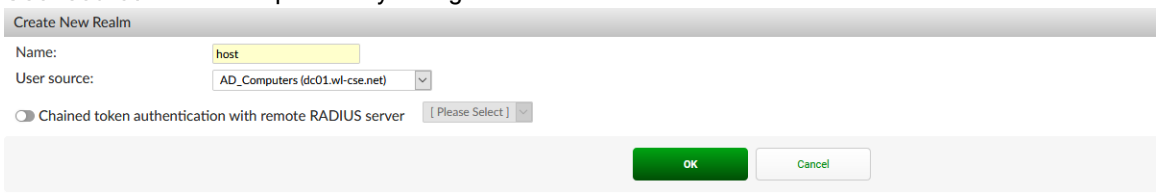
5. Click *OK*.

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.



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*.

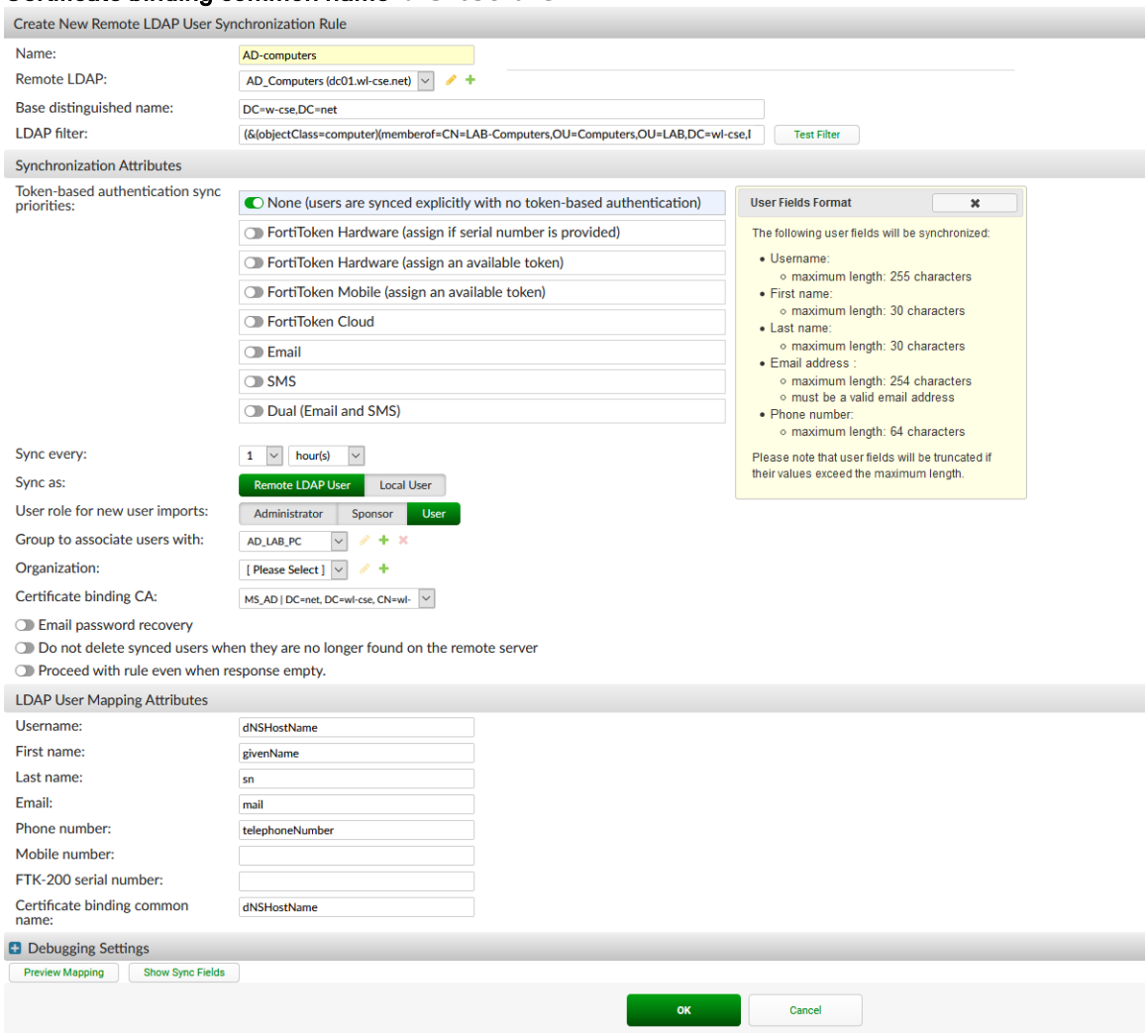
Importing users with a remote user sync rule

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`.



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 82
2. Configuring the RADIUS client on page 82
3. Configuring the EAP server certificate on page 83
4. Creating a RADIUS policy on page 83

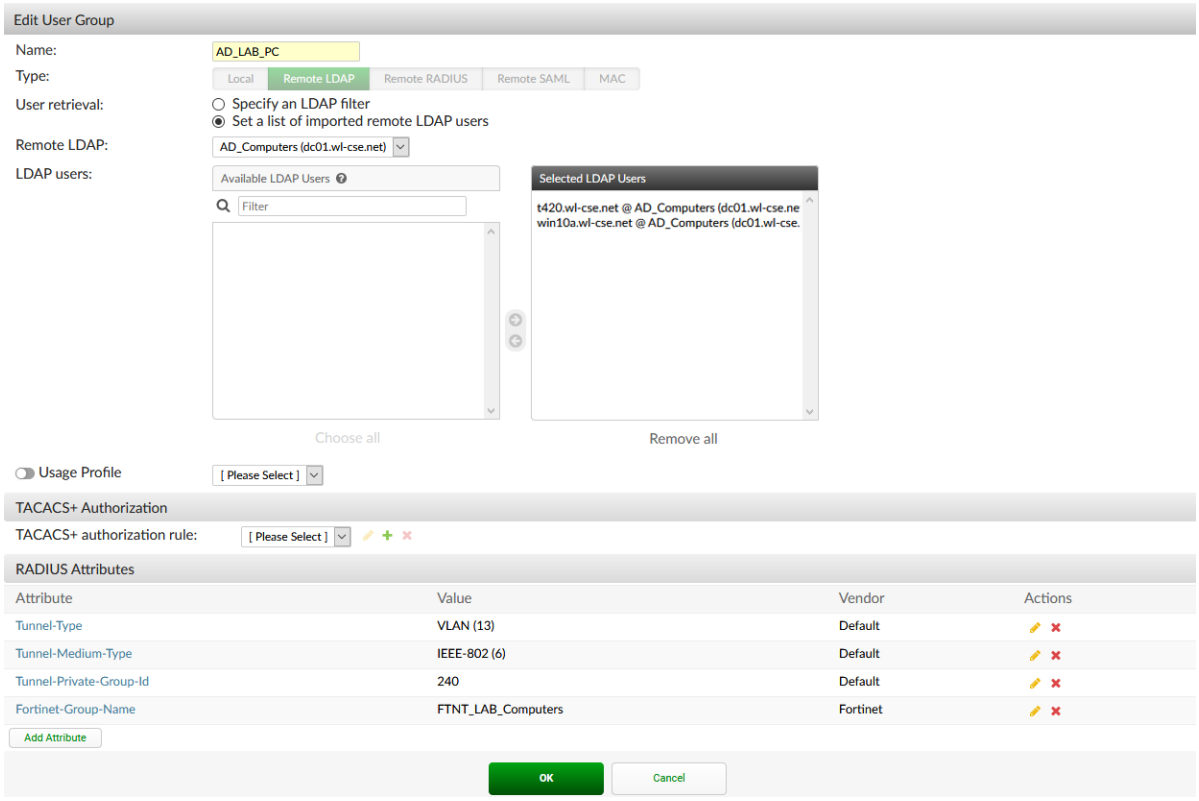
5. Configuring the RADIUS server on FortiGate on page 85

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.

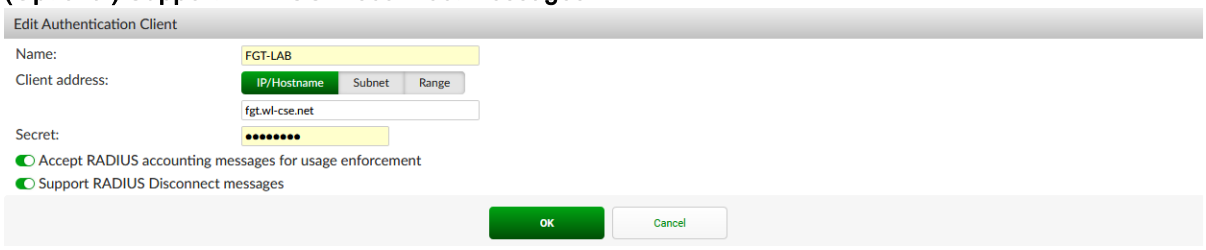


Configuring the RADIUS client

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*.



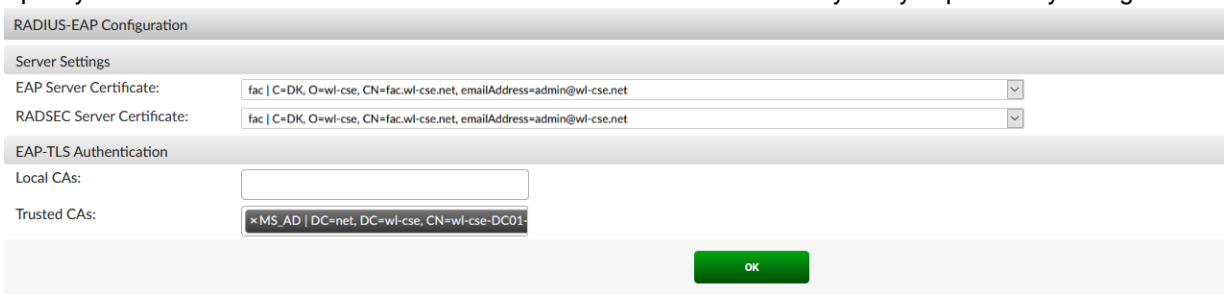
3. Click *OK*.

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.



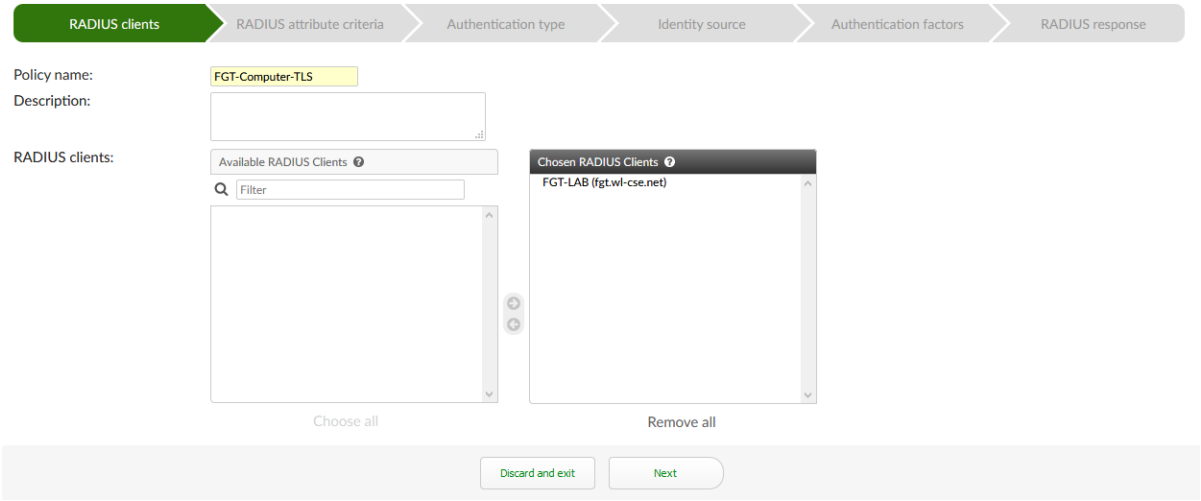
3. Click *OK*.

Creating a RADIUS policy

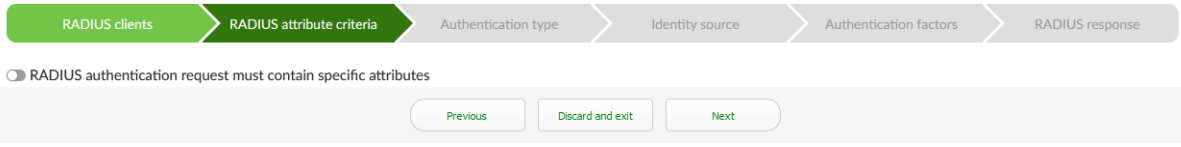
A RADIUS policy must be configured in order to allow RADIUS authentication for the selected client.

To create a RADIUS policy:

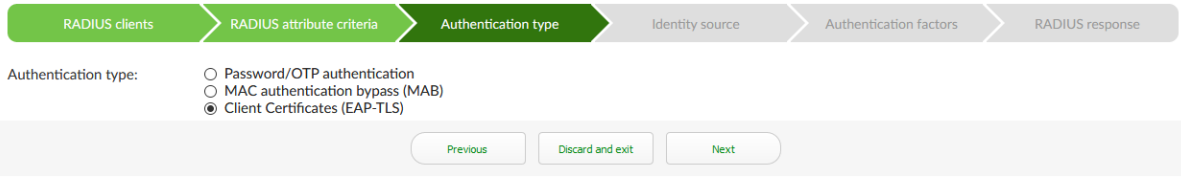
1. Go to *Authentication > RADIUS Service > Policies*, and click *Create New*.
2. Under RADIUS clients, configure the following, and click *Next*.
   a. **Policy name**: Enter a name for this policy, for example: *FGT-Computer-TLS*.
   b. **RADIUS clients**: Add the previously configured FortiGate RADIUS client to the *Chosen RADIUS Clients* section.



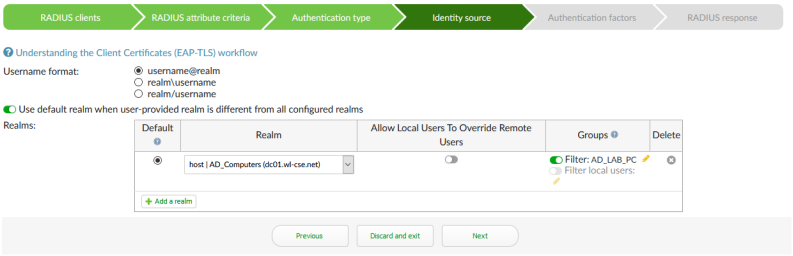
3. Under *RADIUS attribute criteria*, click *Next*.



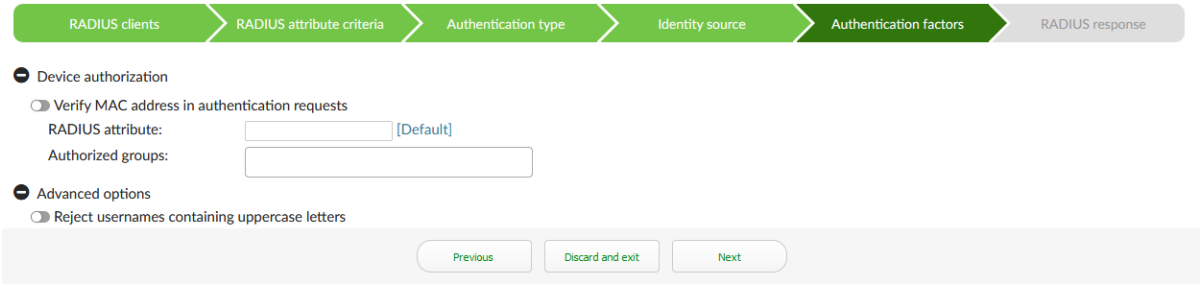
4. Under *Authentication type*, choose *Client Certificates (EAP-TLS)*, and click *Next*.



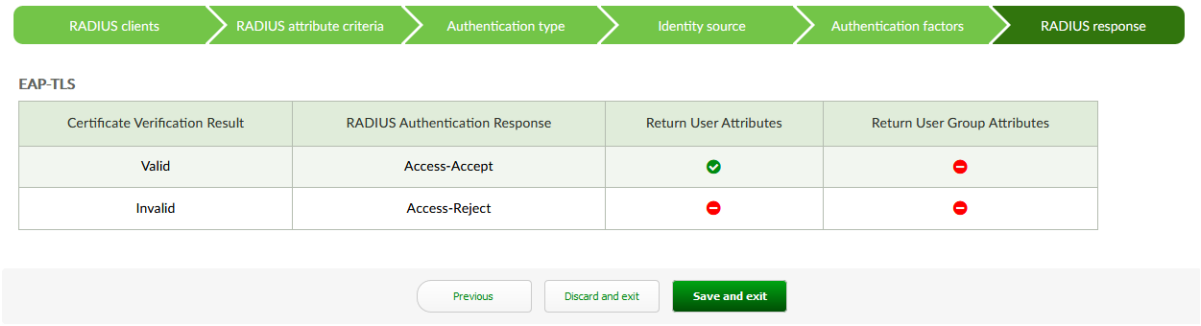
5. Under *Identity source*, configure the following, and click *Next*.
   a. **Username format**: Select your preferred username format, for example: *realm\username*.
   b. **Realms**: In the *Realms* table, select your AD realm.
   To return the RADIUS attributes associated with the group to which the user belongs, the groups need to be added to the group filter list. In this example, add the `AD_LAB_PC` user group previously defined.



6. Under *Authentication factors*, click *Next*.



7. Under *RADIUS response*, click *Save and exit*.



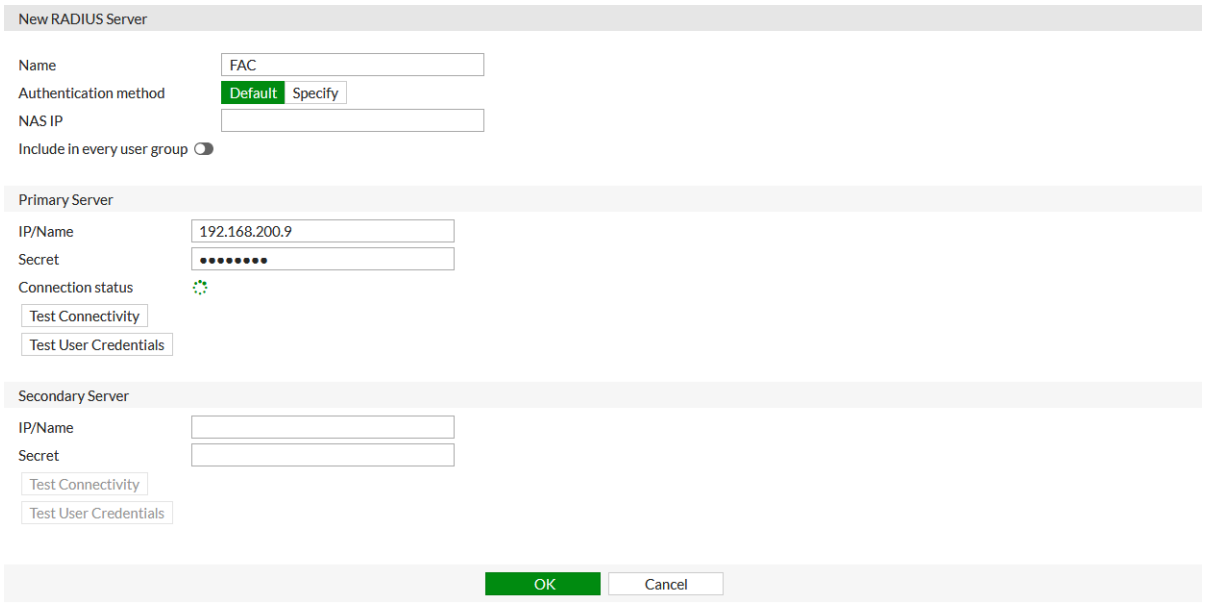
Configuring the RADIUS server on FortiGate

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.



4. Click *OK*.

Configure the SSID and interface objects

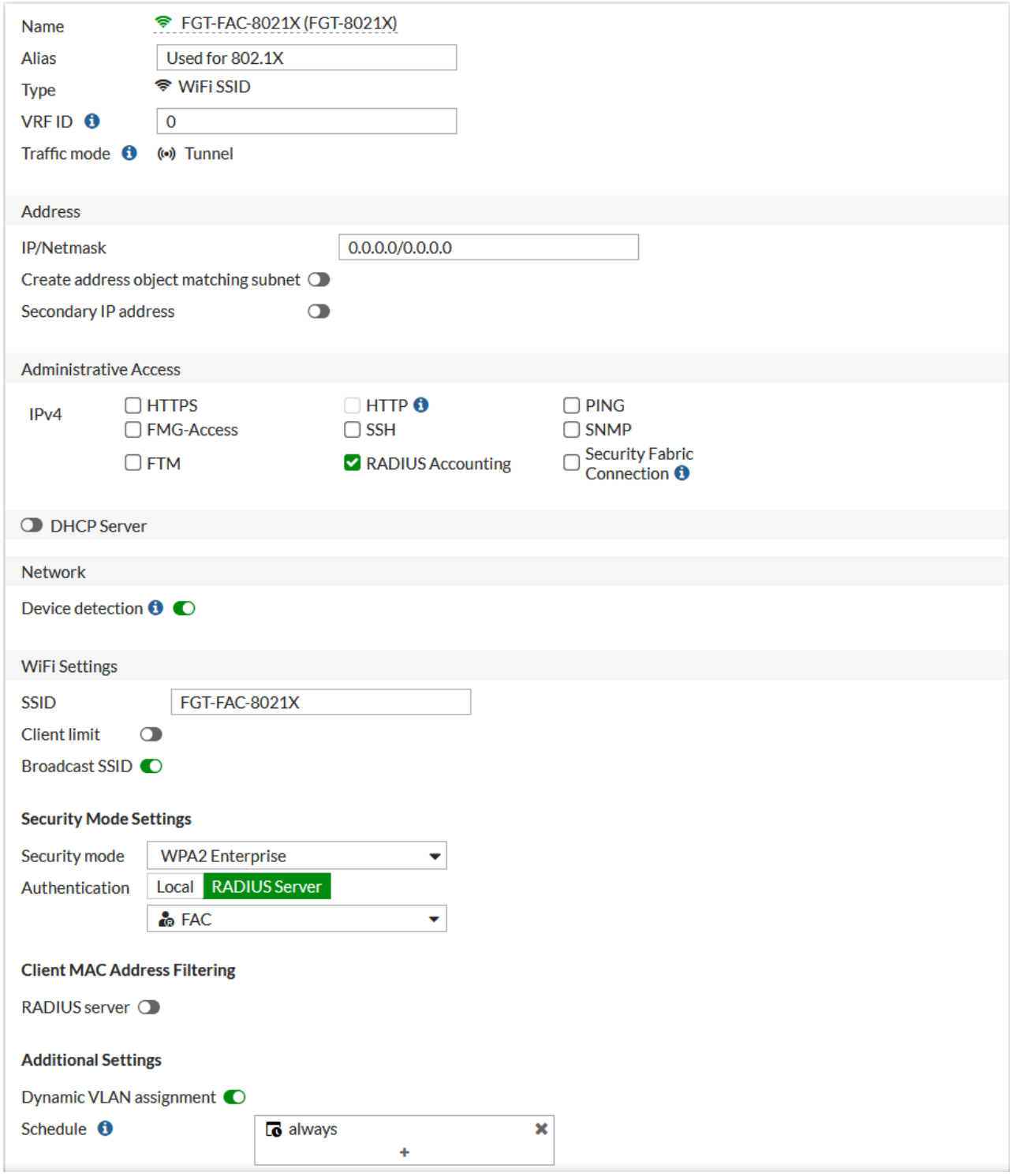
To configure the SSID and interface objects:

1. Creating the SSID on page 87
2. Creating interfaces on page 88

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*.

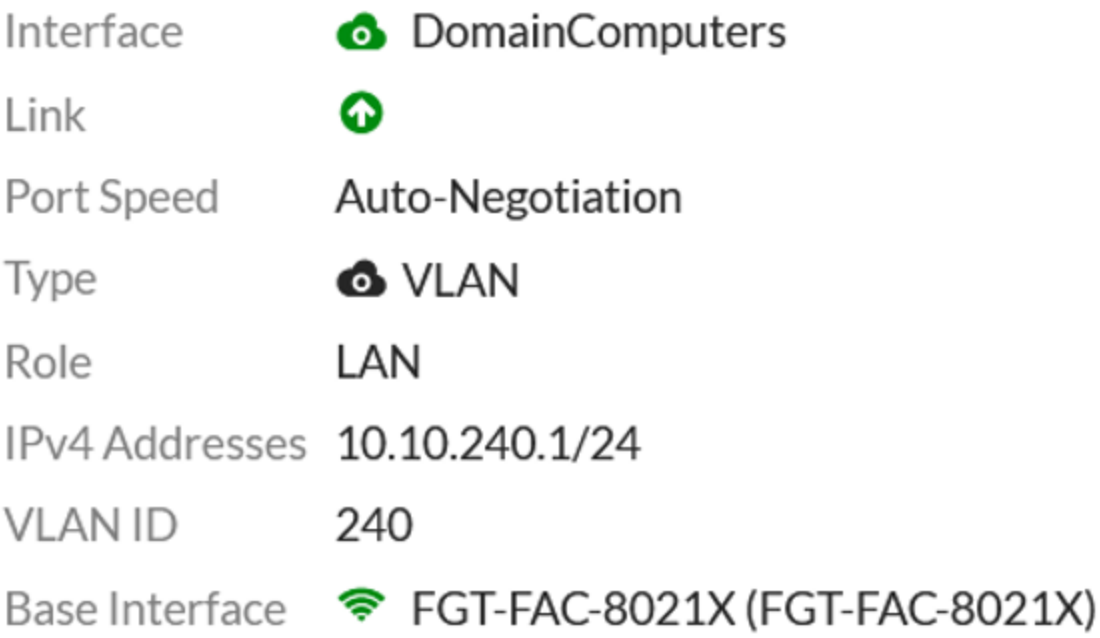


Creating interfaces

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.

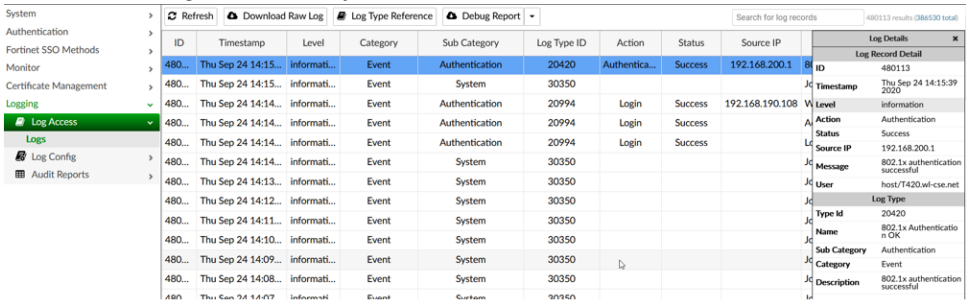


Results

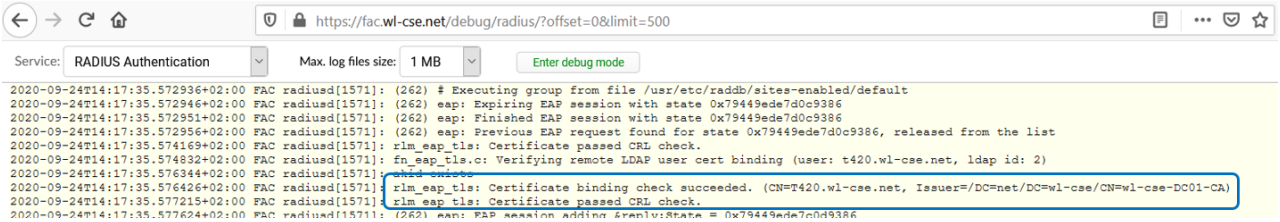
Once the configuration is complete, you should now be able to authenticate your computer using FortiAuthenticator with a Microsoft AD Root CA.

To confirm computer authentication is working as intended:

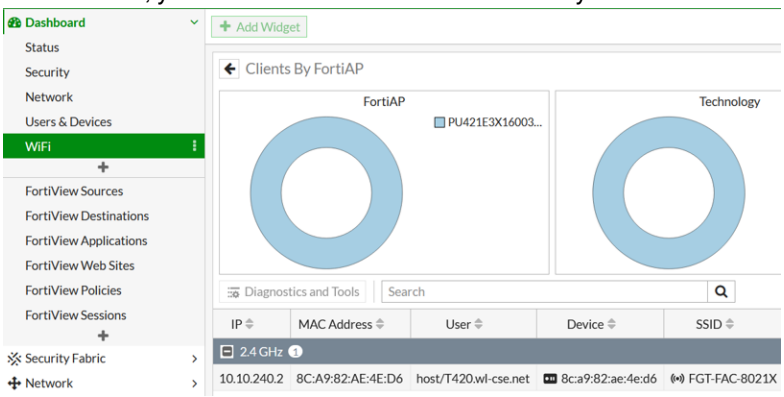
1. When connecting to the client, you can see *Authentication Success* in the FortiAuthenticator logs.



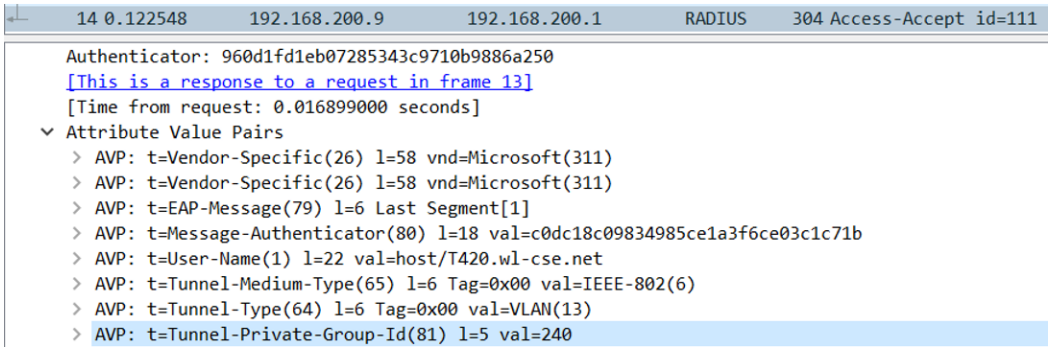
2. When reviewing the debug logs, you can see that certificate binding check has passed.



3. On FortiGate, you can see that the client successfully connected:



4. Packet capture shows the RADIUS-Accept message, including the VLAN 240.



Logging in to FortiGate as an administrator using FIDO2 authentication

For information on FIDO2 authentication, see https://fidoalliance.org/fido2/.

In this example, we will log in to a FortiGate device using FIDO2 authentication method for SAML.

FortiGate acts as the web authentication relying party:

- SAML authentication configured for the admin authentication using FortiAuthenticator as the IdP.

FortiAuthenticator is the web authenticator:

- FortiAuthenticator uses local and remote LDAP users as example.
- FortiAuthenticator is the IdP for FortiGate.

All Fortinet products supporting SAML for authentication can also use FIDO2.

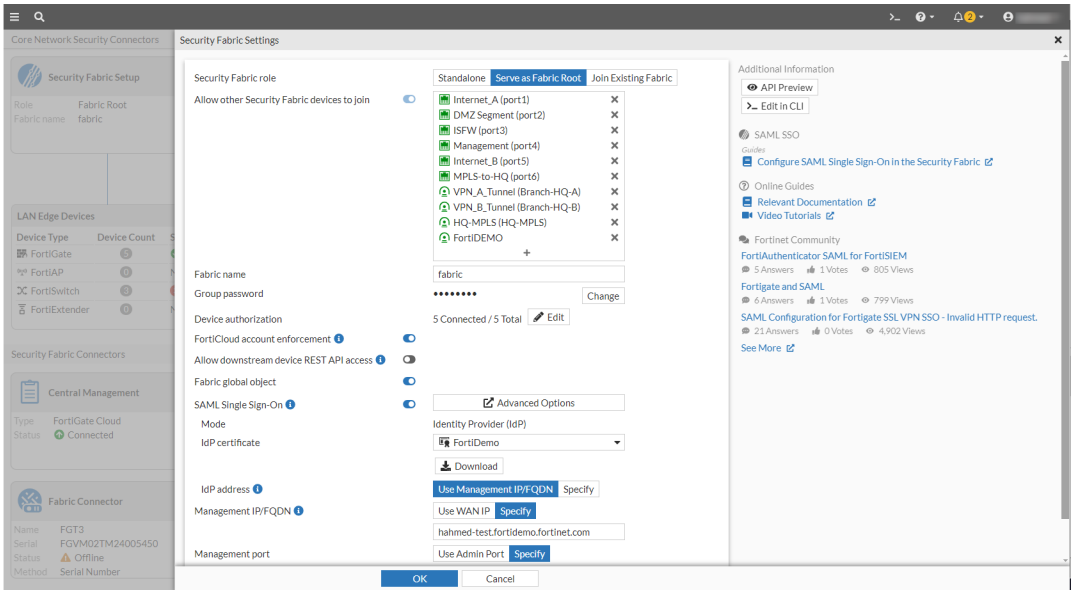
To configure admin login on FortiGate using FIDO2:

1. Configuring SAML on FortiGate on page 90
2. Configuring SAML on FortiAuthenticator on page 92
3. Editing users to set up FIDO authentication on page 93
4. Results on page 95

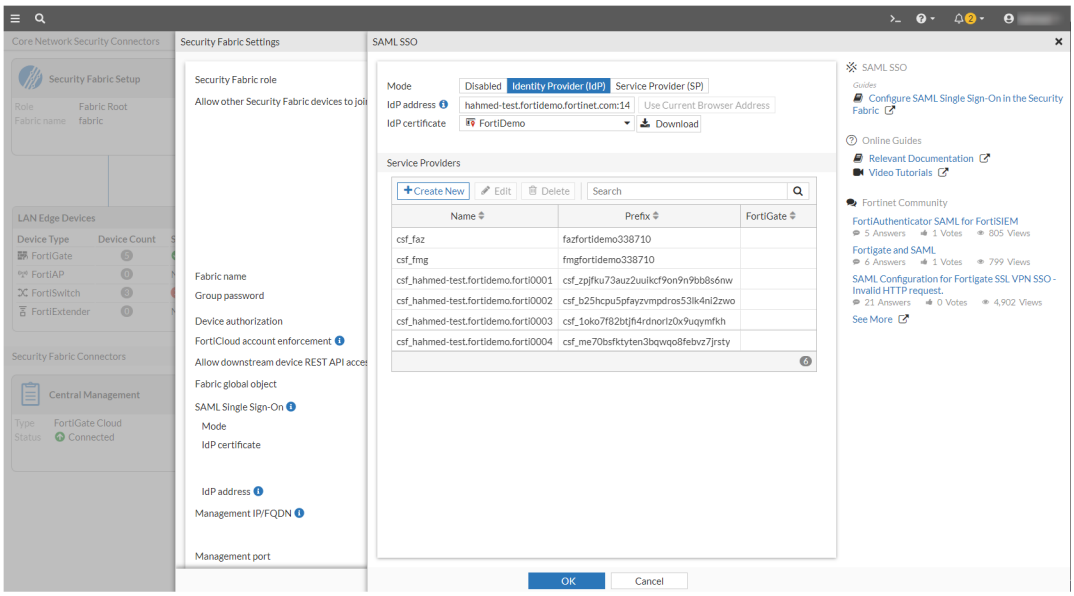
Configuring SAML on FortiGate

To configuring SAML on FortiGate:

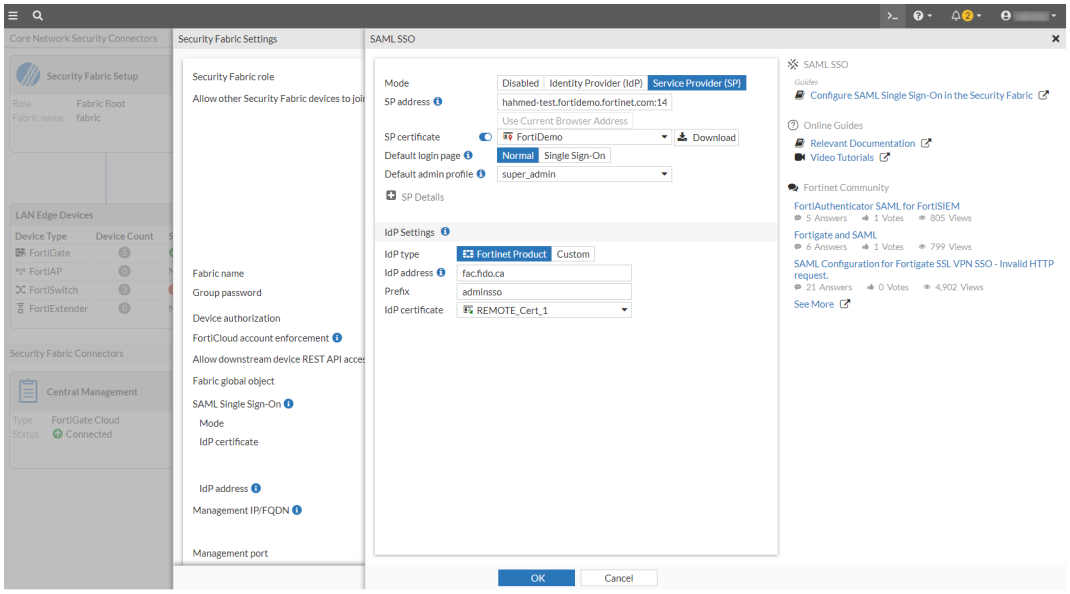
1. Go to *Security Fabric > Fabric Connectors*.
2. Double-click *Security Fabric Setup* to open it.
   The *Security Fabric Settings* window opens.



3. In the *Security Fabric Settings* window, in *SAML Single Sign-On*, click *Advanced Options*.
   A new *SAML SSO* window opens.



4. In the *SAML SSO* window:
   a. In *Mode*, select *Service Provider*.
   b. In *SP address*, ensure that the address is the current browser address.
   c. In *SP certificate* dropdown, select an SP certificate.
   d. In *Default admin profile*, select *super_admin*.
   e. Ensure that *IdP type* is *Fortinet Product*.
   f. In *IdP address*, enter the FQDN for the FortiAuthenticator.
   g. In*Prefix*, enter a prefix.
   h. In the *IdP certificate* dropdown, select the IdP certificate.

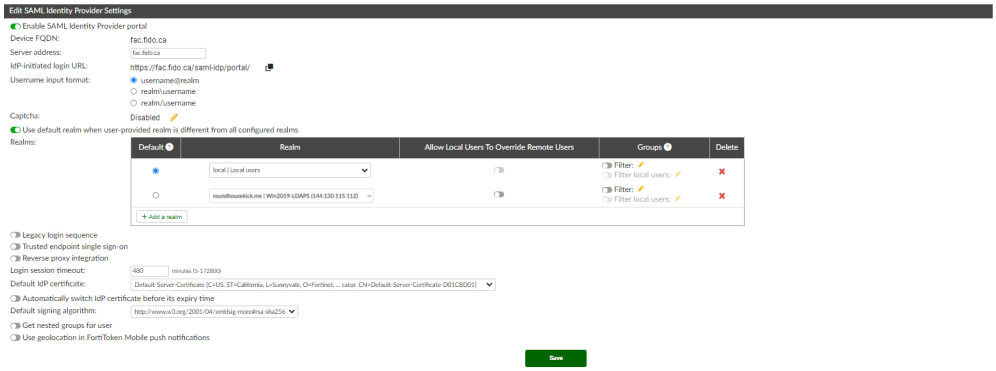


5. Click *OK*.
6. Click *OK*.

Configuring SAML on FortiAuthenticator

To configure SAML general settings on FortiAuthenticator:

1. Go to *Authentication > SAML IdP > General*, and select *Enable SAML Identity Provider portal*.
2. In *Server address*, enter the FQDN for FortiAuthenticator.
3. Enable *Use default realm when user-provided realm is different from all configured realms*.
4. In *Realms*, add realms.
5. Click *Save*.

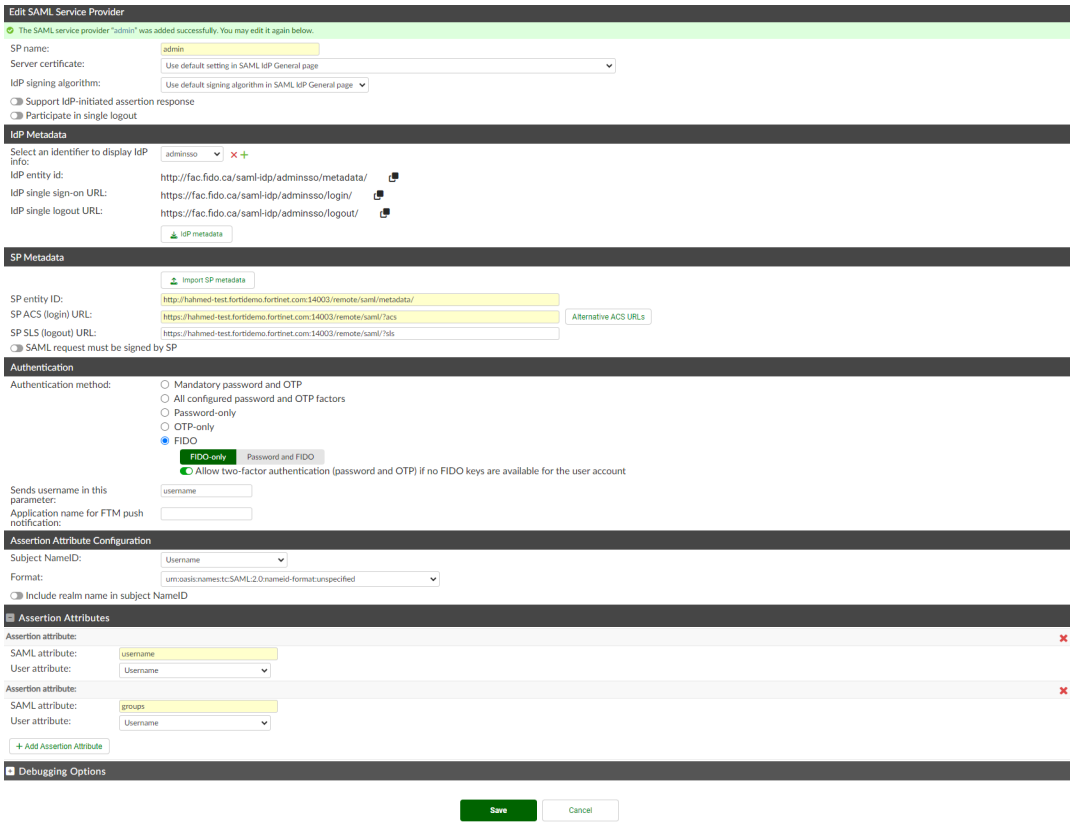


To configure SAML SP settings on FortiAuthenticator:

Here, we add FortiGate SP settings to FortiAuthenticator.

1. Go to *Authentication > SAML IdP > Service Providers*, and select *Create New*.
   The *Create New SAML Service Provider* window opens.
2. In *SP name*, enter the a name for the SP.
3. In *Create an identifier for this IdP*, select *+*, in the *Create an Alternate indentifier* window, enter the same identifier used as the prefix in IdP settings in Configuring SAML on FortiGate on page 90, and click *OK*.
4. In *Authentication method*, select *FIDO*.
   Ensure that *FIDO-only* is selected and *Allow two-factor authentication (password and OTP) if no FIDO keys are available for the user account* is enabled.
5. In *Assertion Attribute Configuration*, keep the default settings.
6. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. In *SAML attribute*, enter `username`.
   b. In the *User attribute* dropdown, select *Email*.
7. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. In *SAML attribute*, enter `groups`
   b. In the *User attribute* dropdown, select *Group*.
8. Click *Save*.
   The *Edit SAML Service Provider* window opens.
9. In the *SP Metadata* pane:
   a. In *SP entity IP*, paste the *Entity ID* from FortiGate.
   b. In *SP ACS (login) URL*, paste *Assertion consumer service URL* from FortiGate.
   c. In *SP SLS (logout) URL*, paste S*ingle logout service URL* from FortiGate.

10. Click *Save*.



Editing users to set up FIDO authentication

To edit a local user to set up FIDO authentication:

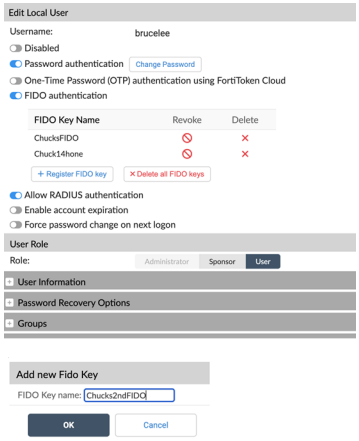
1. Go to *User Management > Local Users*.
2. From the list double-click a local user to edit it.
   The *Edit Local User* window opens.
   If you need to create a new local user, see Local users in the latest *FortiAuthenticator Administration Guide*.
3. Enable *FIDO authentication*.
4. Select *Register FIDO key*.
   The *Add new FIDO Key* window opens.
5. Enter a key name in *FIDO Key name*.
6. Click *OK*.
7. In the *Verify your identity* dialog that appears, select *USB security key*, push the button on the FortiToken 410 (FIDO client) physical device.

   OR

   If using a Mac device, in the *Verify your identity dialog* that appears, select *This device*, register your fingerprint using the *Touch ID* button.

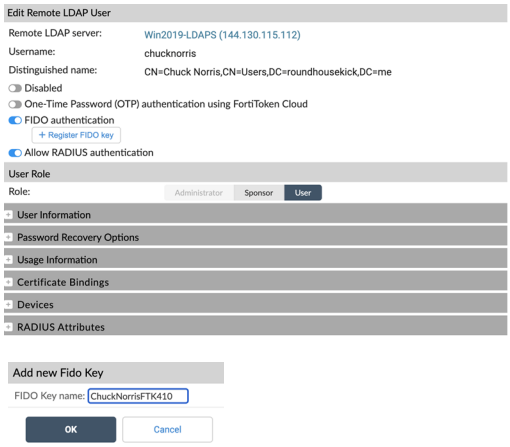
   The FIDO key registration is complete.

8. Click *Save*.



To edit an LDAP user to set up FIDO authentication:

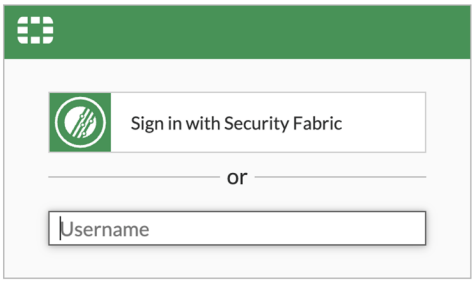
1. Go to *User Management > Remote Users* and select the LDAP tab.
2. From the list, double-click an LDAP user to edit it.
   The *Edit Remote LDAP User* window opens.
   If you need to import a new remote user, see Remote users in the latest *FortiAuthenticator Administration Guide*.
3. Enable *FIDO authentication*.
4. Select *Register FIDO key*.
   The *Add new FIDO Key* window opens.
5. Enter a key name in *FIDO Key name*.
6. Click *OK*.
7. Follow step 7 from Editing a local user to set up FIDO authentication.
8. Click *Save*.



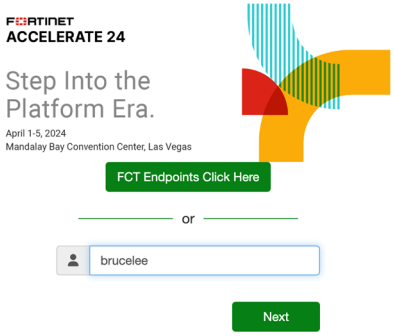
Users can self-provision using a self-service portal.

Results

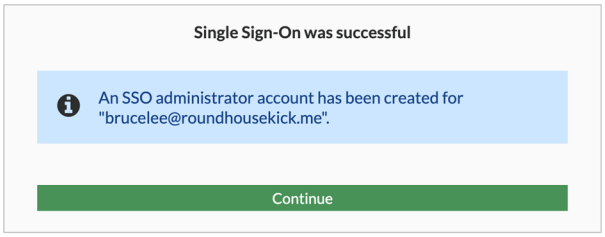
1. On the web browser, go to the FortiGate GUI.
2. Select *Sign in with Security Fabric*.



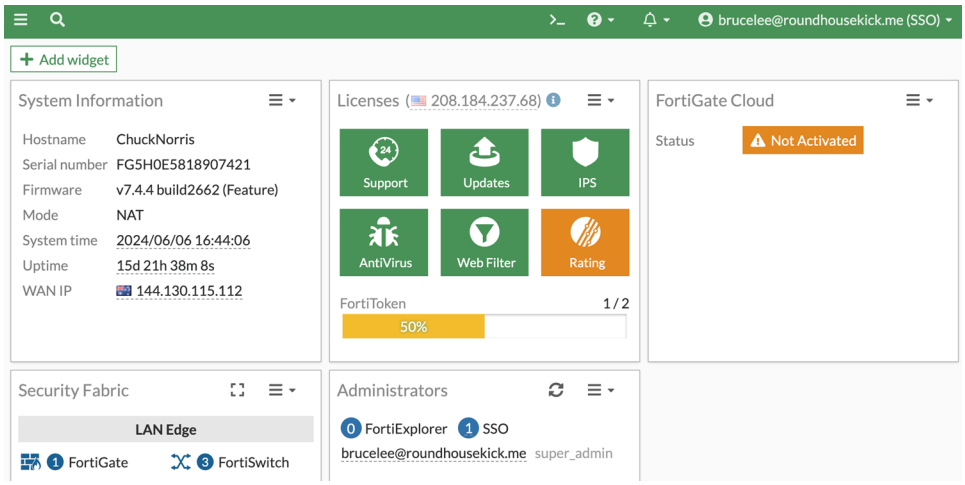
3. In the IdP login screen, enter the user name and click *Next*.



4. In the *Verify your identity* dialog that appears, select *USB security key*, push the button on the FortiToken 410 physical device.
   If this is the first login, the user account is created.
5. Click *Continue*.



You are now logged in to the FortiGate GUI.



Configuring FIDO2 authentication for Agentless VPN

For information on FIDO2 authentication, see https://fidoalliance.org/fido2/.

In this example, we set up an Agentless VPN tunnel that uses FIDO2 authentication.

A FortiToken 410 physical device is used to perform FIDO2 authentication.

FortiAuthenticator is the IdP for FortiGate.

To configure FIDO2 authentication for Agentless VPN:

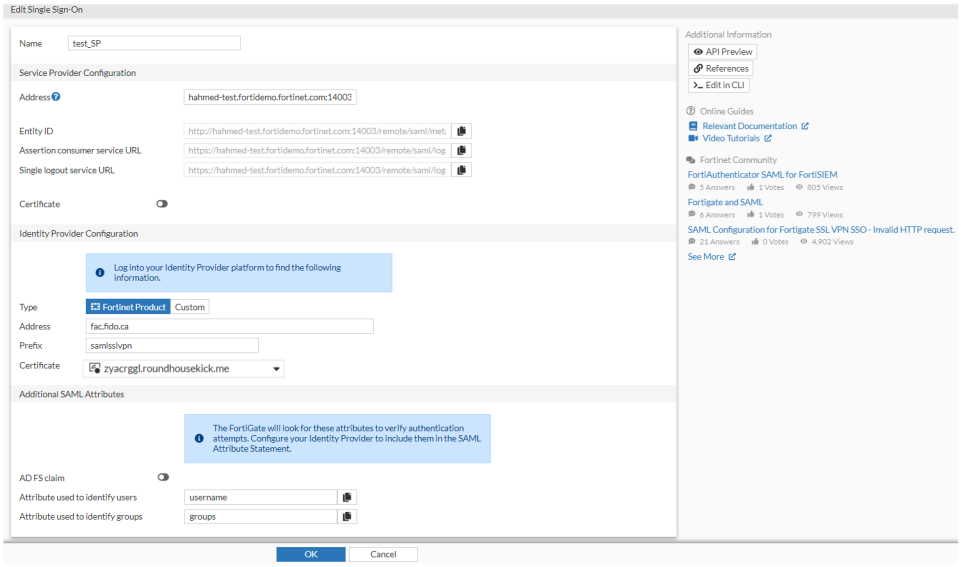
1. Configuring SAML SP on FortiGate on page 96
2. Configuring SAML IdP general settings on FortiAuthenticator on page 97
3. Configuring SP settings on FortiAuthenticator on page 98
4. Editing users to set up FIDO authentication on page 99
5. Creating a user group with the SAML SSO server on page 100
6. Configuring Agentless VPN on FortiGate on page 100
7. Creating a firewall policy for Agentless VPN traffic on page 102
8. Configuring Agentless VPN on FortiClient on page 102
9. Results on page 103

Configuring SAML SP on FortiGate

To configure SAML SP on FortiGate:

1. Go to *User & Authentication* > *Single Sing-On*, and select *Create new*.
   A *New Single Sign-On* wizard opens.
2. In *Name*, enter the name for the SP.
3. Click *Next*.
4. In the *Service Provider Configuration*:
   a. In *Address*, keep the FQDN of the SP (FortiGate).

5. In *Identity Provider Details*:
   a. In *Type*, select *Fortinet Product*.
   b. In *Address*, enter the FQDN of the IdP (FortiAuthenticator).
   c. In *Prefix*, enter a prefix.
   d. In the *Certificate* dropdown, select a certificate.
   If required, click *+* to import a certificate.
6. In the *Additional SAML Attributes* pane:
   a. In *Attribute used to identify users*, enter `username`.
   b. In *Attribute used to identify groups*, enter `groups`.
7. Click *Submit*.



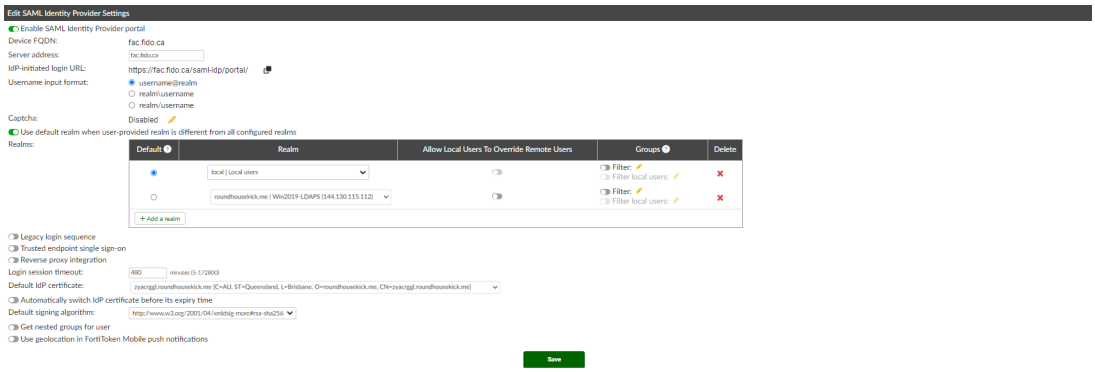
8. Double-click the recently created SP to open it.
9. In the *Service Provider Configuration* pane, copy and save *Entity ID*, *Assertion consumer service URL*, and *Single logout service URL* as a text file on your management computer. This is needed when configuring SP settings on FortiAuthenticator.
   See step 9 in Configuring SP settings on FortiAuthenticator on page 98.

Configuring SAML IdP general settings on FortiAuthenticator

To configure SAML IdP on FortiAuthenticator:

1. Go to *Authentication > SAML IdP > General*, and select *Enable SAMLIdentity Provider portal*.
2. In *Server address*, enter the FQDN address of the FortiAuthenticator.
3. Enable *Use default realm when user-provided realm is different from all configured realms*.
4. In *Realms*, add realms.
5. In *Default IdP certificate* dropdown, select the same certificate as in step `5-d` of Configuring SAML SP on FortiGate on page 96.

6. Click *Save*.

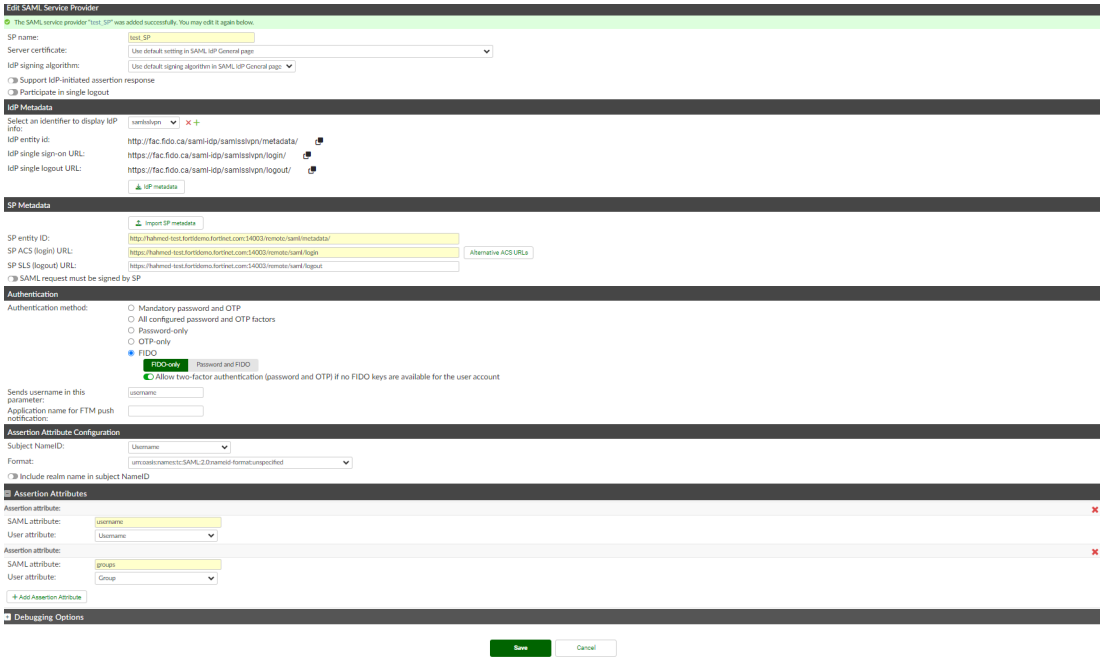


Configuring SP settings on FortiAuthenticator

To configure SP settings on FortiAuthenticator:

1. Go to *Authentication> SAML IdP > Service Providers*, and select *Create New*.
   The *Create New SAML Service Provider* window opens.
2. In *SP name*, enter the name of the SP.
3. In *Create an identifier for this IdP*, select *+*, in the *Create an Alternate indentifier* window, enter the same identifier used as the prefix in IdP settings in Configuring SAML SP on FortiGate on page 96, and click *OK*.
4. In *Authentication method*, select *FIDO*.
   Ensure that *FIDO-only* is selected and *Allow two-factor authentication (password and OTP) if no FIDO keys are available for the user account* is enabled.
5. In *Assertion Attribute Configuration*, keep the default settings.
6. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. In *SAML attribute*, enter `username`.
   b. In the *User attribute* dropdown, select *Email*.
7. In *Assertion Attributes*, select *Add Assertion Attribute*:
   a. In *SAML attribute*, enter `groups`
   b. In the *User attribute* dropdown, select *Group*.
8. Click *Save*.
   The *Edit SAML Service Provider* window opens.
9. From the text file that you saved in step 9 in Configuring SAML SP on FortiGate on page 96, in the *SP Metadata* pane on FortiAuthenticator:
   a. In *SP entity ID*, paste the *Entity ID* from FortiGate.
   b. In *SP ACS (login) URL*, paste *Assertion consumer service URL* from FortiGate.
   c. In *SP SLS (logout) URL*, paste *Single logout service URL* from FortiGate.

10. Click *Save*.



Editing users to set up FIDO authentication

To edit a local user to set up FIDO authentication:

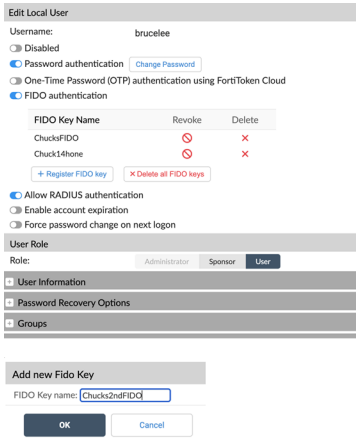
1. Go to *User Management* > *Local Users*.
2. From the list double-click a local user to edit it.
   The *Edit Local User* window opens.
   If you need to create a new local user, see Local users in the latest *FortiAuthenticator Administration Guide*.
3. Enable *FIDO authentication*.
4. Select *Register FIDO key*.
   The *Add new FIDO Key* window opens.
5. Enter a key name in *FIDO Key name*.
6. Click *OK*.
7. In the *Verify your identity* dialog that appears, select *USB security key*, push the button on the FortiToken 410 (FIDO client) physical device.

   OR

   If using a Mac device, in the *Verify your identity dialog* that appears, select *This device*, register your fingerprint using the *Touch ID* button.

   The FIDO key registration is complete.

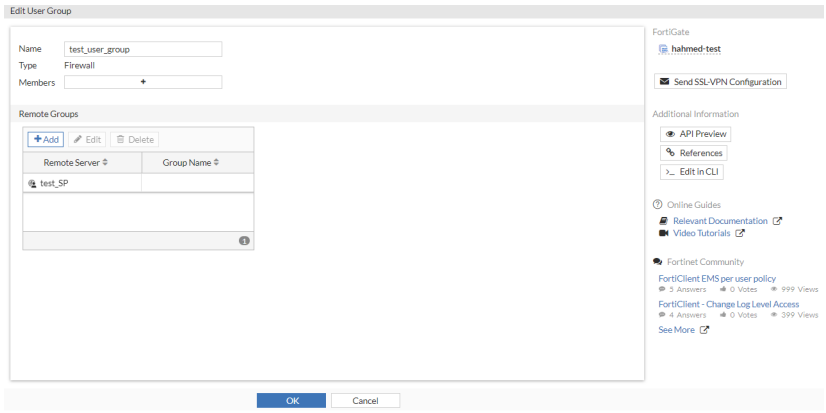
8. Click *Save*.



Creating a user group with the SAML SSO server

To create a user group:

1. Go to *User & Authentication* > *User Groups*, and select *Create New*.
   The *New User Group* window opens.
2. In *Name*, enter a name for the user group.
3. In *Type*, select *Firewall*.
4. In the *Remote Groups* pane, select *Add*:
   The *Add Group Match* window opens.
   a. In *Remote Server*, select the SSO server created in Configuring SAML SP on FortiGate on page 96.
   b. Click *OK*.
5. Click *OK*.

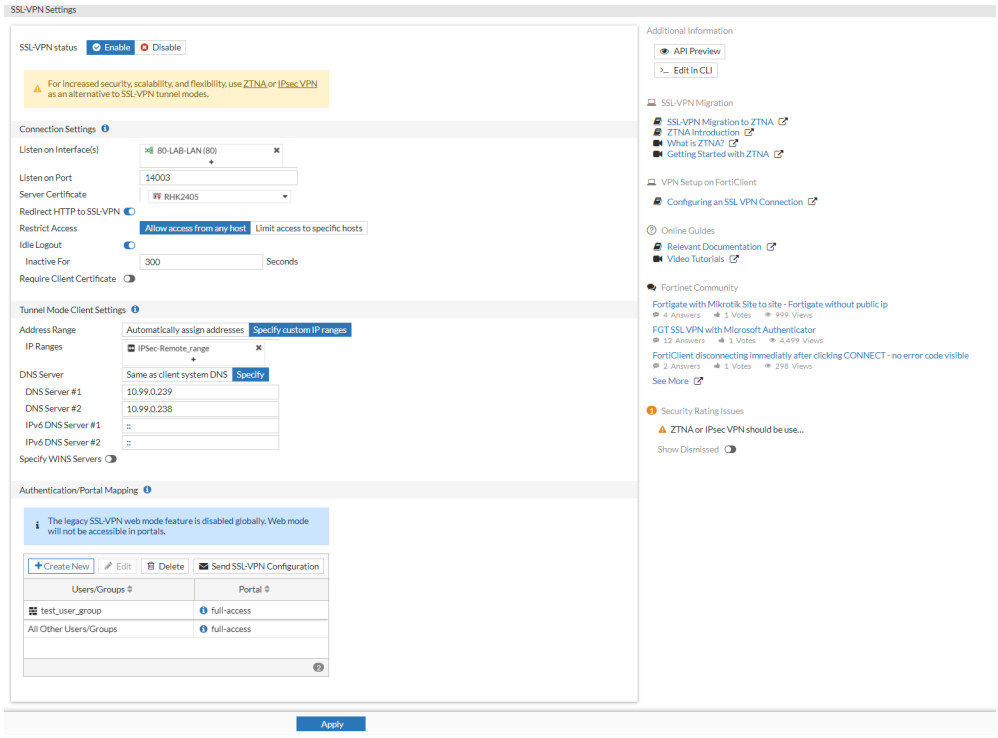


Configuring Agentless VPN on FortiGate

To configure Agentless VPN on FortiGate:

1. Go to *System* > *Feature Visibility*.
2. Enable *Agentless VPN*.

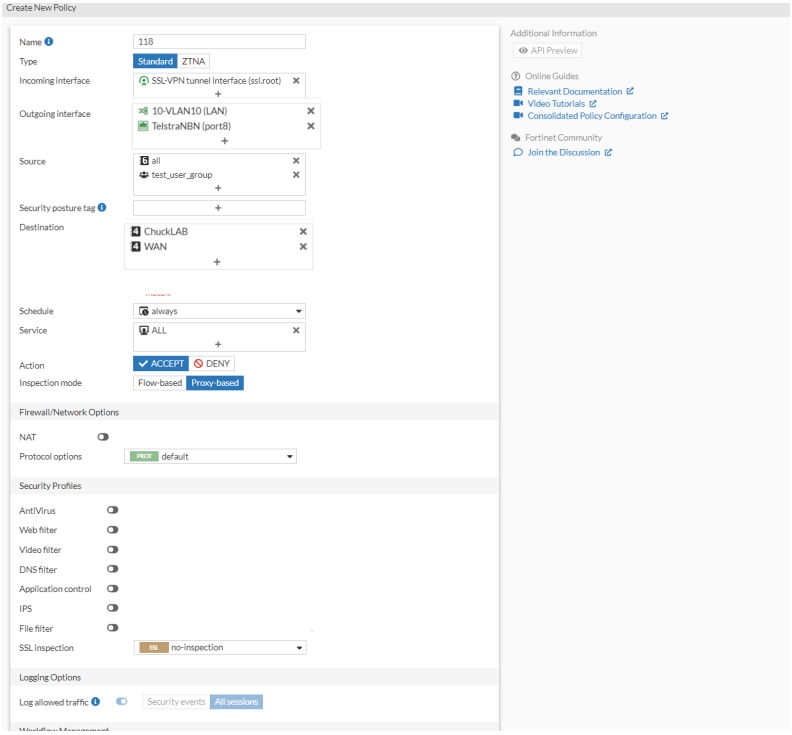
3. Click *Apply*.
   New Agentless VPN related tabs are now ready to be configured in *VPN*.
4. Go to *VPN > Agentless VPN Settings*.
5. In *Listen on Port*, enter *14003*.
   This is the same port appended to the WAN accessible FQDN for the SP (FortiGate).
   See Configuring SAML SP on FortiGate on page 96.
   This port number will be used when configuring FortiClient.
   See Configuring Agentless VPN on FortiClient on page 102.
6. In the *Server Certificate* dropdown, select a server certificate.
7. Enable *Redirect HTTP to Agentless VPN*.
8. In *Restrict Access*, select *Allow access from any host*.
9. In *Address Range*, select *Specify custom IP ranges*.
10. In *IP Ranges*, add IP address ranges.
11. In *DNS Server*, select *Specify*.
12. Enter IP addresses for DNS servers in *DNS Server #1* and *DNS Server #2*.
13. In the *Authentication/Portal Mapping* pane, select *Create New*.
    The *New Authentication/Portal Mapping* window opens.
    a. In *Users/Groups*, select *+*, from the *Select Entries* list, select the user group created in Creating a user group with the SAML SSO server on page 100, and click *Close*.
    b. In the *Portal* dropdown, select *full-access*.
    c. Click *OK*.
14. Click *Apply*.



Creating a firewall policy for Agentless VPN traffic

To configure a firewall policy:

1. Go to *Policy & Objects* > *Firewall Policy*, and select *Create new*.
   The *Create New Policy* window opens.
2. In the *Settings* tab:
   a. In *Name*, enter a name for the firewall policy.
   b. In *Type*, select *Standard*.
   c. In *Incoming interface*, select *+*, from the *Select Entries* list, select an incoming interface, and click *Close*.
   d. In the *Outgoing interface*, select *+*, from the *Select Entries* list, select outgoing interfaces, and click *Close*.
   e. In *Source*:
      i. Select *+*, from the *Select Entries* list, select *all*.
      ii. From the dropdown, select *User*, select the user group created in Creating a user group with the SAML SSO server on page 100, and click *Close*.
   f. In *Destination*, select *destinations*.
   g. In *Service*, select *+*, from the *Select Entries* list, select *ALL*, and click *Close*.
   h. In *Inspection mode*, select *Proxy-based*.
   i. Disable *NAT*.
3. Click *OK*.

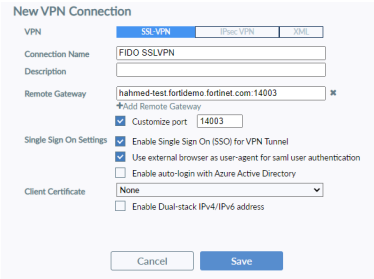


Configuring Agentless VPN on FortiClient

Since the FortiClient mini browser does not support FIDO2, you must use an external browser for FIDO2 authentication.

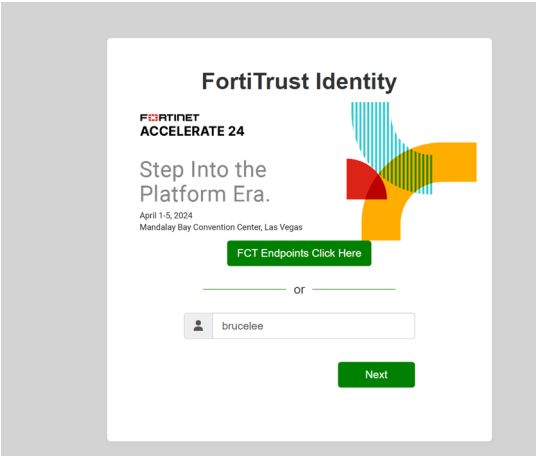
To configure Agentless VPN on FortiClient:

1. Open the FortiClient console.
2. Go to *REMOTE ACCESS* and from the *More Options* icon, select *Add a new connection*.
   The *New VPN Connection* window opens.
3. In *Connection Name*, enter a name.
4. In *Remote Gateway*, enter FQDN from the *Address* field in Configuring SAML SP on FortiGate on page 96.
5. Select *Customize port* and enter the same port number as used in step 5 in Configuring Agentless VPN on FortiGate on page 100.
6. Select *Enable Single Sign On (SSO) for VPN Tunnel* and *Use external browser as user-agent for saml user authentication*.
7. Click *Save*.

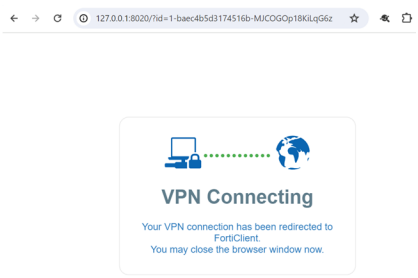


Results

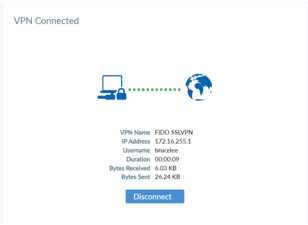
1. On the FortiClient console, go to REMOTE ACCESS.
2. From the dropdown, select the VPN connection created in Configuring Agentless VPN on FortiClient on page 102.
3. Select *Connect*.
   The default web browser is automatically launched by FortiClient.
4. On the FortiAuthenticator login page that open, enter the user name, and click *Next*.



5. In the *Verify your identity* dialog that appears, select *USB security key*, push the button on the FortiToken 410 physical device.
   The web browser completes the authentication and responds to FortiClient.



FortiClient completes the Agentless VPN tunnel setup.



WiFi and onboarding

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 105
2. Select either the Google Workspace or Azure configuration:
   a. Option A - WiFi onboarding with Smart Connect and Google Workspace on page 109
   b. Option B - WiFi onboarding with Smart Connect and Azure on page 118
3. FortiGate configuration on page 139
4. Results on page 149

Initial settings on FortiAuthenticator

To set up the initial configuration on FortiAuthenticator:

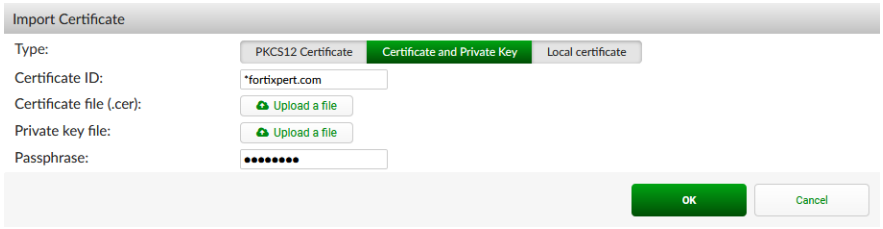
1. Install certificates on page 105
2. Configure the RADIUS client settings on page 107
3. Configure the local root CA on page 107
4. Configure the EAP server certificate and CA for EAP-TLS on page 108

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.

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`.



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.

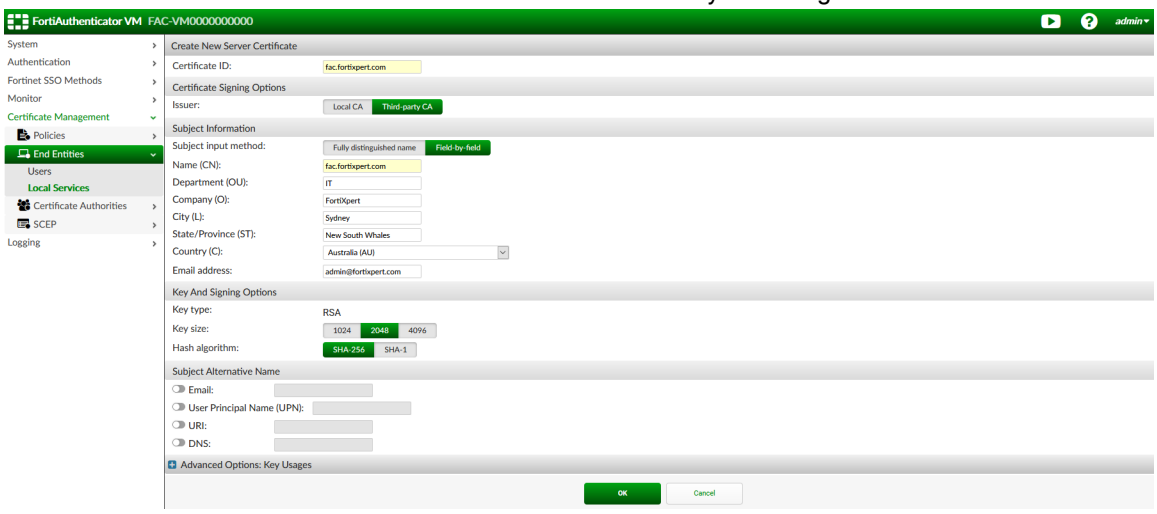
1. In *Certificate Management > End Entities > Local Services*, select the *Create New* button.
   Configure the following settings:
   a. Under *Create New Server Certificate*, set the *Certificate ID* to your certificate name, for example, fac.fortixpert.com.

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.



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.

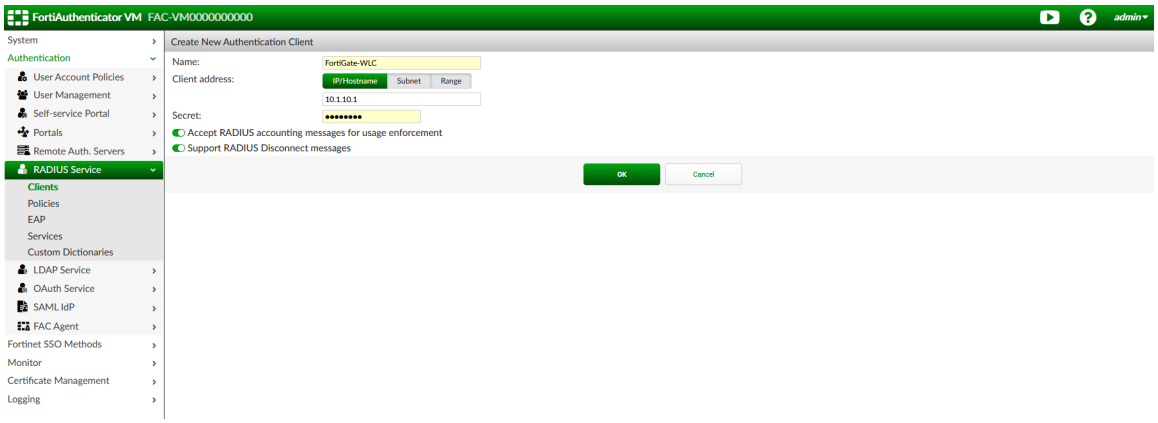
To install local service certificates:

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*.



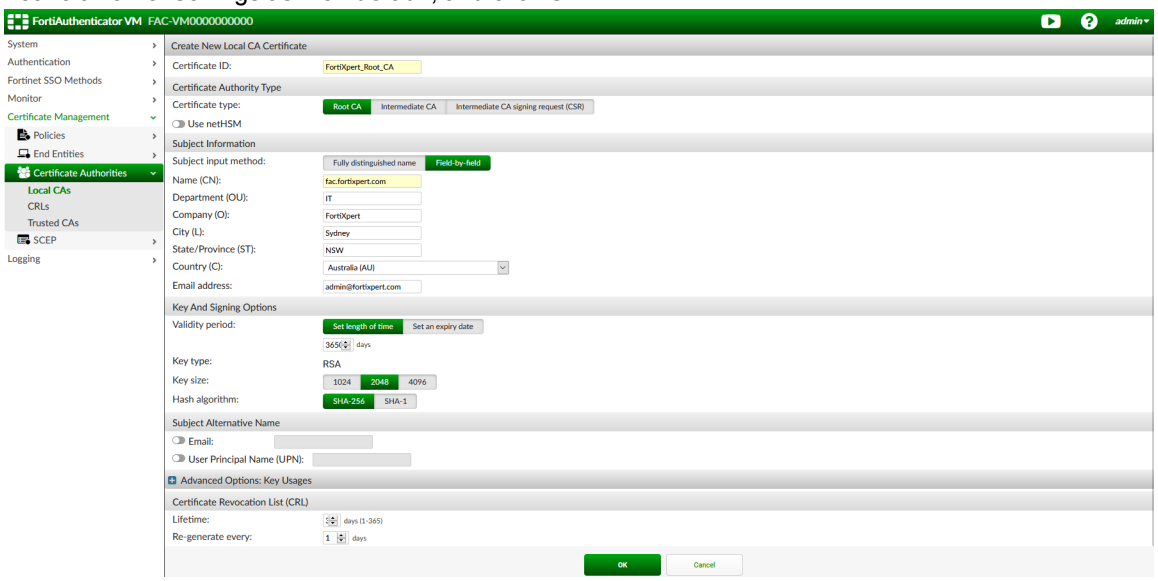
Configure the local root CA

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.

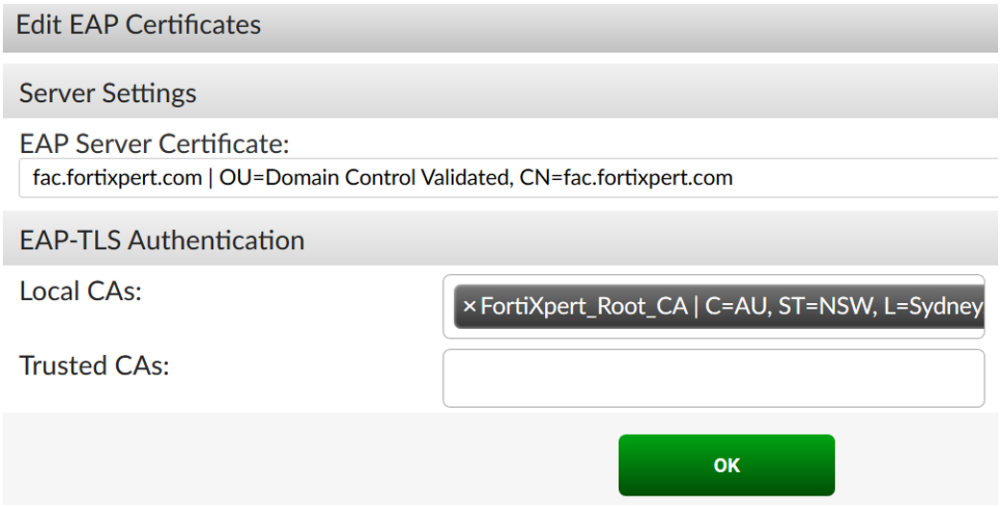
3. Leave all other settings as their default, and click *OK*.



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).



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 109
2. Configure Smart Connect and the captive portal on page 114
3. Configure RADIUS settings on FortiAuthenticator on page 117

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:

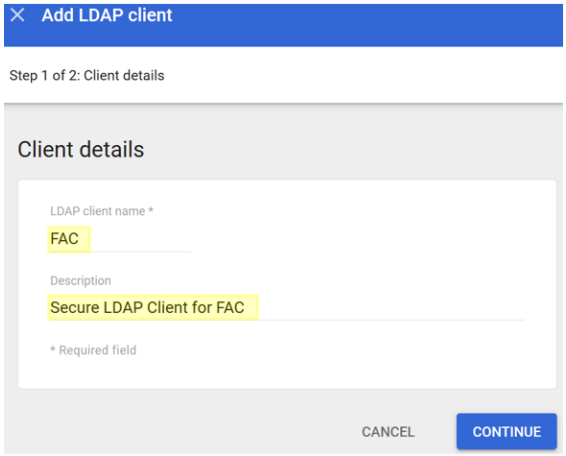
1. Provision the LDAP connector in Google Workspace on page 109
2. Configure certificates on FortiAuthenticator on page 111
3. Configure the remote LDAP server and users on page 112

Provision the LDAP connector in Google Workspace

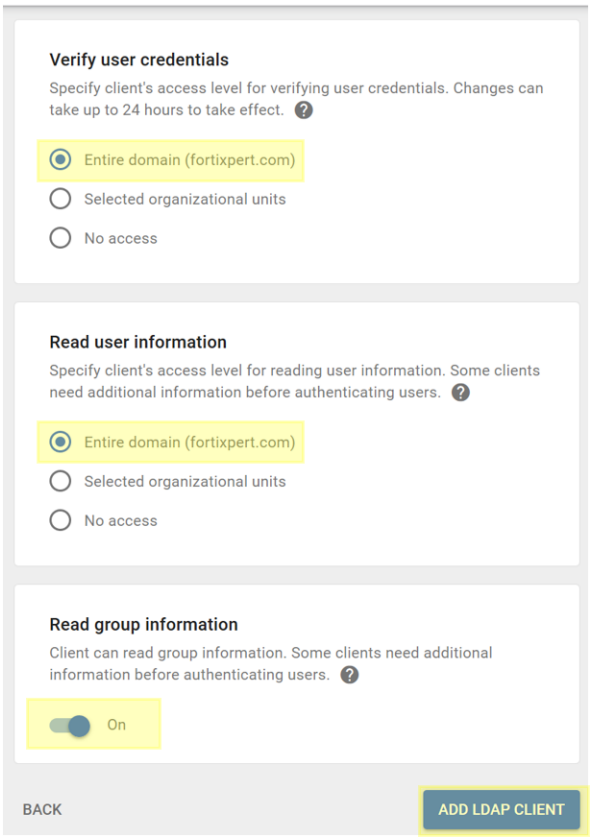
To provision the LDAP connector in Google Workspace:

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*.

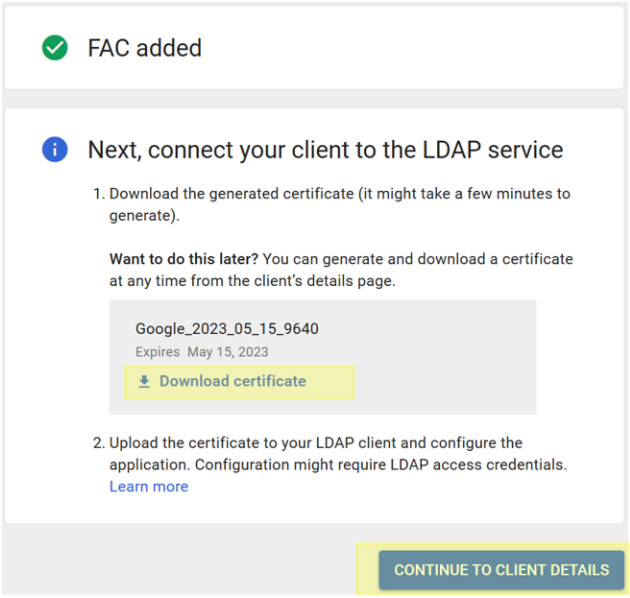


4. Under Add LDAP Client Step 2, configure the following settings:
   a. **Verify User Credentials**: *Entire domain*.
   b. **Read user information**: *Entire domain*.
   c. **Read Group Information**: *On*.
5. Click *Add LDAP Client*.



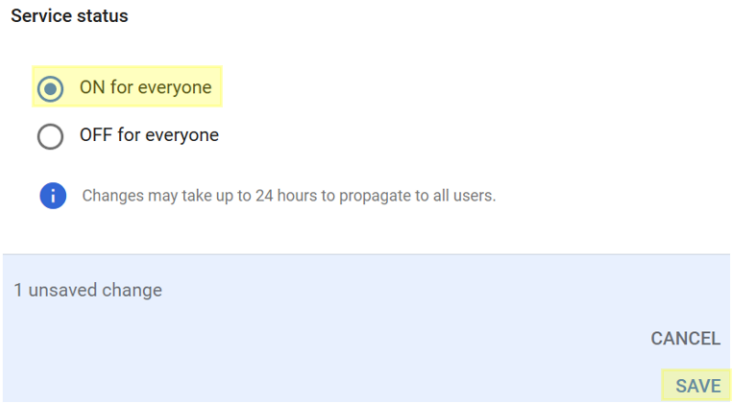
You will now be prompted to connect your client to the LDAP service.

6. Click *Download Certificate* and save the ZIP file.



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*.



8. Click *Save*.

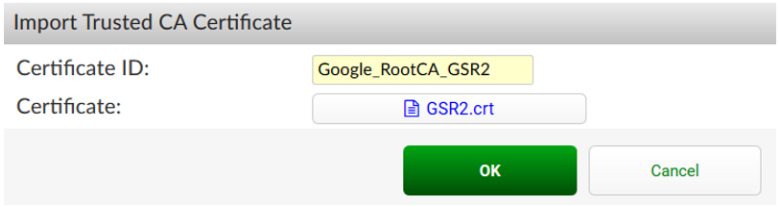
Configure certificates on FortiAuthenticator

To download Google Root CA Certificate:

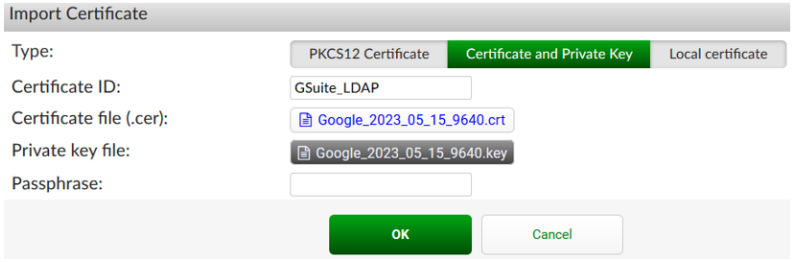
1. Open a new Internet browser and navigate to https://pki.goog.
2. Under *Root CAs* in the *Repository* tab, download the *GS Root R2* certificate in the DER format. The file will be called *GSR2.crt*.

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.



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*.

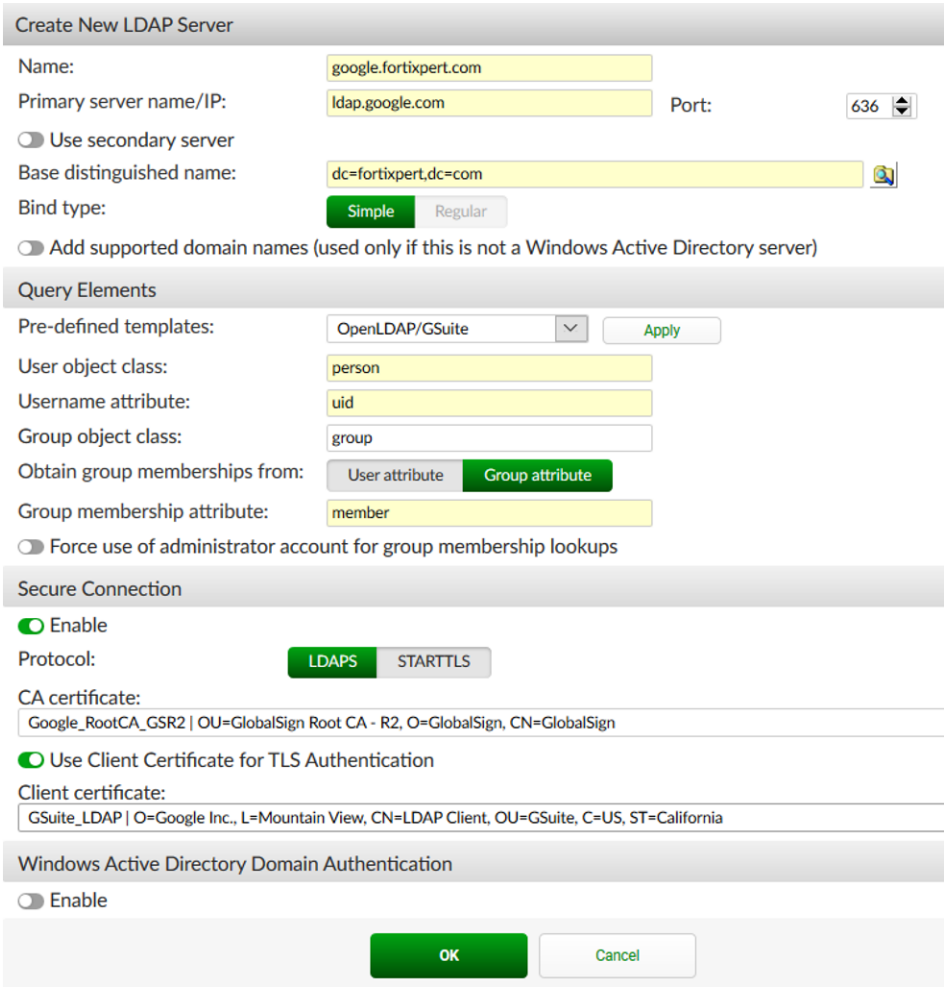


Configure the remote LDAP server and users

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*.



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:

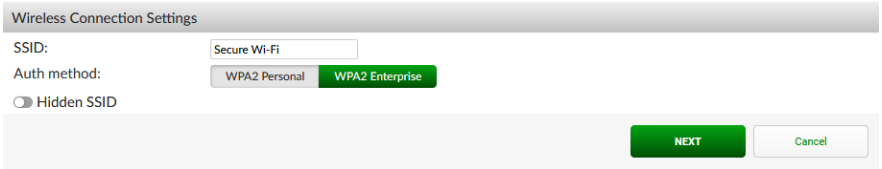
1. Create the Smart Connect profile on page 114
2. Create the captive portal on page 115
3. Create the self-service portal policy on page 116

Create the Smart Connect profile

To create Smart Connect profiles:

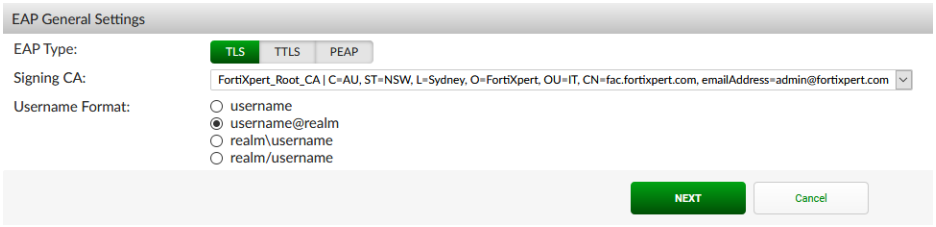
1. Go to *Authentication > Portals > Smart Connect Profiles*, and click *Create New*.
2. Under *General Information*, enter a name for the profile, and click *Next*.

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*.

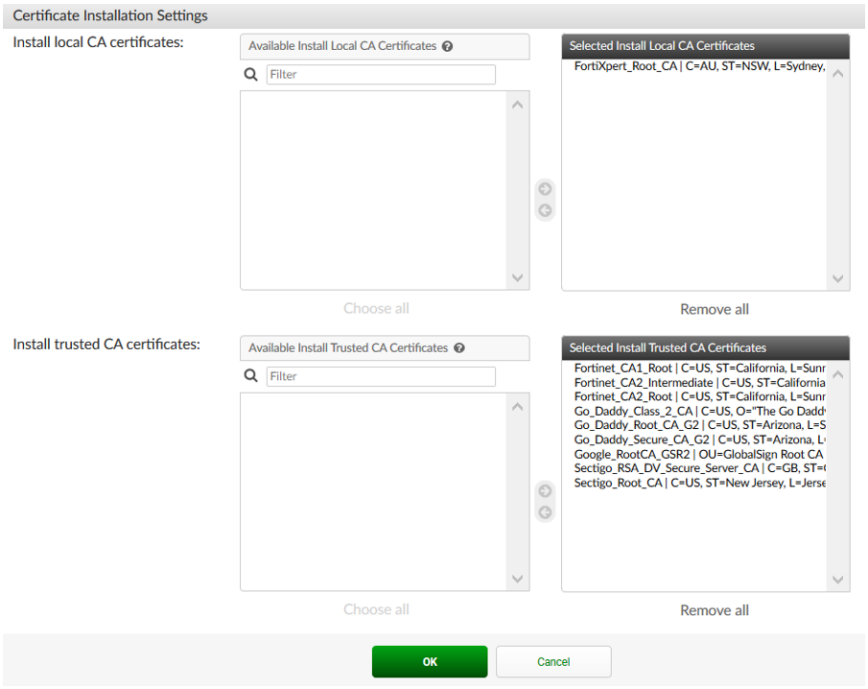


4. Under *EAP General Settings*, set the following and then click *Next*.
   a. **EAP Type**: *TLS*.
   b. **Signing CA**: Select the local Root CA configured earlier.

c. **Username Format**: Select your preference, for example *username@realm*.



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.



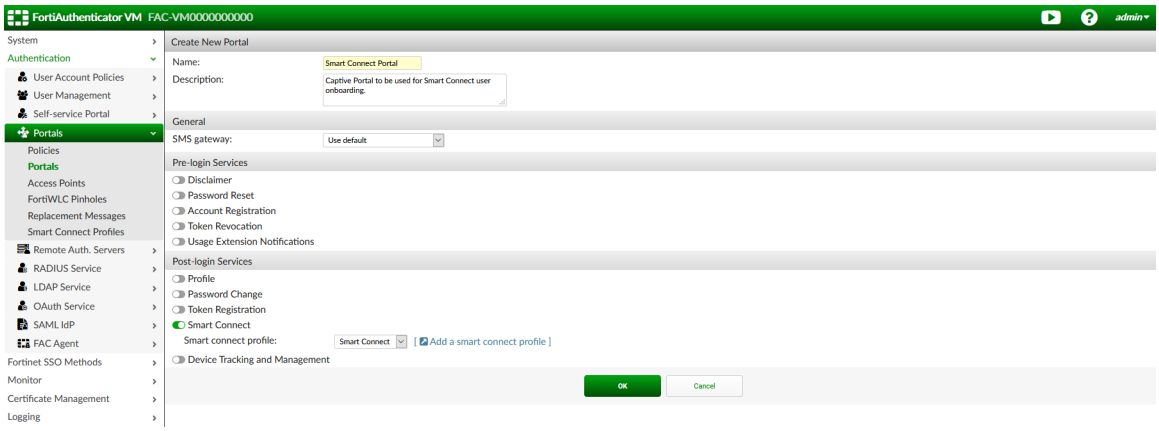
6. Select *OK* to complete the setup of the Smart Connect profile.

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.

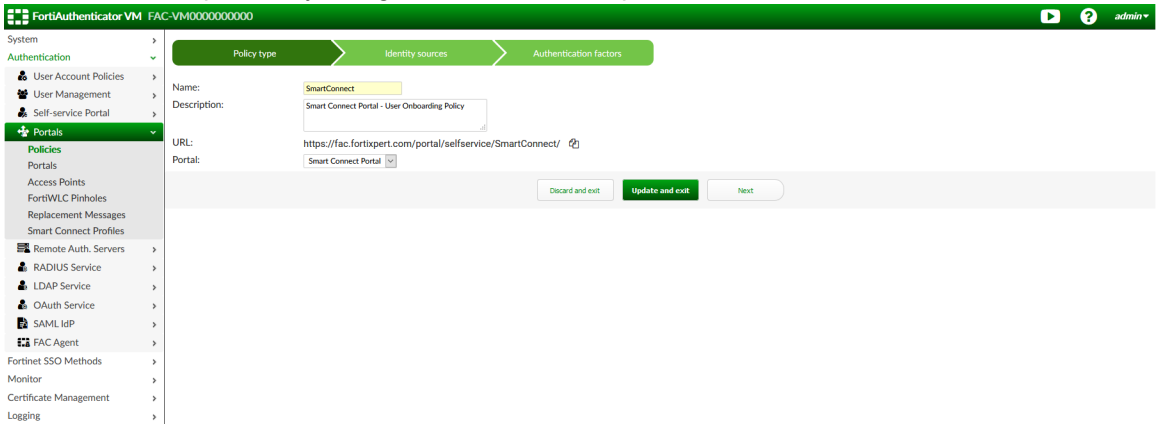
4. Select *OK*.



Create the self-service portal policy

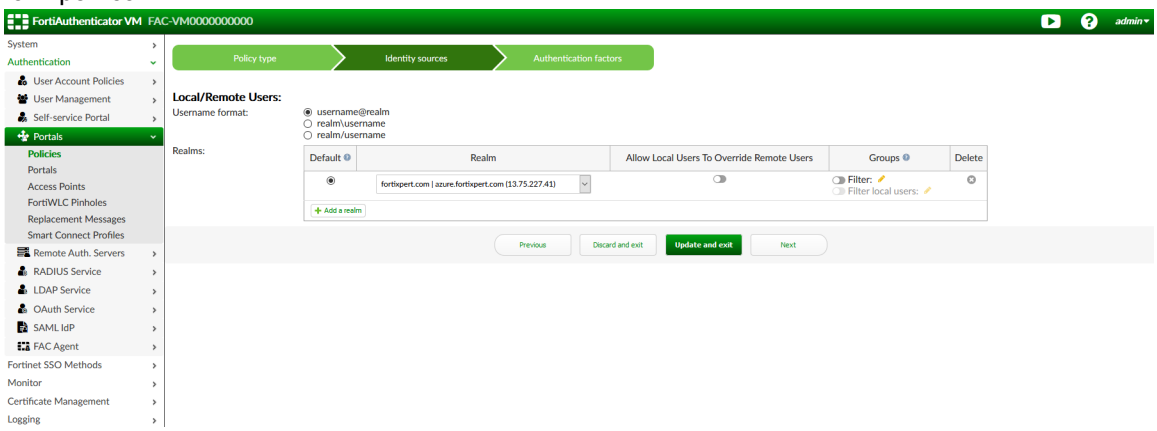
To create a self-service portal policy:

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.



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.

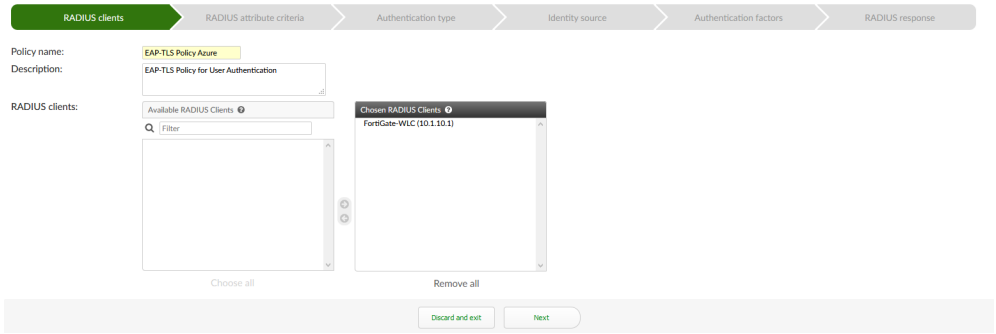


4. Under *Authentication factors*, leave the default options in place, and click *Save and exit*.

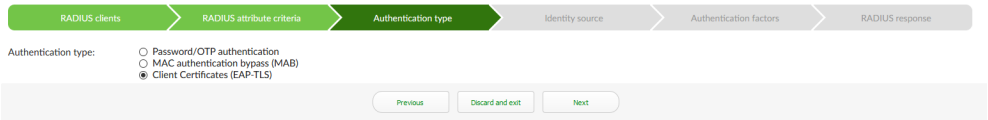
Configure RADIUS settings on FortiAuthenticator

To create a RADIUS service policy:

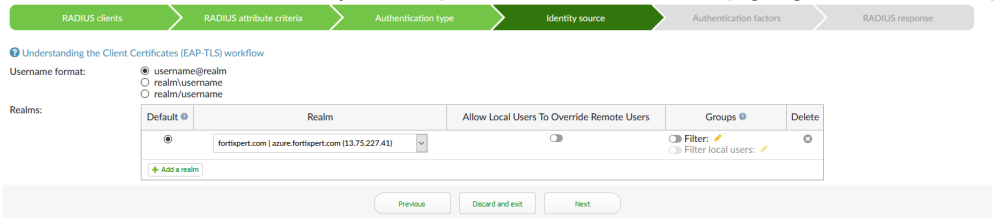
1. Go to *Authentication > RADIUS Service > Policies*, and click *Create New*.
2. Under *RADIUS clients*, set the following and then click *Next*:
   a. **Policy Name**: Enter a name for the policy, for example EAP-TLS Policy Google Workspace.
   b. **Description**: Enter an optional description, for example EAP-TLS Policy for User Authentication.
   c. **RADIUS Clients**: Add the FortiGate to the *Chosen RADIUS Clients* section.



3. Under *RADIUS attribute criteria*, click *Next* without making changes.
4. Under *Authentication type*, select *Client Certificates (EAP-TLS)*, and click *Next*.



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.



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 Entra ID Directory Services via Secure Lightweight Directory Access Protocol

To configure WiFi Onboarding with Azure:

1. Configure Microsoft Entra ID (formerly Microsoft Azure AD) DS LDAPS integration on page 118
2. Configure Smart Connect and the captive portal on page 122
3. Configure RADIUS settings on FortiAuthenticator on page 126

Configure Microsoft Entra ID (formerly Microsoft Azure AD) DS LDAPS integration

This guide does not include information on how to provision Microsoft Entra ID DS. Please refer to Microsoft's support site for instructions on how to do this.

To configure Microsoft Entra ID DS LDAPS integration:

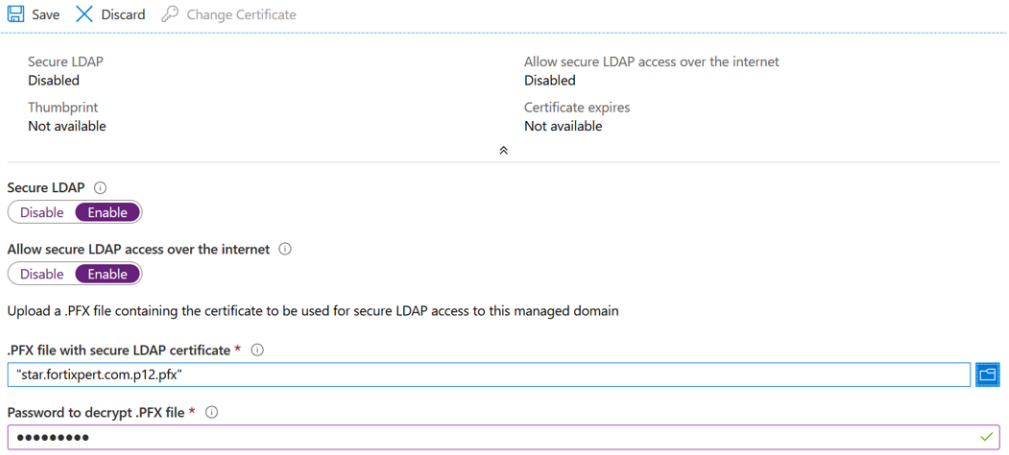
1. Provision the LDAPS connector in Microsoft Entra ID DS on page 118
2. Provision the remote LDAP server on FortiAuthenticator on page 120

Provision the LDAPS connector in Microsoft Entra ID DS

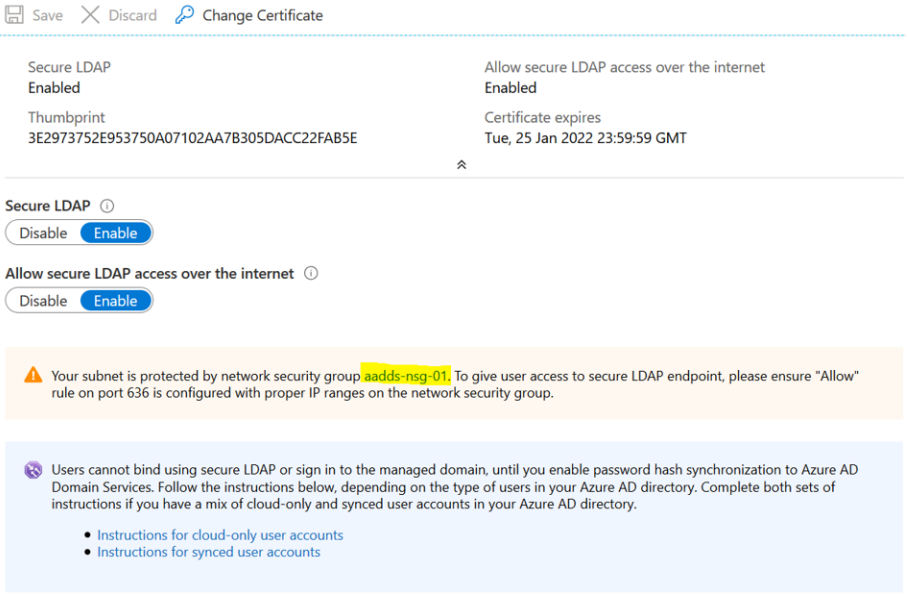
To provision the LDAP connector in Microsoft Entra ID DS:

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.



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.



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*.

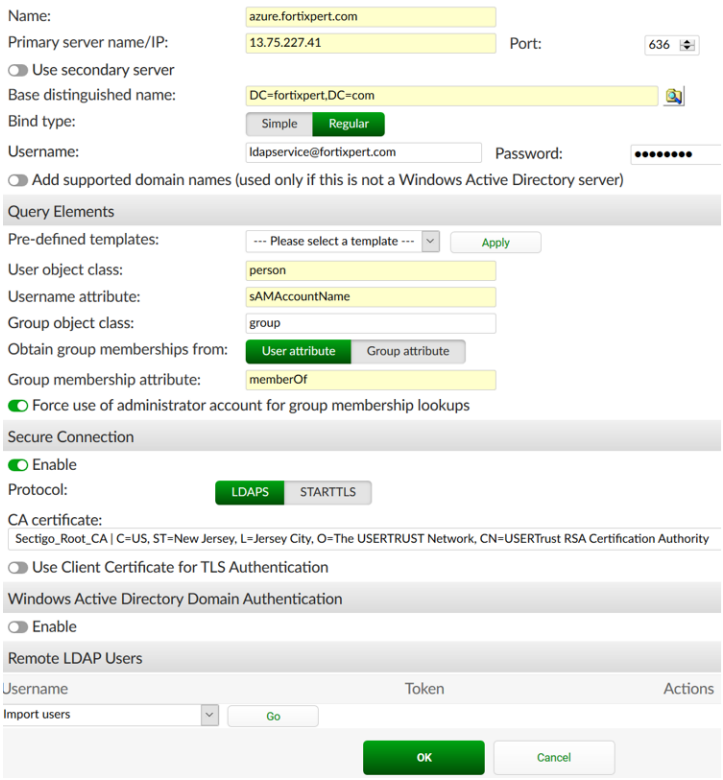
To obtain the LDAPS IP address:

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*.

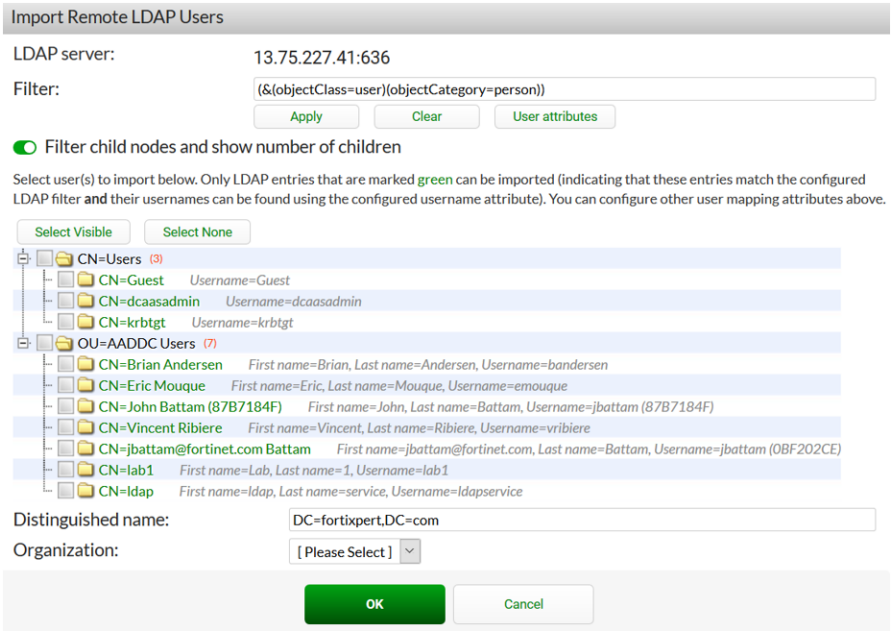


6. Click *OK* to save the remote LDAP server configuration.

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.



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 Microsoft Entra ID DS.

To configure Smart Connect and portals on FortiAuthenticator:

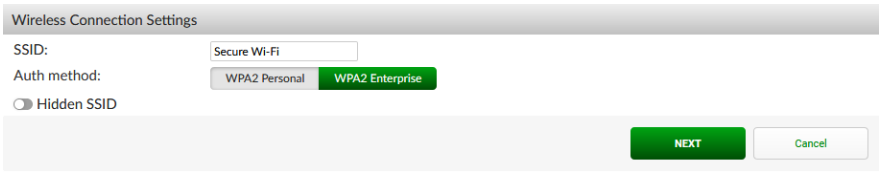
1. Create the Smart Connect profile on page 123
2. Create the captive portal on page 124
3. Create the self-service portal policy on page 125

Create the Smart Connect profile

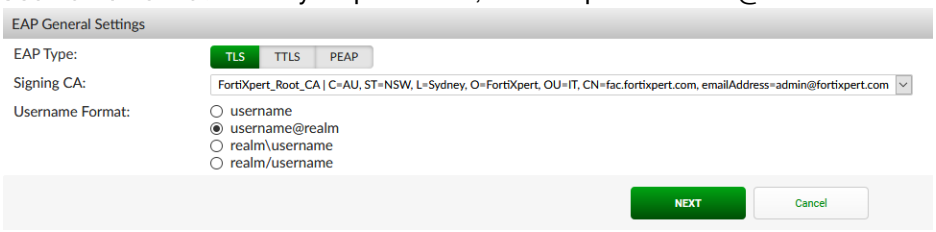
To create Smart Connect profiles:

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*.

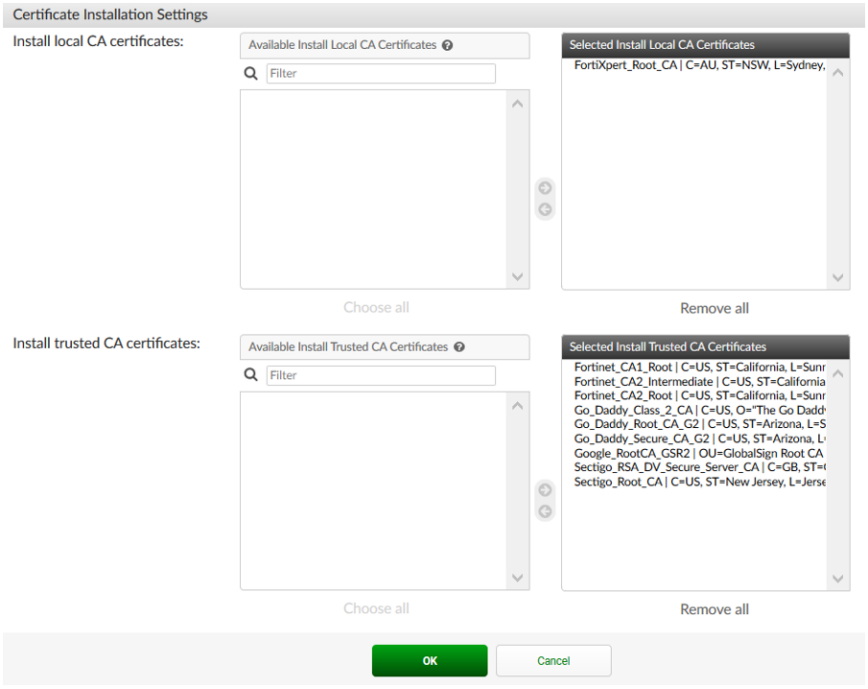
3. Under *Wireless Connection Settings*, set the following and then click *Next*.
   a. **SSID**: Enter your SSID name, for example Secure Wi-Fi.
   b. **Auth method**: *WPA2 Enterprise*.
   c. **Hidden SSID**: *Disabled*.



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*.



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.

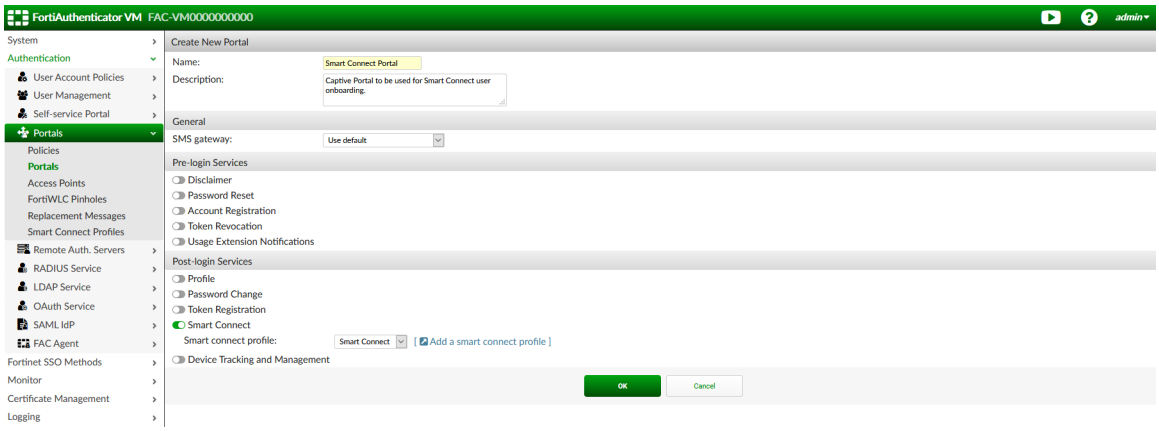


6. Select *OK* to complete the setup of the Smart Connect profile.

Create the captive portal

To create a captive portal:

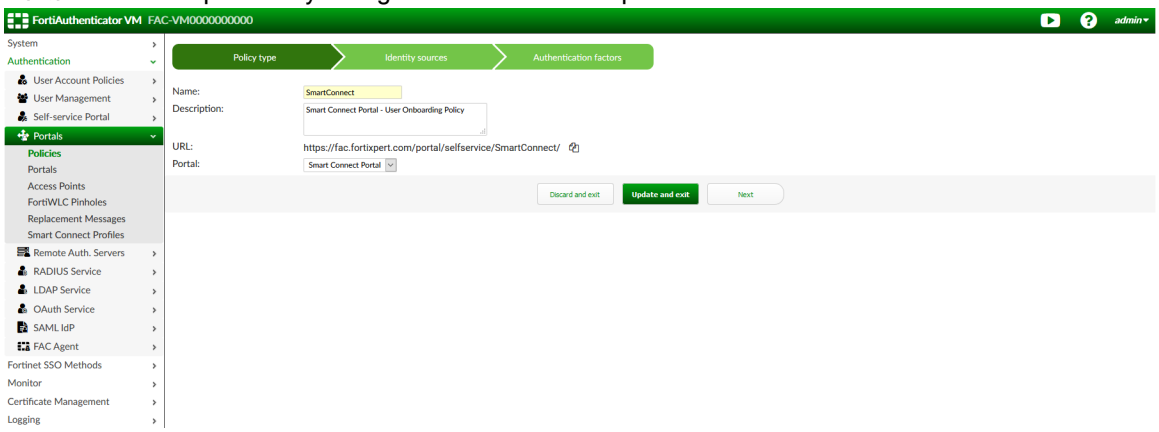
1. Go to *Authentication > Portals > Portals*, and click *Create New*.
2. Under *Create New Portal*, enter a name and optional description for the portal.
3. Under *Post-login services*, enable *Smart Connect* and select the previously configured Smart Connect profile from the dropdown.
4. Select *OK*.



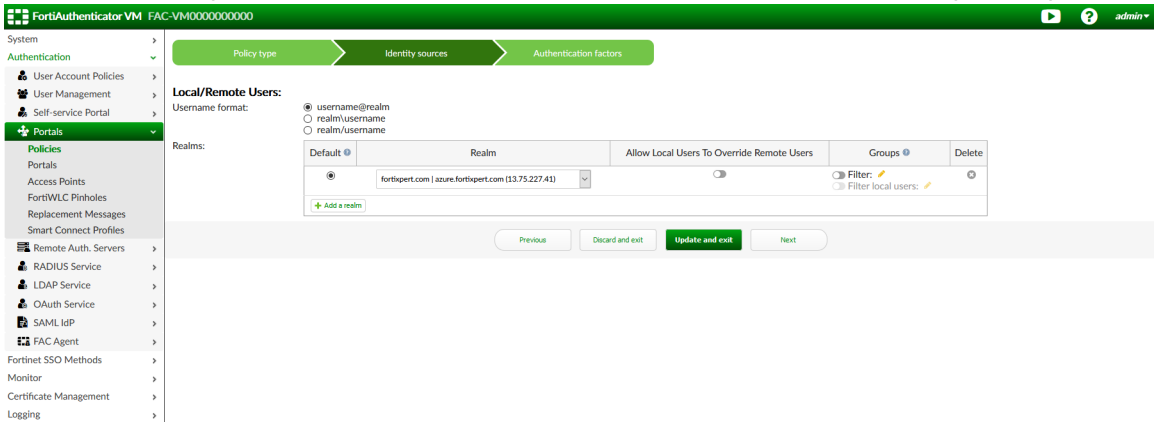
Create the self-service portal policy

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.



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.

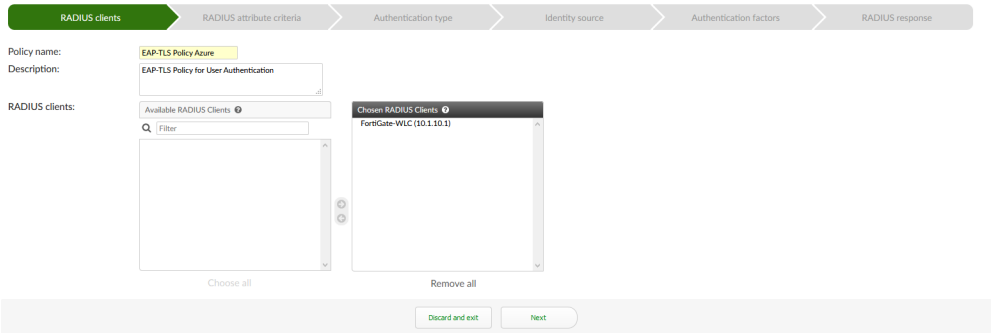


4. Under *Authentication factors*, leave the default options in place, and click *Save and exit*.

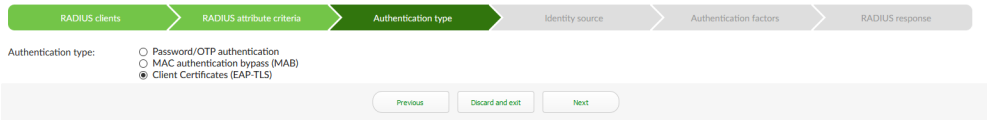
Configure RADIUS settings on FortiAuthenticator

To create a RADIUS service policy:

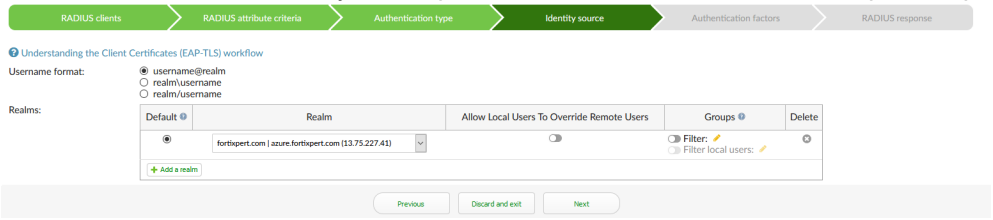
1. Go to *Authentication > RADIUS Service > Policies*, and click *Create New*.
2. Under *RADIUS clients*, set the following and then click *Next*:
   a. **Policy Name**: Enter a name for the policy, for example EAP-TLS Policy Azure.
   b. **Description**: Enter an optional description, for example EAP-TLS Policy for User Authentication.
   c. **RADIUS Clients**: Add the FortiGate to the *Chosen RADIUS Clients* section.



3. Under *RADIUS attribute criteria*, click *Next* without making changes.
4. Under *Authentication type*, select *Client Certificates (EAP-TLS)*, and click *Next*.



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.



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:

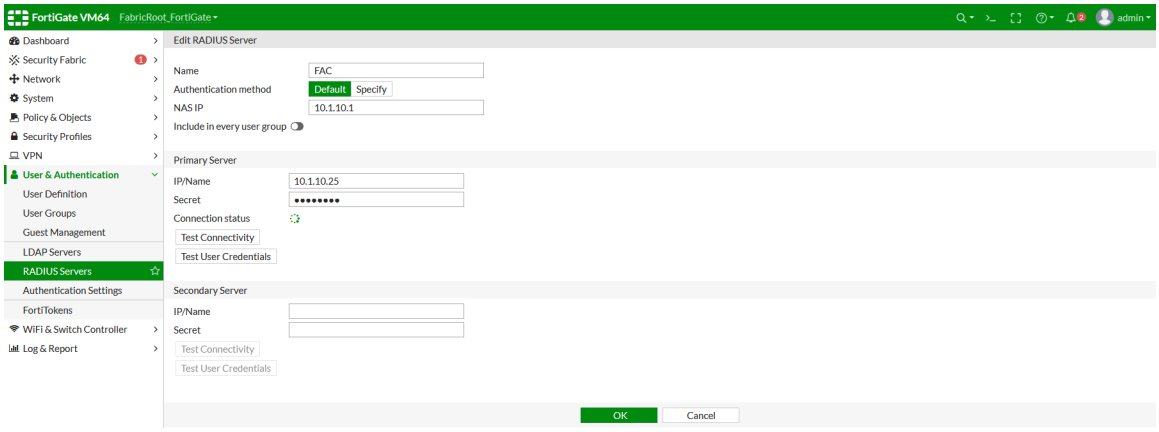
1. Configure the RADIUS server on FortiGate on page 140
2. Create the user group for cloud-based directory user accounts on page 140

3. Provision the Onboarding and Secure WiFi networks on page 141

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*.

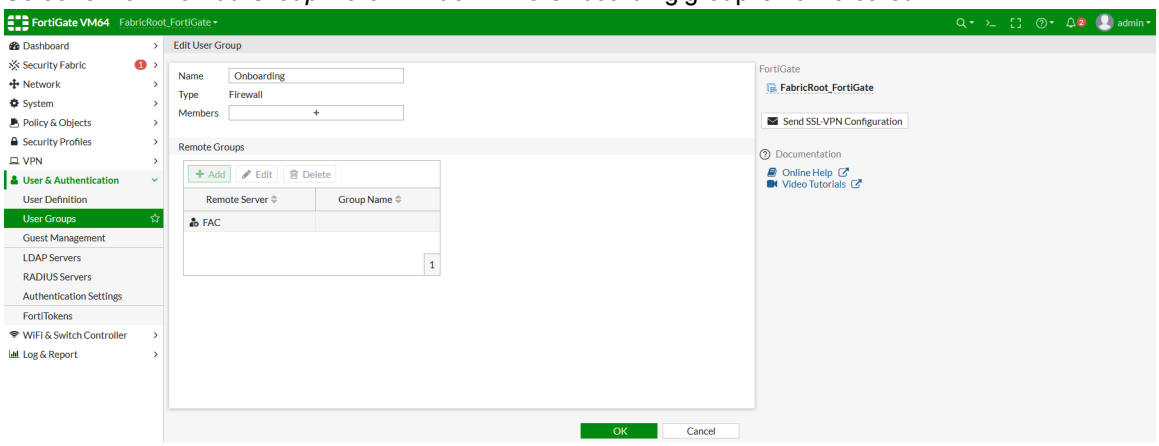


Create the user group for cloud-based directory user accounts

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.

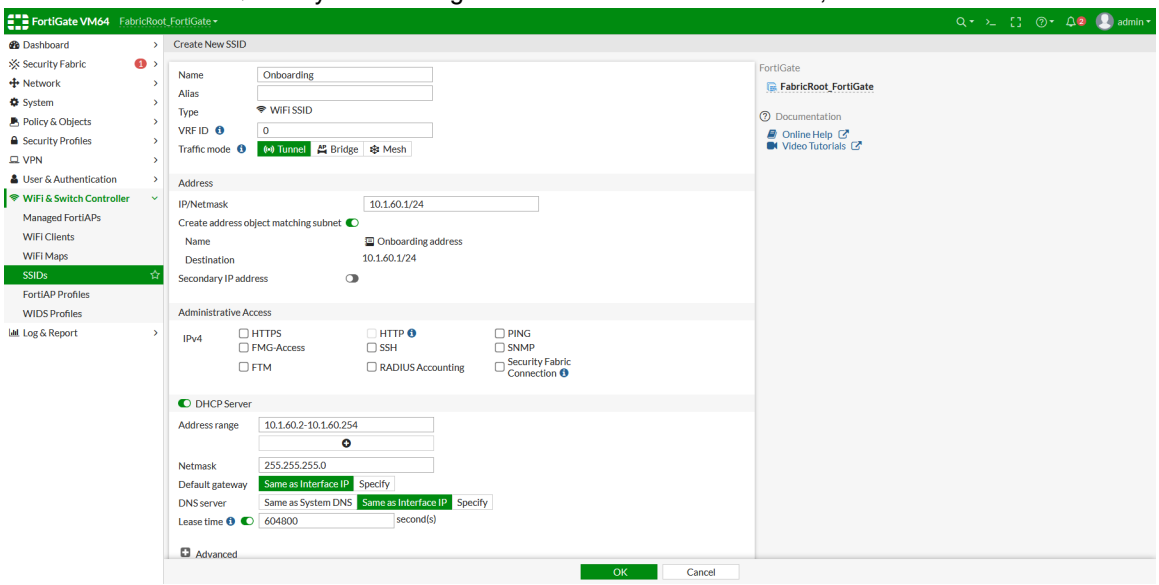
3. Select *OK* on the *Add Group Match* window. The Onboarding group is now created.



Provision the Onboarding and Secure WiFi networks

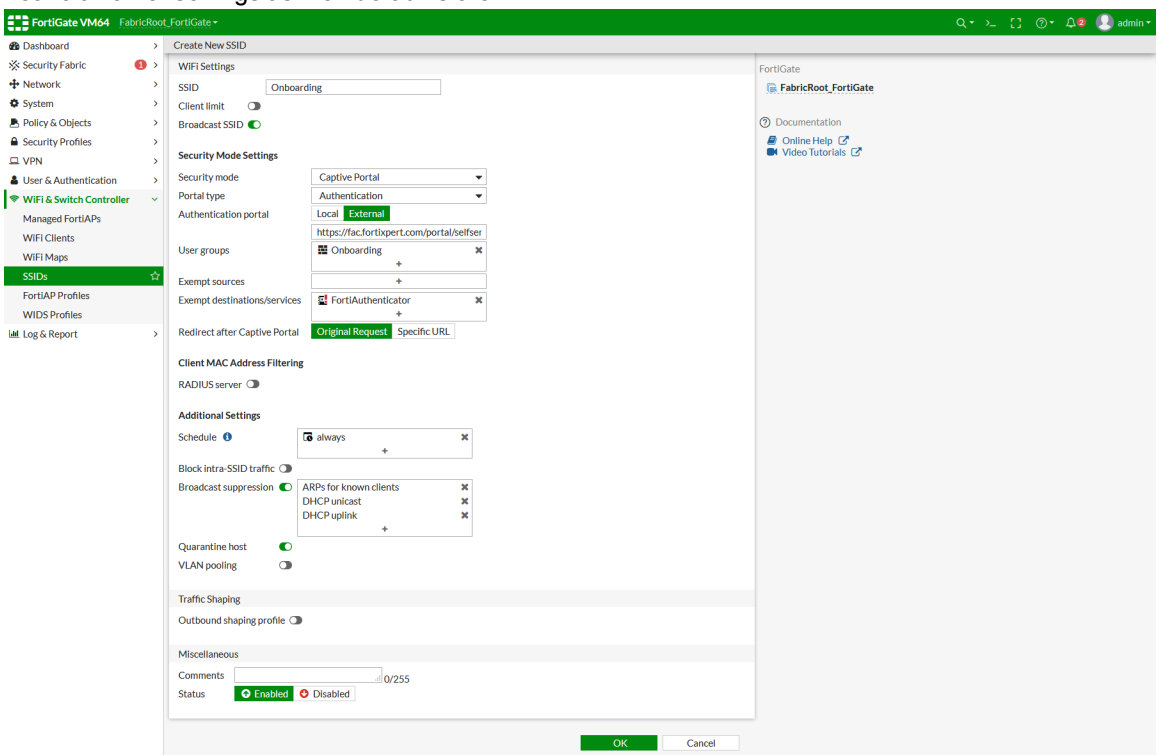
To provision the Smart Connect enabled "Onboarding" SSID:

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*.



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.

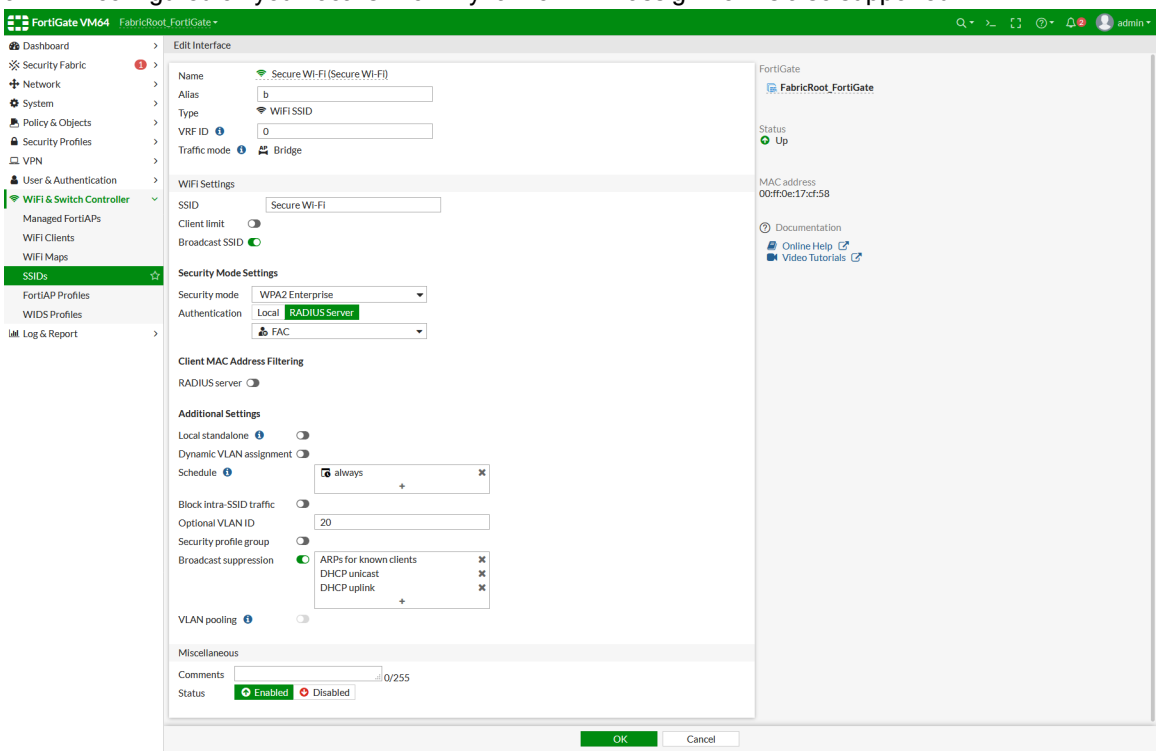


7. Click *OK*.

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.

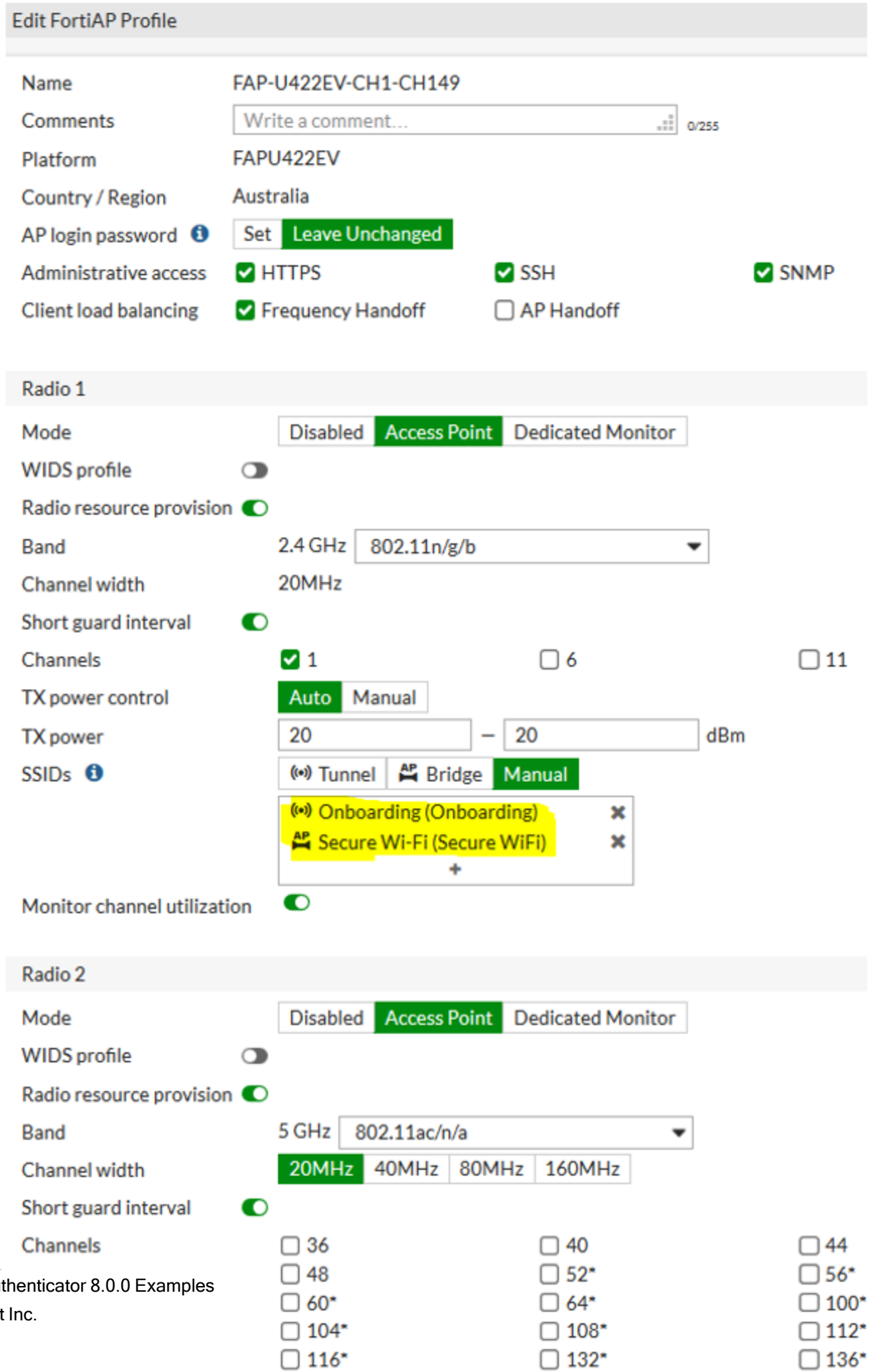


3. Click *OK*.

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.

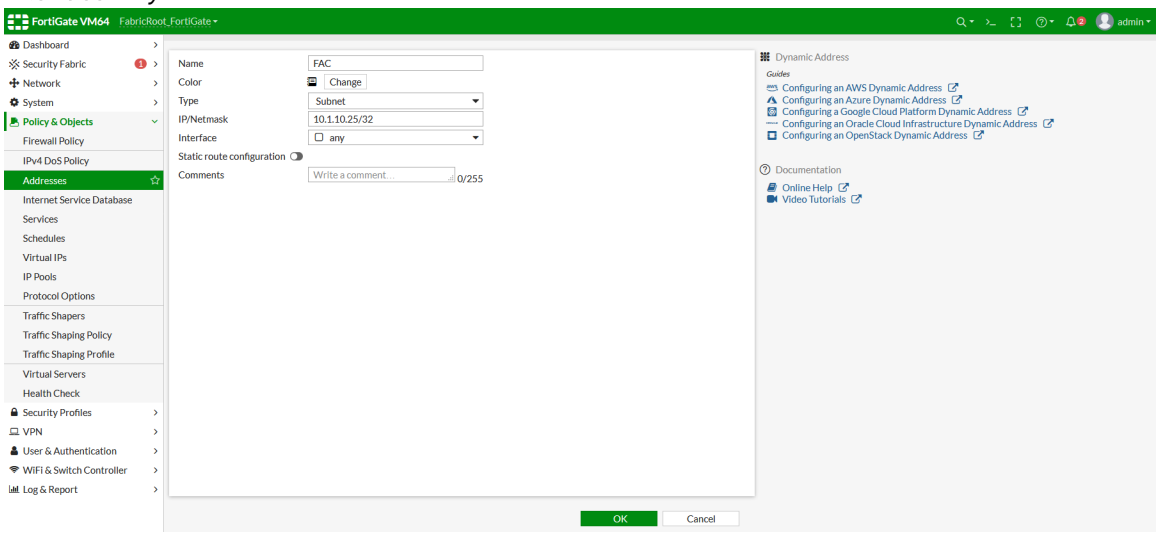
3. Confirm the SSIDs are broadcasting and can be seen by WiFi enabled devices.


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*.

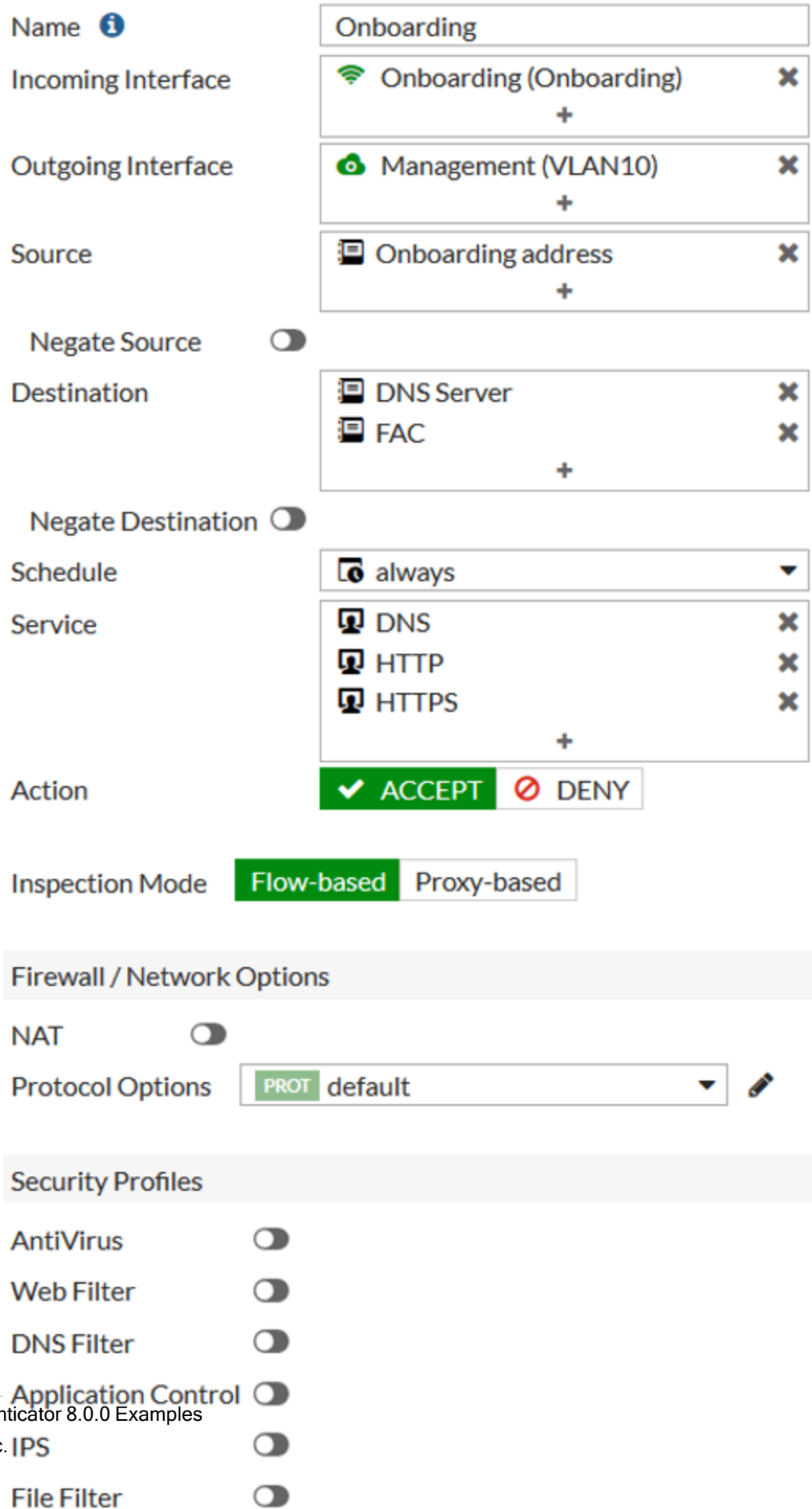


3. Click *OK*.

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

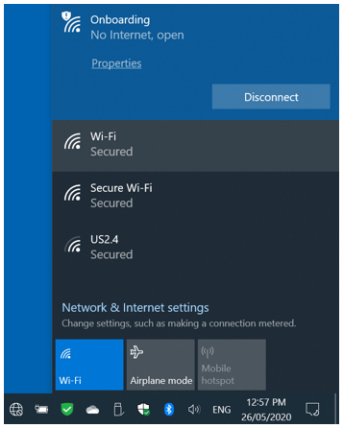
You can now connect your device to the Onboarding SSID and proceed with the Smart Connect onboarding process:

- Smart Connect Windows device onboarding process on page 149
- Smart Connect iOS device onboarding process on page 151

Smart Connect Windows device onboarding process

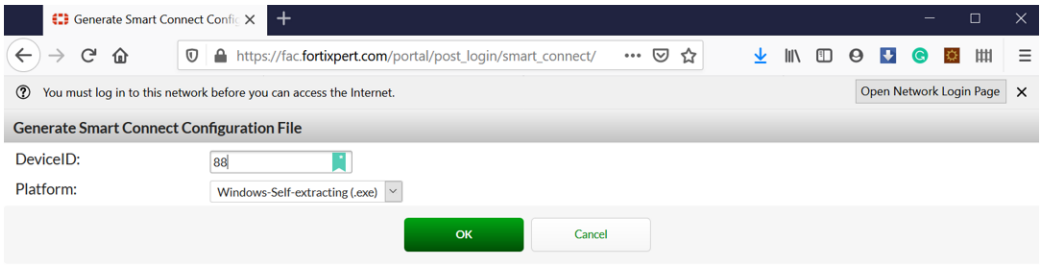
To onboard a Windows device:

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*.

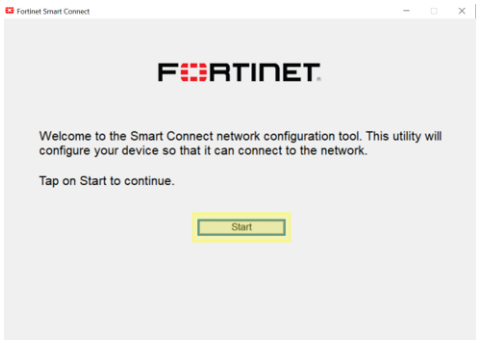
3. Enter a unique *Device ID* and choose your operating system from the *Platform* dropdown. Click *OK*.



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*.



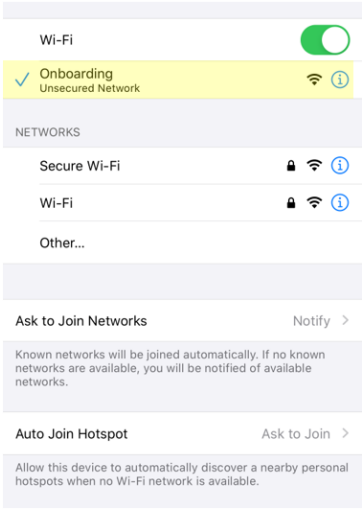
Your device will now be provisioned with the wireless network information and certificates in order to connect to the Secure Wi-Fi SSID.

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:

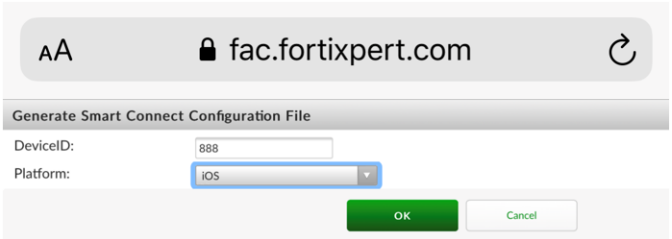
1. On the iOS device, connect to the Onboarding WiFi network.



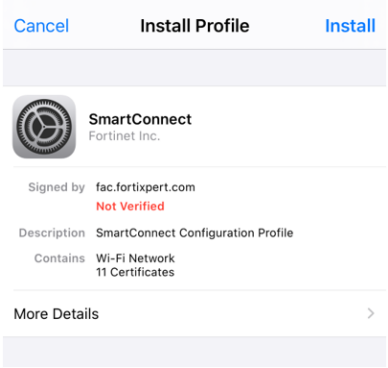
   The FortiAuthenticator login screen is displayed.

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*.



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.



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.

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.

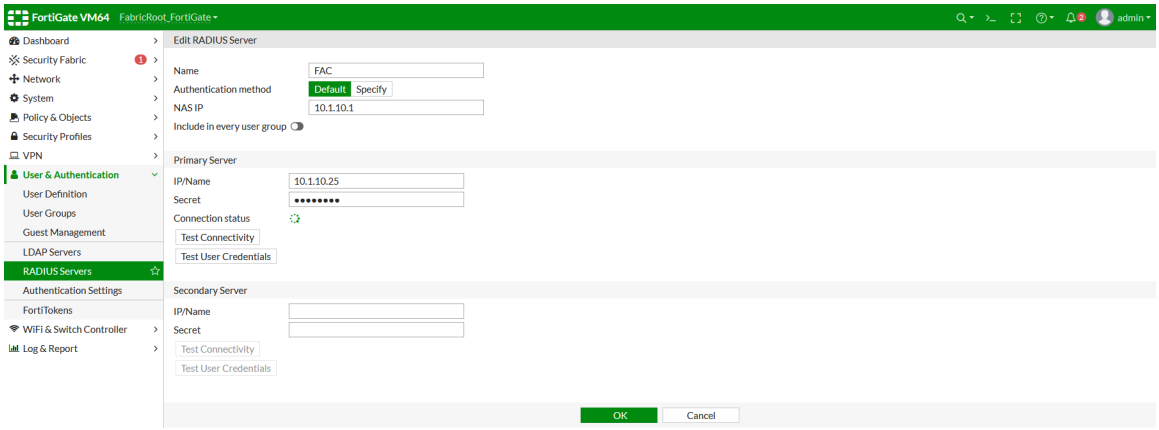
To configure the FortiGate:

1. Configure the RADIUS server on FortiGate on page 140
2. Create the user group for cloud-based directory user accounts on page 140
3. Provision the Onboarding and Secure WiFi networks on page 141

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*.

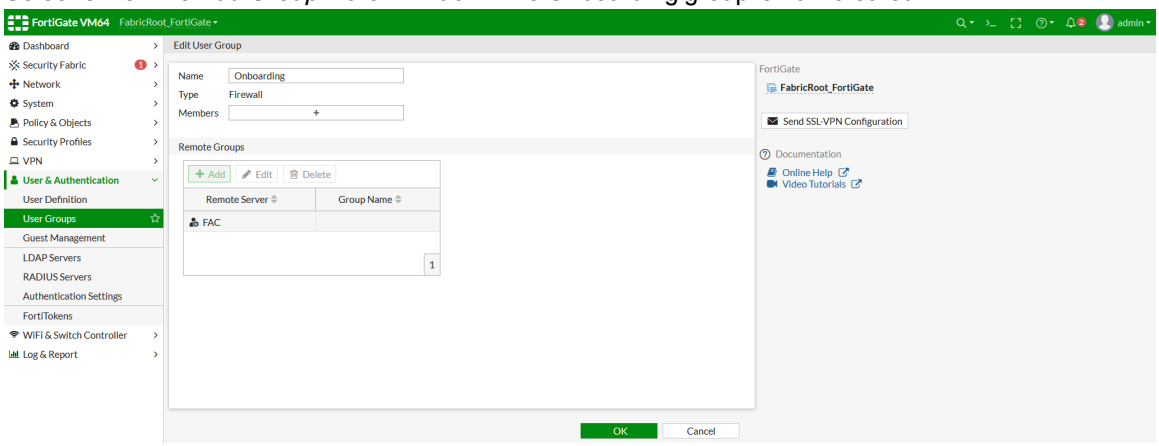


Create the user group for cloud-based directory user accounts

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.

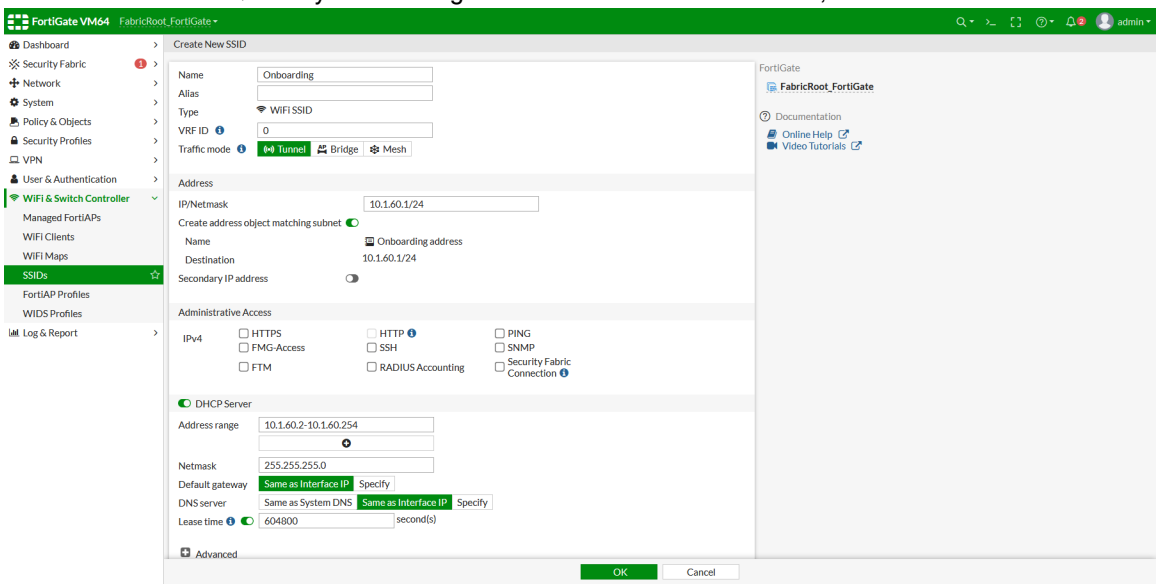
3. Select *OK* on the *Add Group Match* window. The Onboarding group is now created.



Provision the Onboarding and Secure WiFi networks

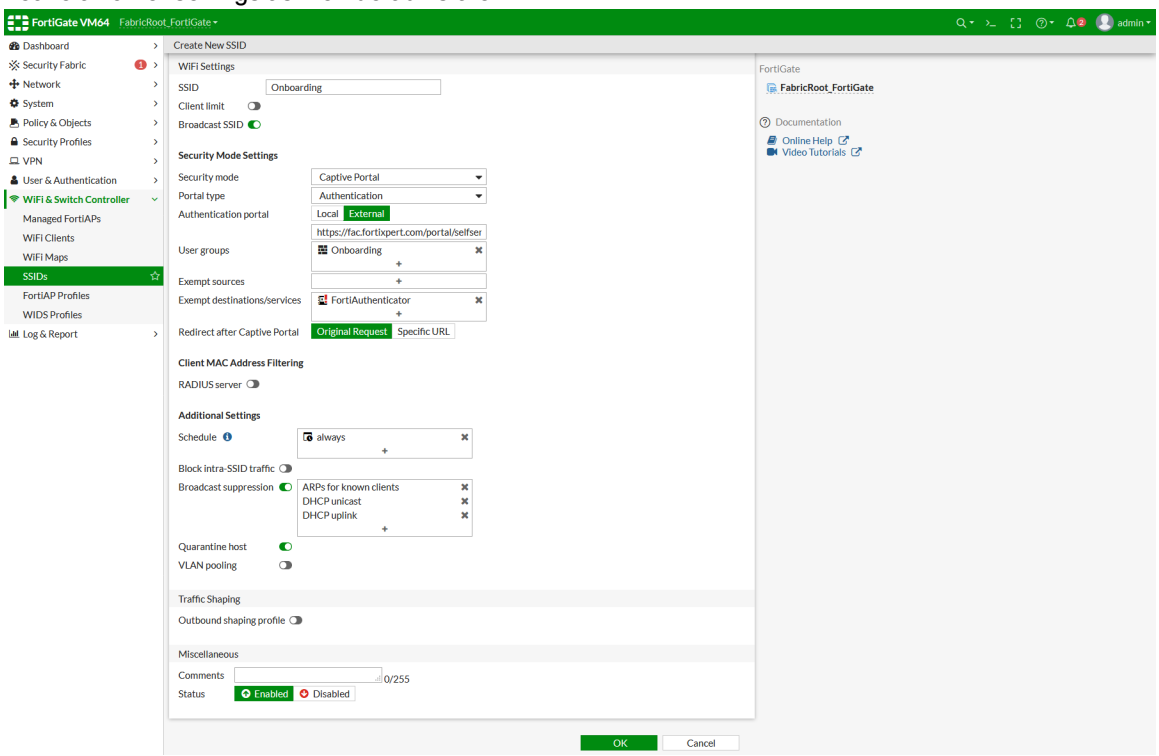
To provision the Smart Connect enabled "Onboarding" SSID:

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*.



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.

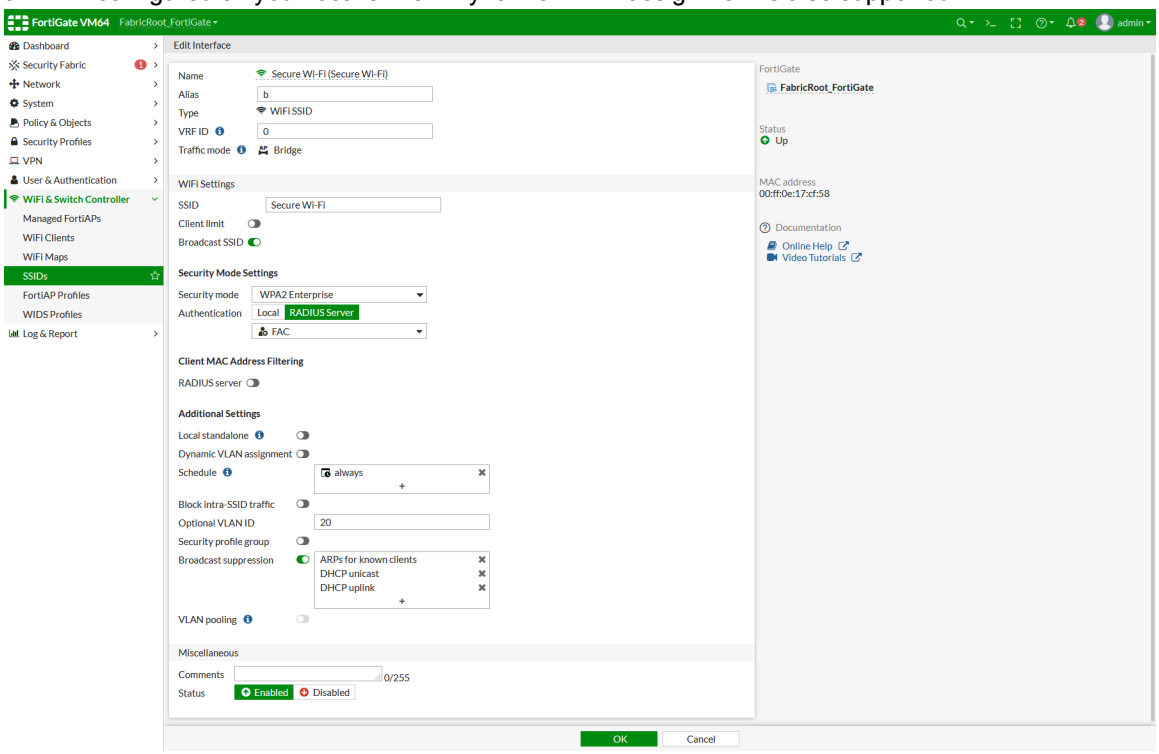


7. Click *OK*.

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.

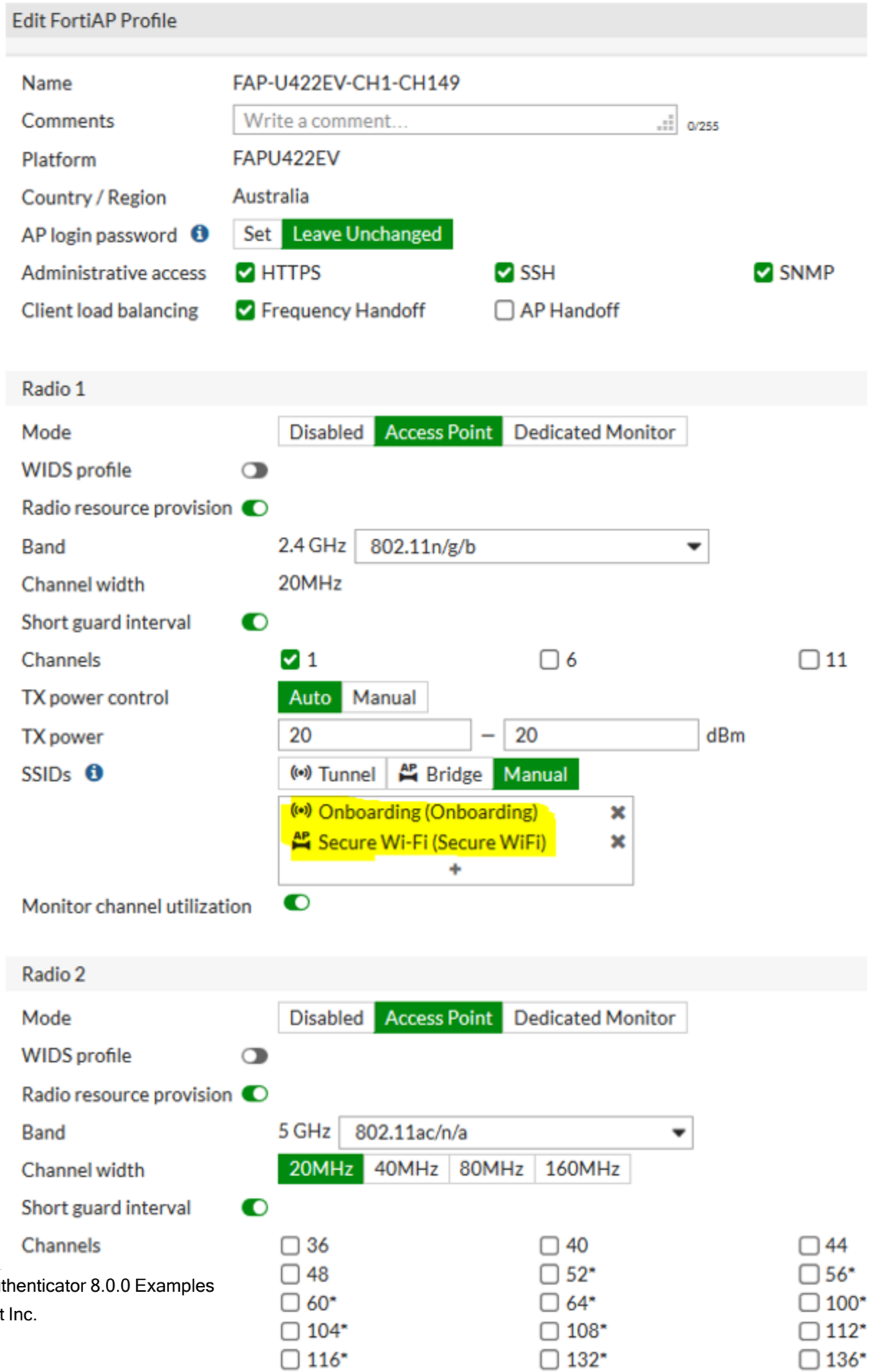


3. Click *OK*.

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.

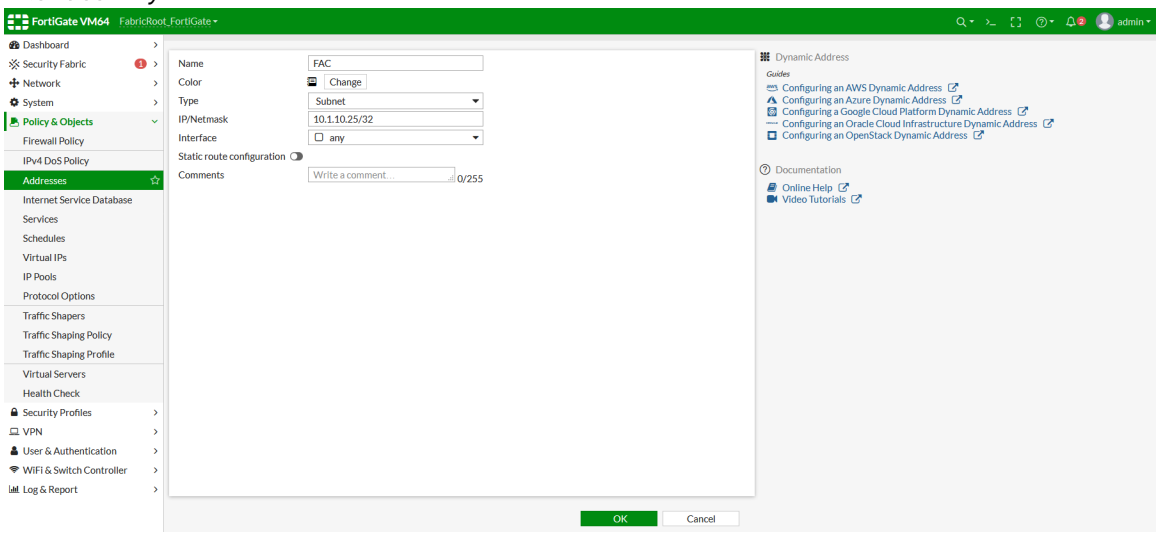
3. Confirm the SSIDs are broadcasting and can be seen by WiFi enabled devices.


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*.

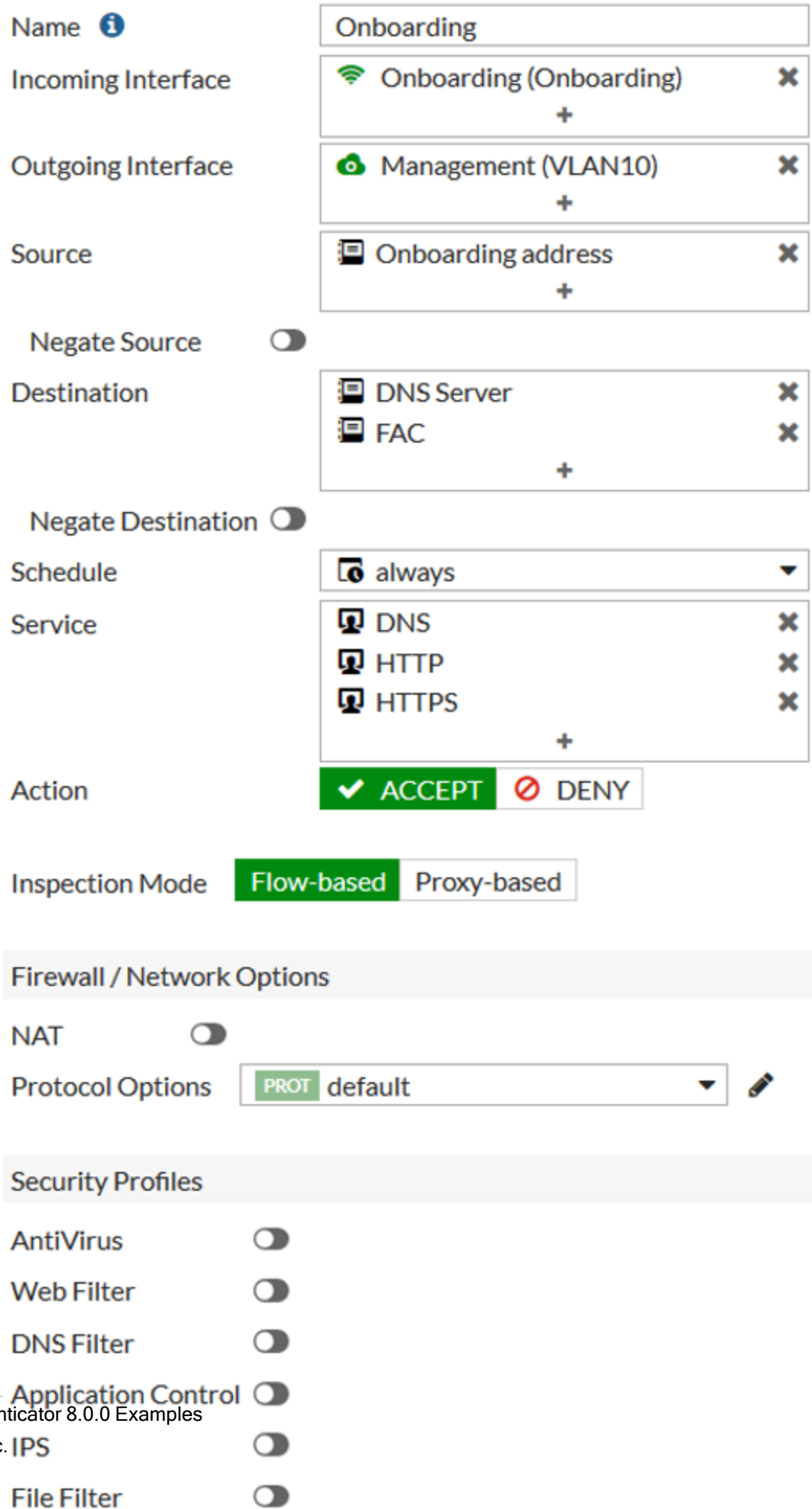


3. Click *OK*.

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

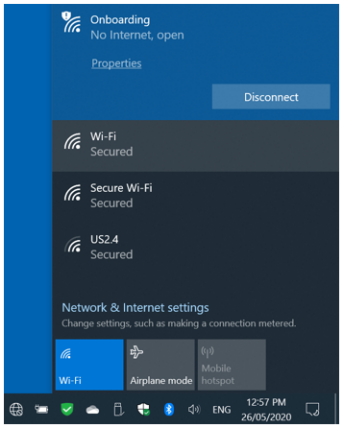
You can now connect your device to the Onboarding SSID and proceed with the Smart Connect onboarding process:

- Smart Connect Windows device onboarding process on page 149
- Smart Connect iOS device onboarding process on page 151

Smart Connect Windows device onboarding process

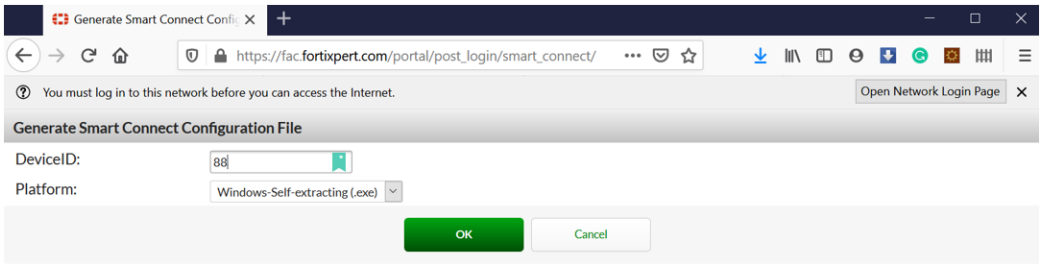
To onboard a Windows device:

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*.

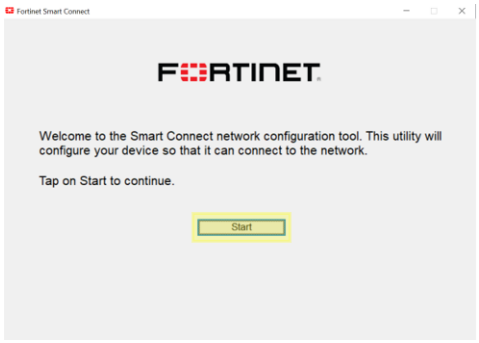
3. Enter a unique *Device ID* and choose your operating system from the *Platform* dropdown. Click *OK*.



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*.



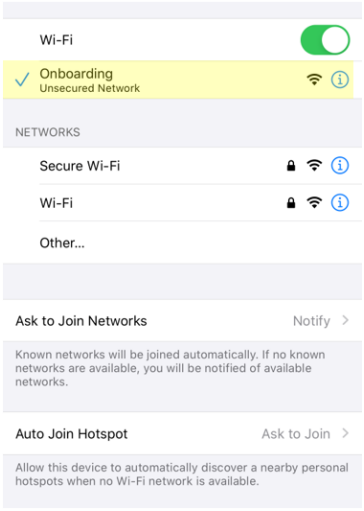
Your device will now be provisioned with the wireless network information and certificates in order to connect to the Secure Wi-Fi SSID.

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:

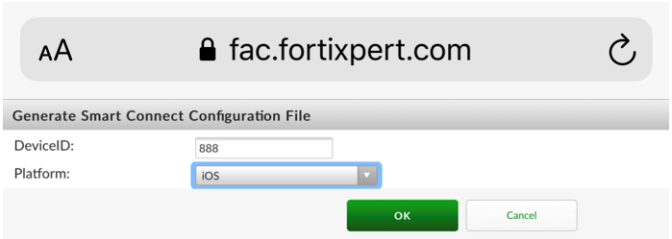
1. On the iOS device, connect to the Onboarding WiFi network.



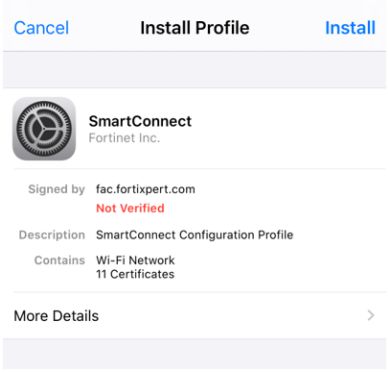
   The FortiAuthenticator login screen is displayed.

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*.



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.



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.

Advanced scenarios

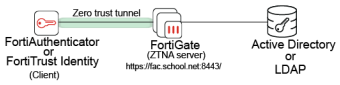
Accessing an AD server with a zero trust tunnel on FortiAuthenticator

A zero trust tunnel allows FortiAuthenticator to securely access TCP-based-on-premise services from the public internet.

Using a zero trust tunnel, you can access an on-premise LDAP/AD server.

Requirements:

This example uses FortiAuthenticator 6.6.0, FortiOS 7.4.2, and an AD server.



In this example:

1. FortiAuthenticator operates as a local certificate authority (CA).
2. FortiAuthenticator generates a client certificate for the connection between FortiAuthenticator and the AD server.
3. The local root CA certificate is exported and installed on the FortiGate in order to authenticate and trust the client connection.
4. FortiGate acts as a ZTNA application gateway allowing FortiAuthenticator to access the AD server using TCP forwarding access proxy.

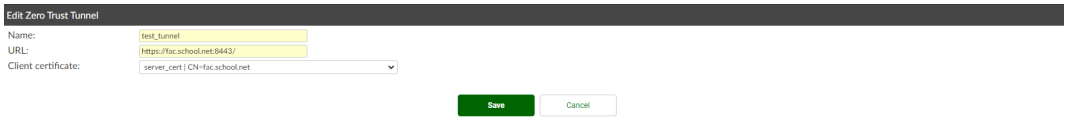
To access an AD server with a zero trust tunnel on FortiAuthenticator:

1. Configure certificate authentication for FortiAuthenticator. See Configuring certificate authentication for FortiAuthenticator on page 155.
2. Configure a zero trust tunnel on FortiAuthenticator. See Configuring a zero trust tunnel on FortiAuthenticator on page 154.
3. Configure an LDAP server on FortiAuthenticator. See Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator on page 154.
4. Configure the FortiGate device as the ZTNA server. See Configuring a ZTNA server on page 158.
5. Configure a ZTNA rule on the ZTNA server. See Configuring a ZTNA rule on page 159.
6. For troubleshooting, see Debugging: Zero trust tunnel related issues on page 160.

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 *Save*.

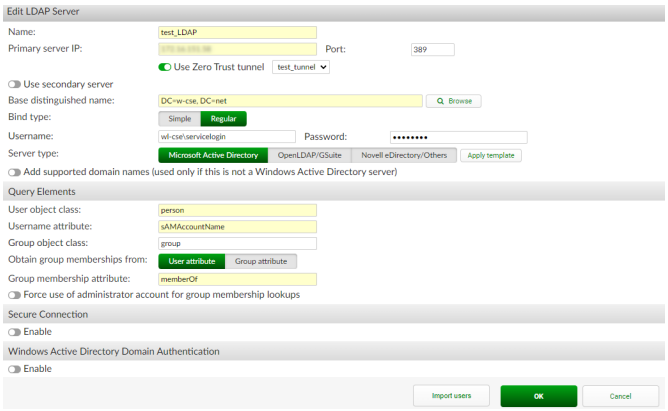


Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator

We configure the AD server 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 154.
   c. In *Primary Server IP*, enter the IP address/FQDN of the AD 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*.



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 *Save*.

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 (`.crt` file) 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 154.

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 address objects on FortiGate for FortiAuthenticator and the LDAP server:

1. Go to *Policy & Objects* > *Addresses*, and select the *Address* tab.
2. In the *Address* tab, select *Create new*.
   The *New Address* window opens.
3. In *Name*, enter a name for the address, e.g., `FAC`.
4. In *IP/Netmask*, enter the public IP address of the FortiAuthenticator with its subnet mask.

`154.52.4.227` and `69.167.109.243` are the WAN IP addresses for FortiAuthenticator Cloud to build zero trust tunnels into an on-prem environment.

Use the IP address with its subnet mask.

5. Click *OK*.
   The address is used when Configuring an authentication rule.
6. Go to *Policy & Objects* > *Addresses*, select the *Address* tab.
7. In the *Address* tab, select *Create new*.
   The *New Address* window opens.
8. In *Name*, enter a name for the address, e.g., `lab-ad-address`.
9. In *IP/Netmask*, enter the private IP address of the LDAP server with its subnet mask.
10. Click *OK*.

To configure an authentication scheme with `user-cert` enabled on FortiGate:

1. Go to *Policy & Objects* > *Authentication Rules*.
2. From the *Create New* dropdown, select *Authentication Scheme*.
   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 on FortiGate:

1. Go to *Policy & Objects > Authentication Rules*.
2. From the *Create New* dropdown, select *Authentication Rule*.
   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 158.
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 *Connect On* pane:
   a. In the *Interface* dropdown, select an external interface.
      The *IP address* and the *Port* fields are automatically set to the selected interface and the default port 443.
      In the dropdown, select *+* to create a new interface.
   b. In *IP address*, enter the external IP address that the ZTNA clients, e.g., FortiAuthenticator, connect to.
   c. In *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.

If *Fortinet_Factory* is not selected as the default certificate, the local root CA configured/exported from FortiAuthenticator and imported to FortiGate can be used.

See:

- Configuring a local root CA
- Exporting the local root CA
- Importing the local root CA

   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.

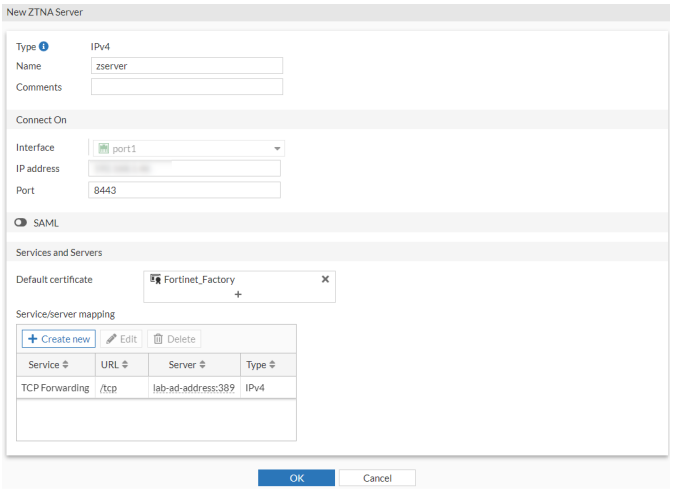
      ii. In *Service*, select *TCP Forwarding*.
      iii. In the *Server* pane:
         i. In the *Address* dropdown, select an address , e.g., `lab-ad-address`.
         ii. In *Ports*, enter a port number for the LDAP server, e.g., 389.

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 154.

By default, LDAP uses port 389.

iv. Click *OK*.

7. Click *OK*.

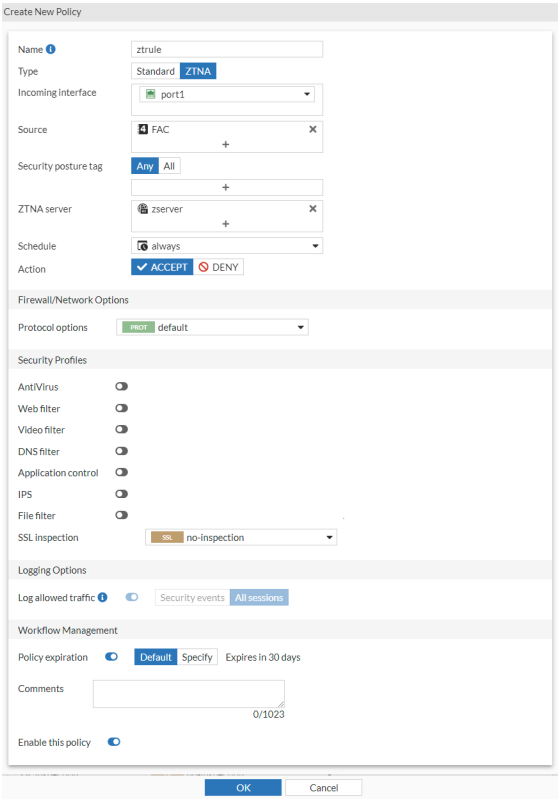


Configuring a ZTNA rule

To configure a ZTNA rule:

1. Go to *Policy & Objects > Firewall Policy*.
2. Select *Create new*.
   The *Create New Policy* window opens.
3. In *Name*, enter a name for the ZTNA policy.
4. Set *Type* to *ZTNA*.
5. In *Incoming Interface*, select the same interface as selected in Configuring a ZTNA server on page 158.
6. In *Source*, select *+*, and from the *Select Entries* list, select the address object for FortiAuthenticator.
   See Address object for FortiAuthenticator, and select *Close*.
7. In *ZTNA Server*, select the server created in Configuring a ZTNA server on page 158.

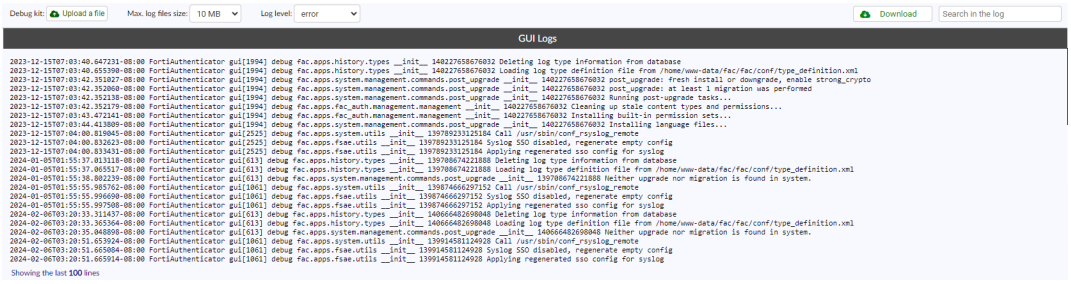
8. Click *OK*.



Debugging: Zero trust tunnel related issues

To debug:

1. Go to `https://<FortiAuthenticator-IP-Address>/debug`.
2. From the tree menu, go to *Others* > *GUI* to see extended FortiAuthenticator debug logs.



You can change the *Log level* to increase or decrease the depth of details.

Accessing WAD debug categories and setting them to the maximum level in a FortiGate ZTNA server:

To access WAD debug categories:

1. In the CLI console, enter the following command:

```
diagnose wad debug enable all
```

`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
```

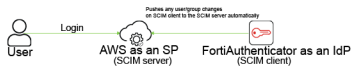
`cert-status`: success

```
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
```

FortiAuthenticator SCIM integration with AWS

System for Cross-domain Identity Management (SCIM) is an open standard for automating user identity information exchange between an identity provider (IdP) and a service provider (SP).

The following shows the SCIM topology being used in this example:



To set up FortiAuthenticator as a SCIM client for AWS as the SCIM SP:

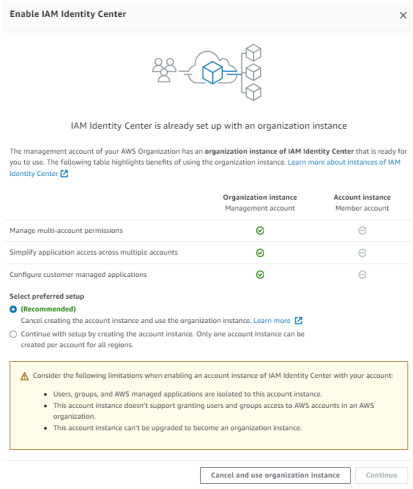
1. Enabling IAM Identity Center in AWS on page 162
2. Changing the identity source from IAM Identity Center to FortiAuthenticator on page 163
   a. Importing SP metadata on page 166
   b. Exporting the IdP metadata to the IAM Identity Center on page 167
   c. Importing the IdP certificate to the IAM Identity Center on page 167
3. Manage provisioning on page 168
4. Creating a local user on page 169
5. Creating a user group on page 170
6. Creating a new SCIM SP on page 171

Enabling IAM Identity Center in AWS

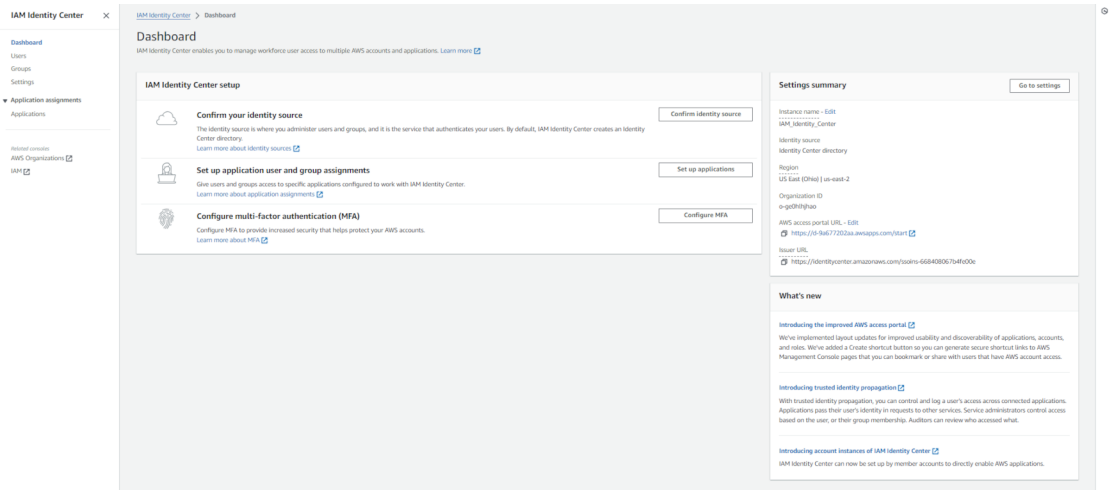
For information on AWS Identity Center, see What is IAM Identity Center.

To enable IAM Identity Center in AWS:

1. Log in to the IAM Identity Center console with administrative privileges.
2. In *Enable IAM Identity Center* on the right, select *Enable*.
   A new *Enable IAM Identity Center* page opens.



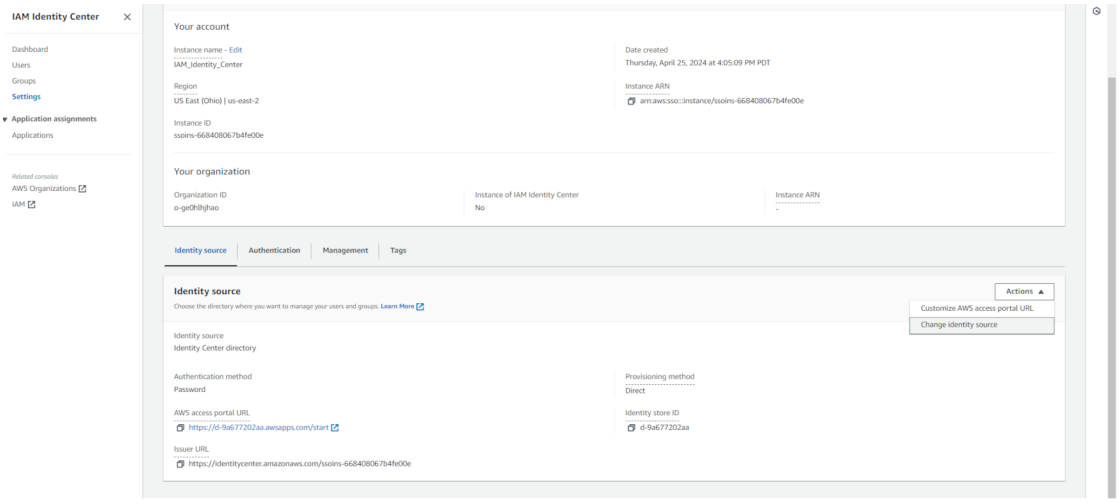
3. In *Select preferred setup*, select *Continue with setup by creating the account instance. Only one account instance can be created per account for all regions*.
4. Select *Continue*.
5. Optionally, select *Add new tag* to add tags to organize AWS resources in your IAM Identity Center instance.
6. Select *Enable*.
   The IAM Identity Center *Dashboard* opens.



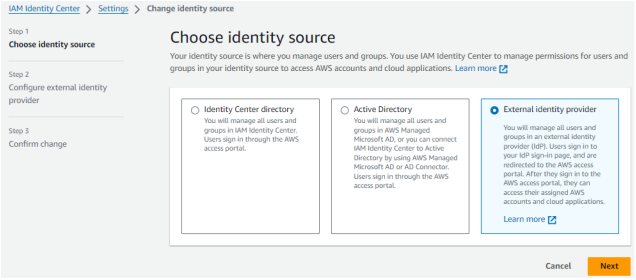
Changing the identity source from IAM Identity Center to FortiAuthenticator

To configure the identity source:

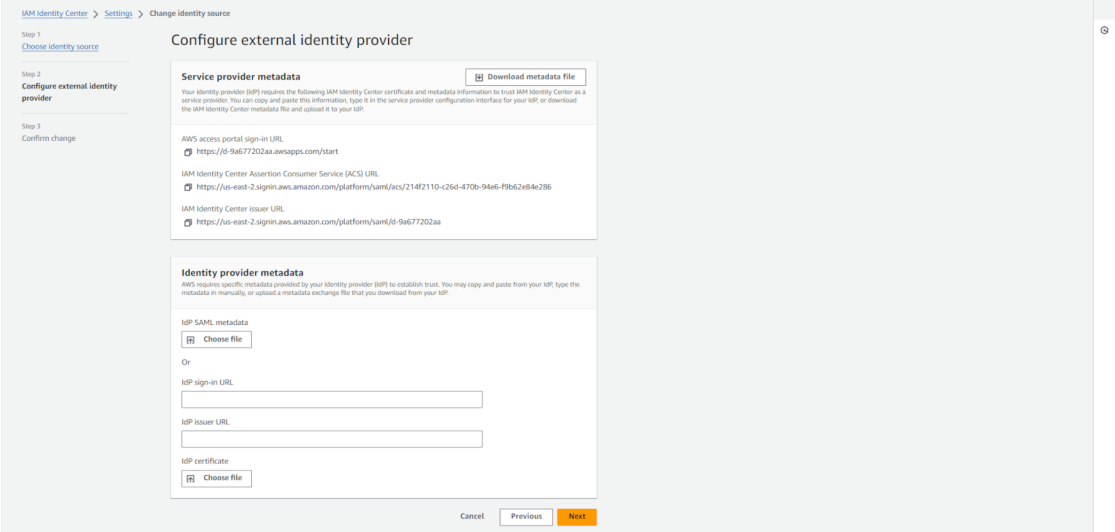
1. Go to *Settings* in IAM Identity Center.
2. In *Identity source*, from the *Actions* dropdown, select *Change identity source*.



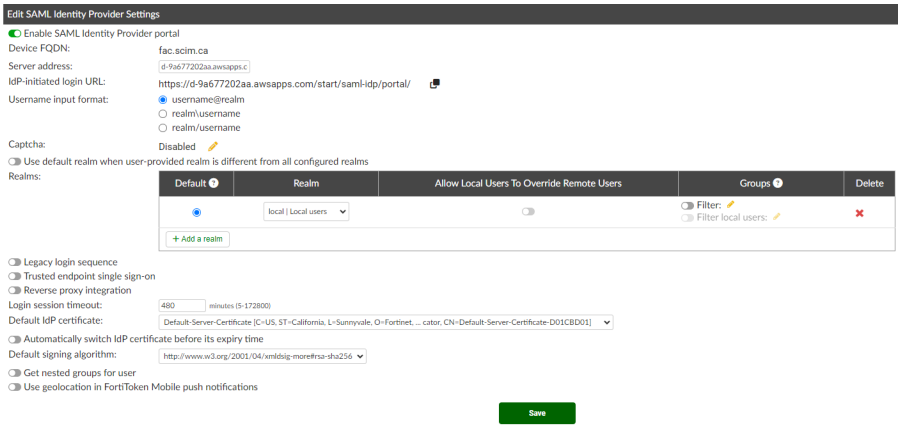
3. In *Choose identity source*, select *External identity provider*.



4. Click *Next*.
   The *Configure external identity provider* page opens.
   Keep the *Configure external identity provider* page open in a separate tab as you need it to perform steps 7, 8, and 9.

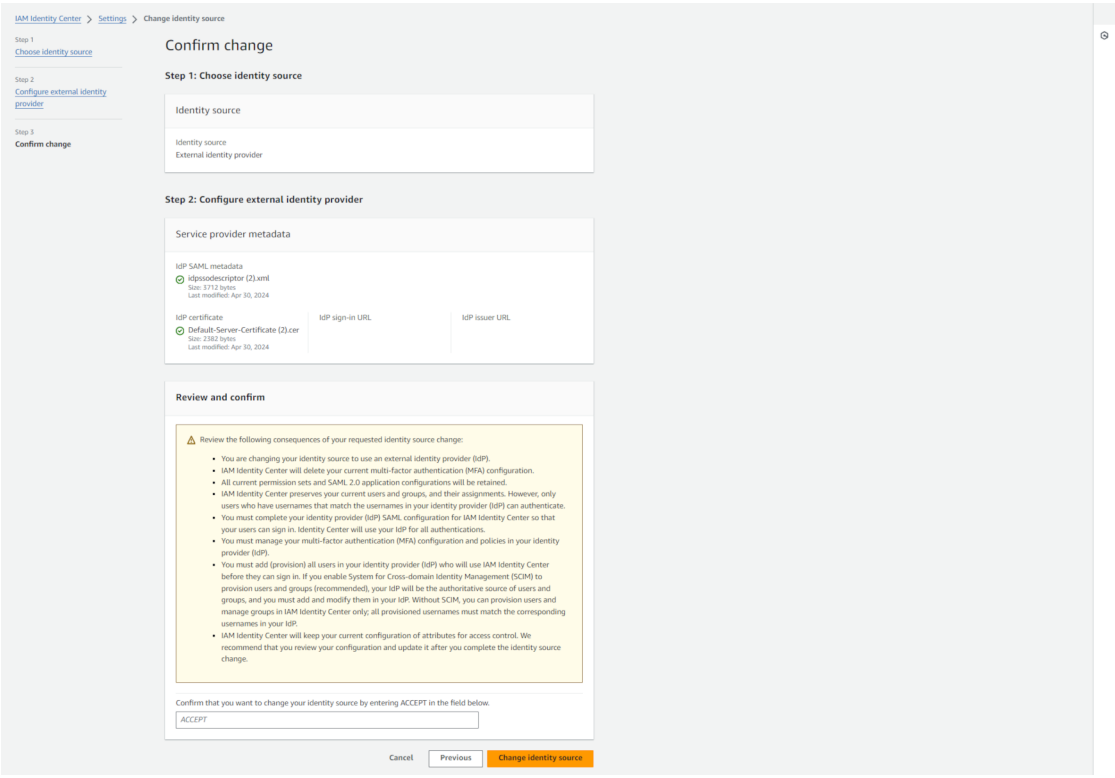


5. On FortiAuthenticator, go to *Authentication > SAML IdP > General*.
   a. Select *Enable SAML Identity Provider portal*.
   b. In *Server address*, enter the *AWS access portal sign-in URL* from the *Configure external identity provider* page in the IAM Identity Center.
   c. Select *Add a realm* to add the default local realm to which the users will be associated.
   d. In *Default IdP certificate*, select a default certificate the IdP uses to sign SAML assertions from the dropdown menu.
      In this example, the `Default-Server-Certificate` is selected.
   e. Select *Save*.

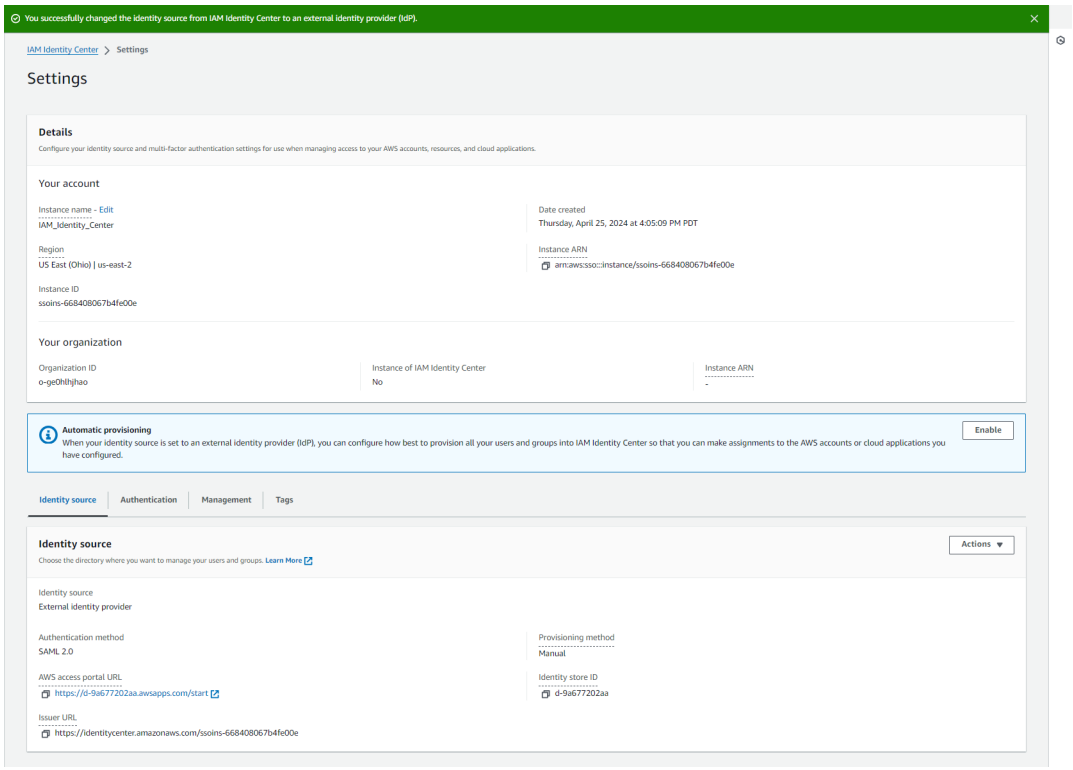


6. On FortiAuthenticator, go to *Authentication > SAML IdP > Service Providers*.
   a. Select *Create New*.
   b. In *SP name*, enter a name for the SP.
   c. In *Create an identifier for this IdP*, select *+*:
      i. In *Create Alternate IdP identifier* window, select *Random* to randomly generate an IdP identifier.
      ii. Click *OK*.
      IdP entity id, *IdP single sign-on URL*, and *IdP single logout URL* are populated automatically.
   d. In *Authentication method*, select *All configured password and OTP factors*.
   e. Click *Save*.
7. To import the SP metadata from the IAM Identity Center, see Importing SP metadata on page 166.

8. To export the IdP metadata to the IAM Identity Center, see Exporting the IdP metadata to the IAM Identity Center on page 167.
9. To import the IdP certificate to the IAM Identity Center, see Importing the IdP certificate to the IAM Identity Center on page 167.
10. Click *Next*.
    The *Confirm change* page opens.



11. Review your settings in the *Confirm change* page and enter *ACCEPT* in the *Confirm that you want to change your identity source by entering ACCEPT in the field below field*.
12. Select *Change identity source*.
    A green banner at the top confirms that you have successfully changed the identity source from IAM Identity Center to an external IdP, in this example, FortiAuthenticator.



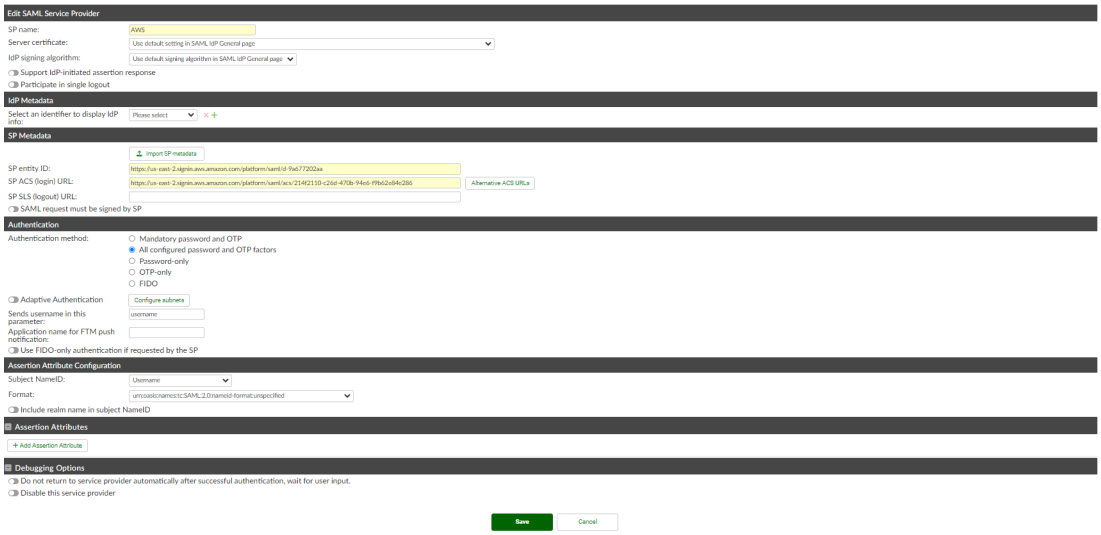
Importing SP metadata

We will be importing the SP metadata from the IAM Identity Center.

To import the SP metadata to the IAM Identity Center:

1. In the *Service Providers* list, click the recently created SP to edit it.
2. In the *Configure external identity provider* page opened in a separate tab as described in step 4 in Changing the identity source from IAM Identity Center to FortiAuthenticator on page 163, under the *Service provider metadata* pane, select *Download metadate file*.
   The SP metadata file is downloaded to your management computer.
3. On FortiAuthenticator, go to *Authentication > SAML IdP > Service Providers* and select the SP entry created in step 6 in Changing the identity source from IAM Identity Center to FortiAuthenticator on page 163.
4. In the *SP Metadata* pane, select *Import SP metadata*.
5. In the *Import Service Provider Metadata* pane, select *Upload a file*, locate the SP metadata file on your management computer, click *Open*.

6. Click *Save*.



Exporting the IdP metadata to the IAM Identity Center

We will be exporting the IdP metadata to the IAM Identity Center.

To export the IdP metadata to the IAM Identity Center:

1. In the *Service Providers* list, click the recently created SP to edit it.
2. In *IdP Metadata*, select an identifier from the dropdown.
3. Select *IdP metadata* to download the IdP metadata to your local computer.
4. In the *Configure external identity provider* page opened in a separate tab as described in step 4 in Changing the identity source from IAM Identity Center to FortiAuthenticator on page 163, under the *Identity provider metadata* pane, select *Choose file* in *IdP SAML metadata*, locate the IdP metadata file on your local computer, and click *Open*.

Importing the IdP certificate to the IAM Identity Center

To import the IdP certificate:

1. In the *Identity provider metadata* pane, we will be importing the IdP certificate.
2. In FortiAuthenticator, for this example, we are using the `Default-Server-Certificate`.
   You can verify the default IdP certificate being used by going to *Authentication > SAML IdP > General*.
3. Go to *Certificate Management > End Entities > Local Services*.
4. Select `Default-Server-Certificate` from the server certificate list, then select *Export Certificate* from the top.
   The IdP certificate is downloaded to your management computer.
5. In the *Configure external identity provider* page opened in a separate tab as described in step 4 in Changing the identity source from IAM Identity Center to FortiAuthenticator on page 163, under the *Identity provider metadata* pane, select *Choose file* in *IdP certificate*.
6. Locate the IdP certificate on your management computer, and click *Open*.
7. Continue from step 10 in Changing the identity source from IAM Identity Center to FortiAuthenticator on page 163.

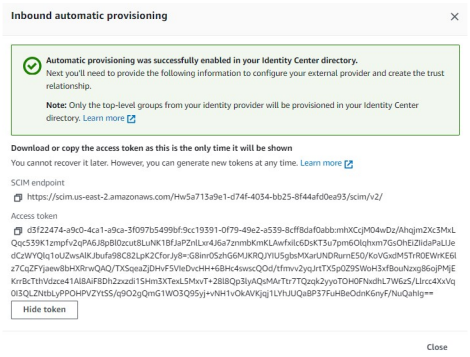
Manage provisioning

To manage provisioning:

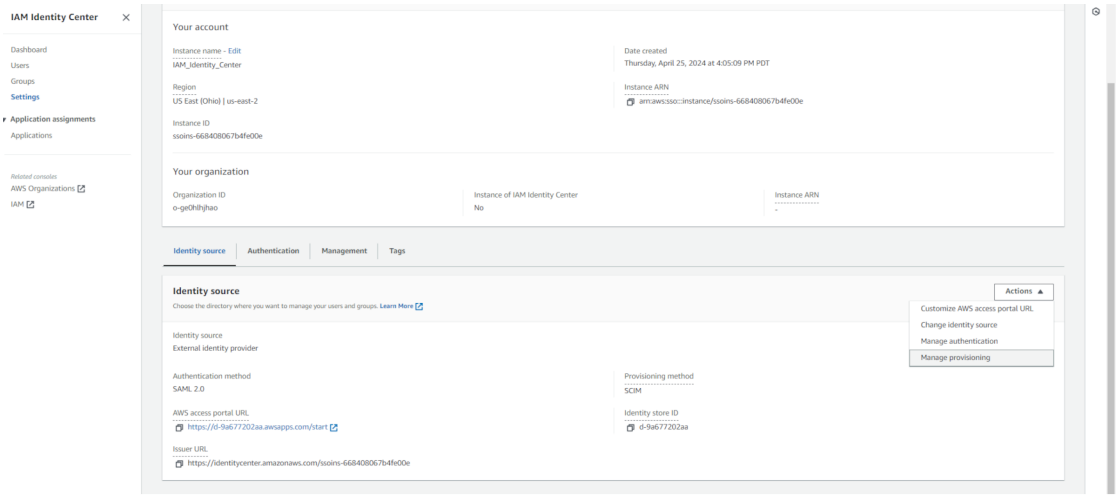
1. Ensure that the automatic provisioning is enabled for your identity center directory.

Copy and save the access token on your management computer as it is required on the FortiAuthenticator side.

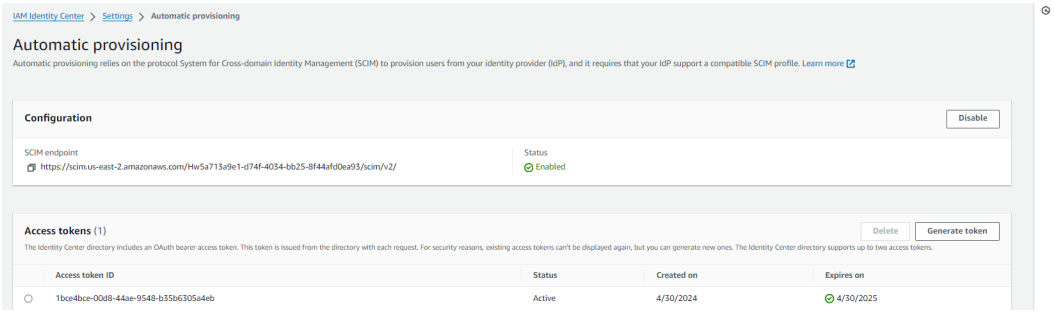
The access token is only displayed once. If you do not save it, you must generate a new access token.



2. Go to *Settings* in the IAM Identity Center.
3. In the *Identity source* tab, from the *Actions* dropdown, select *Manage Provisioning*.



The *Automatic provisioning* tab opens.



AWS generates the *SCIM endpoint* and the *Access token*.

Copy and save the *SCIM endpoint* and the *Access token* on your management computer.

SCIM endpoint and *Access token* are needed on the FortiAuthenticator side.

Creating a local user

To create a local user:

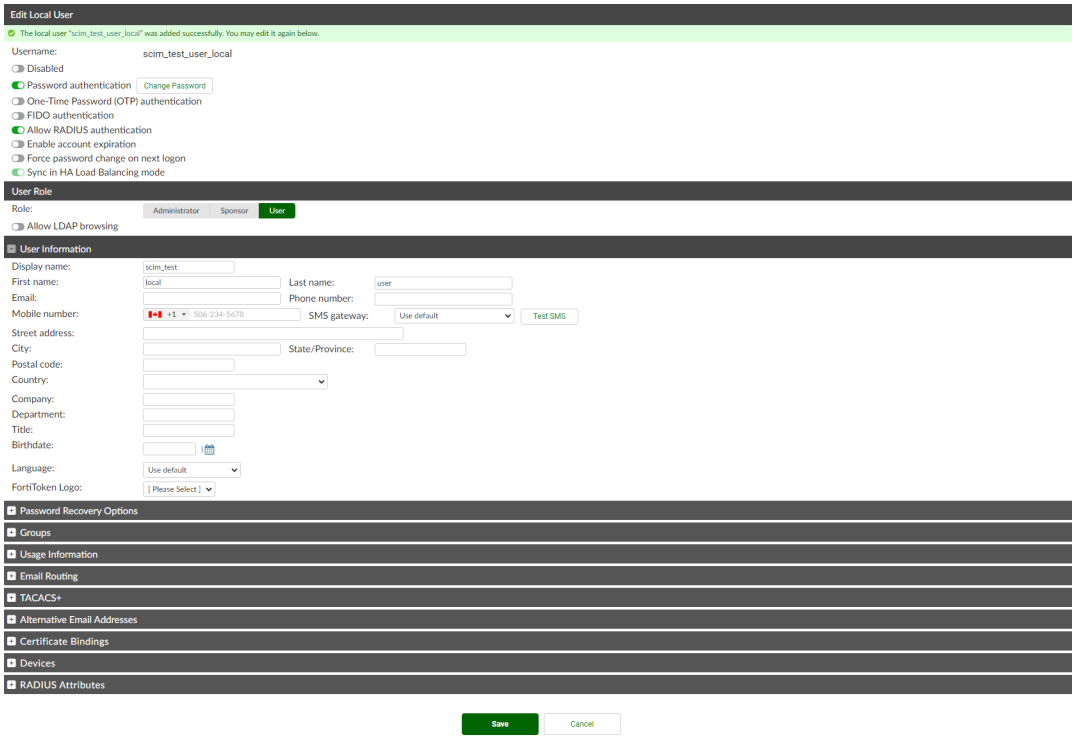
1. On FortiAuthenticator, go to *Authentication > User Management > Local Users*.
2. Select *Create New* to create a new user.
3. In *Username*, enter a user name.
4. Ensure that *Password creation* is set to *Specify a password*.
5. In *Password*, enter a password.
6. Confirm the password in the *Password* confirmation field.
7. Click *Save*.
   The *Edit Local User* window opens.

AWS requires the following four fields:

- *Username*
- *Display name*
- *First name*
- *Last name*

If any of the above user related fields are missing, AWS rejects the sync.

8. Fill in the remaining required fields in the *User Information* pane, i.e., *Display name*, *First name*, and *Last name*.



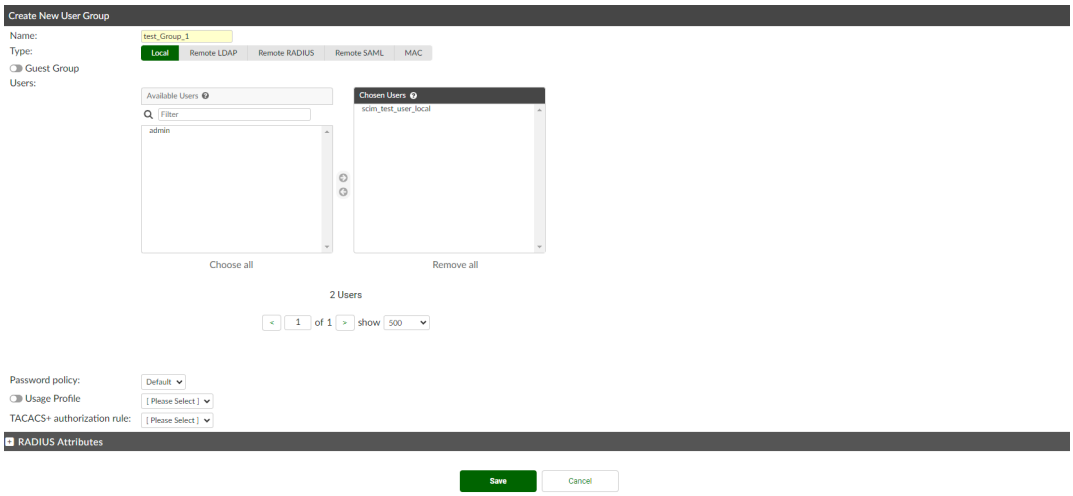
9. Click *Save*.

Creating a user group

To create a user group:

1. On FortiAuthenticator, go to *Authentication > User Management > User Groups*.
2. Select *Create New*.
   The *Create New User Group* window opens.
3. In Name, enter a name for the user group.
4. In Type, select Local.
5. From the *Available Users* list, select the recently created local user in Creating a local user on page 169 and move it to *Chosen Users*.

6. Click *Save*.



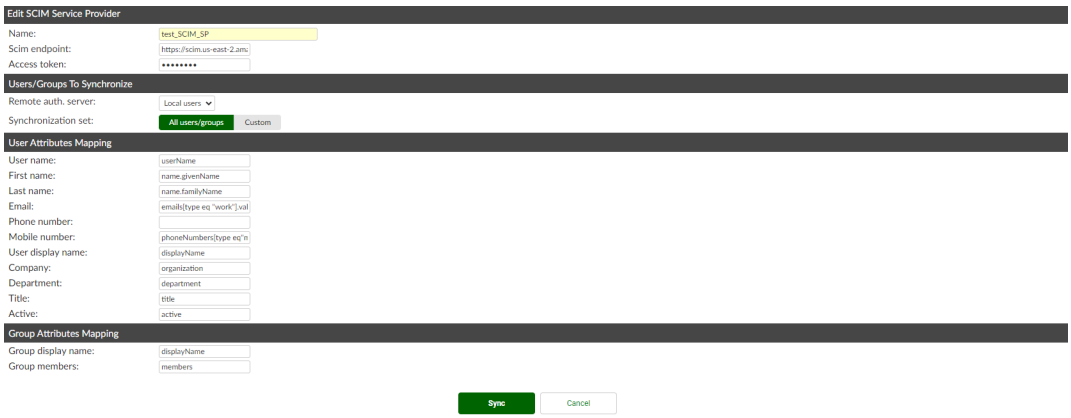
Creating a new SCIM SP

To create a new SCIM SP:

1. In FortiAuthenticator, go to *Authentication > SCIM > Service Provider*.
2. Select *Create New*.
   The *Create New SCIM Service Provider* window opens.
3. In *Name*, enter a name for the SCIM SP.
4. In Scim endpoint, enter the SCIM endpoint URL that you earlier copied and saved in Manage provisioning on page 168.
5. In *Access token*, enter the access token that you earlier copied and saved in Manage provisioning on page 168.

The fields in *User Attributes Mapping* are the variables for the JSON schema being imported to AWS, e.g., the FortiAuthenticator user name will map to the user name of the JSON schema.

6. Click *Sync*.



Log in to a Windows host using SSOMA

In this example:

- We use SSOMA to log in to a Windows host.
- An AD server is the remote LDAP server.

For information on SSOMA, see FortiClient SSO Mobility Agent in the latest *FortiAuthenticator Administration Guide*.

To log in to a Windows host using SSOMA:

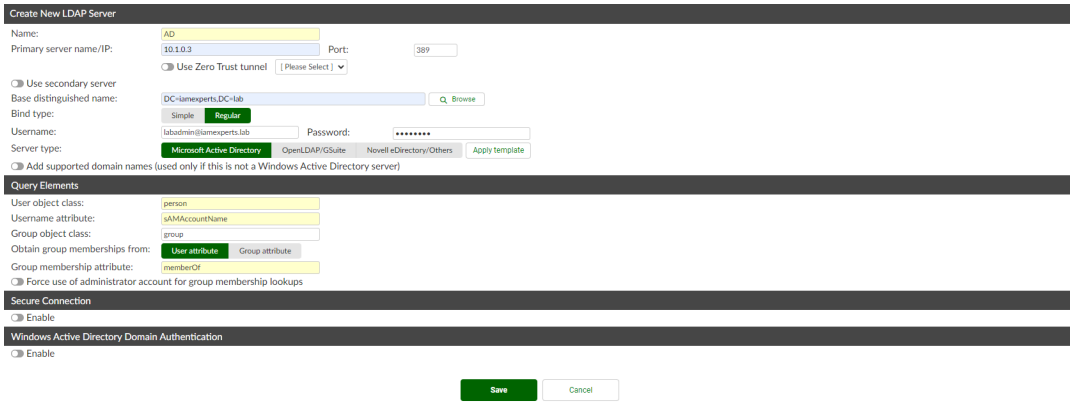
1. Configuring a remote LDAP server on page 172
2. Enabling FSSO service on page 173
3. Configuring SSO settings on page 173
4. Installing SSOMA on page 174
5. Result on page 175

Configuring a remote LDAP server

We configure an LDAP connection to an Active Directory (AD) server on FortiAuthenticator.

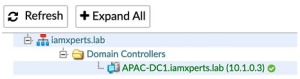
To configure a remote LDAP server on FortiAuthenticator:

1. Go to *Authentication > Remote Auth. Servers > LDAP*, and select *Create New*.
   The *Create New LDAP Server* window opens.
2. In *Name*, enter a name.
3. In *Primary server name/IP*, enter the AD server IP address.
4. In *Base distinguished name*, enter `DC=iamexperts,DC=lab`.
5. In *Bind type*, select *Regular*.
6. In *Username*, enter the user name.
7. In *Password*, enter a password.
8. Ensure that the *Server type* is *Microsoft Active Directory*.
9. Leave the settings in the *Query Elements* pane as default.
10. Click *Save*.



Ensure that you can browse the AD tree (IAM OU) by clicking *Browse* in *Base distinguished name* when editing the LDAP server.

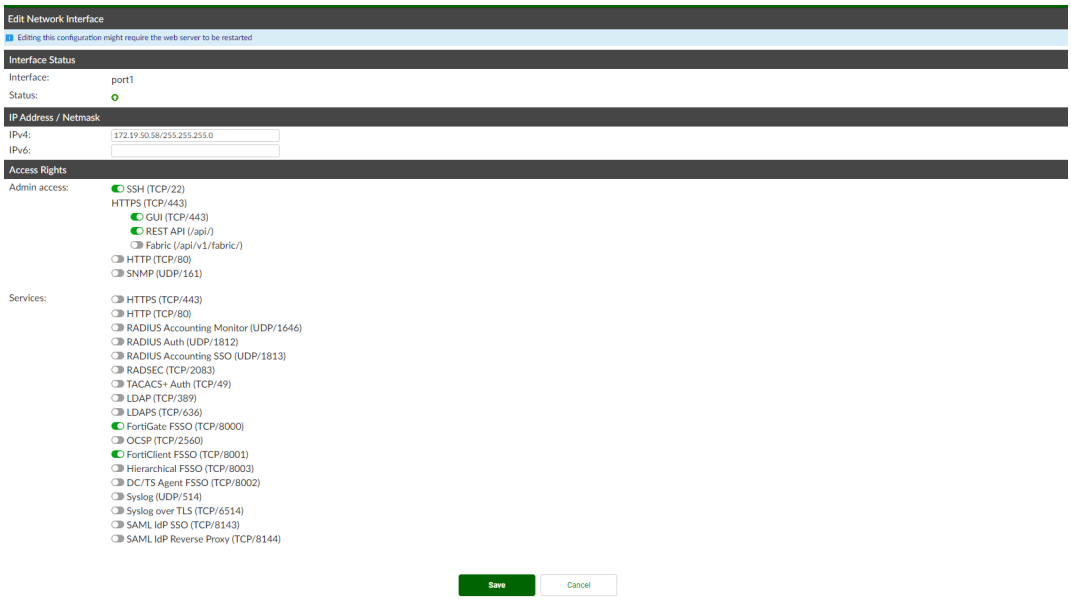
Go to *Monitor > SSO > Domains* to see all the configured DC/LDAP servers as well as the known domains that have been provisioned.



Enabling FSSO service

To enable FSSO service:

1. Go to *System > Network > Interfaces*, and double-click *port1* to edit it.
2. In *Access Rights*, in *Services*, enable *FortiGate FSSO (TCP/8000)* and *FortiClient FSSO (TCP/8001)*.
3. Click *Save*.



FortiAuthenticator restarts.

Configuring SSO settings

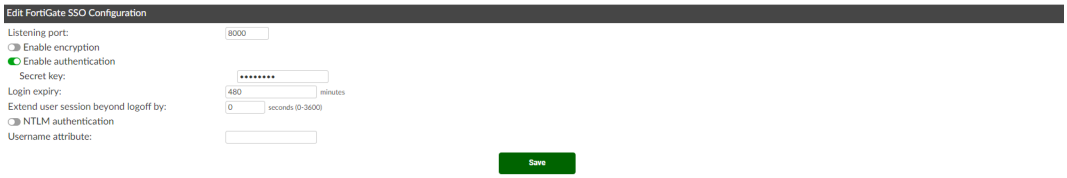
To configure SSO FortiGate setting:

1. **Add a secret key**:
   a. Go to *Fortinet SSO > Settings > FortiGate*.
   b. Select *Enable authentication*.

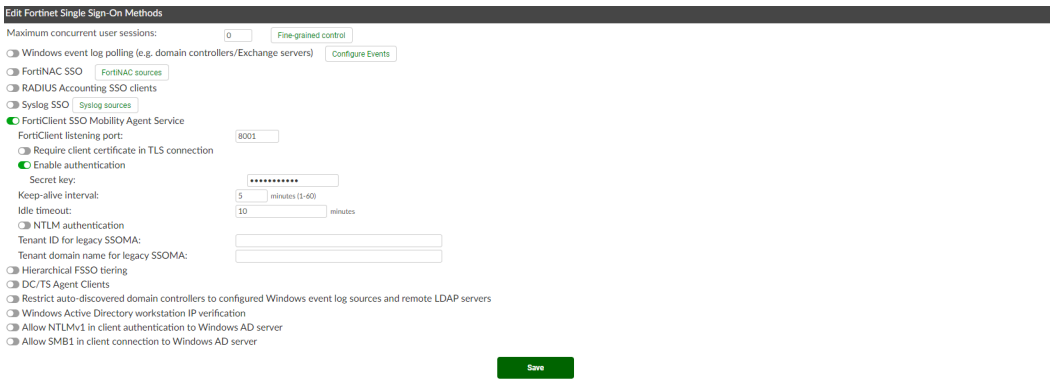
c. Enter a *Secret key*.

The *Secret key* must match the value entered in the FSSO connector on FortiGate.

d. Click *Save*.



2. **Enabling FortiClient SSO Mobility Agent Service**:
   a. Go to *Fortinet SSO > Settings > Methods*.
   b. Enable *FortiClient SSO Mobility Agent Service*.
   c. Ensure that *Enable authentication* is selected and the *Secret key* matches `SSOPSK` set when installing the SSOMA.
   See Installing SSOMA on page 174.
   d. Click *Save*.

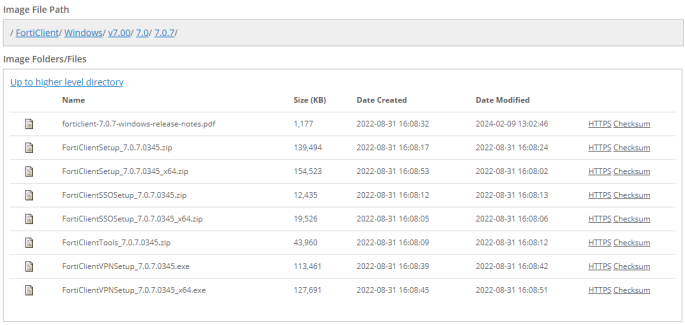


Installing SSOMA

We install SSOMA on a Windows host.

To install SSOMA:

1. Log in to the FortiCare portal.
2. Go to *Support > Firmware Download*.
3. From the *Select Product* dropdown, select *FortiClient*, and select *Download*.
4. In Image *Folders/Files*, go to *Windows*, and download the SSOMA setup zip file (`FortiClientSSOSetup_7.x.x.x_x64.zip`) from one of the version directories.



5. Extract and save the installer to `C:\Fortinet`.
6. In Command Prompt, go to the directory where the `FortiClient.msi` was extracted.

```
cd C:\Fortinet\
```

7. In the Command Prompt, run the following command:

```
FortiClientSSO.msi SSOSERVER="10.255.255.12" SSOPORT="8001" SSOPSK="F0rtiXperts"
```

`SSOSERVER` is your FortiAuthenticator IP address or FQDN.

`SSOPORT` is the *FortiClient listening port* in *Fortinet SSO > Settings > Methods* when *FortiClient SSO Mobility Agent Service* is enabled.

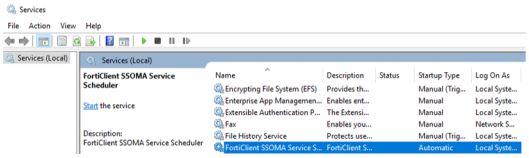
See Configuring SSO settings on page 173.

`SSOPSK` is the *Secret key* set up in *Fortinet SSO > Settings > Methods* when *FortiClient SSO Mobility Agent Service* and *Enable authentication* are selected.

See Configuring SSO settings on page 173.

The installer runs and the SSOMA service is started.

8. You can check if the SSOMA service is running by going to *Services* on the Windows host.



Result

1. Log in to the Windows host.
2. Go to *Monitor > SSO > SSO Sessions* to see information about the recent SSO session.

FortiAuthenticator SSOMA for native Microsoft Entra ID joined workstation

In this example, an endpoint is joined to Microsoft Entra ID. When the endpoint connects to the network, the SSOMA shares the identity and the IP address with the FortiAuthenticator.

The FortiAuthenticator then does a group lookup and shares the identity with the FortiGate device.

If the endpoint now moves from a wired to a wireless connection, the SSOMA shares the updated IP address with FortiAuthenticator which then shares the information with the FortiGate device.

For information on this feature, see *FSSO for cloud-native Azure AD users* in the *FortiAuthenticator 6.5.5 Administration Guide*.

Prerequisites:

- FortiAuthenticator 6.5.0 or above
- FortiClient 7.2.0 or above
- A Windows 10/11 endpoint that supports Microsoft Entra ID
- Microsoft Entra ID tenant

Authentication flow:

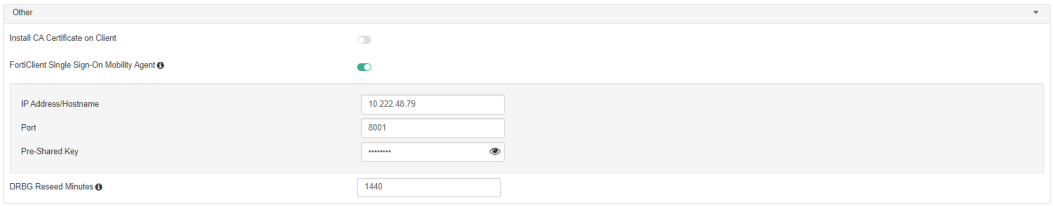
1. The user logs on to Microsoft Entra ID joined workstation.
2. The SAML session is transparently set up in the background on Azure.
3. SSOMA retrieves the user identity.
4. SSOMA shares the user name and the IP address with FortiAuthenticator.
5. FortiAuthenticator retrieves the group information (OAuth).
6. FortiAuthenticator sends the user identity to FortiGate devices configured to receive.
7. Identity-based access to all FortiGate service is provided transparently without the user needing to reenter credentials.

FortiAuthenticator SSOMA for native Microsoft Entra ID joined workstation

Enabling SSOMA on FortiClient EMS

To enable SSOMA on FortiClient EMS:

1. Go to *Endpoint Profiles > System Settings*.
2. Select *Edit* next to a profile to edit it.
3. Switch to the *Advanced* tab.
4. In *Other*:
   a. Enable *FortiClient Single Sign-On Mobility Agent*.
   b. In IP Address/Hostname, enter the IP address for the endpoint.
   c. In *Port*, enter `8001`.
   d. Enter a pre-shared key.
5. Click *Save*.



Configuring `prefer_azure` on the EMS

Configuring `prefer_azure` on the EMS

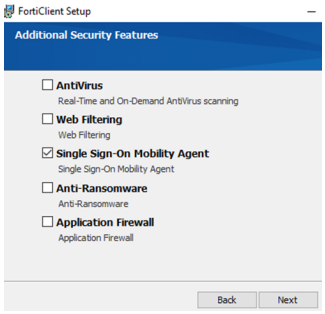
1. In EMS, edit the desired endpoint profile's XML configuration to match the IP address, port, and PSK configured on the FortiAuthenticator, and to have FortiClient detect Azure user information and send it to FortiAuthenticator.

```
<fssoma>
      <enabled>1</enabled>
      <serveraddress>10.222.48.79</serveraddress>
      <presharedkey>Fortinet123!</presharedkey>
      <prefer_azure>1<prefer_azure>
<fssoma>
```

To set up `prefer_azure_registry` key on SSOMA, see:
https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-How-to-install-a-standalone-Windows-FSSO-Mobility/ta-p/298044

Installing SSOMA with FortiClient

When installing FortiClient on the endpoint, make sure to select *Single Sign-On Mobility Agent* in the *Additional Security Features* window.



Check that the configuration that you added in Enabling SSOMA on FortiClient EMS on page 177 is applied on FortiClient in *Settings > Advanced*.

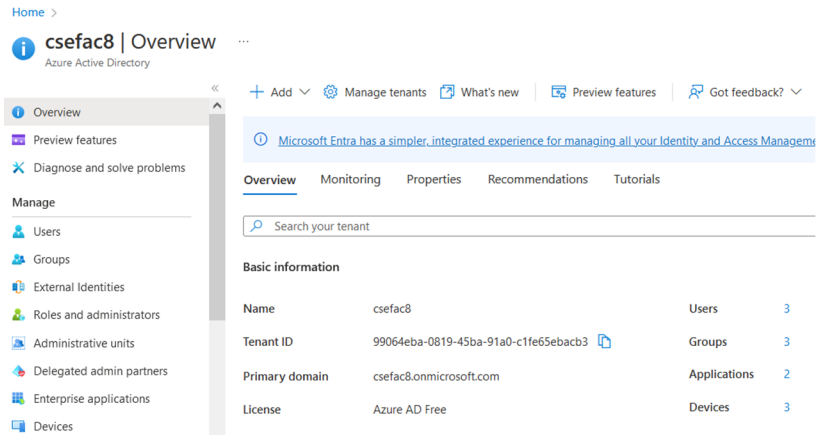
To install the standalone Windows FSSO Mobility Agent, see Technical Tip: How to install a standalone Windows FSSO Mobility Agent.

Creating a Microsoft Entra ID tenant

To create a Microsoft Entra ID tenant:

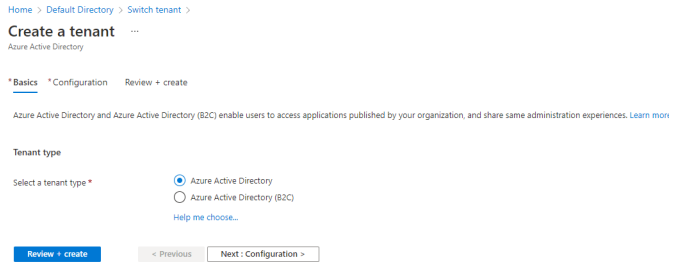
To create a tenant:

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

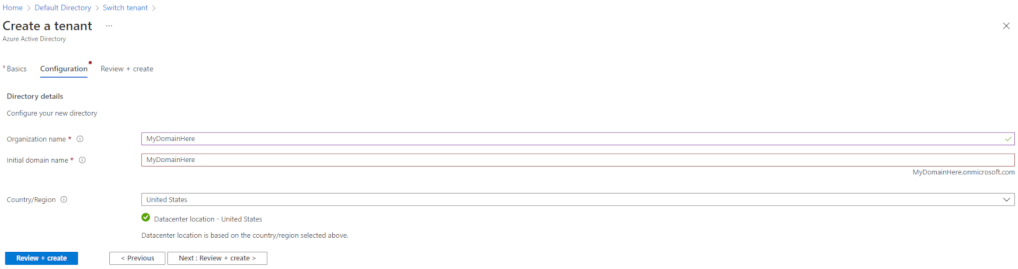


3. In *Overview*, Select *Manage tenants*, and then select *Create*.
   Create a tenant window opens.

4. In the *Basics* tab, select *Azure Active Directory* as the tenant type, and select *Next: Configuration*.



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



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

To switch to the correct directory:

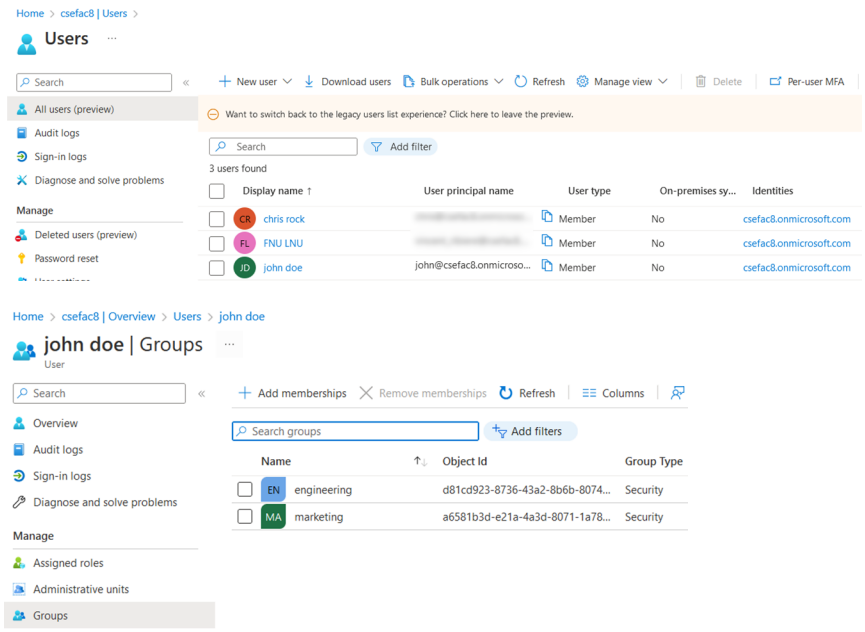
1. Click the user icon on the top right.
2. Select *Switch directory*.
3. From the list, select *Switch* for the directory you intend to use.

Creating a user and associating with groups

We create a user `john doe` associated with *engineering* and *marketing* groups on the Azure portal.

To create a user and associate it with groups:

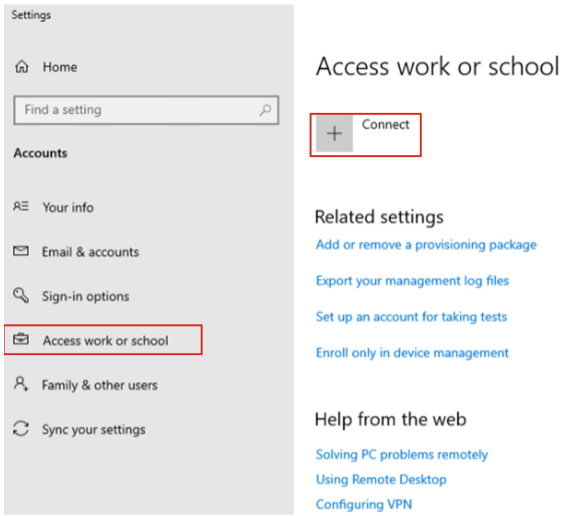
1. In Azure portal, go to *Users*.
2. Select *+New user*.
3. In *Basics*:
   a. In *User principal* name, enter a user name.
   b. In *Display name*, enter a display name.
   c. In *Password*, enter a password.
   d. Select *Account enabled*.
   e. Click *Next: Properties*.
4. In the *Properties* tab, fill in user identity, job, and contact information.
5. Click *Next: Assignments*.
6. In *Assignments*:
   a. Select *+Add group*.
   b. From *Select group*, select *engineering* and *marketing* groups.
   c. Click *Next: Review + create*.



Joining the Windows 10 endpoint to Microsoft Entra ID

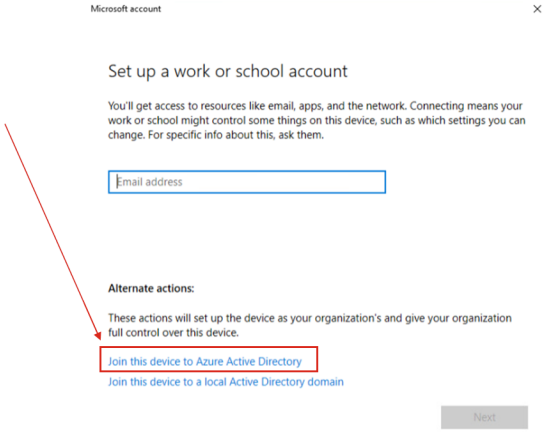
To join the Windows 10 endpoint to Microsoft Entra ID:

1. On the Windows 10 endpoint, open *Settings* > *Email & accounts*.
2. Select *Access work or school*.
3. Select *Connect*.

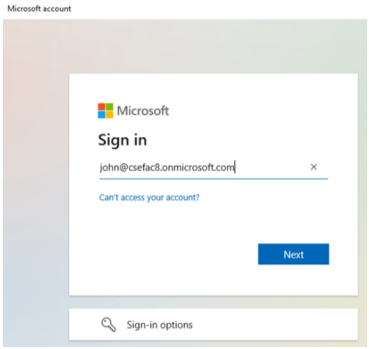


Ensure that the endpoint is not joined to an on-prem AD domain.

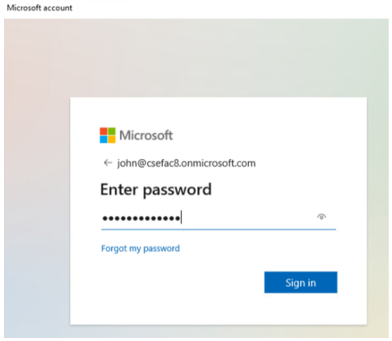
4. Select *Join this device to Azure Active Directory*.



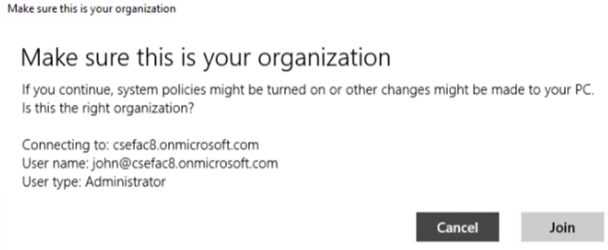
5. Sign in with the Microsoft Entra ID user, e.g., *john@csefac8.onmicrosoft.com*, and click *Next*.

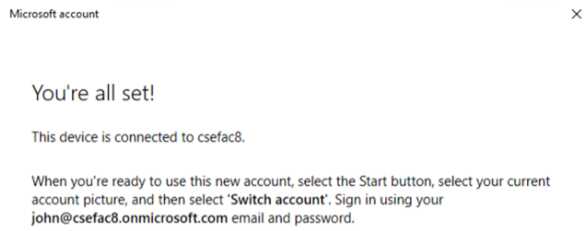


6. Enter the password and click *Sign in*.



7. Note that the domain is the Microsoft Entra ID primary domain and select *Join*.

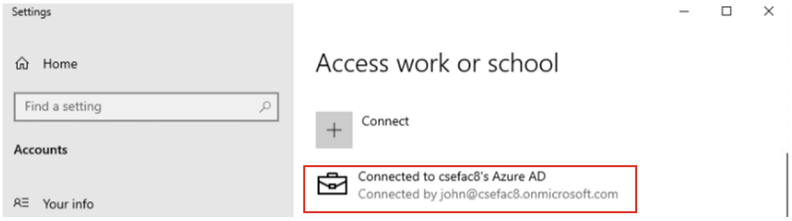




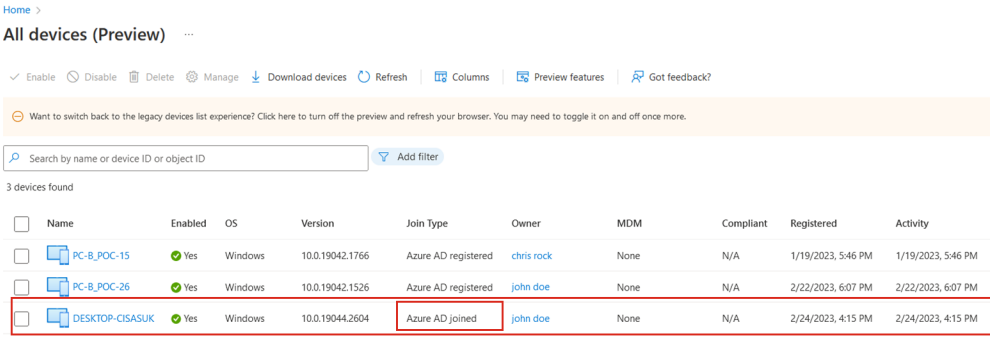
Verifying that the endpoint is domain joined

To verify that the endpoint is domain joined:

1. On the endpoint, open *Settings* > *Email & accounts*.
2. Select *Access work or school*.
   You will see that the endpoint is connected to the Microsoft Entra ID tenant configured in Creating a Microsoft Entra ID tenant on page 178.



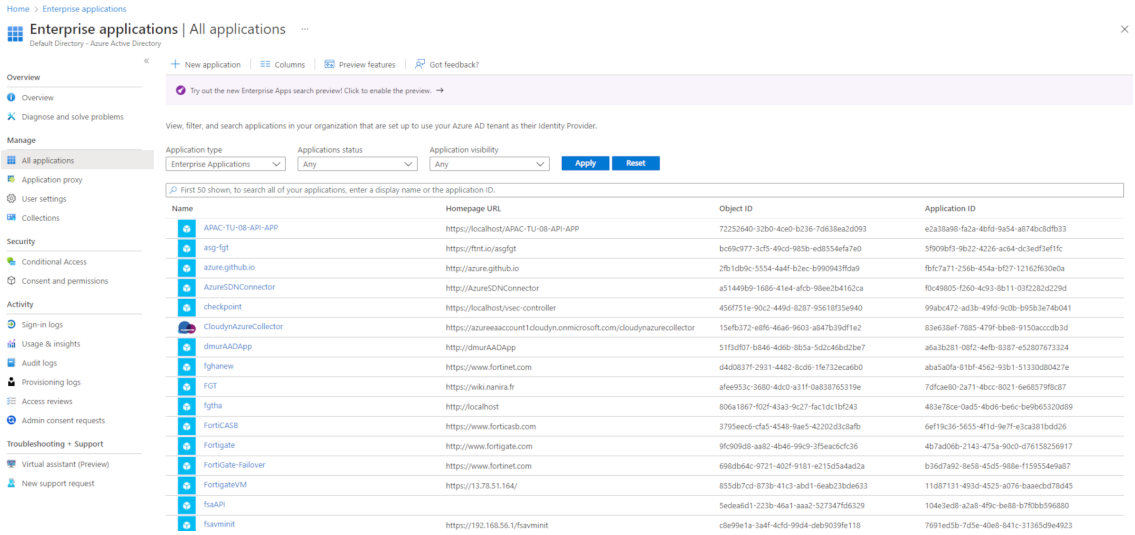
3. On the Azure portal, in *All devices*, you can see that the endpoint is Microsoft Entra ID joined.



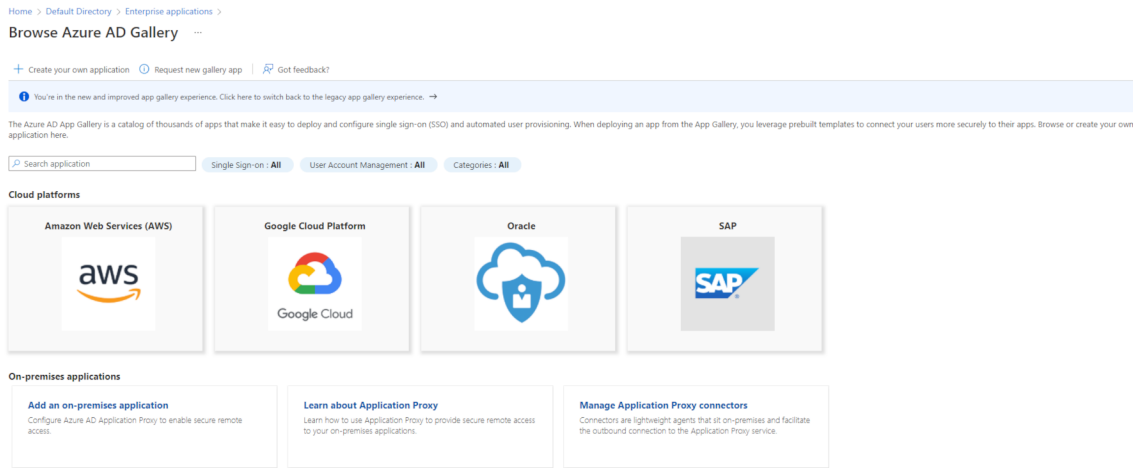
Creating FortiAuthenticator enterprise application

To create a FortiAuthenticator enterprise application:

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

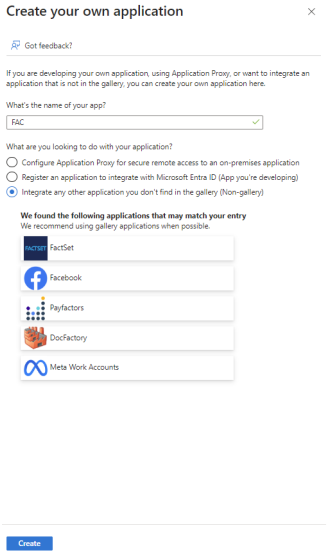


2. In *Enterprise applications*, select *New application*.
The *Browse Azure AD Gallery* page opens.

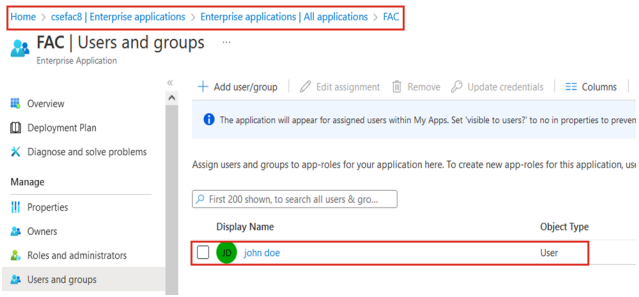


3. In the *Browse Azure AD Gallery*, select *Create your own application*.
The *Create your own application* window opens.

4. In the *Create your own application* window, enter a name for the application, and select *Create*.



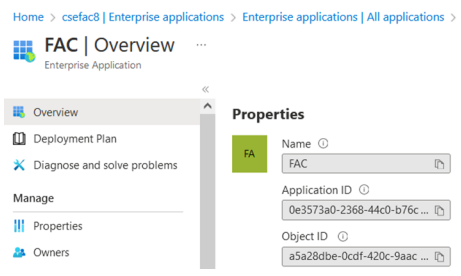
5. In the newly created enterprise application, select *Assign users and groups*.
6. Select *Add user/group*.
7. In the *Add Assignment* page, select *None Selected*.
8. From *Users and groups*, select to add the user created in Creating a user and associating with groups on page 179.
9. Select *Assign* to assign the user to the application.



Getting application ID and the authentication key

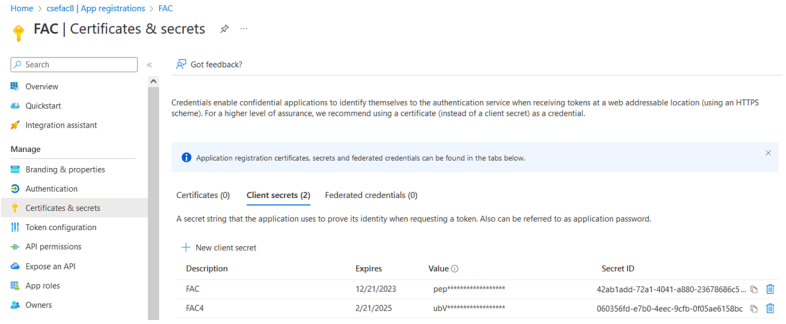
The application ID and key is needed for MS Graph API (OAuth based).

Note down the *Application ID* for the application created in Creating FortiAuthenticator enterprise application on page 183.



To get the authentication key:

1. In the Microsoft Entra ID tenant created in Creating a Microsoft Entra ID tenant on page 178, go to *Manage > App registrations*.
2. In the *All applications* tab, select the application created in Creating FortiAuthenticator enterprise application on page 183.
3. Go to *Manage > Certificates & secrets*.
4. Select *New client secret*.
5. In *Add a client secret*:
   a. Enter a description.
   b. Click *Add*.
      The key is displayed.
   c. Copy and save the key value on your management computer. You cannot retrieve the key later.

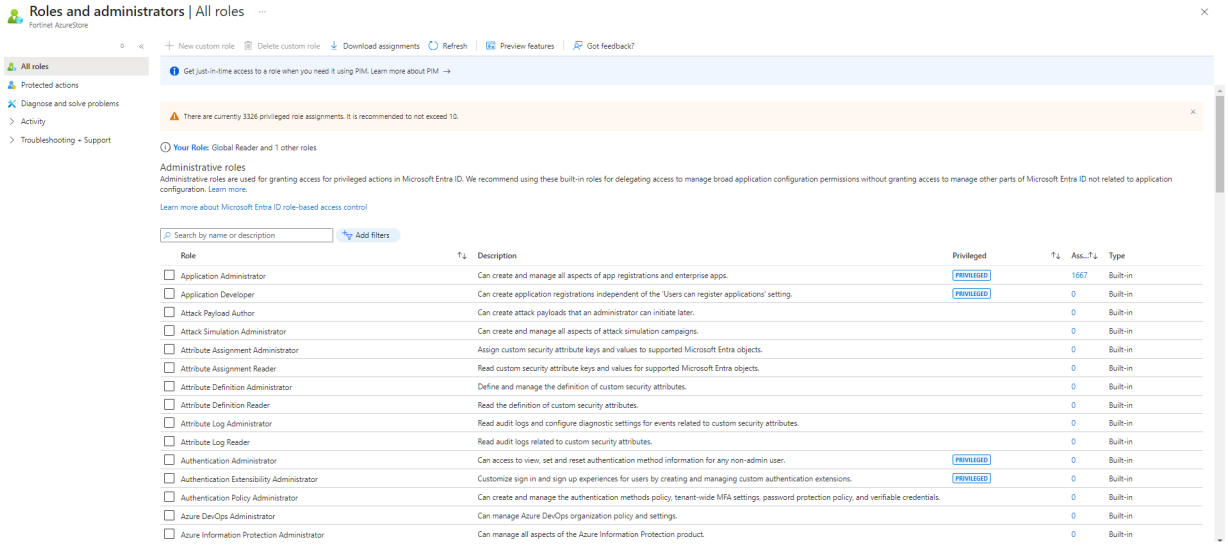


Adding the application to directory readers role

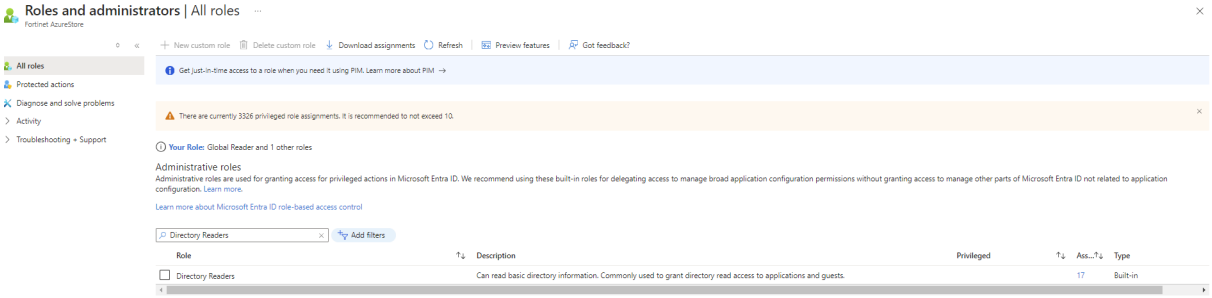
We assign Directory Readers role for the application created in Creating FortiAuthenticator enterprise application on page 183. The role allows the application to read the directory to determine the group membership for users.

To add the application to directory readers role:

1. In the Azure portal, go to *Microsoft Entra ID > Roles and administrators*.



2. In the search bar, enter *Directory Readers*.

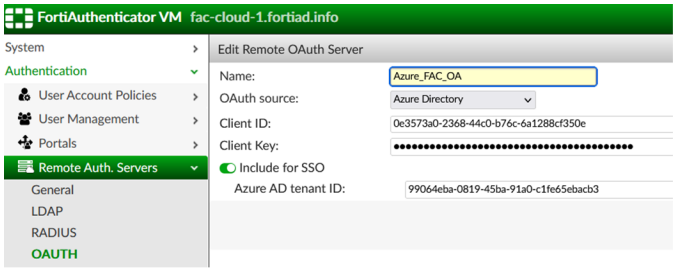


3. Select *Directory Readers*, click *Description*, and go to *Assignments*.
4. Select *Add assignments*.
5. From the list, look up the application, select, and click *Add*.

Provisioning OAuth API on FortiAuthenticator

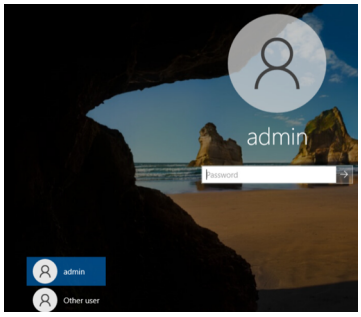
To provision OAuth API on FortiAuthenticator:

1. On FortiAuthenticator, go to *Authentication > Remote Auth. Servers > OAUTH*.
2. Select Create New.
3. Enter a name for the remote OAuth server.
4. In *OAuth source*, select *Azure Directory*.
5. In *Client ID*, enter the application ID from Getting application ID and the authentication key on page 184.
6. In *Client Key*, enter the authentication key from Getting application ID and the authentication key on page 184.
7. Enable *Include for SSO*, and in *Azure AD tenant ID*, enter the tenant ID from Creating a Microsoft Entra ID tenant on page 178.
   Azure AD tenand ID is used used by FortiAuthenticator upon receiving SSOMA update from FortiClient to know which OAuth server /Azure tenant to query.
8. Click *Save*.

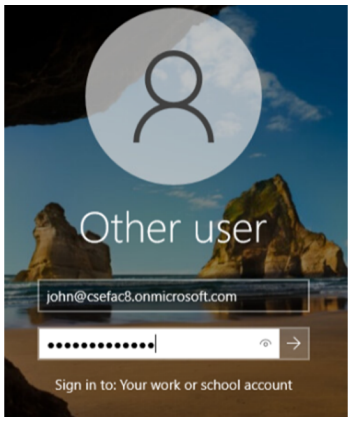


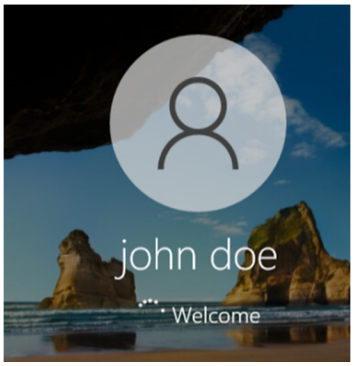
Results

1. When logging in to Microsoft Entra ID, select *Other user*.



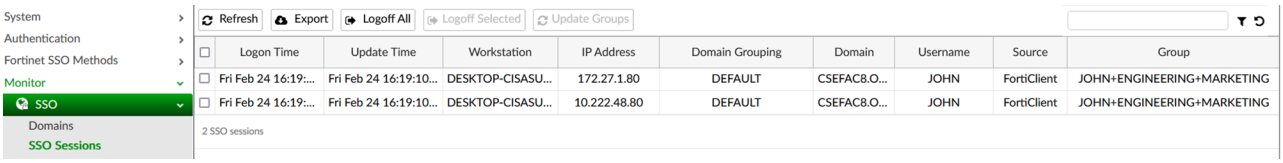
2. Log in as *john@csefac8.onmicrosoft.com*.



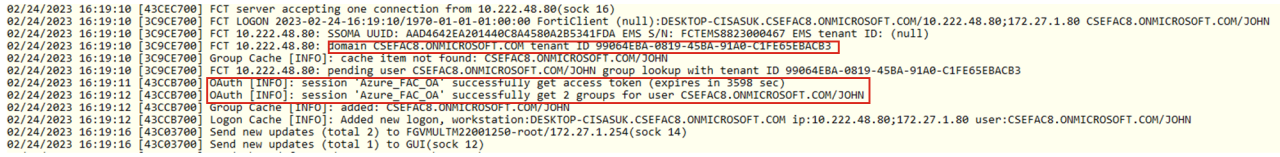


FSSO sessions and debug logs

On FortiAuthenticator, when you go to *Monitor > SSO Sessions*, you can see the FSSO sessions.



Go to extended debug logs `https://<FortiAuthenticator-IP-Address>/debug` to see FSSO debug logs in *Log Categories > Single Sign On*.



Federation and identity integrations (SAML, OAuth)

SAML IdP proxy for Azure

This example 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 189
2. Configuring the remote SAML server on page 190
3. Creating a remote SAML user synchronization rule on page 194
4. Configuring an Azure realm on page 191
5. Configuring SAML IdP settings on page 192
6. Configuring SP settings on FortiAuthenticator on page 193
7. Configuring the login page replacement message on page 192
8. Results on page 193

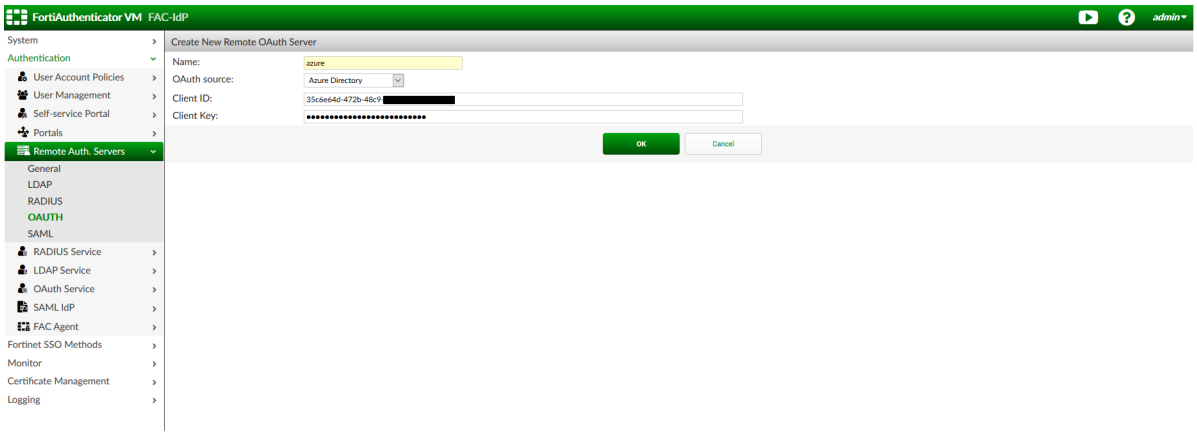
Configuring OAuth settings

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 190 and Creating a remote SAML user synchronization rule on page 194.

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.

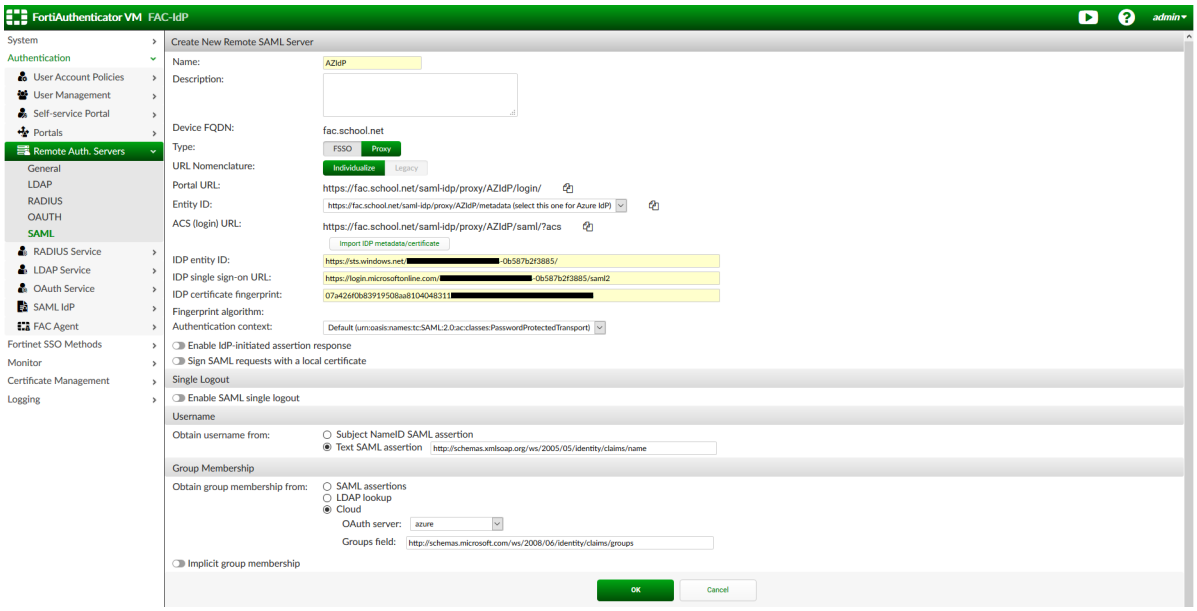


4. Click *OK* to save changes.

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 189.
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.



6. Click *OK* to save changes.

Configuring an Azure realm

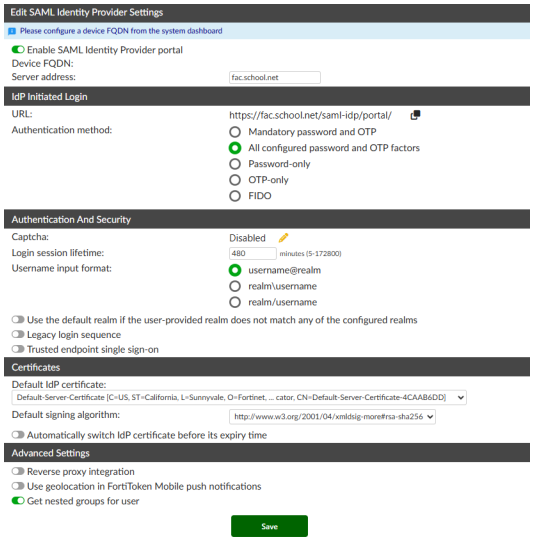
To create an Azure realm and add it to the IdP:

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. Select *Enable SAML Identity Provider portal*, and enter the following:
   a. **Server address**: Enter the FortiAuthenticator FQDN.
   b. **Default IdP certificate**: Select a default certificate to use.

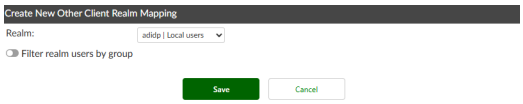


3. Click *Save*.

To add a realm:

Starting FortiAuthenticator 6.6.3, to add a realm for SAML IdP, go to *Authentication > SAML IdP > User Sources*.

1. Go to *Authentication > SAML IdP > User Sources*, and select *Create New*.
2. From the *Realm* dropdown, select the realm associated with the remote server for Azure IdP.



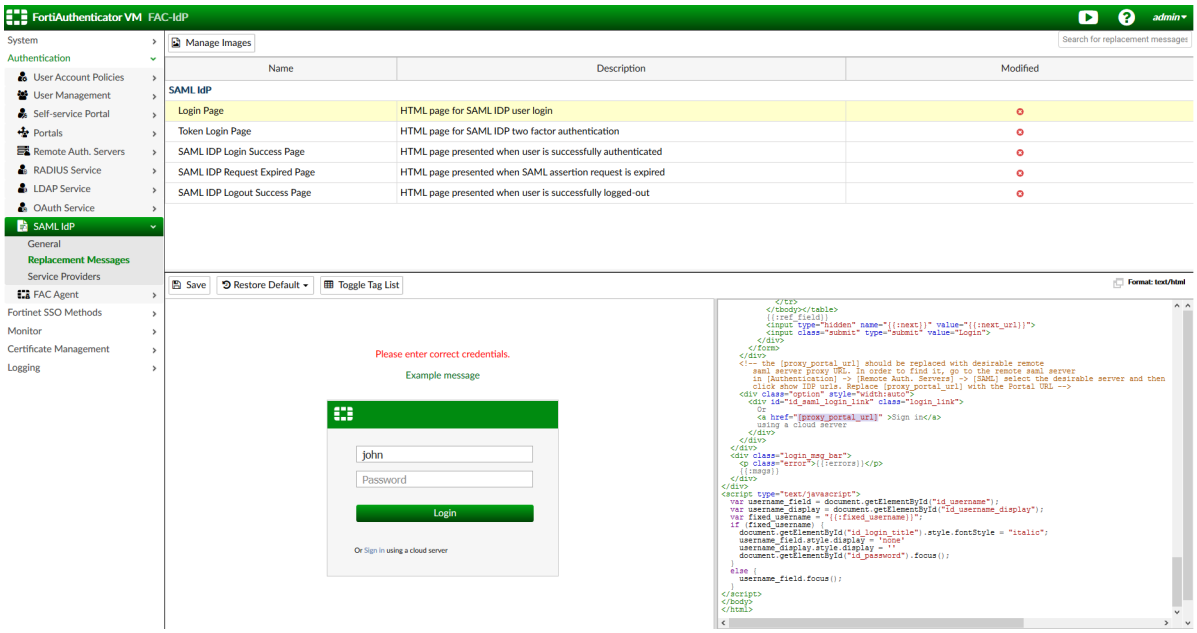
3. Click *Save*.

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.



4. Click *Save*.

Results

To test Azure login through the SP:

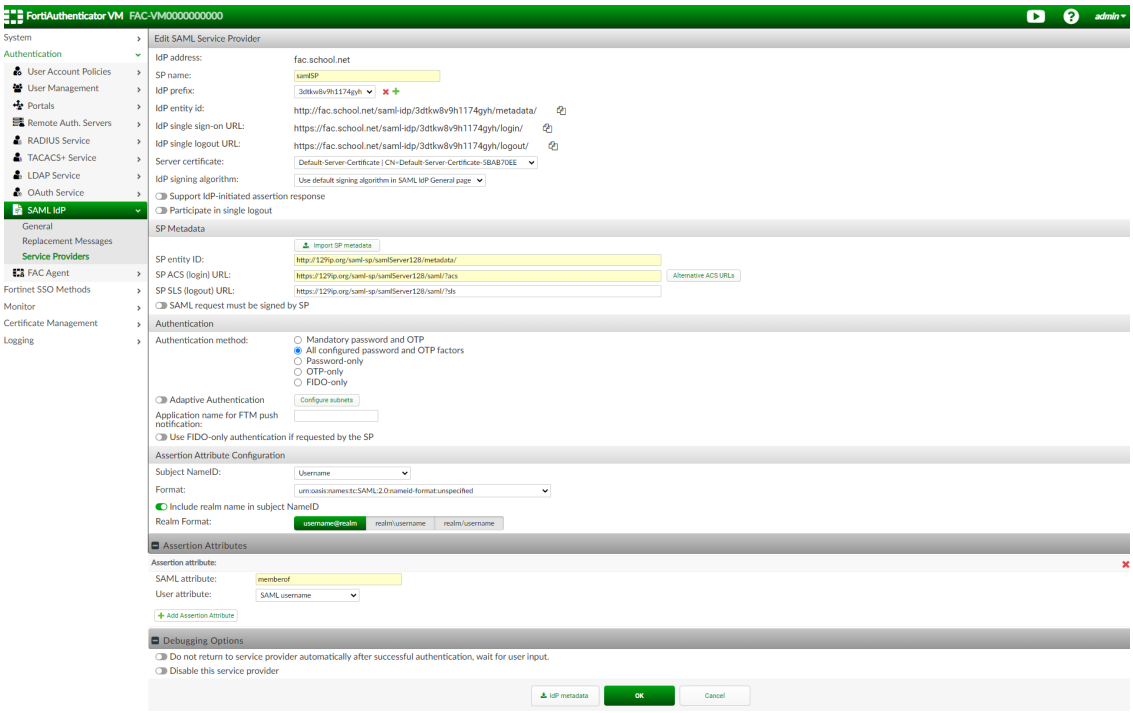
1. Enter in the portal login URL from the service provider in a new browser.
   You are redirect you to the FAC's IdP-server and proxy page.
2. Click on the link below the login options to be redirected to Microsoft's login page.

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 192.
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*.

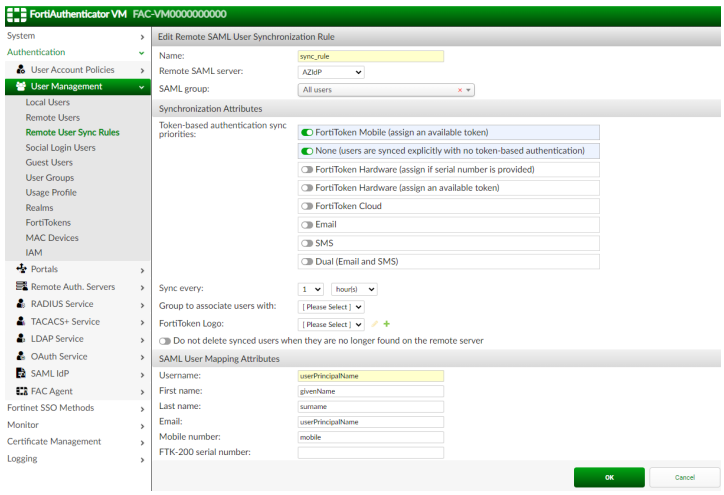


10. Click *OK* to save changes.

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 190.
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)*.



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

SAML IdP proxy for Google Workspace

This example 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 195
2. Configuring the remote SAML server on page 196
3. Creating a remote SAML user synchronization rule on page 197
4. Configuring a Google Workspace Realm on page 197
5. Configuring IdP settings on page 198
6. Configuring SP settings on FortiAuthenticator on page 198
7. Configuring the login page replacement message on page 199
8. Results on page 200

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 196 and Creating a remote SAML user synchronization rule on page 197.

To configure remote OAuth settings:

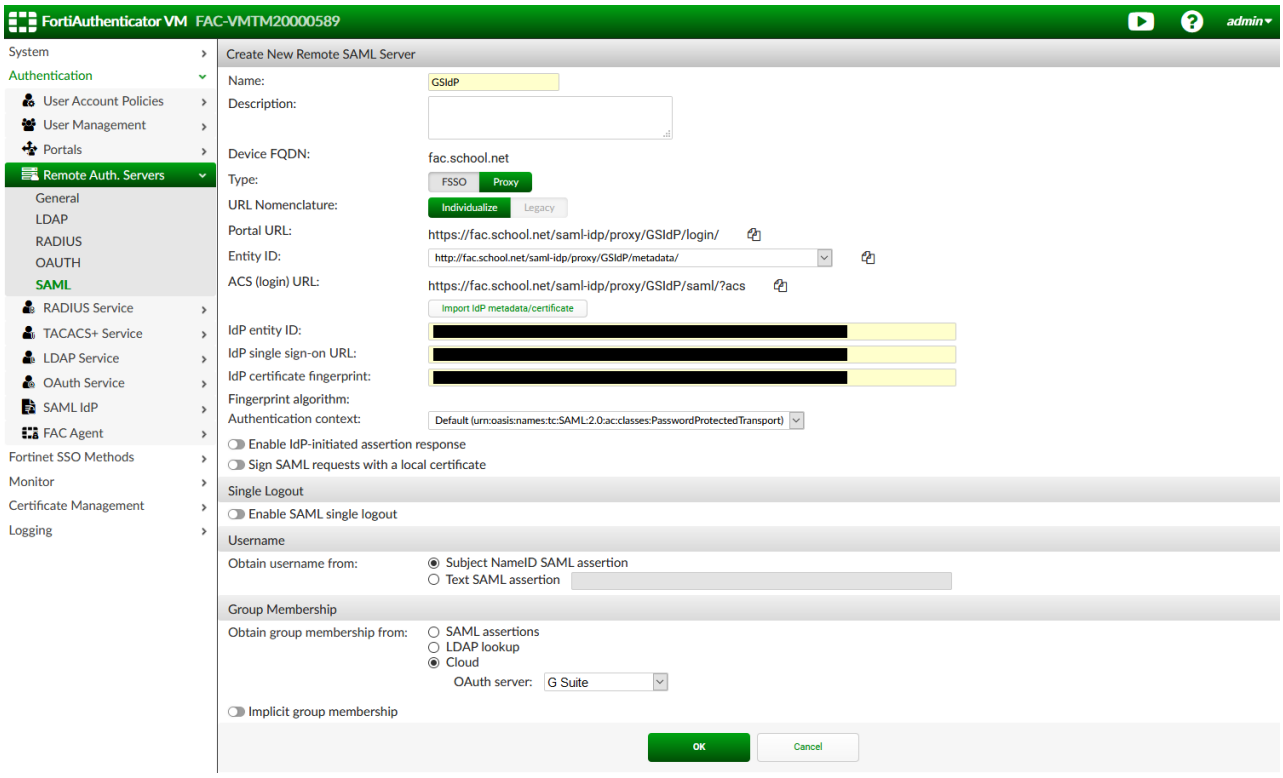
1. On FortiAuthenticator, go to *Remote Auth. Servers* > *OAUTH*, and click *Create New*.
2. Provide a name for the server and select *Google Workspace Directory* as the OAuth source.

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.

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 195.
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.

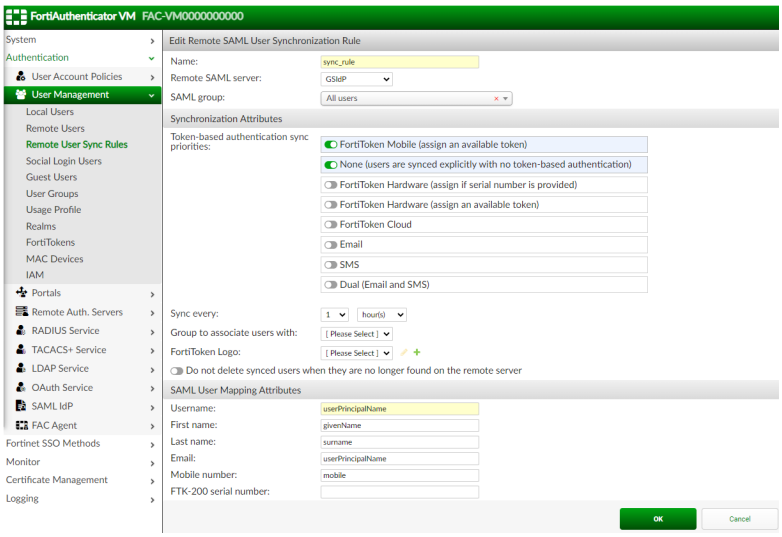


6. Click *OK* to save your changes.

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 196.
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)*.



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

Configuring a Google Workspace Realm

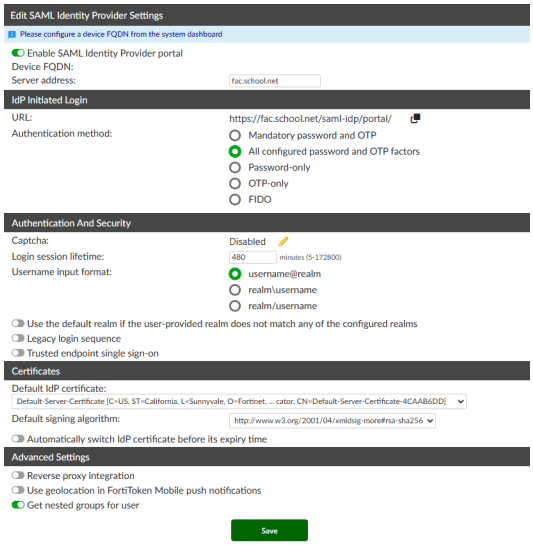
To create a Google Workspace Realm and add it to the IdP:

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. Select *Enable SAML Identity Provider portal*, and enter the following:
   a. **Server address**: Enter the FortiAuthenticator FQDN.
   b. **Default IdP certificate**: Select a default certificate to use.



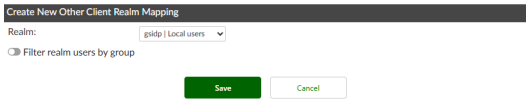
3. Click *Save*.

To add a realm:

Starting FortiAuthenticator 6.6.3, to add a realm for SAML IdP, go to *Authentication > SAML IdP > User Sources*.

---

1. Go to *Authentication > SAML IdP > User Sources*, and select *Create New*.
2. From the *Realm* dropdown, select the realm associated with the remote server for Google Workspace.



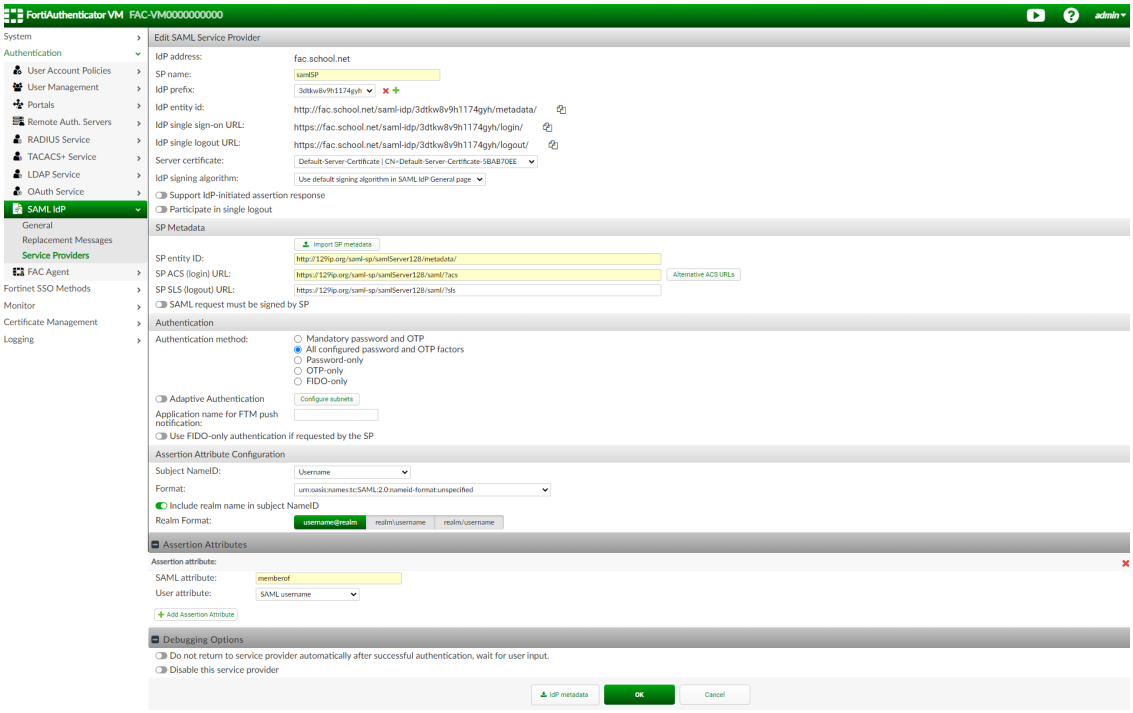
3. Click *Save*.

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 198.
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*.



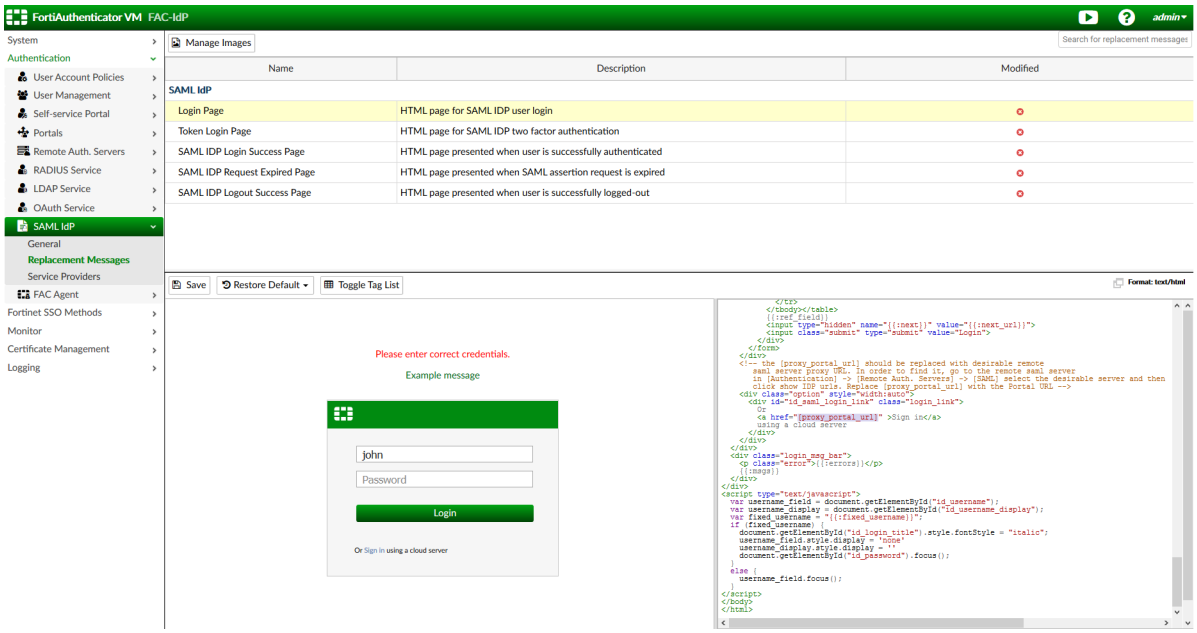
10. Click *OK* to save changes.

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.



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

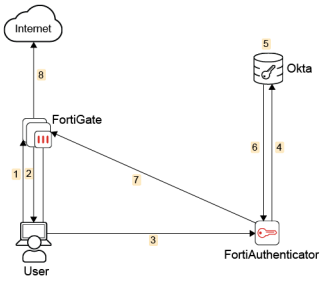
In this example, you will provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator as the service provider (SP) and Okta, a cloud-based user directory, as the identity provider (IdP).

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.

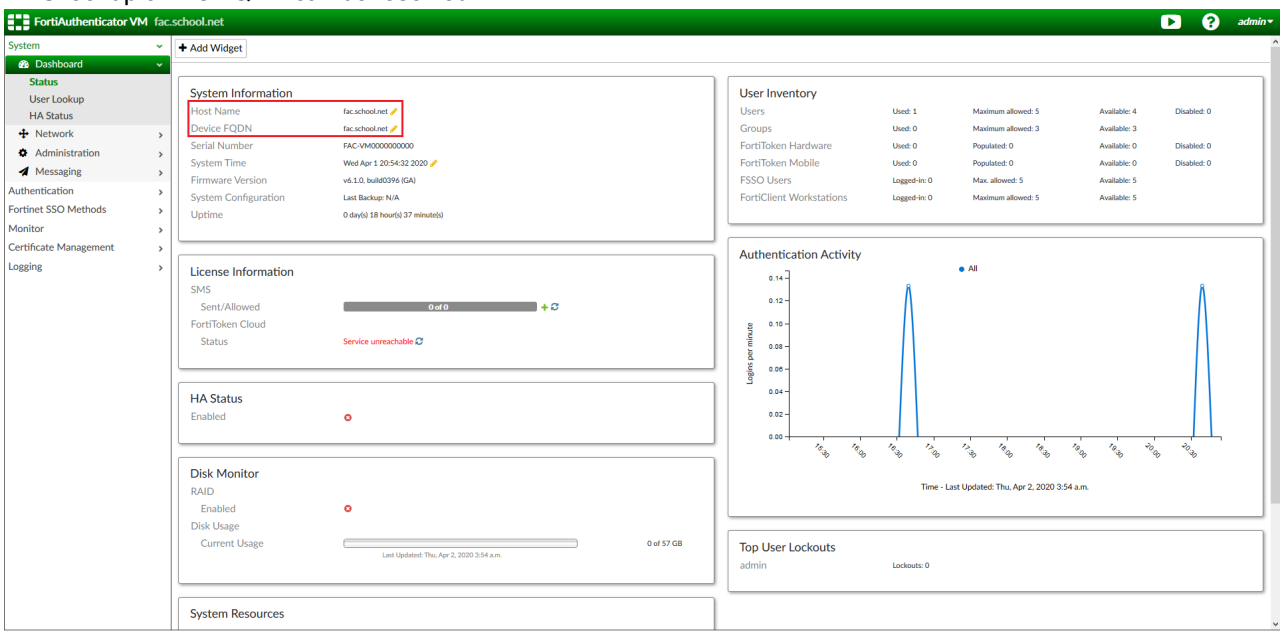


1. The user attempts to access internet using FortiGate.
2. The FortiGate captive portal offloads the request.
3. The user is redirected by the FortiGate to the FortiAuthenticator SAML SP portal URL configured for Okta.
4. The FortiAuthenticator SAML SP portal URL is redirected to the FortiAuthenticator IdP Single Sign-On URL which is the Okta SSO URL.
   This is the SAML request for authentication.
5. The user authenticates with the username and password.
   Okta Verify Push or manual Okta MFA code can be entered if configured.
6. Okta sends the SAML assertion containing the user and group authentication to the FortiAuthenticator SAML SP ACS (login) URL.
7. FortiAuthenticator consumes the assertion and sends user and group information via the SSO connector to the FortiGate.
8. The user browses the internet based on FortiGate identity based policies.

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.

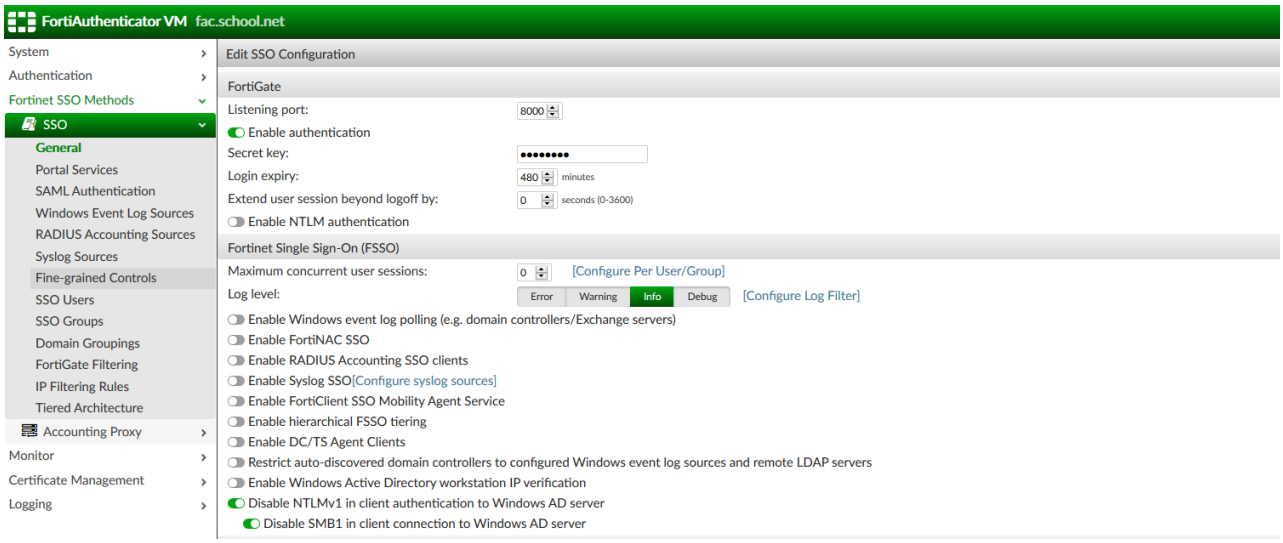


3. On FortiGate, open the CLI Console and enter the following command using the FortiAuthenticator host name and internet-facing IP address.

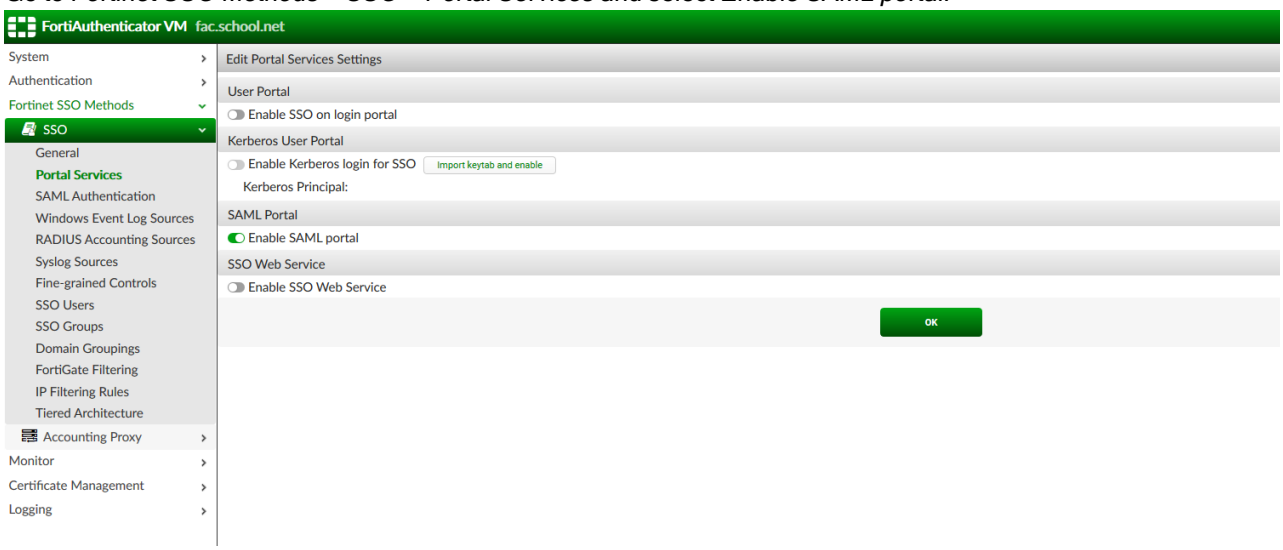
```
config system dns-database
   edit school.net
      config dns-entry
         edit 1
            set hostname fac.school.net
            set ip 192.168.50.100
         next
      end
      set domain school.net
   next
```

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.

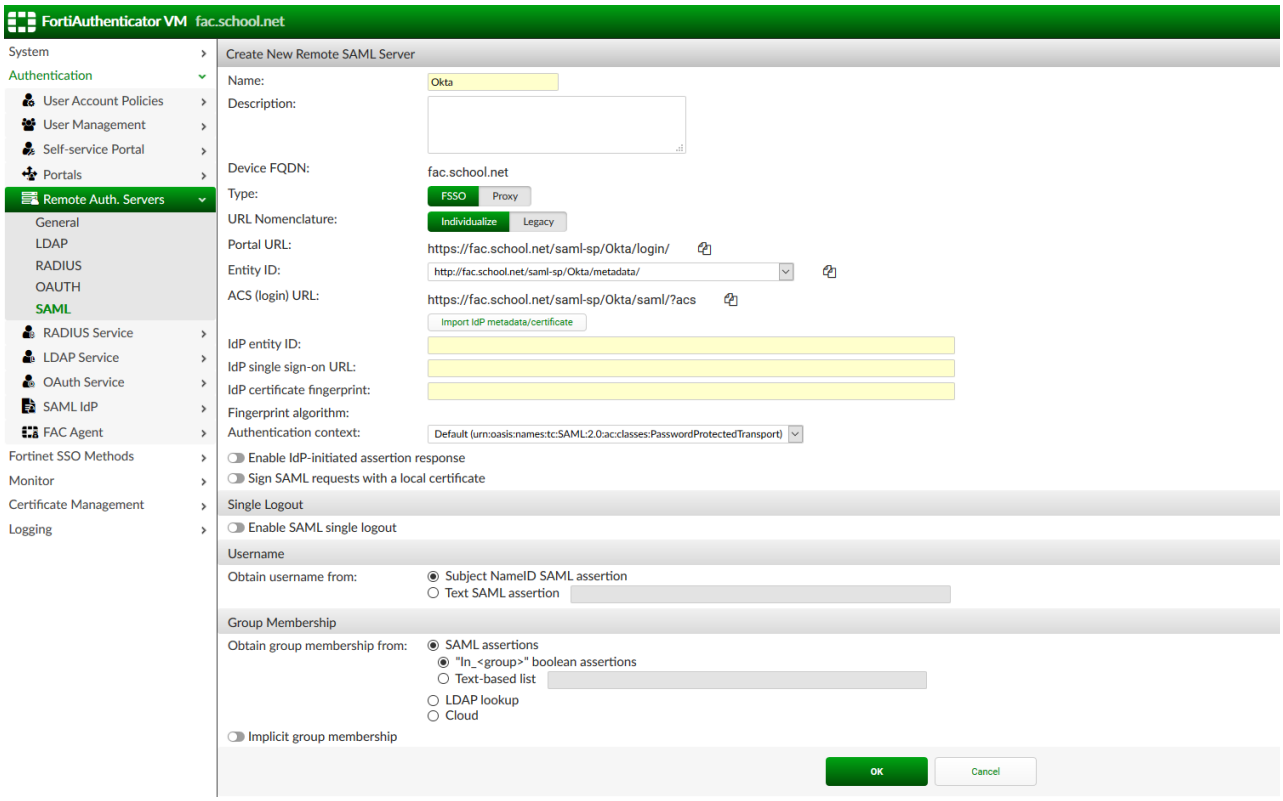


2. Go to *Fortinet SSO Methods > SSO > Portal Services* and select *Enable SAML portal*.



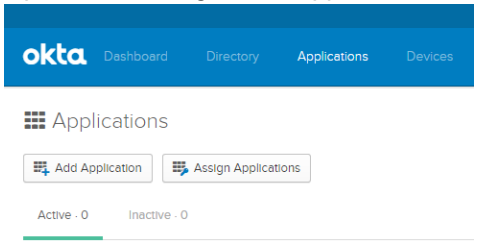
3. Next, go to *Authentication > Remote Auth. Servers > SAML*, and click *Create New*. Enter Okta as the name.

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.

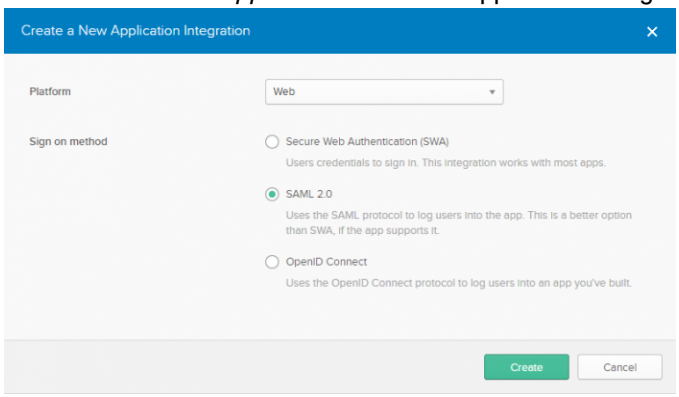

FortiAuthenticator VM fac.school.net
System
Authentication
User Account Policies
User Management
Self-service Portal
Portals
Remote Auth. Servers
General
LDAP
RADIUS
OAUTH
SAML
RADIUS Service
LDAP Service
OAuth Service
SAML IdP
FAC Agent
Fortinet SSO Methods
Monitor
Certificate Management
Logging
Create New Remote SAML Server
Name:
Okta
Description:
Device FQDN:
fac.school.net
Type:
FSSO
Proxy
URL Nomenclature:
Individualize
Legacy
Portal URL:
https://fac.school.net/saml-sp/Okta/login/
Entity ID:
http://fac.school.net/saml-sp/Okta/metadata/
ACS (login) URL:
https://fac.school.net/saml-sp/Okta/saml/?acs
Import IdP metadata/certificate
IdP entity ID:
IdP single sign-on URL:
IdP certificate fingerprint:
Fingerprint algorithm:
Authentication context:
Default (urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport)
Enable IdP-initiated assertion response
Sign SAML requests with a local certificate
Single Logout
Enable SAML single logout
Username
Obtain username from:
Subject NameID SAML assertion
Text SAML assertion
Group Membership
Obtain group membership from:
SAML assertions
"In_<group>" boolean assertions
Text-based list
LDAP lookup
Cloud
Implicit group membership
OK
Cancel

Configuring the Okta developer account IdP application

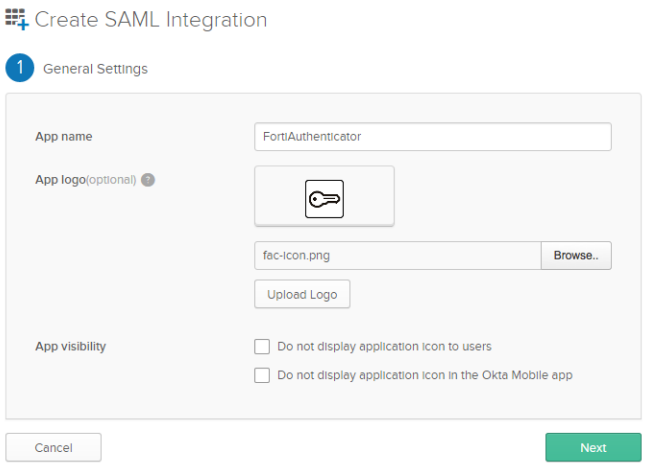
1. Open a browser, go to the *Applications* tab and select *Add Application*.



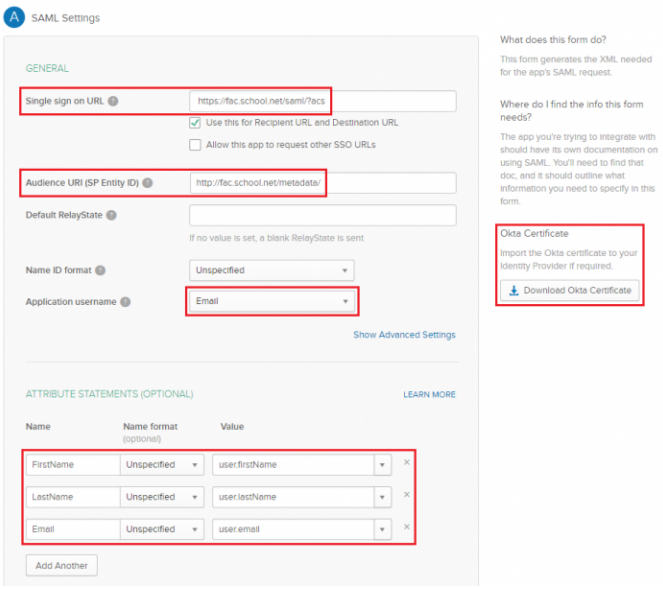
2. Select *Create New App* and create a new application using the SAML 2.0 sign on method.



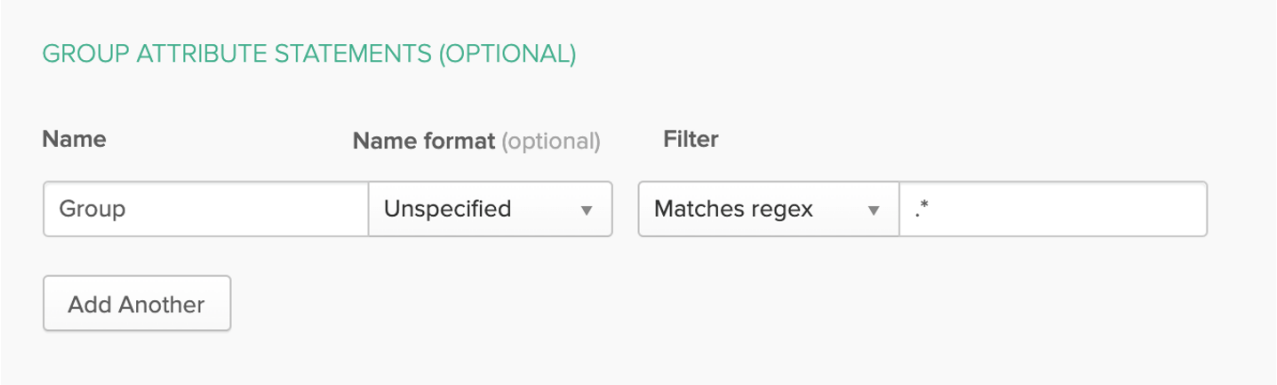
3. Enter a custom app name, and select *Next*. You may upload an app logo if you wish.
The name entered here is the name of the portal that users will log into.



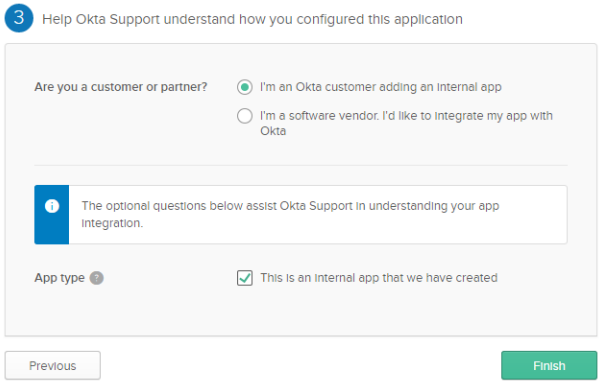
4. Under *A - SAML Settings*, set *Single sign on URL* and *Audience URL (SP Entity ID)* to the *ACS* and *Entity URLs* (respectively) from FortiAuthenticator.
Users will be required to provide their email address as their username, and their first and last names (as seen in the example).
Before continuing, select *Download Okta Certificate*. This will be imported to the FortiAuthenticator later.



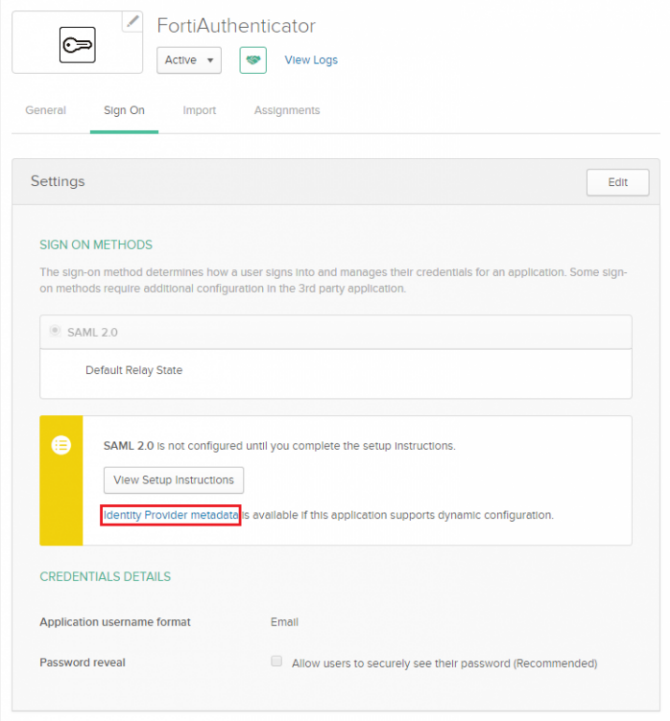
In the section below, configure a *Group* attribute to match on FortiAuthenticator. The word *Group* (case-sensitive) must be entered in *Text-based list* under *Obtain Group Membership from: SAML assertions* inside the remote SAML setup configuration on FortiAuthenticator. Regex matching is the most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



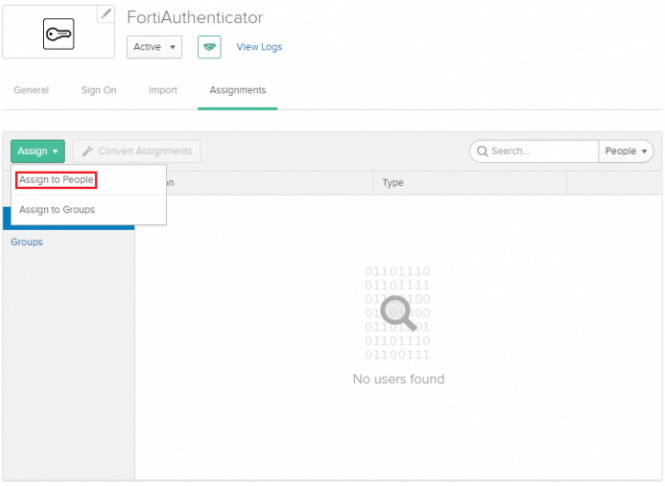
5. In the last step, confirm that you are an Okta customer, and set the *App type* to an internal app. Select *Finish*.



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

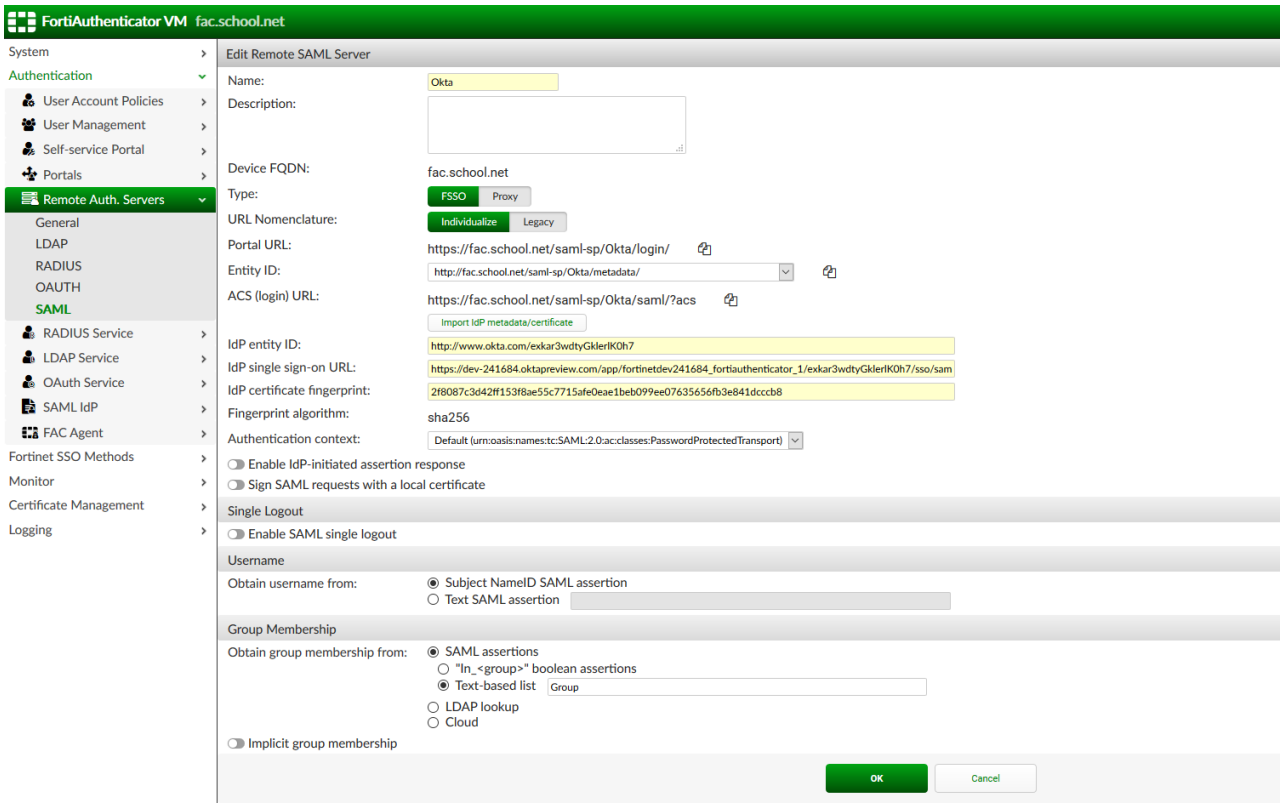


7. Finally, open the *Assignments tab* and select *Assign > Assign to people*.
Assign the users you wish to add to the application. This will permit the user to log in to the application's portal.
Save your changes, and select *Done*.

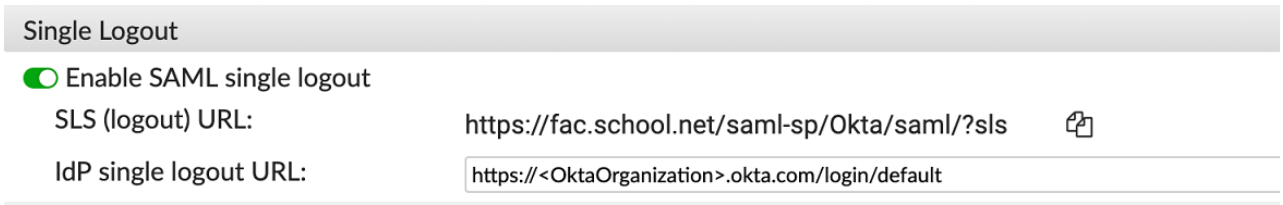


Importing the IdP certificate and metadata on FortiAuthenticator

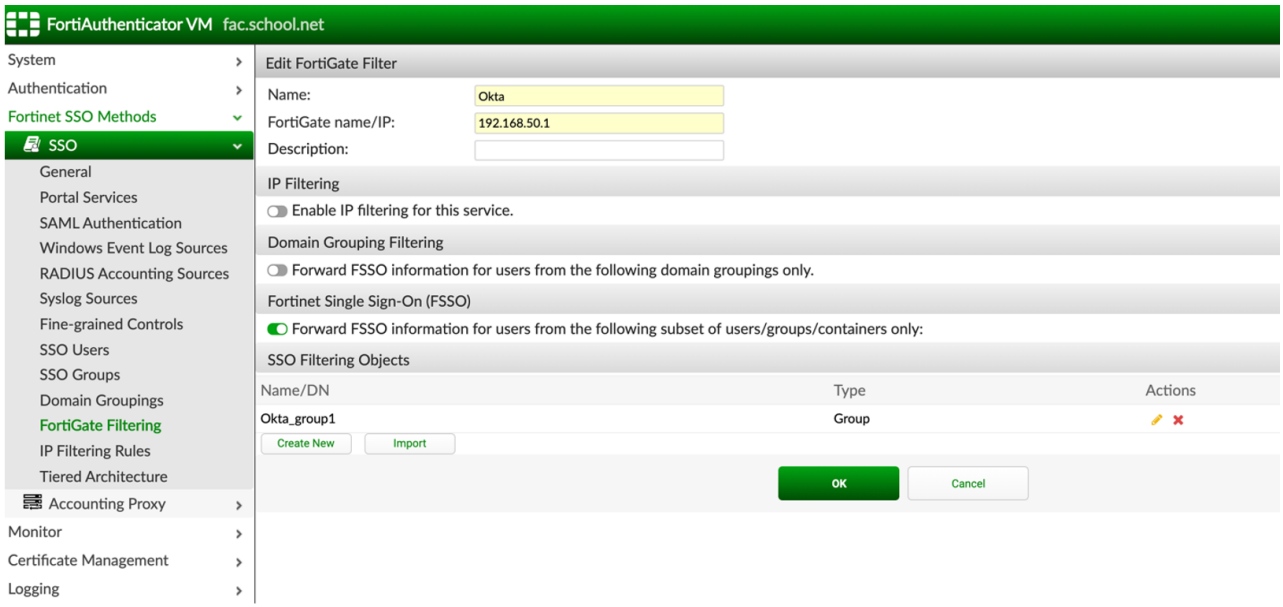
1. On FortiAuthenticator, go to *Authentication > Remote Auth. Servers > SAML*, and import the IdP metadata and certificate downloaded from Okta.
This will automatically fill in the IdP fields. Select *OK* to save your changes.



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`.



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.

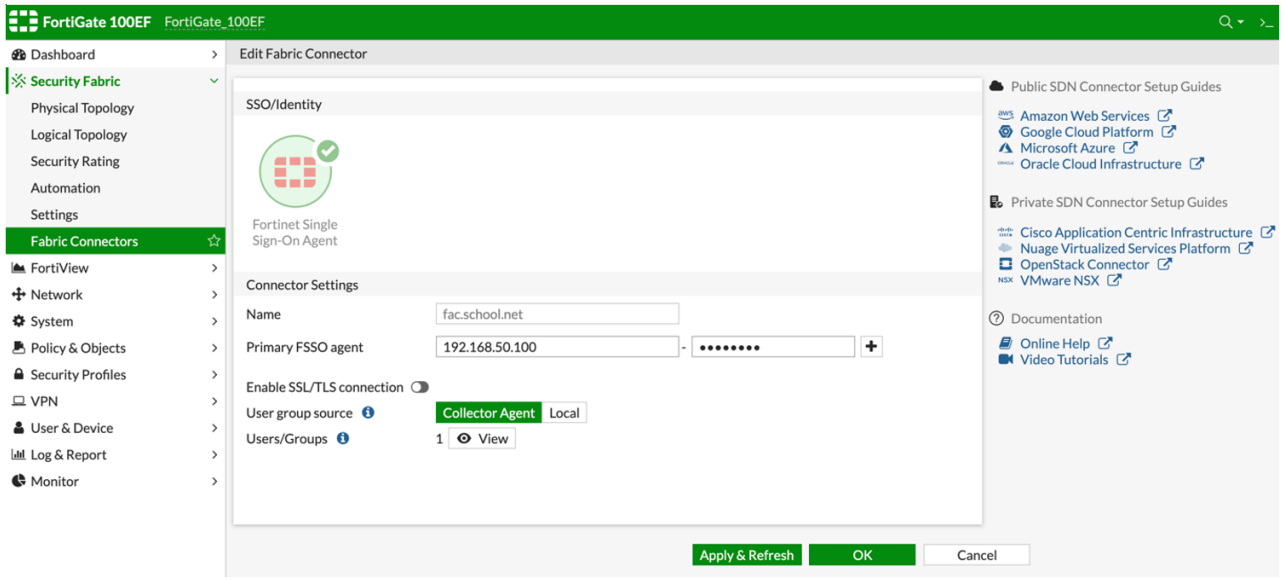


The names entered for the filter must be the same as the group names created in Okta. Failing to enter the exact same names will result in the SSO information not being pushed to FortiGate.

Configuring FSSO on FortiGate

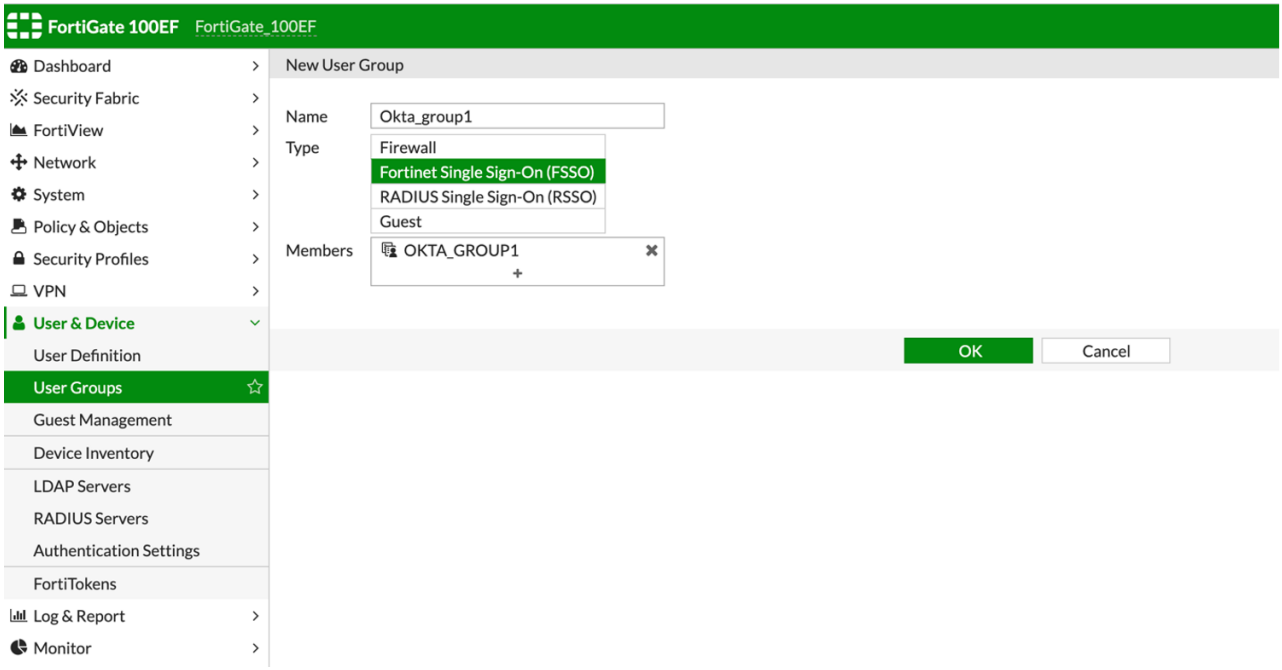
To configure FSSO on FortiGate:

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*.



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.*



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*.

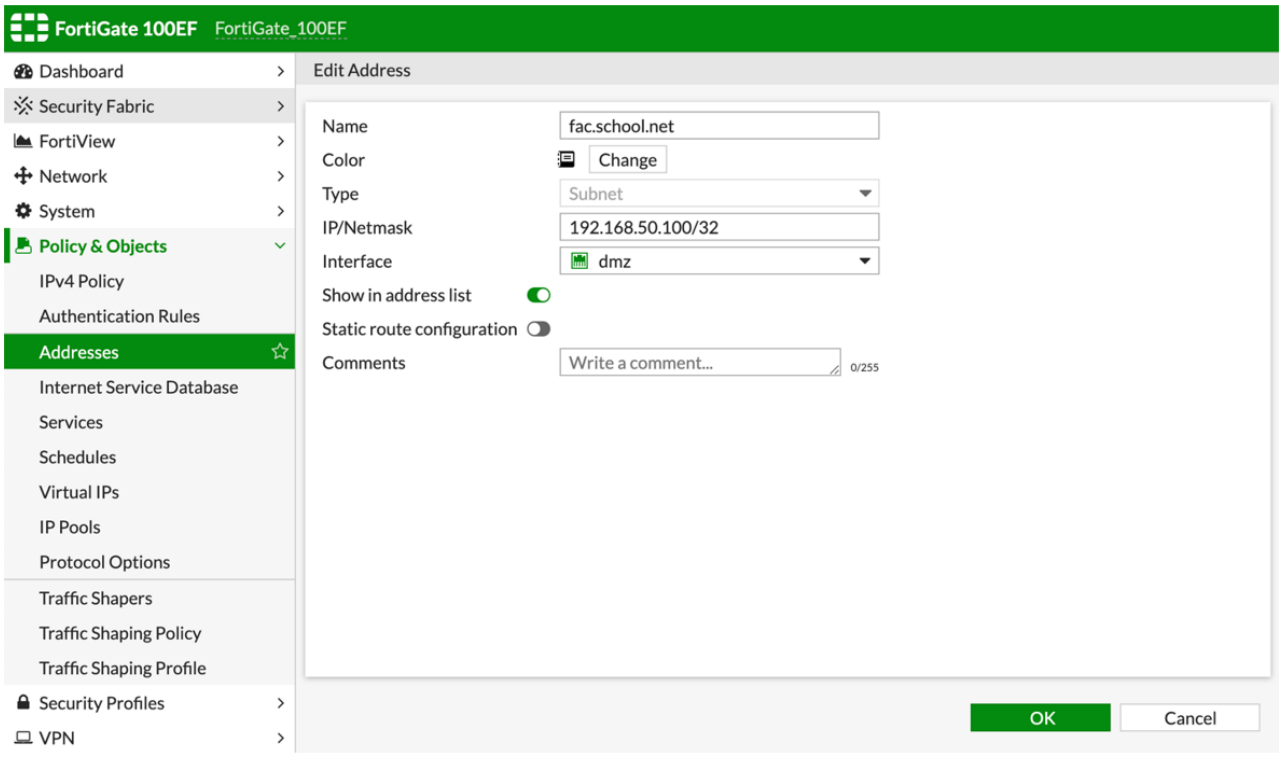
Replace **<FortiAuthenticator-FQDN>** with the DNS name of the FortiAuthenticator.

```
<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

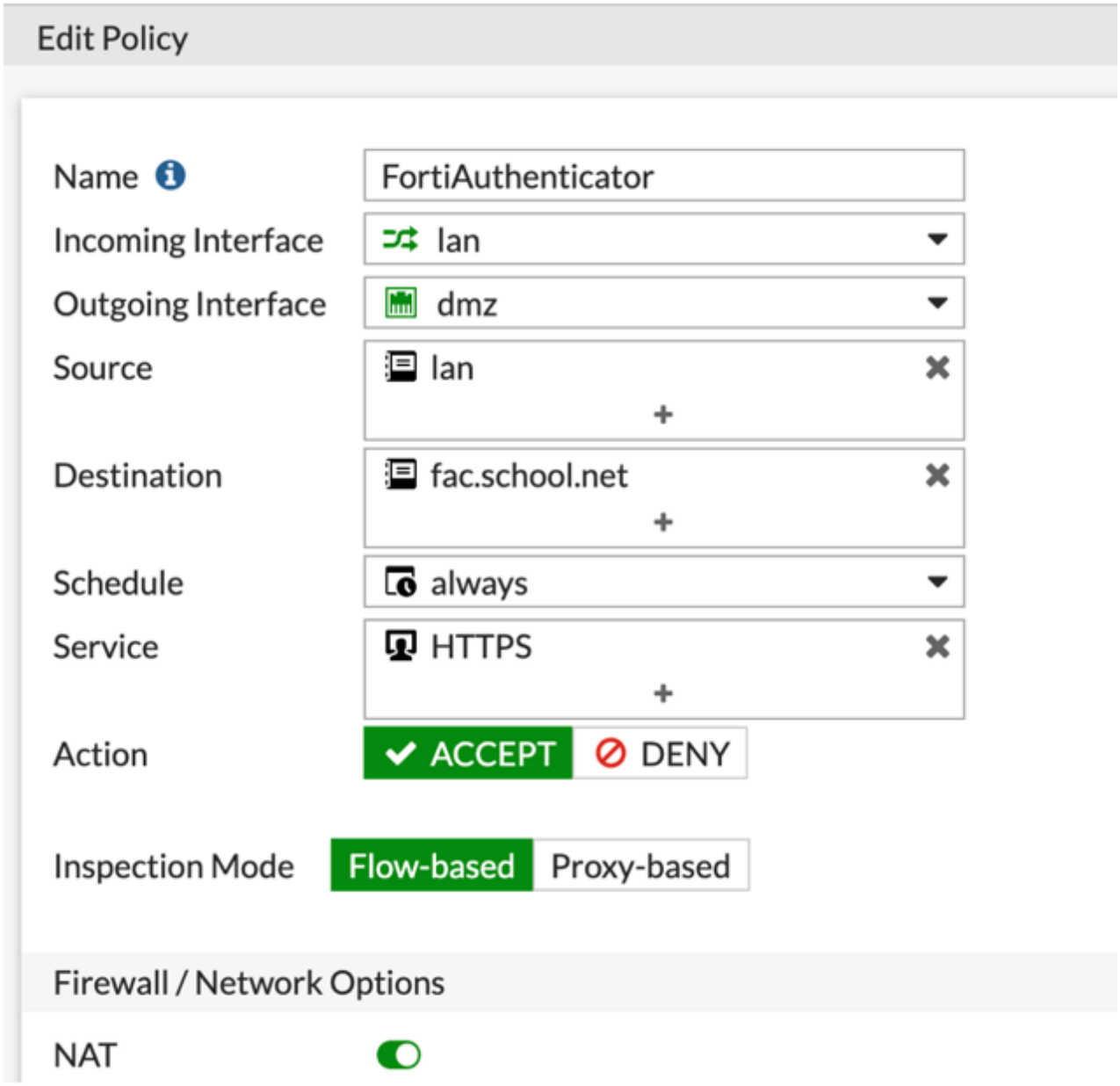
To configure addresses objects and policies on FortiGate:

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

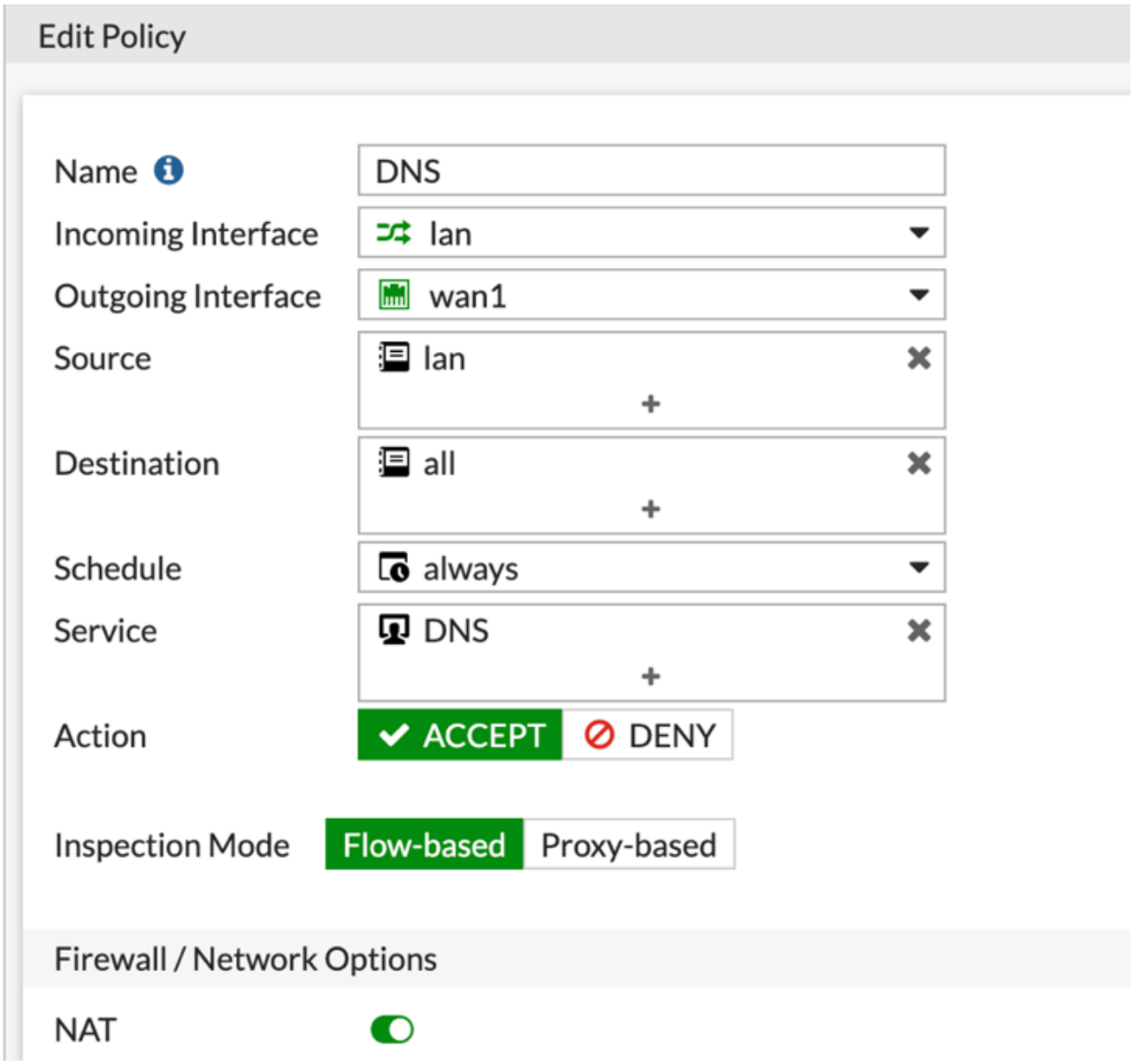


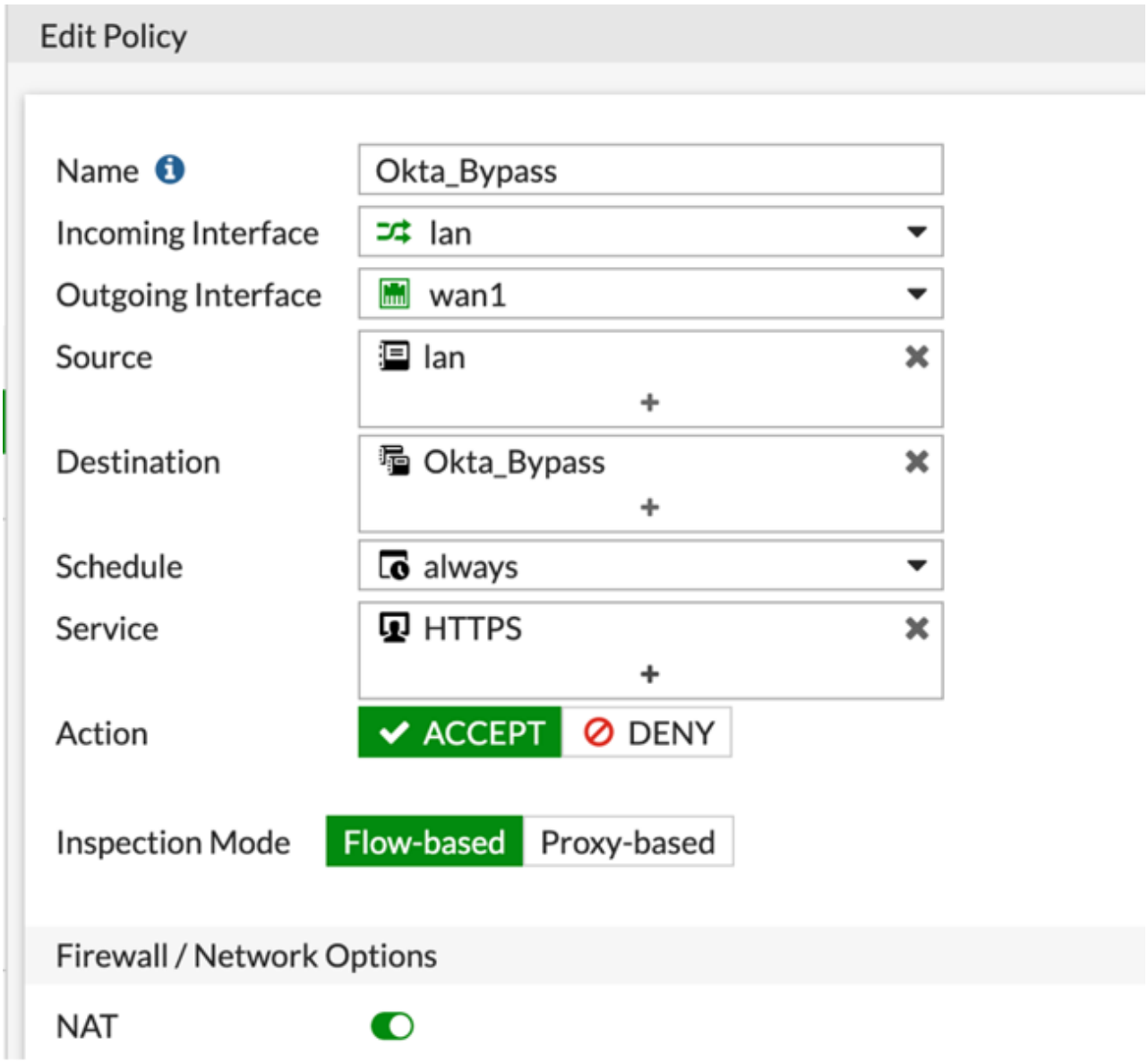
2. Create the FQDN objects below.
   - *.okta.com
   - *.mtls.okta.com
   - *.oktapreview.com
   - *.mtls.oktapreview.com
   - *.oktacdn.com
   - *.okta-emea.com
   - *.mtls.okta-emea.com
   - *.kerberos.okta.com
   - *.kerberos.okta-emea.com
   - *.kerberos.oktapreview.com

   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:

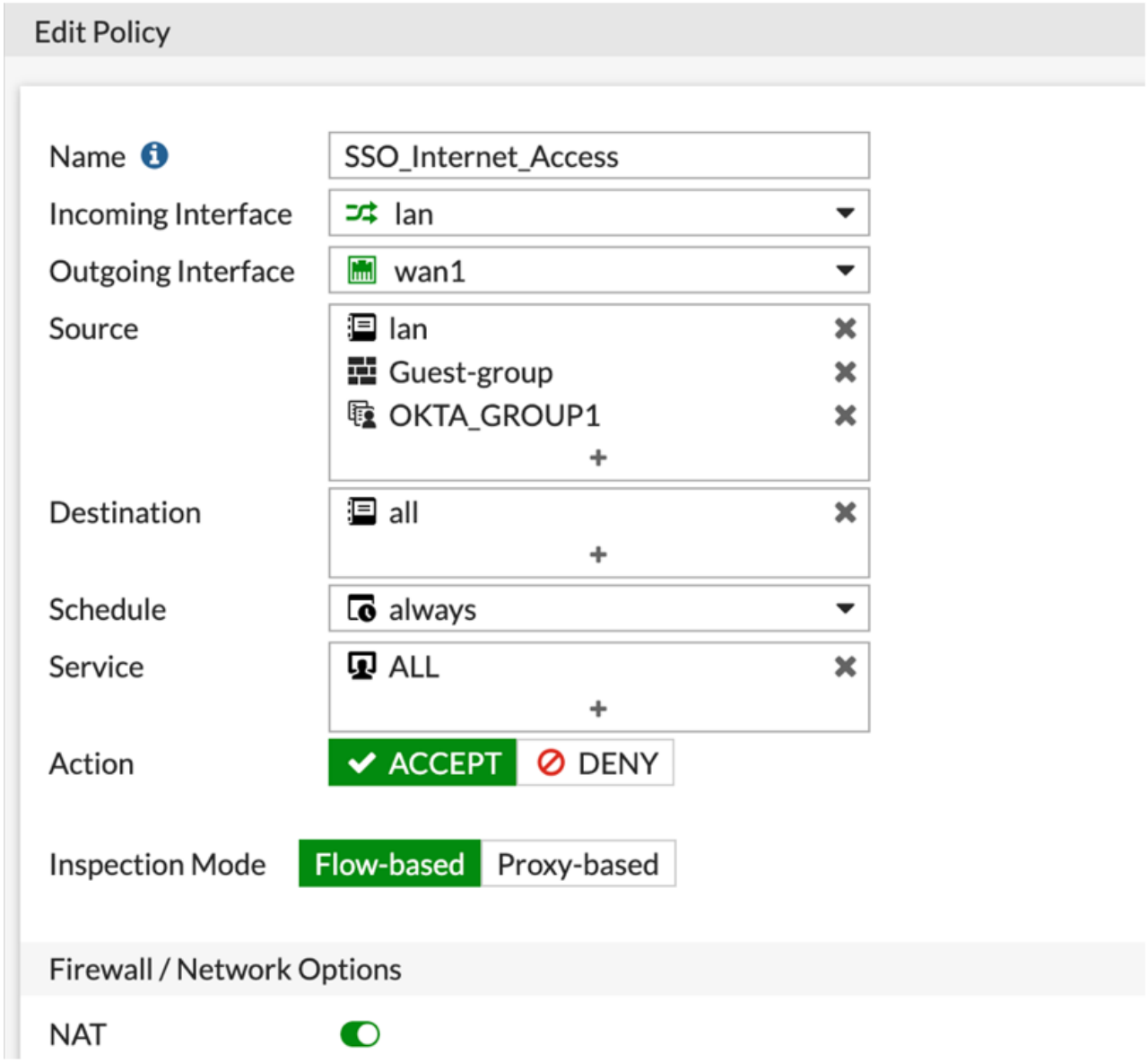


Add the following three policies in order:


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



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.

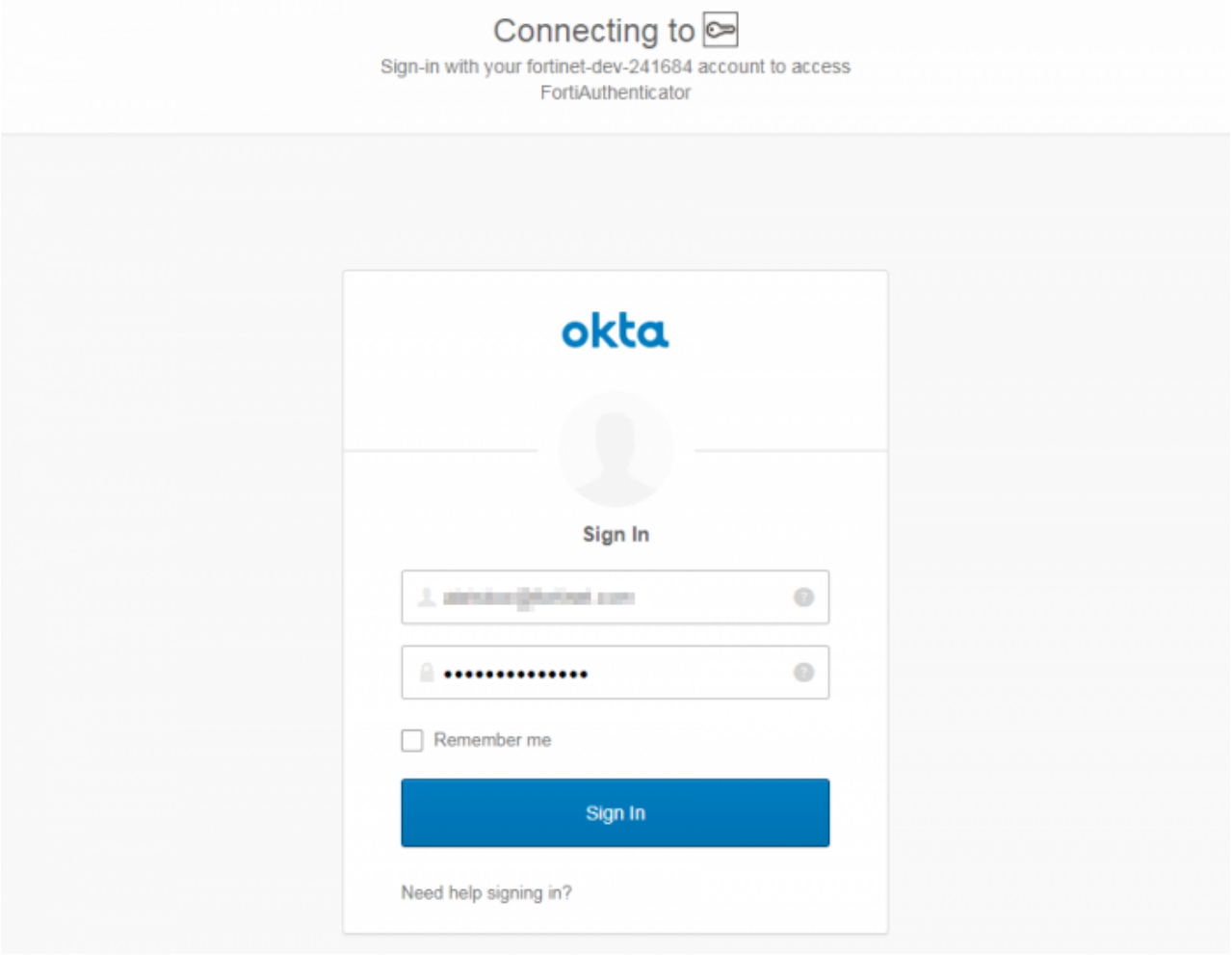


Results

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

Alternatively, you can directly navigate to the portal URL.

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

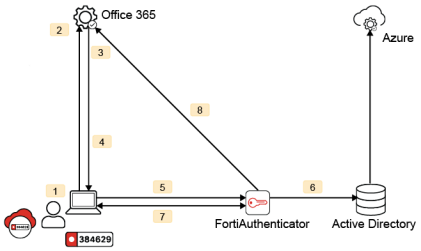


   The assertion is pushed to FortiAuthenticator where the user is authenticated.
2. On FortiAuthenticator, go to *Monitor > SSO > SSO Sessions* to view the user and assigned user group.
3. On FortiGate, go to *Monitor > Firewall User Monitor* to view user information, and confirm that the user has been authenticated via FSSO.

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. For more information on how to do this, please see the FortiAuthenticator Administration Guide.



1. The user browses to O365 login page.
2. The user enter the UPN to begin login.
   O365 determines the domain is federated.
3. O365 redirects the browser to the `PassvieLogonUri` configured for the domain.
4. The `PassvieLogonUri` is the IdP single sign-on URL configured for the O365 SP on the FortiAuthenticator.
5. The user enters the UPN and password in the FortiAuthenticator IdP logon.
6. FortiAuthenticator validates the username and password.
7. The user is prompted for 2FA.
   The 2FA push approval is sent by the user.
8. Authentication is completed by FortiAuthenticator and the browser is redirected to the O365 home page.

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

1. Configure the remote LDAP server on FortiAuthenticator on page 218
2. Configure SAML settings on FortiAuthenticator on page 219
3. Configure two-factor authentication on FortiAuthenticator on page 220
4. Configuring FortiAuthenticator SAML with Microsoft Entra ID (formerly Azure AD) on page 221
5. Configure Microsoft Entra ID Connect on page 222
6. Results on page 229

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.

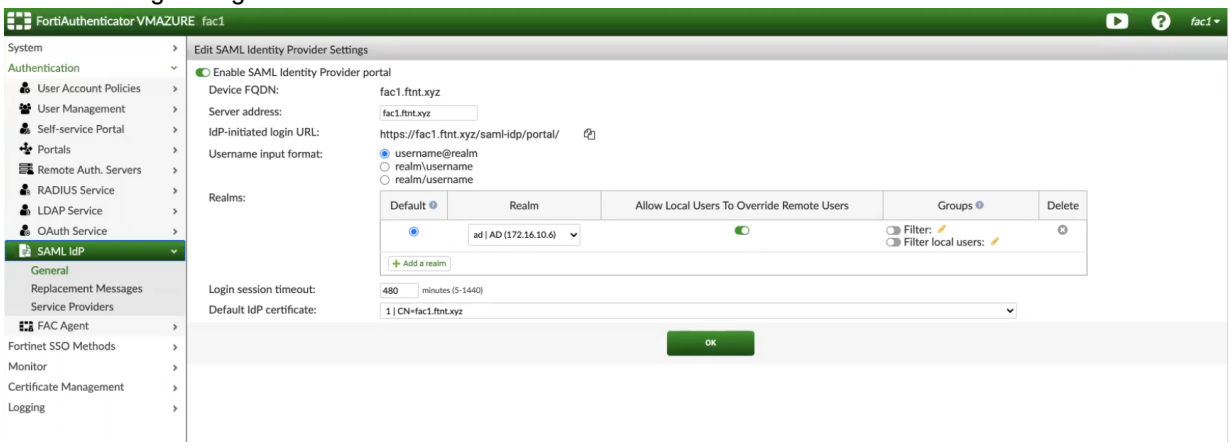
To configure the Active Directory realm:

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.

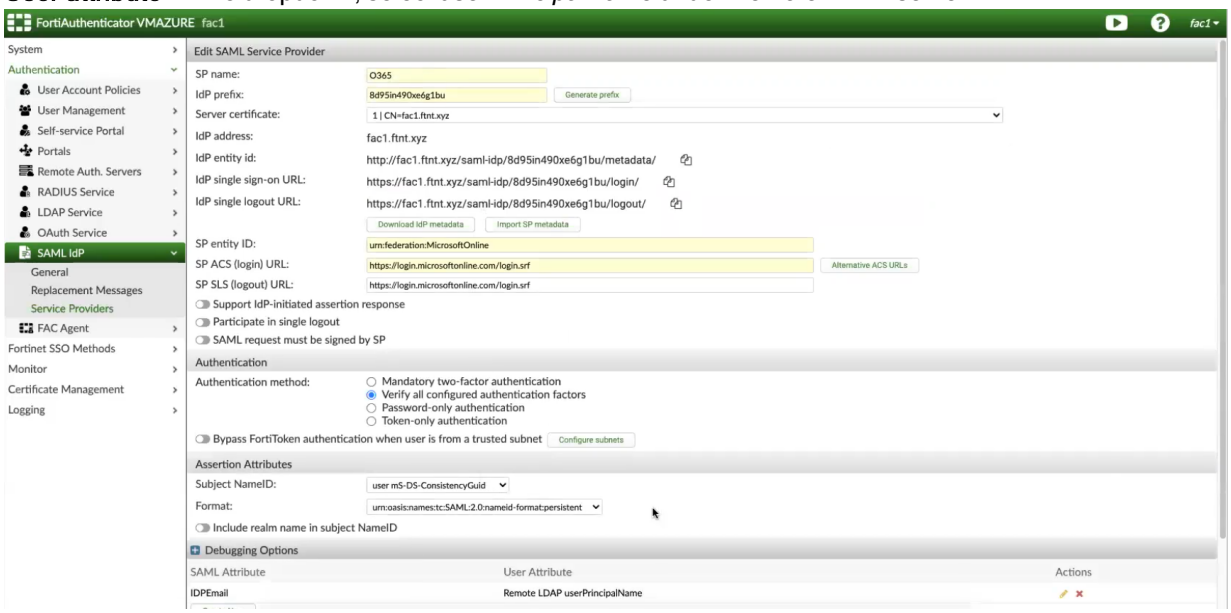


3. Click *OK* to save your changes.

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*.

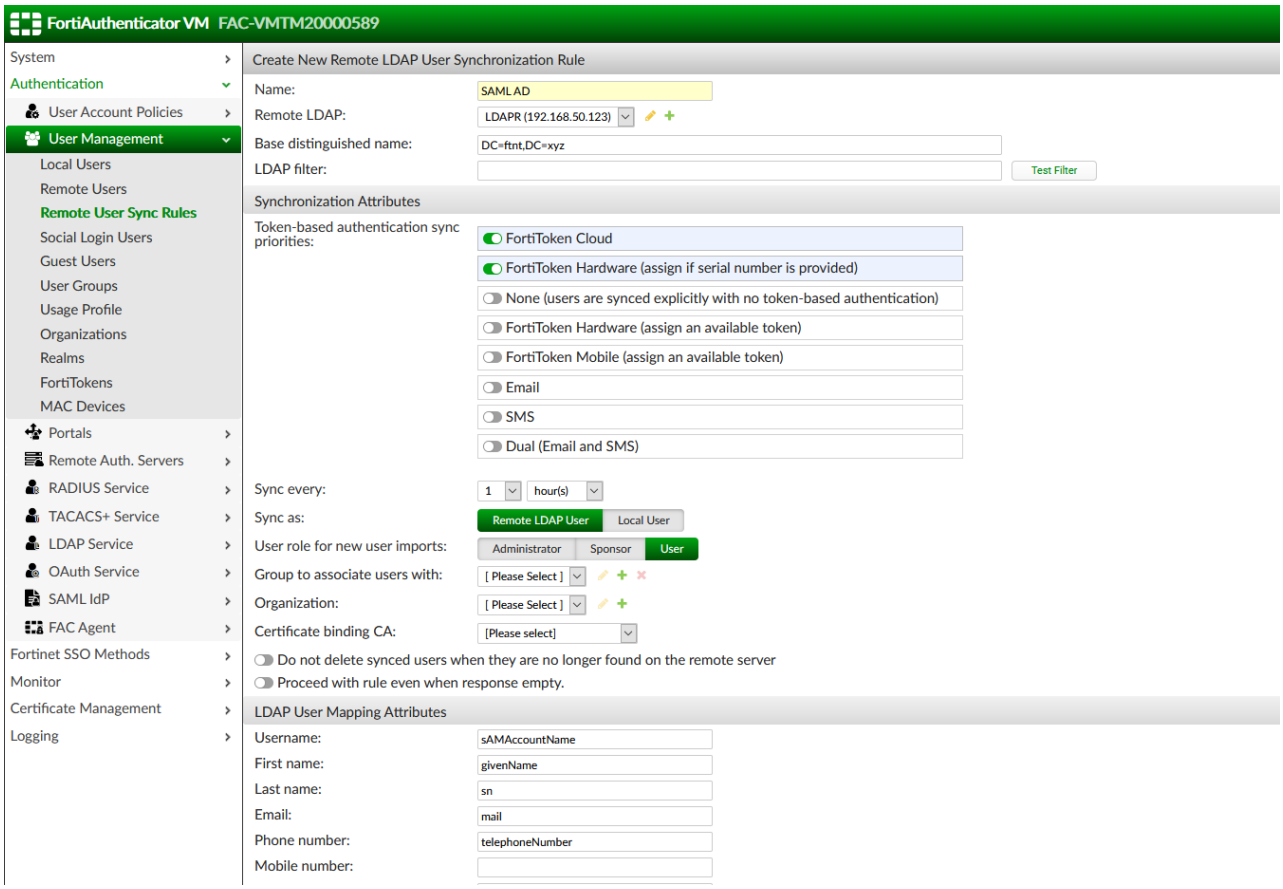


5. Click *OK* to save your changes.

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)*.



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.

Configuring FortiAuthenticator SAML with Microsoft Entra ID (formerly Azure AD)

This shows how to configure a domain and integrate FortiAuthenticator as an SP in Microsoft Entra ID using Microsoft Graph PowerShell.

To configure FortiAuthenticator SAML with Microsoft Entra ID:

Step 0: Install the required module

```
Install-Module Microsoft.Graph -Scope CurrentUser
```

Step 1: Connect to Microsoft Graph

```
   Connect-MgGraph -Scopes "Domain.ReadWrite.All", "Directory.AccessAsUser.All", "User.Read.All",
"Application.ReadWrite.All"
```

Step 2: Define domain and federation settings

```
  $domain = "contoso.com"
  $PassiveLogOnUri= "https://auth.fortitrustid.forticloud.com/saml-idp/h9p8jetp8eez364e/login/"
  $LogOffUri= "https://auth.fortitrustid.forticloud.com/saml-idp/h9p8jetp8eez364e/logout/"
  $IssuerUri= "https://auth.fortitrustid.forticloud.com/saml-idp/h9p8jetp8eez364e/metadata/"
  $MetadataExchangeUri = "https://auth.fortitrustid.forticloud.com/saml-
idp/h9p8jetp8eez364e/metadata/"
  $ActiveSignInUri= "https://auth.fortitrustid.forticloud.com/saml-idp/h9p8jetp8eez364e/login/"
  $SigningCert= Get-Content "C:\path\auth.fortitrustid.forticloud.cer" -Raw
  $DisplayName = "contoso.com"
  $FederatedIdpMfaBehavior = "acceptIfMfaDoneByFederatedIdp"
```

Step 3: Create and verify the domain

```
  New-MgDomain -Name $domain
 Get-MgDomainVerificationDnsRecord -DomainId $domain
```

Update your DNS records to complete domain verification.

Step 4: Configure federation

```
  New-MgDomainFederationConfiguration -DomainId $domain -PassiveSignInUri $PassiveLogOnUri -
SignOutUri $LogOffUri -IssuerUri $IssuerUri -MetadataExchangeUri $MetadataExchangeUri -
SigningCertificate $SigningCert -DisplayName $DisplayName -FederatedIdpMfaBehavior
$FederatedIdpMfaBehavior -PreferredAuthenticationProtocol "saml" -ActiveSignInUri $ActiveSignInUri
```

Step 5: Revert to Entra ID as the IdP (if needed)

```
  Update-MgDomain -DomainId $domain -AuthenticationType "Managed"
```

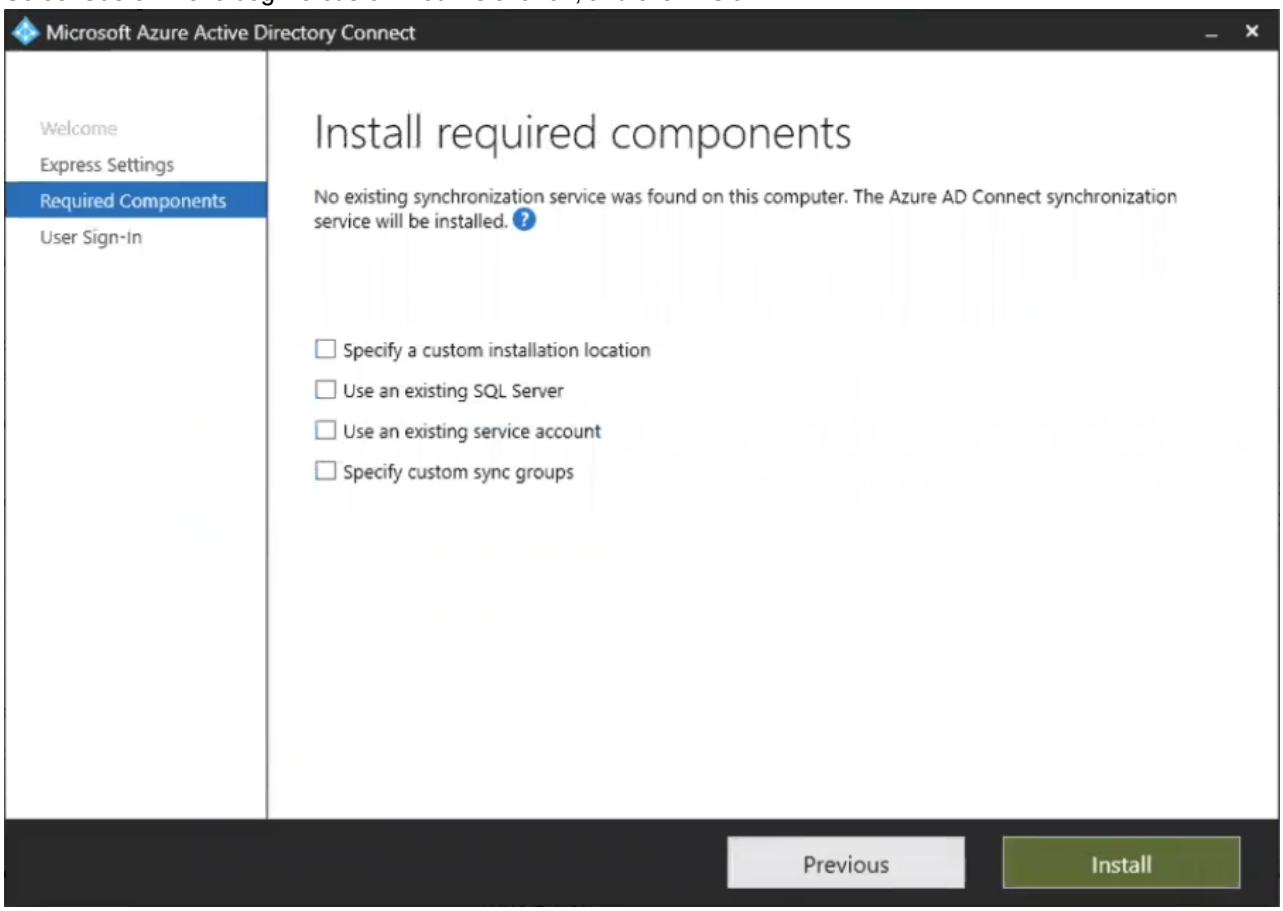
Configure Microsoft Entra ID Connect

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

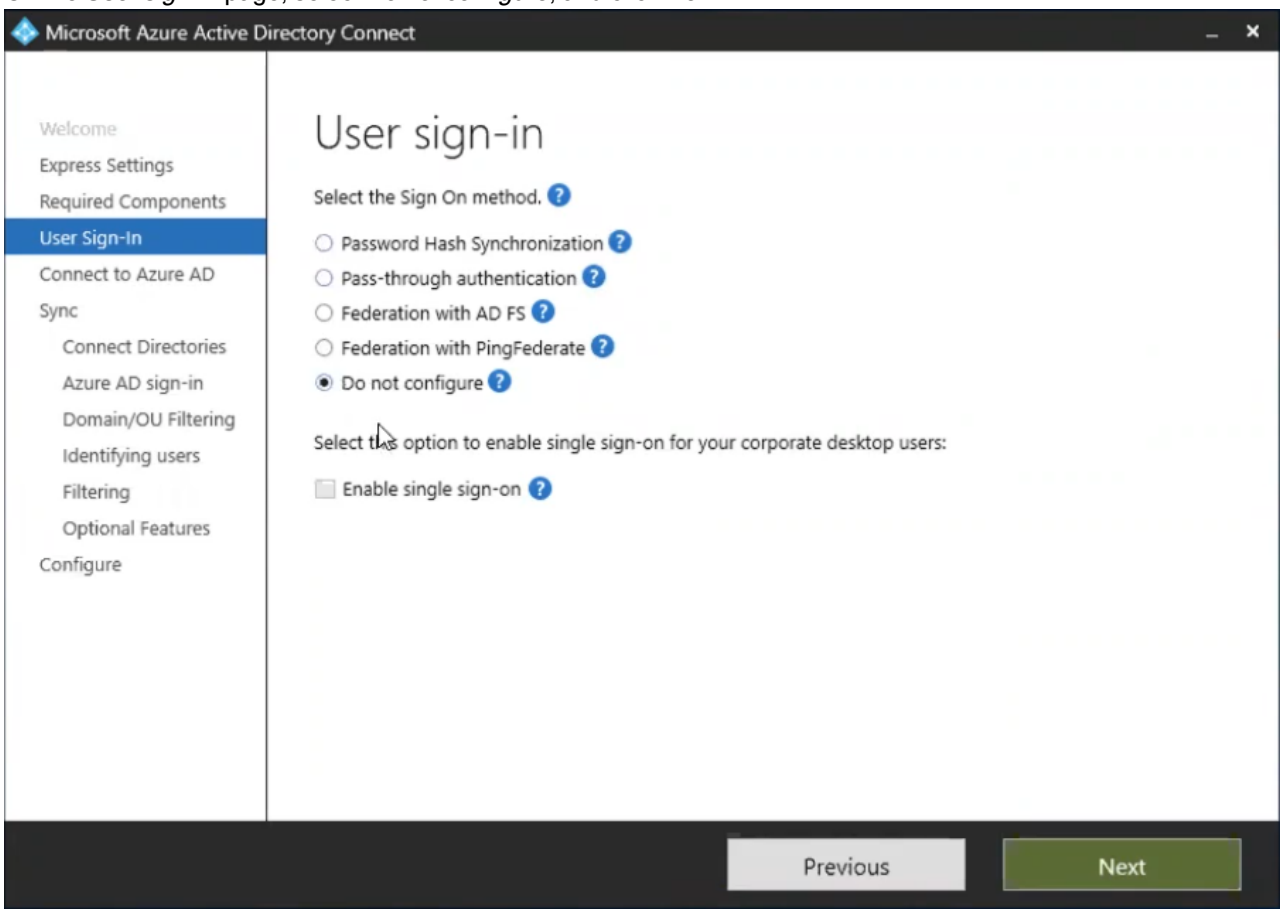
To configure Microsoft Entra ID Connect:

1. Launch Microsoft Entra ID Connect to create a synchronization service to sync attributes from Active Directory to Office365.

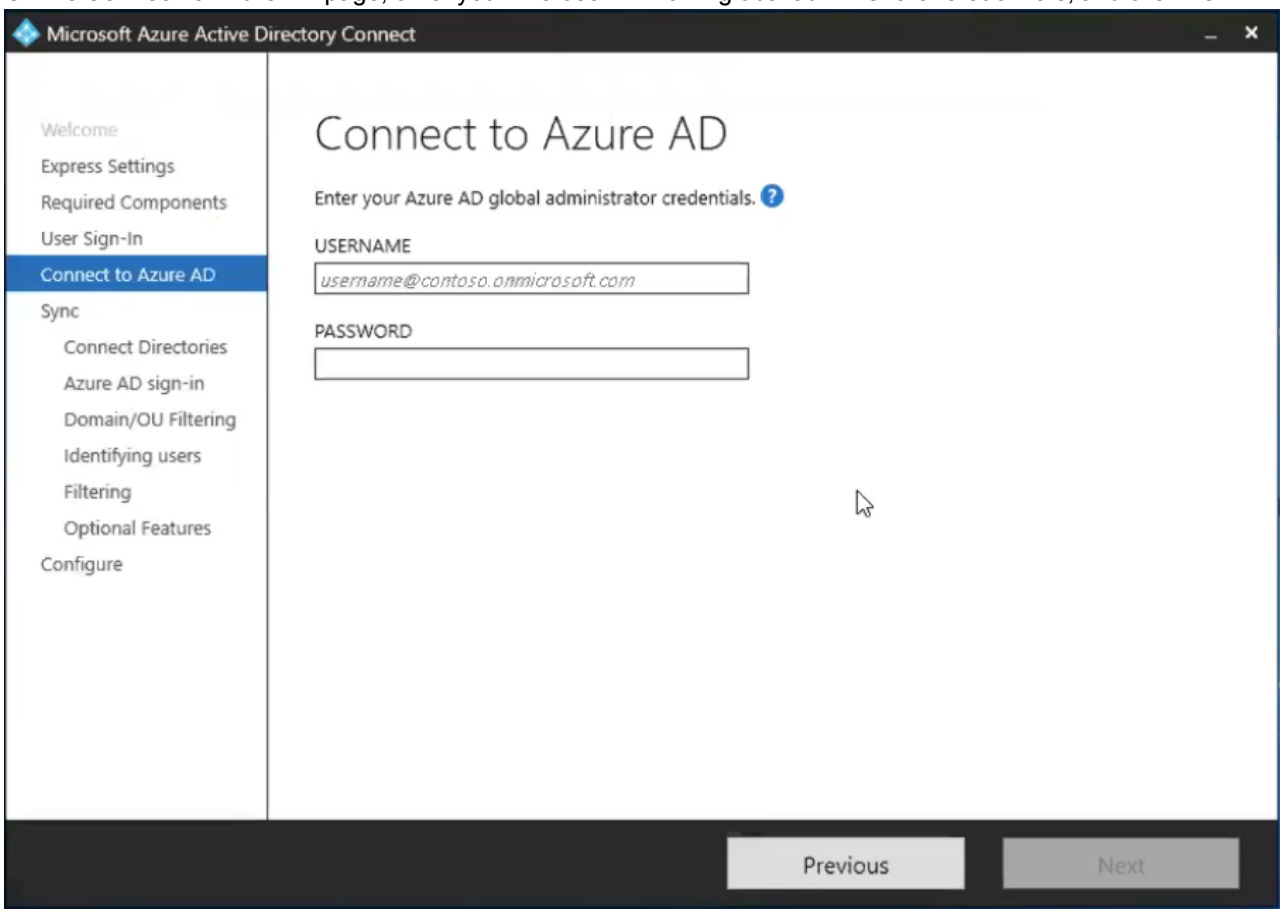
2. Select *Customize* to begin a customized installation, and click *Install*.



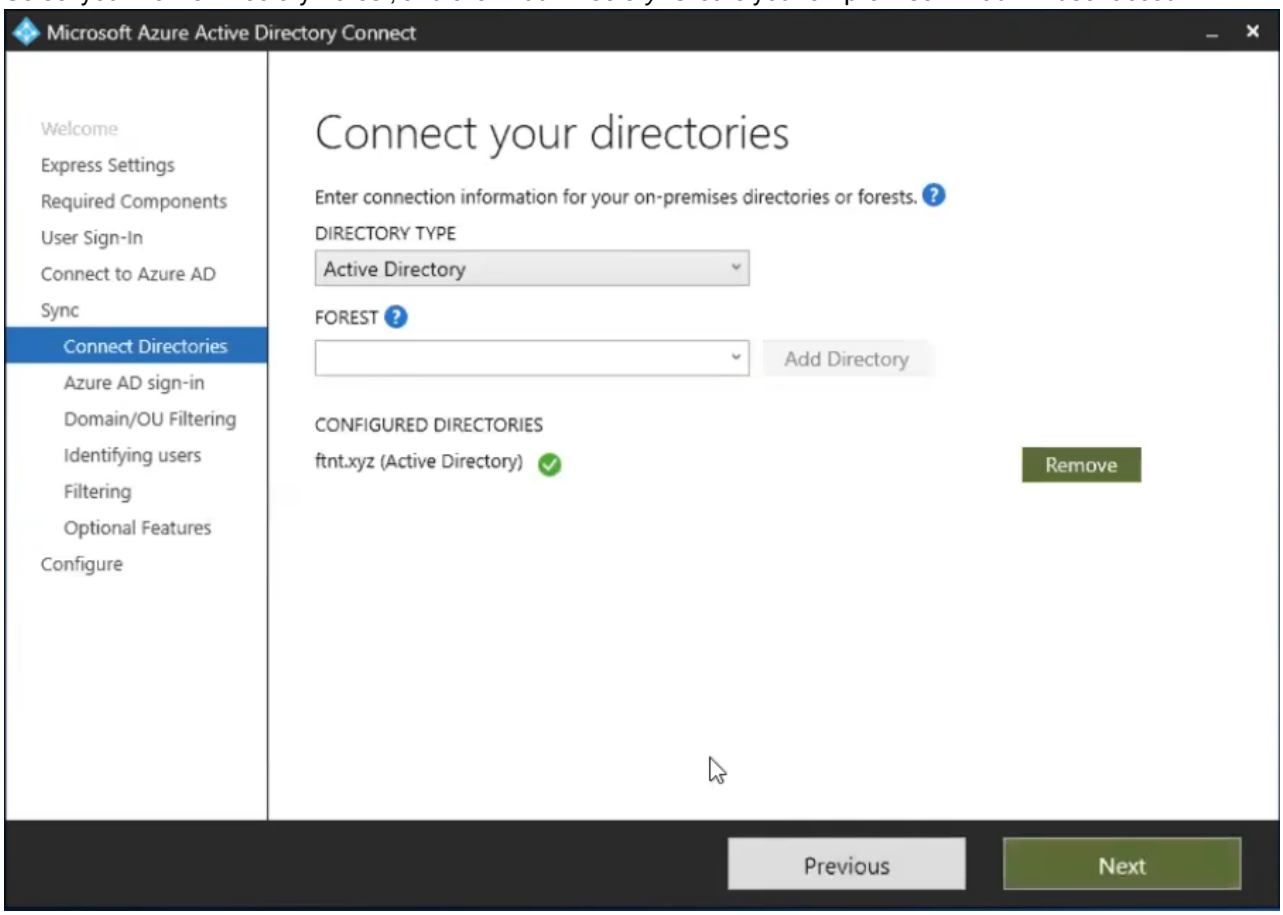
3. On the *User sign-in* page, select *Do not configure*, and click *Next*.



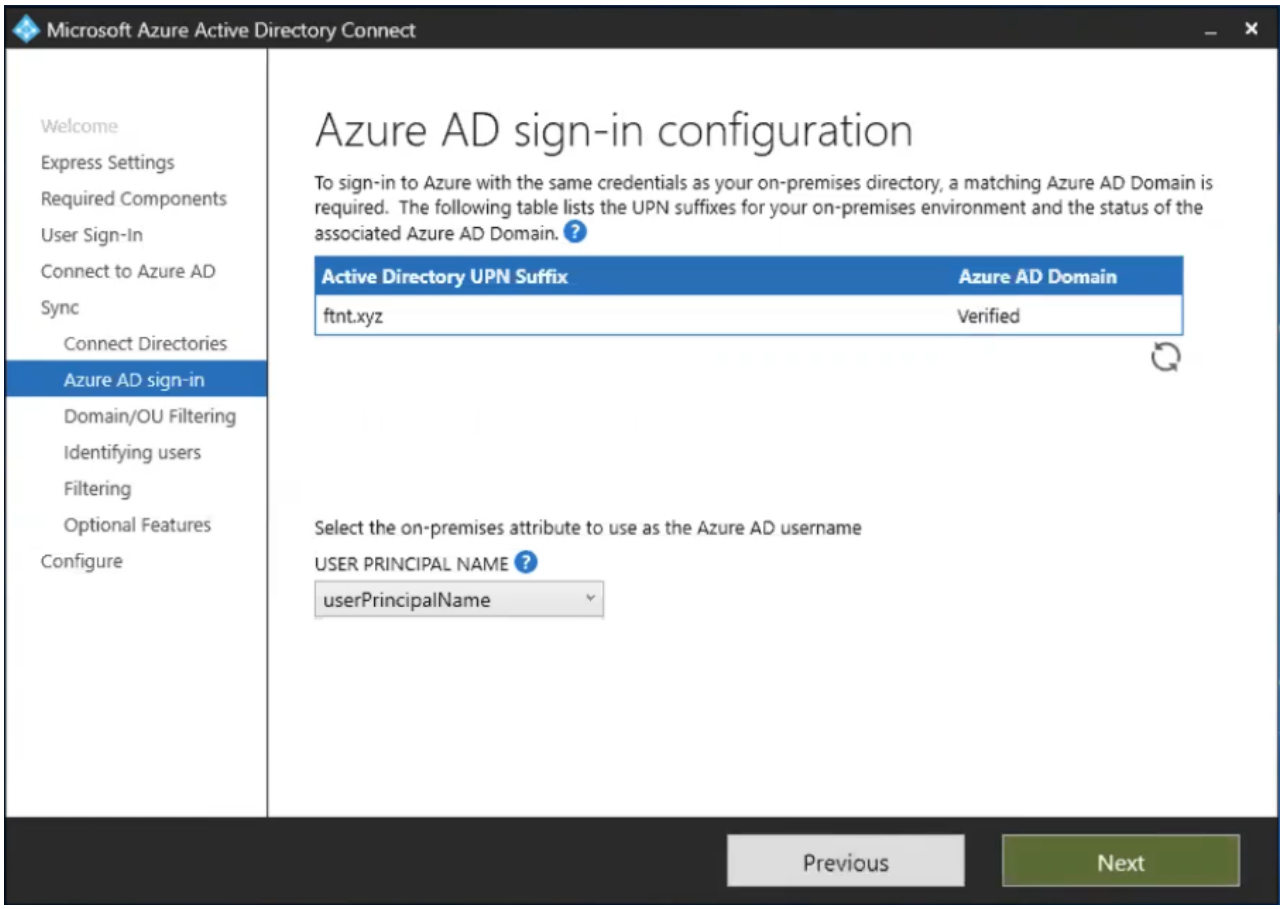
4. On the *Connect to Azure AD* page, enter your Microsoft Entra ID global administrator credentials, and click *Next*.



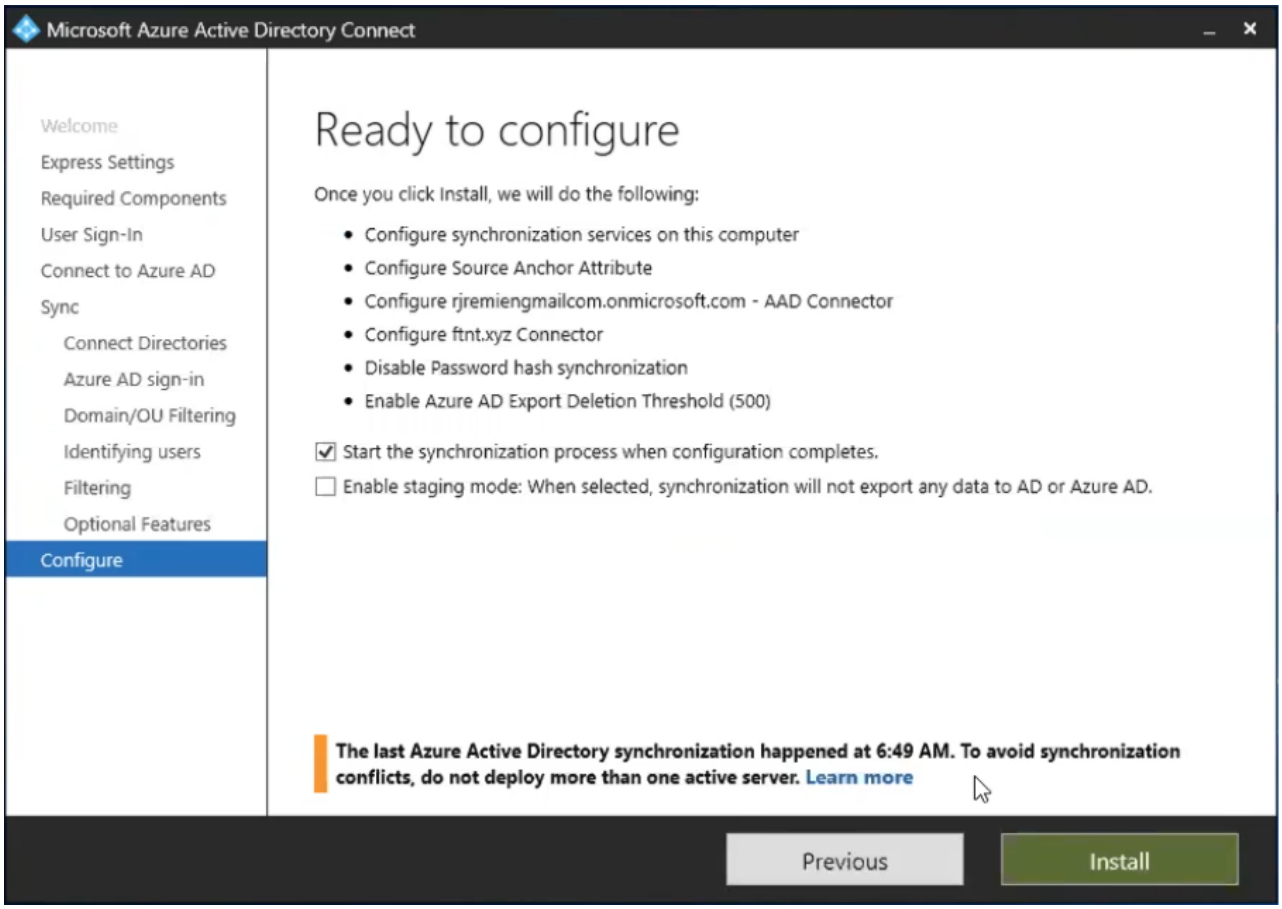
5. Select your Active Directory Forest, and click *Add Directory*. Create your on-premise AD admin user account.



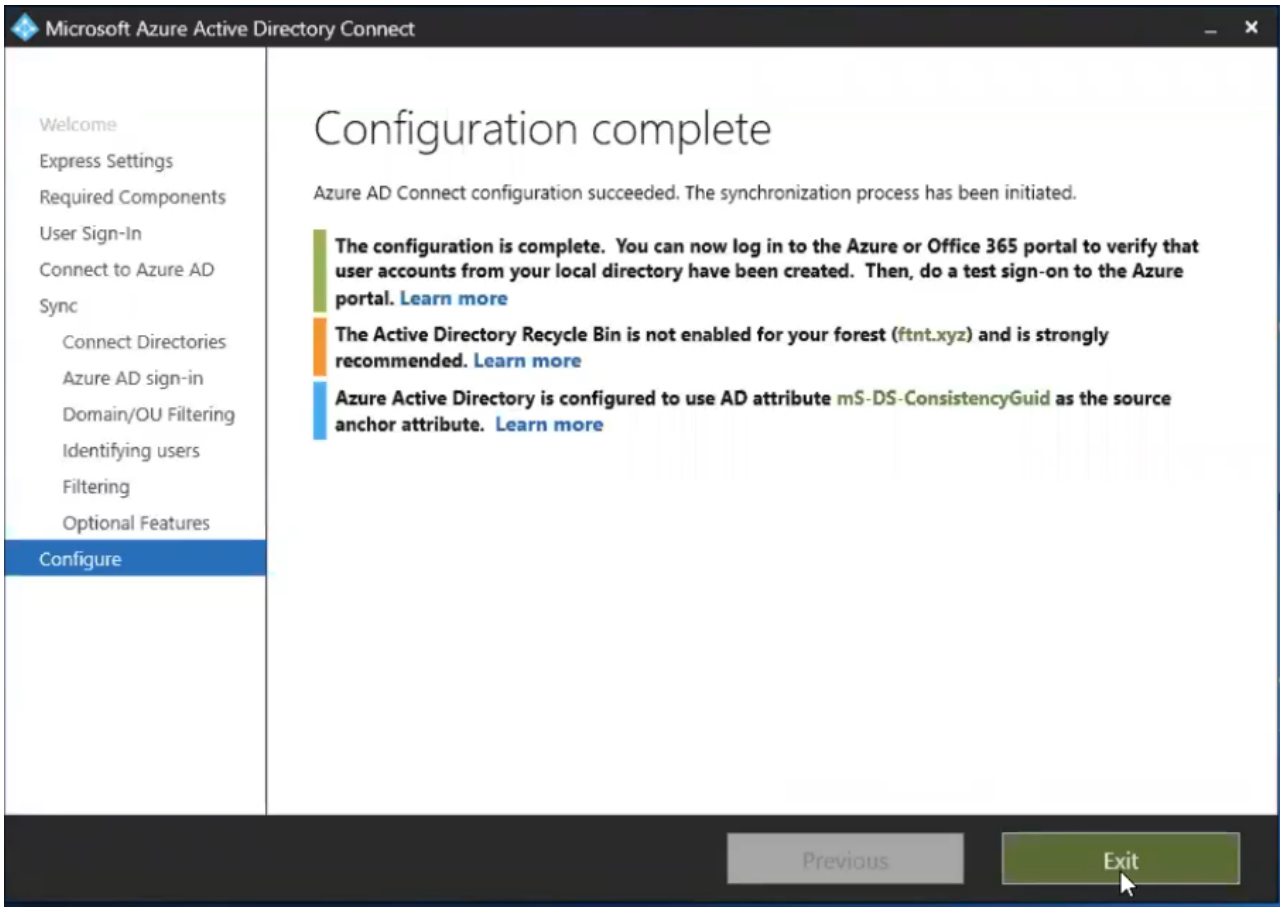
When finished, click *Next*. If completed successfully, you will see your domain has been verified.
Click *Next* again.


Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
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
Previous
Next

6. Click *Next* on the remaining pages in the configuration wizard, and click *Install* on the *Ready to configure* page.



7. Once the installation is complete, you are presented with the Configuration complete page which provides a summary of the configuration changes.

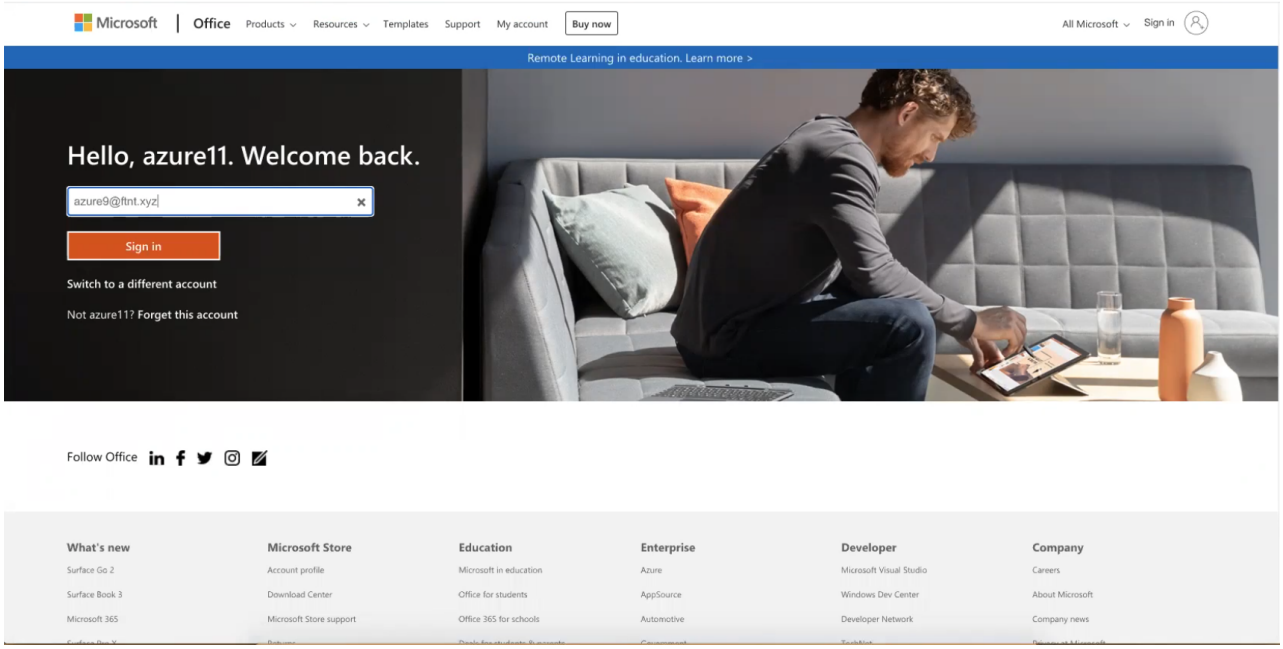


Results

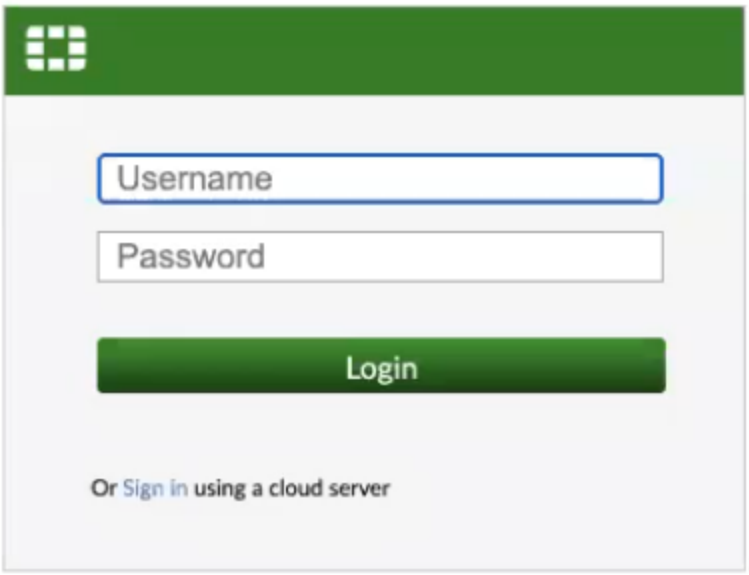
Once configured, Active Directory synchronized users can sign in to Office 365 using two-factor authentication from FortiAuthenticator.

To sign in to Office 365 using FortiAuthenticator with two-factor authentication:

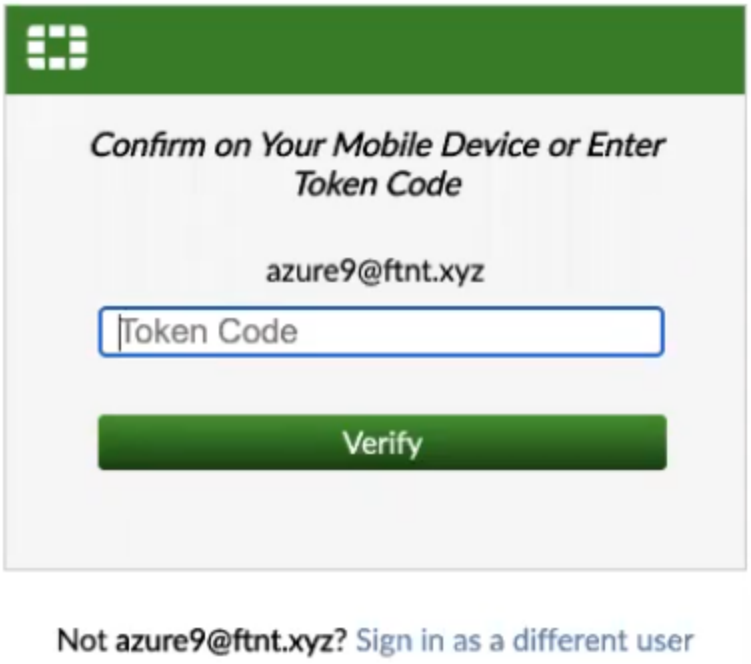
1. Navigate to Office 365 and click *Sign in* or *Switch to a different account*.
2. Enter a user account with domain and click *Sign in*.



3. Authentication is redirected to FortiAuthenticator. Enter your user credentials, and click *Login*.



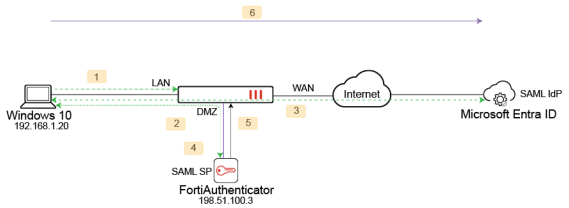
Enter your 2FA token or approve the access request from your FortiToken push request.



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

SAML FSSO with FortiAuthenticator and Microsoft Entra ID (formerly 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 Entra ID, as the identity provider (IdP).



1. The client connects to FortiGate, which redirects the user to the FortiAuthenticator captive portal.
2. The client connects to FortiAuthenticator (SAML SP), which redirects the user to Microsoft Entra ID (SAML IdP).
3. The client connects to the Microsoft Entra ID to perform authentication. It receives SAML token on successful authentication.
4. The client updates the SP with its SAML token.
5. The authenticated user is synced with the FortiGate device.
6. The user can now pass from LAN to WAN.

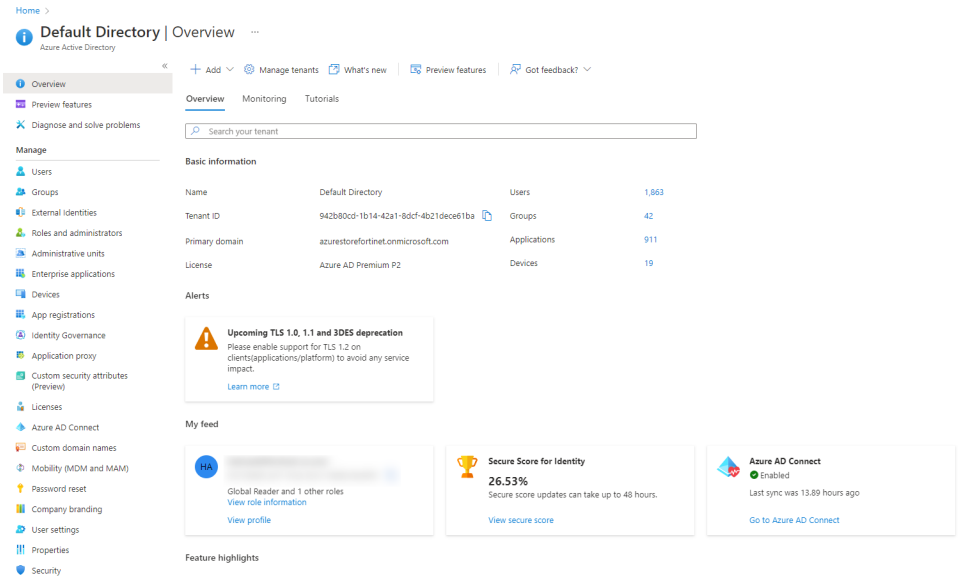
To configure SAML FSSO with FortiAuthenticator and Microsoft Entra ID:

1. Microsoft Azure related configurations:
   a. Creating a tenant in Azure Portal on page 232.
   b. Creating an enterprise application in Azure Portal on page 234.
   c. Setting up single sign-on for an enterprise application on page 235
      i. Adding a user group SAML attribute to the enterprise application on page 236.
      ii. Adding users to an enterprise application on page 237.
   d. Adding the enterprise application as an assignment on page 237.
   e. Registering the enterprise application with Microsoft identity platform and generating authentication key on page 238.
2. FortiAuthenticator related configurations:
   a. Creating a remote OAuth server with Azure application ID and authentication key on page 238.
   b. Creating a remote SAML server on page 239.
   c. Setting up SAML SSO in FortiAuthenticator on page 240.
3. FortiGate related configurations:
   a. Adding an FSSO agent on page 241.
   b. Configuring an interface to use an external captive portal on page 242.
   c. Configuring a policy to allow a local network to access Microsoft Azure services on page 241.
   d. Creating an exempt policy to allow users to access the captive portal on page 242.
4. Results on page 243.

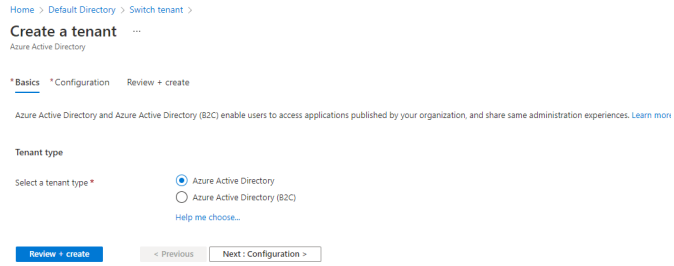
Creating a tenant in Azure Portal

To create a tenant:

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



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*.



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

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

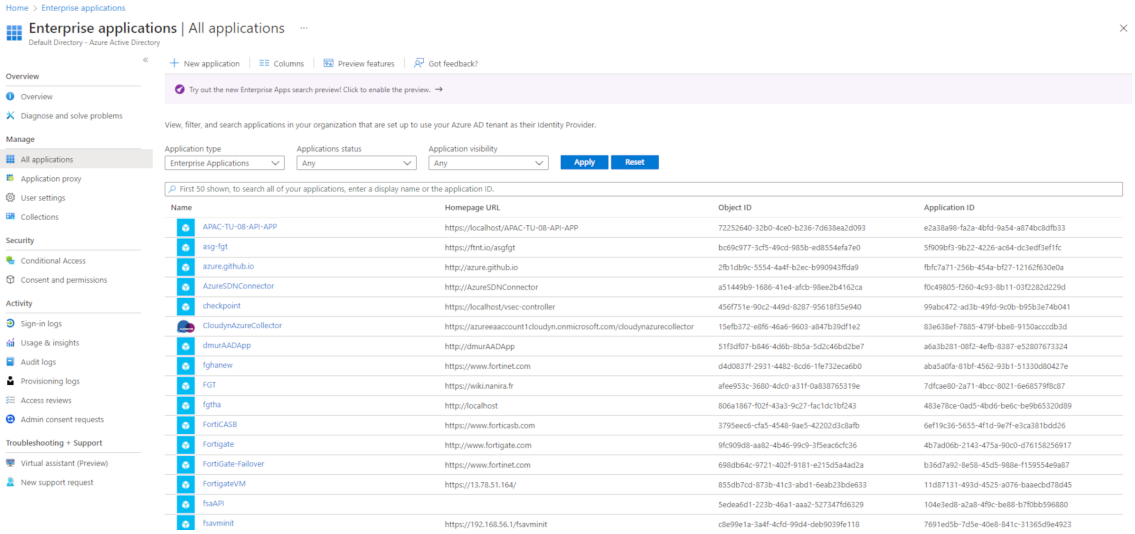
To switch to the correct directory:

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.

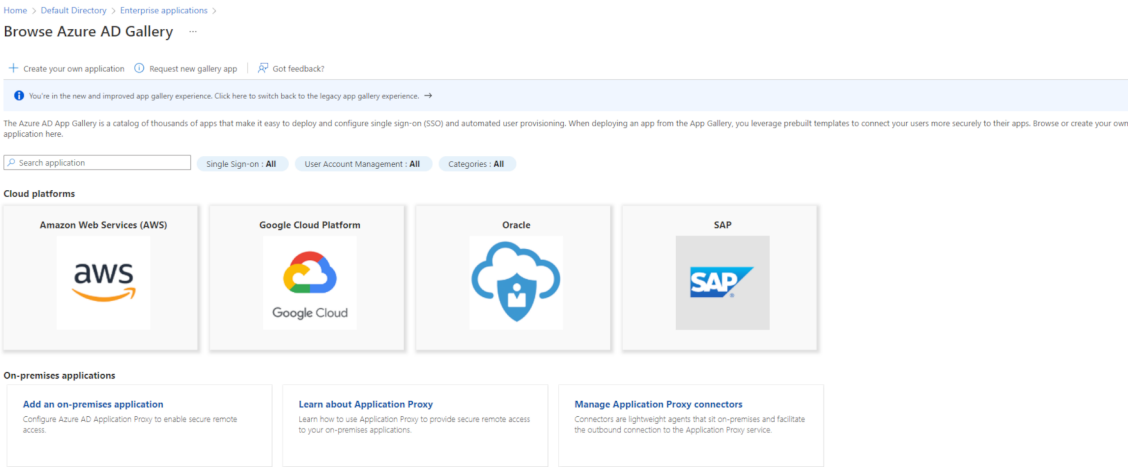
Creating an enterprise application in Azure Portal

To create an enterprise application:

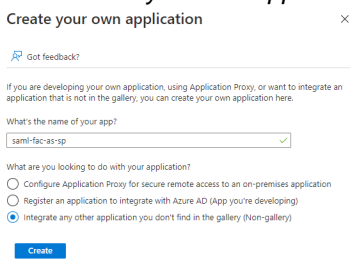
1. Go to *Azure Active Directory* > *Enterprise applications*.



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



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*.

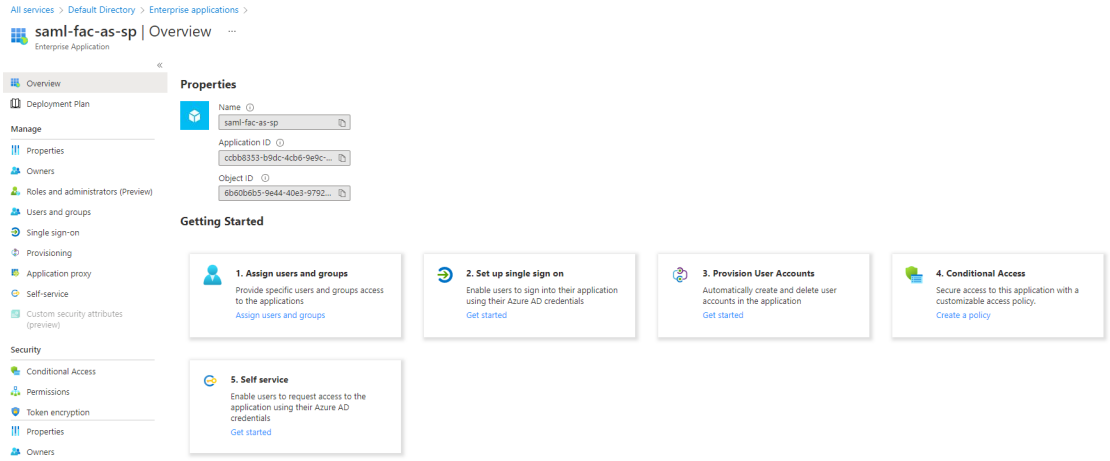


Setting up single sign-on for an enterprise application

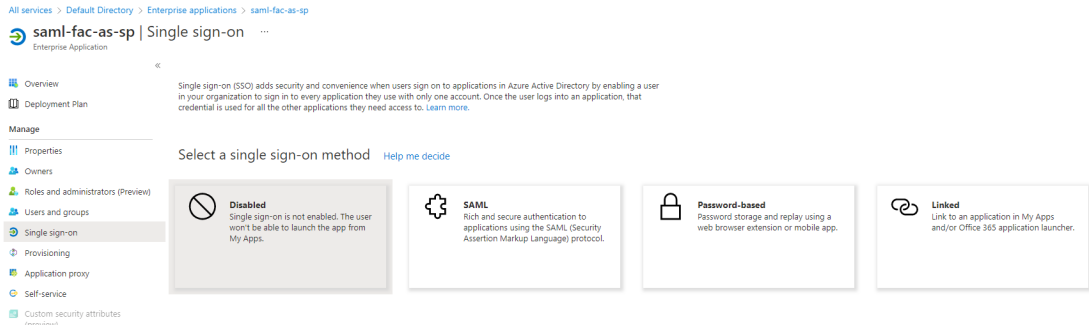
Once the application is created, you can set up single sign-on for your application.

To set up single sign-on:

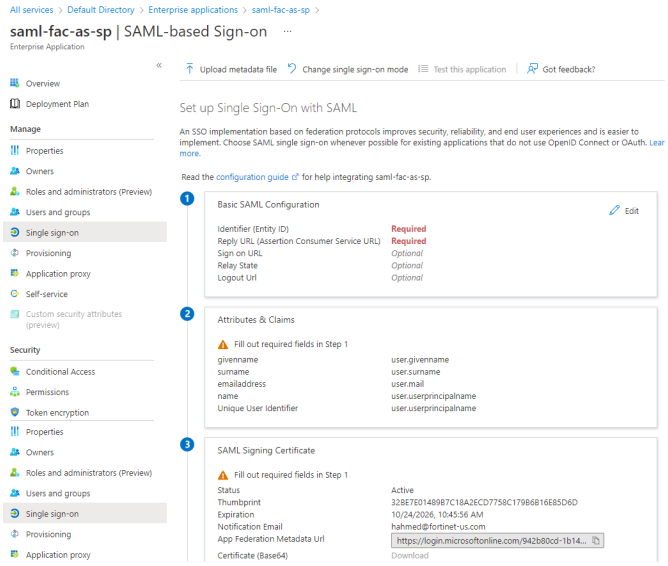
1. Go to *Azure Active Directory > Enterprise applications*.
2. In *Enterprise applications*, enter the name of your enterprise application in the search bar, and click the application to open it.
   See Creating an enterprise application in Azure Portal on page 234.



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



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



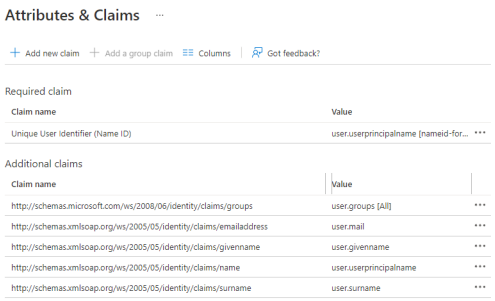
5. In the *SAML-based Sign-on* window, select *Edit* in the *Basic SAML Configuration* pane.
6. In the *Basic SAML Configuration* window, enter the following information from the FortiAuthenticator SP:
   a. In *Identifier (Entity ID)*, enter the SP entity ID.
   b. In *Reply URL (Assertion Consumer 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*.

See Adding a user group SAML attribute to the enterprise application on page 236 and Adding users to an enterprise application on page 237.

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 235, 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.

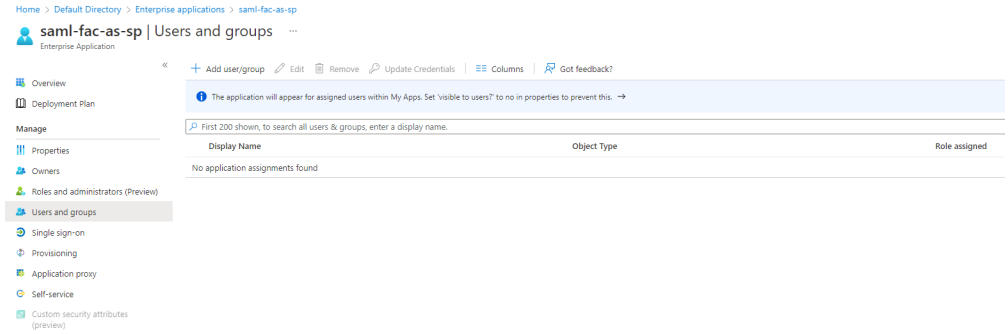


In the *SAML Signing Certificate* pane, download the certificate file (base64) needed to configure the remote SAML server.

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 235, go to *Users and Groups*.



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 237.
5. In *Client Key*, enter the authentication key created in Registering the enterprise application with Microsoft identity platform and generating authentication key on page 238.
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

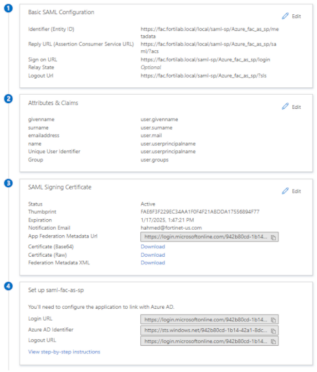
To create a remote SAML server:

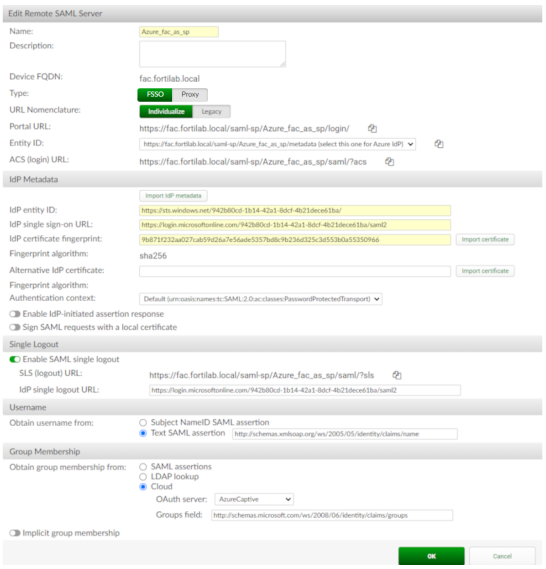
1. Go to *Authentication > Remote Auth. Servers > SAML* and select *Create New*.
   The *Create New Remote SAML Server* window opens.
2. Enter a name for the remote SAML server.
   The name of the remote SAML server is then used when configuring SAML single sign-on in Azure.
3. Select *Type* as *FSSO*.

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 238
11. Click *OK*.

The following shows the relation between the Microsoft Entra ID IdP and the remote SAML server.





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 239.
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 Microsoft Entra ID:

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 Microsoft Entra ID 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 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*.

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*.

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

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 2FA:

1. Configure FortiAuthenticator as an SP in ADFS on page 244
2. Configure the remote SAML server on FortiAuthenticator on page 244
3. Configure SAML settings on FortiAuthenticator on page 245
4. Configure two-factor authentication on FortiAuthenticator on page 247
5. Configure FortiAuthenticator replacement messages on page 248
6. Results on page 248

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*

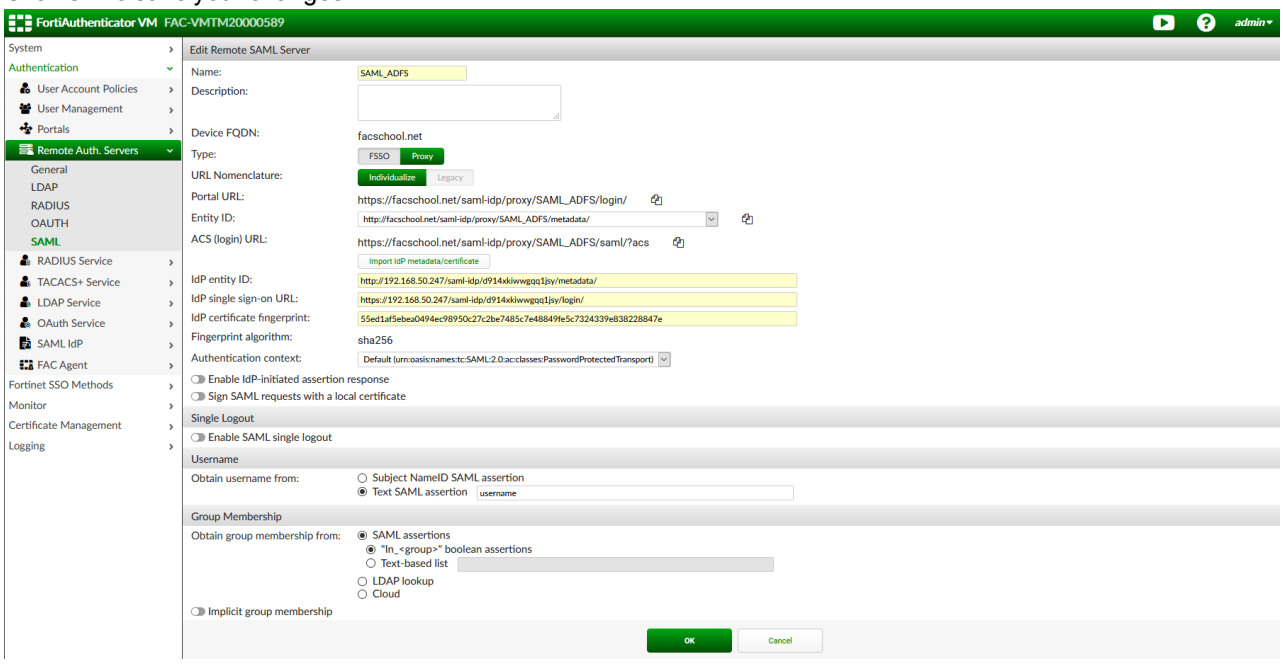
Configure the remote SAML server on FortiAuthenticator

Configure a remote SAML server connected to the ADFS IdP.

To configure the remote SAML server on FortiAuthenticator:

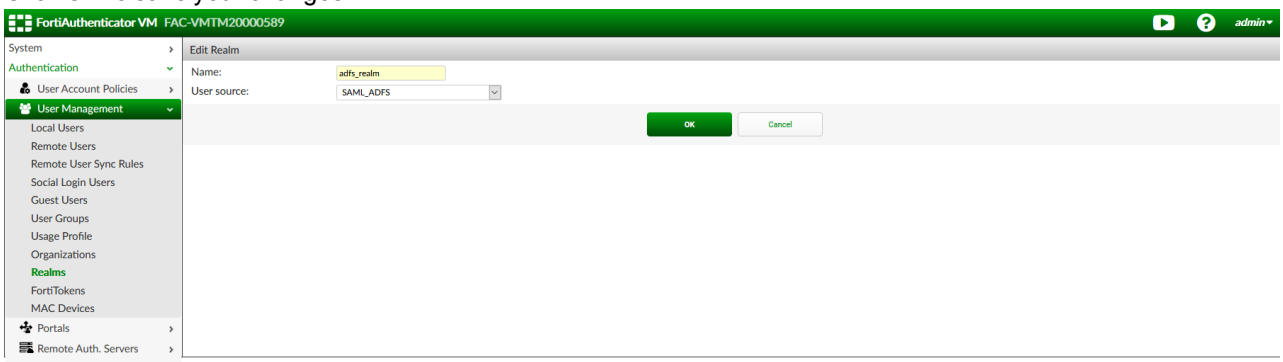
1. Go to *Authentication > Remote Auth. Servers > SAML* and click *Create New*.
2. Configure the remote SAML server:
   a. **Name**: Provide a name for the remote SAML server.
   b. **Type**: *Proxy*
   c. **IdP Settings**: Enter the *IdP entity ID*, *IdP Single sign-on URL*, and *IdP certificate fingerprint*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

3. Click *OK* to save your changes.



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.

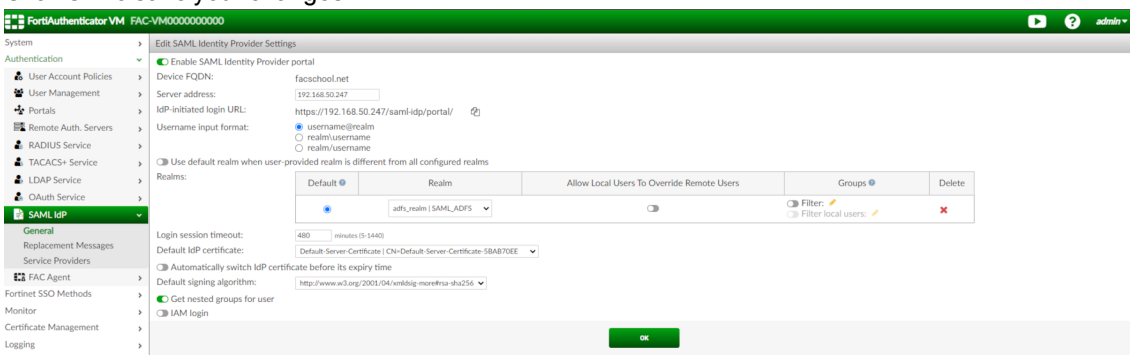


Configure SAML settings on FortiAuthenticator

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.

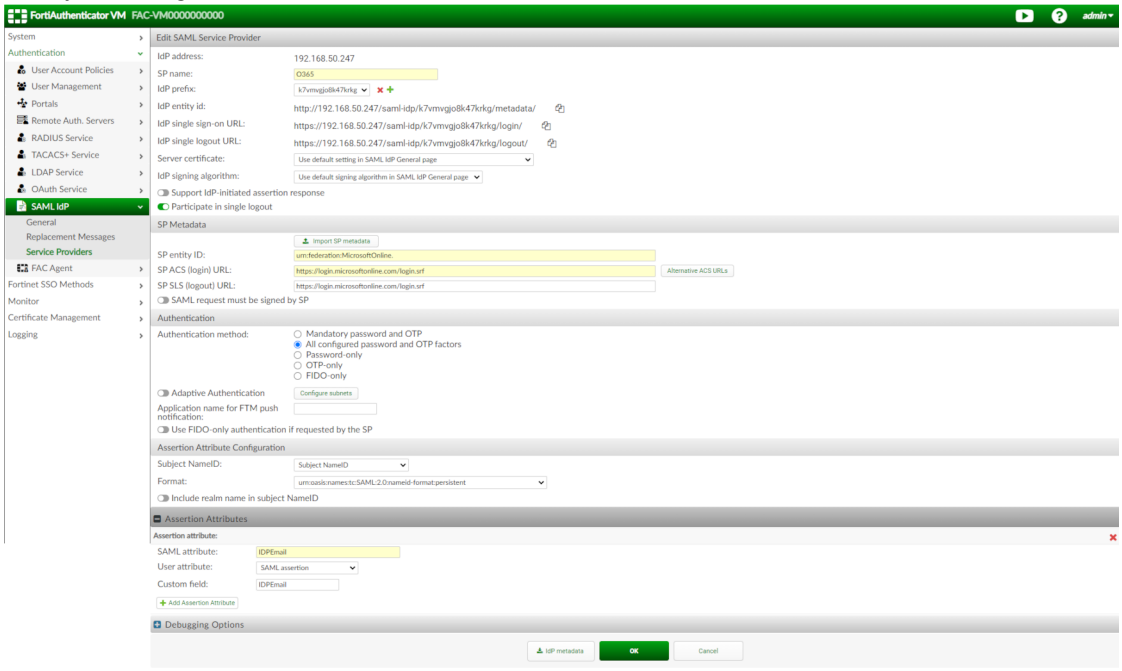
3. Click *OK* to save your changes.



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.



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.

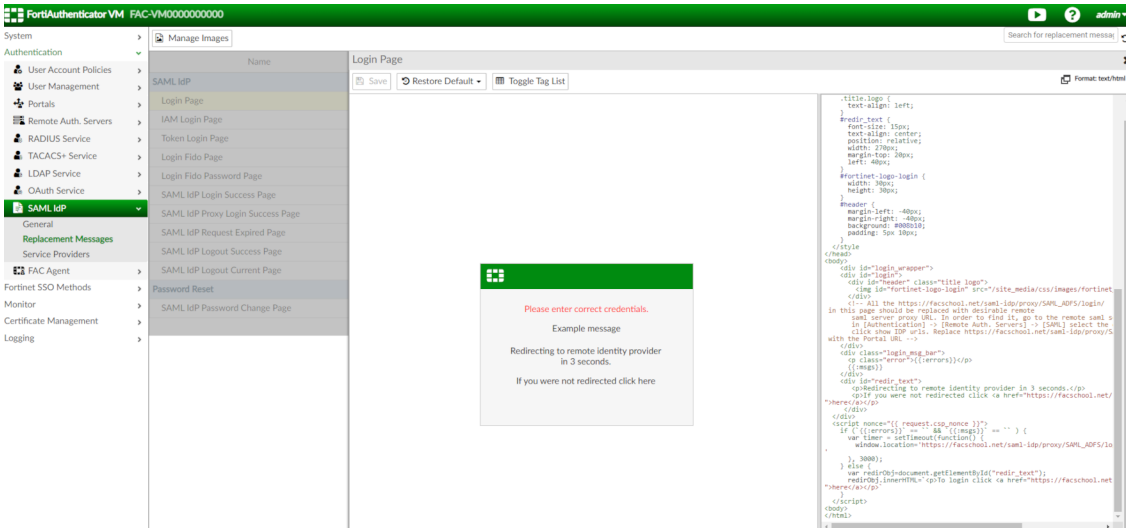
To configure remote users with two-factor authentication:

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*.

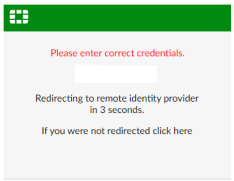


Results

Once configured, Active Directory synchronized users can sign in to Office 365 using two-factor authentication from FortiAuthenticator.

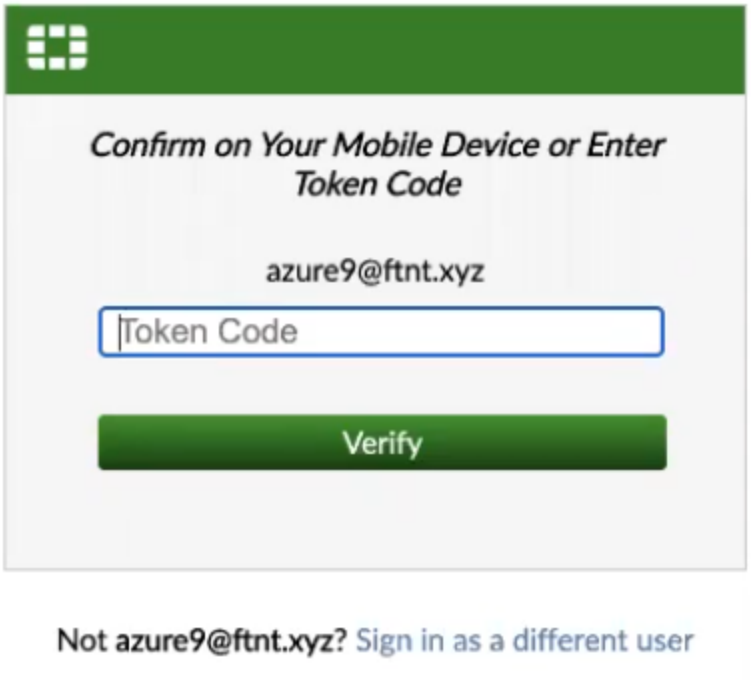
To sign in to Office 365 using FortiAuthenticator with two-factor authentication:

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



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.



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

Agentless VPN SAML authentication using FortiAuthenticator with OneLogin as SAML IdP

Using this example, you can set up a SAML authentication based Agentless 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 Agentless 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 Agentless 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 example

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

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

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

1. OneLogin related configurations:
   a. Creating an OneLogin application on page 251
   b. Configuring an application on OneLogin on page 251
      i. Configuring application parameters on OneLogin on page 253
      ii. Configuring SSO on OneLogin on page 254
   c. Granting user access to the application on page 255
2. FortiAuthenticator related configurations:
   a. Configuring a remote SAML server on page 256
   b. Configuring an OneLogin realm on page 258
   c. Creating remote SAML users on page 258
   d. Configuring SAML IdP settings on page 259
   e. Configuring FortiAuthenticator replacement message on page 260
   f. Configuring FortiGate SP settings on FortiAuthenticator on page 260
3. FortiGate related configurations:
   a. Uploading SAML IdP certificate to the FortiGate SP on page 262
   b. Creating SAML user and server on page 263
   c. Mapping Agentless VPN authentication portal on page 265
   d. Increasing remote authentication timeout using FortiGate CLI on page 266
   e. Configuring a policy to allow users access to allowed network resources on page 266

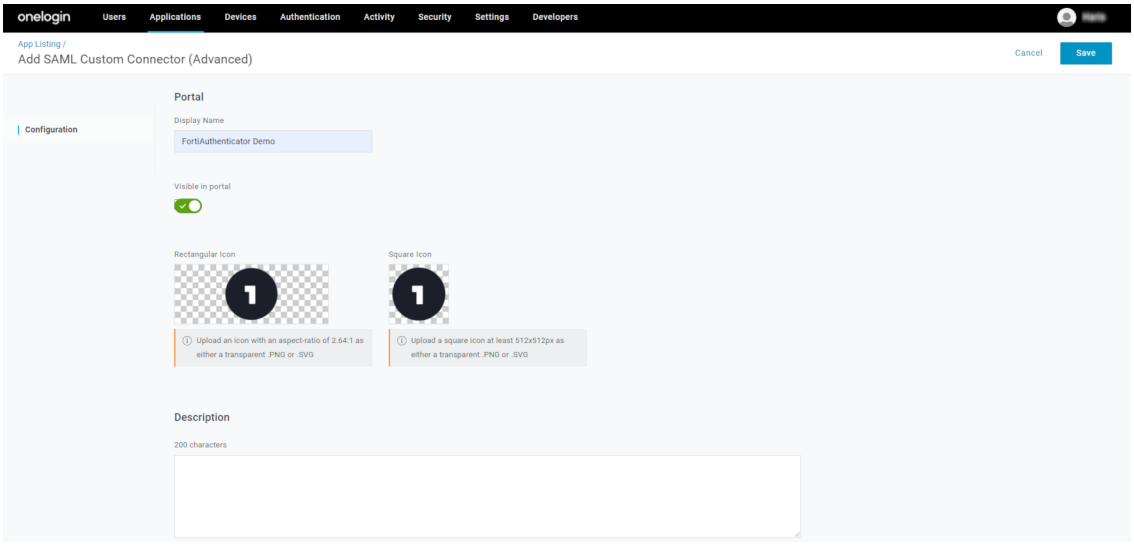
Creating an OneLogin application

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*.



See Configuring an application on OneLogin on page 251, Configuring application parameters on OneLogin on page 253, and Configuring SSO on OneLogin on page 254.

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 251, 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.

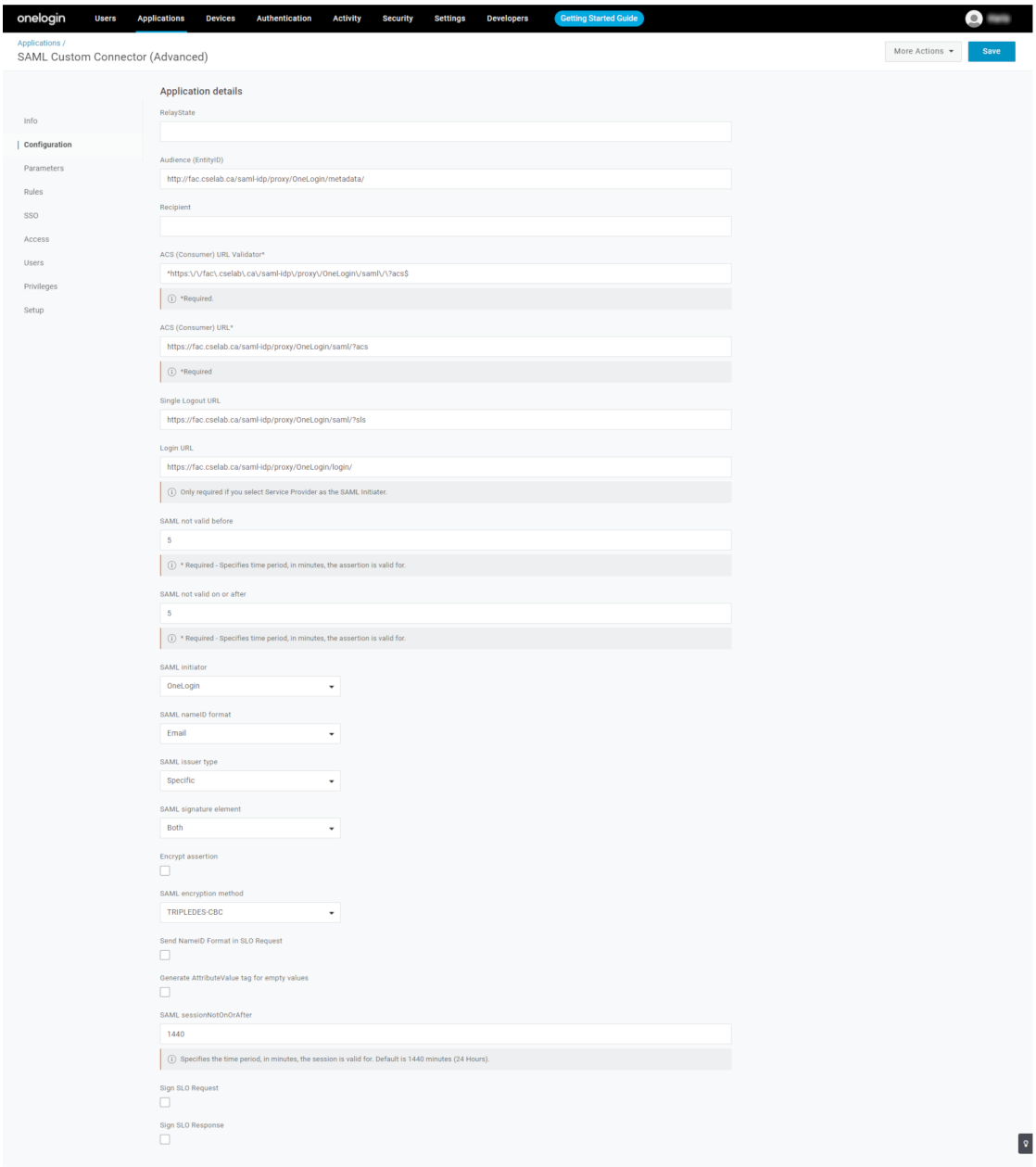
The *ACS (Consumer) URL Validator* must start with a "^", end with a "$", and have a "\" preceding every "/", "?" and ".".

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 256.



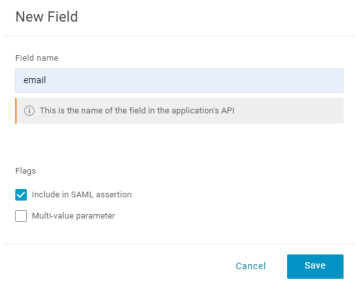
Configuring application parameters on OneLogin

To configure an email application parameters on OneLogin:

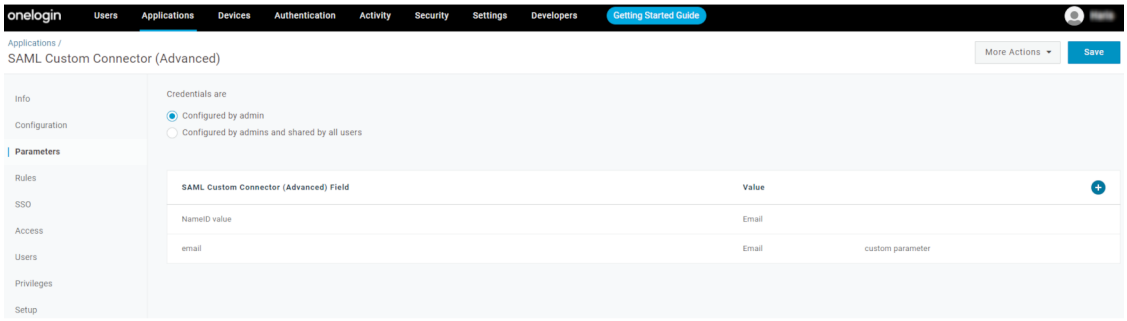
1. Go to *Applications* > *Applications*, from the applications list select your application.
2. Go to the *Parameters* tab and select *+*.
   The *New Field* dialog opens.
3. In the *New Field* dialog:
   a. In *Field* name, enter a name.
   b. Select the *Include in SAML assertion* checkbox

c. Click *Save*.

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

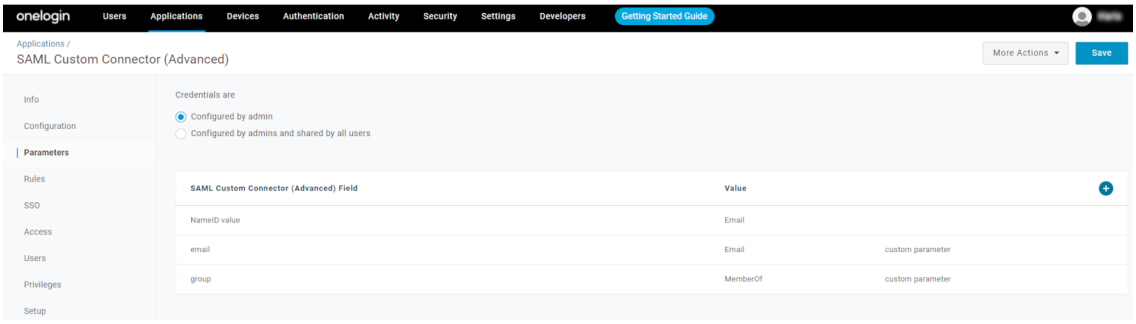


Once the field is configured, the window should appear as shown below.



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.



Configuring SSO on OneLogin

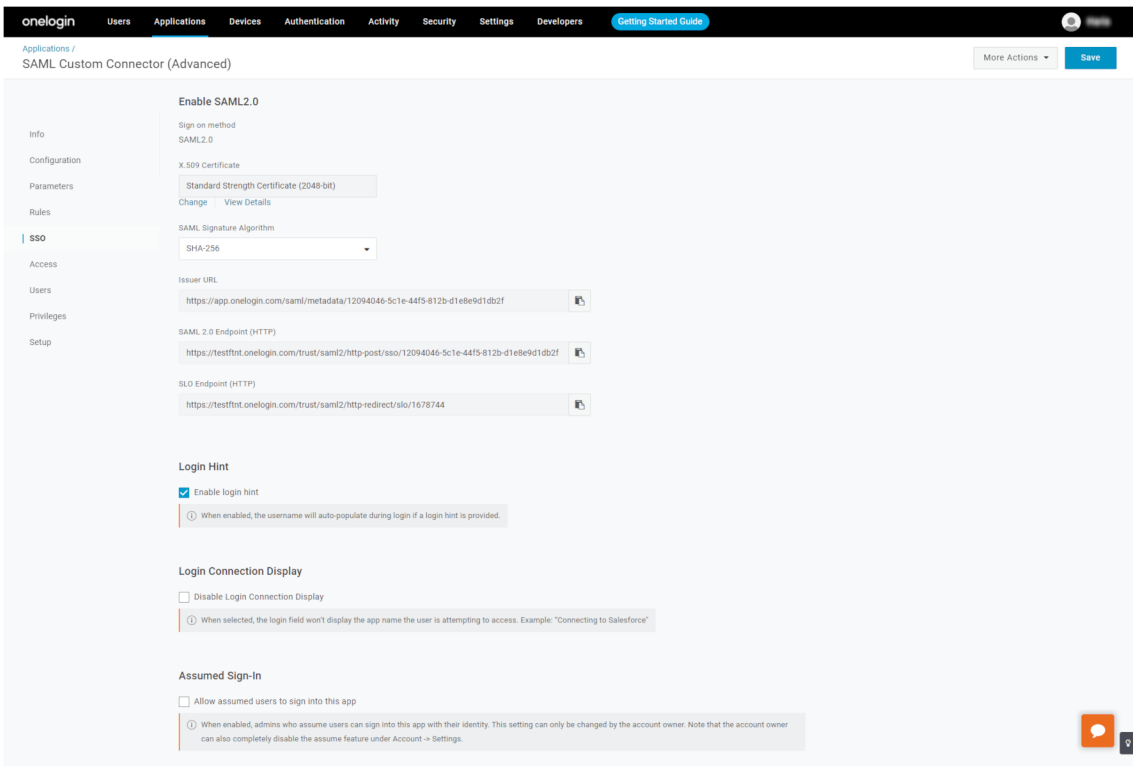
To configure SSO on OneLogin:

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*.

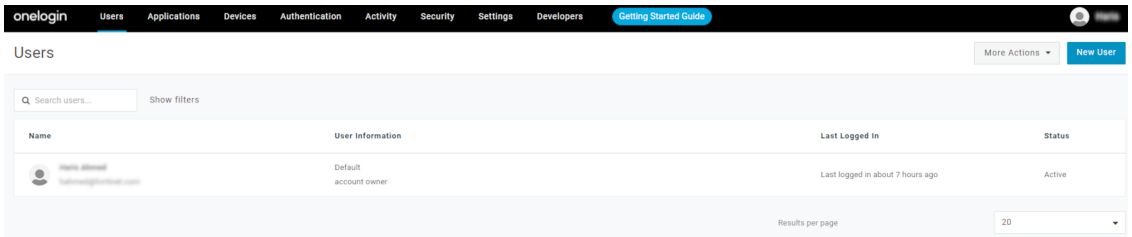
Select a format from the dropdown and download the certificate.



Granting user access to the application

To grant user access to the application:

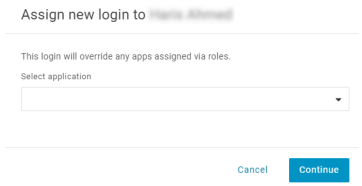
1. Go to *Users* > *Users*.



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.



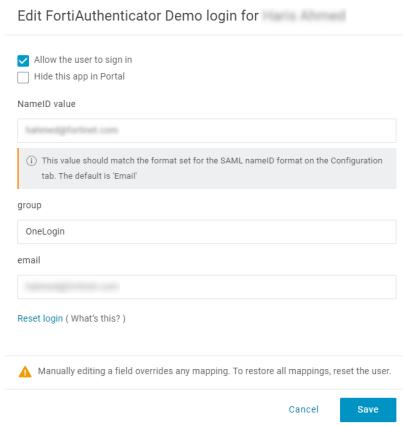
5. In the new dialog that appears:
   a. Ensure that *Allow the user to sign in* is selected.
   b. In *NameID value*, enter the user email address.
   c. In *group*, enter *OneLogin*.

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 260 and Configuring a policy to allow users access to allowed network resources on page 266.

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



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 254 and Configuring application parameters on OneLogin on page 253.

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*.

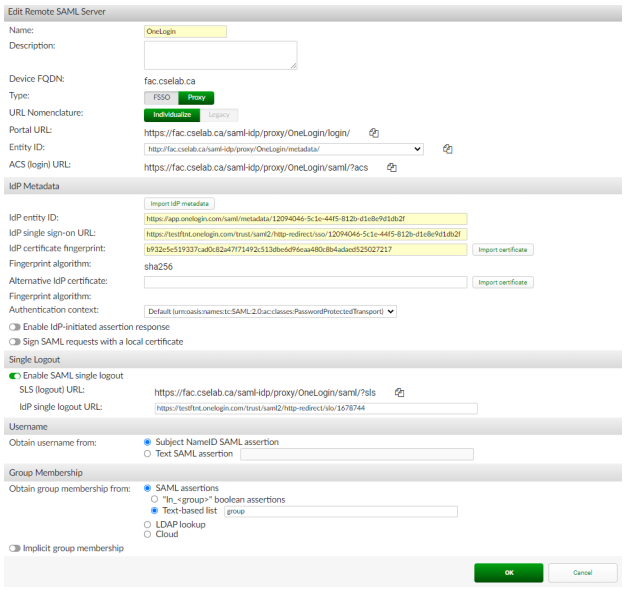
The *Portal URL* is the SAML SP login URL.

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*.

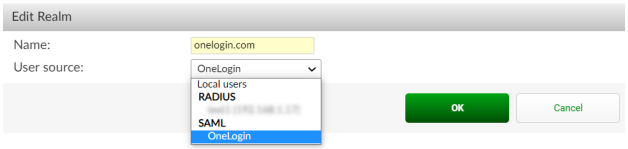


Once the OneLogin application is set up and a certificate is associated with the application, you can download the IdP metadata by going to *More Actions > SAML Metadata* in one of the tabs when configuring the application.

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 256.
4. Click *OK*.



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 256.

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*.

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

Configuring SAML IdP settings

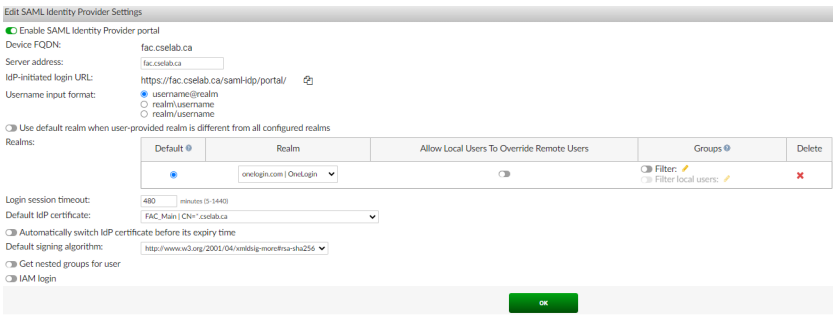
To configure SAML IdP settings:

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 Sy*stem > Dashboard > Status*.

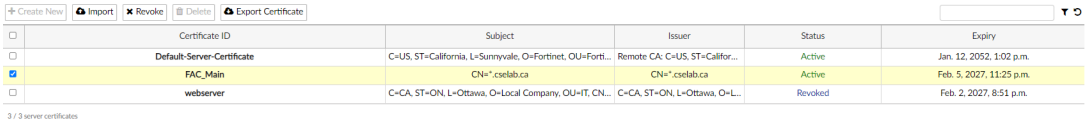
   FQDN must be reachable via DNS for users using the service.

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 258. 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 262.
   To export the IdP certificate, see Exporting the IdP certificate.
7. Ensure that *Get nested groups for user* is disabled.
8. Click *OK*.



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*.



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 256.
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 259.
   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 263.
   b. **SP ACS (login) URL**: Enter the *SP single sign-on URL* from Creating SAML user and server on page 263.
   c. **SP SLS (logout) URL**: Enter the *SP single logout URL* from Creating SAML user and server on page 263.

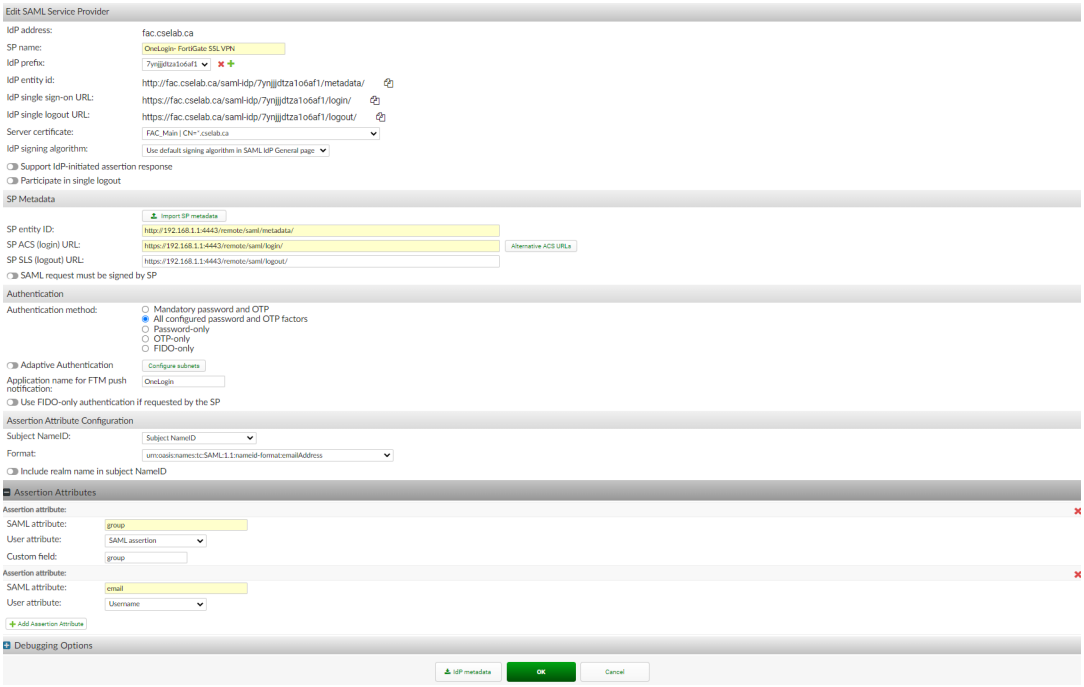
   SP entity ID, *SP ACS (login) URL*, and *SP SLS (logout) URL* must match their respective configurations on the FortiGate SP side.

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 263.

9. Click *OK* to save changes.

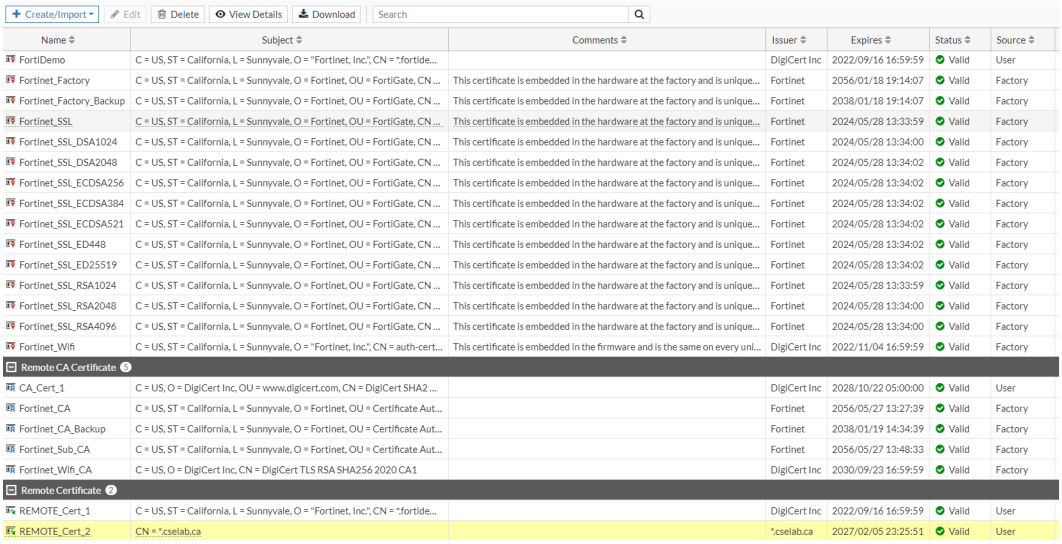


Uploading SAML IdP certificate to the FortiGate SP

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 263.

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 263.

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 Agentless VPN in *VPN > Agentless VPN Settings > Listen on Interface(s)*.

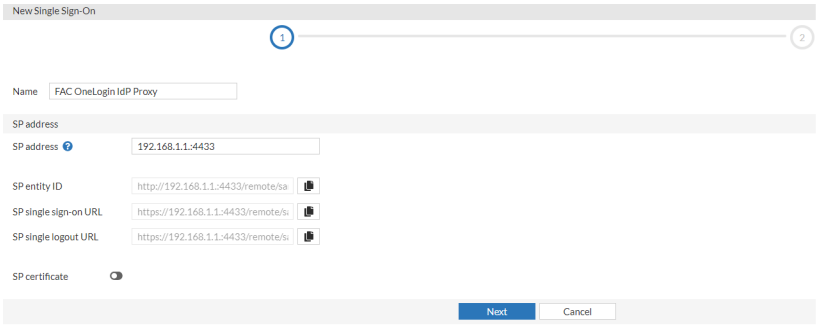
The port should be the same port configured in *VPN > Agentless VPN Settings > Listen on Port*.

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.

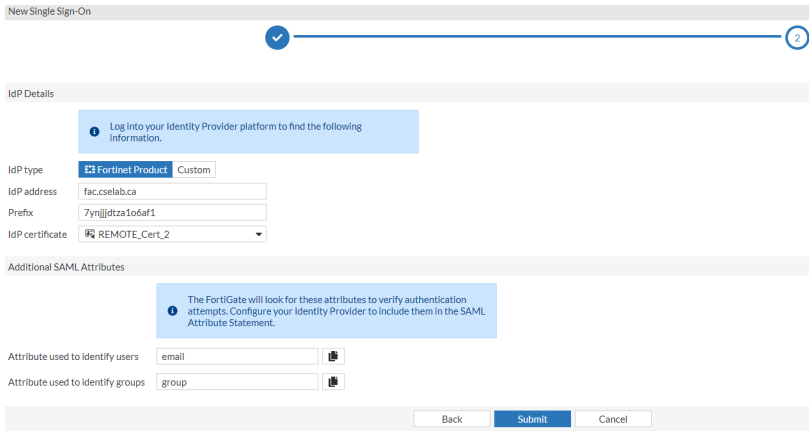
See Configuring FortiGate SP settings on FortiAuthenticator on page 260.

4. Click *Next*.



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 259.
   c. In *Prefix*, enter the *IdP prefix* from Configuring FortiGate SP settings on FortiAuthenticator on page 260.
   d. In the *IdP certificate* dropdown, select the certificate from Uploading SAML IdP certificate to the FortiGate SP on page 262.
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 260.



7. Click *Submit*.

To create the SAML group:

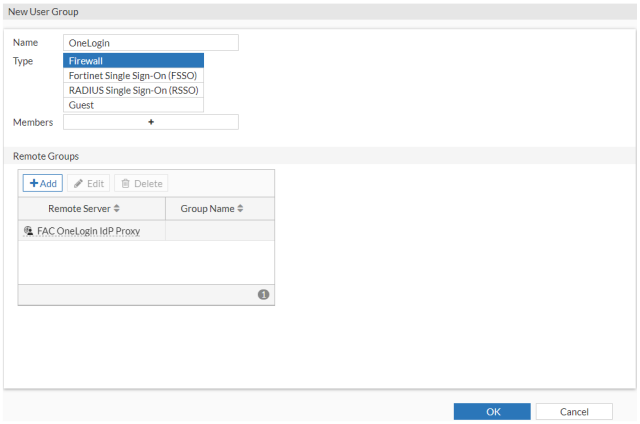
1. Go to *User & Authentication >User Groups* and click *Create New*.
2. Enter a name for the group.
3. In *Remote Groups*, select *Add*.
   The *Add Group Match* window opens.
4. In the *Remote Server* dropdown, select *FAC OneLogin IdP Proxy*.

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*.



Mapping Agentless VPN authentication portal

To map Agentless VPN authentication portal:

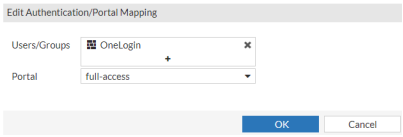
1. Go to *VPN > Agentless VPN Settings*.
2. In the *Authentication/Portal Mapping* pane:
   a. Select *Create New*.
      The *New Authentication/Portal Mapping* window opens.
   b. In *User/Groups*, select *+*, search and select the SAML user group configured in Creating the SAML group.

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*.



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 *Agentless 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 Agentless 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 Agentless VPN with FortiAuthenticator as SAML IdP

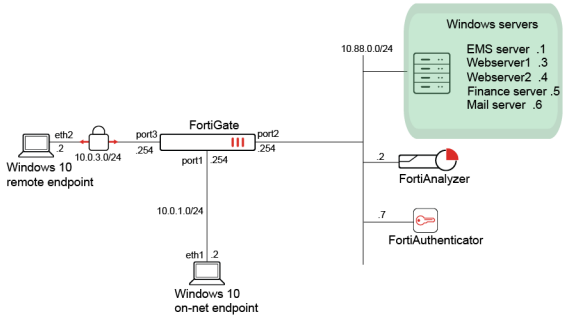
Starting FortiOS 7.6.3, SSL VPN web mode is renamed Agentless VPN.
See IPsec and SSL VPN or Agentless VPN in the latest FortiOS New Features Guide.

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 Agentless 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 Agentless VPN:

1. The user initiates an Agentless 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 Agentless 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.

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. 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.

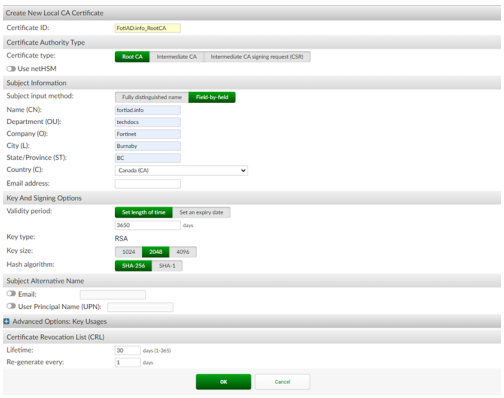
Furthermore, in this scenario, the CA on the FortiAuthenticator will also sign the Agentless VPN certificate used by the FortiGate. This certificate must also be exported and loaded on the FortiGate.

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*.



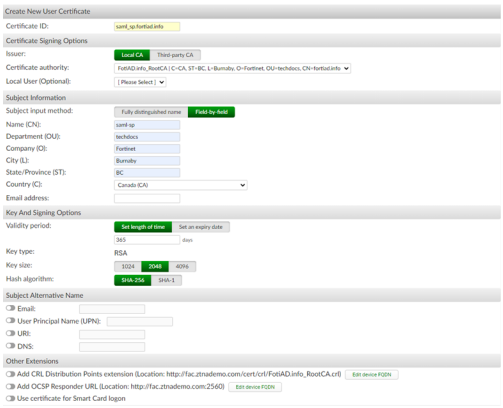
To export the created local CA:

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*.

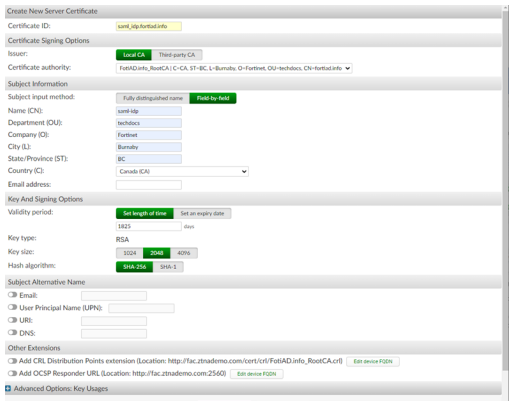


To export the user certificate:

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*.

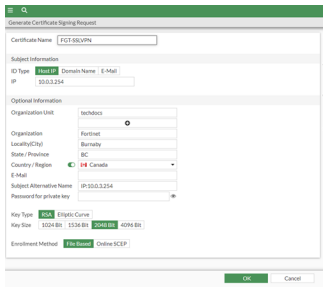


To export the server certificate:

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.

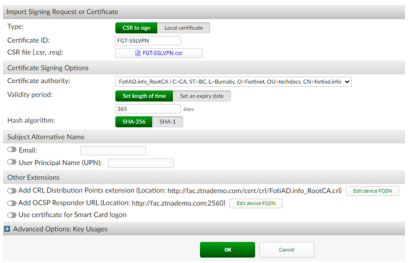
To create and sign a user certificate for FortiGate Agentless VPN web portal:

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*.



4. On the *Certificates* list page, select the user certificate you have created under *Local Certificate*.

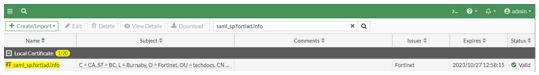
5. Click *Download* to download the CSR file.
6. On FortiAuthenticator, go to *Certificate Management* > *End Entities* > *Users*, and click *Import*.
7. Enter a certificate Id.
8. Select *Upload a file* to locate and upload the CSR file created from the FortiGate.
9. In the *Certificate authority* dropdown,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



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*.

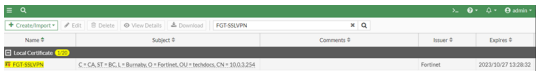


To import the SAML IdP remote certificate:

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*.

To import the user certificate for the FortiGate Agentless 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*.



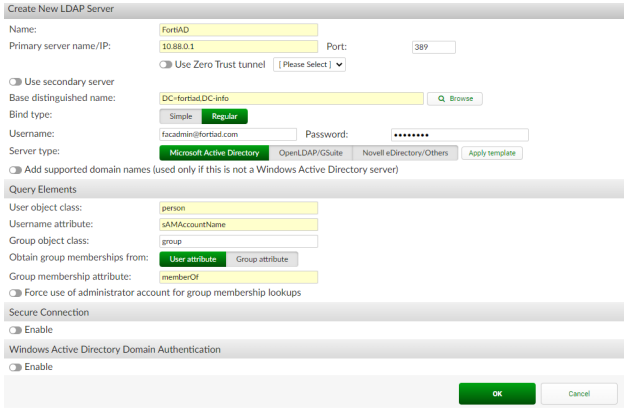
FortiAuthenticator user management

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.



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

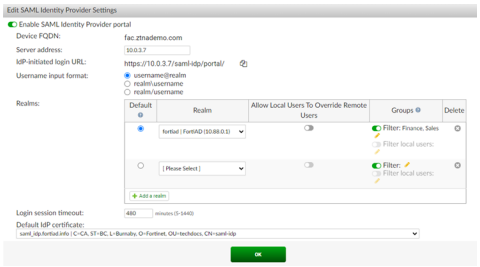
• **FortiGate (SP)** - 10.0.3.254:10443 (10443 is used for access related to Agentless VPN based on the default listening port for Agentless VPN. Change this accordingly when listening on a different port)

In general, the URLs used for the SP and IdP configurations in a Agentless 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:

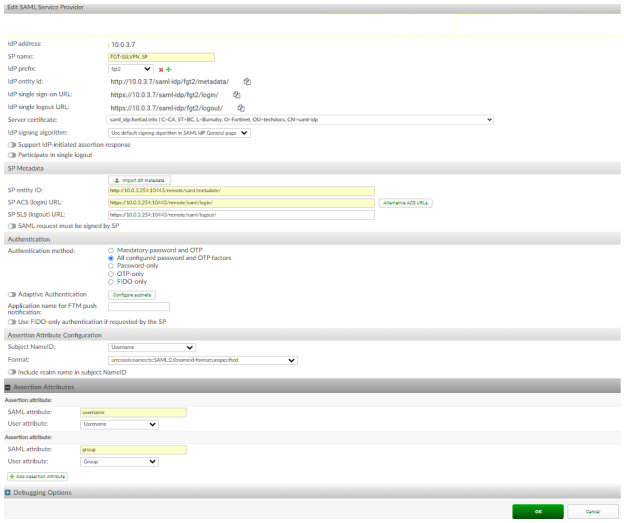
1. Go to *Authentication > SAML IdP > General*.
2. Enable *SAML Identity Provider portal*.
3. Enter the server address. This address must be accessible by the client endpoint.
4. In *Realms*, select *Add a realm* and select the recently created realm from the dropdown.
5. In *Groups*, enable *Filter*, 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*.



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*.



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
```

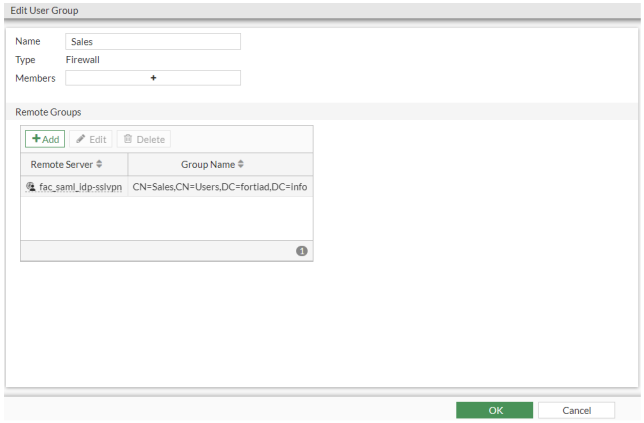
- The setting `set cert <certificate>` corresponds to the SP certificate imported to the FortiGate as a local certificate earlier in the example.
- The setting `set idp-cert <certificate>` corresponds to the IdP certificate imported to the FortiGate as a remote certificate earlier in the example.

FortiGate user management

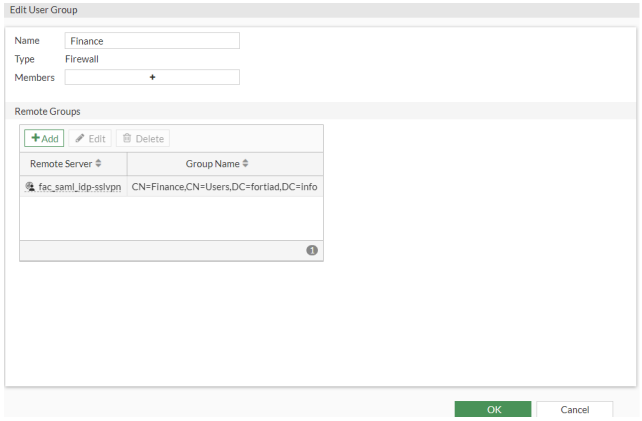
Once user authentication is successful on FortiAuthenticator, it sends a SAML assertion back to the client with the username and group information. When the client redirects this information to the FortiGate SAML SP, the FortiGate must process the assertion and match the correct user group for access control.

To configure user groups for Finance and Sales in FortiGate:

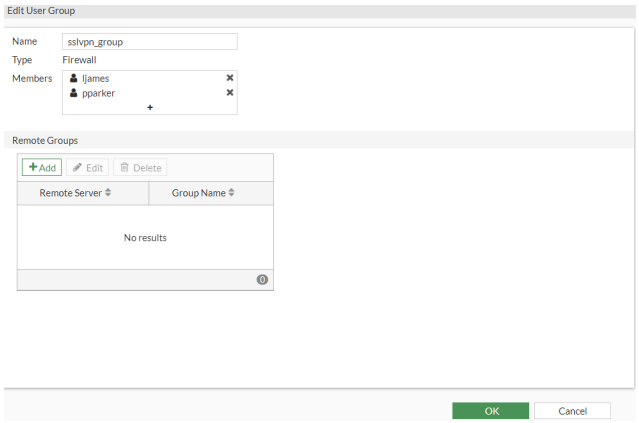
1. Go to *User & Authentication > User Groups* and select *Create New*.
2. To create a user group for **Sales**:
   a. In *Name*, enter *Sales*.
   b. In *Remote Groups*, click *Add*.
   c. Choose the SAML SSO settings as the *Remote Server*.
   d. Set *Groups* to *Specify* and enter the group name `CN=Sales,CN=Users,DC=fortiad,DC=info`.
   e. Click *OK*.



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*.



Besides the groups for SAML users, a non-SAML placeholder group needs to be created in order for Agentless VPN portal to be active. The following shows a placeholder group named `sslvpn_group` with 2 local users.



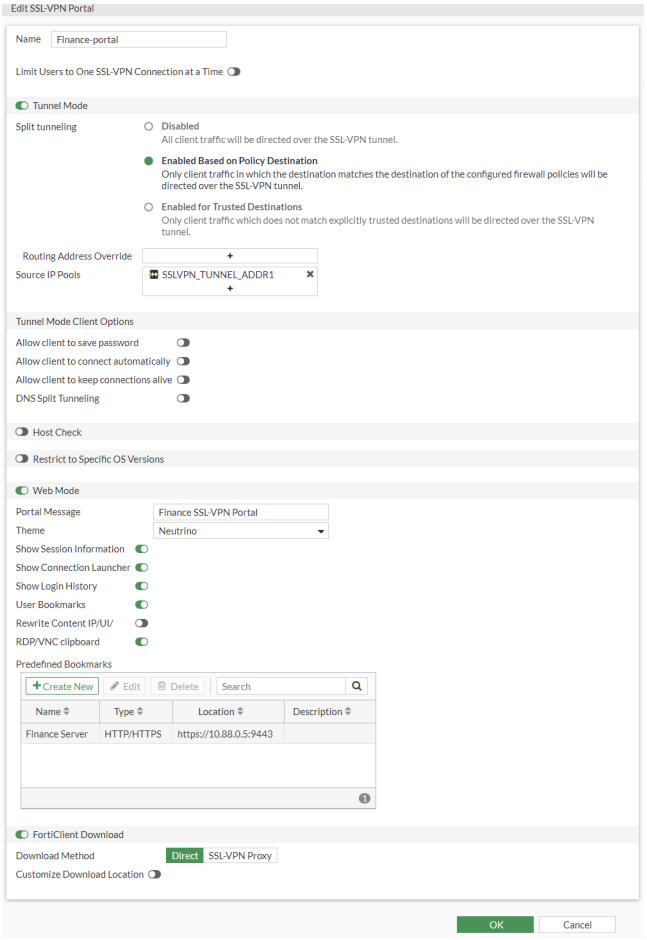
FortiGate Agentless VPN configurations

Configure Agentless 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 Agentless VPN portals for Finance and Sales users:

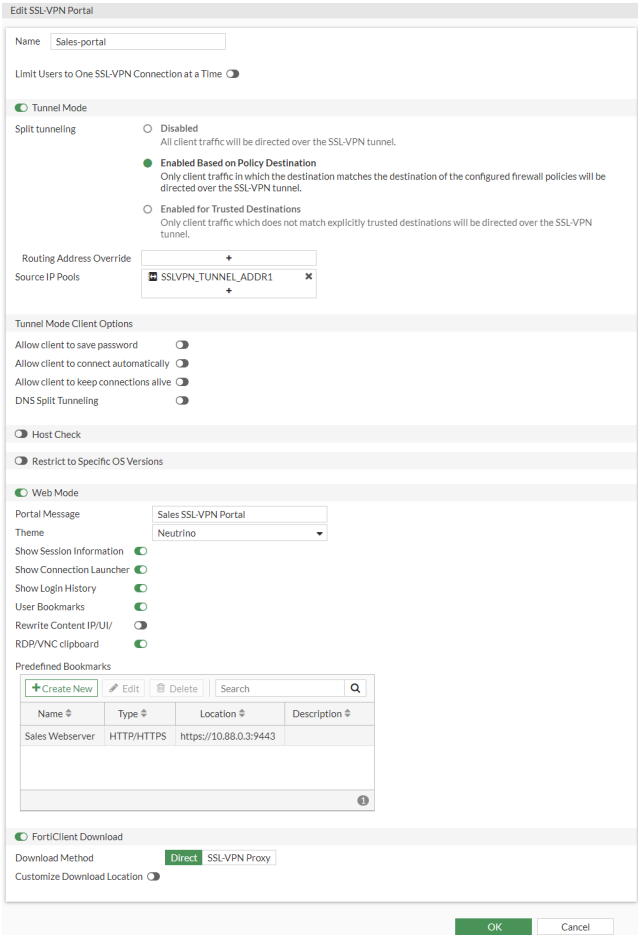
1. Go to *VPN > Agentless VPN Portals* and click *Create New*.
2. To create a profile named **Finance-portal**:
   a. In *Name*, enter *Finance-portal*.
   b. Enable *Tunnel Mode* with split tunneling set to *Enabled Based on Policy Destination*.
   c. Set *Source IP Pools* to a desired pool.
   d. Enable *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*.



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`.

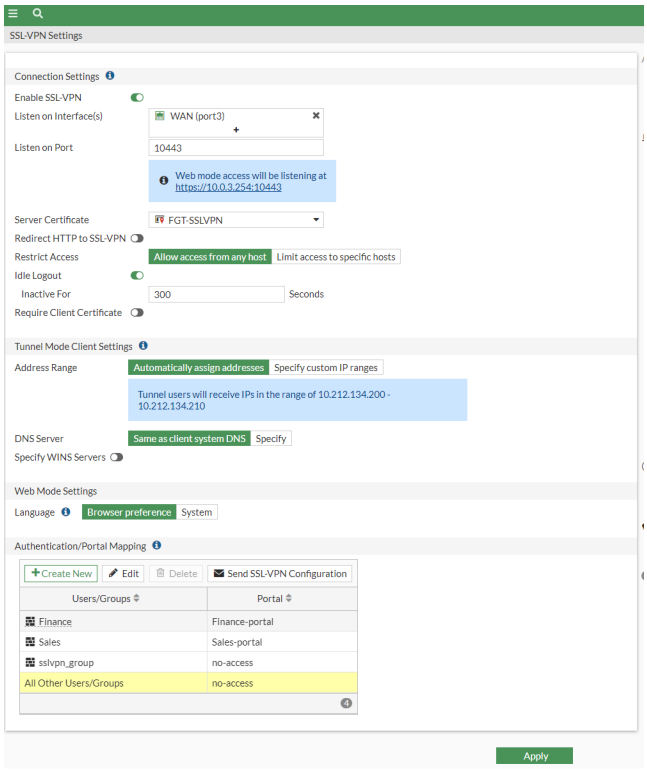
f. Click *OK*.



To configure Agentless VPN settings:

1. Go to *VPN > Agentless VPN Settings* and enable Agentless 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*.

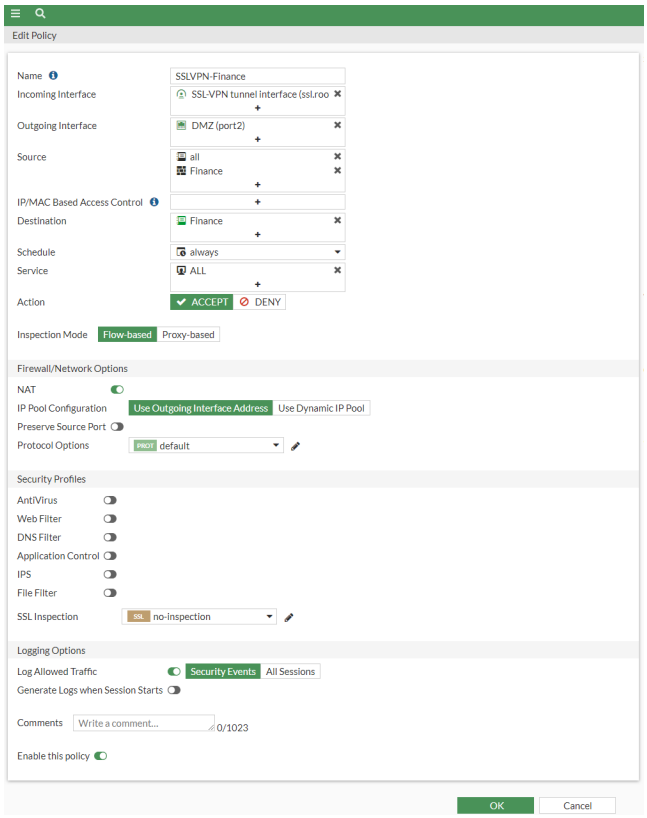
d. For *All other Users/Groups*, set *Portal* to *no-access*.



To configure firewall policies for access control:

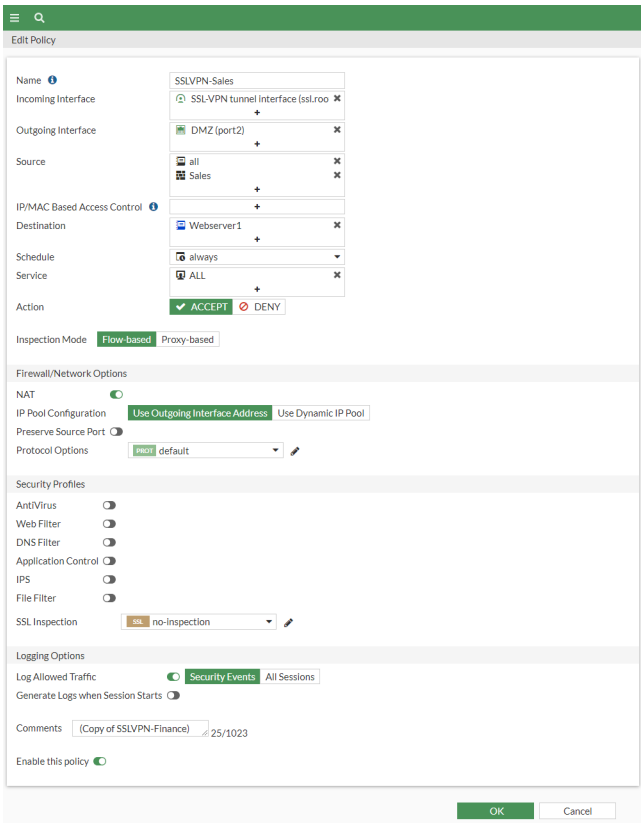
1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Create a policy named *SSLVPN-Finance*.
   a. Set *Incoming Interface* to *Agentless VPN tunnel interface (ssl.root)*.
   b. Set *Outgoing Interface* to *port2*.
   c. Set *Source* to *all* and *User* to *Finance*.
   d. Set *Destination* 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*.



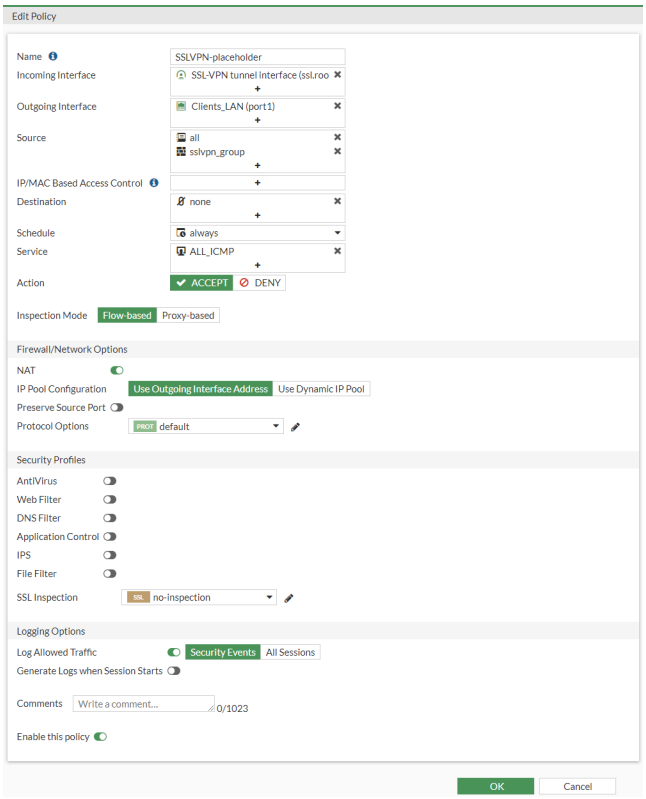
3. Create a policy named *SSLVPN-Sales*.
   a. Set *Incoming Interface* to *Agentless VPN tunnel interface (ssl.root)*.
   b. Set *Outgoing Interface* to *port2*.
   c. Set *Source* to *all* and *User* to *Sales*.
   d. Set *Destination* to the *Webserver1* address object. If needed, create this object with the IP address of `10.88.0.3/32`.
   e. Set *Service* to *ALL*.
   f. Configure other settings as needed.

g. Click *OK*.



4. Create a placeholder policy named *SSLVPN-placeholder*.
   a. Set *Incoming Interface* to *Agentless 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*.



FortiClient configurations

In Agentless VPN tunnel mode, the FortiClient will initiate the connection. Below are two ways of configuring the Agentless VPN connection profile.

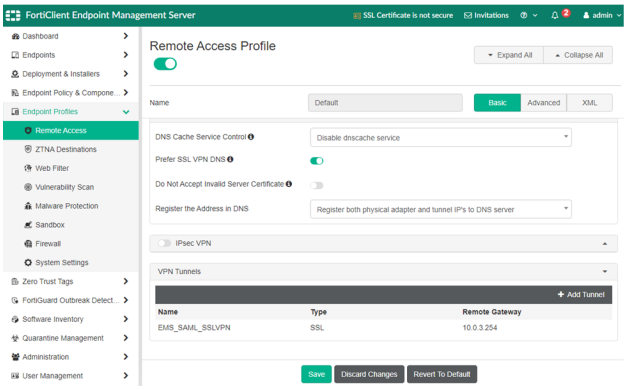
To configure an Agentless VPN remote access profile on FortiClient:

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 *Agentless 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*.

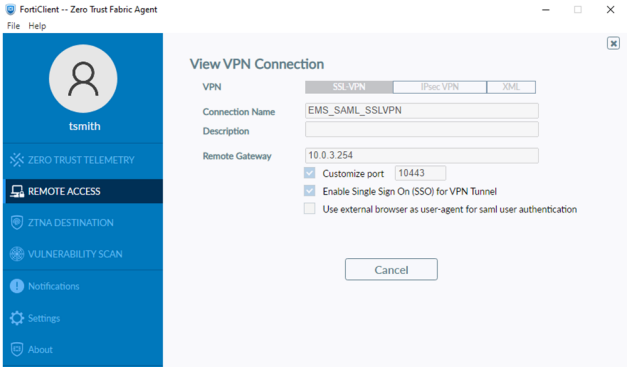
To configure an Agentless VPN remote access profile on FortiClient EMS:

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*.



9. Shortly after, the FortiClient endpoint should receive the newly synced *EMS_SAML_SSLVPN* profile.

10. View the settings on FortiClient.



Testing and verification

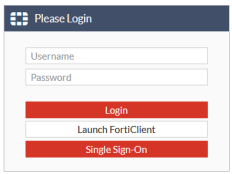
The following demonstrates connection via Web mode and Tunnel mode using SAML authentication. Review the authentication process at the beginning of this deployment scenario to understand how the process works.

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 Agentless VPN web portal.

Web mode Agentless VPN

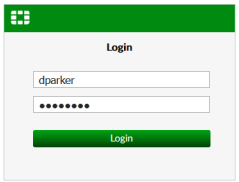
To verify a Web mode Agentless VPN connection with the Finance user Dan Parker (dparker):

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*.

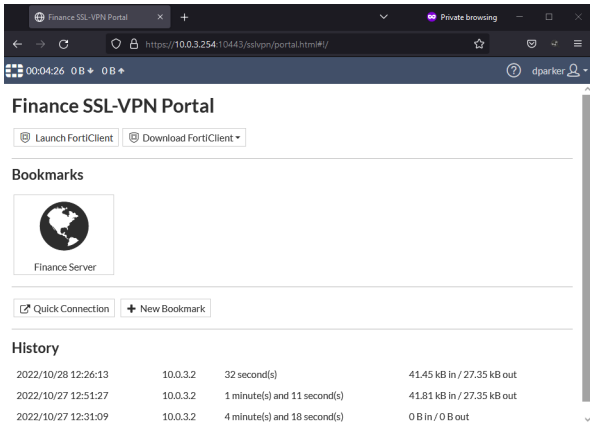


In the background, the FortiAuthenticator authenticates this user over the LDAP connection to the Windows AD. If the authentication succeeds and matches a user group on FortiAuthenticator, FortiAuthenticator sends a SAML

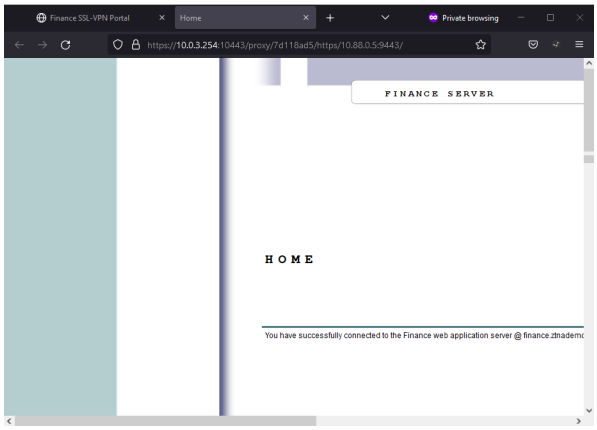
assertion back to the browser containing the username and group information.

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 Agentless VPN Portal.

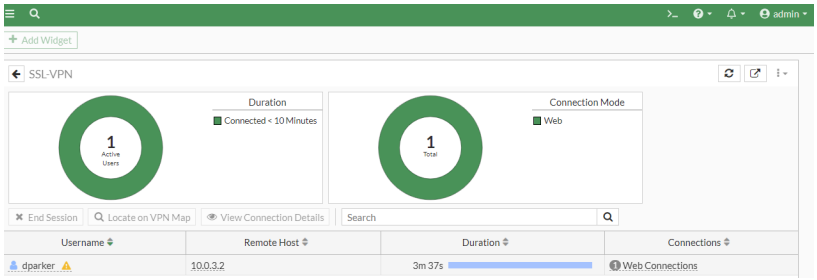


4. Clicking on the Finance Server bookmark, the user can access the Finance server.



To verify the login status on the FortiGate and FortiAuthenticator:

1. On FortiGate, go to *Dashboard* > *Network* and expand the *Agentless VPN* widget.

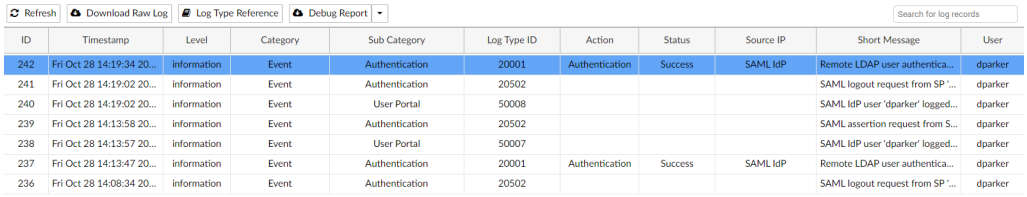


2. From *Log & Report* > *System Events*, switch to *VPN Events* log.
   Alternatively, in the CLI console, enter the following commands:

```
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
```

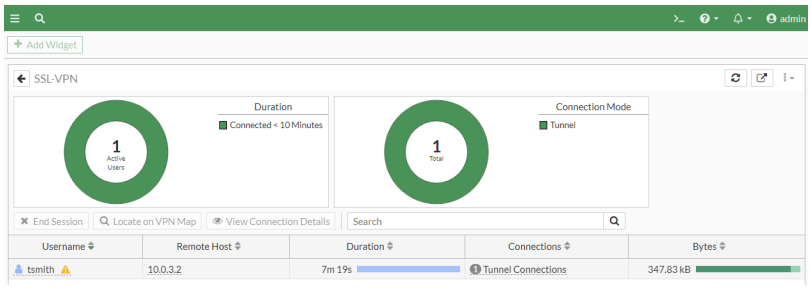
3. On FortiAuthenticator, go to *Logging* > *Log Access* > *Logs*.
   The SAML IdP authentication for dparker will be displayed.



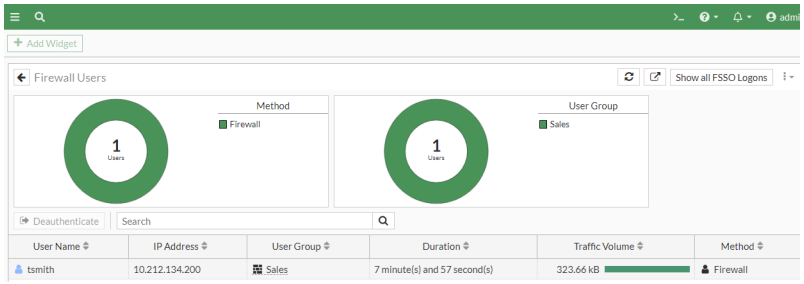
ID	Timestamp	Level	Category	Sub Category	Log Type ID	Action	Status	Source IP	Short Message	User
242	Fri Oct 28 14:19:34 20...	information	Event	Authentication	20001	Authentication	Success	SAML IdP	Remote LDAP user authentica...	dparker
241	Fri Oct 28 14:19:02 20...	information	Event	Authentication	20502				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

To verify the login status on the FortiGate and FortiAuthenticator:

1. On FortiGate, go to *Dashboard* > *Network* and expand the *Agentless VPN* widget.



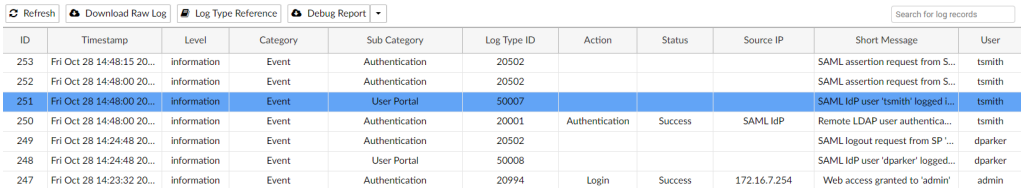
2. Go to *Dashboard* > *User & Devices* and expand the *Firewall Users* widget.



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.


Refresh | Download Raw Log | Log Type Reference | Debug Report | Search for log records

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

FortiGate

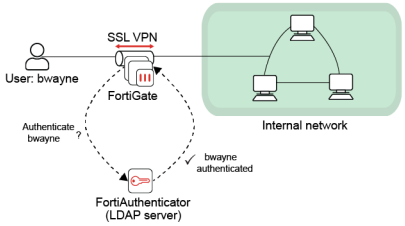
Certificate and SSL inspection

VPN and authentication

Additionally, see Agentless VPN SAML authentication using FortiAuthenticator with OneLogin as SAML IdP on page 249 and Configuring FIDO2 authentication for Agentless VPN on page 96.

LDAP authentication for Agentless VPN with FortiAuthenticator

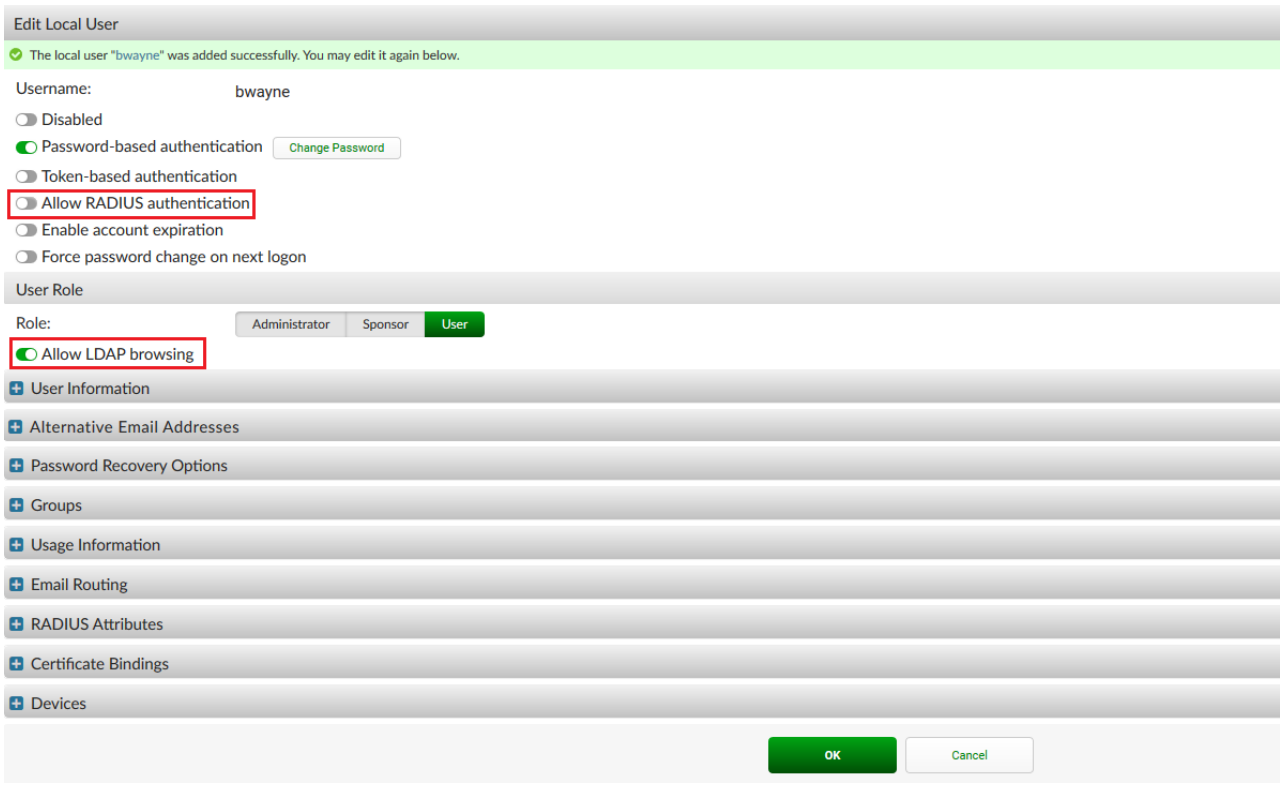
This example describes how to set up FortiAuthenticator to function as an LDAP server for FortiGate Agentless VPN authentication. It involves adding users to FortiAuthenticator, setting up the LDAP server on the FortiAuthenticator, and then configuring the FortiGate to use the FortiAuthenticator as an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



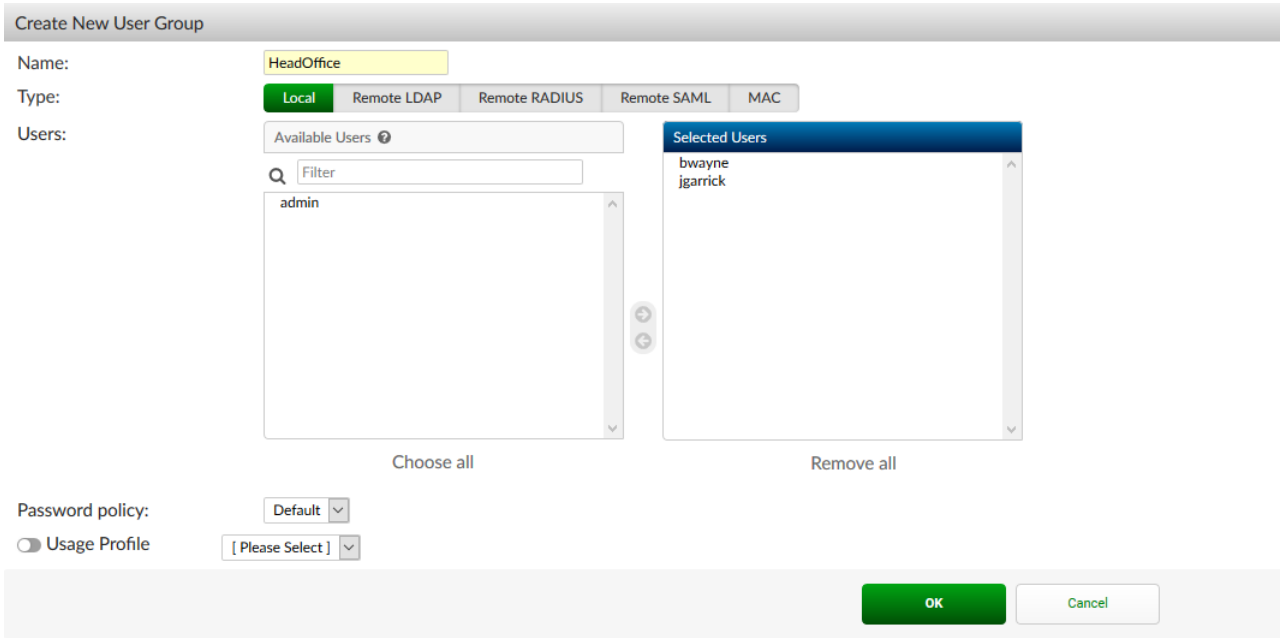
Creating the user and user group on the FortiAuthenticator

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 example.
   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.



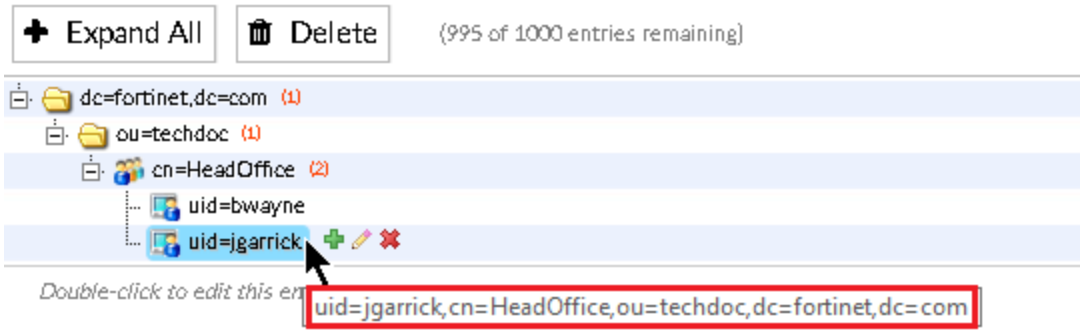
2. Create another user with the same settings. Later, you will use `jgarrick` on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use `bwayne` credentials to connect to the VPN tunnel.
3. Next go to *Authentication > User Management > User Groups*, and create a user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



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.

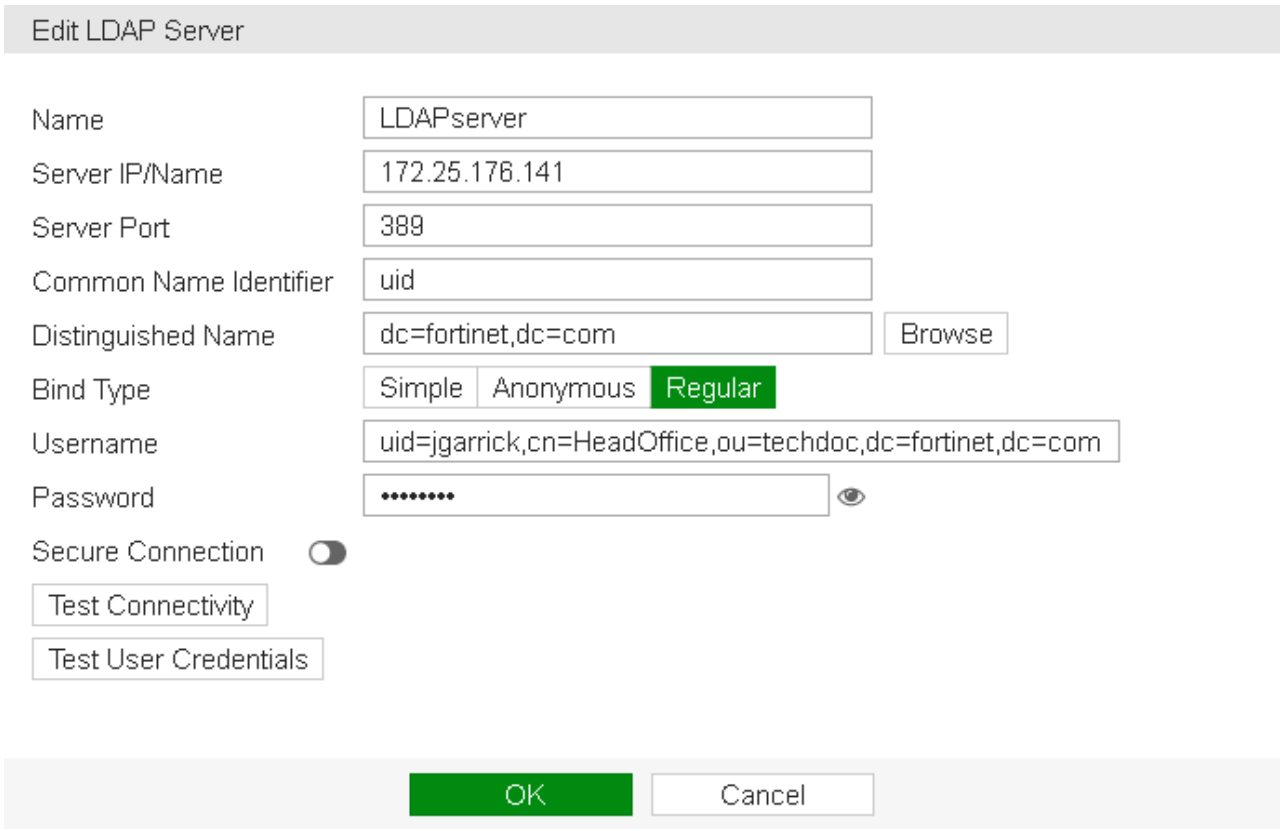


   Later, you will use `jgarrick` on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use `bwayne` credentials to connect to the VPN tunnel.

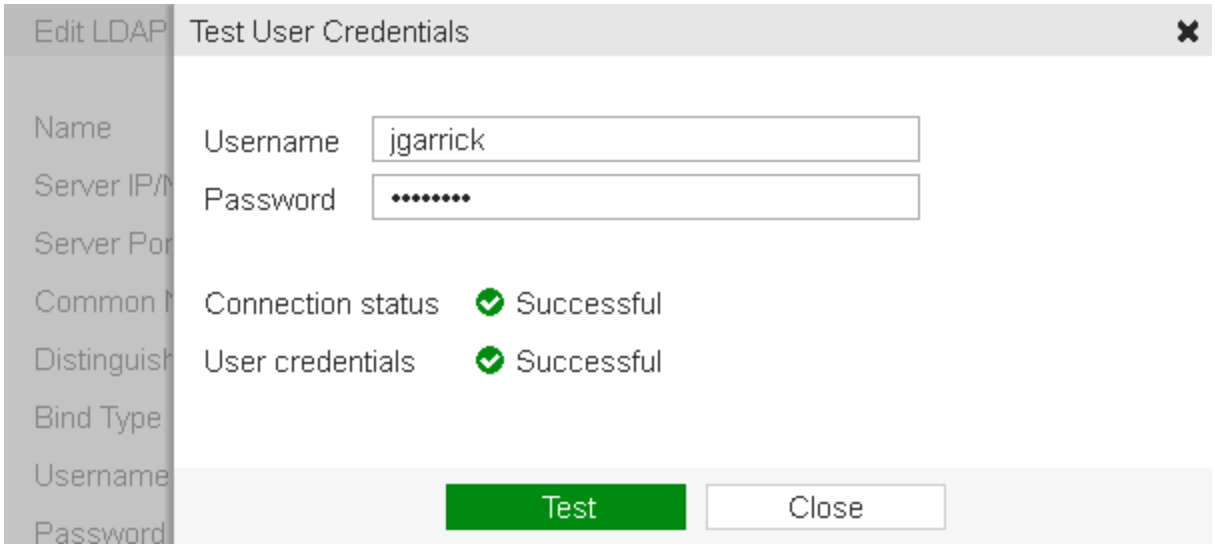
Connecting the FortiGate to the LDAP server

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.



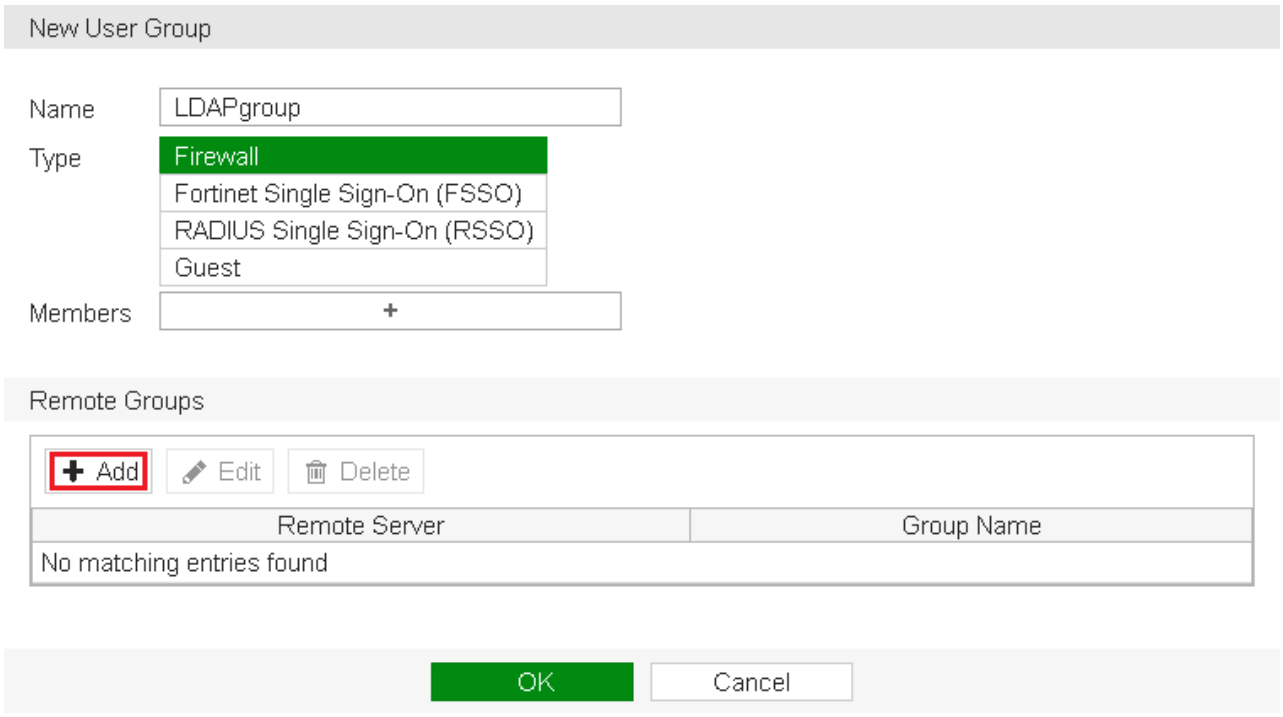
2. Select *Test Connectivity* to determine a successful connection.
Then select *Test User Credentials* to query the LDAP directory using jgarrick's credentials. The query is successful.



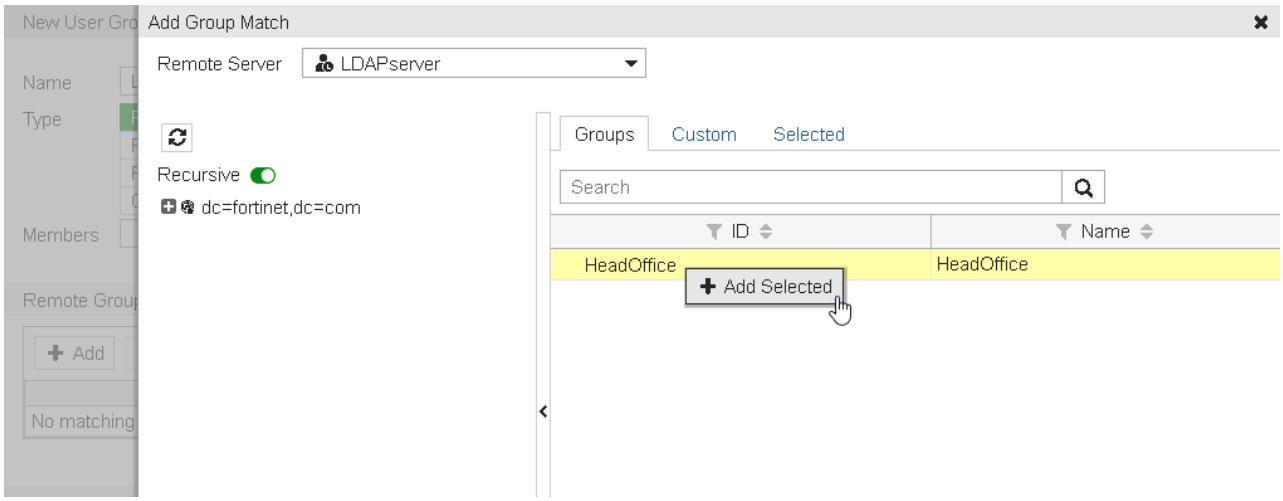
Creating the LDAP user group on the FortiGate

To create the LDAP user group:

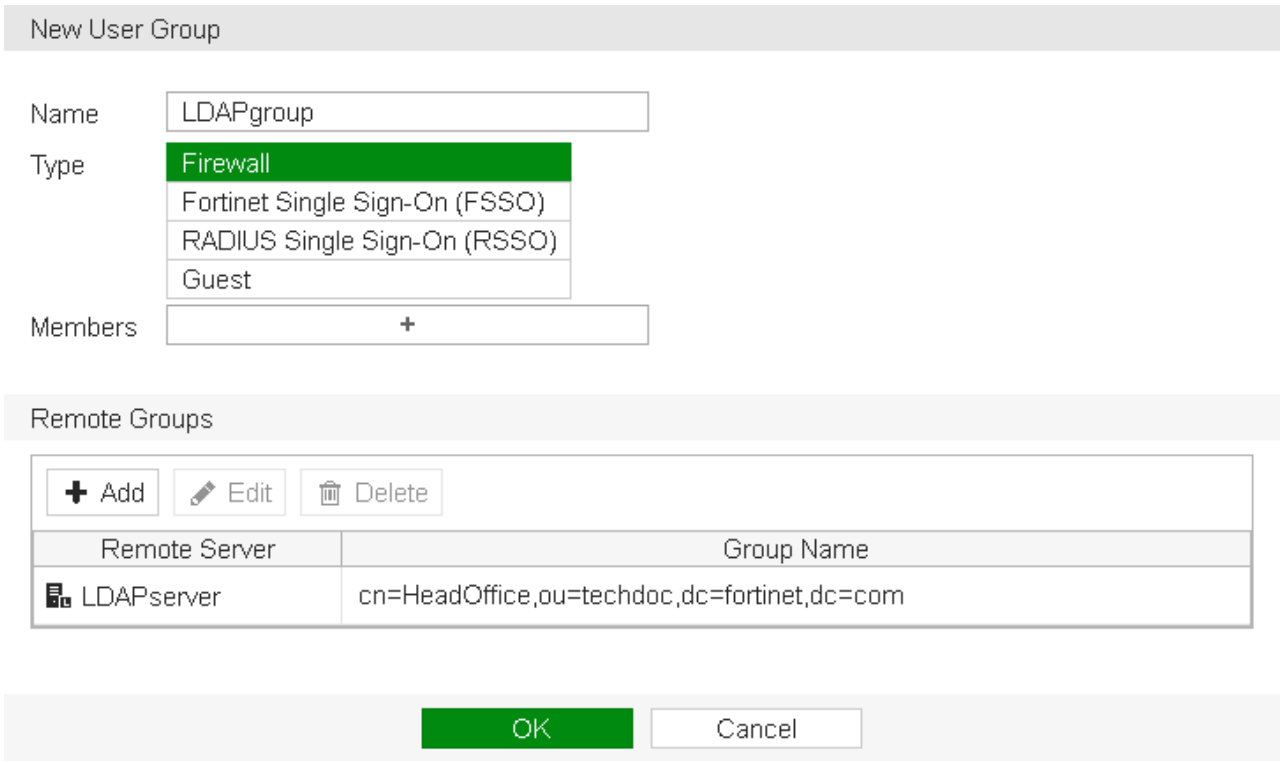
1. Go to *User & Device > User Groups*, and select *Create New*.
   Enter a name for the user group. Under *Remote Groups* select *Add*.



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*.



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



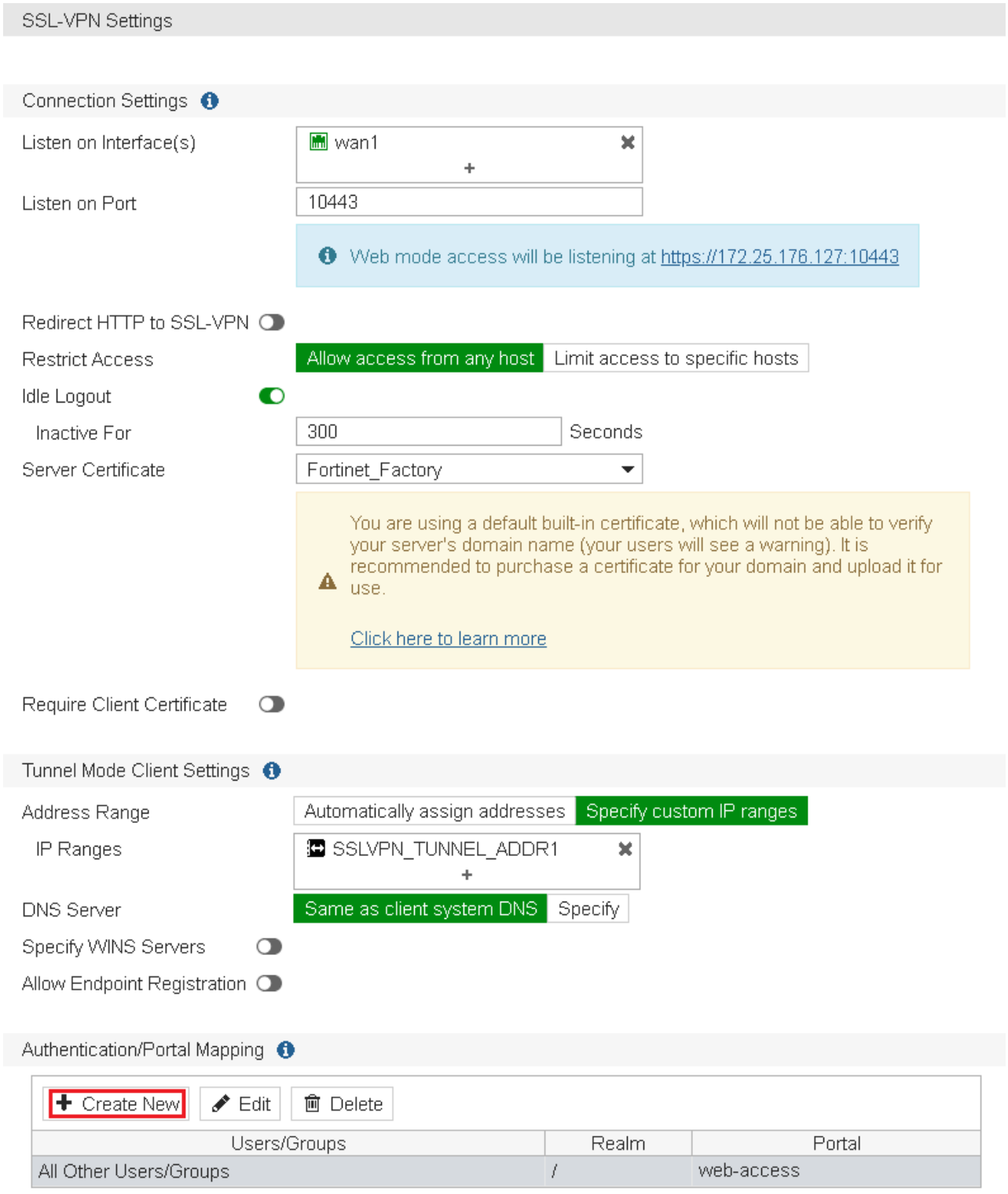
Configuring the Agentless VPN

To configure the Agentless VPN:

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

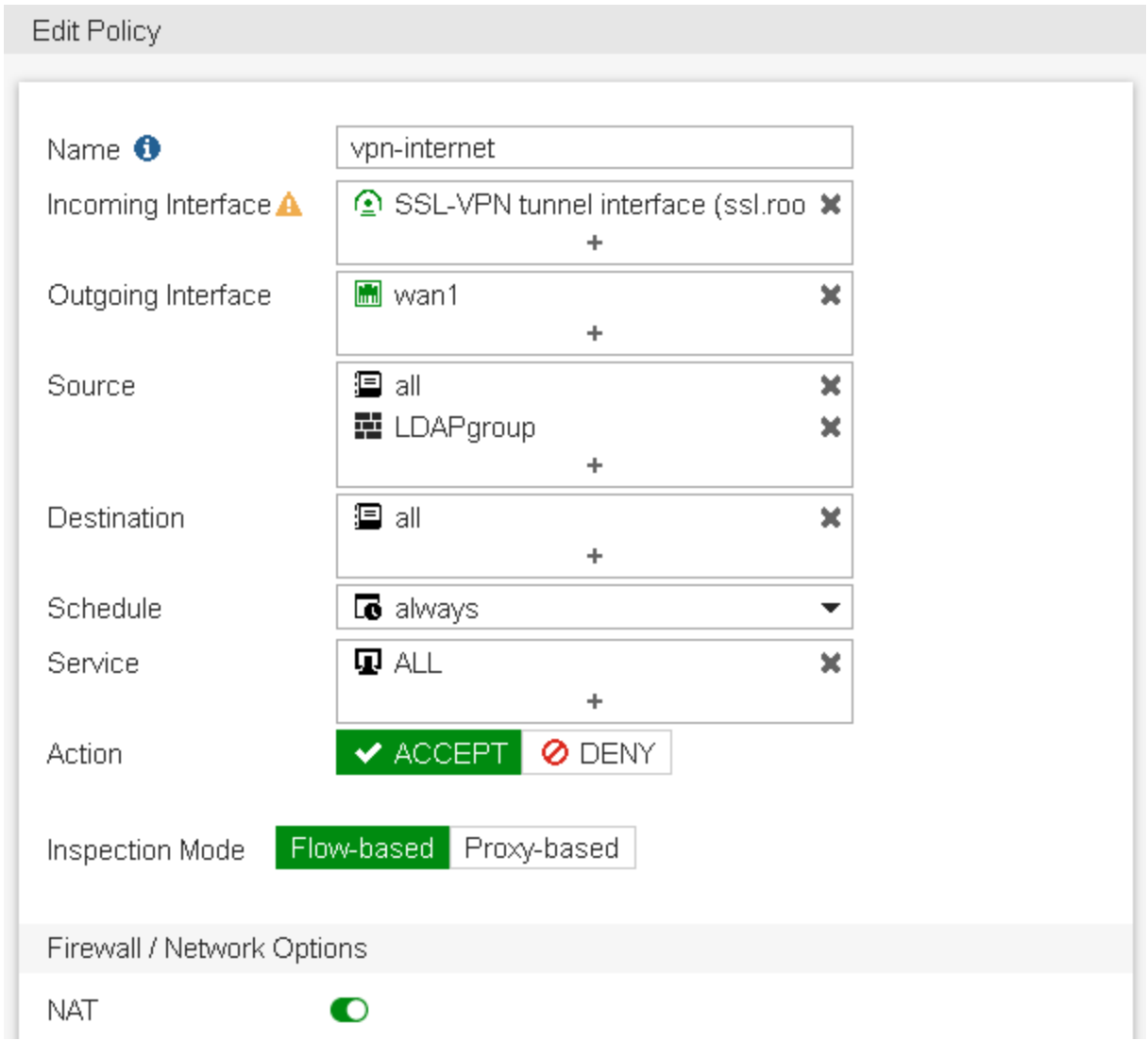
2. Go to *VPN > Agentless VPN Settings*.
   Under *Connection Settings* set *Listen on Port* to `10443`.

Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set it to *SSLVPN_TUNNEL_ADDR1*.
Under *Authentication/Portal Mapping*, select *Create New*.



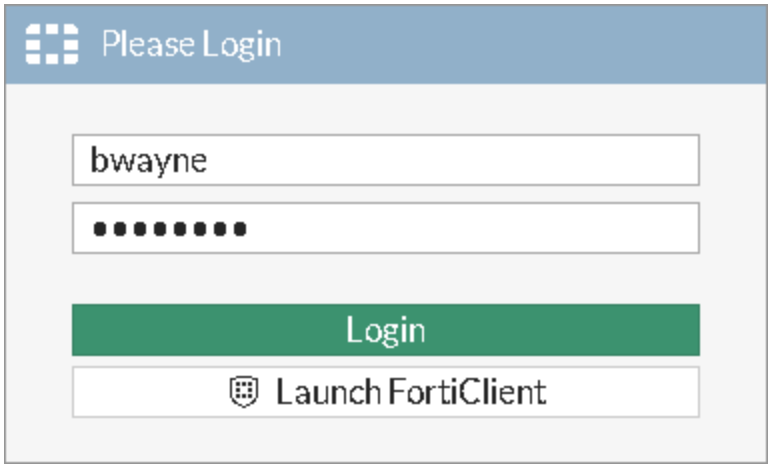
3. Assign the *LDAPgroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to the desired portal. Select *Apply*.

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

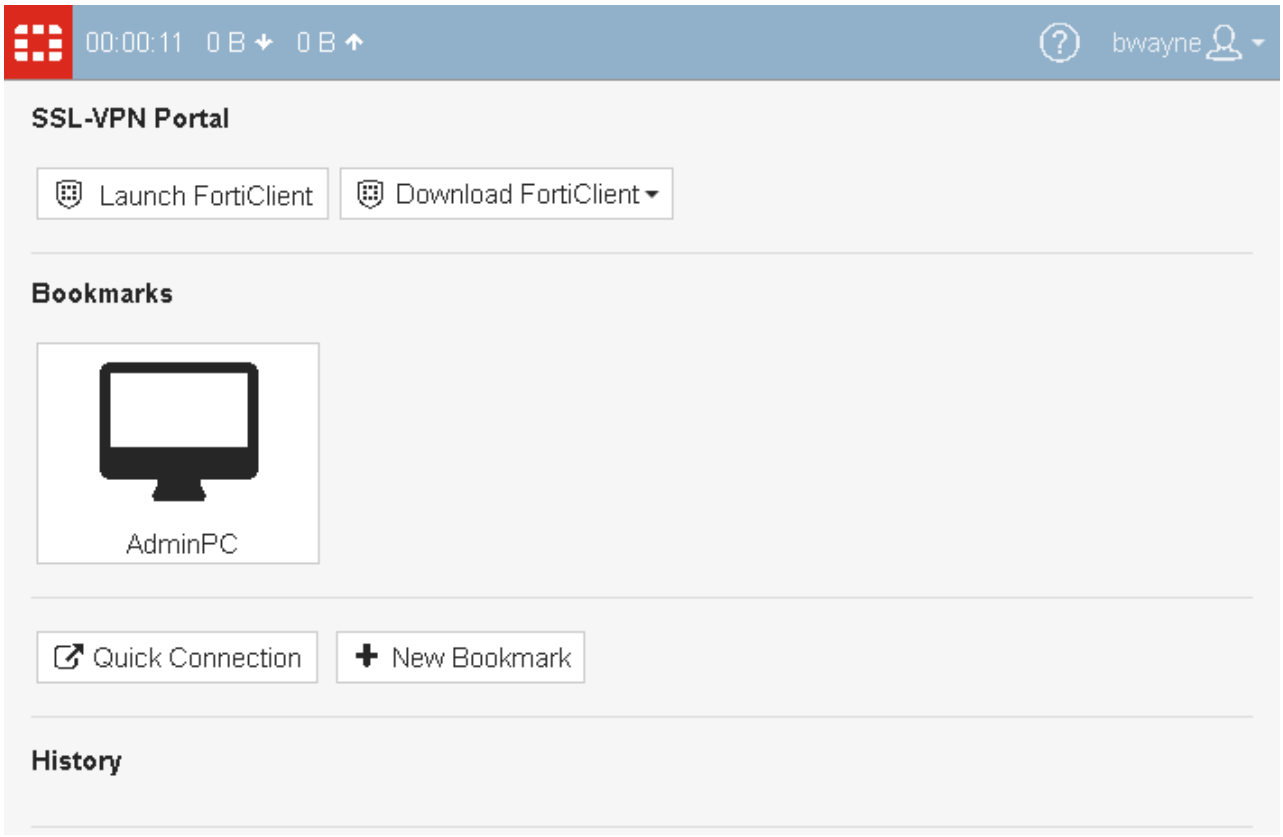


Results

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



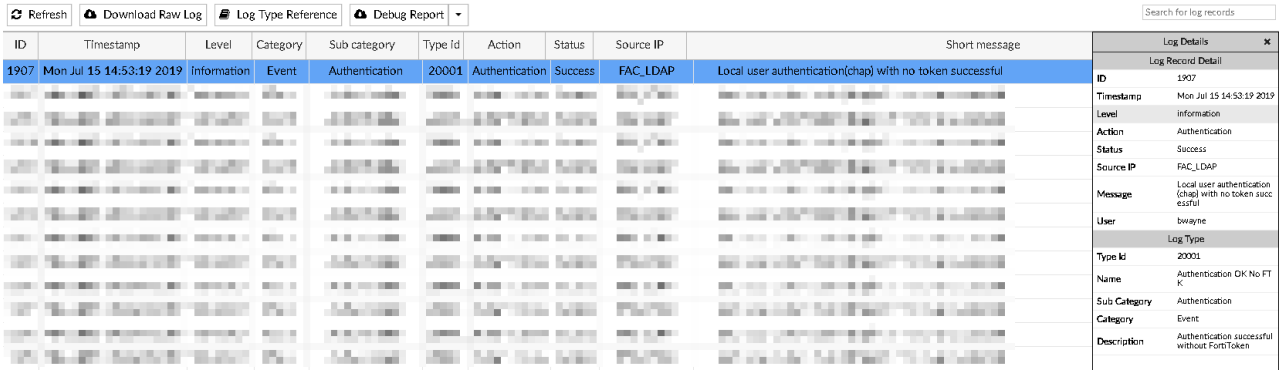
2. The user is now successfully logged into the Agentless VPN Portal.



3. On the FortiGate, go to *Monitor* > *Agentless 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.

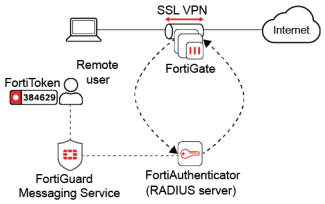


SMS two-factor authentication for Agentless VPN

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

When a user attempts to connect to this Agentless 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.

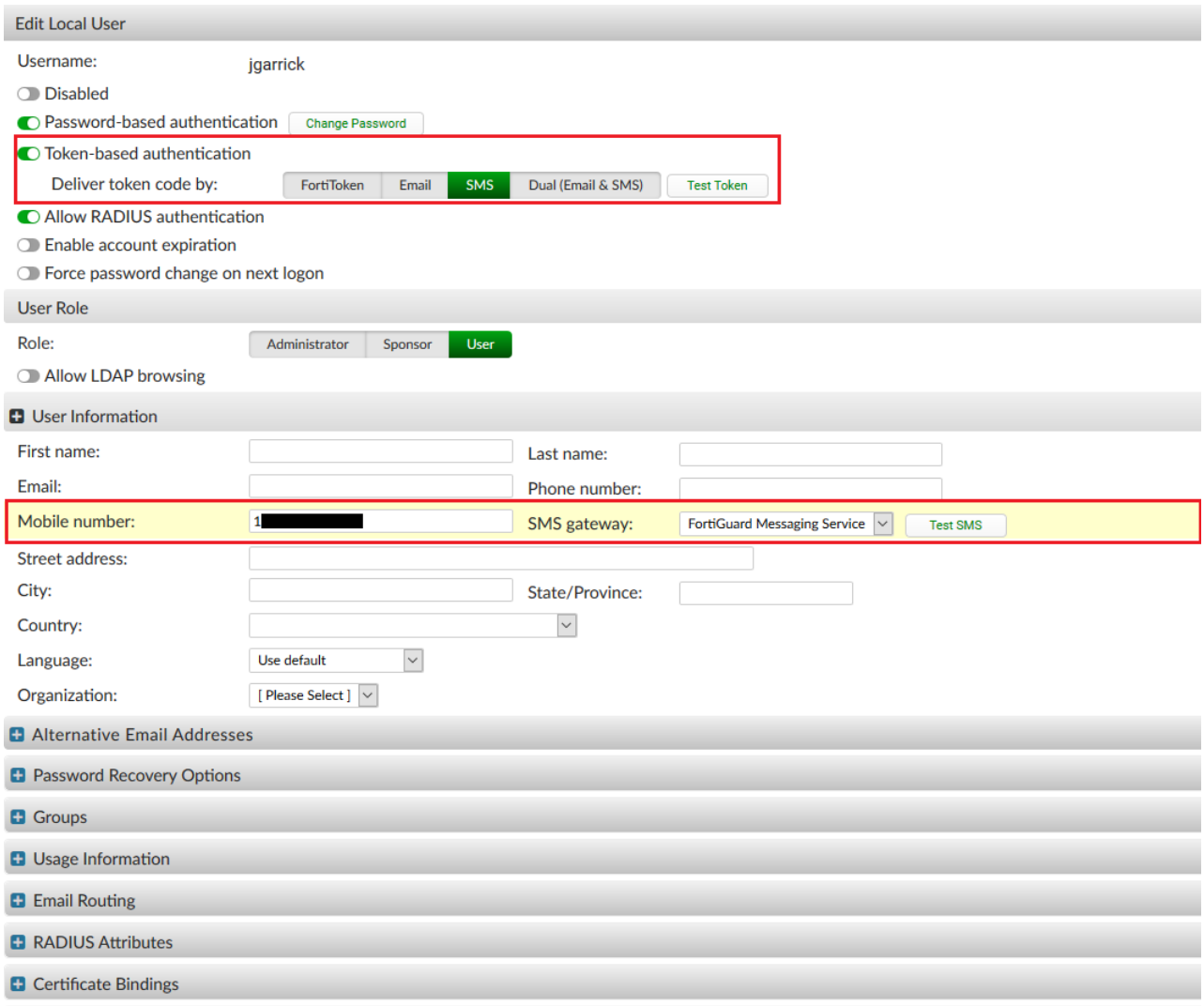
Although this example uses the FortiGuard Messaging Service, it will also work with any compatible SMS service you configure as an SMS Gateway.



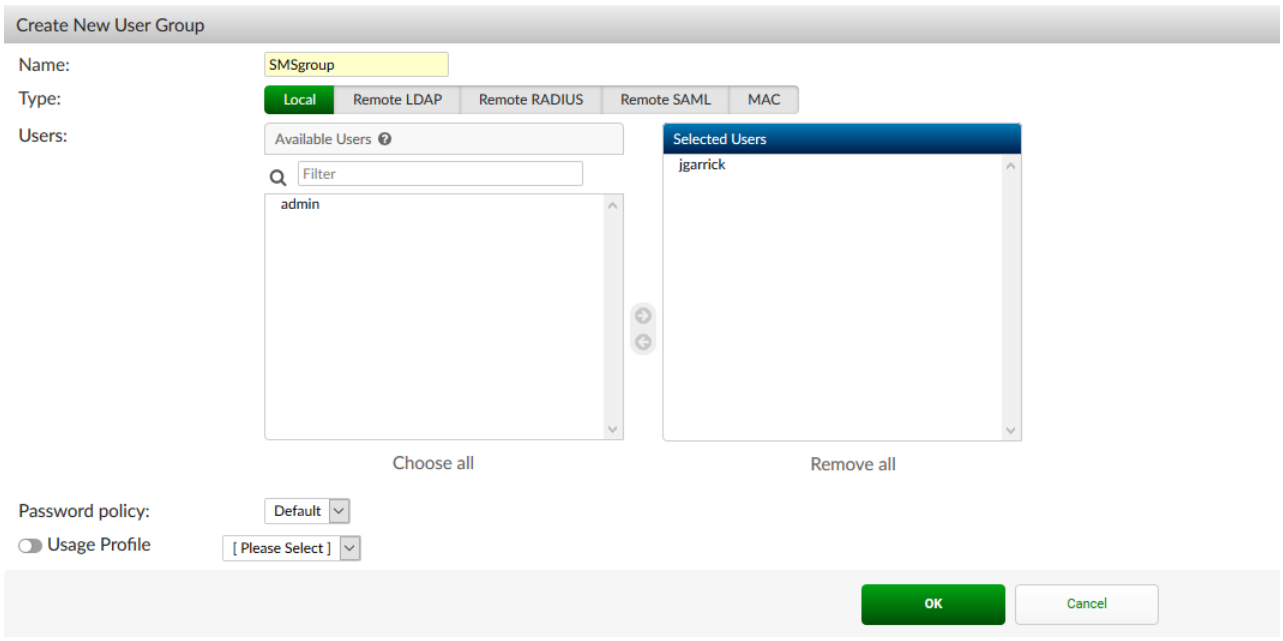
Creating an SMS user and user group on the FortiAuthenticator

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*.



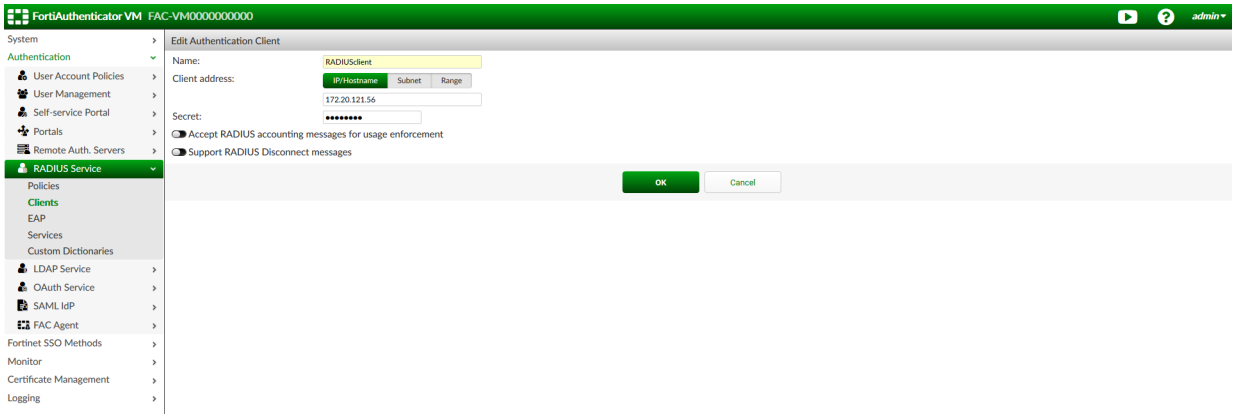
2. Go to *Authentication > User Management > User Groups* and add the above user to a new SMS user group (in the example, *SMSgroup*).



Configuring the FortiAuthenticator RADIUS client

To create the RADIUS client:

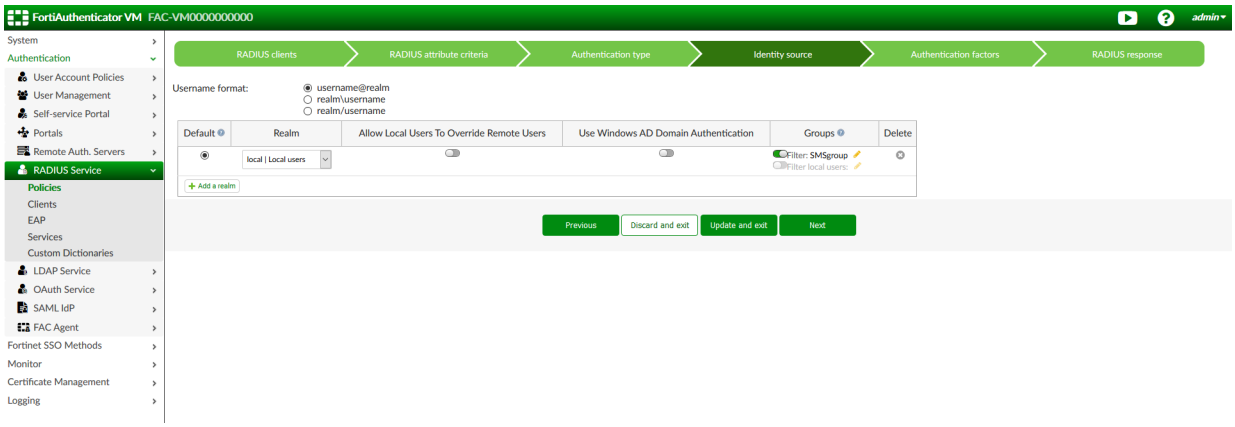
1. On the FortiAuthenticator, go to *Authentication > RADIUS Service > Clients*, and select *Create New*.
2. Enter a *Name*, the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.
3. Click *OK*.



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.

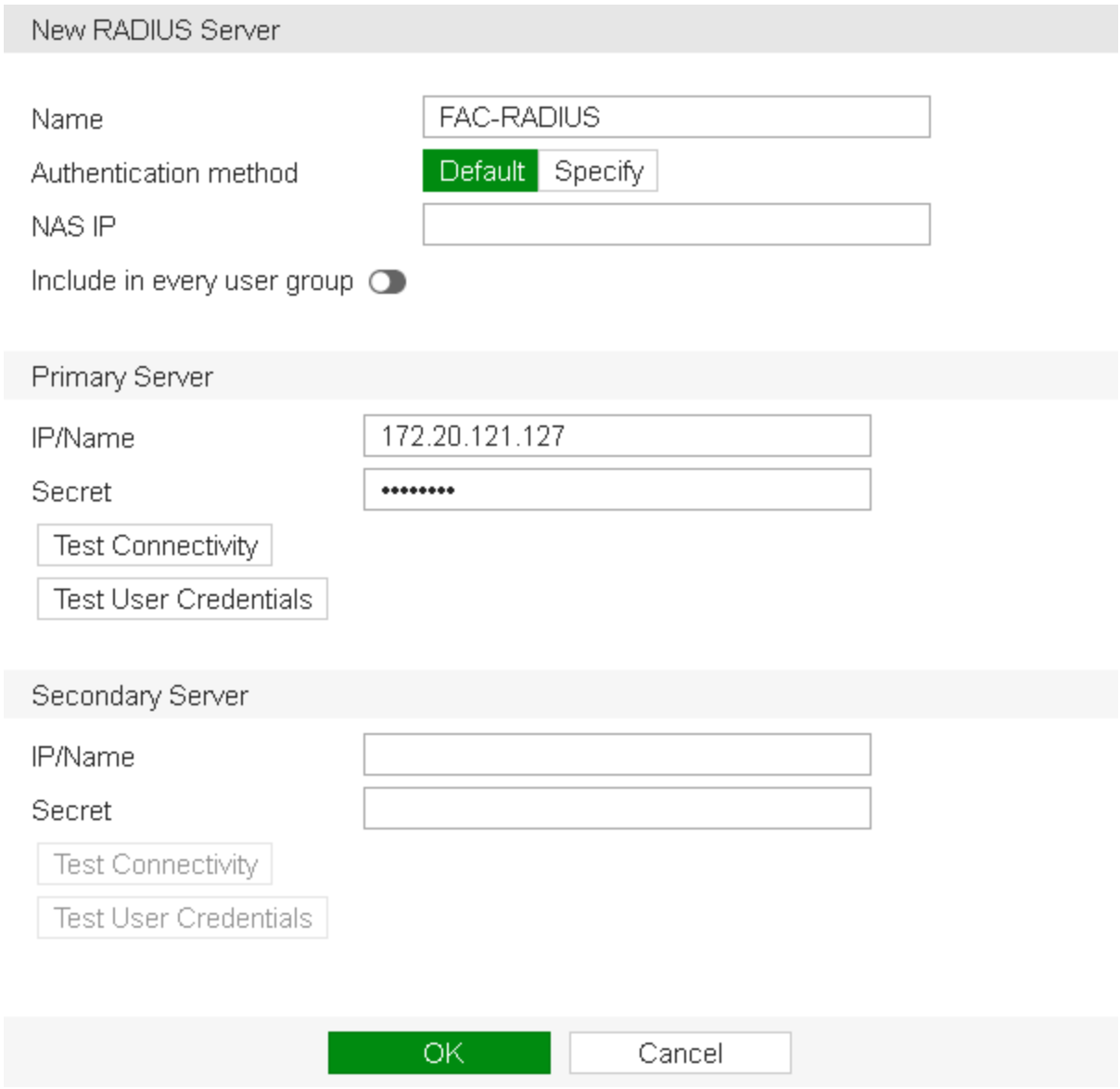


6. Set the authentication method to *Mandatory two-factor authentication*.
7. Click *Save and Exit*.

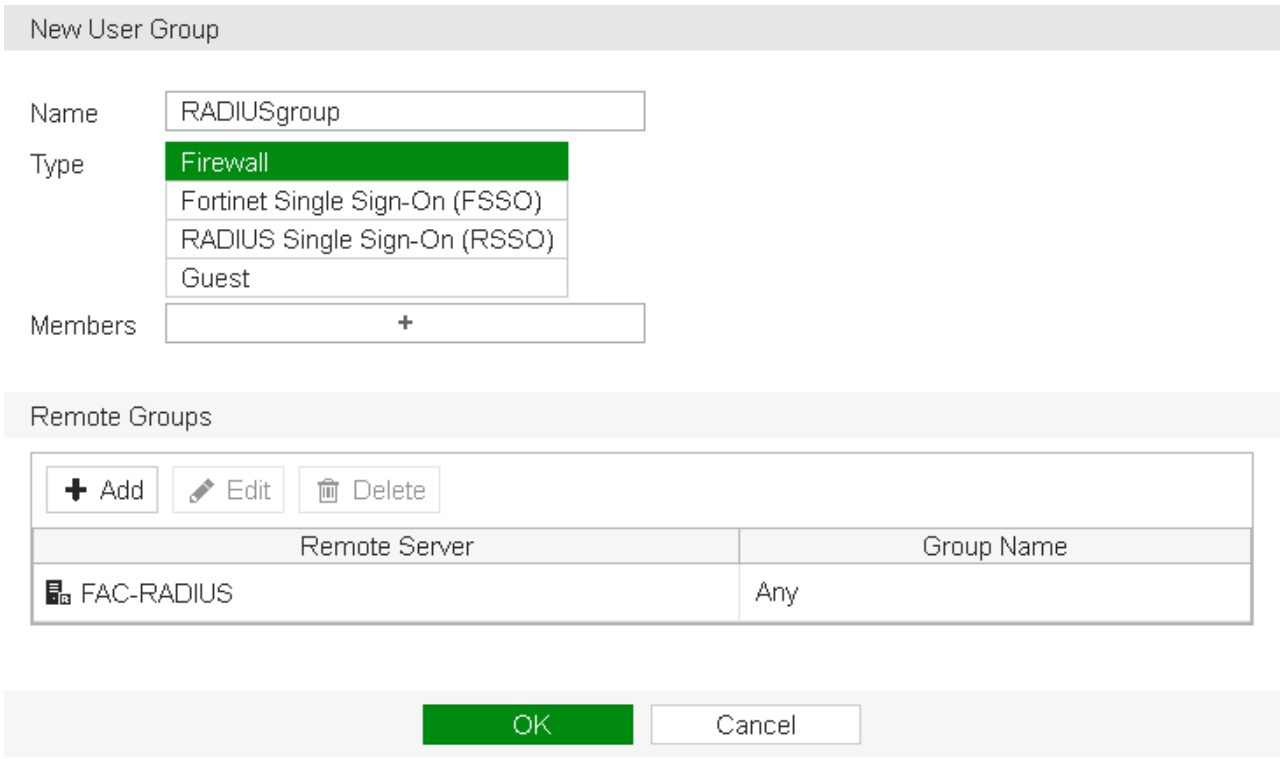
Configuring the FortiGate authentication settings

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.



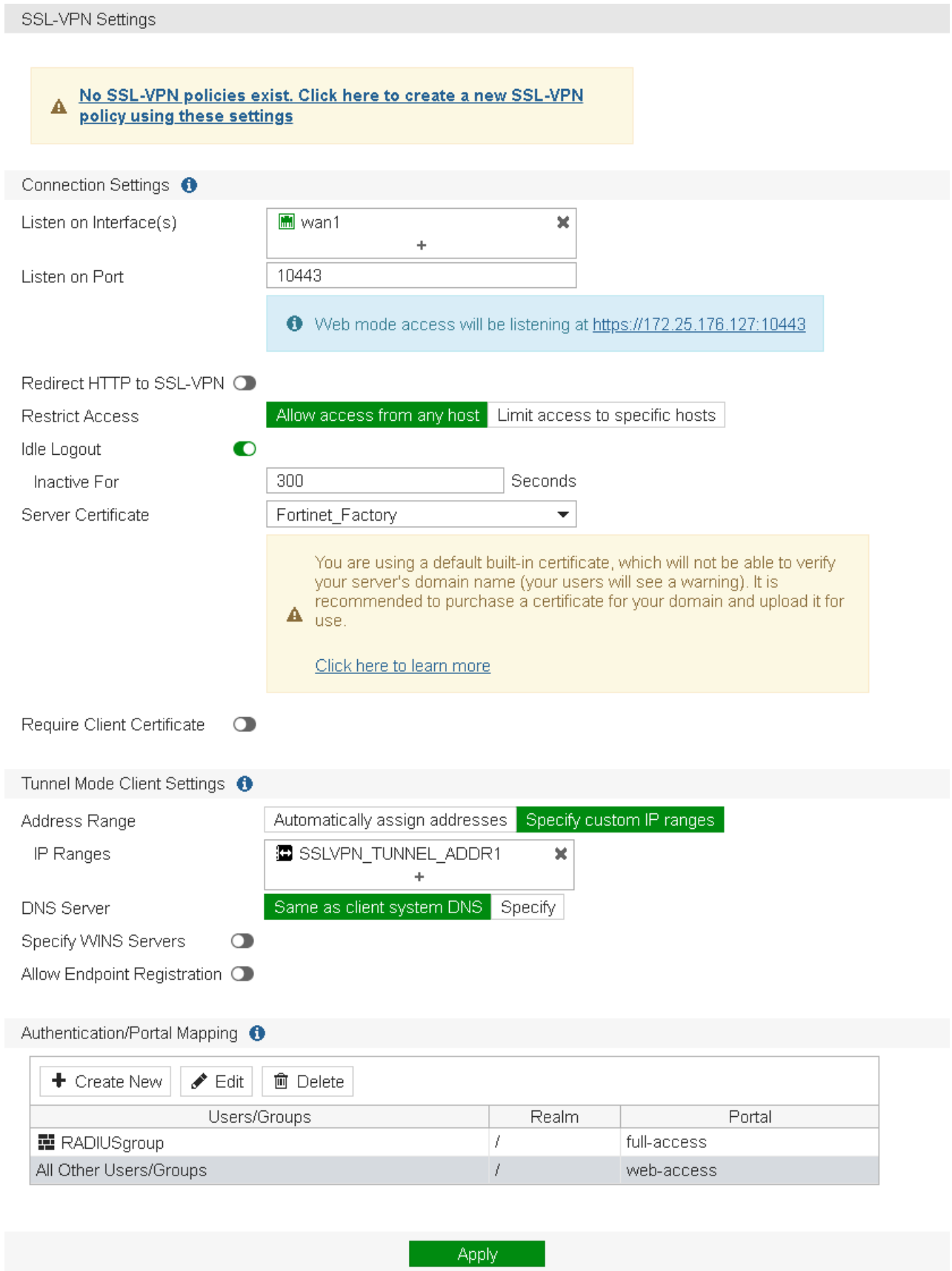
2. Next, go to *User & Device > User Groups* and create a RADIUS user group called *RADIUSgroup*. Set the *Type* to *Firewall* and add the RADIUS server to the *Remote groups* table.



Configuring the Agentless VPN

Configure the Agentless VPN settings:

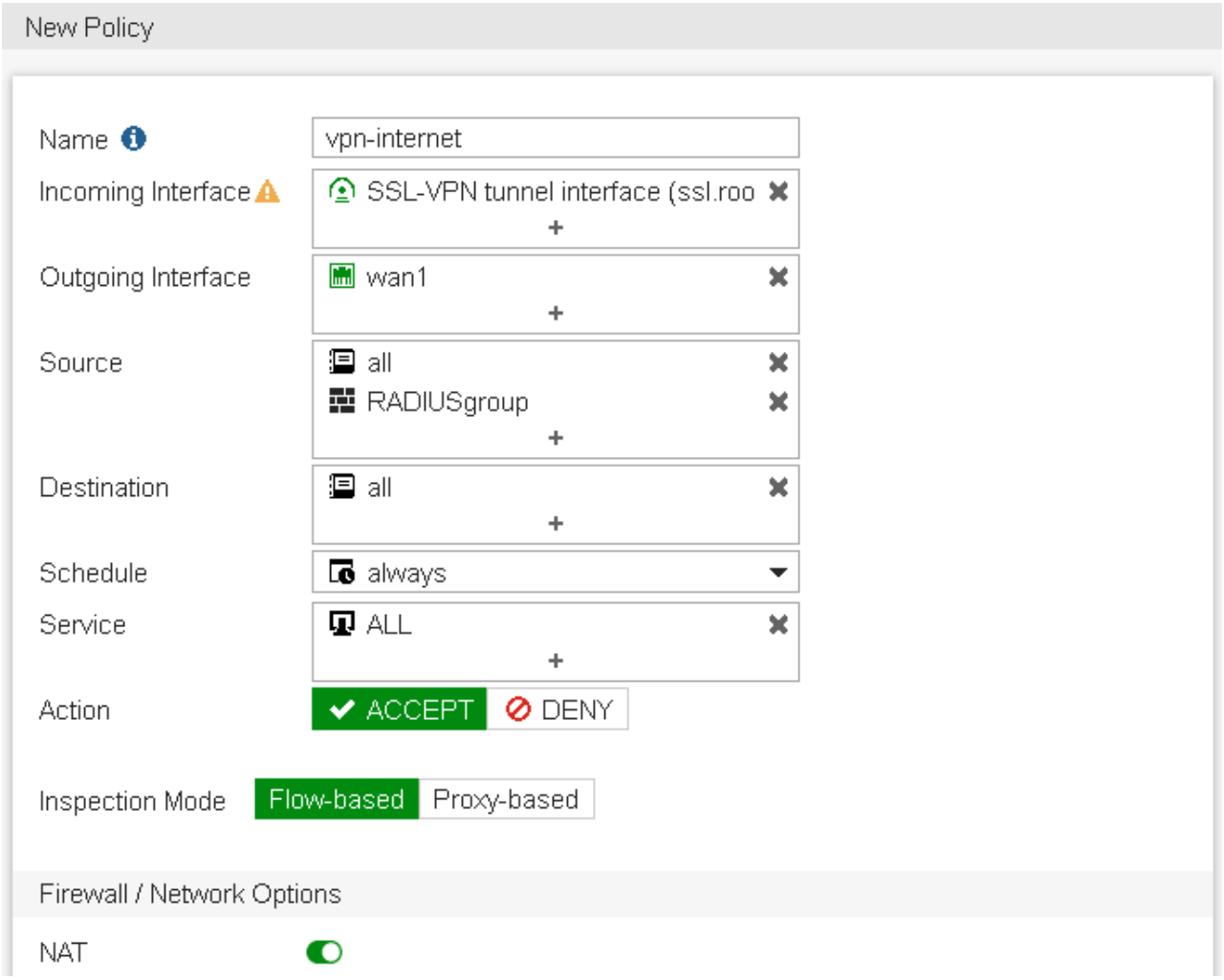
1. Go to *VPN > Agentless VPN Settings*.
   Under *Connection Settings*, set *Listen on Port* to `10443`. Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set *IP Ranges* to the Agentless VPN tunnel address range.
   Under *Authentication/Portal Mapping*, select *Create New*.
   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
Create New
Edit
Delete
Users/Groups
Realm
Portal
RADIUSgroup
/
full-access
All Other Users/Groups
/
web-access
Apply

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 Agentless VPN policy, including the *RADIUSgroup*, as shown.

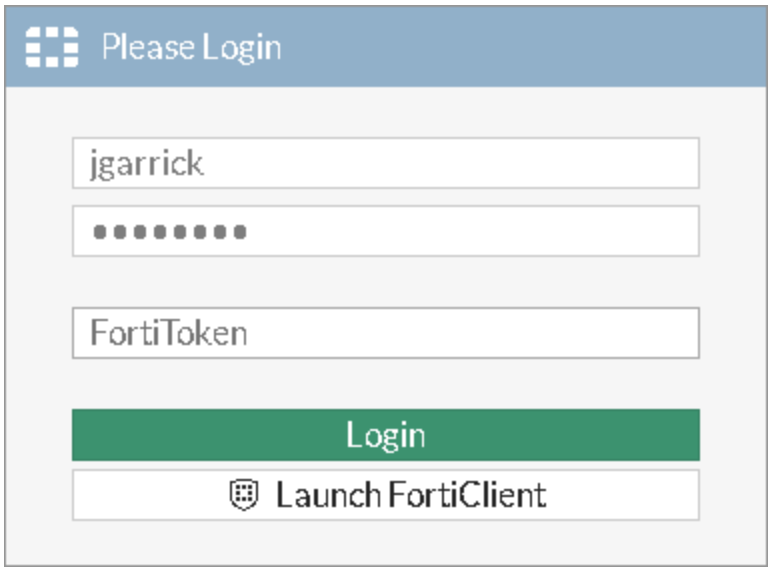


Results

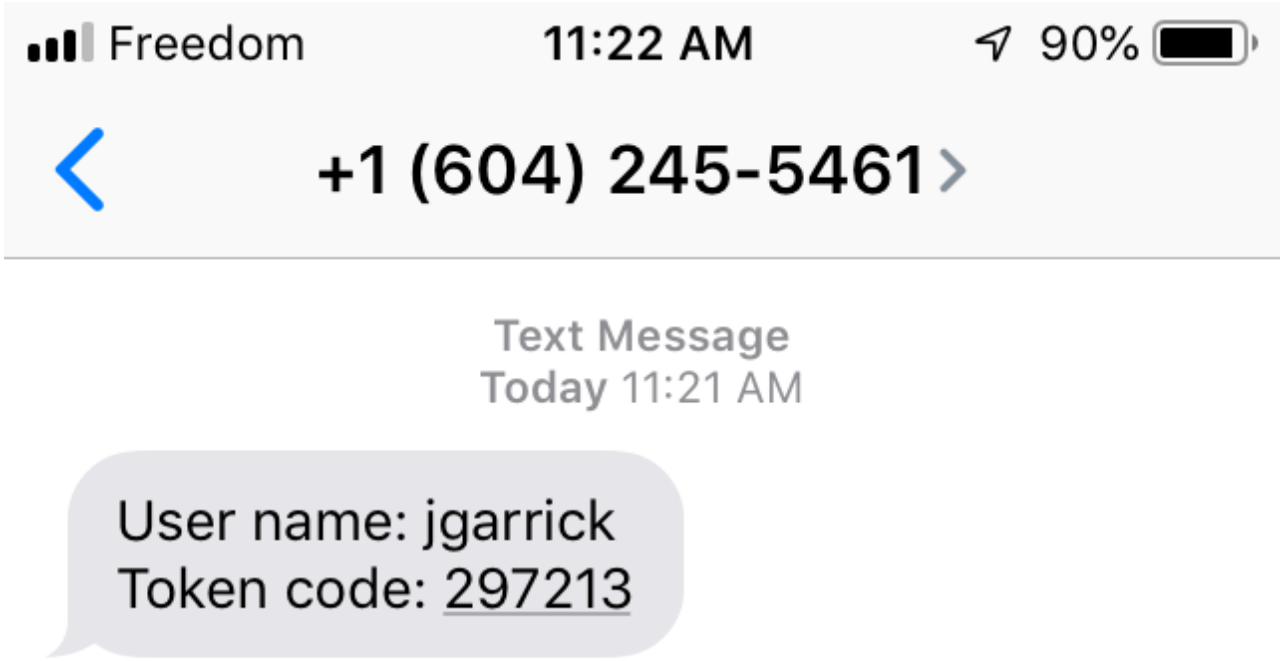
In this example, we will use the web portal to access the Agentless VPN and test the two-factor authentication.

To test two-factor authentication:

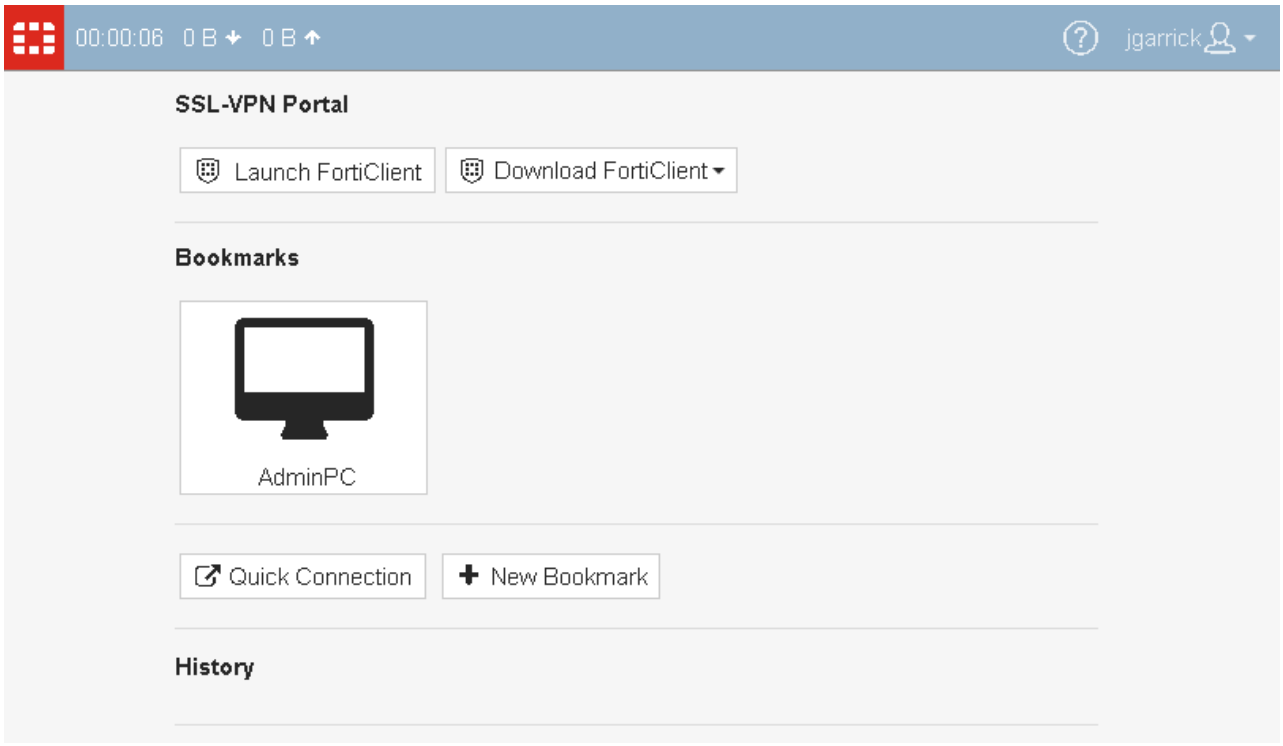
1. Open a browser and navigate to the Agentless VPN web portal, in this case *https://172.25.176.127:10443*. Enter a valid username and password and select *Login*. You should be prompted to enter a *FortiToken Code*.



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 Agentless VPN login portal and select *Login*.

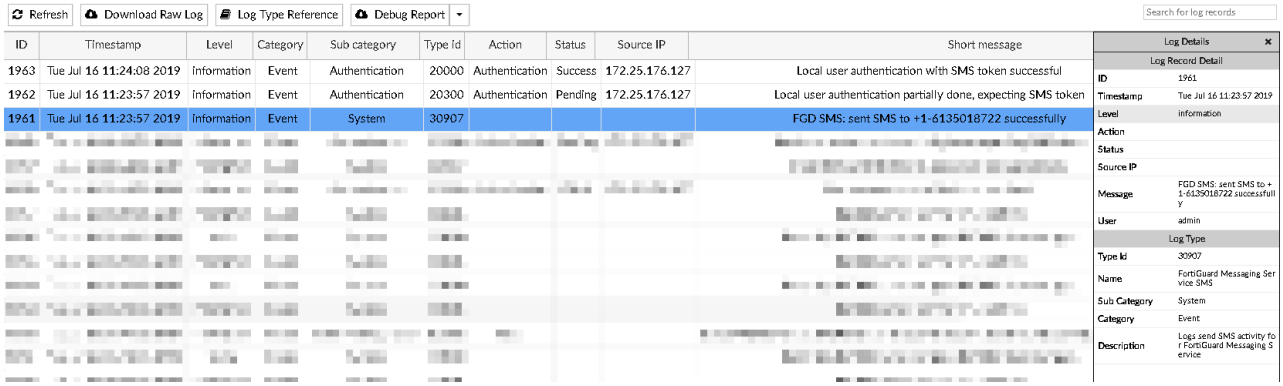

Freedom
11:22 AM
90%
+1 (604) 245-5461
Text Message
Today 11:21 AM
User name: jgarrick
Token code: 297213

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



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

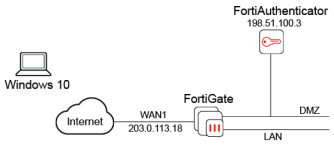
5. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* to confirm the user's connection.



FortiGate Agentless 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 Agentless VPN connection. This allows authentication of Agentless 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:



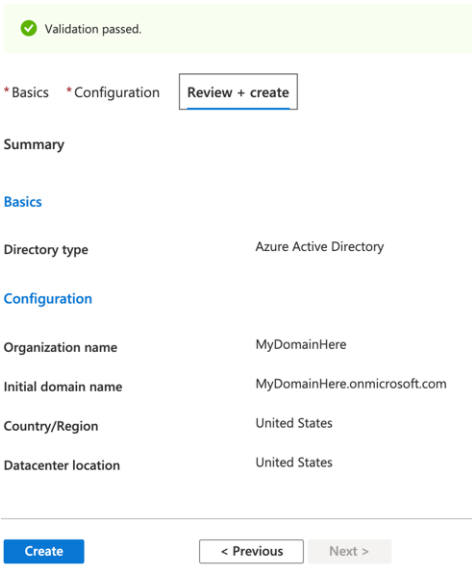
To configure FortiAuthenticator as the IdP proxy for Azure:

1. Configuring Azure on page 309
2. Configuring FortiAuthenticator on page 312
3. Configuring FortiGate on page 318
4. Results on page 320

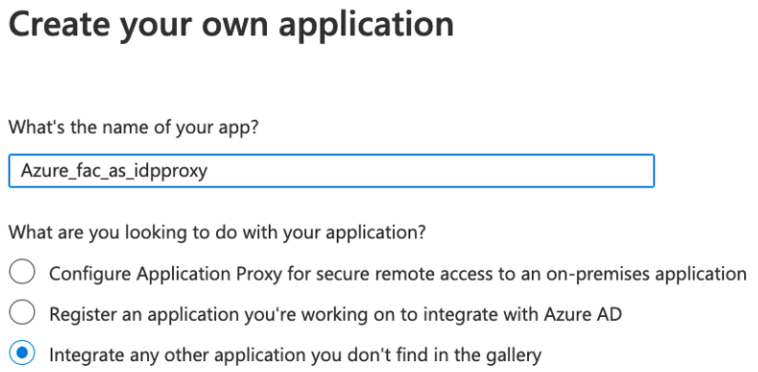
You need Microsoft Entra ID Premium P1 or P2 to perform group-based assignments to an Enterprise App. Microsoft Entra ID Free tier only supports user-based assignments.

Configuring Azure

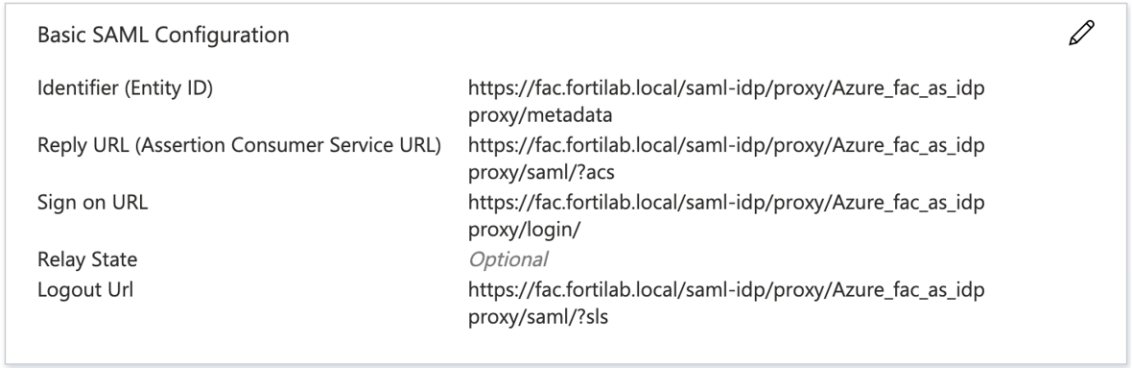
1. Login to the Azure portal. If you do not yet have a directory or need to create a new one, go to *Azure AD* and click *Create a tenant*.
   Configure the directory with the following settings:
   a. **Select a directory type**: *Azure Active Directory*.
   b. **Organization name**: Enter a name for 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.



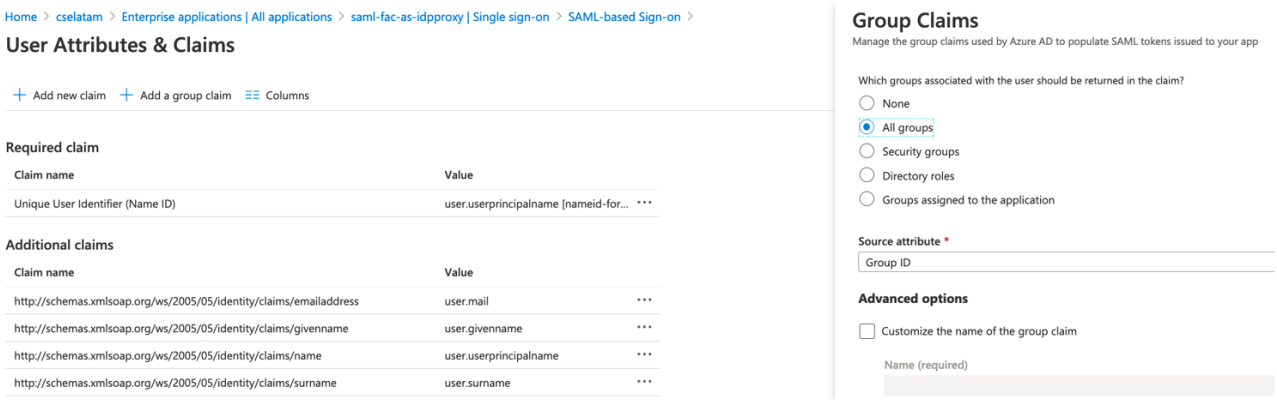
2. Go to *Enterprise Applications*, and select *Create your own application*. Enter a name for your application, for example: `Azure_fac_as_idpproxy`.



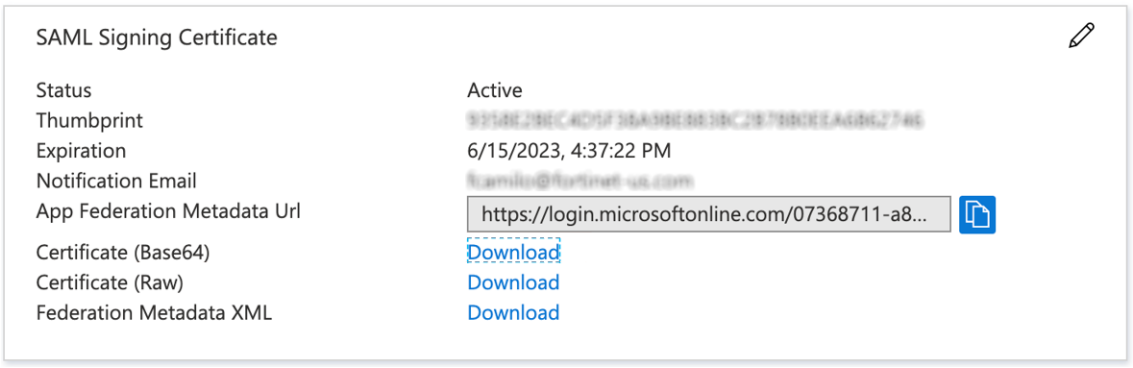
3. Go to the *Single Sign-on* section, select *SAML*, and edit the basic SAML configuration.
Here you will include information obtained from FortiAuthenticator. In this example, the FortiAuthenticator FQDN is *fac.fortilab.local*, and the name of the server is defined as *Azure_fac_as_idpproxy*. You should adjust these settings to match your FortiAuthenticator's configuration.



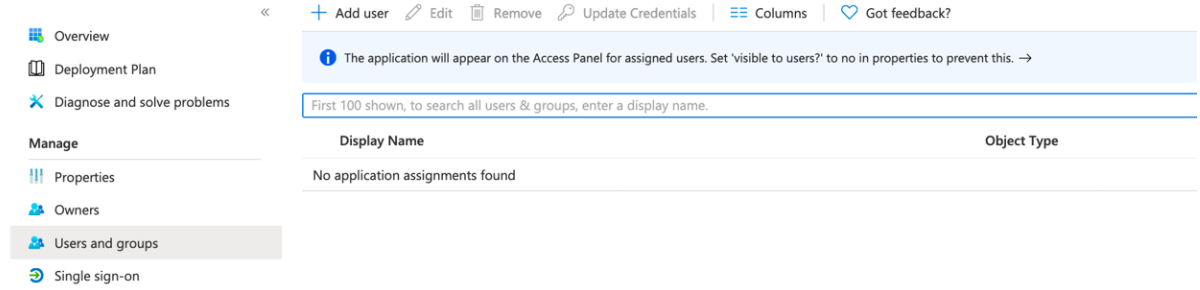
4. Edit the *User Attributes & Claims* section to insert any attributes required for the SAML assertion. In this example, only user groups have been included.
Click the edit icon, and then click *Add a group claim*. Select *All groups*.



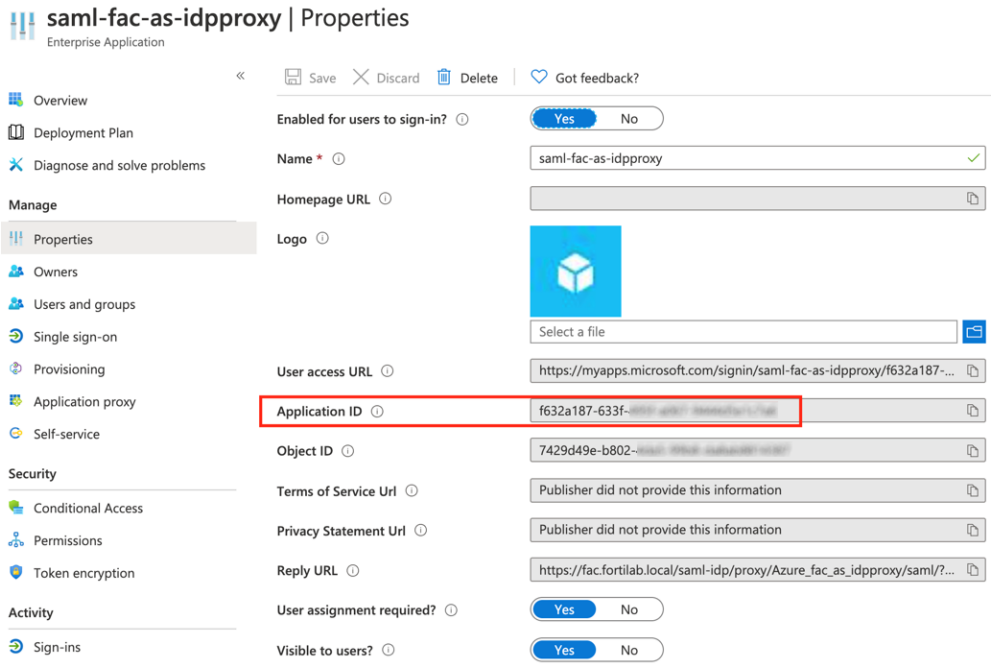
5. Download the certificate file. It will be used later when configuring FortiAuthenticator.



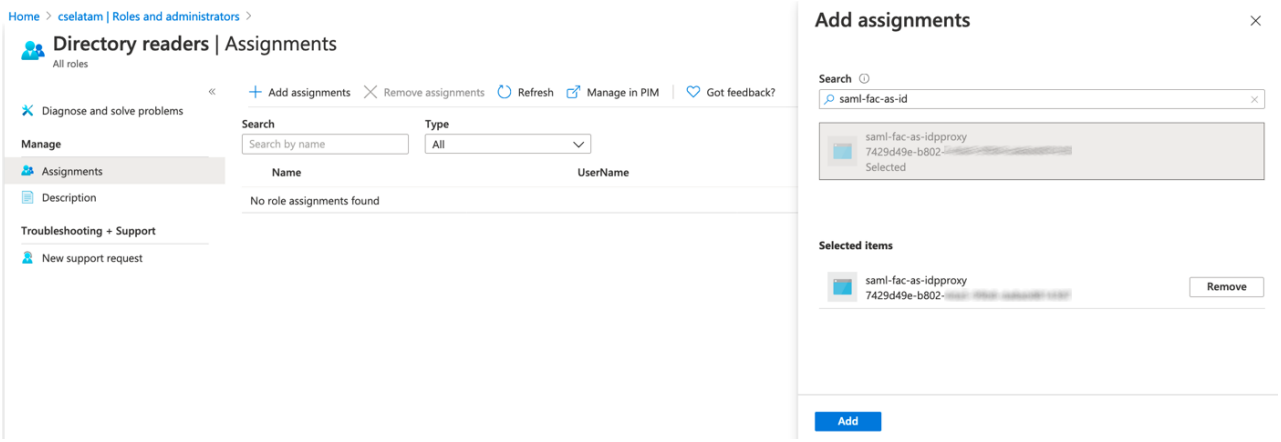
6. Go to *Users and Groups*, and click *Add user*. Include all users that will be able to authenticate using this application.



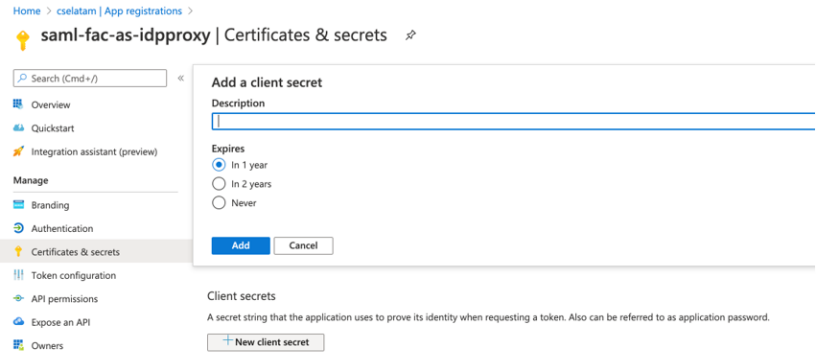
7. Go to *Properties* and get the *Application ID*. This will be required later.



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.



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



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

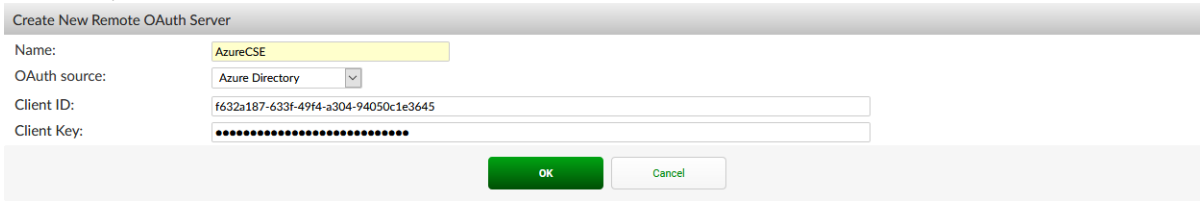
Configure the remote servers

A remote OAuth server is used to obtain group membership from Microsoft Entra ID. 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*.

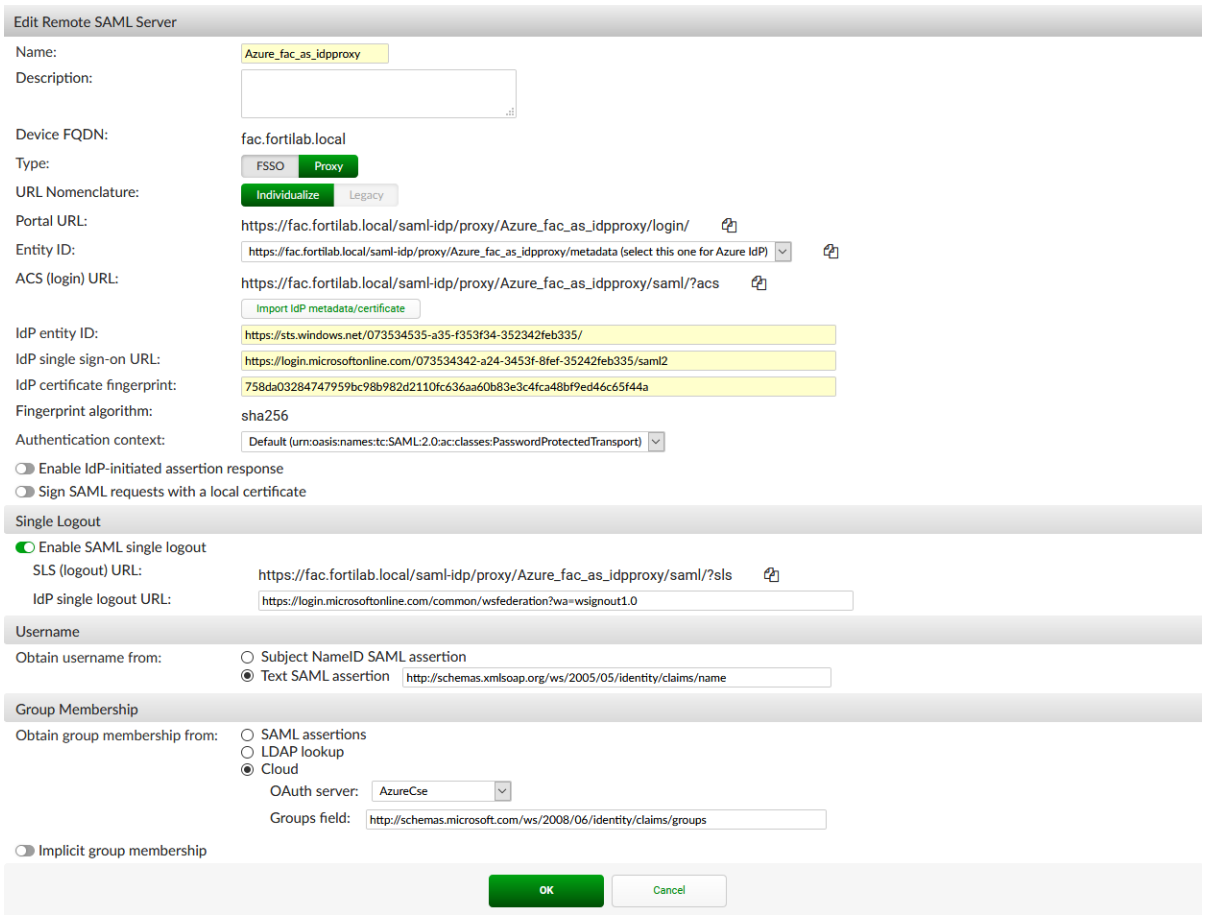
- **Client Key**: Enter your Azure key.



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.

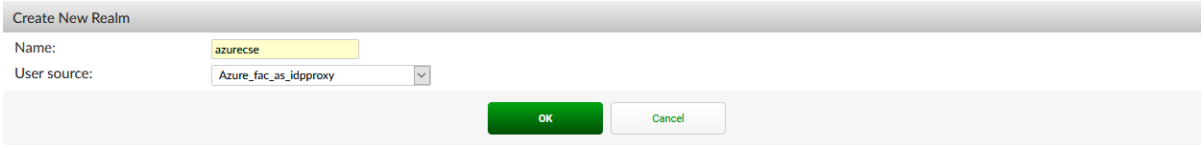


6. Click *OK*.

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.

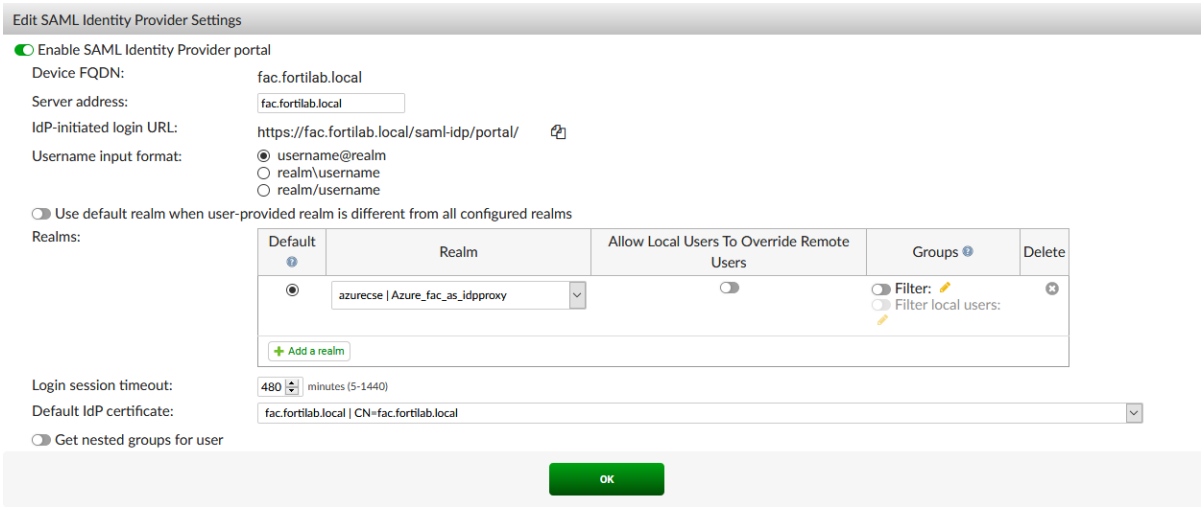


3. Click *OK*.

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.

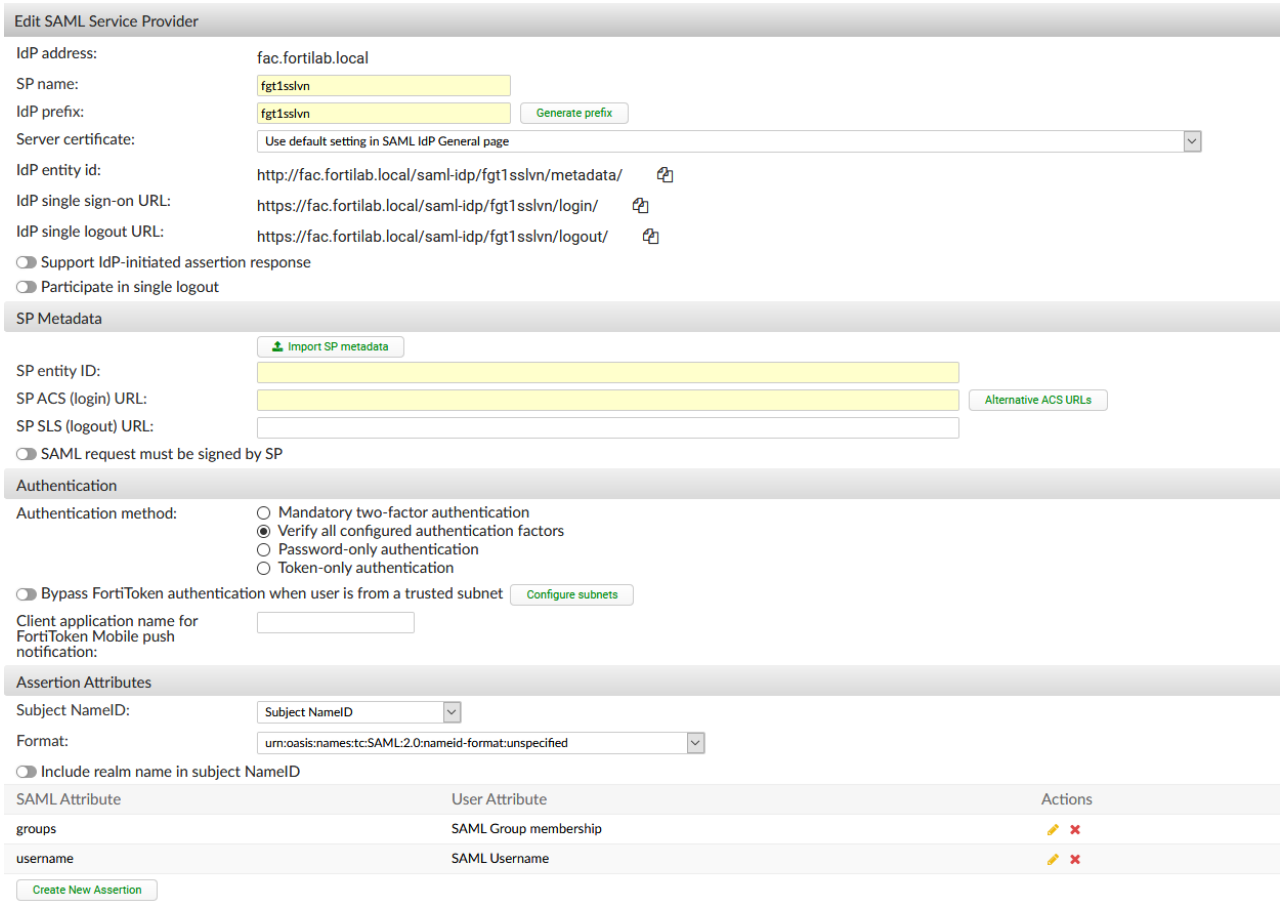


2. Click *OK*.
   You will also need to download your IdP certificate for use later. It can be downloaded from *Certificate Management > End Entities*.

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 318.
   - Attribute 1: SAML attribute: *groups*, User attribute: *SAML Group membership*.
   - Attribute 2: SAML attribute: *username*, User attribute: *SAML Username*.

5. Click *Save*.



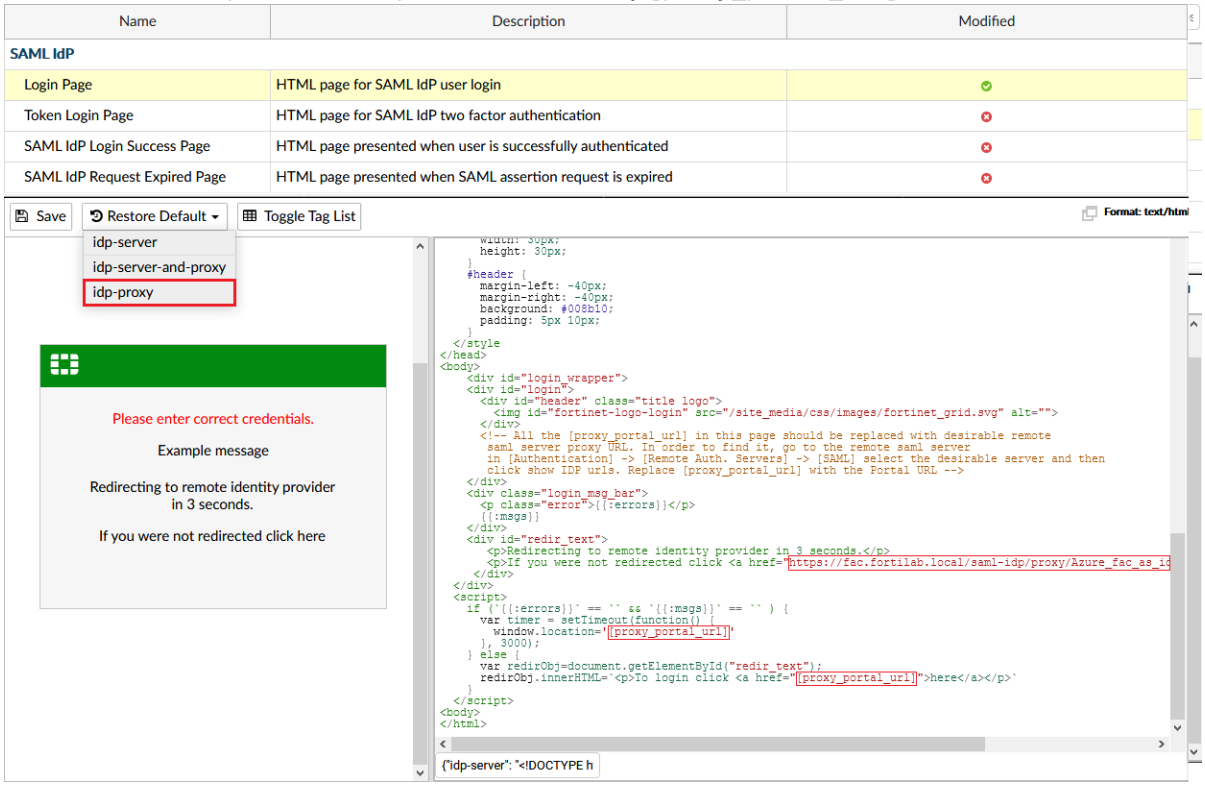
Once the settings have been saved, you will see that additional options are available.

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.



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 Agentless VPN link is `https://203.0.113.18:10443`. This can be replaced with the Agentless 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 315

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 314.

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 Agentless 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 Microsoft Entra ID. This can only be done through the FortiGate CLI.

To increase the remote authentication timeout:

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

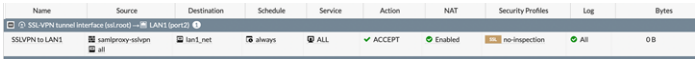
```
config system global
   set remoteauthtimeout 60
end
```

Configure the Agentless VPN

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

To add a portal to your Agentless VPN:

1. Go to *VPN > Agentless VPN Settings*, and edit your Agentless 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 Agentless VPN settings.
5. Configure your Agentless VPN rules as required.

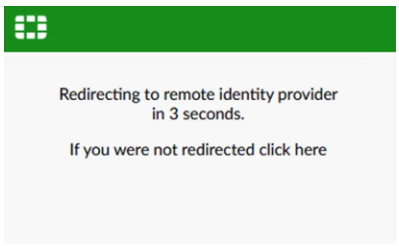


For more information on configuring Agentless VPN on FortiGate, see the FortiGate Administration Guide.

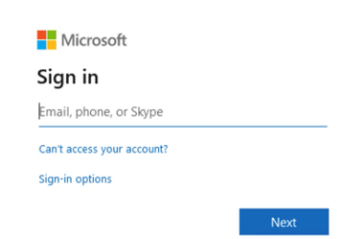
Results

To sign in to your Agentless VPN:

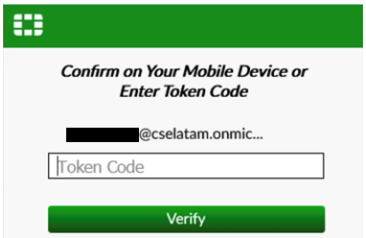
1. Once the user tries to connect to the Agentless VPN web portal, FortiGate will redirect the user to FortiAuthenticator.



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



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



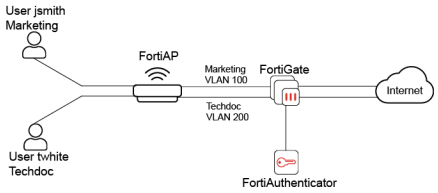
4. The user is now connected to the Agentless VPN.

WiFi and RADIUS

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*).

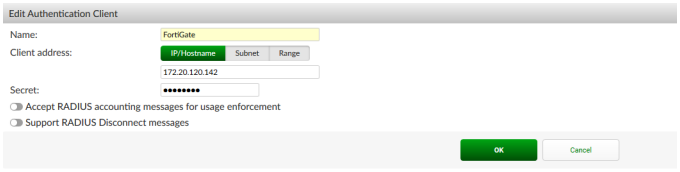



```
config certificate ca
    edit {name}
    # CA certificate.
        set name {string}   Name. size[79]
        set ca {string}   CA certificate as a PEM file.
        set range {global | vdom}   Either global or VDOM IP address range for the CA certificate.
                global  Global range.
                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

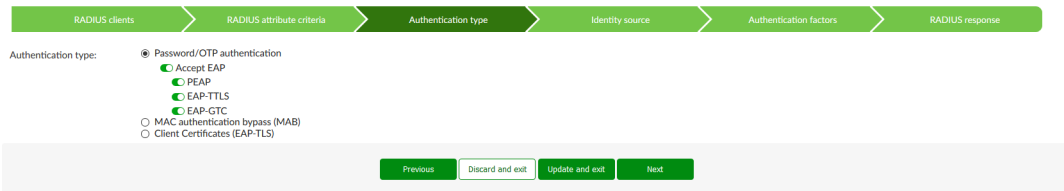
To create the RADIUS client:

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.



To create the RADIUS policy:

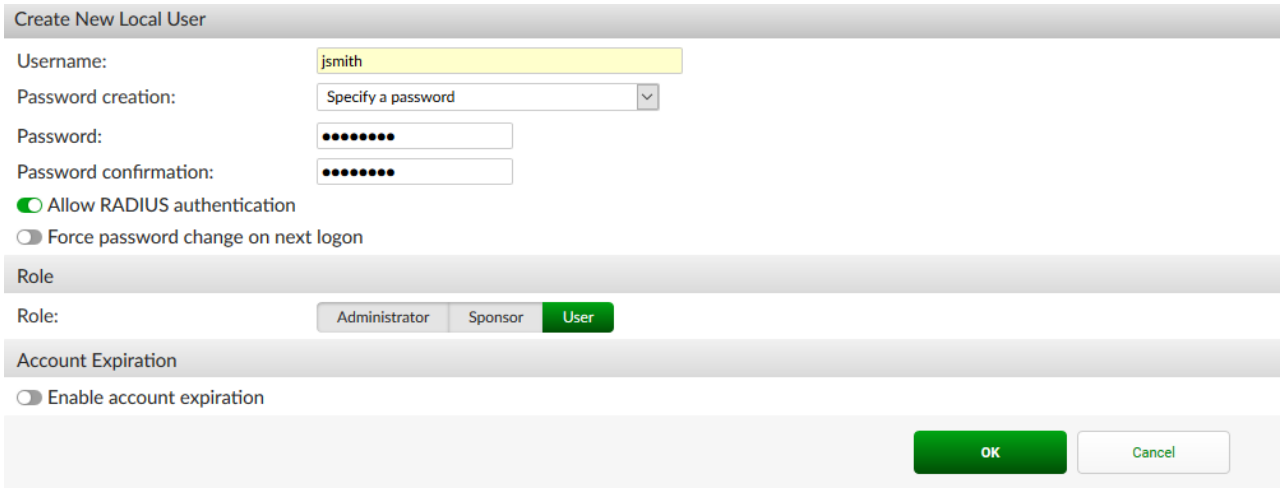
1. Go to *Authentication > RADIUS Service > Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. Do not configure RADIUS attribute criteria.
4. Choose *Password/OTP* authentication as the authentication type and enable all *EAP*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



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.

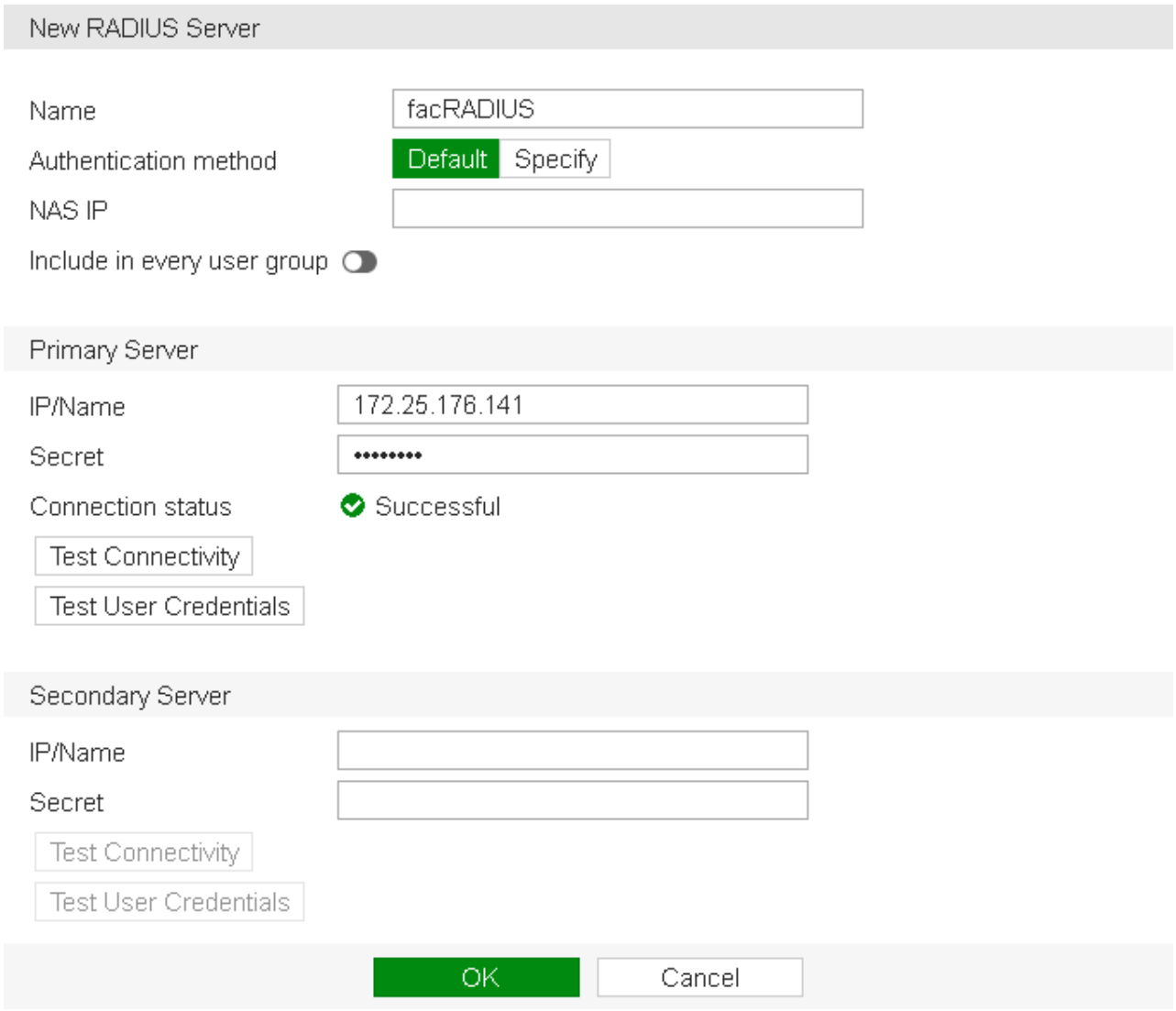


2. For each user, add the following RADIUS attributes which specify the VLAN information to be sent to the FortiGate.
   The *Tunnel-Private-Group-Id* attribute specifies the VLAN ID.
   In this example, jsmith is assigned VLAN *100* and twhite is assigned VLAN *200*.

Adding the RADIUS server to the FortiGate

To add the RADIUS server to the FortiGate:

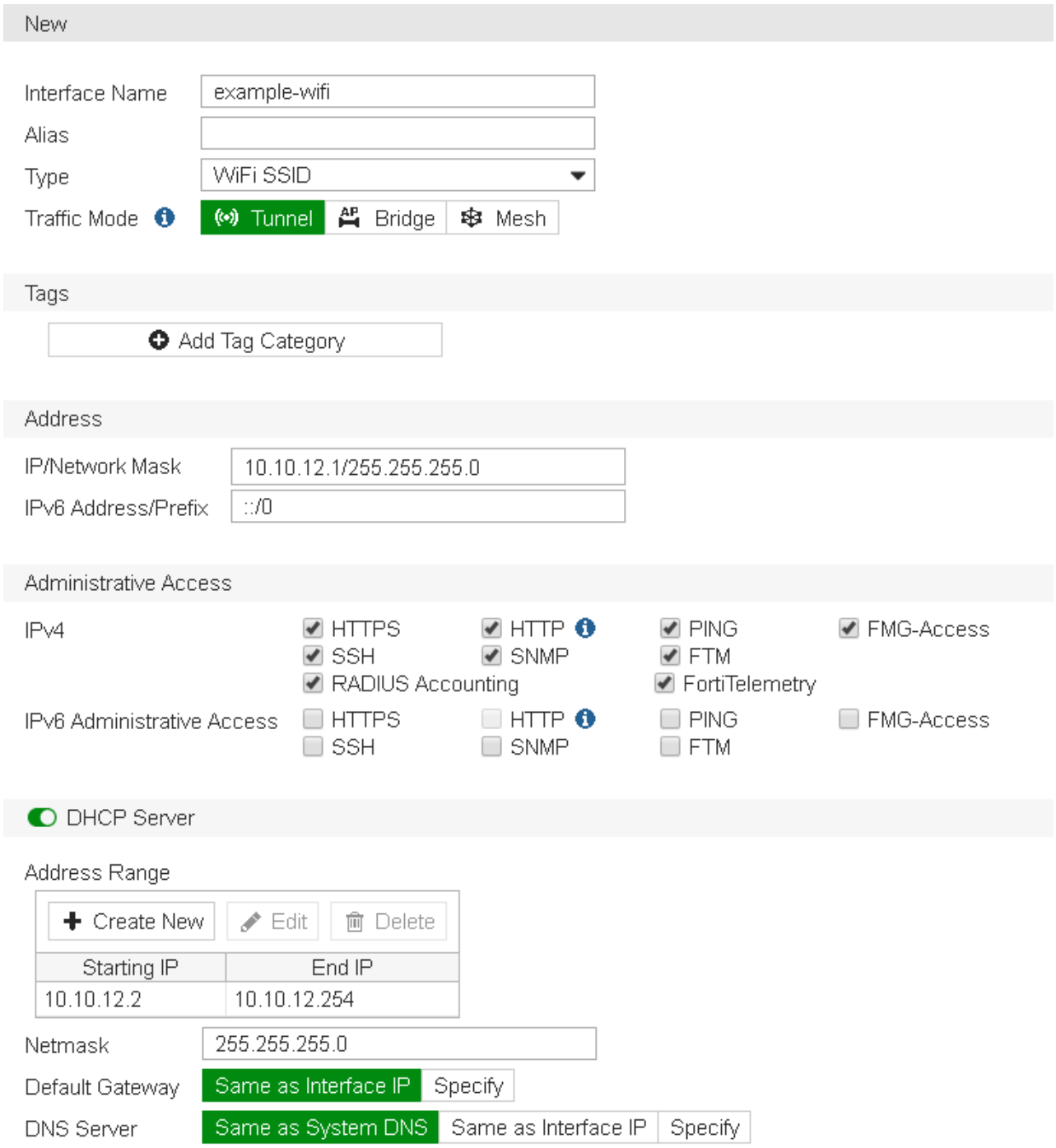
1. On the FortiGate, go to *User & Device > RADIUS Servers* and select *Create New*.
   Enter the FortiAuthenticator IP address and the server *Secret* entered on the FortiAuthenticator earlier.
   Select *Test Connectivity* to confirm the successful connection.



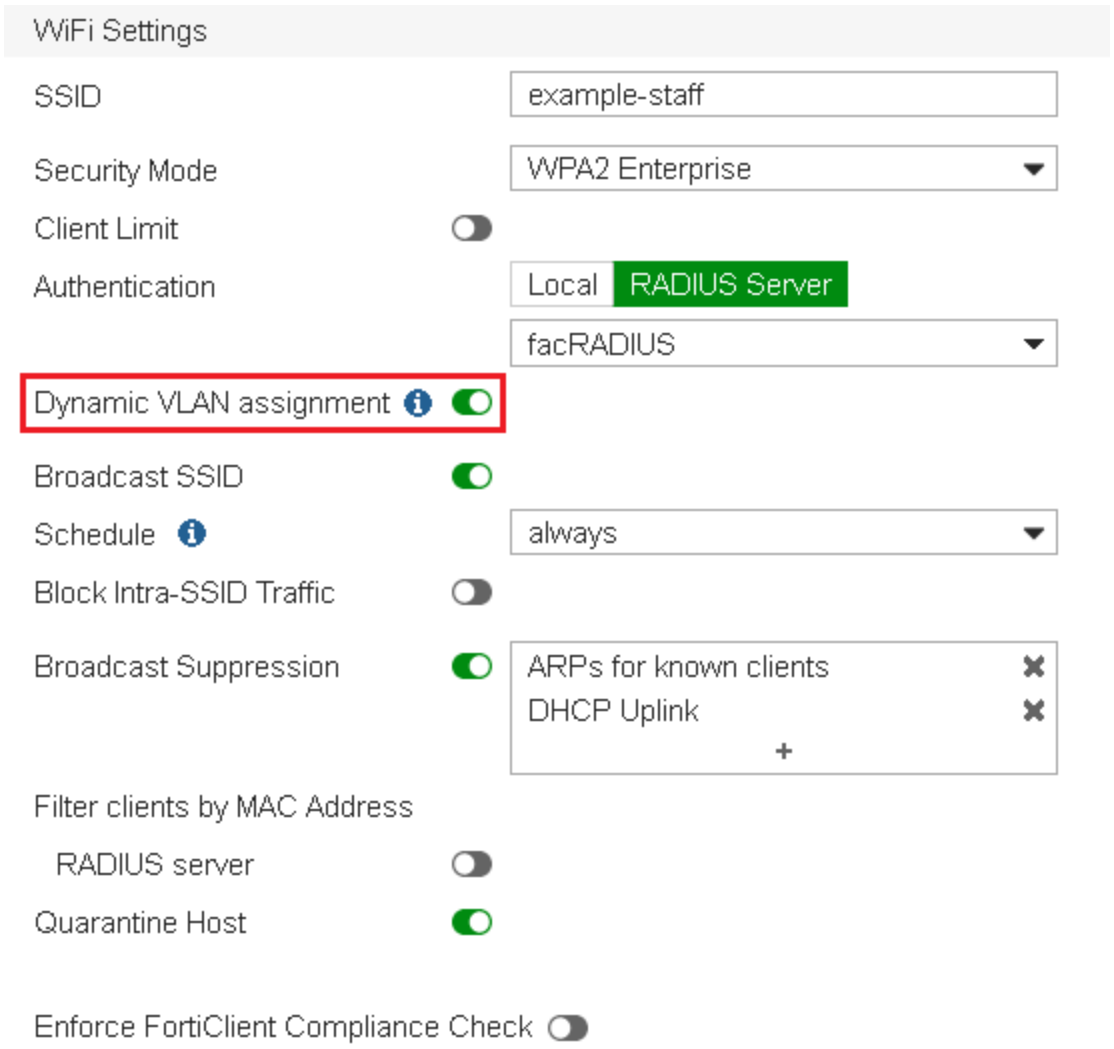
Creating an SSID with dynamic VLAN assignment

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.



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



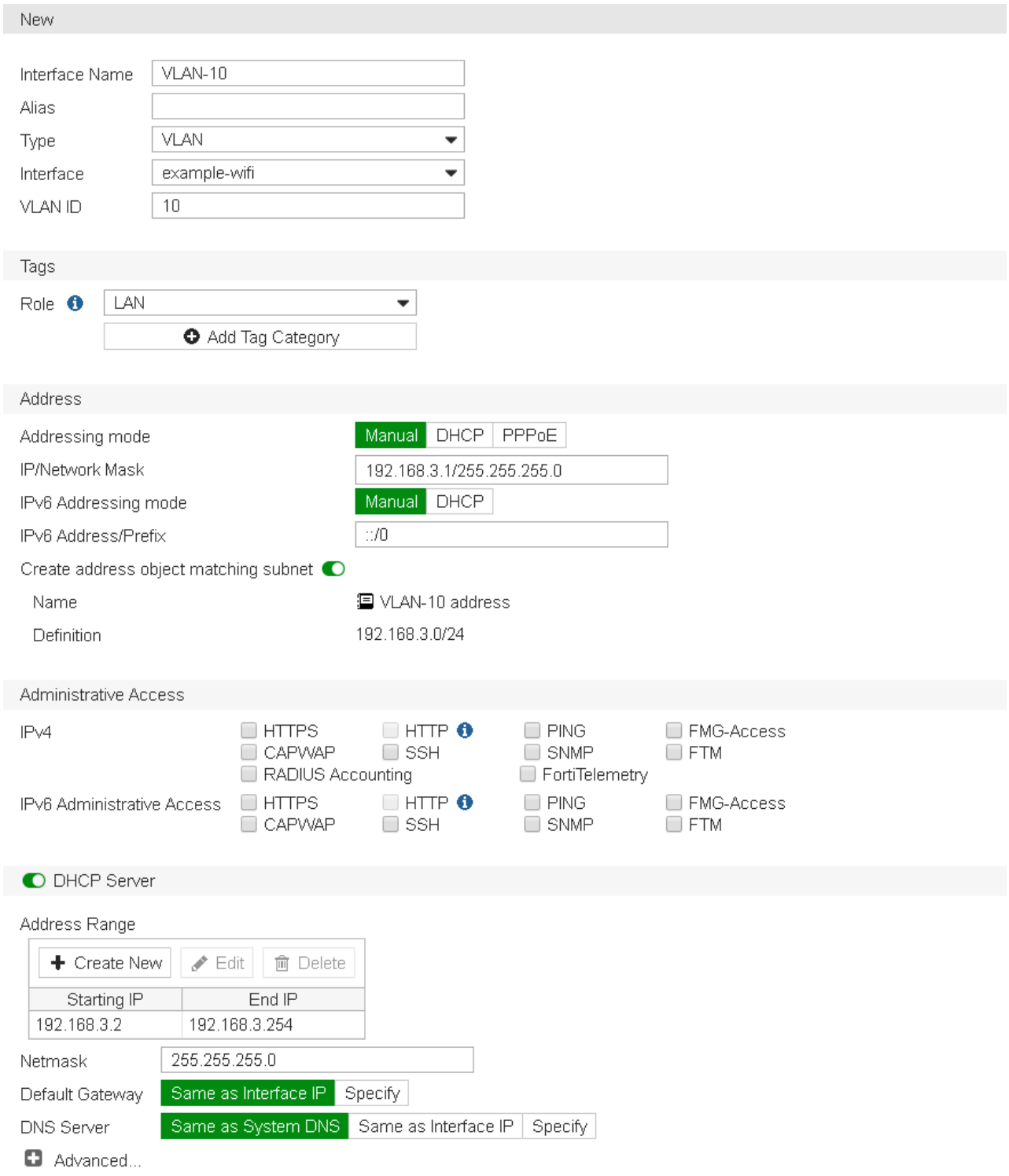
3. Then open the *CLI Console* and enter the following command to assignment and set the VLAN ID to `10`. This VLAN is used when RADIUS does not assign a VLAN:

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

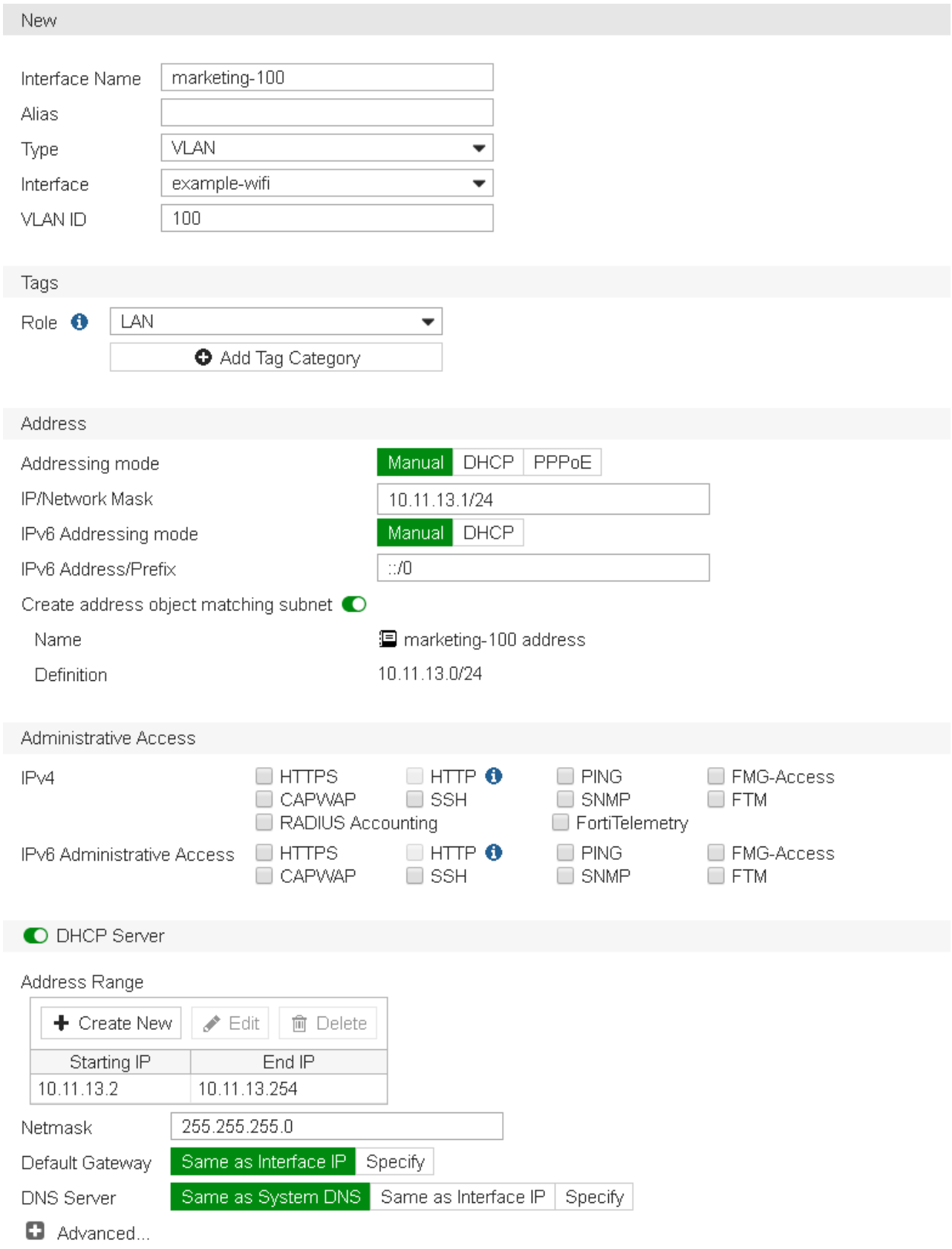
Creating the VLAN interfaces

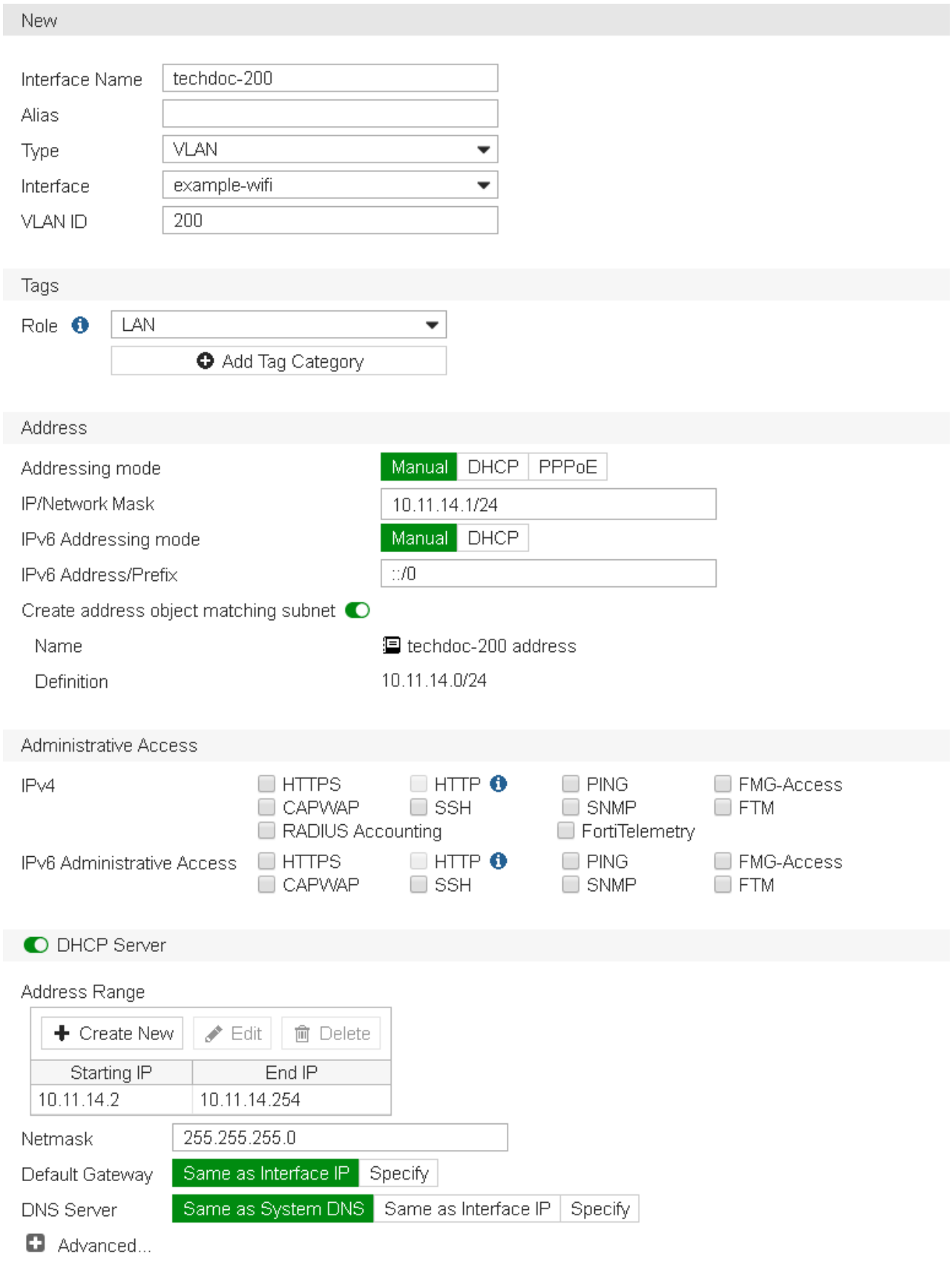
To create the VLAN interfaces:

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



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

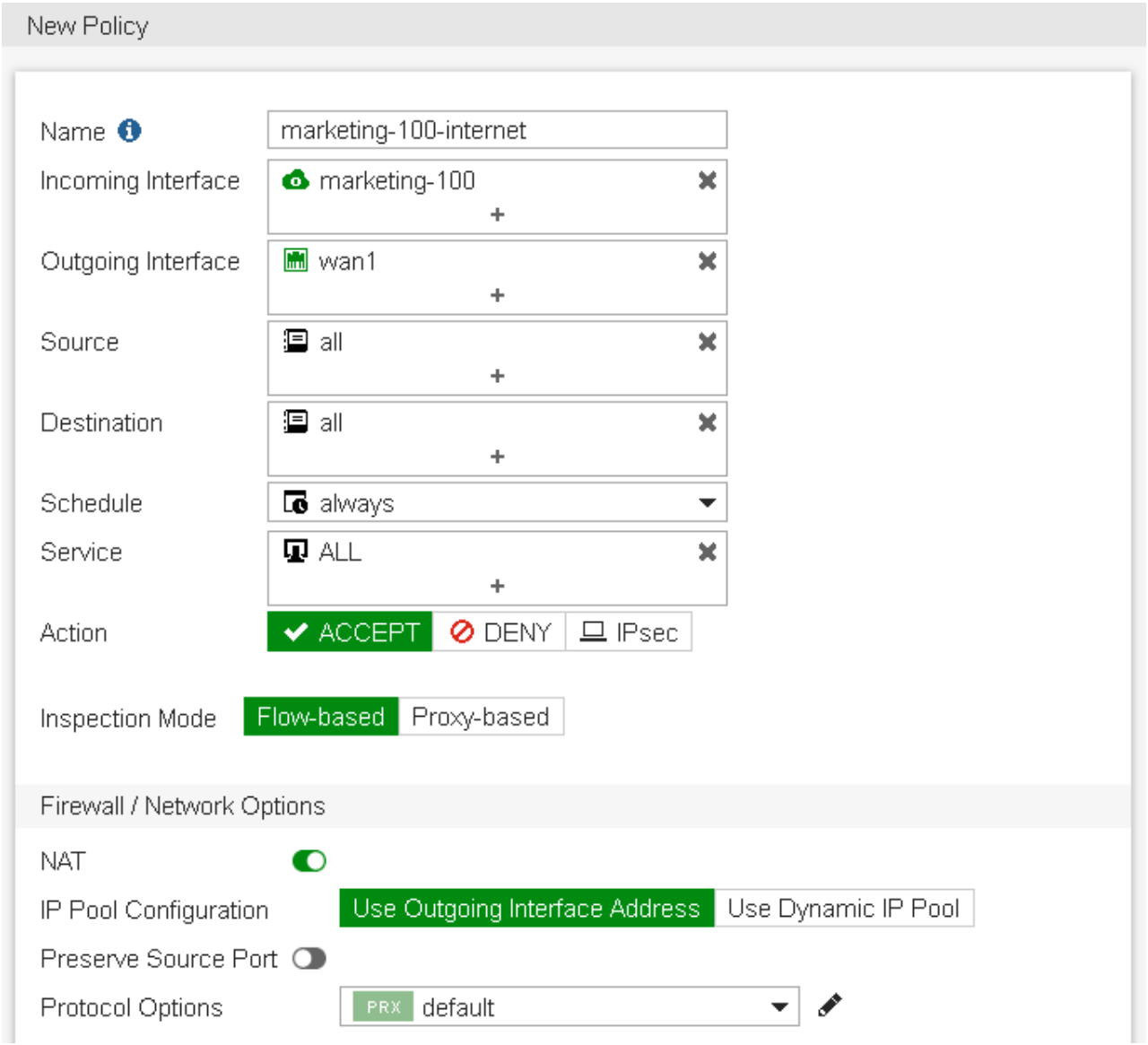

New
Interface Name
marketing-100
Alias
Type
VLAN
Interface
example-wifi
VLAN ID
100
Tags
Role
LAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
PPPoE
IP/Network Mask
10.11.13.1/24
IPv6 Addressing mode
Manual
DHCP
IPv6 Address/Prefix
::/0
Create address object matching subnet
Name
marketing-100 address
Definition
10.11.13.0/24
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry
IPv6 Administrative Access
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
DHCP Server
Address Range
Create New
Edit
Delete
Starting IP
End IP
10.11.13.2
10.11.13.254
Netmask
255.255.255.0
Default Gateway
Same as Interface IP
Specify
DNS Server
Same as System DNS
Same as Interface IP
Specify
Advanced...


New
Interface Name
techdoc-200
Alias
Type
VLAN
Interface
example-wifi
VLAN ID
200
Tags
Role
LAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
PPPoE
IP/Network Mask
10.11.14.1/24
IPv6 Addressing mode
Manual
DHCP
IPv6 Address/Prefix
::/0
Create address object matching subnet
Name
techdoc-200 address
Definition
10.11.14.0/24
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry
IPv6 Administrative Access
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
DHCP Server
Address Range
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

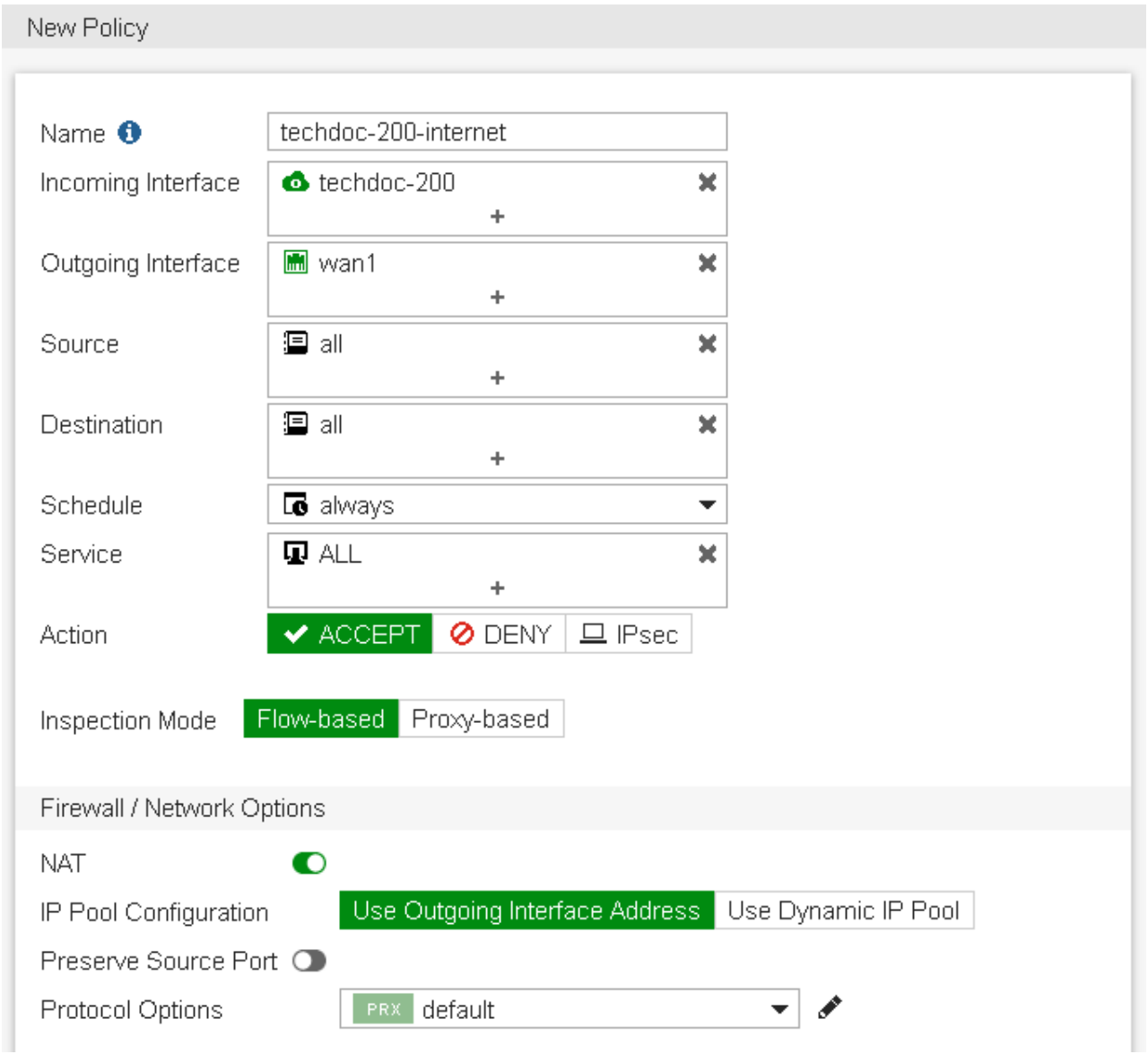
To create the security policies:

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



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

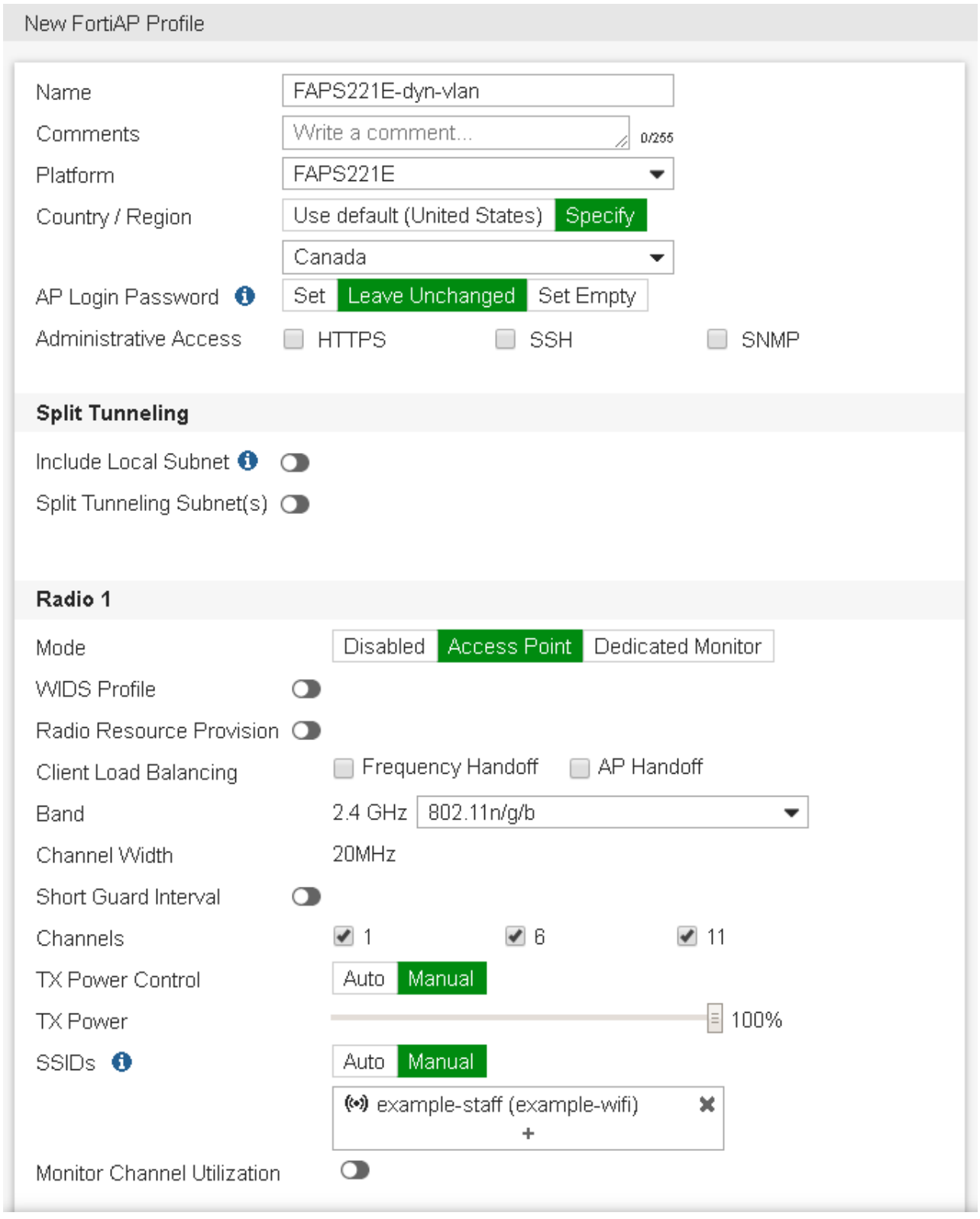
3. Create another policy that allows outbound traffic from *techdoc-200* to the Internet.
   For this policy too, under *Logging Options*, enable logging for *All Sessions*.



Creating the FortiAP profile

To create the FortiAP profile:

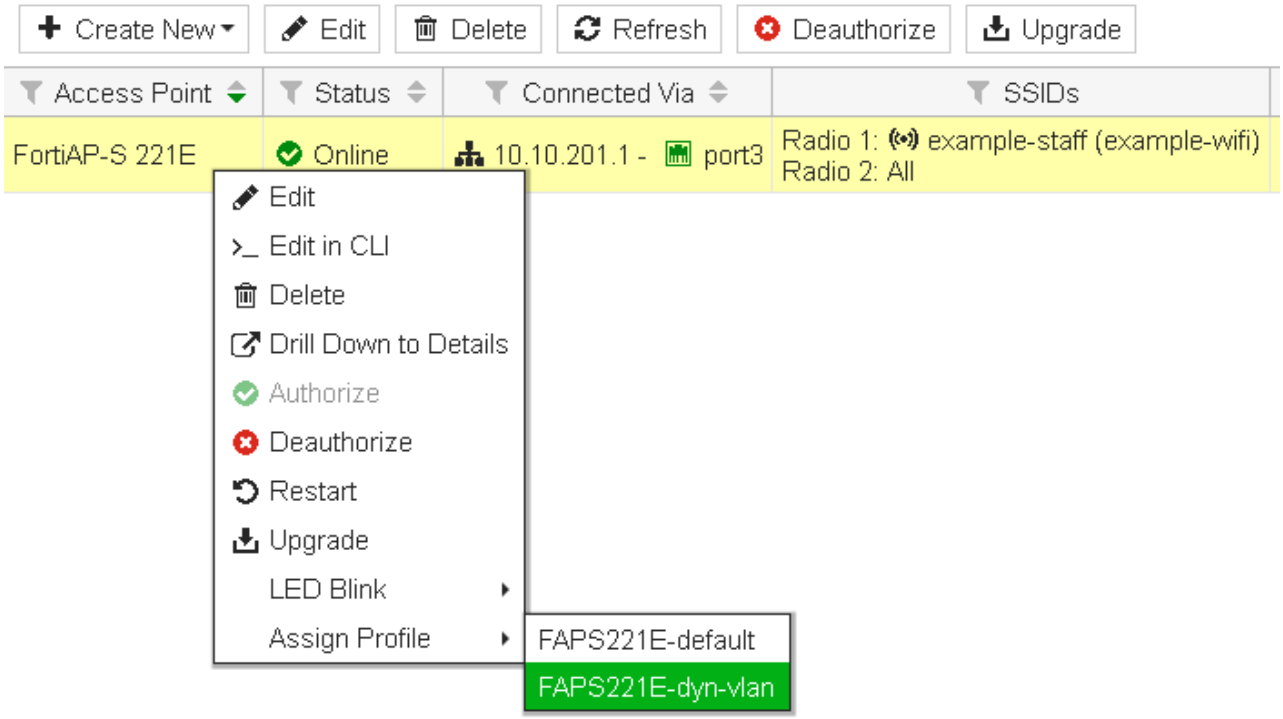
1. Go to *WiFi & Switch Controller* > *FortiAP Profiles*.
   Create a new profile for your FortiAP model and select the new SSID for both *Radio 1* and *Radio 2*.


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.



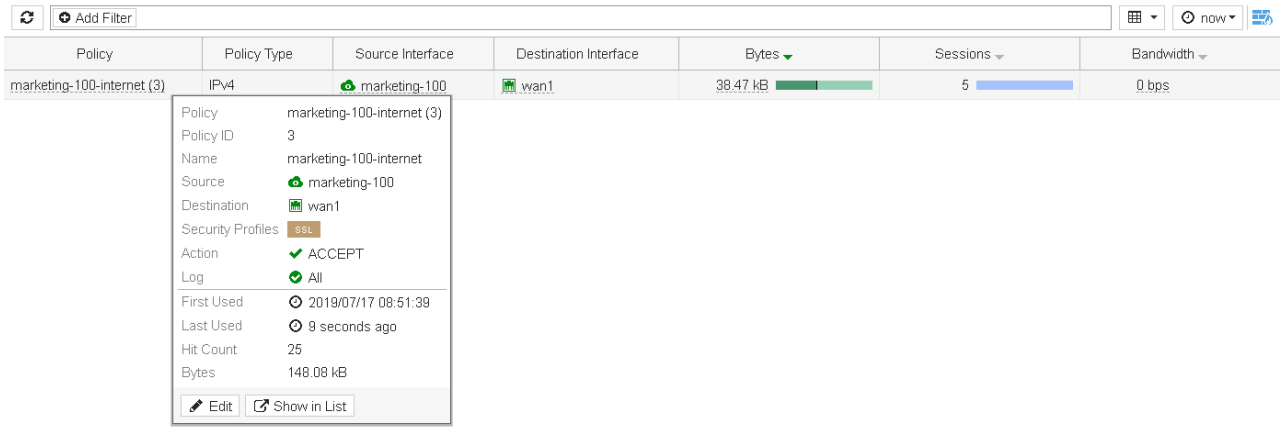
Results

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

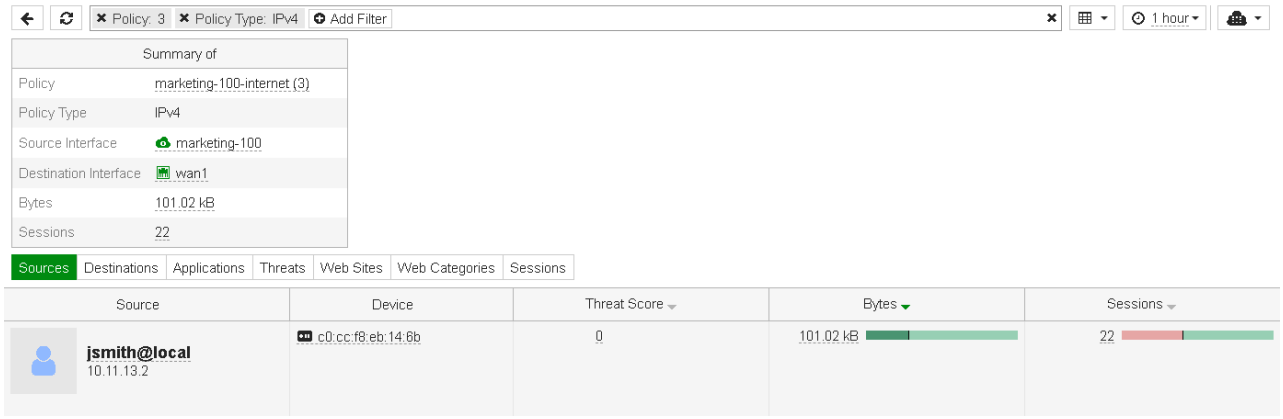
Both twhite and jsmith can connect to the SSID with their credentials and access the Internet.

If a certificate warning message appears, accept the certificate.

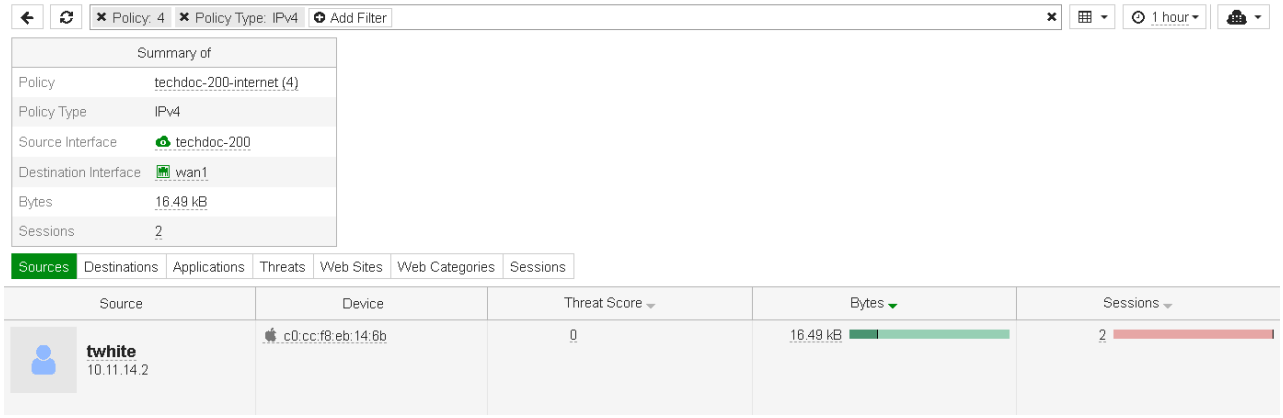
1. Go to *FortiView > Policies*.
   Note that traffic for jsmith and twhite will pass through different policies. In this example, the *marketing-100-internet* policy is displayed, indicating that jsmith has connected to the WiFi.



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



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.



WiFi using FortiAuthenticator RADIUS with certificates

This example 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.

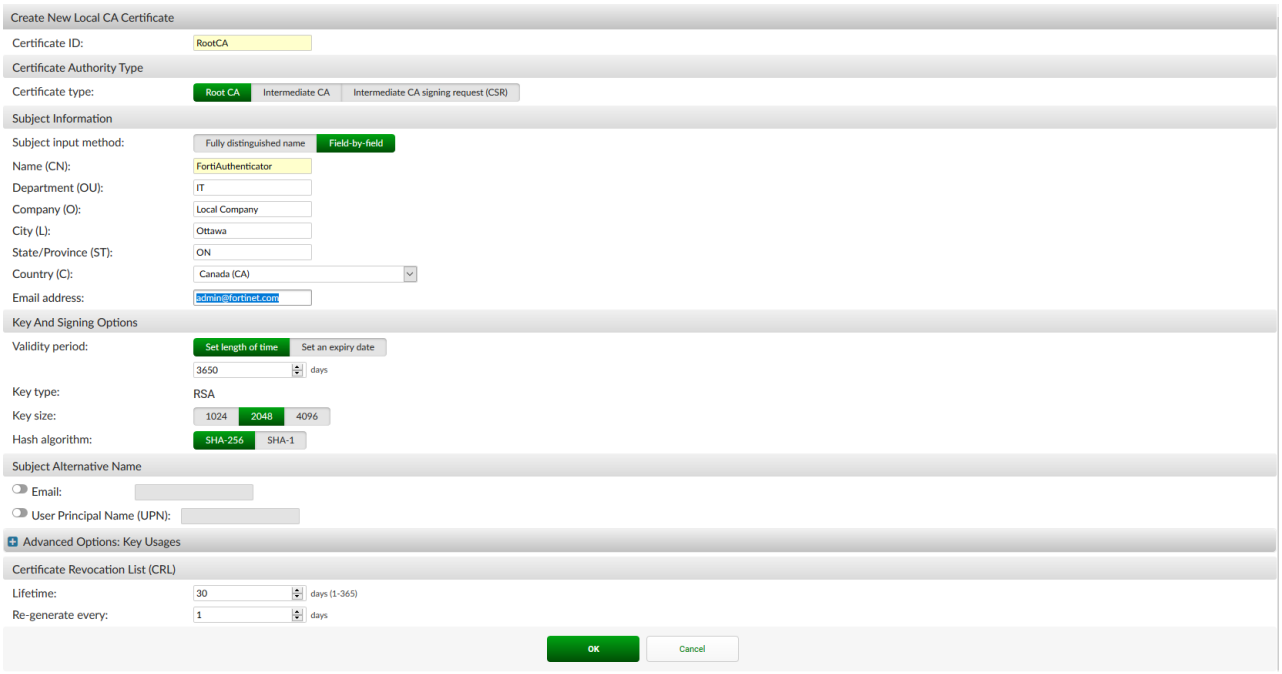
This example specifically focuses on the configuration of the FortiAuthenticator, FortiGate, and Windows 10 computer.

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.

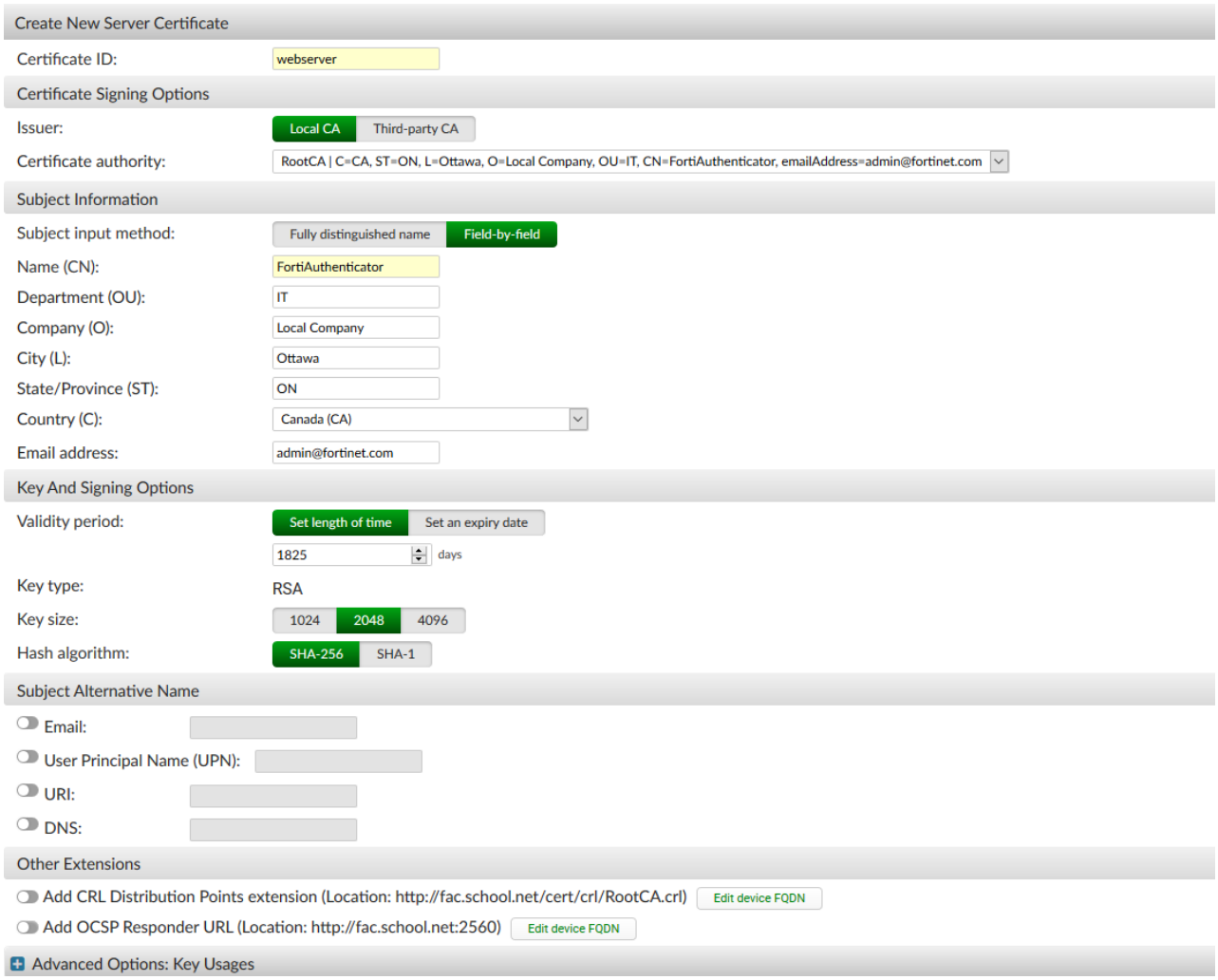


Creating a local service certificate on FortiAuthenticator

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.

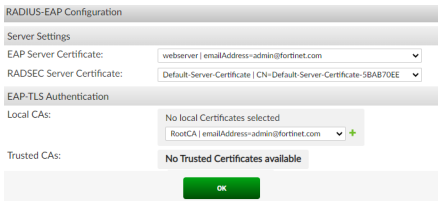


Configuring RADIUS EAP on FortiAuthenticator

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 > General*.
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*.

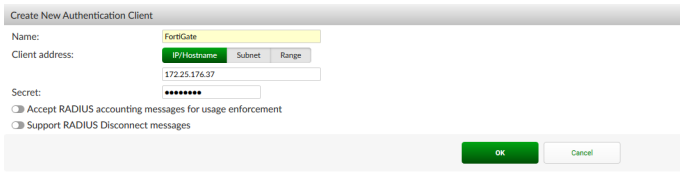


Configuring RADIUS client on FortiAuthenticator

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.



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)*.

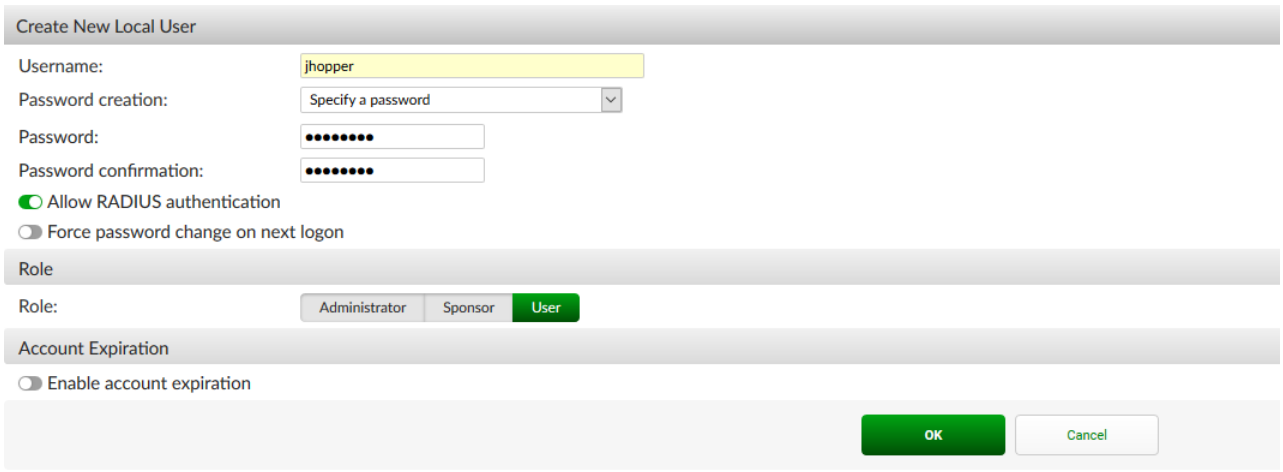
5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
6. Set the authentication method to *Password only authentication*.
7. Review the RADIUS response, and click *Save and Exit*.

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.

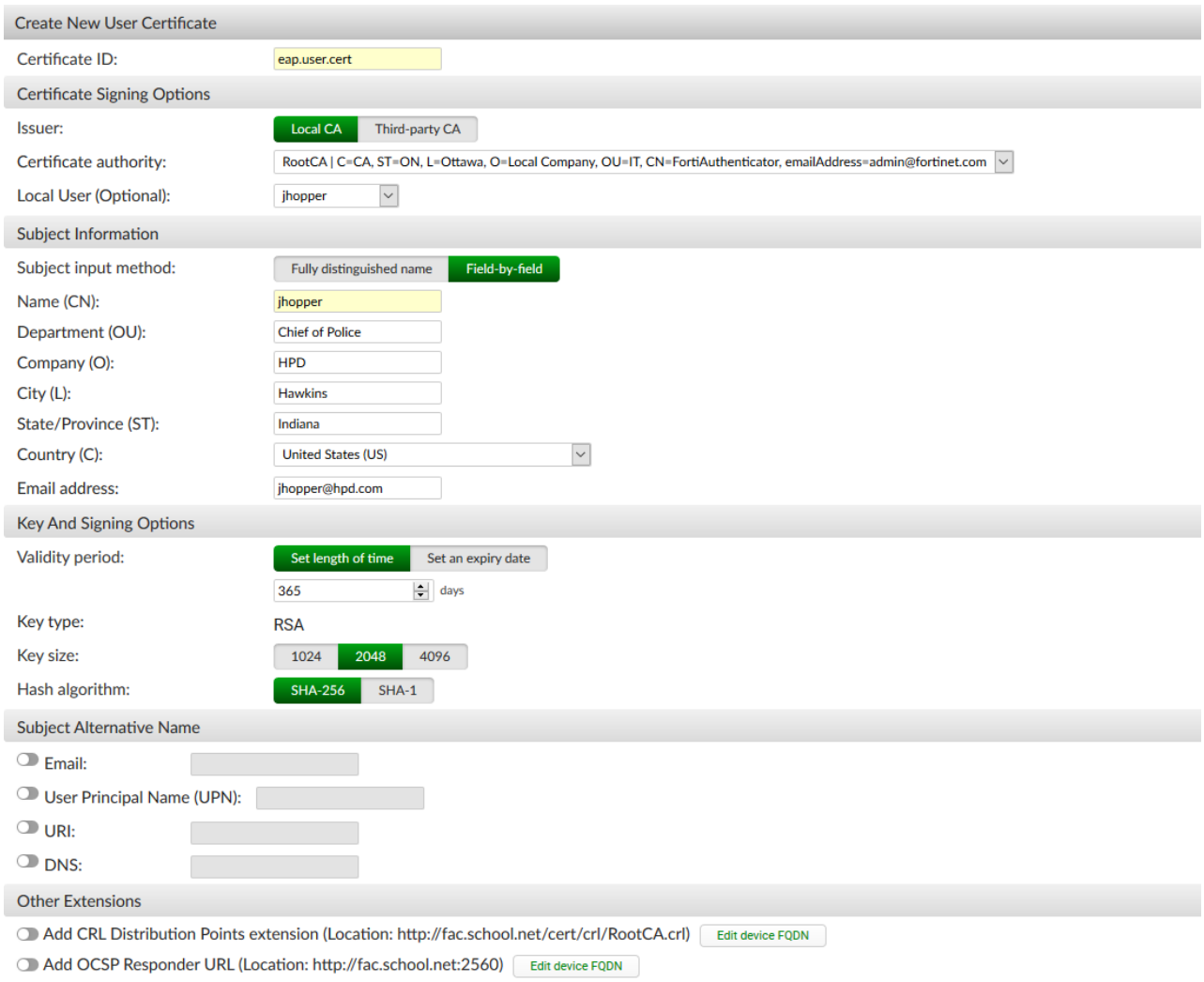


Configuring local user certificate on FortiAuthenticator

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.

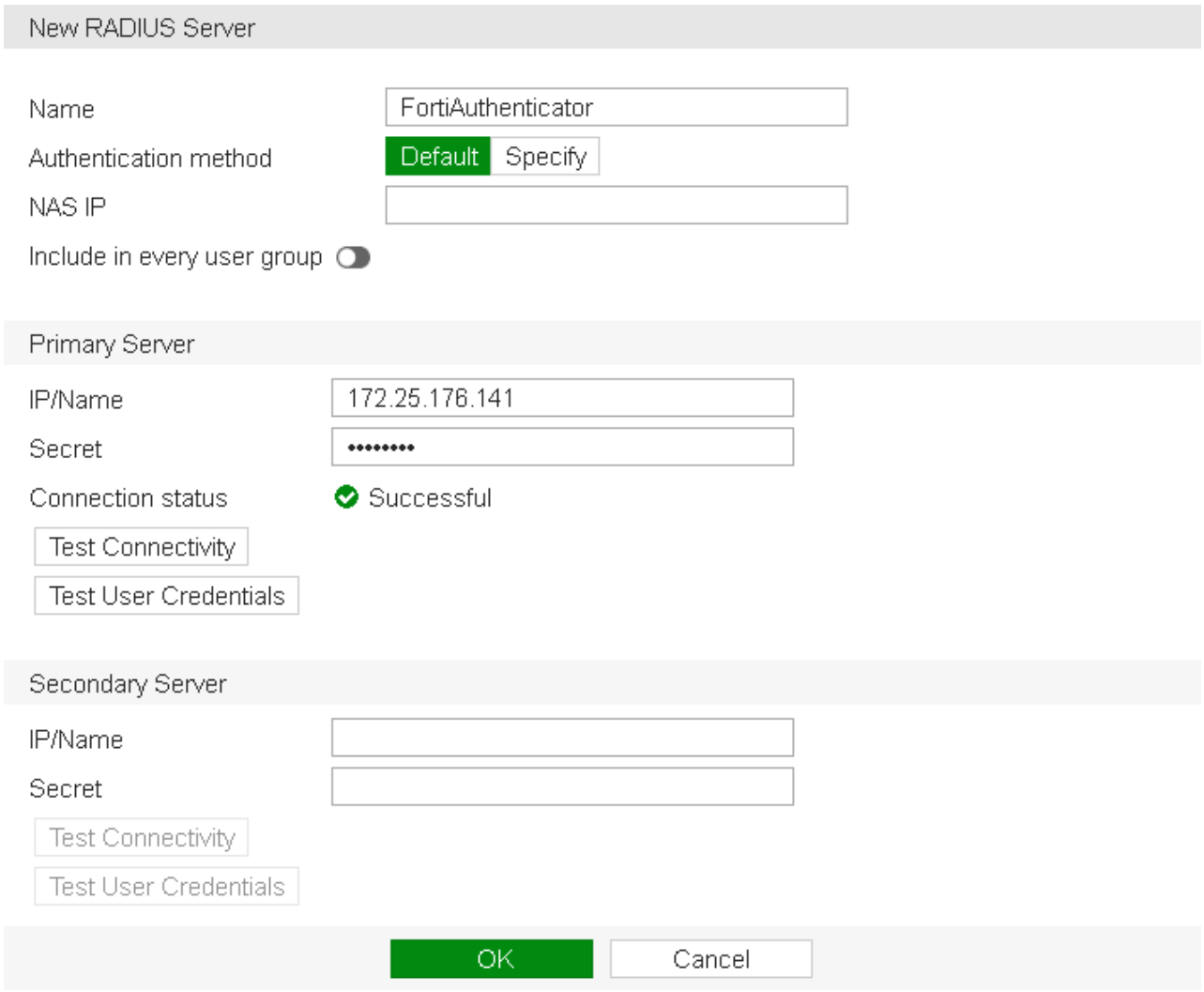


Creating RADIUS server on FortiGate

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.

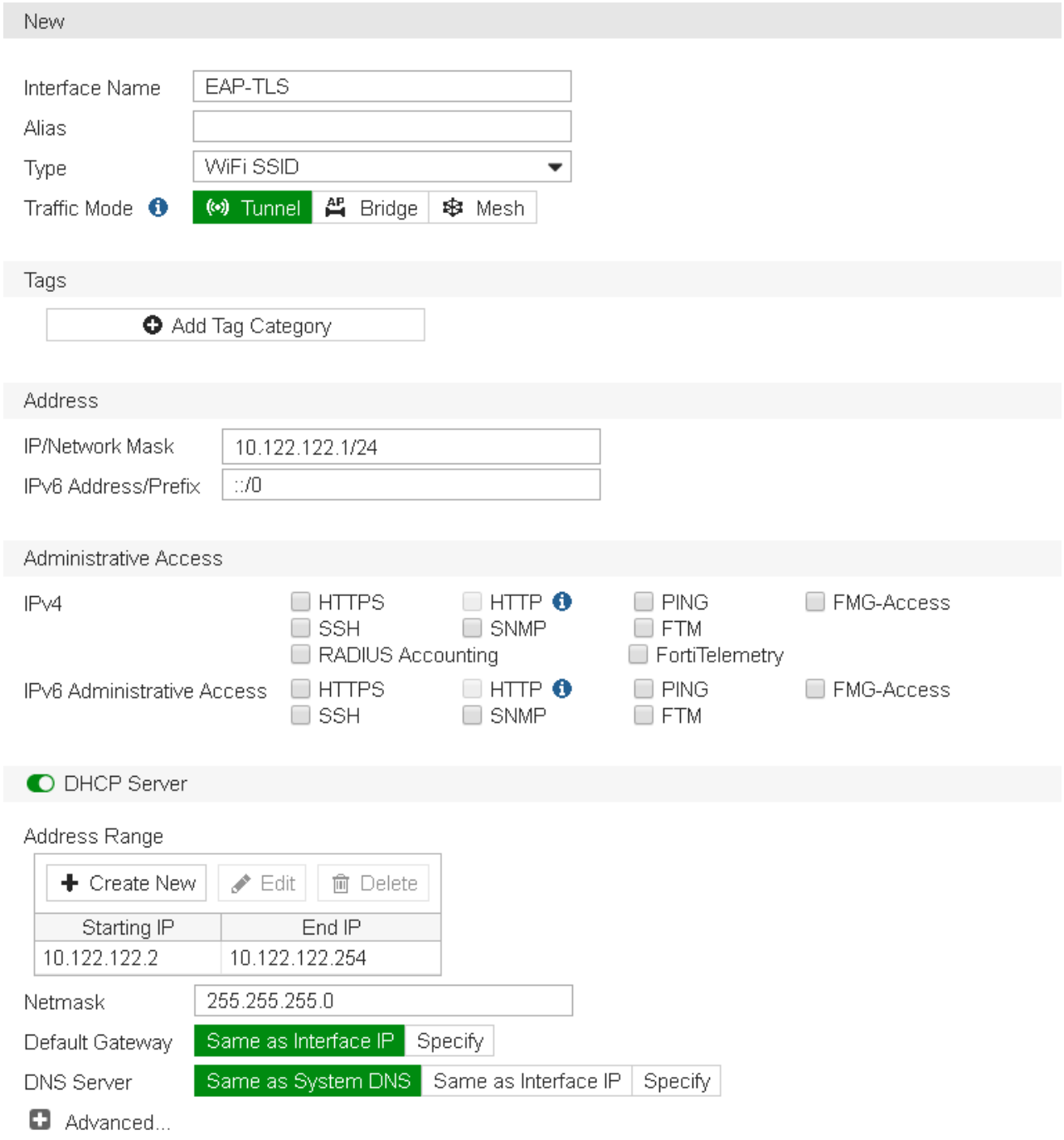


Creating WiFi SSID on FortiGate

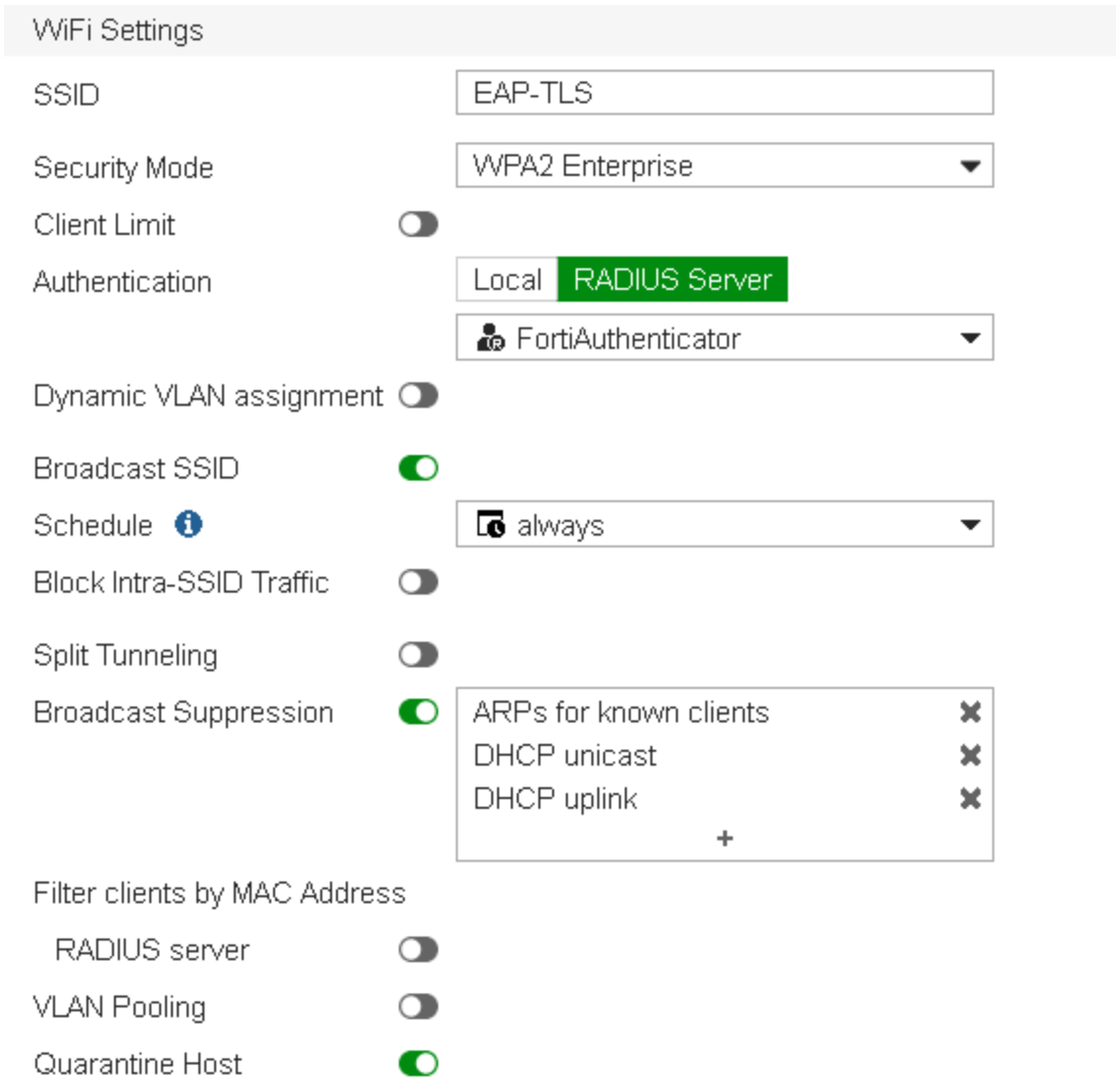
In order for the WiFi client to connect using its certificate a SSID has to be configured on the FortiGate to accept this type of authentication.

To create the WiFi SSID:

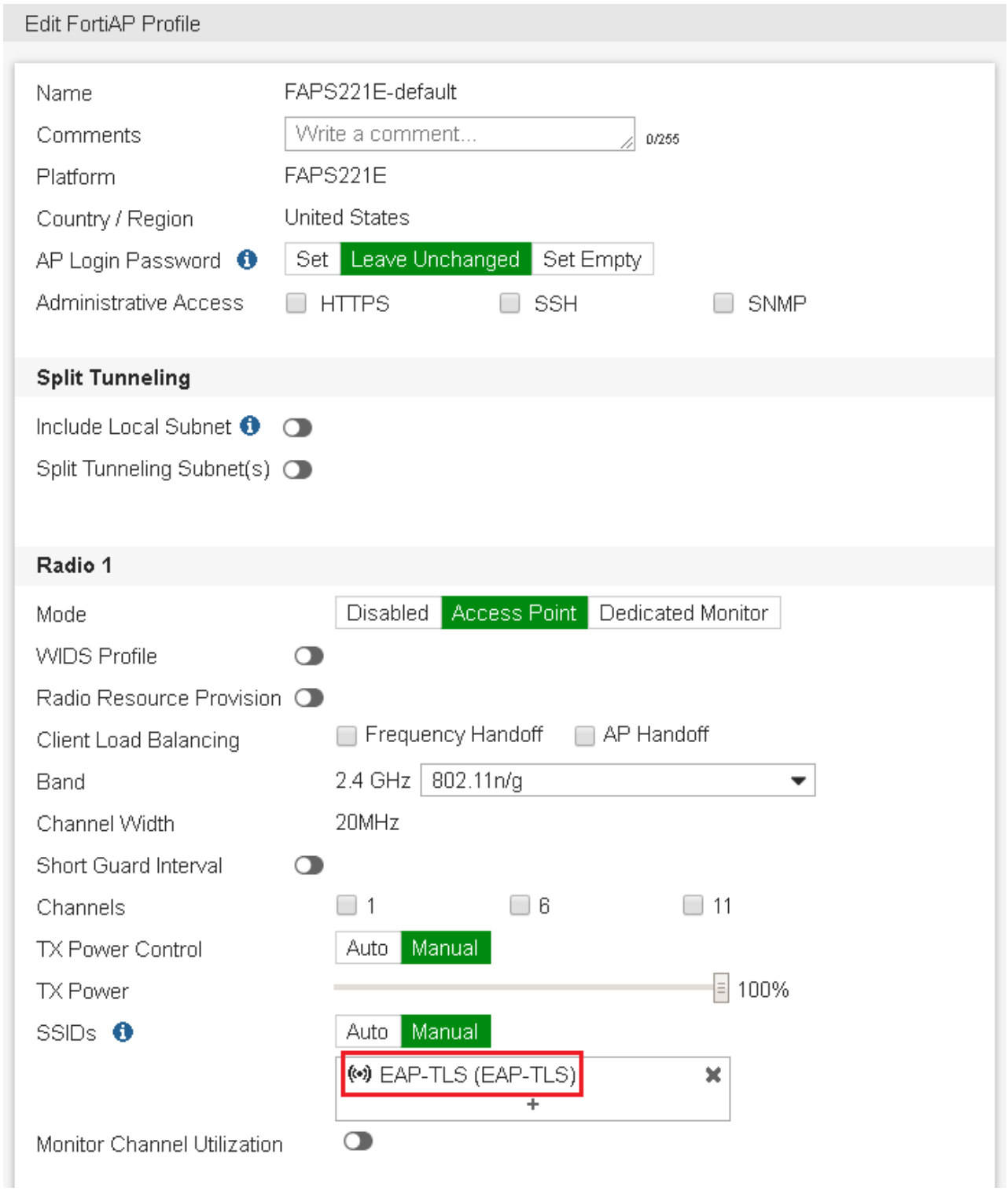
1. Go to *WiFi & Switch Controller* > *SSID* and create an SSID with DHCP for clients.



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



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*.



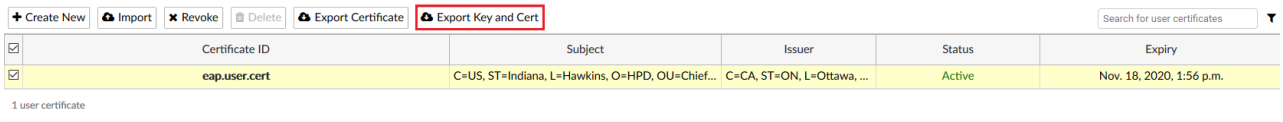
4. Then go to *Policy & Objects* > *IPv4 Policy* and create a policy that allows outbound traffic from the *EAP-TLS* wireless interface to the Internet.

Exporting user certificate from FortiAuthenticator

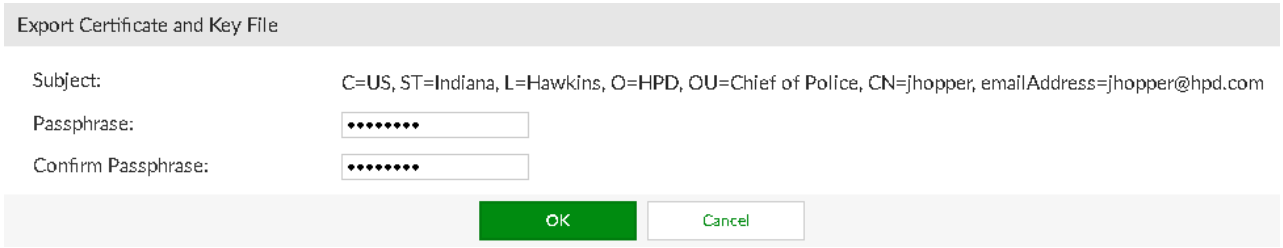
In order for the WiFi client to authenticate with the RADIUS server, the user certificate created in the FortiAuthenticator must first be exported.

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*.



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*.

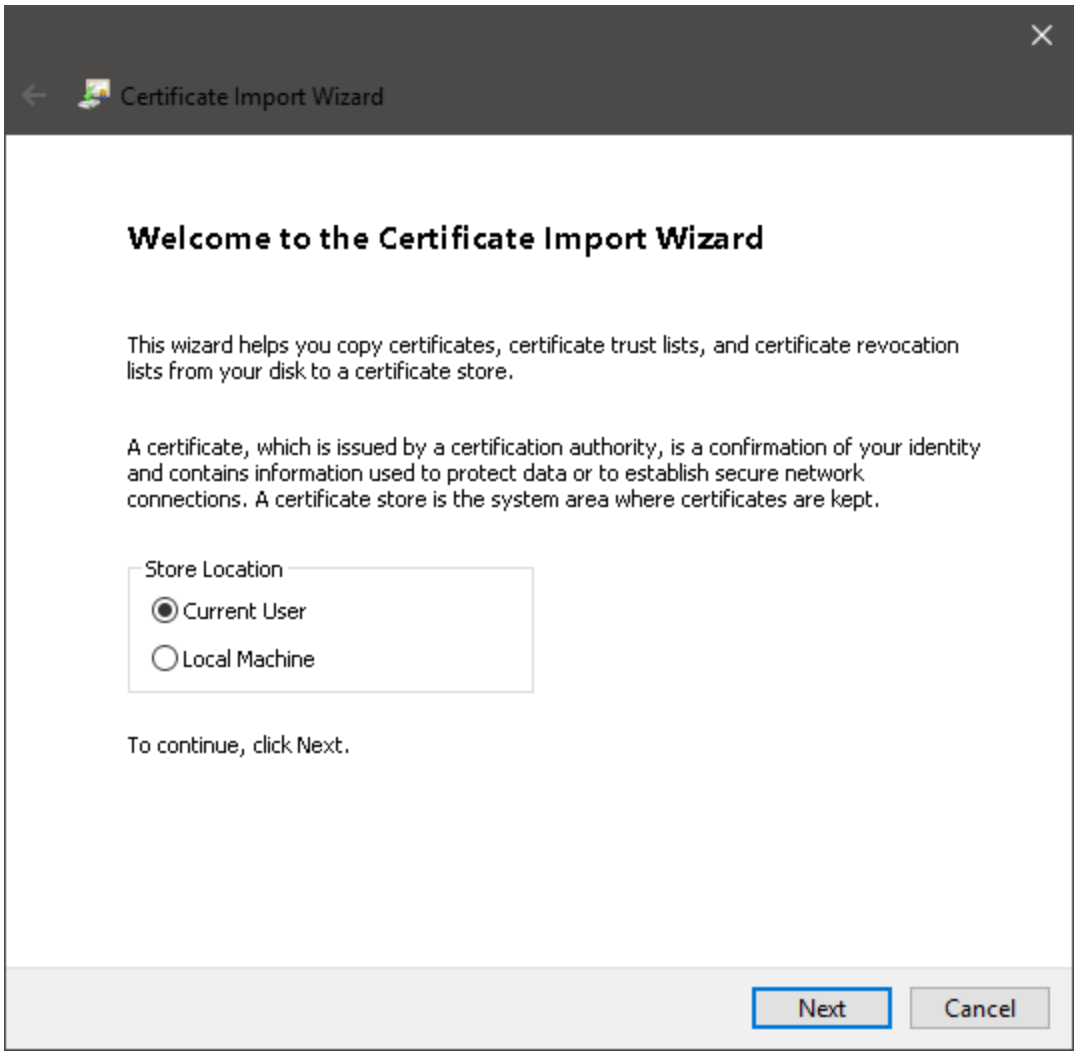


3. Select *Download PKCS#12 file* to pull this certificate to the Widows 10 computer. Select *Finish*.

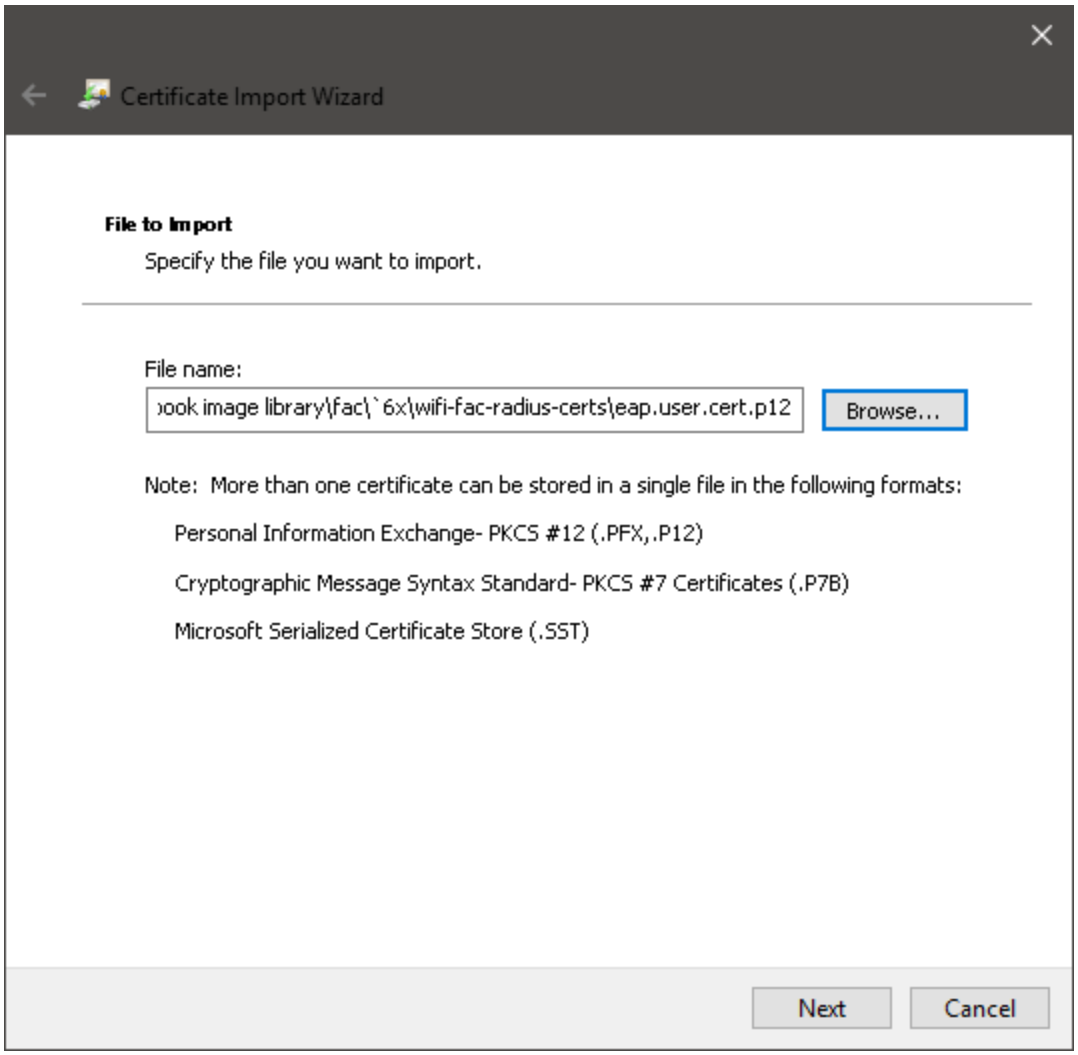
Importing user certificate into Windows 10

To import the user certificate:

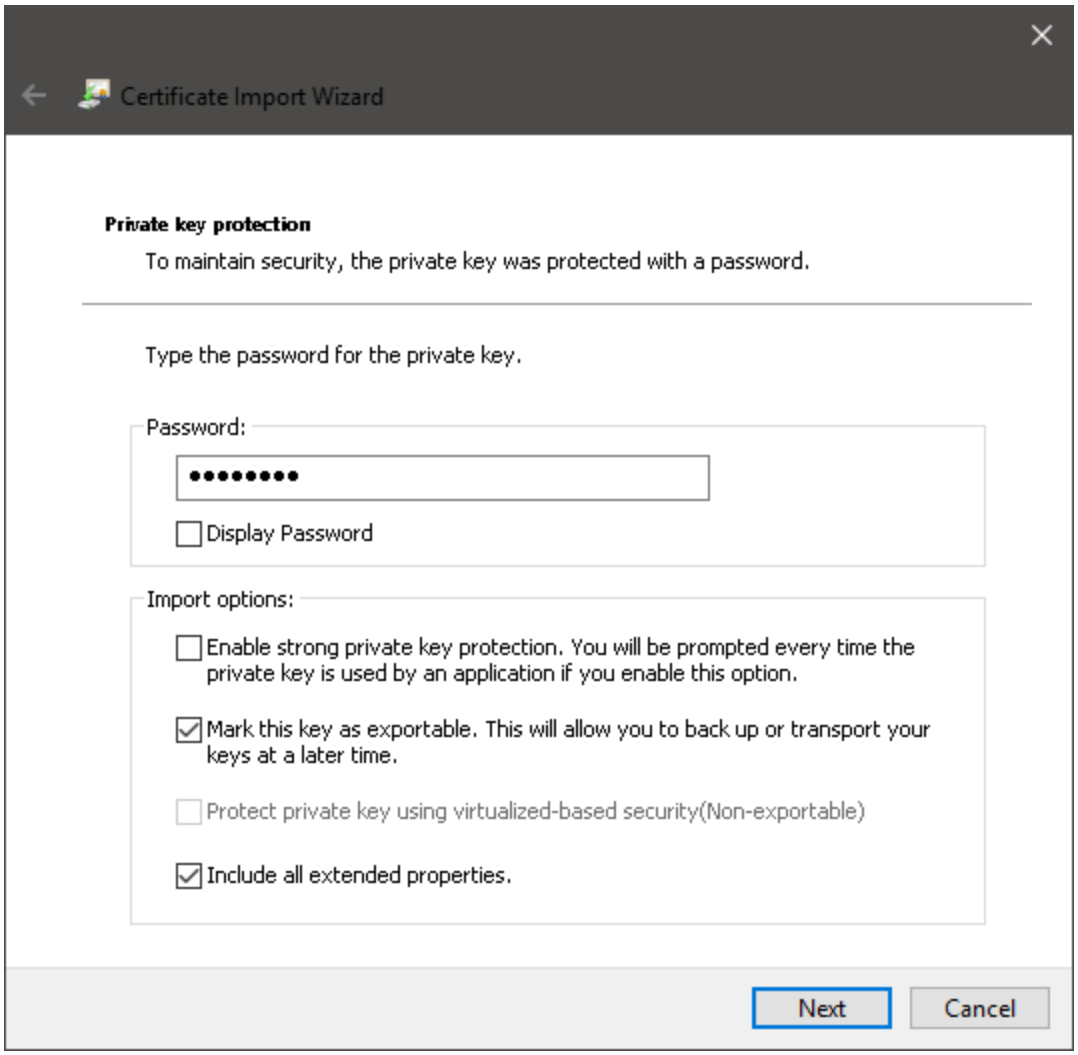
1. On the Windows 10 computer, double-click the downloaded certificate file from the FortiAuthenticator. This will launch the *Certificate Import Wizard*. Select *Next*.



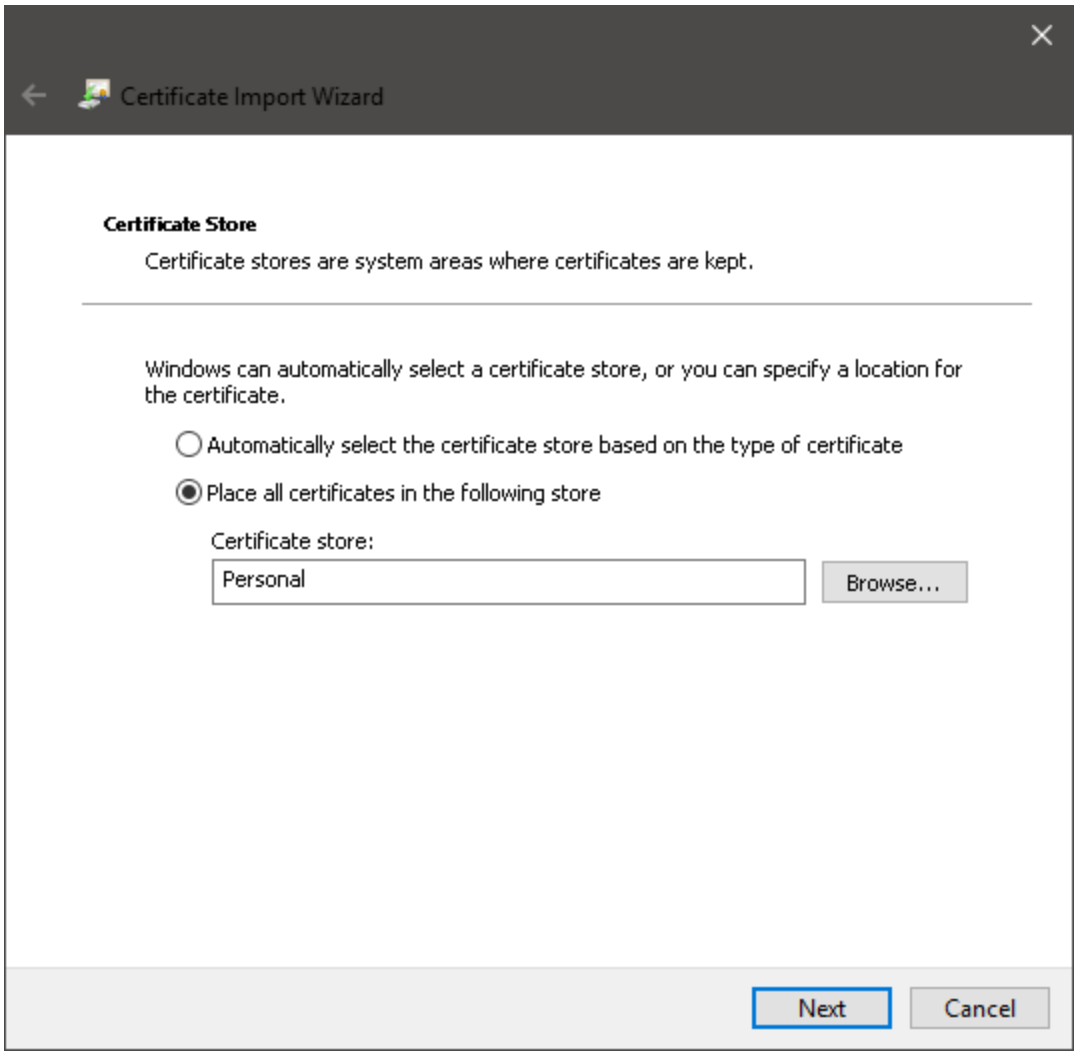
2. Make sure the correct certificate is shown in the *File name* section in the *File to Import* window. Select *Next*.



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*.



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.

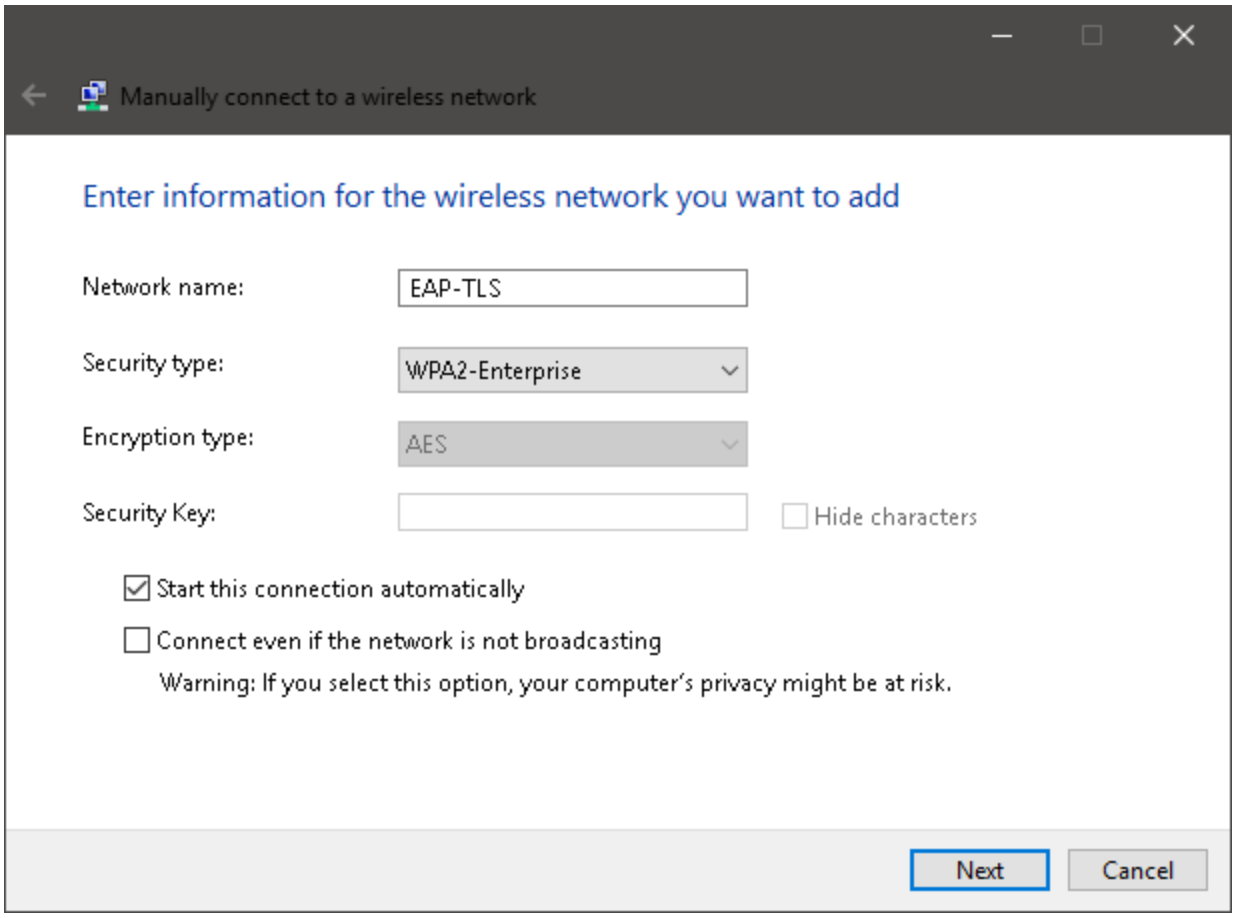


Configuring Windows 10 wireless profile to use certificate

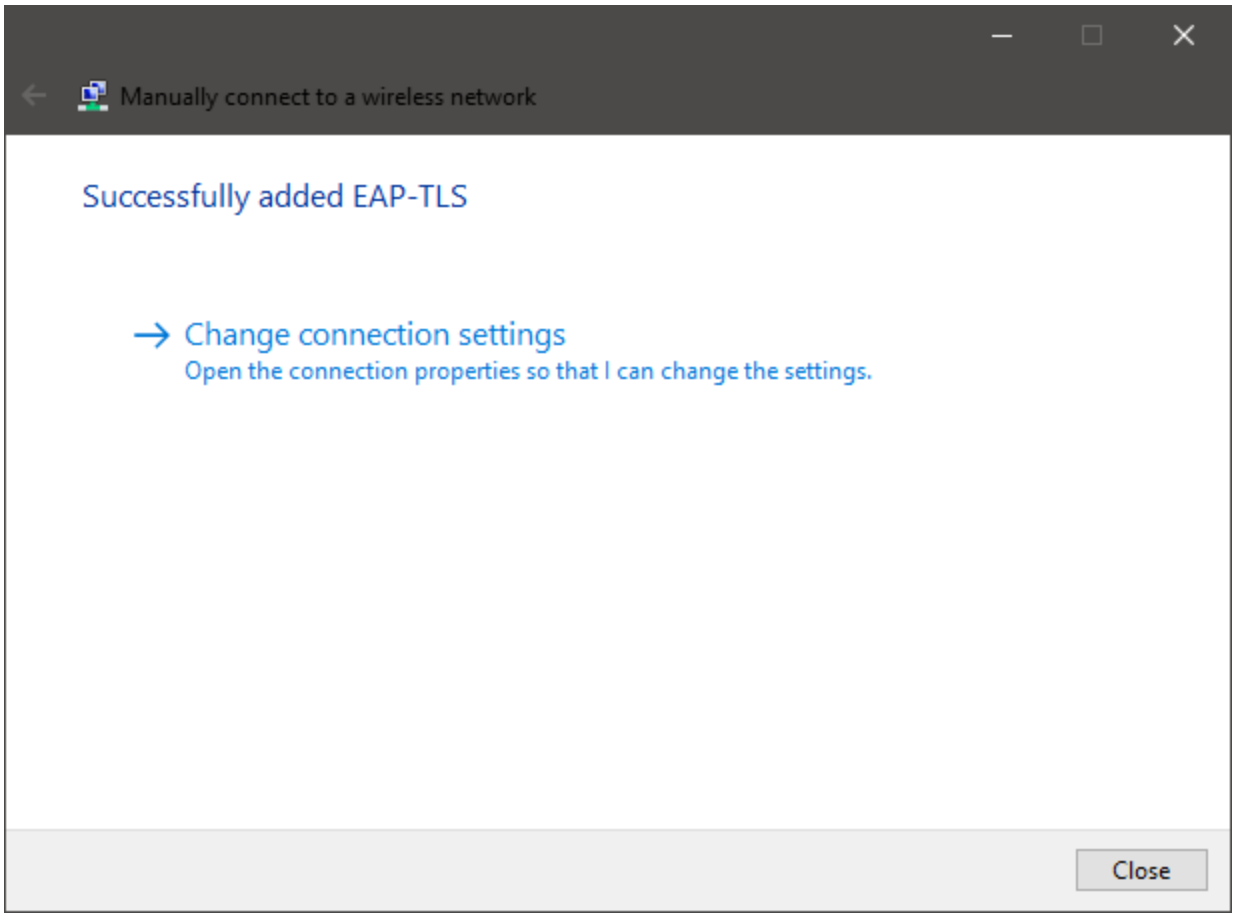
Create a new wireless SSID for this secure connection, in this case EAP-TLS.

To create a wireless SSID:

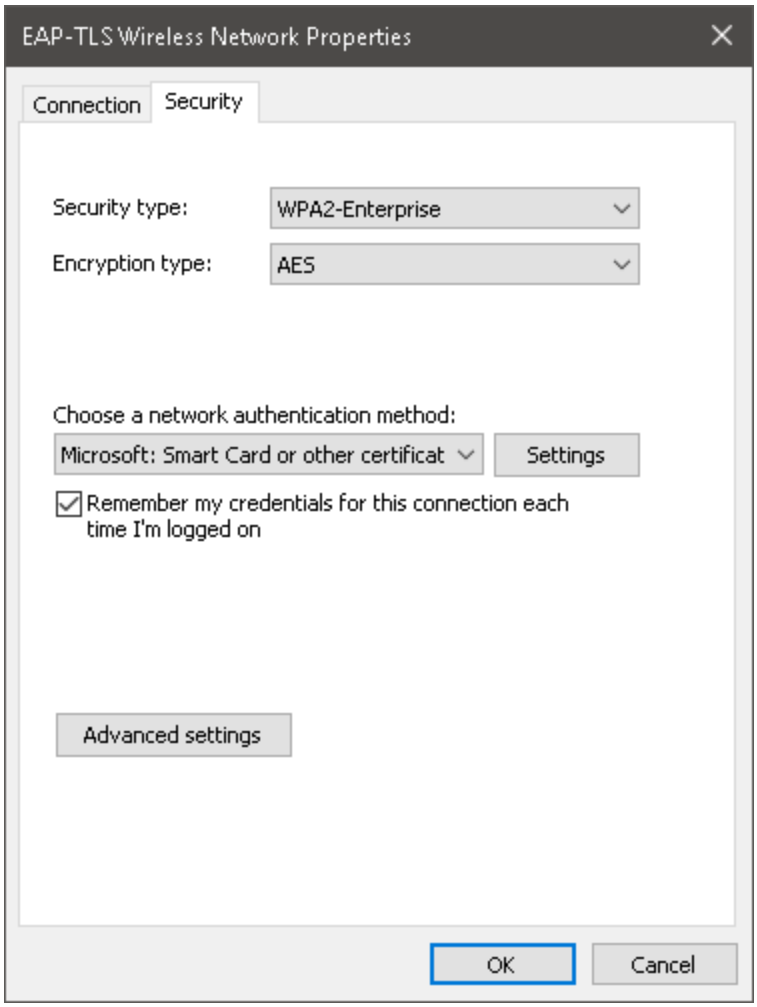
1. On Windows 10, got to *Control Panel > Network and Sharing Center > Set up a new connection or network > Manually connect to a wireless network*. Enter a *Network name* and set *Security type* to *WPA2-Enterprise*. The *Encryption type* is set to *AES*.



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

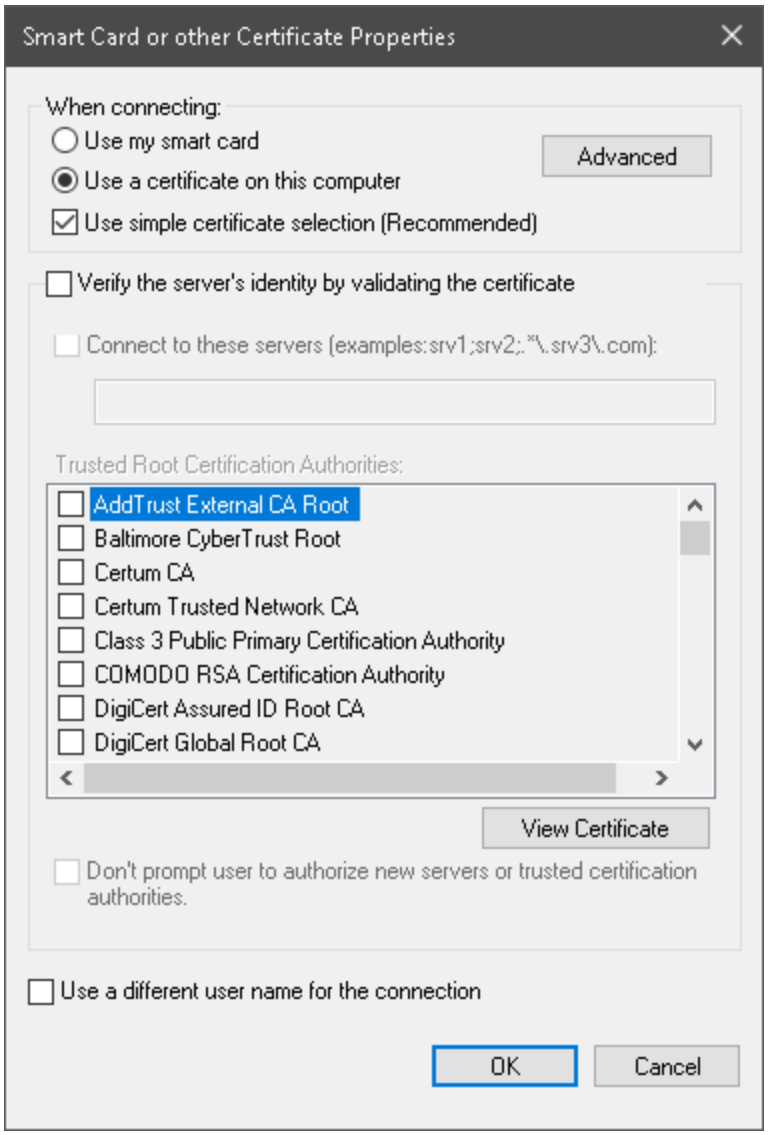


3. In the *Security* tab, set *Choose a network authentication method* to *Microsoft: Smart card or other certificates*, and select *Settings*.



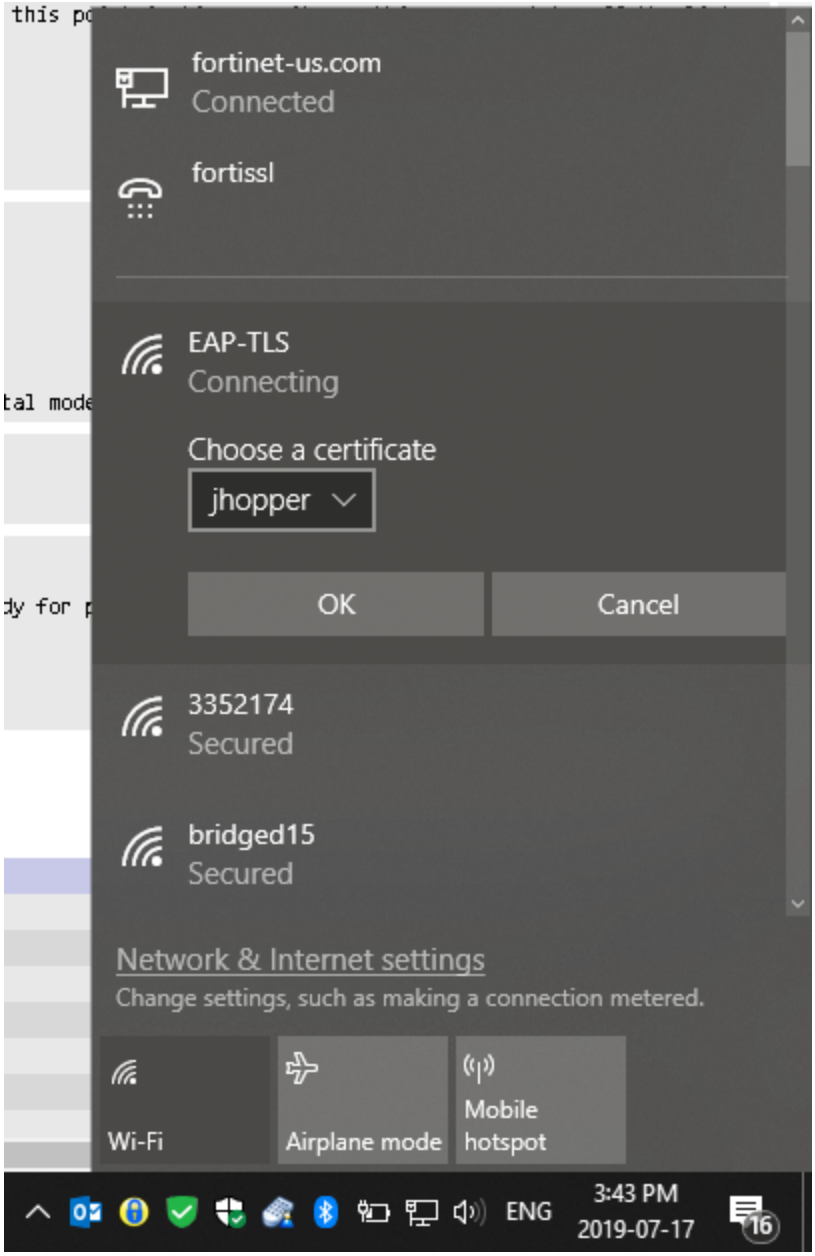
4. Enable both *Use a certificate on this computer* and *Use simple certificate selection*.
   Note that, for simplification purposes, *Verify the server's identity by validating the certificate* has been disabled. However EAP--TLS allows the client to validate the server as well as the server validate 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.

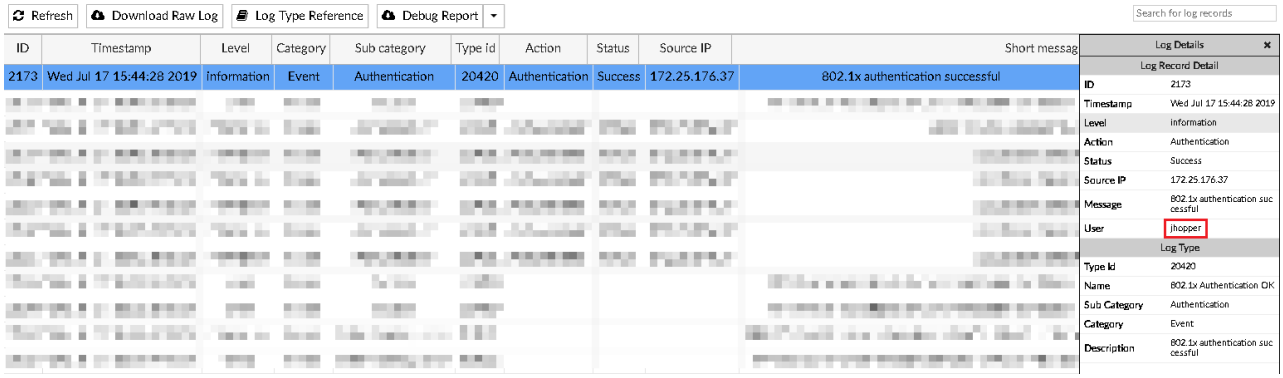

Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Advanced
Use simple certificate selection (Recommended)
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root 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
View Certificate
Don't prompt user to authorize new servers or trusted certification authorities.
Use a different user name for the connection
OK
Cancel

Results

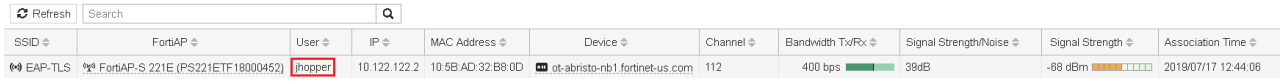
1. On the user's device, attempt to connect to the WiFi. Select the user's certificate and select *OK*.



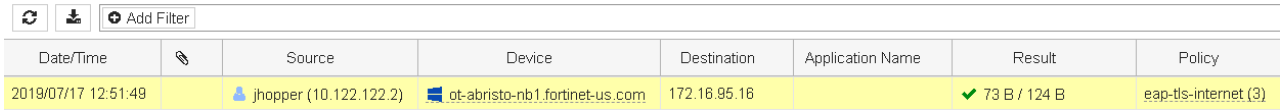
2. On the FortiAuthenticator, go to *Logging* > *Log Access* > *Logs* to confirm the successful authentication.

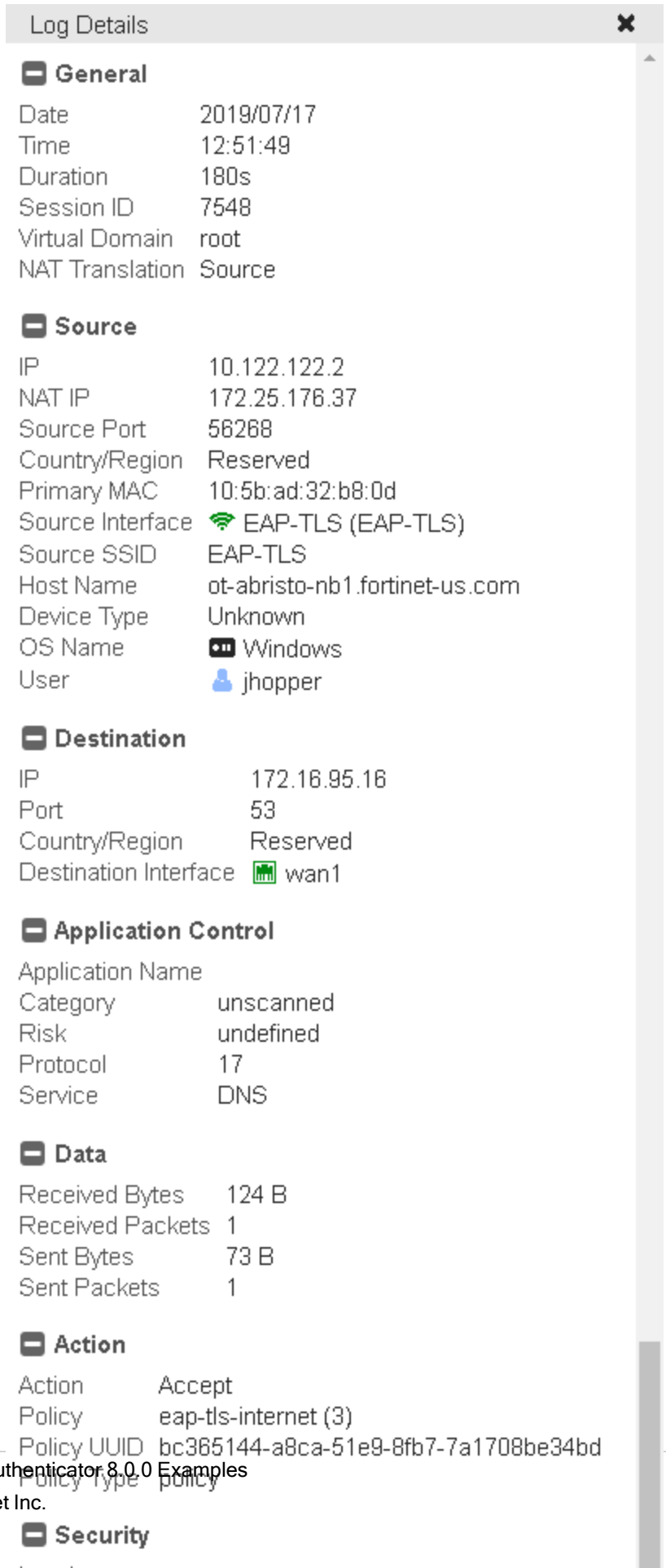


3. On the FortiGate, go to **Monitor > WiFi Client Monitor** to view various information about the client.



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

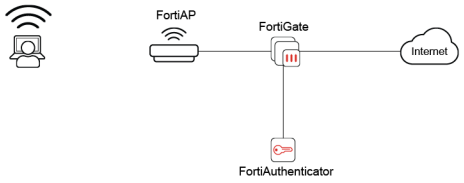



Log Details
General
Date 2019/07/17
Time 12:51:49
Duration 180s
Session ID 7548
Virtual Domain root
NAT Translation Source
Source
IP 10.122.122.2
NAT IP 172.25.176.37
Source Port 56268
Country/Region Reserved
Primary MAC 10:5b:ad:32:b8:0d
Source Interface EAP-TLS (EAP-TLS)
Source SSID EAP-TLS
Host Name 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.

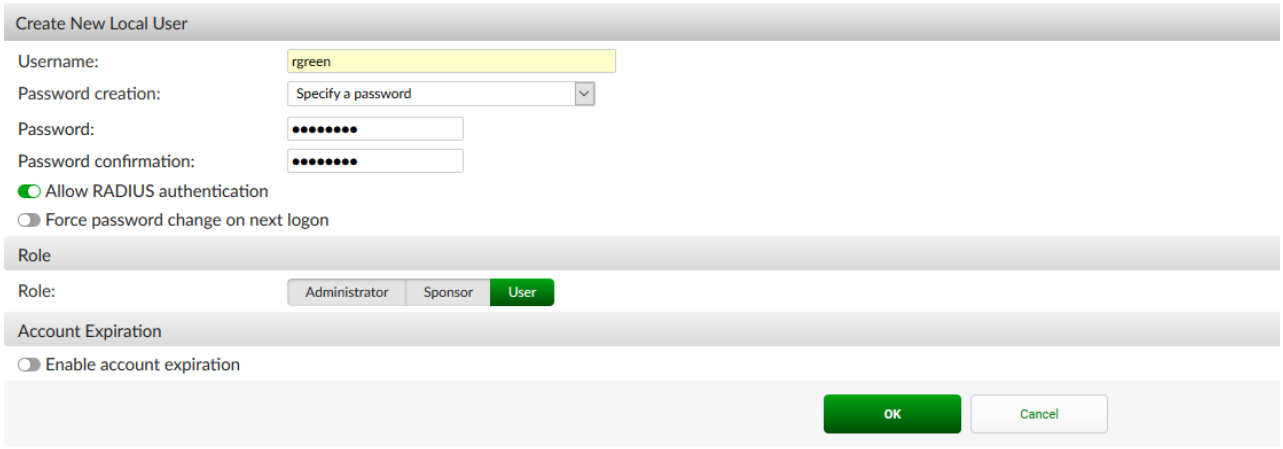
The RADIUS server is a FortiAuthenticator that is used authenticate users who belong to the employees user group.



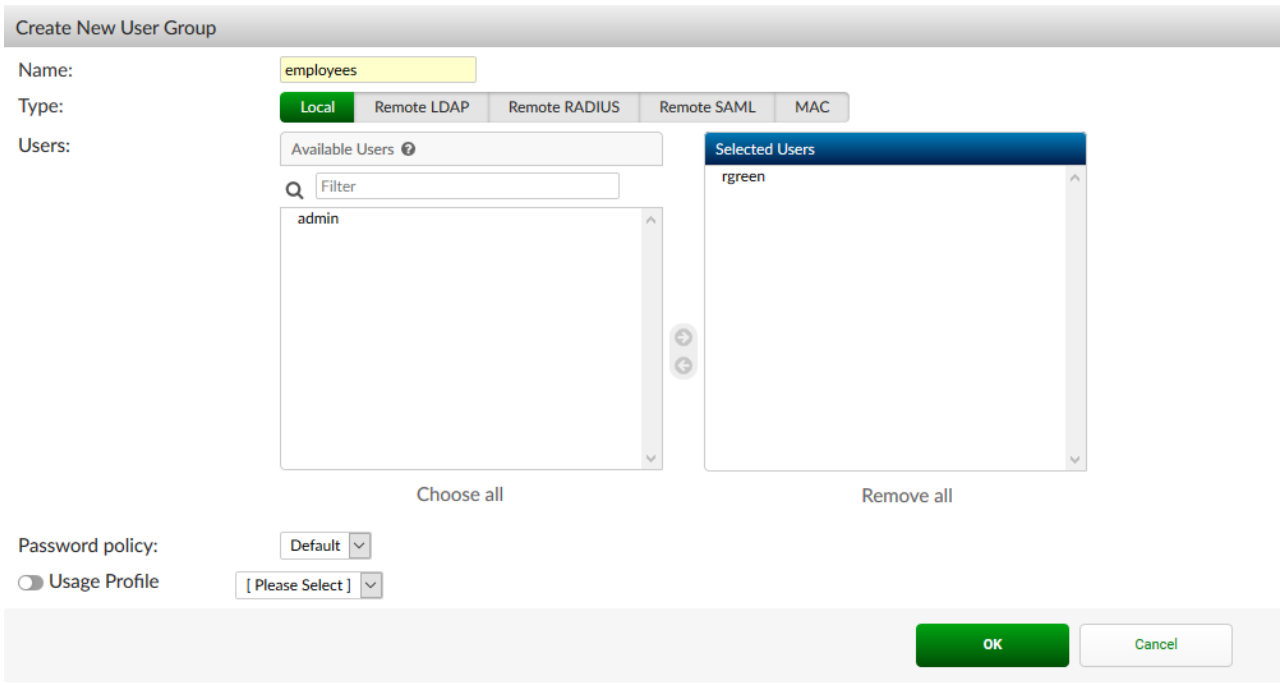
Creating users and user groups on the FortiAuthenticator

To create users and user groups:

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



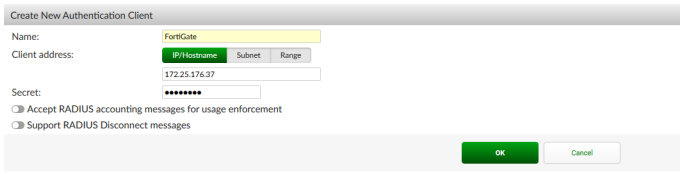
2. Then go to *Authentication > User Management > User Groups* and create a local user group (employees), adding the newly created user.



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.



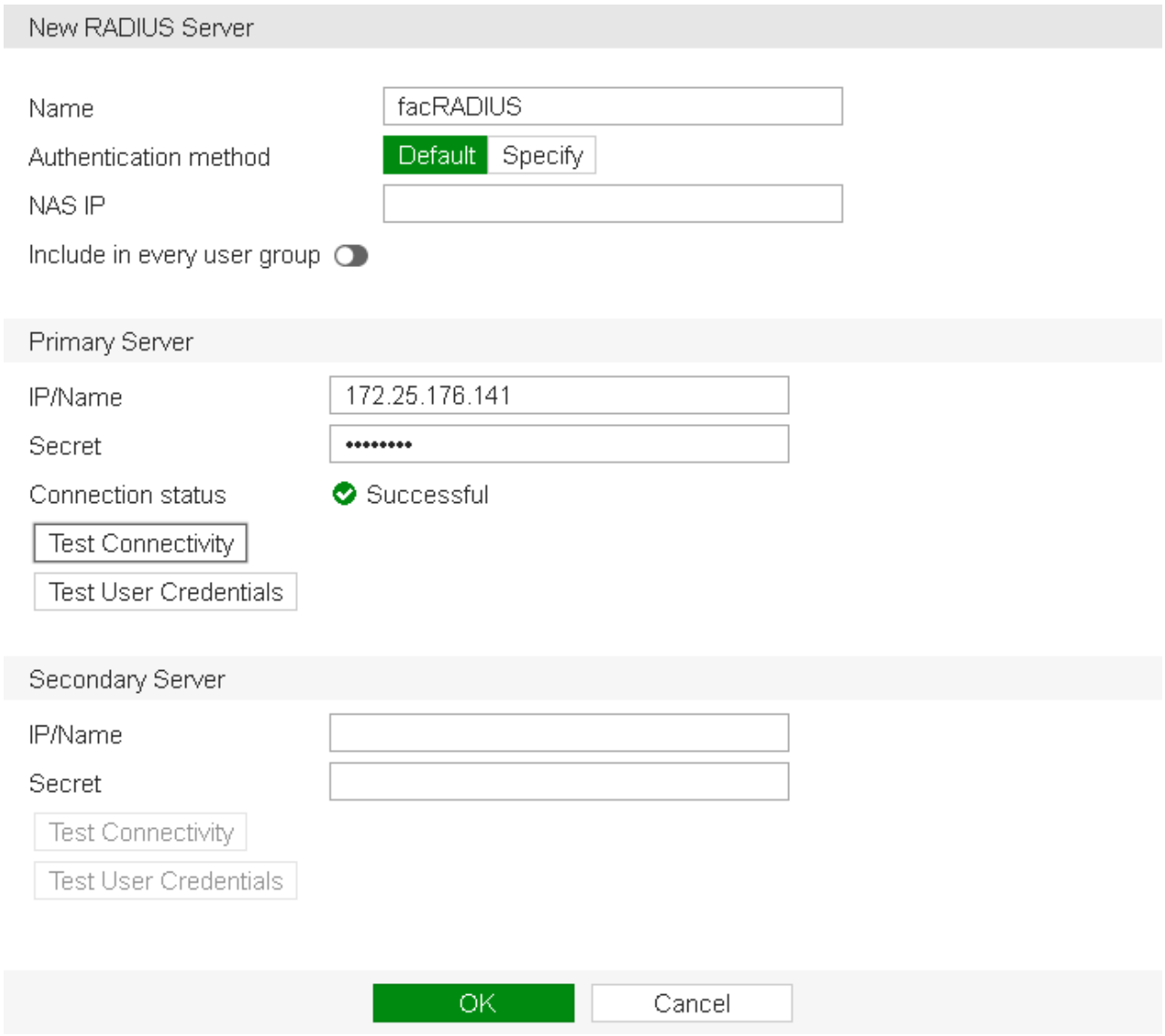
To create the RADIUS policy:

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:

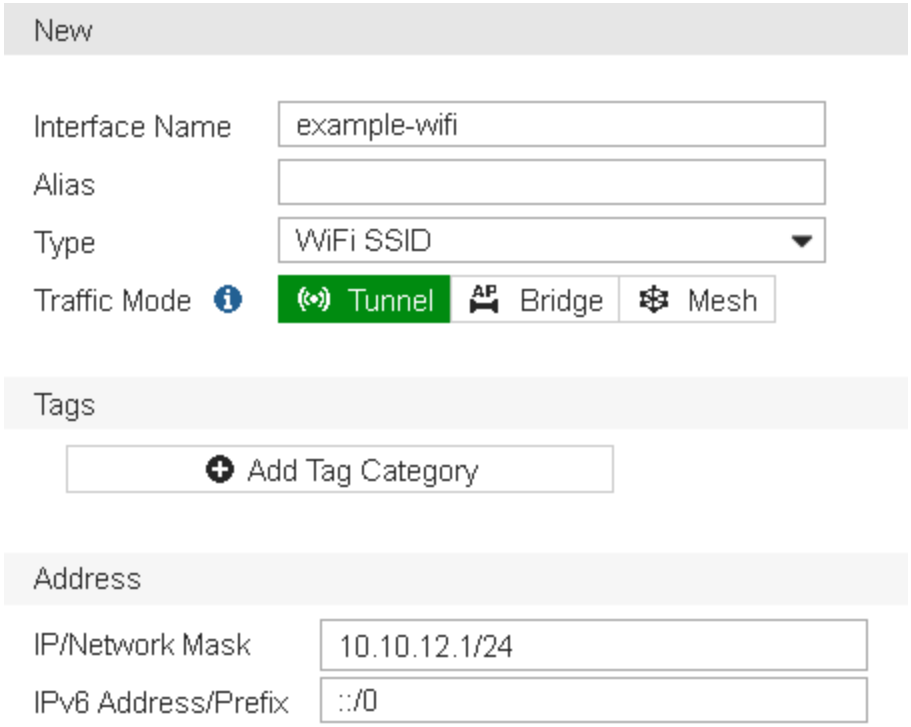
1. Go to *User & Device > RADIUS Servers* and add the FortiAuthenticator as a RADIUS server.
Select *Test Connectivity* to confirm the successful connection.



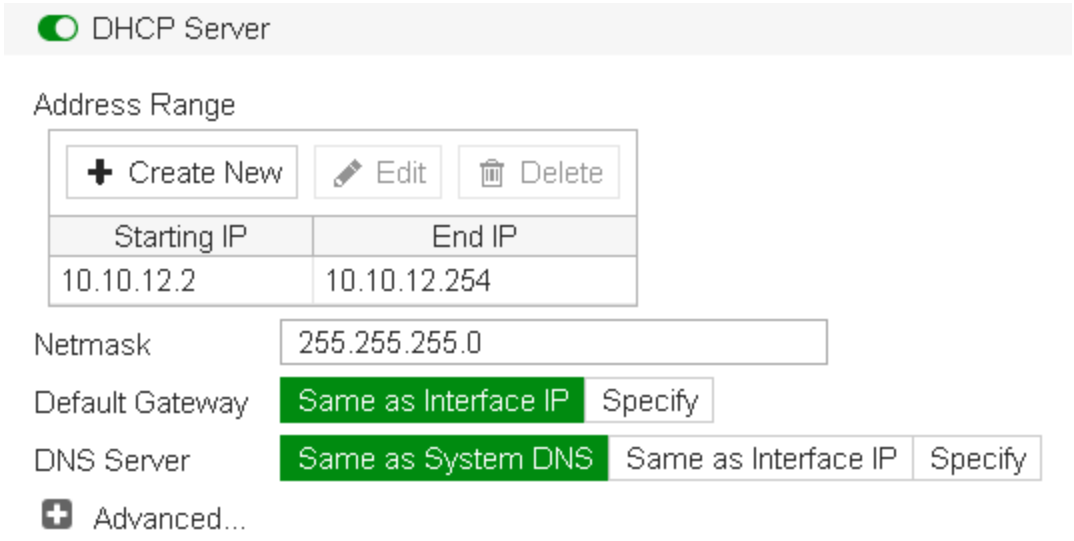
Creating SSID and set up authentication

To create an SSID and set up authentication:

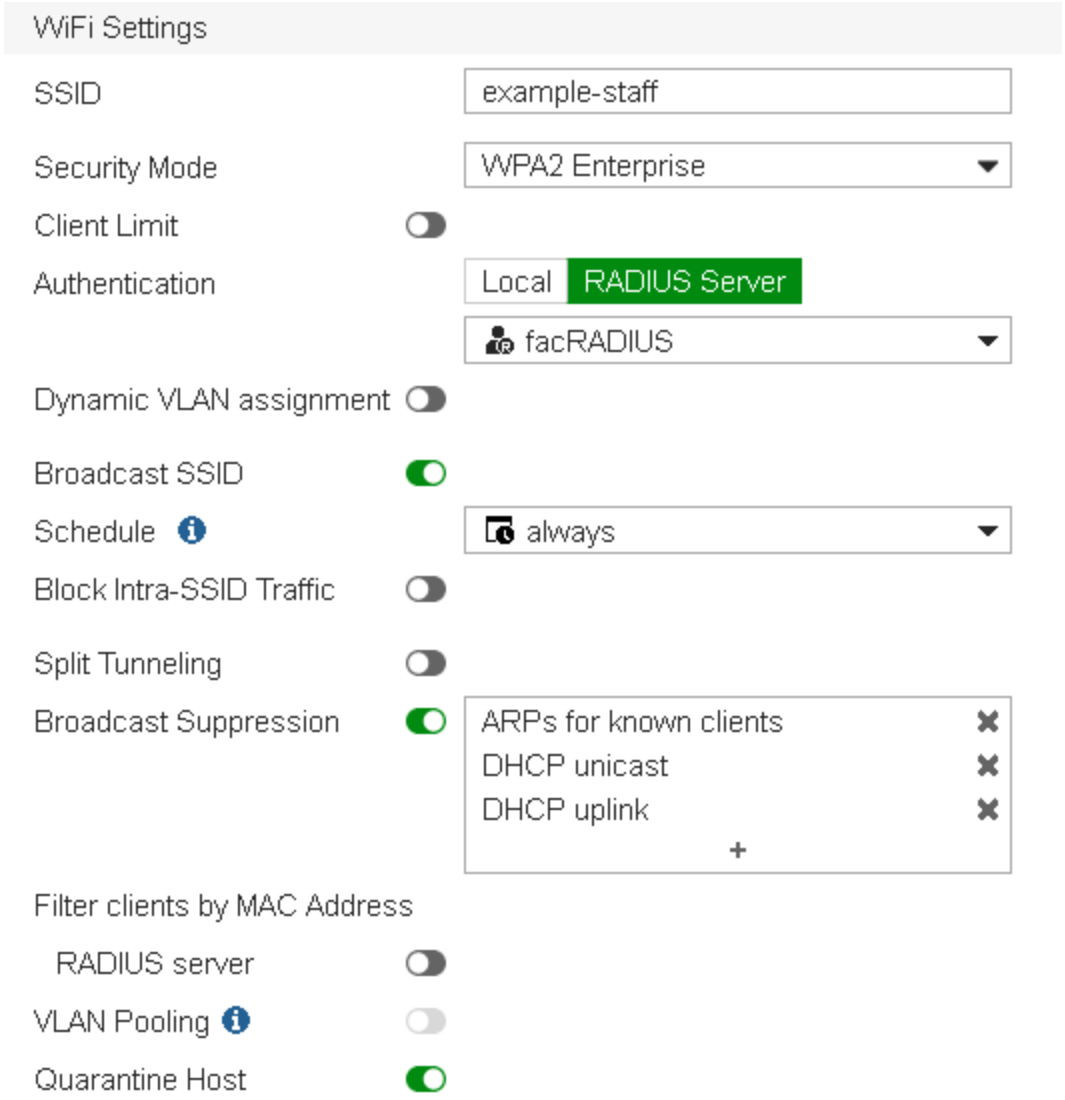
1. Go to *WiFi & Switch Controller* > *SSID* and define your wireless network.



2. Set up DHCP for your clients.



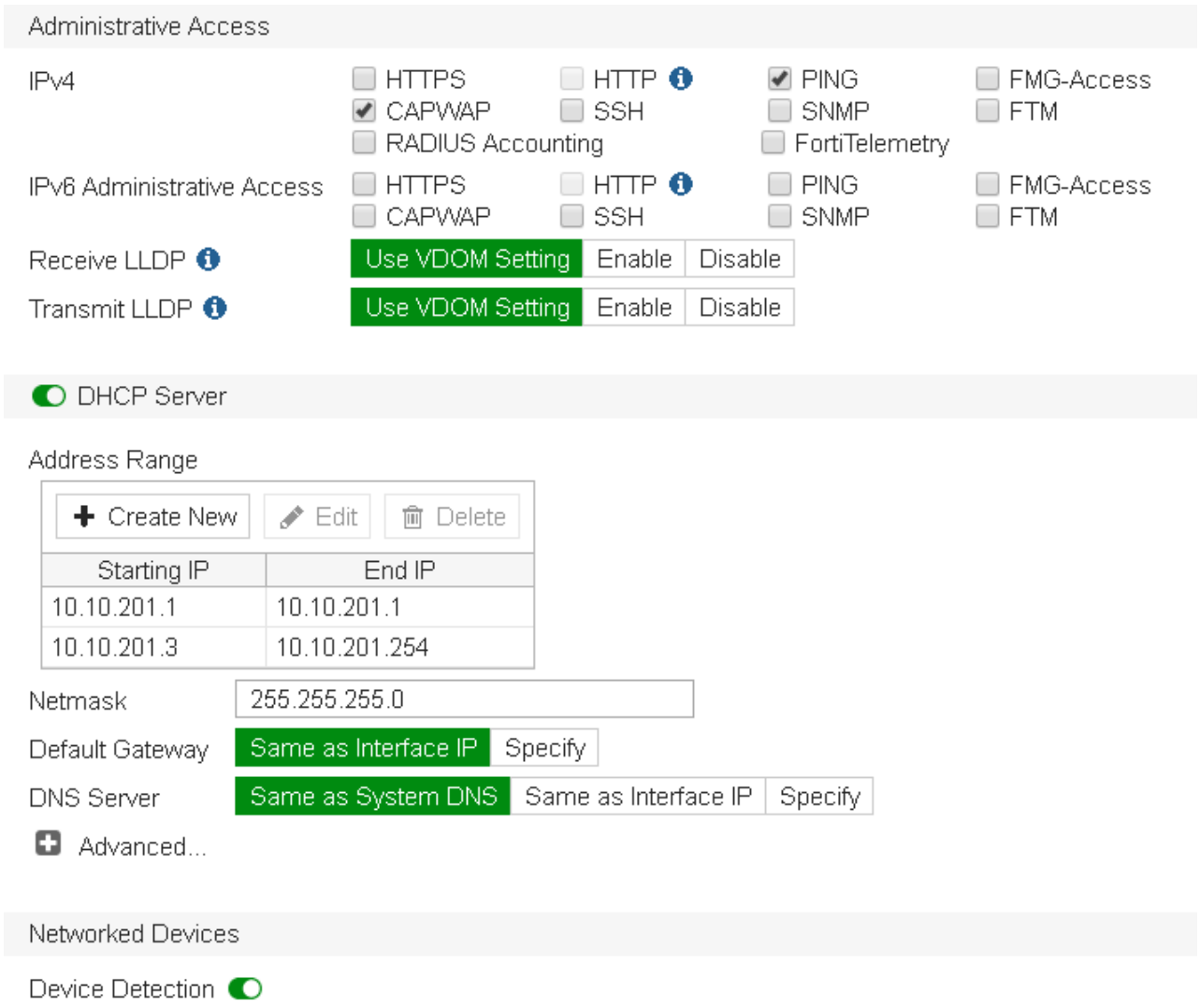
3. Configure WPA2 Enterprise security that uses the RADIUS server.



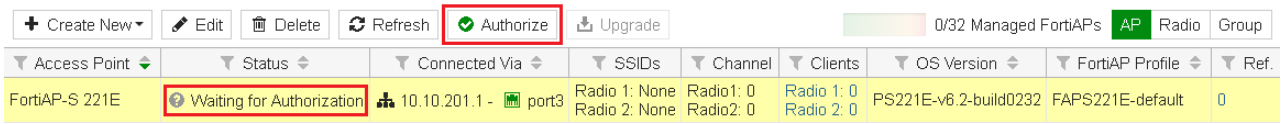
Connecting and authorizing the FortiAP

To connect and authorize the FortiAP:

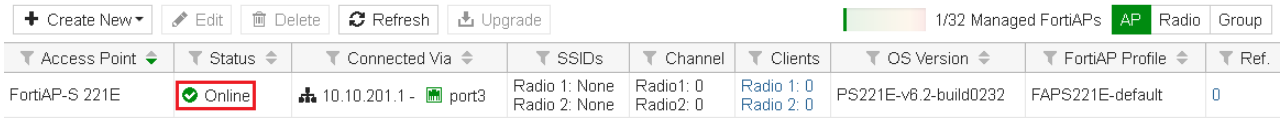
1. Go to *Network* > *Interfaces* and configure a dedicated interface for the FortiAP.
   Under *Administrative Access*, enable *PING* and *CAPWAP*, and enable *DHCP Server*.
   Under *Networked Devices*, enable *Device Detection*.



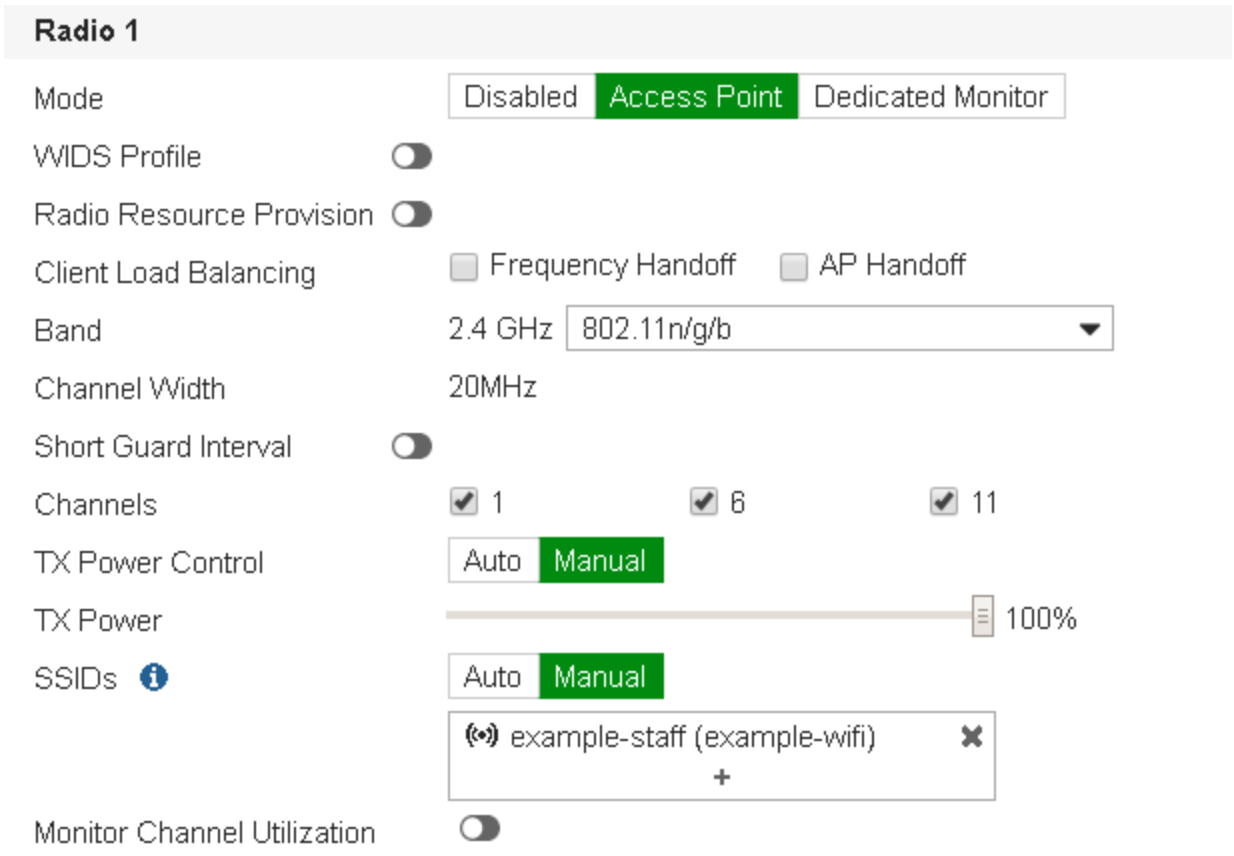
2. Connect the FortiAP unit to the interface. Then go to *WiFi & Switch Controller > Managed FortiAPs*. Notice the *Status* is showing *Waiting for Authorization*.
When the FortiAP is listed, select and *Authorize* it.



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



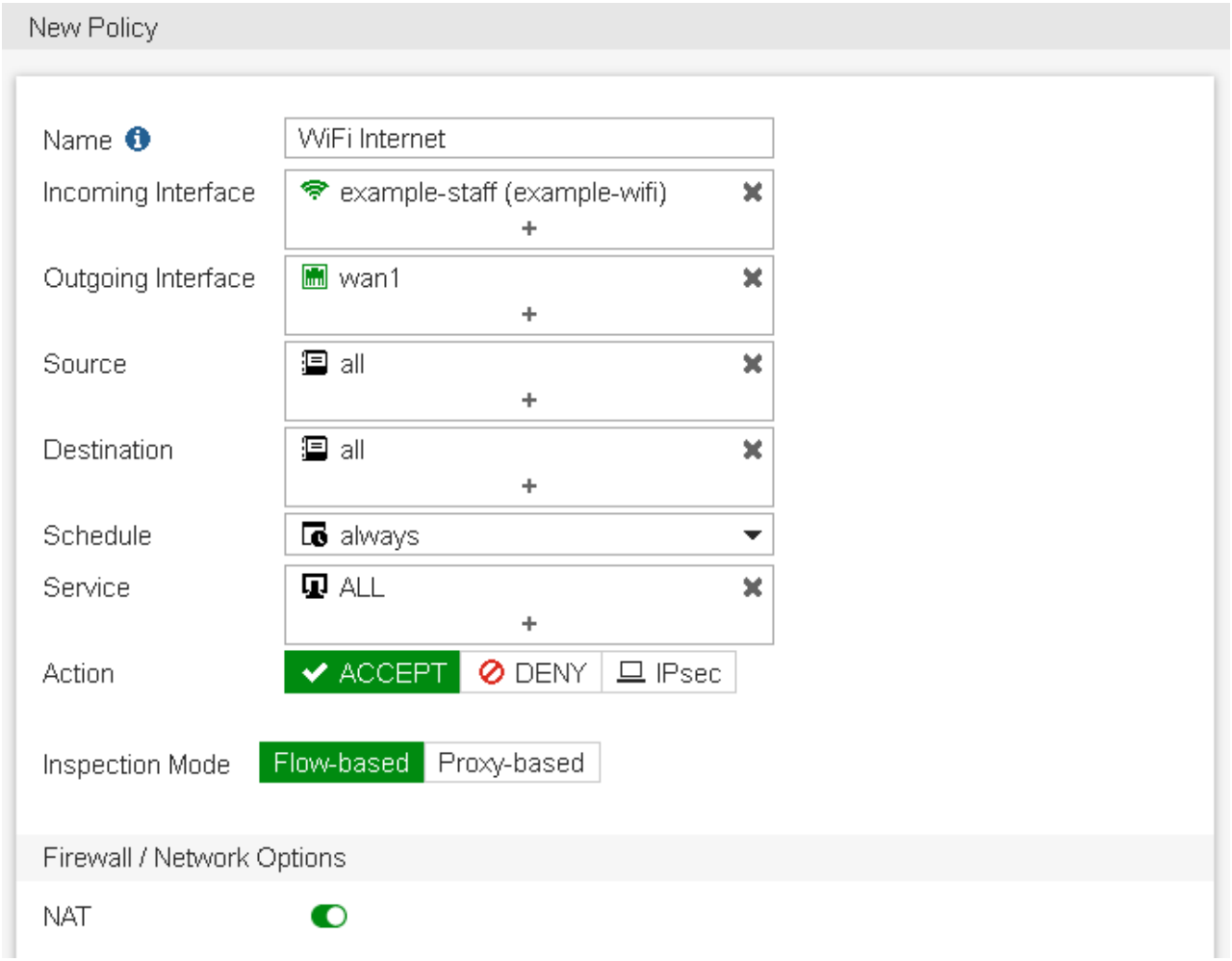
4. Go to *WiFi & Switch Controller > FortiAP Profiles* and edit the profile.
This example uses a FortiAP-S 221E, so the *FAPS221E-default* profile applies.
For each radio, make sure to select your *SSID*.


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

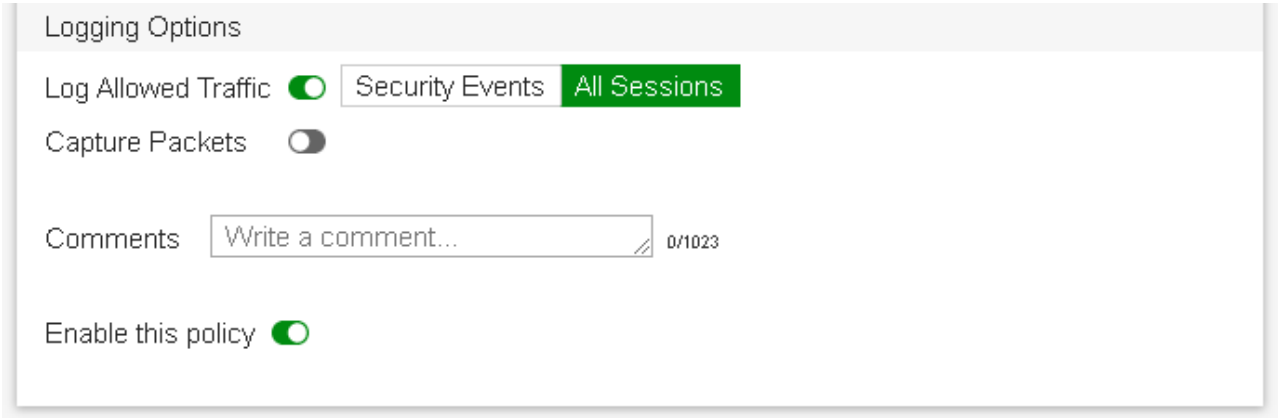
Creating the security policy

To create the security policy:

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

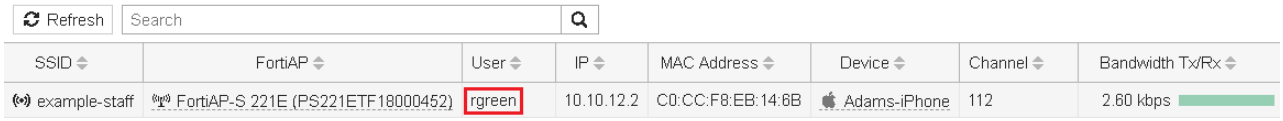


2. Under *Logging Options*, enable *Log Allowed Traffic* and *All Sessions*.



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.

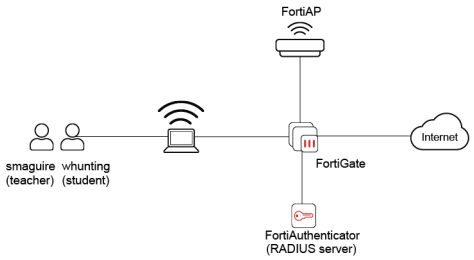


WiFi with WSSO using FortiAuthenticator RADIUS and Attributes

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 example 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.

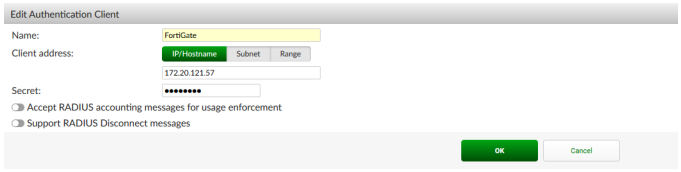
For this example, the student security policy applies a more restrictive web filter.



Registering the FortiGate as a RADIUS client on the FortiAuthenticator

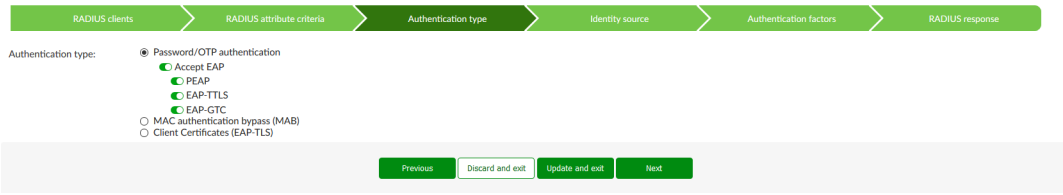
To create the RADIUS client:

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.



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.

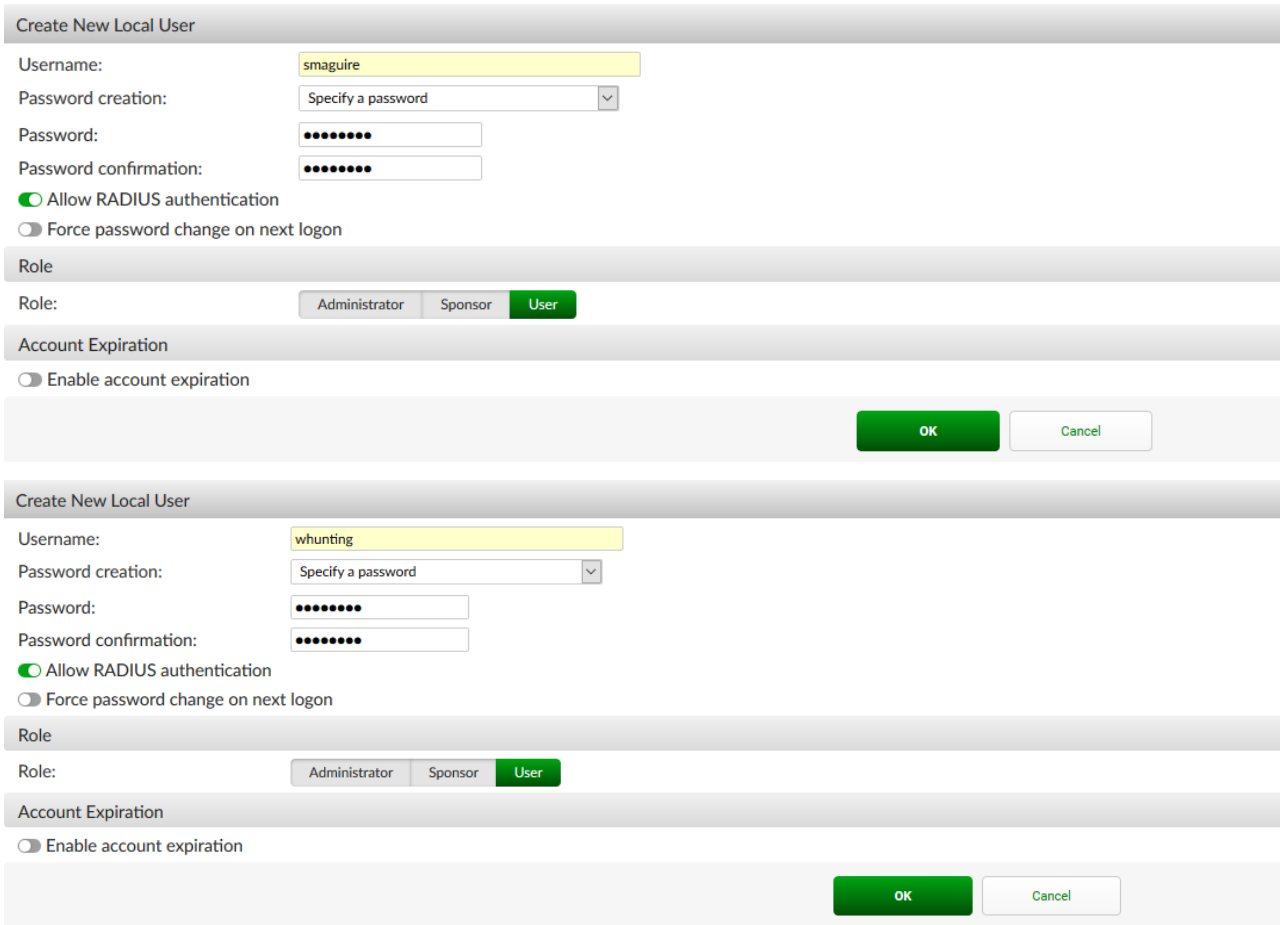


5. Choose a username format (in this example: *username@realm*), select the *Local* realm.
6. Review the remaining configurations, and click *Save and Exit*.

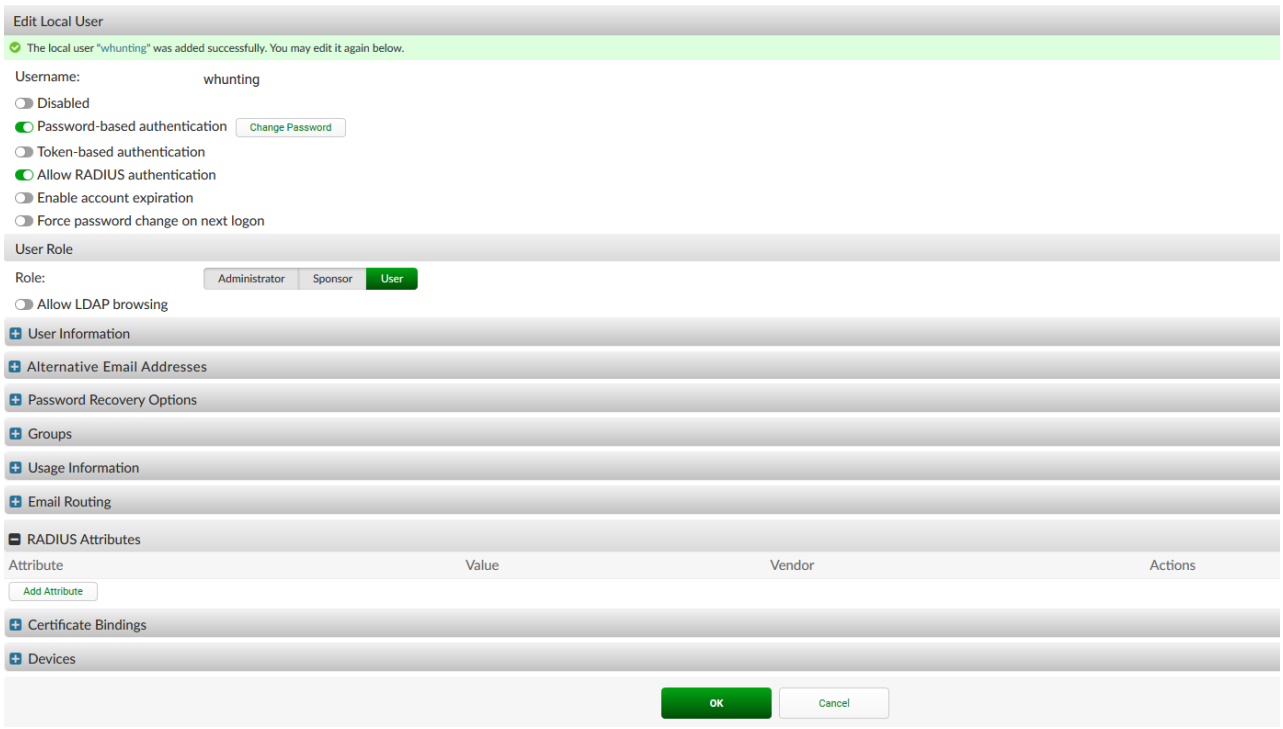
Creating users on the FortiAuthenticator

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*).



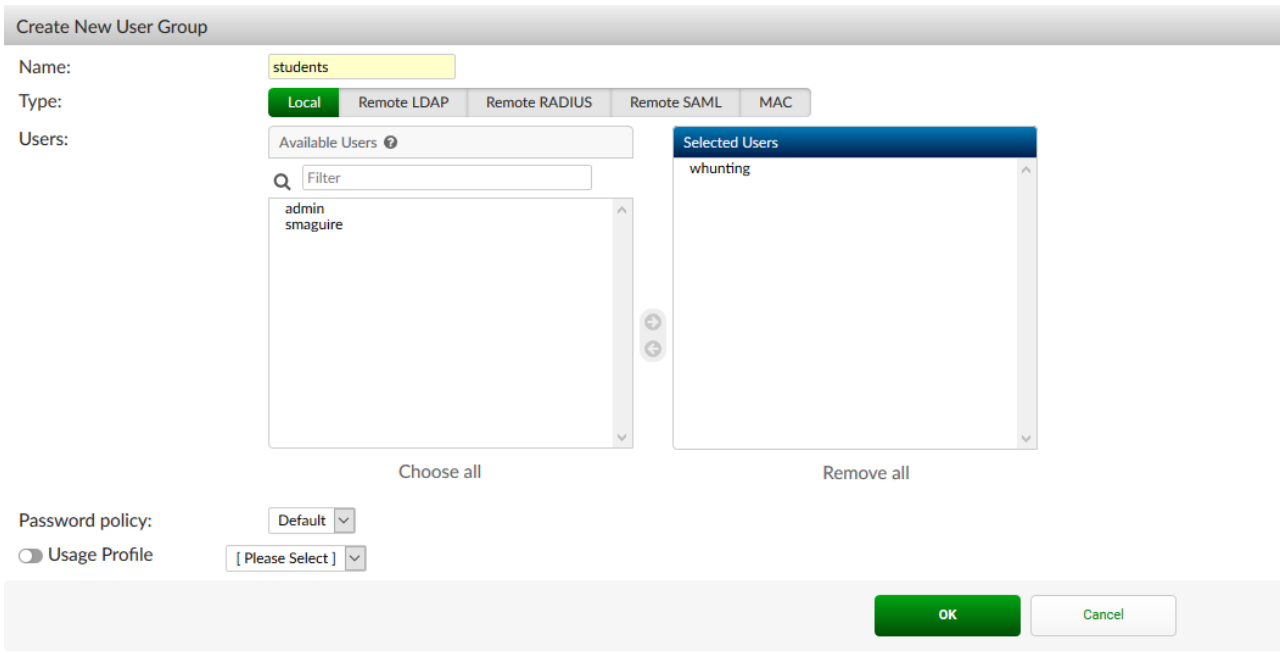
2. Note that, after you create the users, *RADIUS Attributes* appears as an option.
   If your configuration involves multiple users, it is more efficient to add RADIUS attributes in their respective user groups, in the next step.



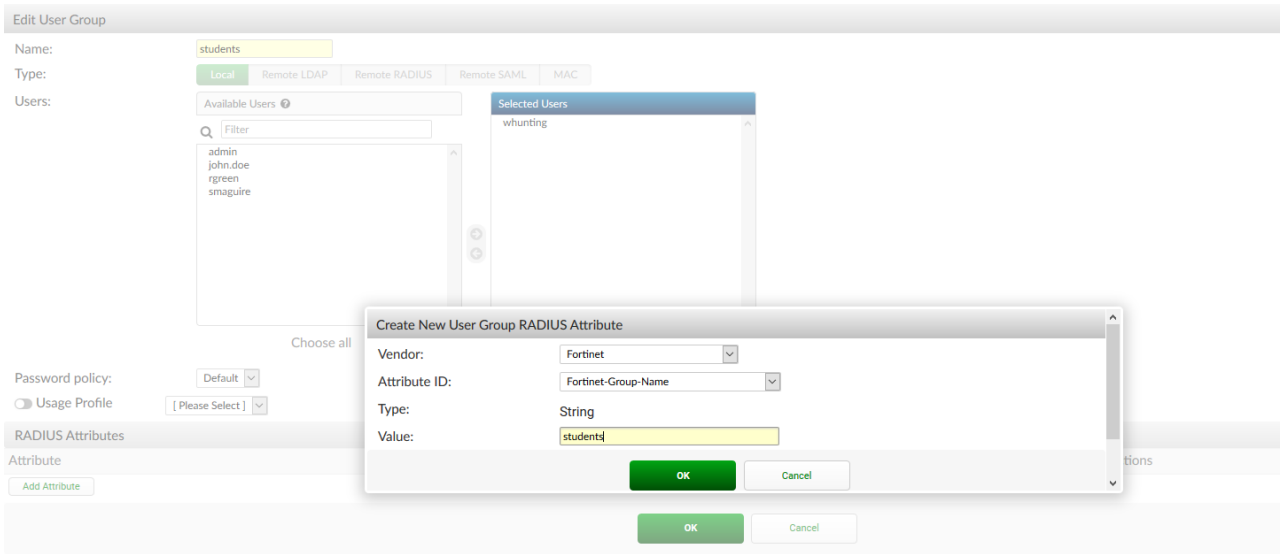
Creating user groups on the FortiAuthenticator

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.



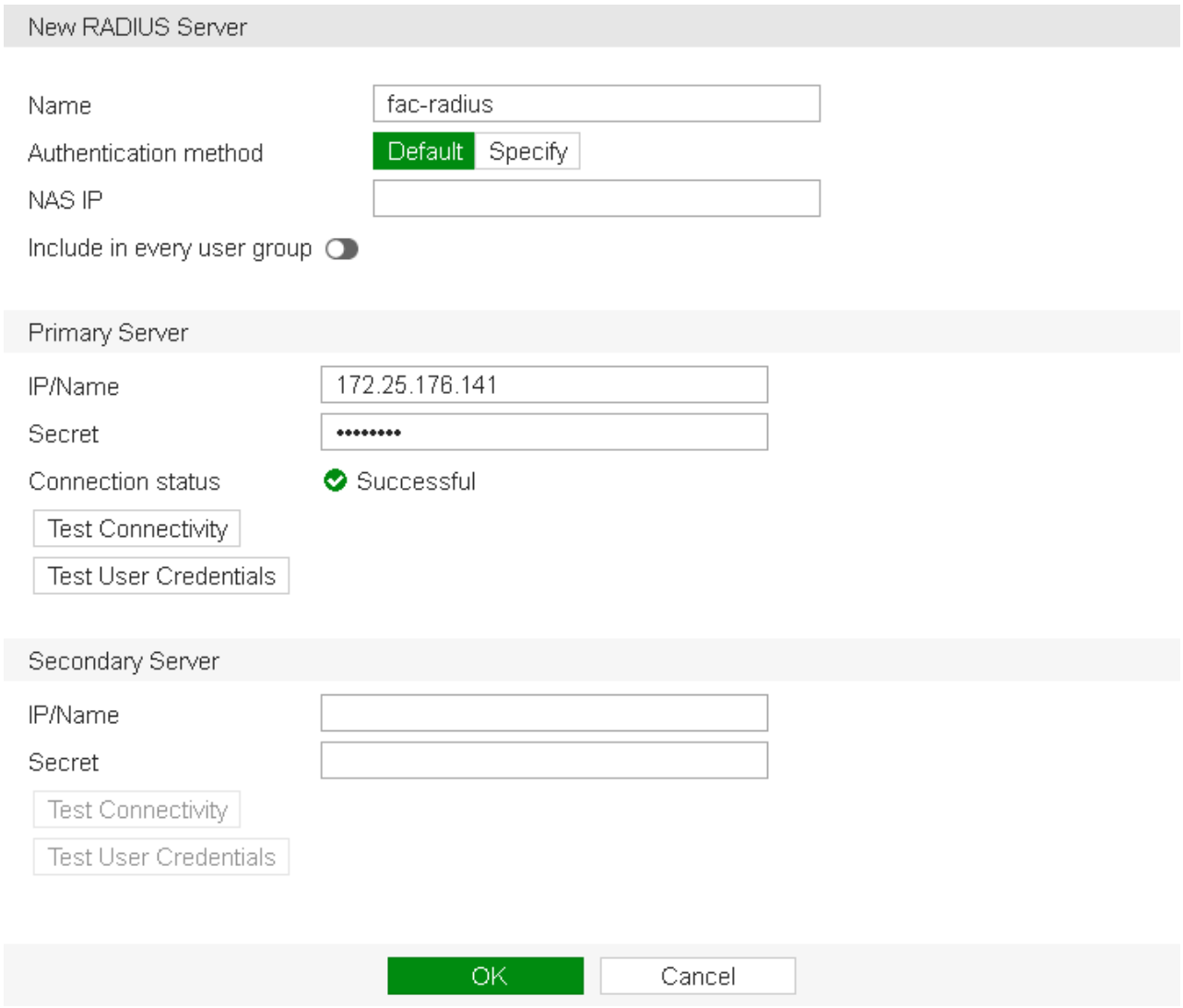
2. Once created, edit both user groups and select *Add Attribute*.
3. Add the *Fortinet-Group-Name* RADIUS attribute to each group, which specifies the user group name to be sent to the FortiGate.



Configuring the FortiGate to use the FortiAuthenticator as the RADIUS server

To configure the FortiGate to use the FortiAuthenticator RADIUS server:

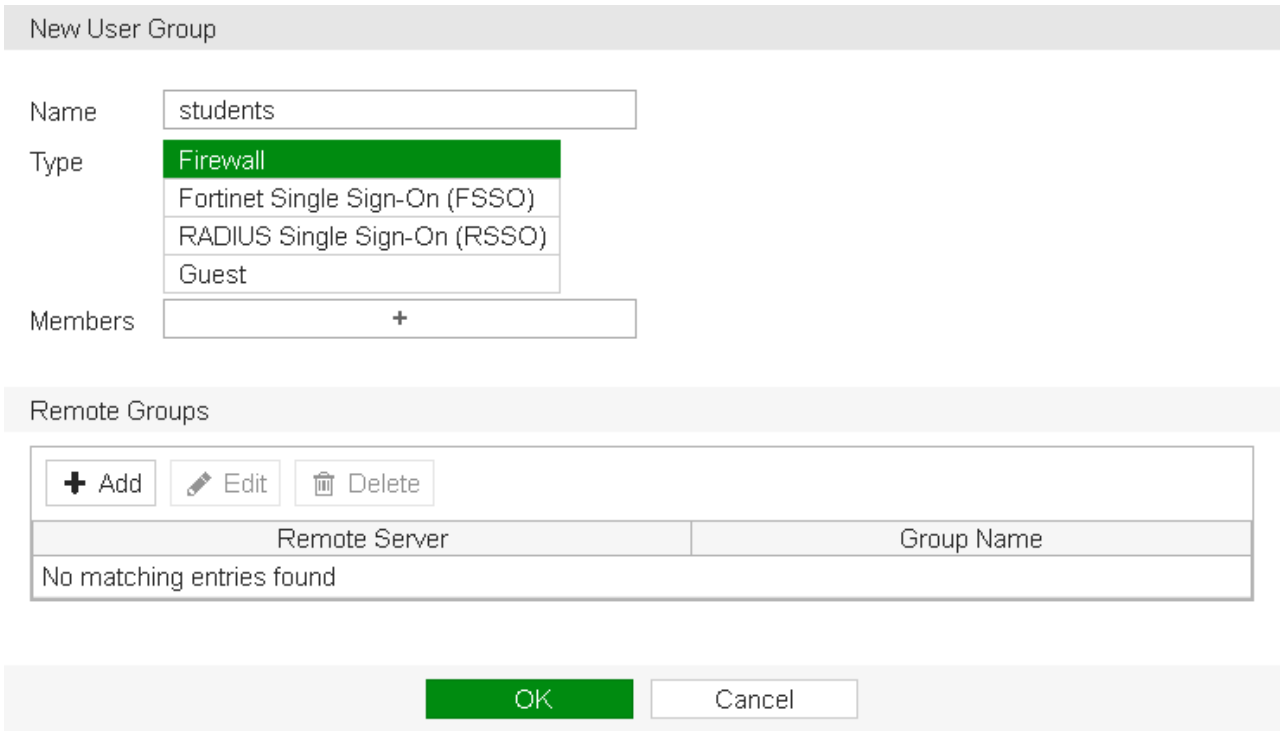
1. On the FortiGate, go to *User & Device > RADIUS Servers* and select *Create New*.
   Enter a *Name*, the Internet-facing IP address of the FortiAuthenticator, and enter the same *Primary Server Secret* entered on the FortiAuthenticator.
   Select *Test Connectivity* to confirm the successful connection.



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.

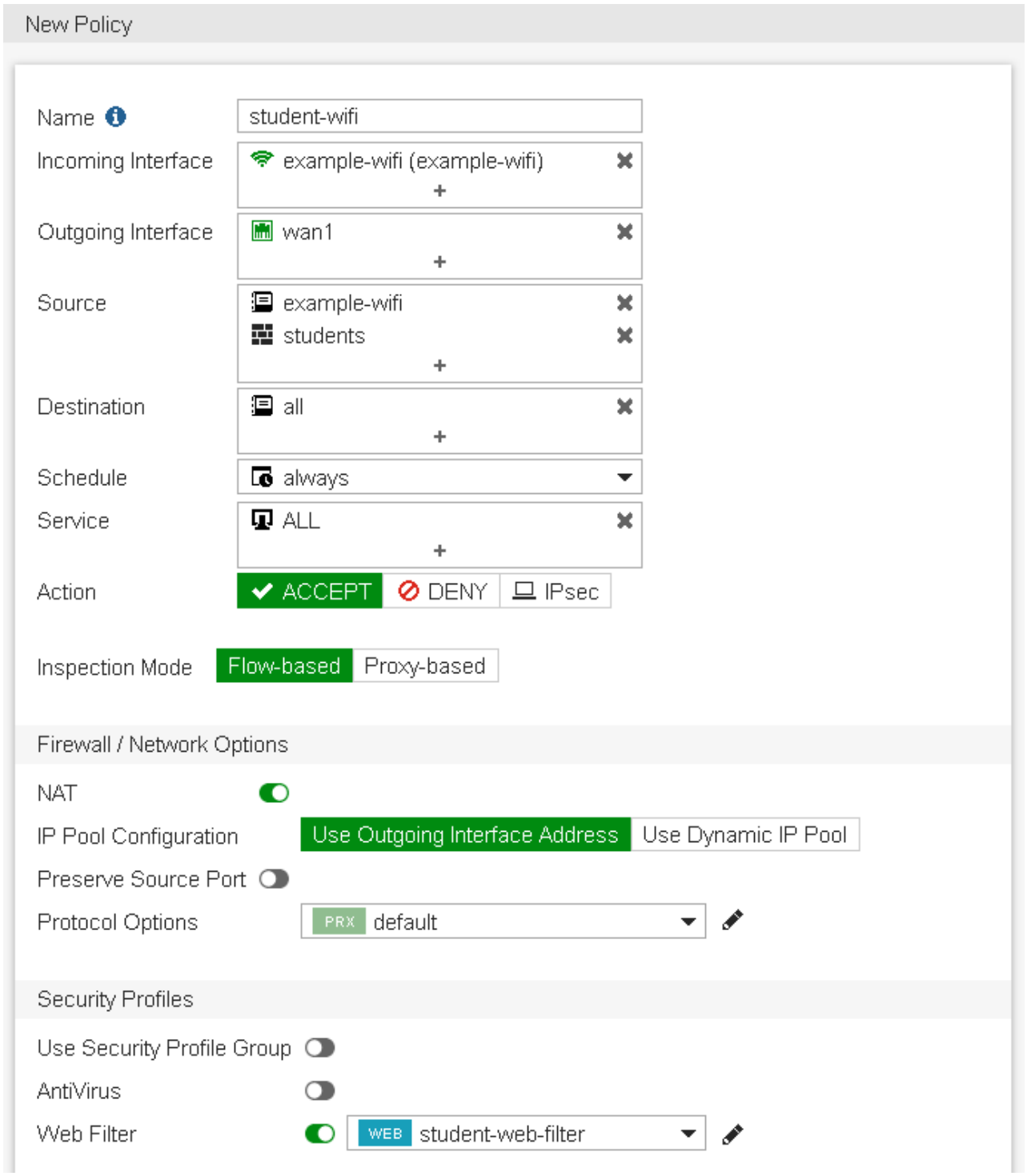


Do not add any members to either group.

Creating security policies

To create a security policy:

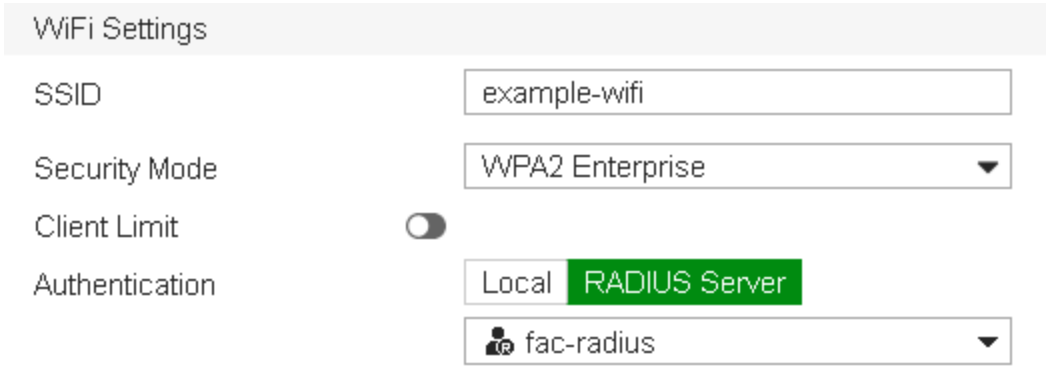
1. Go to *Policy & Objects* > *IPv4 Policy* and select *Create New*.
   Create two policies (*student-wifi* and *teacher-wifi*) with WiFi-to-Internet access: one policy with *Source* set to the *students* user group, and the other set to *teachers*. Make sure to add the SSID address (*example-wifi*) 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
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
Use Security Profile Group
AntiVirus
Web Filter
WEB
student-web-filter

Configuring the SSID to RADIUS authentication

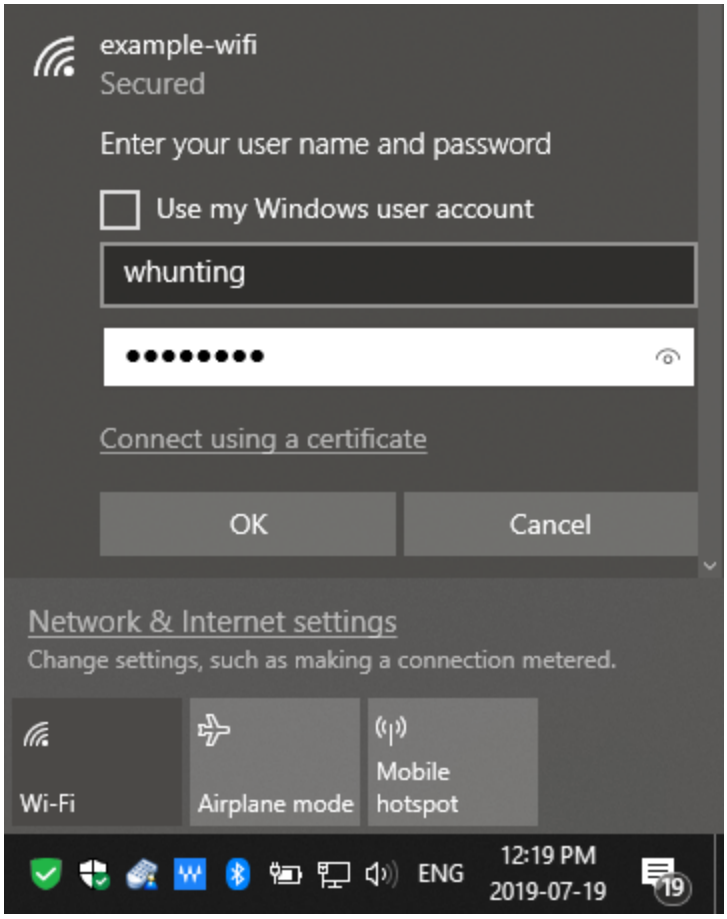
To configure the SSID to RADIUS authentication:

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

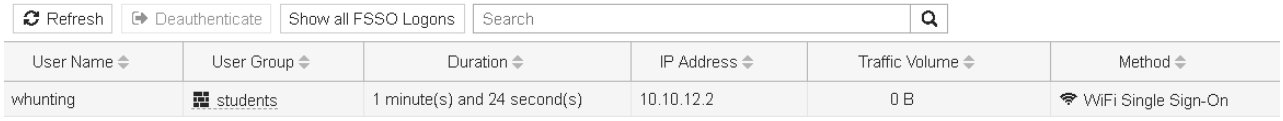


Results

1. Connect to the WiFi network as a student.



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.

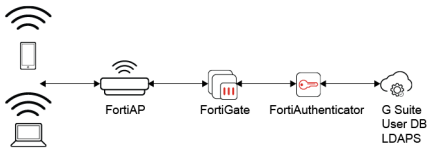


802.1X authentication using FortiAuthenticator with Google Workspace User Database

This example 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.

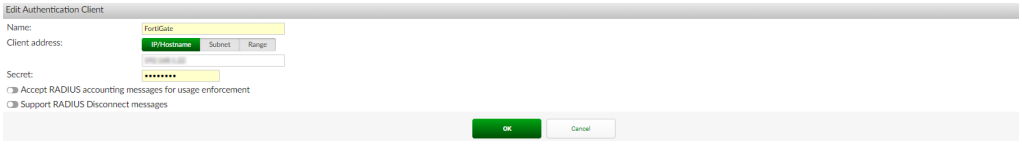
To configure 802.1X authentication using FortiAuthenticator with Google Workspace User Database:

1. Configuring FortiGate as a RADIUS client on page 372.
2. Configuring Google Workspace as an LDAP server. See Google Workspace integration using LDAP on page 412.
3. Creating a realm and RADIUS policy with EAP-TTLS authentication on page 373.
4. Configuring FortiAuthenticator as a RADIUS server in FortiGate on page 374.
5. Configuring a WPA2-Enterprise with FortiAuthenticator as the RADIUS server on page 374.
6. Configuring Windows or macOS to use EAP-TTLS and PAP on page 375.

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.



Creating a realm and RADIUS policy with EAP-TTLS authentication

To create a realm for the Google Workspace LDAP server:

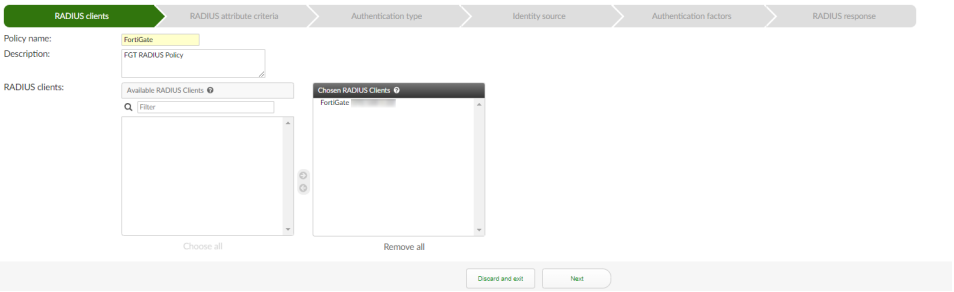
1. Go to *Authentication > User Management > Realms*, click *Create New*.
2. Enter a *Name* for the realm.

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

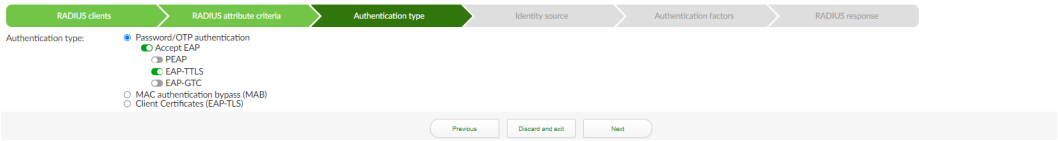
3. Select the previously set Google Workspace LDAP server for the realm from the *User source* dropdown.
4. Click *OK* to create the new realm.

To create a RADIUS policy:

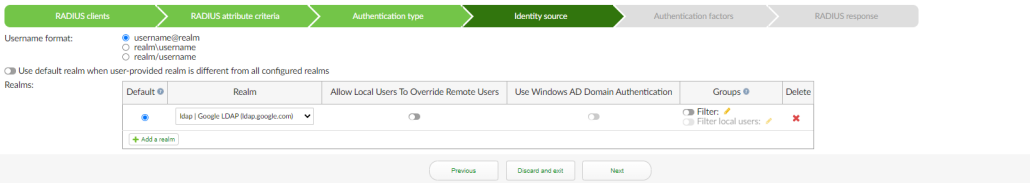
1. In *Authentication > RADIUS Service > Policies*, click *Create New*.
2. For RADIUS clients, enter an identifiable policy name and description, and add the newly created RADIUS client to the policy. Click *Next*.



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*.



   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*.

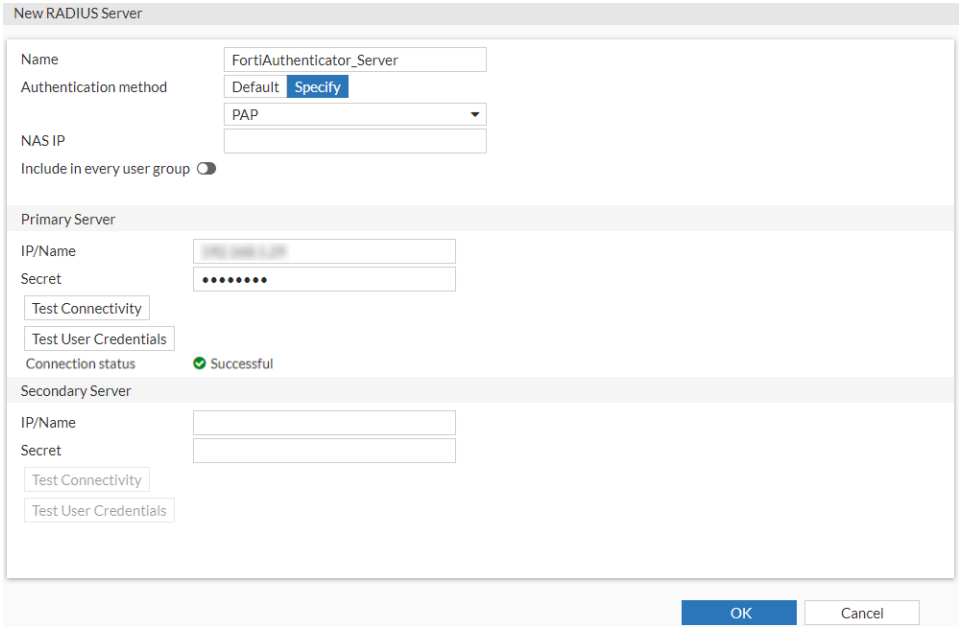


5. For *Authentication factors*, select *Every configured password and OTP factors*, and click *Next*.
   In this menu you can also enable the option to *Allow FortiToken Mobile push notifications*.
6. For *RADIUS response*, review the policy, and click *Save and exit*.

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.



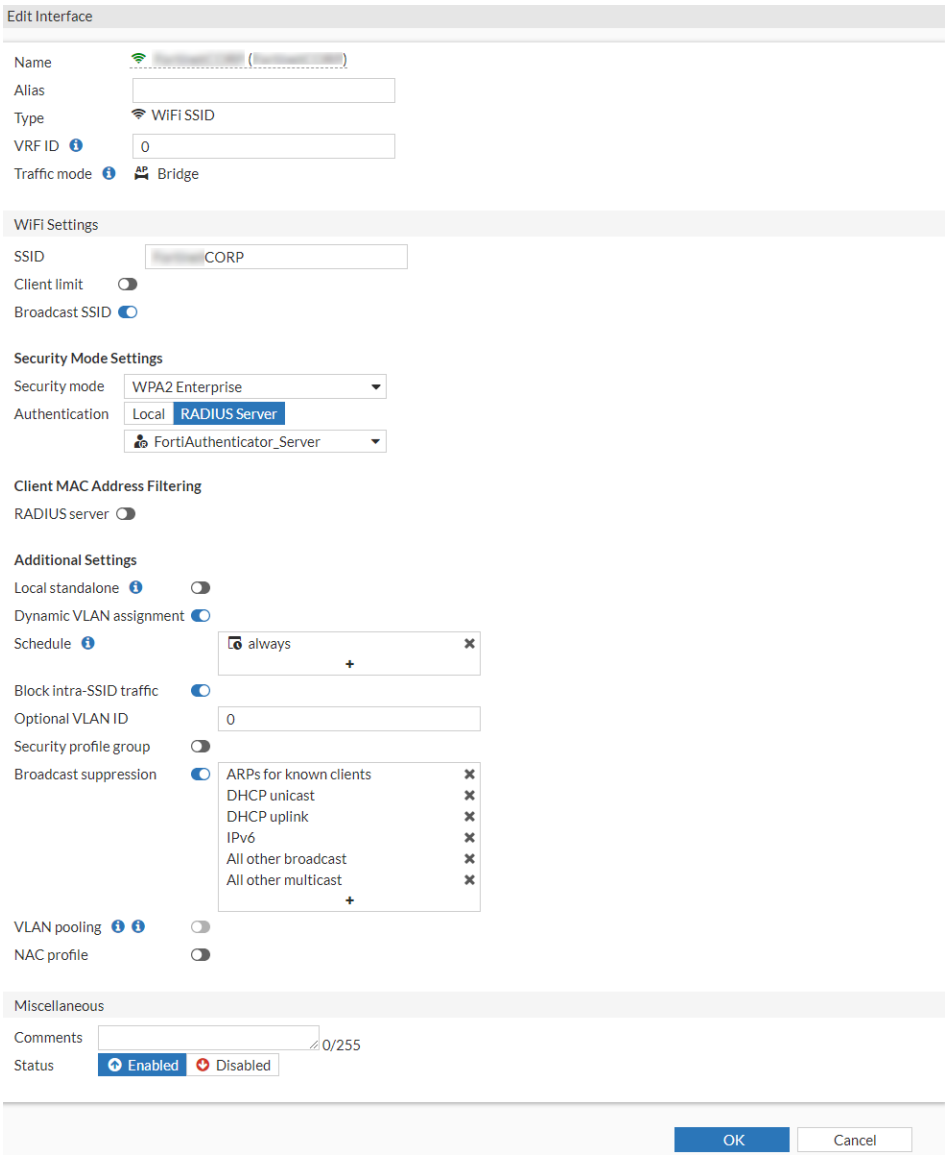
Configuring a WPA2-Enterprise with FortiAuthenticator as the RADIUS server

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.

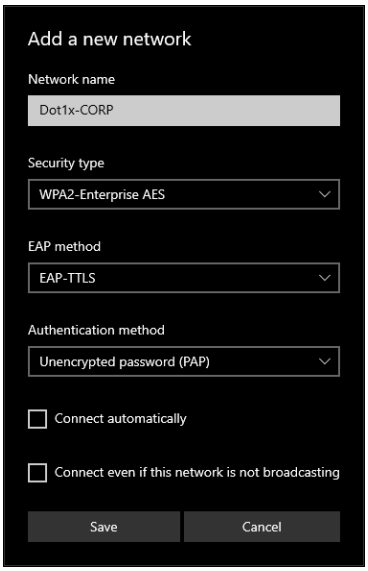


Configuring Windows or macOS to use EAP-TTLS and PAP

To configure Windows to use EAP-TTLS and PAP:

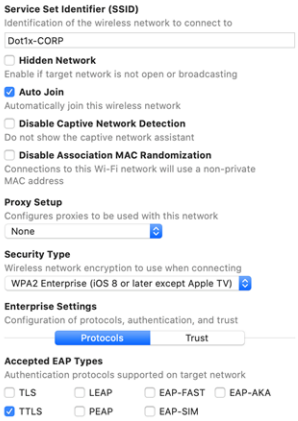
1. Go to *Settings > Network & Internet*.
2. Select the *Wi-Fi* tab, and click *Manage known networks*.
3. Select *Add a new network*.

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*.



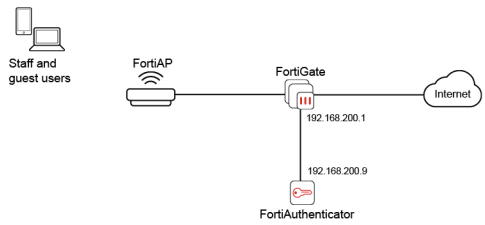
To configure macOS to use EAP-TTLS and PAP:

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*.



Guest portals with FortiAuthenticator

FortiAuthenticator as a Wireless Guest Portal for FortiGate



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

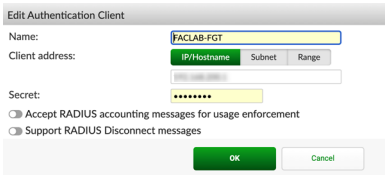
To set up FortiAuthenticator as a wireless guest portal:

1. Configuring FortiGate as a RADIUS client on page 377.
2. Creating a user group on FortiAuthenticator for guest users on page 378.
3. Creating a guest portal on FortiAuthenticator on page 378.
4. Configuring an access point on FortiAuthenticator on page 379.
5. Configuring a captive portal policy on FortiAuthenticator on page 379.
6. Configuring FortiAuthenticator as a RADIUS server on FortiGate on page 381.
7. Creating a guest group on FortiGate on page 381.
8. Creating a wireless guest SSID on FortiGate on page 382.
9. Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet on page 384.
10. Configuring firewall authentication portal settings on FortiGate on page 384.

Configuring FortiGate as a RADIUS client

To configure FortiGate as a RADIUS client:

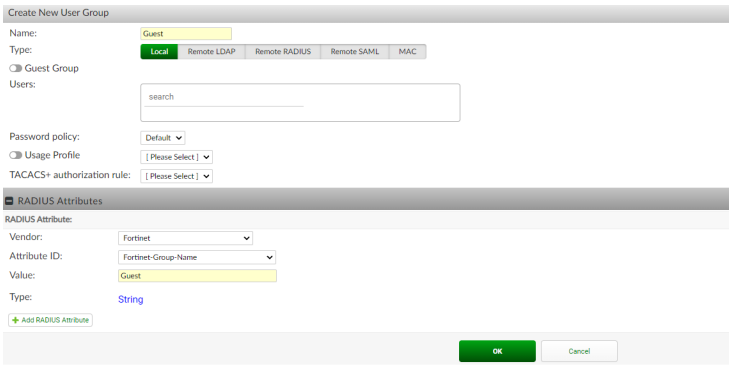
1. In *Authentication > RADIUS Service > Clients*, click *Create New*.
2. Enter a unique name for the RADIUS client and the IP address from which it will be connecting.
   This is the IP address of the RADIUS client itself, here, FortiGate, not the IP address of the end-user's device.
   You may enter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



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*.

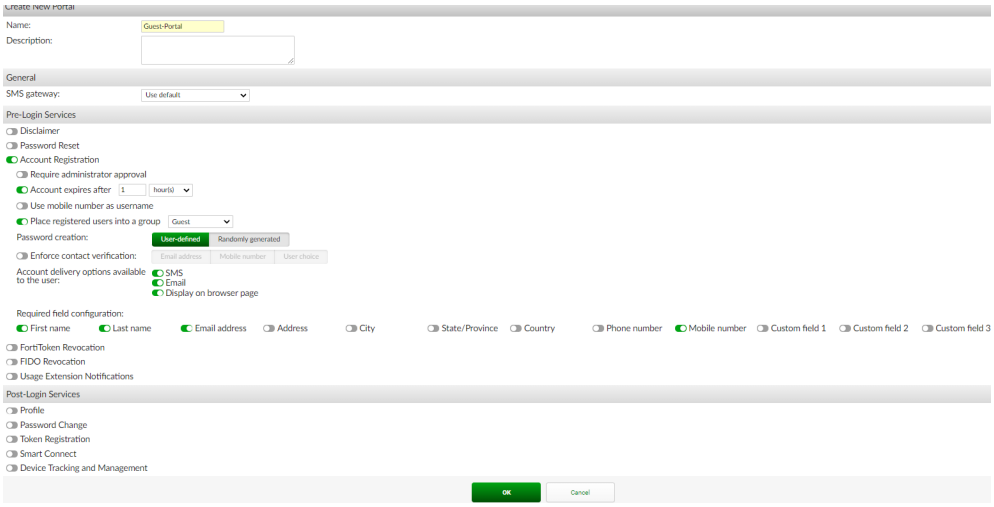


Creating a guest portal on FortiAuthenticator

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*.



Configuring an access point on FortiAuthenticator

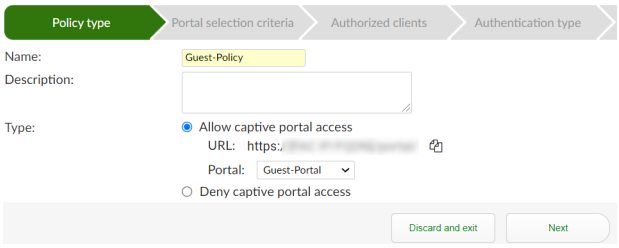
To configure an access point:

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 add a range of client IP address.
4. Click *OK*.
   For more information, see Access points in the latest *FortiAuthenticator Administration Guide*.

Configuring a captive portal policy on FortiAuthenticator

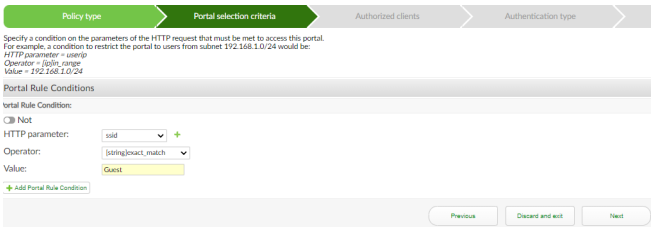
To configure an allow access captive portal policy:

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 378.
   d. Click *Next*.

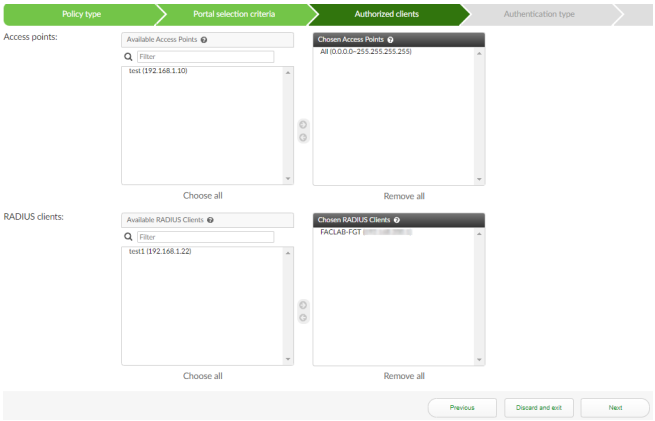


3. In the *Portal selection criteria* tab:

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*.

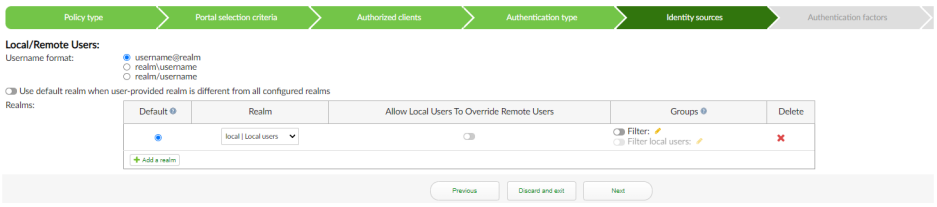


4. In the *Authorized clients* tab:
a. From *Access points*, select the access point defined in Access points.
b. From *RADIUS clients*, select the FortiGate RADIUS client defined in RADIUS clients.
c. Click *Next*.



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*.

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*.

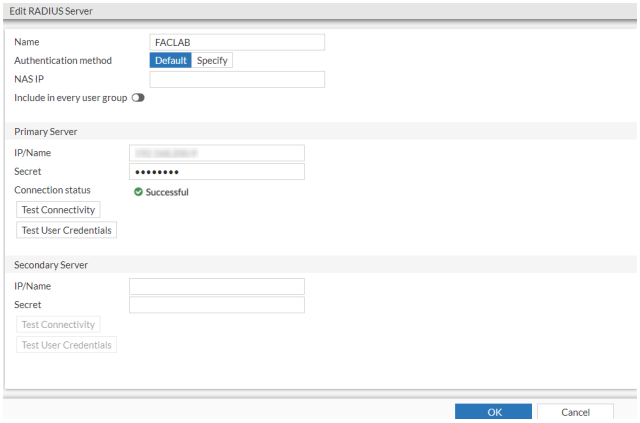


7. In the *Authentication Factors* tab, click *Next*.
8. In the *RADIUS response* tab, review the policy, and click *Save and exit*.

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.

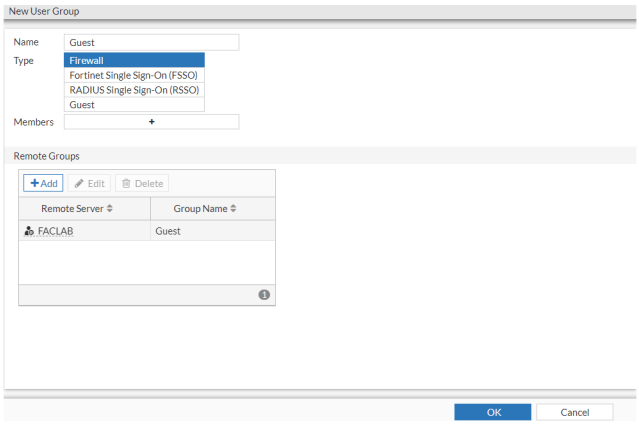


Creating a guest group on FortiGate

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*.

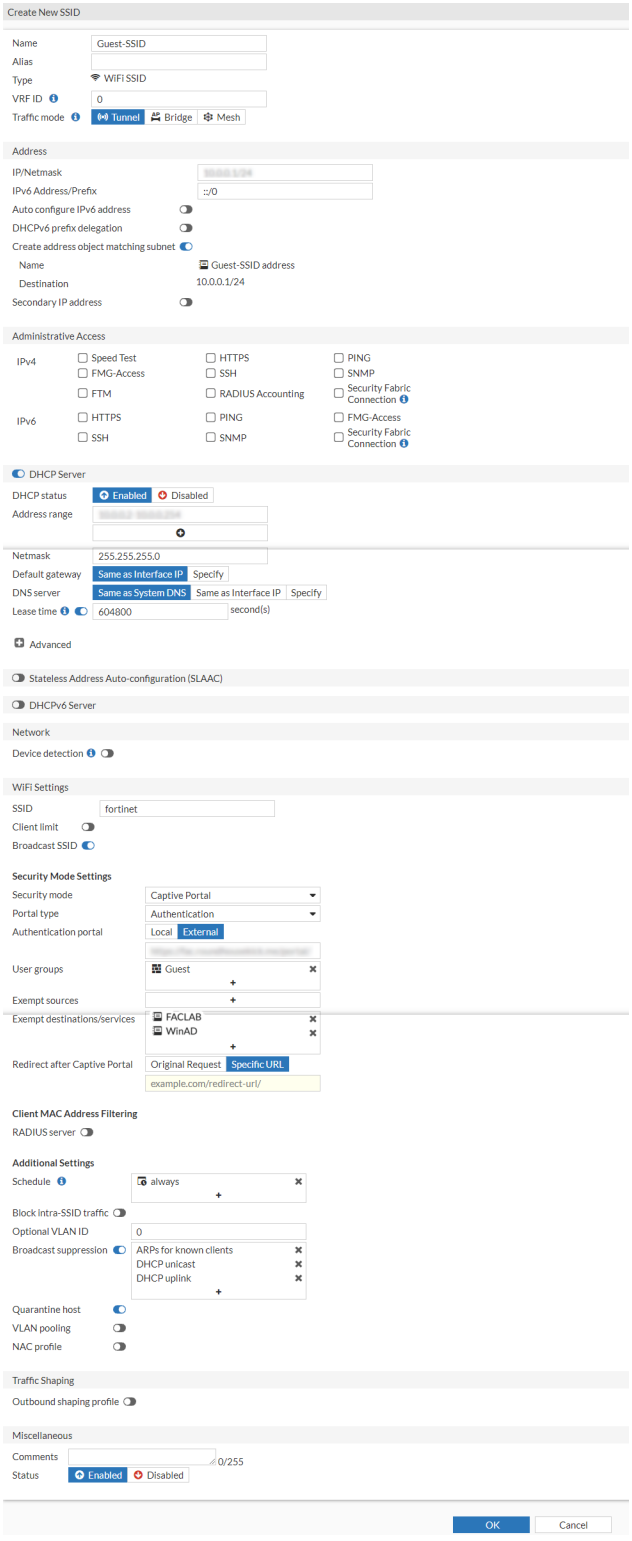


Creating a wireless guest SSID on FortiGate

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
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
FMG-Access
FTM
HTTPS
SSH
RADIUS Accounting
PING
SNMP
Security Fabric Connection
IPv6
HTTPS
SSH
PING
SNMP
FMG-Access
Security Fabric Connection
DHCP Server
DHCP status
Enabled
Disabled
Address range
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
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
OK
Cancel

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:

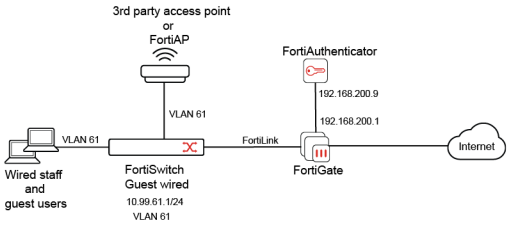
```
config firewall auth-portal
  set portal-addr <addr> #portal-addr setting must be an FQDN that resolves to the interface
        IP address of the guest SSID. The client must be able to resolve this using the DNS
        server configured in the DHCP scope.
end
```

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 {http | https} #http coupled with auth-secure-http is a safe choice and
       should not be disabled except in a few environments.
  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 example walks you through setting up FortiAuthenticator as a wired guest portal.

The example 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:

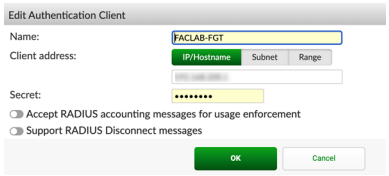
1. Configuring FortiGate as a RADIUS client on page 386.
2. Creating a user group on FortiAuthenticator for guest users on page 386.
3. Creating a guest portal on FortiAuthenticator on page 387.
4. Configuring an access point on FortiAuthenticator on page 388.

5. Configuring a captive portal policy on FortiAuthenticator on page 388.
6. Configuring FortiAuthenticator as a RADIUS server on FortiGate on page 389.
7. Creating a guest group on FortiGate on page 390.
8. Creating a wired guest interface on FortiSwitch on page 390.
9. Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet on page 392.
10. Configuring firewall authentication portal settings on FortiGate on page 393.

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.



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
```

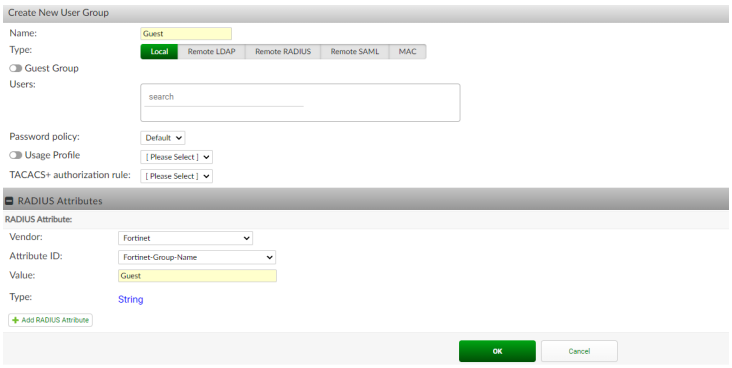
Creating a user group on FortiAuthenticator for guest users

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.

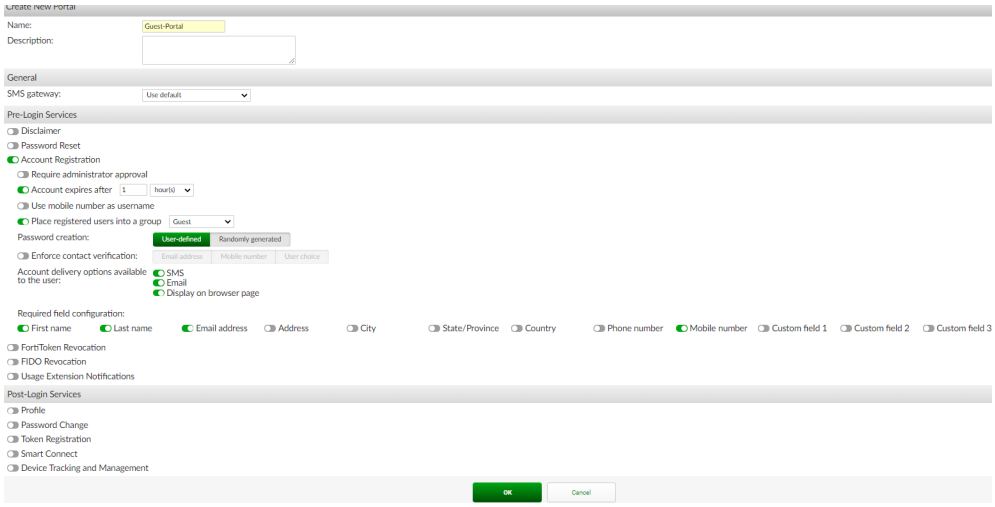
5. Click *OK*.



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*.



Configuring an access point on FortiAuthenticator

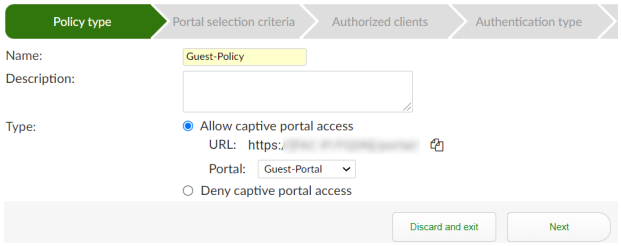
To configure an access points:

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 add a range of client IP address.
4. Click *OK*.
   For more information, see Access points in the latest *FortiAuthenticator Administration Guide*.

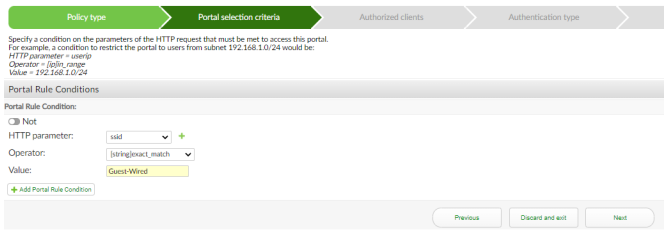
Configuring a captive portal policy on FortiAuthenticator

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 387.
   d. Click *Next*.

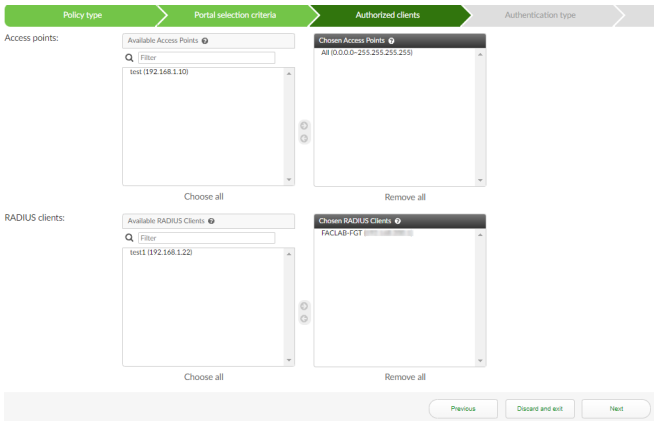


3. In the *Portal selection criteria* tab:
   a. In the *HTTP parameter* dropdown, select *ssid* to match.
   b. In the *Operator* dropdown, *select [string]exact_match*.
   c. In *Value*, enter the name of the interface configured on the FortiGate with captive portal authentication required. Here, `Guest-Wired`.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



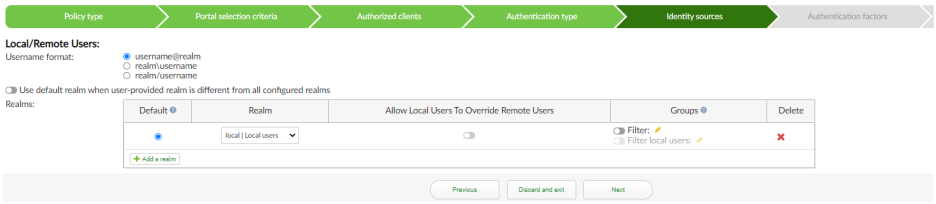
4. In the *Authorized clients* tab:
   a. From *Access points*, select the access point defined in Access points.
   b. From *RADIUS clients*, select the FortiGate RADIUS client defined in RADIUS clients.

c. Click *Next*.



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*.

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*.



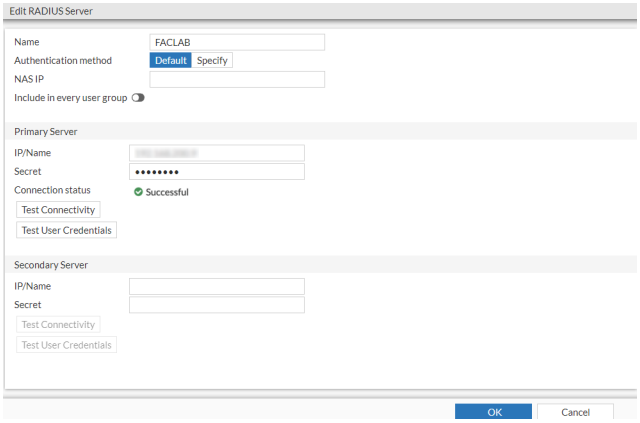
7. In the *Authentication Factors* tab, click *Next*.
8. In the *RADIUS response* tab, review the policy, and click *Save and exit*.

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*.

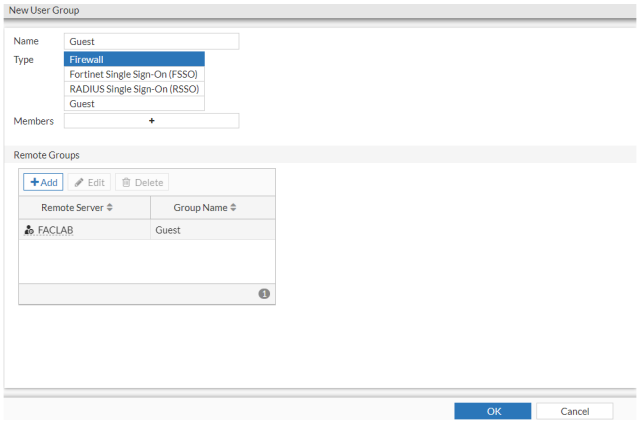
7. Click *OK* to save changes.



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*.



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:

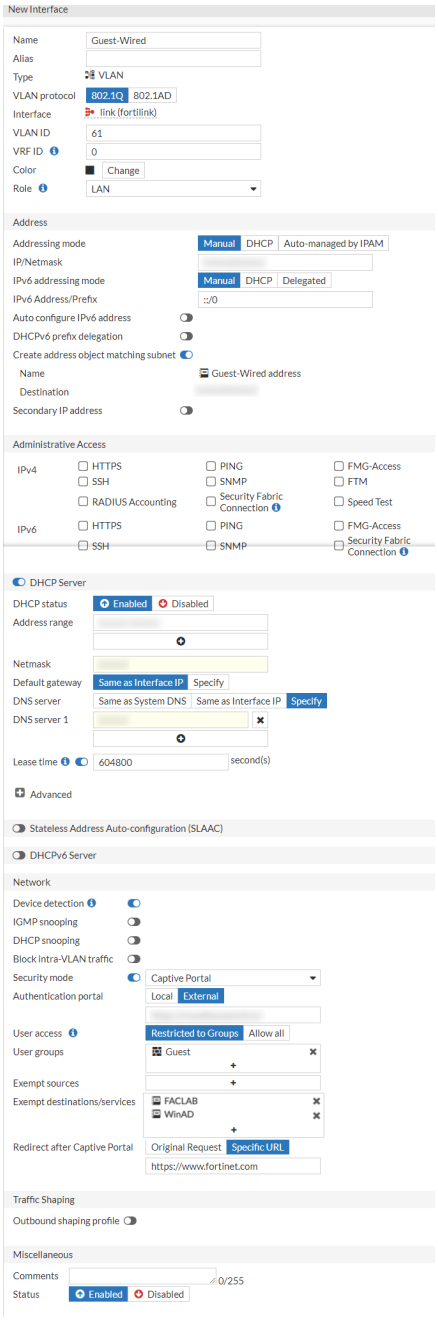
1. Go to *WiFi & Switch Controller > FortiSwitch VLANs*.
2. Select *Create New*.
3. In the *New Interface* window, enter a name for the interface. Optionally, enter an alias.
4. Select *802.1Q* as the *VLAN protocol*.
5. Ensure that a FortiLink interface member is selected in *Interface*.
6. In *VLAN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

11. Click *OK*.



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 {http | https} #http coupled with auth-secure-http is a safe choice and
        should not be disabled except in a few environments.
  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
```

FortiManager-FortiAnalyzer

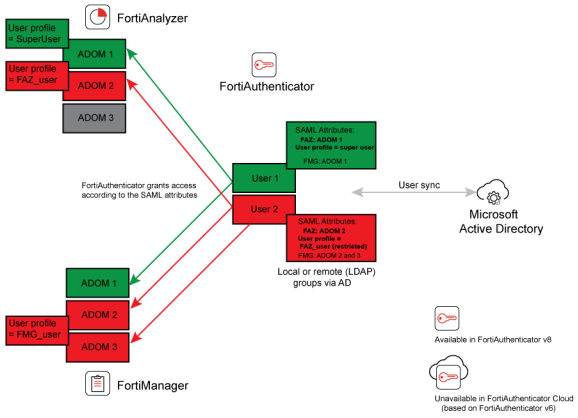
SAML IdP custom multi-value attributes for FortiManager and FortiAnalyzer

In this example, FortiManager and FortiAnalyzer are configured with custom SAML assertion attributes where FortiAuthenticator acts as the IdP.

The example also demonstrates how the feature works with SP specific group filters and admin profiles.

This example uses local users, but the feature also works with LDAP users.

Topology



On FortiAnalyzer:

- `User 1` belongs to `ADOM 1`.
- `User 2` belongs to `ADOM 2`.

On FortiManager:

- `User 1` belongs to `ADOM 1`.
- `User 2` belongs to both `ADOM 2` and `ADOM 3`.

Prerequisites

1. FortiAuthenticator v8.0 with SAML custom value feature.
   See the new feature description for SAML IdP: Custom multi-value SAML attributes in the *FortiAuthenticator 8.0.0 Administration Guide*.
   Note: This feature is not available in FortiAuthenticator Cloud.

2. A FortiManager device with ADOM(s) and different admin profile setup.
3. A FortiAnalyzer device with ADOM(s) with different admin profile setup.

Benefits

1. Different users who log in to FortiManager and FortiAnalyzer are assigned ADOMs and admin profiles with varying access levels, e.g.,
   a. ADOM 1 and 2, `super user`
   b. ADOM 3, `read-only`.

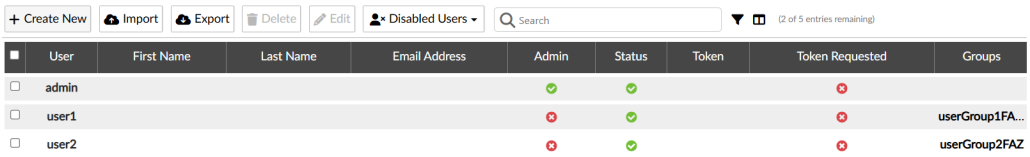
Configuring SAML IdP custom multi-value attributes for FortiManager and FortiAnalyzer:

1. Configuring local users on FortiAuthenticator on page 395
2. Creating user groups on FortiAuthenticator on page 395
3. Results: FortiAnalyzer on page 398
4. Creating SPs for FortiManager-FortiAnalyzer on page 399
5. Results: FortiManager on page 400

Configuring local users on FortiAuthenticator

To configure local users on FortiAuthenticator:

1. Go to *Authentication > User Management > Local Users*, and select *Create New*.
   The *Create New Local User* window opens.
2. Enter a name for the local user.
3. Ensure that *Password creation* is *Specify a password*.
4. Enter the password.
5. Reenter the password to confirm.
6. Ensure that the *Role* is *User*.
7. Click *Save*.
   `user1` is created.
   Repeat steps 1 - 7 to create another local user: `user2`.
   The following displays the list of created users.



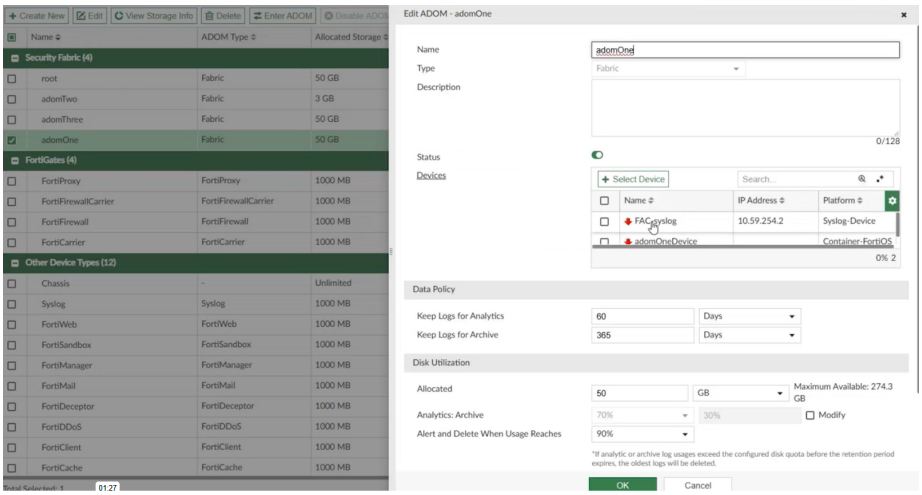
Creating user groups on FortiAuthenticator

To create a new user group:

1. Go to *Authentication > User Management > User Groups*, and select *Create New*.
   The *Create New User Group* window opens.

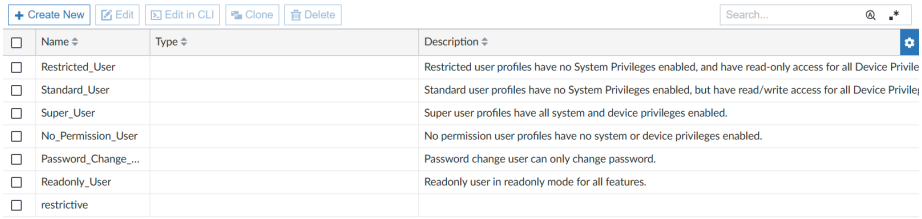
2. Enter a name for the user group.
3. Ensure that the *Type* is *Local*.
4. From the *Available Users* list, move `user1` to the *Chosen Users* list.
   In *SAML Assertion Attributes*:
   a. Select *Add SAML Assertion Attribute*:
      i. In *Attribute name*, enter `adoms`.
      ii. In *Attribute value*, enter `adomOne`.

`adomOne` is available on FortiAnalyzer with the `adomOneDevice`.



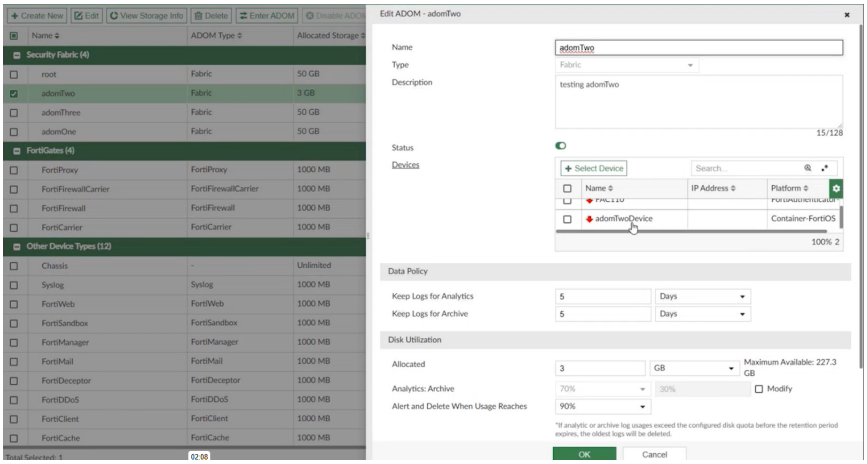
   b. Select *Add SAML Assertion Attribute*:
      i. In *Attribute name*, enter `profilename`.
      ii. In *Attribute value*, enter `Super_User`.

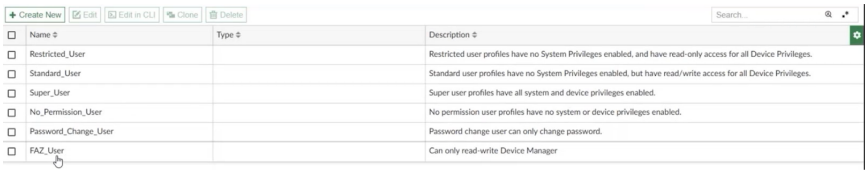
The `Super_User` admin profile has all the system and device privileges.



For `userGroup2FAZ` with `user2`, the following SAML assertion attributes are used:

- *Attribute name, Attribute value*:
  `adoms`, `adomTwo`
- *Attribute name, Attribute value*:
  `profilename`, `FAZ_User`





For `userGroup1FMG` with `user1`, the following assertion attributes are used:

- *Attribute name, Attribute value*:
  `adoms`, `adomOne`
- *Attribute name, Attribute value*:
  `profilename`, `Restricted_User`

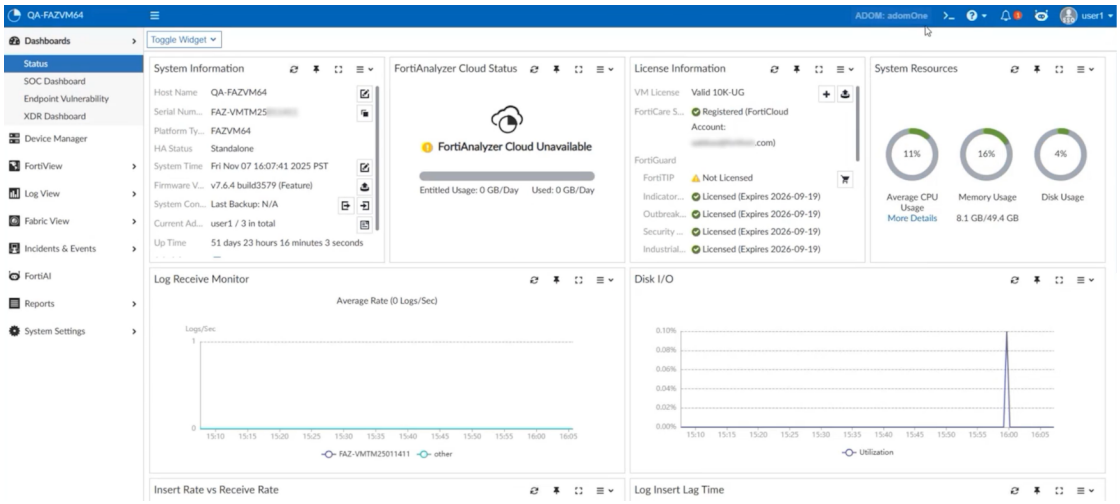
For `userGroup2FMG` with `user2`, the following assertion attributes are used:

- *Attribute name, Attribute value*:
  `adoms`, `adomTwo`
- *Attribute name, Attribute value*:
  `profilename`, `FMG_User`
- *Attribute name, Attribute value*:
  `adoms`, `adomThree`

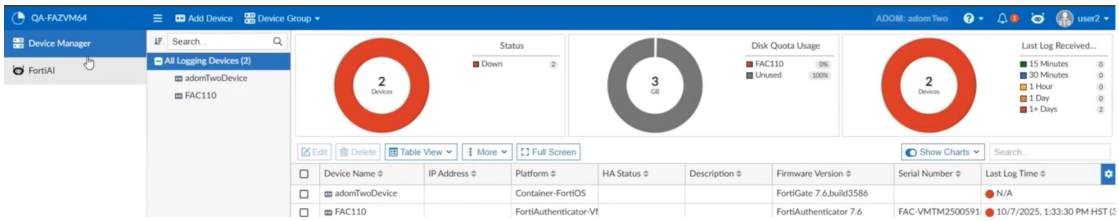
5. Click *Save*.
   The `userGroup1FAZ` user group is created.
   Repeat steps `1` - `5` to create remaining user groups: `userGroup1FMG`, `userGroup2FAZ`, and `userGroup2FMG`.
   The following displays the list of created user groups.

Results: FortiAnalyzer

1. Log in to FortiAnalyzer as `user1`.
   The `user1` belongs to `adomOne`.



2. Log in to FortiAnalyzer as `user2`.
   The `user2` belongs to `adomTwo`.



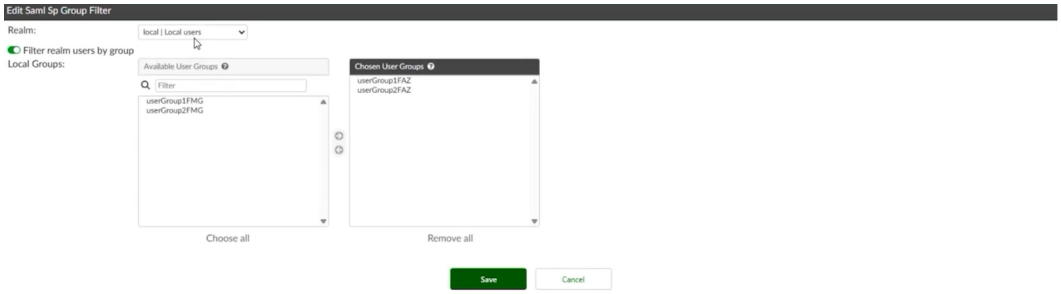
Creating SPs for FortiManager-FortiAnalyzer

We create SPs for FortiManager and FortiAnalyzer and apply custom attributes to SPs.

Each SP can have specific user group filter containing custom SAML assertion attributes.

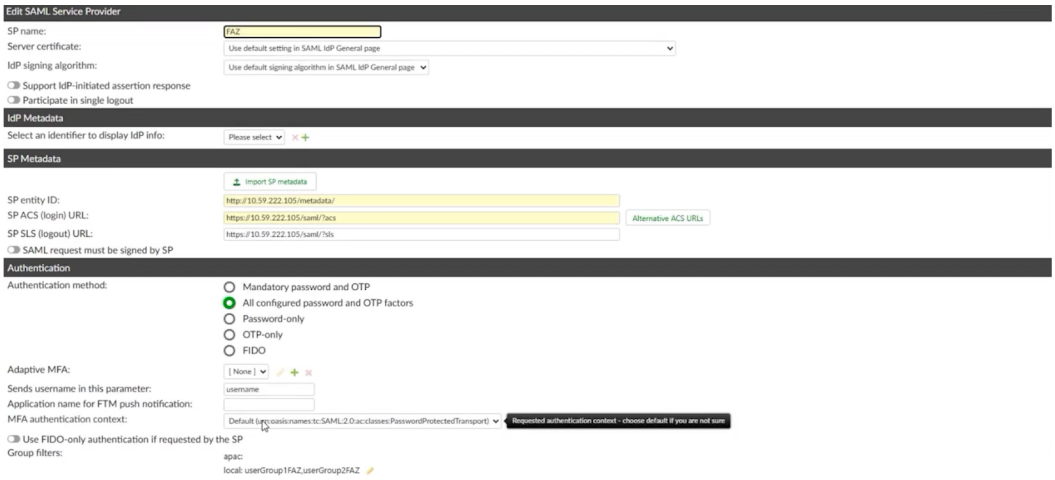
To create an SP for FortiAnalyzer:

1. Go to *Authentication > SAML IdP > Service Providers*, and select *Create New*.
   The *Create New SAML Service Provider window opens*.
2. Enter the SP name.
3. Enter the *SP entity ID*, *SP ACS (login URL)*, and *SP SLS (logout) URL*.
4. Ensure that the *Authentication method* is *All configured password and OTP factors*.
5. In *Group filters*, select *+*, and select *Create New*.
   The *Create New Saml Sp Group Filter* window opens.
   a. Enable *Filter realm users by group*.
   b. From the *Available User Groups* list, move `userGroup1FAZ` and `userGroup2FAZ` to the *Chosen User Groups* list.
   c. Click *Save*.

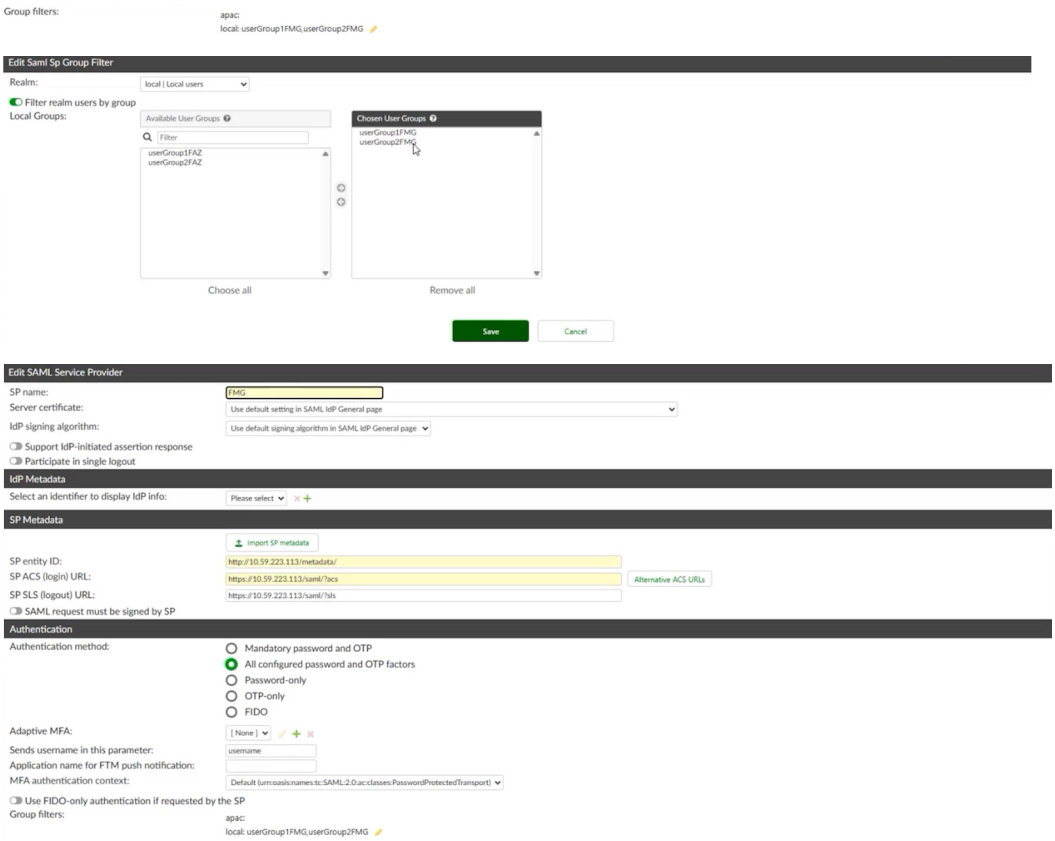


The *Group filters* option now has the new group filter.

6. Click *Save*.

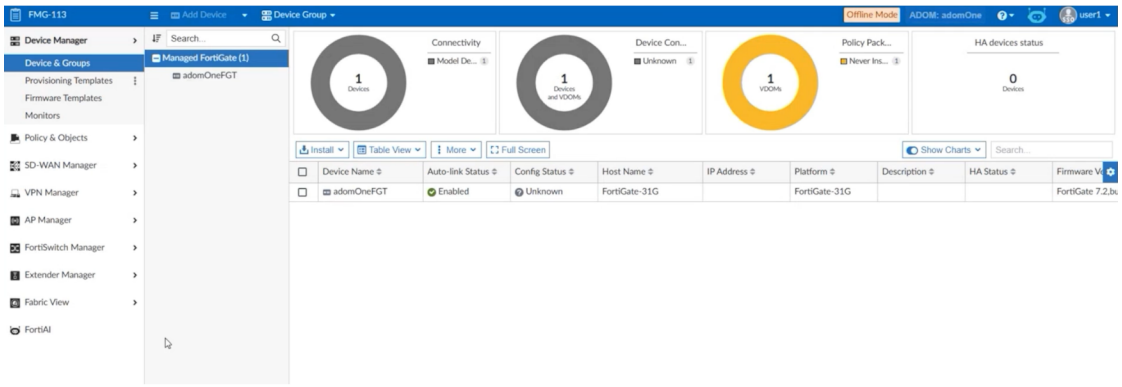


Similarly, create an SP for FortiManager with a group filter with `userGroup1FMG`, `userGroup2FMG`.

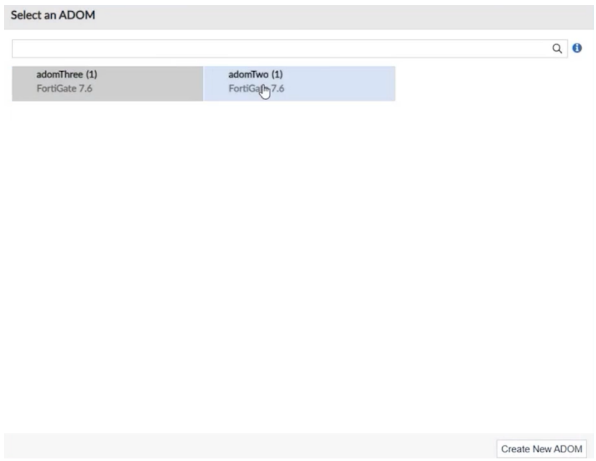


Results: FortiManager

1. Log in to FortiManager as `user1`.
   The `user1` belongs to `adom0ne`.



2. Log in to FortiManager as `user2`.
   FortiManager lets you choose between `adomThree` or `adomTwo`.



FortiAnalyzer- Event handlers for FortiAuthenticator

Introduction

FortiAnalyzer includes predefined ZTNA login event handlers that evaluate FortiAuthenticator authentication logs (normalized Fabric logs) to generate events for brute-force and anomalous login behavior.

In FortiAnalyzer, the handlers are available under *Incidents & Events > Event Handlers*.

1. **ZTNA Brute Force Login**
   Description:
   Detects brute-force authentication attempts and suspicious failed login patterns targeting ZTNA/FortiAuthenticator.
   Use cases:
   - High volume of failed authentication attempts from multiple non-existing users
   - Authentication failures originating from multiple geographic locations
   - Brute force login attacks
   - High volume of failed authentications targeting the same non-existing user

- Low-and-slow brute force login attempts targeting the same user

2. **ZTNA Login Anomaly Detection**
   Description:
   Identifies anomalous or suspicious successful and failed authentication behaviors related to ZTNA access.
   Use cases:
   - Failed authentication attempts to multiple services
   - Successful authentication from multiple geographic locations
   - Successful authentication from multiple endpoints
   - Successful authentication from sanctioned countries
   - Impossible travel login detection

For more information on the event handlers, see the ZTNA login event handlers in the latest *FortiAnalyzer Administration Guide*.

Detecting ZTNA Login attacks with FortiAuthenticator 8.0 and FortiAnalyzer

Demonstrates how FortiAuthenticator 8.0 forwards authentication logs to FortiAnalyzer, where predefined ZTNA login event handlers detect brute-force attempts and login anomalies for Zero Trust Network Access.

Prerequisites

- FortiAuthenticator 8.0 with remote logging configured in *Logging > Log Config > Log Settings*.
  FortiAuthenticator can send logs to a remote syslog server instead of storing locally.
- FortiAnalyzer 7.6.2 or above with predefined event handlers available and enabled in *Incidents & Events > Event Handlers*.

Use the *Event Handlers* page *Search* to look up the default event handlers instead of the browser look up.

ZTNA Brute Force Login Example on page 402

ZTNA Login Anomaly Detection Example on page 404

Results on page 404

Troubleshooting on page 404

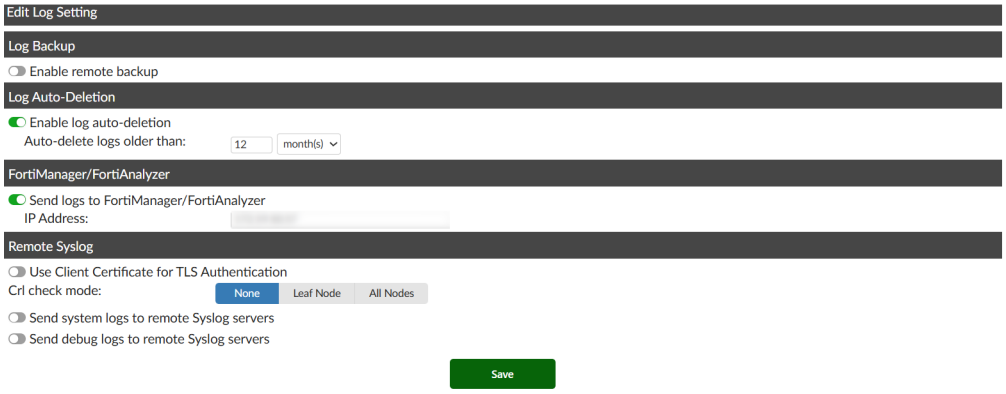
ZTNA Brute Force Login EXAMPLE

Configuring FortiAuthenticator

Sending logs to FortiAnalyzer.

To configure FortiAuthenticator:

1. Go to *Logging > Log Config > Log Settings*.
2. In the *FortiManager/FortiAnalyzer* pane, enable *Send logs to FortiManger/FortiAnalyzer*, and enter the *FortiAnalyzer IP address*.
3. Click *Save*.



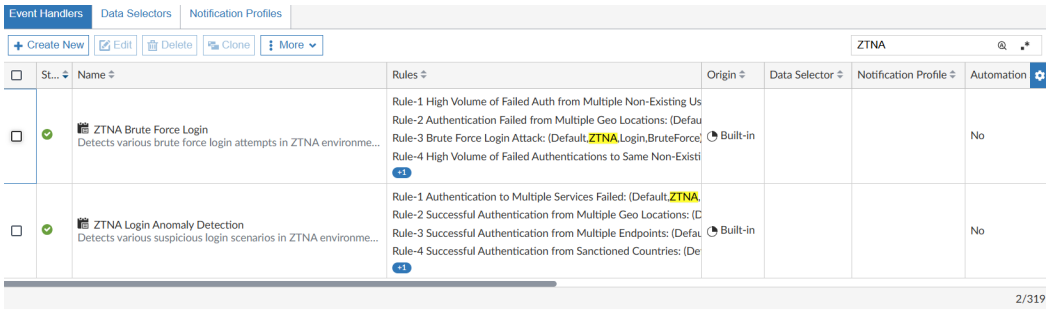
Configuring FortiAnalyzer

Enabling event handlers and scope.

To configure FortiAnalyzer:

1. Go to *Incidents & Events > Event Handlers*.

Use the *Event Handlers* page *Search* to look up the default *ZTNA Brute Force Login* event handler instead of the browser look up.



2. Double-click to open the default *ZTNA Brute Force Login* event handler.
3. In *Data Selector*, select a data selector that includes the FortiAuthenticator device.
   Optionally, attach a *Notification Profile* to send alerts when an event is generated by the event handler.
   See Creating notifications profiles in the latest *FortiAnalyzer Administration Guide*.
   To create a new data selector, see Creating data selectors in the latest *FortiAnalyzer Administration Guide*.
4. Click *OK*.

Test

1. From an external client, perform multiple ZTNA login attempts:
   a. Use invalid usernames
   b. Repeat failures for a valid user (using incorrect password)
   c. Attempt logins from multiple source locations
2. Confirm authentication failures appear on FortiAuthenticator in *Logging > Log Access > Logs*.

ZTNA Login Anomaly Detection EXAMPLE

Configure FortiAuthenticator similar to ZTNA Brute Force Login Example on page 402.

Configure FortiAnalyzer similar to ZTNA Brute Force Login Example on page 402. Ensure that default *ZTNA Login Anomaly Detection* event handler is used instead.

1. On FortiAuthenticator:
   a. Log in to from a Location A, then again within minutes log in from Location B, or use a different endpoint to login.
   b. Go to *Logging > Log Access > Logs* and verify the authentication logs.

Results

- FortiAuthenticator records both failed and successful ZTNA authentication events.
- FortiAnalyzer evaluates authentication logs using the predefined ZTNA event handlers.
- When detection conditions are met:
  - Security events are generated in *Incidents & Events > Event Monitor*.
  - Events include:
    - *User*
    - Source IP address and geolocation
    - The detection rule that triggered the event appears as *Subject* in the *Events Details* pane.
    - Event severity

Troubleshooting

- **Unable to find the event handlers**
  - Ensure you are in a Fabric ADOM.
- **No events shows up**
  - Verify that FortiAuthenticator is assigned to the same ADOM and sending logs.
  - Ensure that the event handler *Data Selector* includes the FortiAuthenticator device.
- Use *Debug logs* at `https://<fac-ip>/debug` (RADIUS, Web Server, SSO, etc.) when troubleshooting issues.

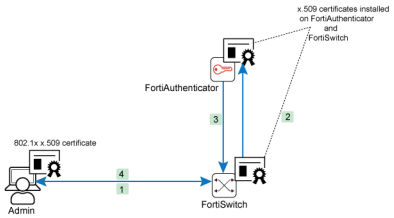
FortiSwitch

Configuring RADSec between FortiAuthenticator and FortiSwitch

In this example, a FortiSwitch (`FSW-1`) authenticates administrative logins through FortiAuthenticator (`FAC-RADIUS-01`) using RADIUS over TLS (RADSec).

RADSec encrypts all RADIUS traffic over `TCP/2083` using X.509 certificates.

Topology



1. Client connects to FortiSwitch using 802.1x EAP-TLS certificate.
2. Forward RADIUS access request to FortiAuthenticator via RADSec tunnel to ensure encryption.
3. FortiAuthenticator responds with an `ACCEPT` RADIUS response over RADSec.
4. FortiSwitch allows client network access.

Prerequisites

- FortiAuthenticator 8.0 with a valid certificate (CA-signed or self-signed).
- A FortiSwitch device with management access and firmware version 7.6.4 or above.
- Network connectivity between FortiSwitch and FortiAuthenticator on port `2083`.
- Administrative credentials for FortiAuthenticator and FortiSwitch.

To configure RADSec between FortiAuthenticator and FortiSwitch:

1. Configuring FortiAuthenticator on page 406
2. Configuring FortiSwitch on page 409
3. Verification on page 410

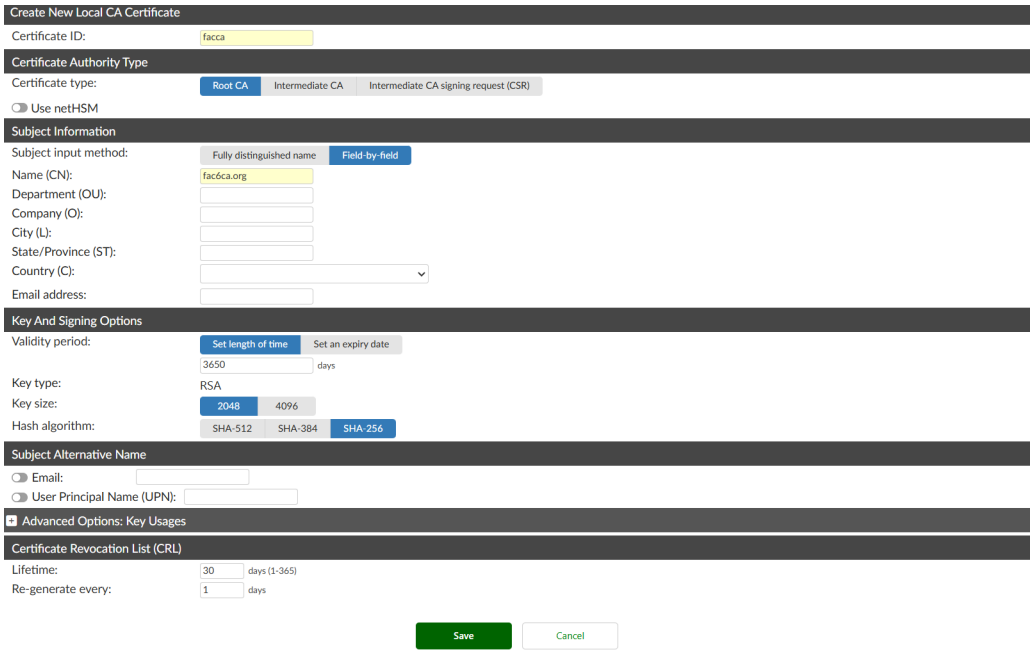
Configuring FortiAuthenticator

Creating or importing certificates

FortiAuthenticator must present a server certificate for RADSec.

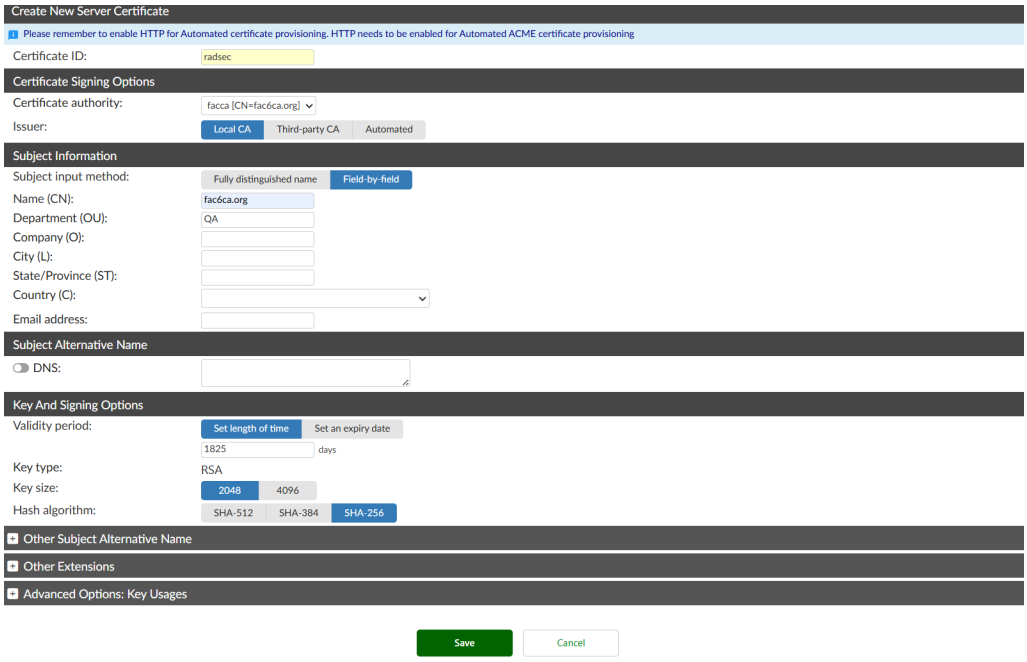
Option A: Using a local CA

1. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*, and select *Create New* to create a new local CA.
   a. In *Certificate ID*, enter a unique ID for the CA certificate.
   b. In *Certificate type*, select *Root CA*.
   c. In *Subject input method*, select *Field-by-field*.
   d. In *Name (CN)*, enter `fac6ca.org`.
   e. Click *Save*.



2. Go to *Certificate Management* > *End Entities* > *Local Service*, and select *Create New* to create a server certificate using the CA created in step 1.
   a. In *Certificate ID*, enter a unique ID for the certificate.
   b. In *Certificate authority*, select the CA created in step 1.
   c. In *Name (CN)*, enter `fac6ca.org`.
   d. In *Department (OU)*, enter `QA`.

e. Click *Save*.



Option B: Importing a public CA

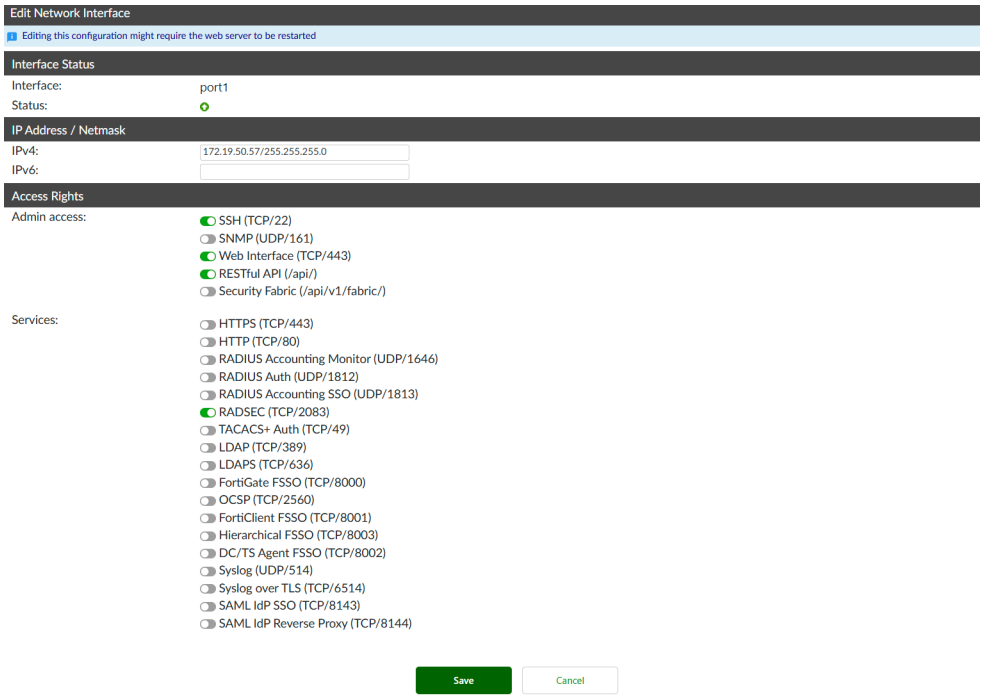
Import the trusted CA under *Trusted CAs*, then import your matching server certificate.

1. Go to *Certificate Management* > *Certificate Authorities* > *Trusted CAs*, and select *Import*.
2. In *Certificate ID*, enter the certificate ID.
3. Select *Upload a file* to locate the certificate file on your computer, and select *Import* to import the trusted CA.

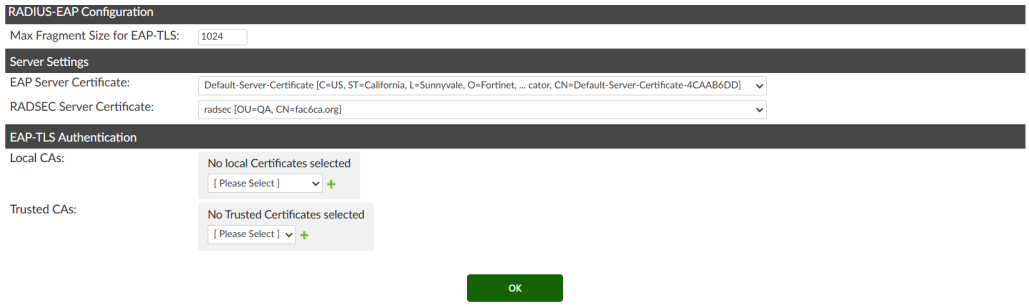
Enabling RADSec and assigning the Certificate

1. Go to *System* > *Network* > *Interfaces*.
2. Edit the interface FortiSwitch will connect to, and enable `RADSEC (TCP/2083)`.

3. Click *Save*.



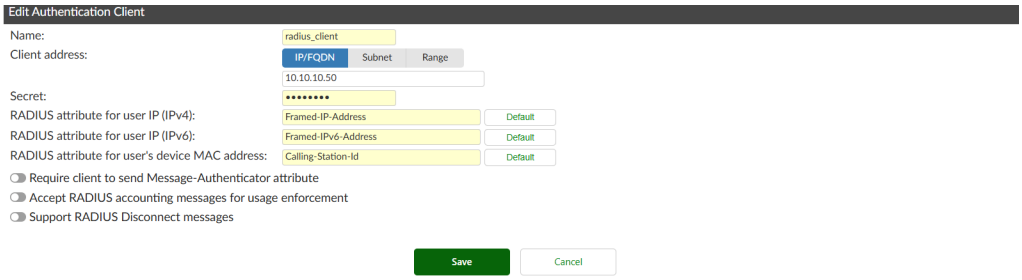
4. Go to *Authentication > RADIUS Service > General*.
5. In *RADSEC Server Certificate*, select the server certificate created in step 2 of Option A: Using a local CA on page 406.
6. Click *OK*.



Adding FortiSwitch as a RADIUS client

1. Go to *Authentication > RADIUS Service > Clients*, and select *Create New*.
2. Enter a name for the client.
3. In *Client address*, select *IP/FQDN*, and enter `10.10.10.50` (the FortiSwitch IP address).
4. Enter a secret.

5. Click *Save*.



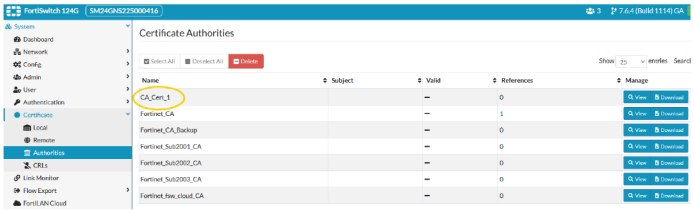
6. Add the client to an appropriate RADIUS policy.

Configuring FortiSwitch

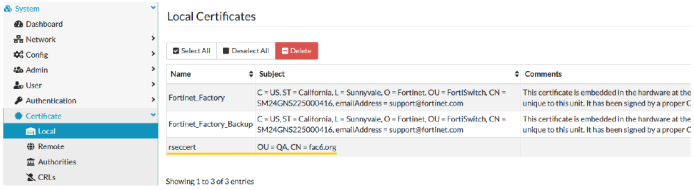
Importing CA and creating Client Certificate

FortiSwitch must trust the CA that signs FortiAuthenticator RADSec certificate.

1. In FortiAuthenticator, export the CA certificate by going to *Certificate Management > Certificate Authorities > Local CAs*.
   a. From the list, select the CA certificate created in Option A: Using a local CA on page 406, and select *Export Certificate*.
      The CA certificate is downloaded to your management computer.
2. On FortiSwitch, go to *System > Certificates > Authorities*.
   a. Import the CA certificate and note the name with which it is saved on FortiSwitch.



3. Create a local certificate on FortiSwitch to be used for RADSec communication with FortiAuthenticator.



Alternatively, create a certificate on FortiAuthenticator and import the certificate to FortiSwitch.

Skip if FortiAuthenticator uses a publicly trusted CA already included in FortiSwitch.

Configuring RADIUS server via CLI

FortiSwitch requires CLI configuration to enable RADIUS over TLS.

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

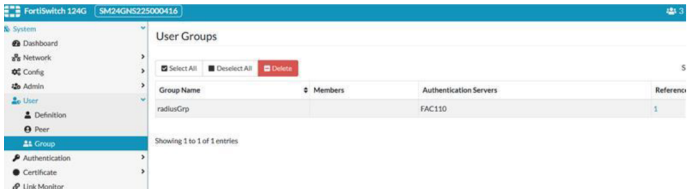
```
config user radius
 edit "FAC-RADSEC"
  set server "<FortiAuthenticator-IP>"
  set secret <shared-secret>
  set radius-port 2083
  set transport-type TLS
  set radsec-server-ca-cert "<CA-Certificate-Name>"
  set radsec-client-cert "<Local-Certificate-Name>"
 next
end
```

FortiSwitch is now configured to authentication users via RADSec against FortiAuthenticator.

Verification

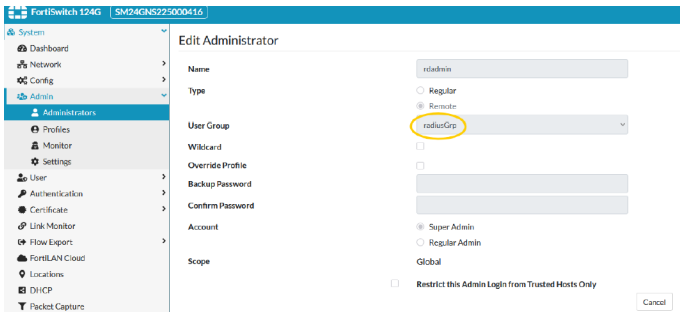
Configuring a remote admin group

1. On FortiSwitch, create a user group and reference the FortiAuthenticator RADIUS server as its authentication server.



Creating a remote admin account

1. Create a new admin account on the FortiSwitch and set it as the remote admin.
   Reference the user group created in Configuring a remote admin group on page 410 as the user group.



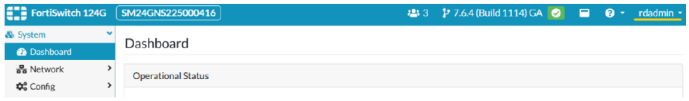
Creating matching local user on FortiAuthenticator

1. On FortiAuthenticator, create a local user with the same name as the admin account on FortiSwitch, and add the local user realm to the RADIUS policy on FortiAuthenticator.

Test login

1. Log in to FortiSwitch (in a private browser session) using the new admin account.
   This carries the RADSec authentication against FortiAuthenticator.

   You are now logged in to FortiSwitch using the remote RADIUS admin account.



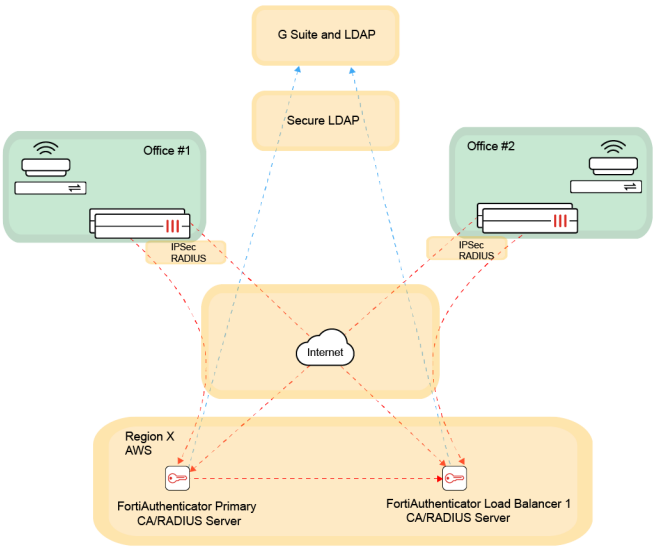
3rd party integrations

The chapter includes FortiAuthenticator examples for 3rd party integrations.

Google workspace

Google Workspace integration using LDAP

This example 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.



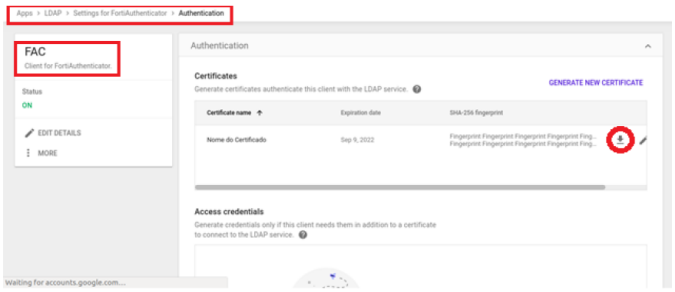
1. Generating the Google Workspace certificate on page 413
2. Importing the certificate to FortiAuthenticator on page 414
3. Configuring LDAP on the FortiAuthenticator on page 415
4. Troubleshooting on page 416

Generating the Google Workspace certificate

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

To generate certificate authentication:

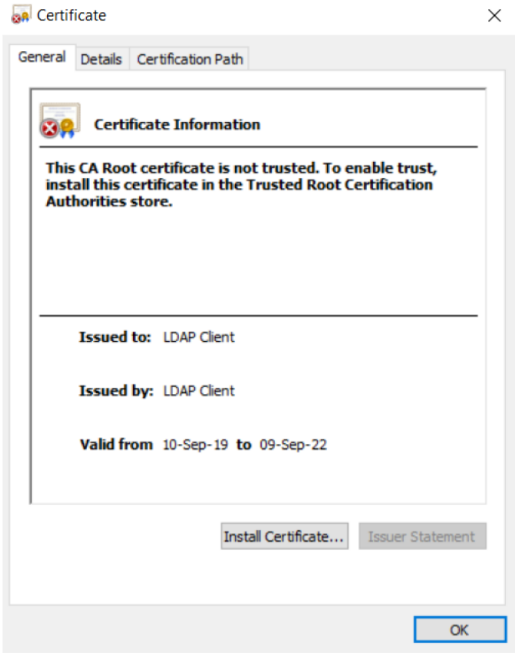
1. From the Google Admin console, go to *Apps* > *LDAP*.
2. Select one of the clients in the list.
3. Click the *Authentication* card.
4. Click *GENERATE NEW CERTIFICATE*, then click the download icon to download the certificate.
5. Upload the certificate to your client, and configure the application.
   Depending on the type of LDAP client, configuration may require LDAP access credentials. See Generate access credentials.



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

Example:

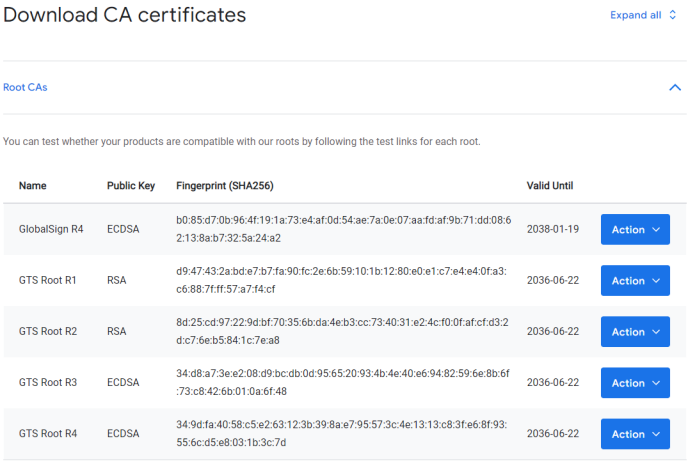
- Cert: `Google_2022_09_09_72372.crt`
- Key: `Google_2022_09_09_72372.key`



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`



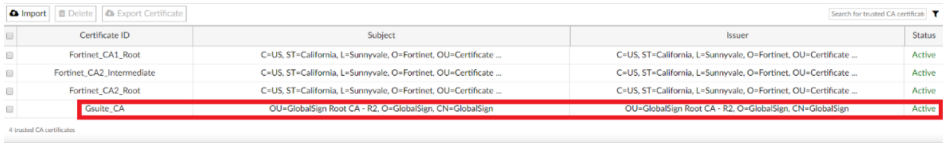
Importing the certificate to FortiAuthenticator

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*.

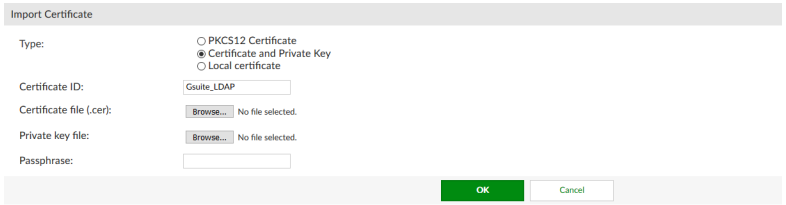
Results:



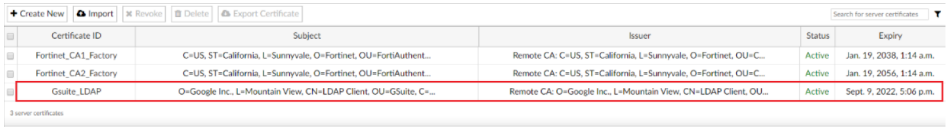
You can now import the LDAP certificate generated by Google Workspace.

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*.
4.



Results:

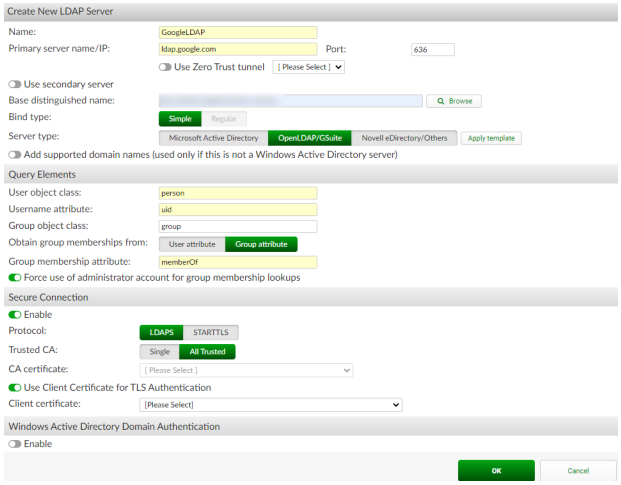


Configuring LDAP on the FortiAuthenticator

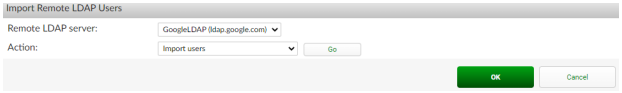
Now you can finish the LDAPS configuration using client authentication through certificate.

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.



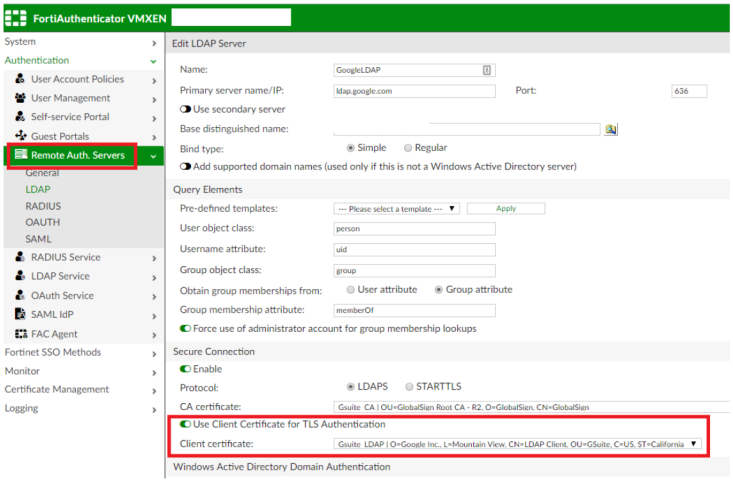
2. Select *OK*.
   If required, you can now import users by selecting *Import users* when editing the LDAP server, selecting the LDAP server from the *Remote LDAP server* dropdown, and clicking the *Go* button next to the *Import users* dropdown. This is not a required step, but can be done in cases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



Troubleshooting

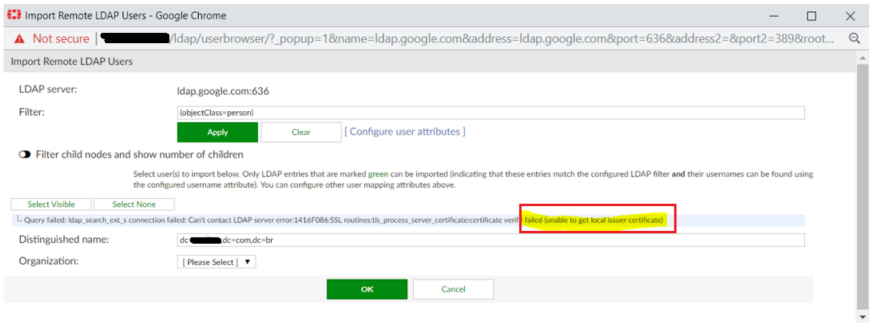
Missing option to use client certificate for TLS authentication

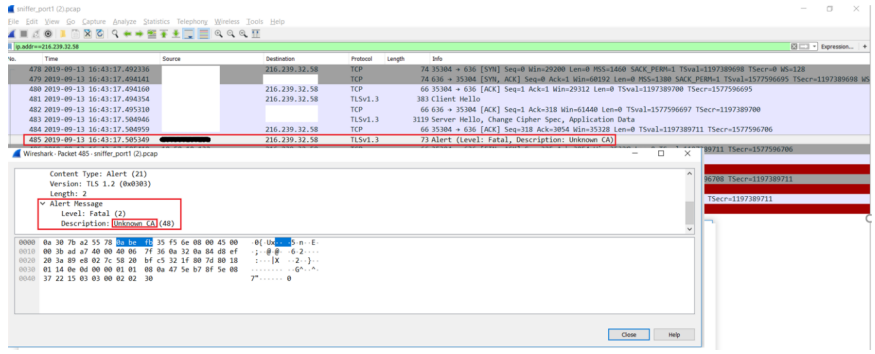
Use Client Certificate for TLS Authentication is only supported in FortiAuthenticator 6.0.1 and higher.



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 413.





Microsoft

- SAML FSSO with FortiAuthenticator and Microsoft Entra ID (formerly Microsoft Azure AD) on page 231
- Office 365 SAML authentication using FortiAuthenticator with 2FA on page 244
- Office 365 SAML authentication using FortiAuthenticator with 2FA in Azure/ADFS hybrid environment on page 217
- FortiAuthenticator SSOMA for native Microsoft Entra ID joined workstation on page 176
- Option B - WiFi onboarding with Smart Connect and Azure on page 118

AWS

- FortiAuthenticator SCIM integration with AWS on page 161

OKTA

OneLogin

Safenet Luna HSM

SAMBA 4

Using Samba 4 AD domain for FSSO

This example explains how to configure FSSO with Samba 4 and FortiAuthenticator using Syslog SSO.

FortiAuthenticator receives the logon events form `samba ad-dc` using Syslog and sends them to the FortiGate firewall via the FSSO connector.

The setup allows FortiGate to create policies based on Active Directory groups by collecting IP addresses of workstations where the domain users log in.

Prerequisites

- FortiGate 7.6
- FortiAuthenticator 6.6.3
- Debian 12 with Samba 4 Domain Controller and `rsyslogd`
- Client PC with Windows 10

To use Samba 4 AD domain for FSSO:

1. Configuring Samba 4 domain controller on page 419
2. Enabling Syslog messages on FortiAuthenticator on page 419
3. Adding Samba 4 server as an LDAP server on page 420
4. Enabling Syslog SSO on page 421
5. Creating a matching rule on page 421
6. Creating Syslog sources on page 422
7. Configure an FSSO agent on page 422
8. Monitoring authenticated users on page 424

Configuring Samba 4 domain controller

To configure Samba 4 DC:

1. Edit the `smb.conf` (Samba 4 configuration) file.
   a. Open `/etc/samba/smb.conf` and add the following under `[global]`:

```
[global]
log level = 3
vfs object = full_audit
full_audit:success = connect disconnect
full_audit:failure = disconnect
full_audit:prefix = User-Name:%U|Client-IP:%I|%S
full_audit:facility = local5
```

2. Configure `rsyslog`:
   a. Create a new configuration file `/etc/rsyslog.d/00-samba.conf` and add:

```
if $programname == 'smbd_audit' and $syslogseverity == '5' then @192.168.200.97
```

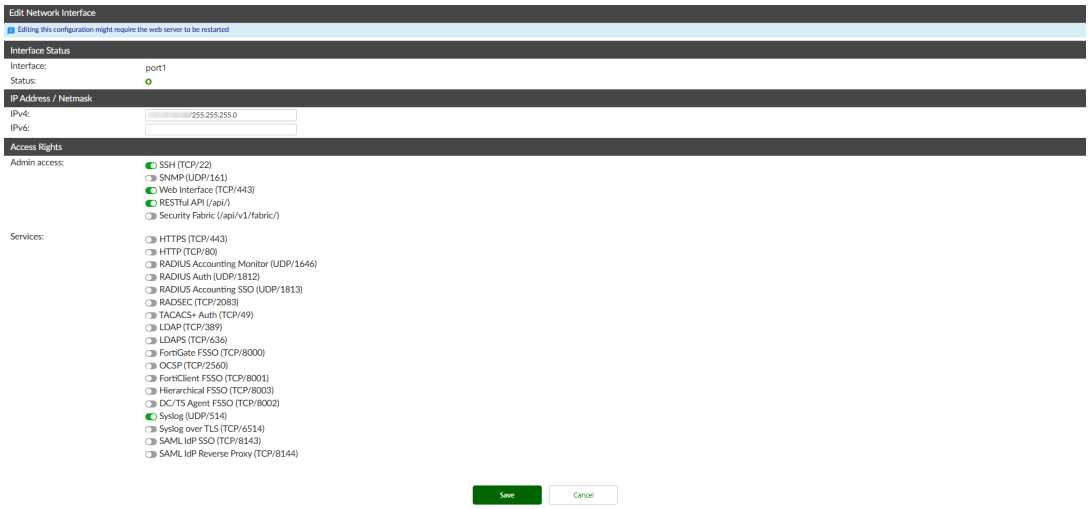
   The logs created by `smbd_audit` are sent to FortiAuthenticator at `192.168.200.97`.

Enabling Syslog messages on FortiAuthenticator

To enable Syslog messages on FortiAuthenticator:

1. Open the interface being used by going to *System > Network > Interfaces* and clicking the in-use interface.
2. In *Services*, enable *Syslog (UDP/514)*.

3. Click *Save*.



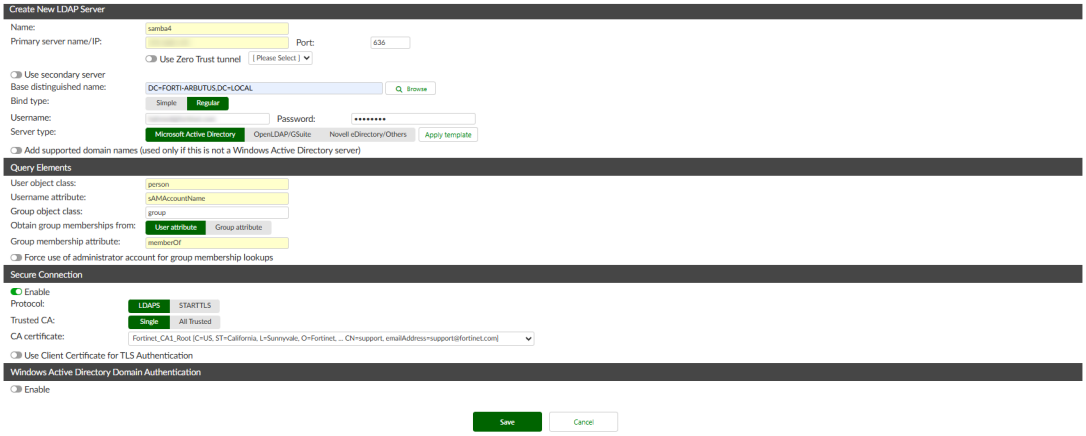
Adding Samba 4 server as an LDAP server

FortiAuthenticator checks the received usernames against the LDAP server to verify the existence and group memberships.

To add Samba 4 server as an LDAP server:

1. Go to *Authentication > Remote Auth. Servers > LDAP* and select *Create New*.
   The *Create New LDAP Server* window opens.
2. In *Name*, enter a name for the Samba 4 server.
3. In *Primary server name/IP*, enter the IP address for the Samba 4 server.
4. In *Base distinguished name*, enter a base distinguished name for the server.
5. Ensure that *Bind type* is *Regular*, and enter a username and password.
6. Ensure the *Server type* is *Microsoft Active Directory*.
7. In the *Query Elements* pane. keep the default values:
8. In the *Secure Connection* pane:
   a. Select *Enable*.
   b. In *Protocol*, select *LDAP*.
   c. Ensure that *Trusted CA* is *Single*.
   d. In *CA certificate*, select a CA certificate to verify the server certificate.

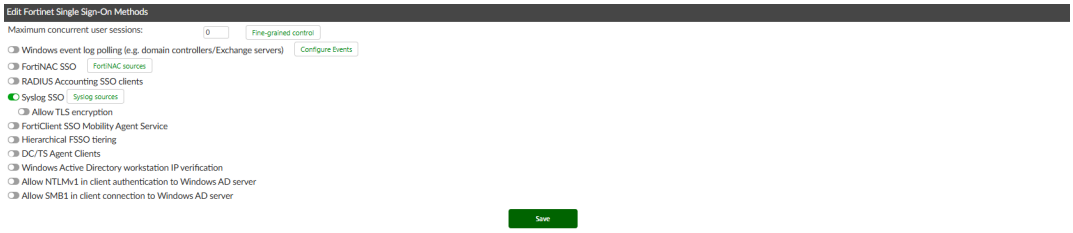
9. Click *Save*.



Enabling Syslog SSO

To enable Syslog SSO:

1. Go to *Fortinet SSO > Settings > Methods*.
2. Enable *Syslog SSO*.
3. Click *Save*.

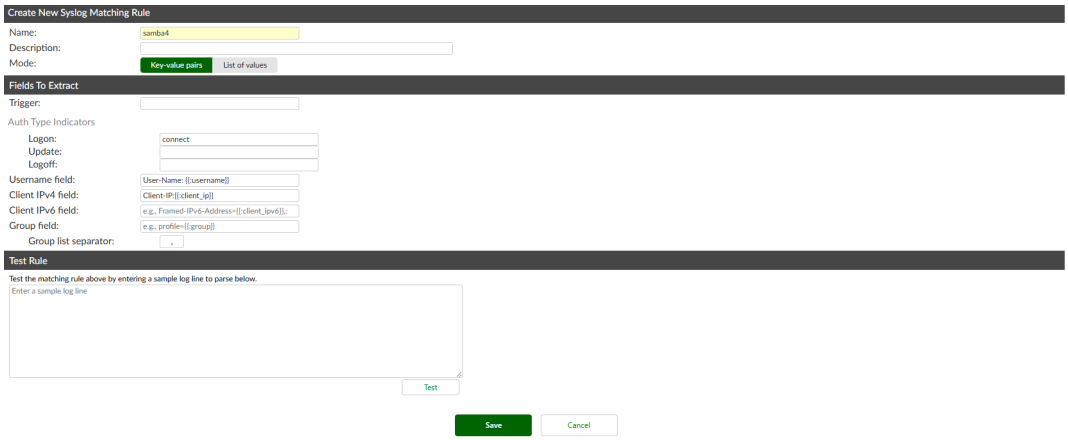


Creating a matching rule

To create a matching rule:

1. Go to *Fortinet SSO > Methods > Syslog* and select the *Matching Rules* tab.
2. Select *Create New*.
   The *Create New Syslog Matching Rule window* opens.
3. In *Name*, enter a name for the matching rule.
4. Ensure that the *Mode* is *Key-value* pairs.
5. In the *Fields to Extract* pane:
   a. In *Logon*, enter `connect`.
   b. In *Username field*, enter `User-Name: {{:username}}`.
   c. In *Client IPv4 field*, enter `Client-IP:{{:client_ip}}` .

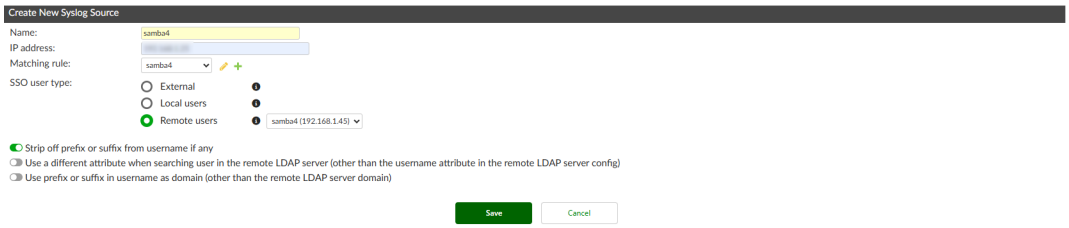
6. Click *Save*.



Creating Syslog sources

To create a Syslog sources:

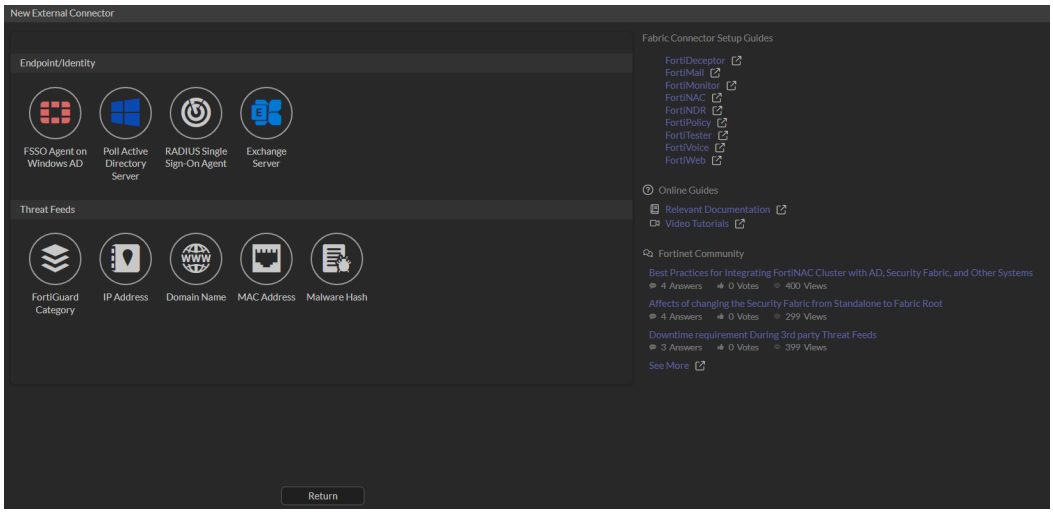
1. Go to *Fortinet SSO > Methods > Syslog* and select the *Syslog Sources* tab.
2. Select *Create New* to create a new Syslog source.
   The *Create New Syslog Source window* opens.
3. In *Name*, enter a name for the Syslog source.
4. In *IP address*, enter the IP address of the Samba 4 DC. See Configuring Samba 4 domain controller on page 419.
5. In the *Matching rule* dropdown, select the matching rule created in Creating a matching rule on page 421.
6. In *SSO user type*, select *Remote users*.
   a. From the dropdown, select the remote LDAP server created in Adding Samba 4 server as an LDAP server on page 420.
7. Ensure that *Strip off prefix or suffix from username if any* is enabled.
8. Click *Save*.



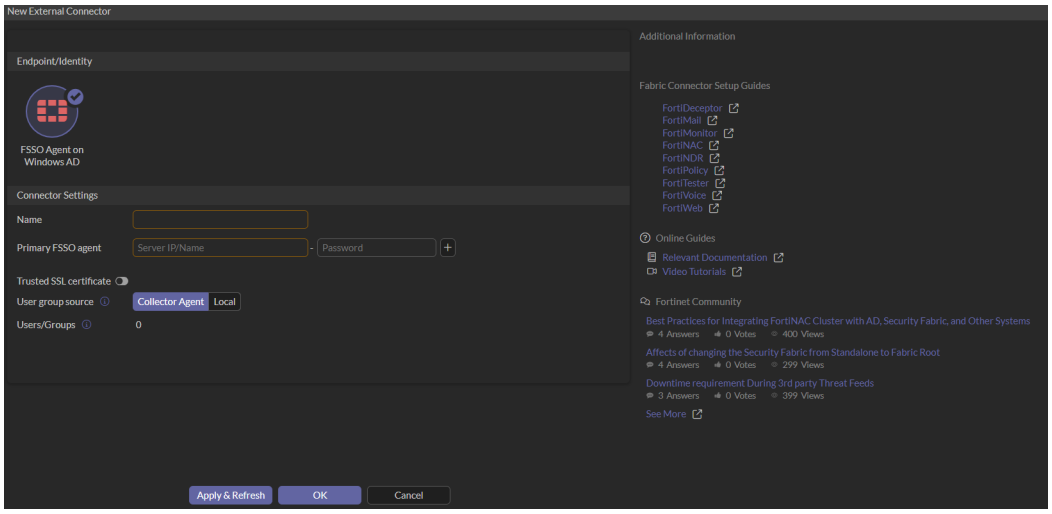
Configure an FSSO agent

To configure an FSSO agent:

1. In the `root` VDOM, go to *Security Fabric > External Connectors*.
2. Select *Create New*.
   The *New External Connector window* opens.

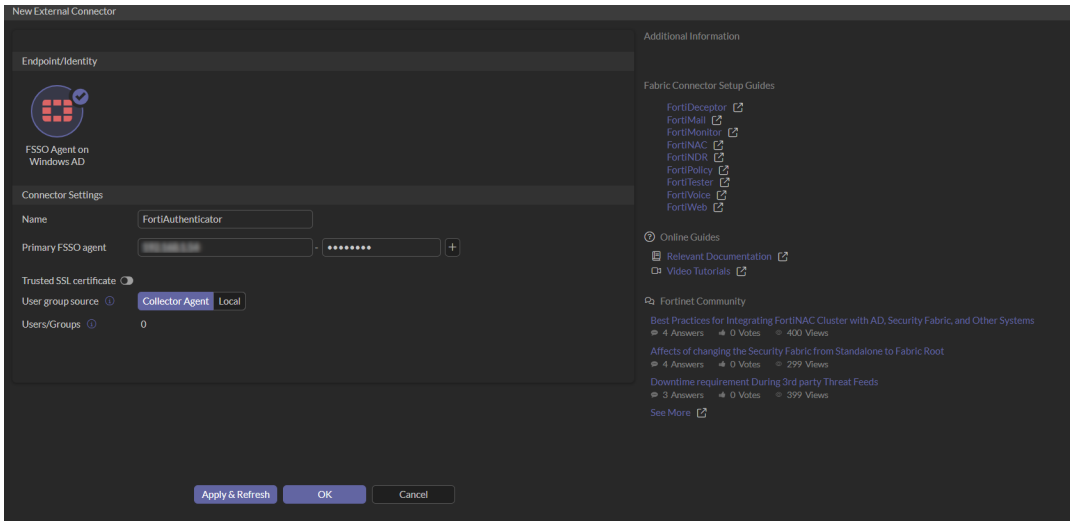


3. In *Endpoint/Identity*, select *FSSO Agent on Windows AD*.



4. In the *Connector Settings* pane:
   a. In *Name*, enter FortiAuthenticator.
   b. In *Primary FSSO agent*, enter the IP address of the FortiAuthenticator server that runs the FSSO Collector Agent, and enter the password.

5. Click *OK*.



Alternatively, use the following CLI commands to configure the FSSO agent on FortiAuthenticator:

```
config user fsso
 edit "FortiAuthenticator"
  set server <FortiAuthenticator_IP>"
  set password <Your_Password>"
 next
end
```

Monitoring authenticated users

To monitor authenticated users in FortiGate:

1. Go to *Dashboard > Firewall User Monitor*.
2. Click *Show all FSSO Logons*.
   Alternatively, in the CLI console enter the following commands:

```
diagnose firewall auth list
```

www.fortinet.com