

Cookbook

FortiAuthenticator 6.5.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



July 23, 2024

FortiAuthenticator 6.5.0 Cookbook

23-650-779541-20250723

TABLE OF CONTENTS

Change Log	9
Certificate management	10
FortiAuthenticator as a Certificate Authority	10
Creating a new CA on the FortiAuthenticator	11
Installing the CA on the network	11
Creating a CSR on the FortiGate	15
Importing and signing the CSR on the FortiAuthenticator	17
Importing the local certificate to the FortiGate	17
Configuring the certificate for the GUI	18
Results	19
FortiAuthenticator certificate with SSL inspection	19
Creating a CSR on the FortiGate	20
Creating an Intermediate CA on the FortiAuthenticator	22
Importing the signed certificate on the FortiGate	22
Configuring full SSL inspection	23
Results	25
FortiAuthenticator certificate with SSL inspection using an HSM	27
Configuring the NetHSM profile on FortiAuthenticator	28
Creating a local CA certificate using an HSM server	29
Creating a CSR on the FortiGate	29
Creating an Intermediate CA on the FortiAuthenticator	31
Importing the signed certificate on the FortiGate	31
Configuring full SSL inspection	32
Results	34
FortiToken and FortiToken Mobile	36
FortiToken Mobile Push for SSL VPN	36
Adding a FortiToken to the FortiAuthenticator	37
Adding the user to the FortiAuthenticator	38
Creating the RADIUS client and policy on the FortiAuthenticator	40
Connecting the FortiGate to the RADIUS server	42
Configuring the SSL-VPN	44
Results	46
Guest Portals	50
FortiAuthenticator as Guest Portal for FortiWLC	50
Creating the FortiAuthenticator as RADIUS server on the FortiWLC	50
Creating the Captive Portal profile on the FortiWLC	51
Creating the security profile on the FortiWLC	52
Creating the QoS rule on the FortiWLC	53
Creating the ESS Profile on the FortiWLC	55
Creating FortiWLC as RADIUS client on the FortiAuthenticator	56
Creating the portal and access point on FortiAuthenticator	57
Creating the portal policy on FortiAuthenticator	58
Results	59
FortiAuthenticator as a Wireless Guest Portal for FortiGate	59
Configuring FortiGate as a RADIUS client	60

Creating a user group on FortiAuthenticator for guest users	60
Creating a guest portal on FortiAuthenticator	61
Configuring an access point on FortiAuthenticator	61
Configuring a captive portal policy on FortiAuthenticator	62
Configuring FortiAuthenticator as a RADIUS server on FortiGate	63
Creating a guest group on FortiGate	64
Creating a wireless guest SSID on FortiGate	64
Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet	67
Configuring firewall authentication portal settings on FortiGate	67
FortiAuthenticator as a Wired Guest Portal for FortiGate	68
Configuring FortiGate as a RADIUS client	69
Creating a user group on FortiAuthenticator for guest users	70
Creating a guest portal on FortiAuthenticator	70
Configuring an access point on FortiAuthenticator	71
Configuring a captive portal policy on FortiAuthenticator	71
Configuring FortiAuthenticator as a RADIUS server on FortiGate	73
Creating a guest group on FortiGate	73
Creating a wired guest interface on FortiSwitch	74
Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet	76
Configuring firewall authentication portal settings on FortiGate	77
MAC authentication bypass	78
MAC authentication bypass with dynamic VLAN assignment	78
Configuring MAC authentication bypass on the FortiAuthenticator	78
Configuring the user group	79
Configuring RADIUS settings on FortiAuthenticator	80
Configuring the 3rd-party switch	81
Results	82
Self-service Portal	85
FortiAuthenticator user self-registration	85
Creating a self-registration user group	85
Enabling self-registration	86
Creating a new SMTP server	89
Results - Self-registration	90
Results - Administrator approval	92
VPNs	95
LDAP authentication for SSL VPN with FortiAuthenticator	95
Creating the user and user group on the FortiAuthenticator	96
Creating the LDAP directory tree on the FortiAuthenticator	97
Connecting the FortiGate to the LDAP server	98
Creating the LDAP user group on the FortiGate	99
Configuring the SSL-VPN	100
Results	104
SMS two-factor authentication for SSL VPN	105
Creating an SMS user and user group on the FortiAuthenticator	106
Configuring the FortiAuthenticator RADIUS client	107
Configuring the FortiGate authentication settings	108
Configuring the SSL-VPN	110
Creating the security policy for VPN access to the Internet	112

Results	112
WiFi authentication	116
Assigning WiFi users to VLANs dynamically	116
Configuring the FortiAuthenticator	117
Adding the RADIUS server to the FortiGate	118
Creating an SSID with dynamic VLAN assignment	119
Creating the VLAN interfaces	121
Creating security policies	125
Creating the FortiAP profile	126
Connecting and authorizing the FortiAP	128
Results	128
WiFi using FortiAuthenticator RADIUS with certificates	130
Creating a local CA on FortiAuthenticator	130
Creating a local service certificate on FortiAuthenticator	131
Configuring RADIUS EAP on FortiAuthenticator	131
Configuring RADIUS client on FortiAuthenticator	132
Configuring local user on FortiAuthenticator	133
Configuring local user certificate on FortiAuthenticator	133
Creating RADIUS server on FortiGate	134
Creating WiFi SSID on FortiGate	135
Exporting user certificate from FortiAuthenticator	139
Importing user certificate into Windows 10	139
Configuring Windows 10 wireless profile to use certificate	143
Results	148
WiFi RADIUS authentication with FortiAuthenticator	151
Creating users and user groups on the FortiAuthenticator	151
Registering the FortiGate as a RADIUS client on the FortiAuthenticator	152
Configuring FortiGate to use the RADIUS server	153
Creating SSID and set up authentication	154
Connecting and authorizing the FortiAP	155
Creating the security policy	158
Results	159
WiFi with WSSO using FortiAuthenticator RADIUS and Attributes	159
Registering the FortiGate as a RADIUS client on the FortiAuthenticator	160
Creating users on the FortiAuthenticator	160
Creating user groups on the FortiAuthenticator	162
Configuring the FortiGate to use the FortiAuthenticator as the RADIUS server	163
Configuring user groups on the FortiGate	164
Creating security policies	165
Configuring the SSID to RADIUS authentication	167
Results	168
802.1X authentication using FortiAuthenticator with Google Workspace User Database	168
Configuring FortiGate as a RADIUS client	169
Creating a realm and RADIUS policy with EAP-TTLS authentication	170
Configuring FortiAuthenticator as a RADIUS server in FortiGate	171
Configuring a WPA2-Enterprise with FortiAuthenticator as the RADIUS server	171
Configuring Windows or macOS to use EAP-TTLS and PAP	173

LDAP Authentication	175
Google Workspace integration using LDAP	175
Generating the Google Workspace certificate	175
Importing the certificate to FortiAuthenticator	177
Configuring LDAP on the FortiAuthenticator	178
Troubleshooting	178
SAML Authentication	180
SAML IdP proxy for Azure	180
Configuring OAuth settings	180
Configuring the remote SAML server	181
Creating a remote SAML user synchronization rule	182
Configuring an Azure realm	183
Configuring SAML IdP settings	183
Configuring SP settings on FortiAuthenticator	183
Configuring the login page replacement message	184
Results	185
SAML IdP proxy for Google Workspace	185
Configuring OAuth settings	186
Configuring the remote SAML server	186
Creating a remote SAML user synchronization rule	187
Configuring a Google Workspace Realm	188
Configuring IdP settings	188
Configuring SP settings on FortiAuthenticator	189
Configuring the login page replacement message	190
Results	190
SAML FSSO with FortiAuthenticator and Okta	191
Configuring DNS and FortiAuthenticator's FQDN	191
Enabling FSSO and SAML on FortiAuthenticator	192
Configuring the Okta developer account IdP application	195
Importing the IdP certificate and metadata on FortiAuthenticator	197
Configuring FSSO on FortiGate	199
Office 365 SAML authentication using FortiAuthenticator with 2FA	206
Configure the remote LDAP server on FortiAuthenticator	207
Configure SAML settings on FortiAuthenticator	208
Configure two-factor authentication on FortiAuthenticator	209
Configure the domain and SAML SP in Microsoft Azure AD PowerShell	210
Configure Microsoft Azure AD Connect	213
Results	219
FortiGate SSL VPN with FortiAuthenticator as the IdP proxy for Azure	221
Configuring Azure	223
Configuring FortiAuthenticator	226
Configuring FortiGate	230
Results	232
SAML FSSO with FortiAuthenticator and Microsoft Azure AD	233
Creating a tenant in Azure Portal	234
Creating an enterprise application in Azure Portal	235
Setting up single sign-on for an enterprise application	236
Adding the enterprise application as an assignment	239

Registering the enterprise application with Microsoft identity platform and generating authentication key	239
Creating a remote OAuth server with Azure application ID and authentication key	240
Creating a remote SAML server	240
Setting up SAML SSO in FortiAuthenticator	241
Adding an FSSO agent	242
Configuring an interface to use an external captive portal	242
Configuring a policy to allow a local network to access Microsoft Azure services	243
Creating an exempt policy to allow users to access the captive portal	244
Results	244
Office 365 SAML authentication using FortiAuthenticator with 2FA in Azure/ADFS hybrid environment	245
Configure FortiAuthenticator as an SP in ADFS	245
Configure the remote SAML server on FortiAuthenticator	245
Configure SAML settings on FortiAuthenticator	246
Configure two-factor authentication on FortiAuthenticator	248
Configure FortiAuthenticator replacement messages	249
Results	249
SSL VPN SAML authentication using FortiAuthenticator with OneLogin as SAML IdP	250
Prerequisites and scope of the recipe	251
Creating an OneLogin application	252
Configuring an application on OneLogin	252
Granting user access to the application	256
Configuring a remote SAML server	257
Configuring an OneLogin realm	259
Creating remote SAML users	259
Configuring SAML IdP settings	260
Configuring FortiAuthenticator replacement message	261
Configuring FortiGate SP settings on FortiAuthenticator	261
Uploading SAML IdP certificate to the FortiGate SP	263
Creating SAML user and server	264
Mapping SSL VPN authentication portal	266
Increasing remote authentication timeout using FortiGate CLI	267
Configuring a policy to allow users access to allowed network resources	267
FortiGate SSL VPN with FortiAuthenticator as SAML IdP	268
Certificate management	269
FortiAuthenticator user management	273
SAML IdP and SP configurations	274
FortiGate user management	277
FortiGate SSL VPN configurations	278
FortiClient configurations	284
Testing and verification	286
Computer Authentication	291
Computer authentication using FortiAuthenticator with MS AD Root CA	291
Configure the certificates and Root CA	292
Configure LDAP users on FortiAuthenticator	293
Configure RADIUS authentication	296
Configure the SSID and interface objects	301

Results	303
WiFi onboarding using FortiAuthenticator Smart Connect	305
Initial settings on FortiAuthenticator	305
Install certificates	306
Configure the RADIUS client settings	307
Configure the local root CA	308
Configure the EAP server certificate and CA for EAP-TLS	309
Option A - WiFi onboarding with Smart Connect and Google Workspace	309
Configure Google Workspace LDAPS Integration	310
Configure Smart Connect and the captive portal	315
Configure RADIUS settings on FortiAuthenticator	318
Option B - WiFi onboarding with Smart Connect and Azure	319
Configure Azure AD DS LDAPS integration	319
Configure Smart Connect and the captive portal	324
Configure RADIUS settings on FortiAuthenticator	328
FortiGate configuration	328
Configure the RADIUS server on FortiGate	329
Create the user group for cloud-based directory user accounts	329
Provision the Onboarding and Secure WiFi networks	330
Results	338
Smart Connect Windows device onboarding process	338
Smart Connect iOS device onboarding process	340
ZTNA	342
Setting up a zero trust tunnel	342
Configuring a zero trust tunnel on FortiAuthenticator	342
Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator	343
Configuring certificate authentication for FortiAuthenticator	343
Configuring a ZTNA server	346
Configuring a ZTNA rule	347
Debugging	348

Change Log

Date	Change Description
2023-02-21	Initial release.
2023-03-06	Updated Generating the Google Workspace certificate on page 175 and Configuring LDAP on the FortiAuthenticator on page 178 .
2023-03-28	Added Debugging on page 348 . Updated: • Setting up a zero trust tunnel on page 342 • Configuring a zero trust tunnel on FortiAuthenticator on page 342 • Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator on page 343 • Configuring certificate authentication for FortiAuthenticator on page 343 • Configuring a ZTNA server on page 346
2023-06-09	Updated Configuring FSSO on FortiGate on page 199 .
2023-07-11	Updated Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 210 .
2023-08-21	Updated Configuring RADIUS client on FortiAuthenticator on page 132 .
2023-12-05	Updated Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 210 .
2024-01-10	Updated Creating a remote OAuth server with Azure application ID and authentication key on page 240 .
2025-07-22	Updated Configuring firewall authentication portal settings on FortiGate on page 77 .
2025-07-23	Updated Configuring firewall authentication portal settings on FortiGate on page 77 and Configuring firewall authentication portal settings on FortiGate on page 67 .

Certificate management

This section describes managing certificates with the FortiAuthenticator device.

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

FortiAuthenticator as a Certificate Authority

1. Create CA certificate on FAC



2. Download CA certificate to browser



3. Create CSR on FGT



6. Import signed certificate and apply to Admin GUI access



4. Import and sign CSR on FAC



5. Download signed certificate



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

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

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

Creating a new CA on the FortiAuthenticator

To create a new CA:

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

Create New Local CA Certificate

Certificate ID:

Certificate Authority Type

Certificate type: Root CA Intermediate CA Intermediate CA signing request (CSR)

☐ Use netHSM

Subject Information

Subject input method: Fully distinguished name Field-by-field

Name (CN):

Department (OU):

Company (O):

City (L):

State/Province (ST):

Country (C):

Email address:

Key And Signing Options

Validity period: Set length of time Set an expiry date

days

Key type: RSA

Key size: 1024 2048 4096

Hash algorithm: SHA-256 SHA-1

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

+ Advanced Options: Key Usages

Certificate Revocation List (CRL)

Lifetime: days (1-365)

Re-generate every: days

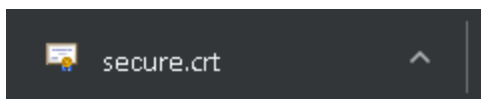
OK Cancel

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

+ Create New	Import	Revoke	Delete	Export Certificate	Export Key and Cert	Search for local CA certificates
☒	Certificate ID	Subject	Issuer	Status	CA Type	
☒	secure	CN=secure	CN=secure	Active	Root CA	

1 local CA certificate

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

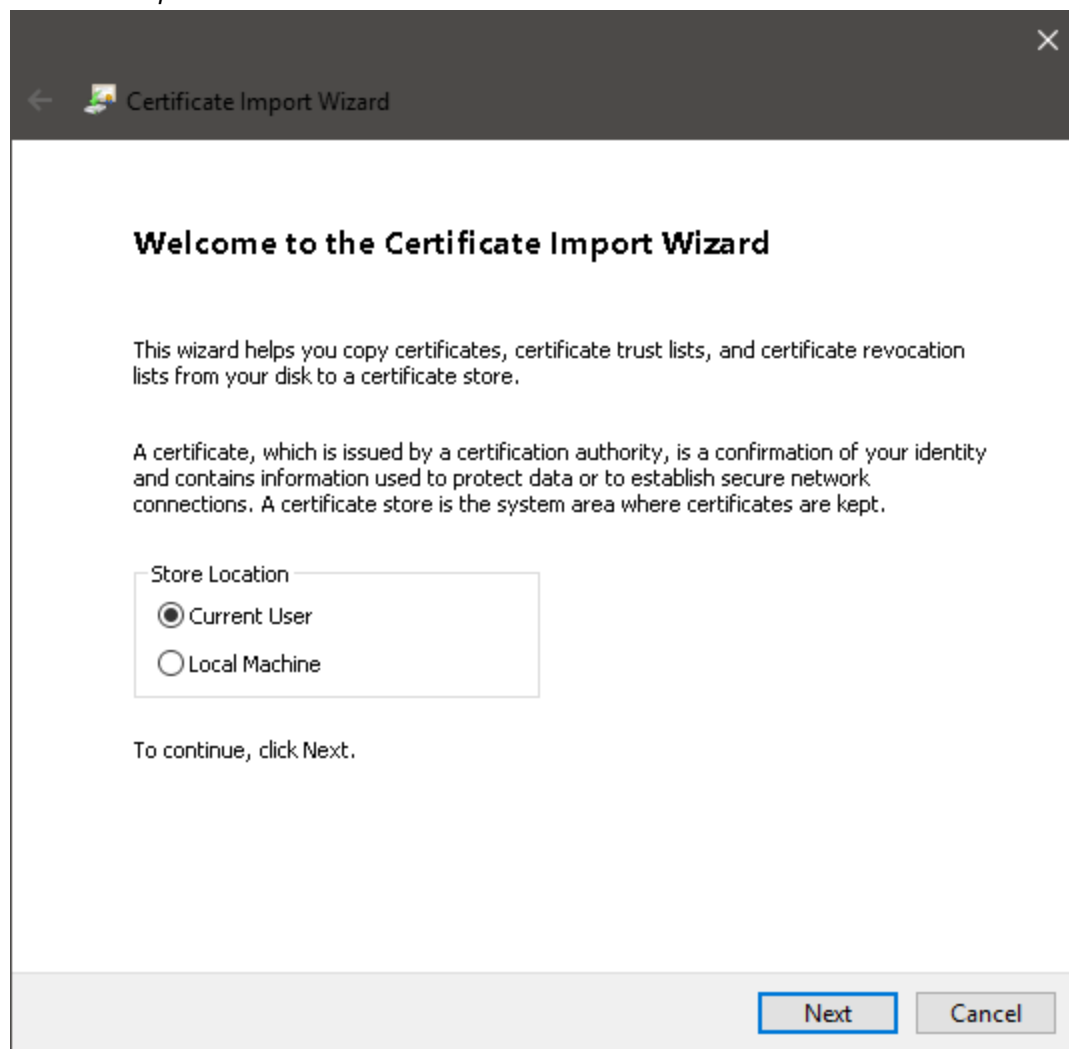


Installing the CA on the network

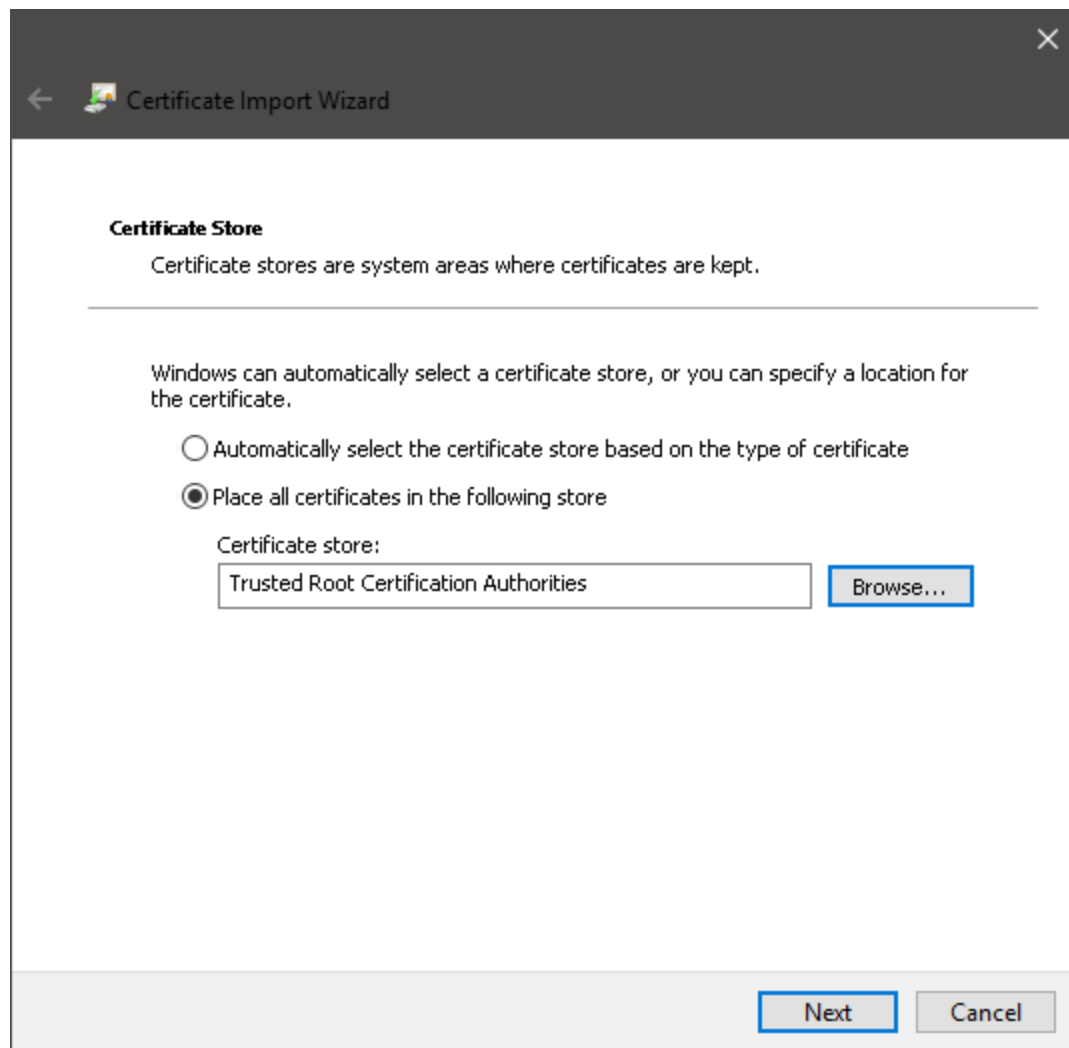
The certificate must now be installed on the computers in your network as a trusted root CA. The steps below show different methods of installing the certificate, depending on your browser.

Internet Explorer and Chrome

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



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

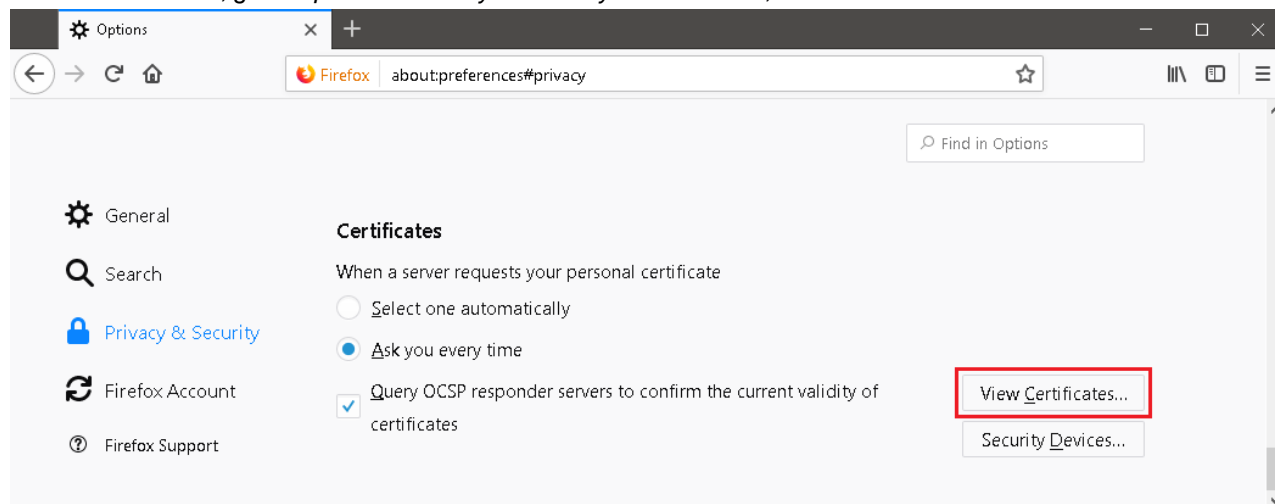


3. Finish the Wizard and select Yes to confirm and install the certificate.

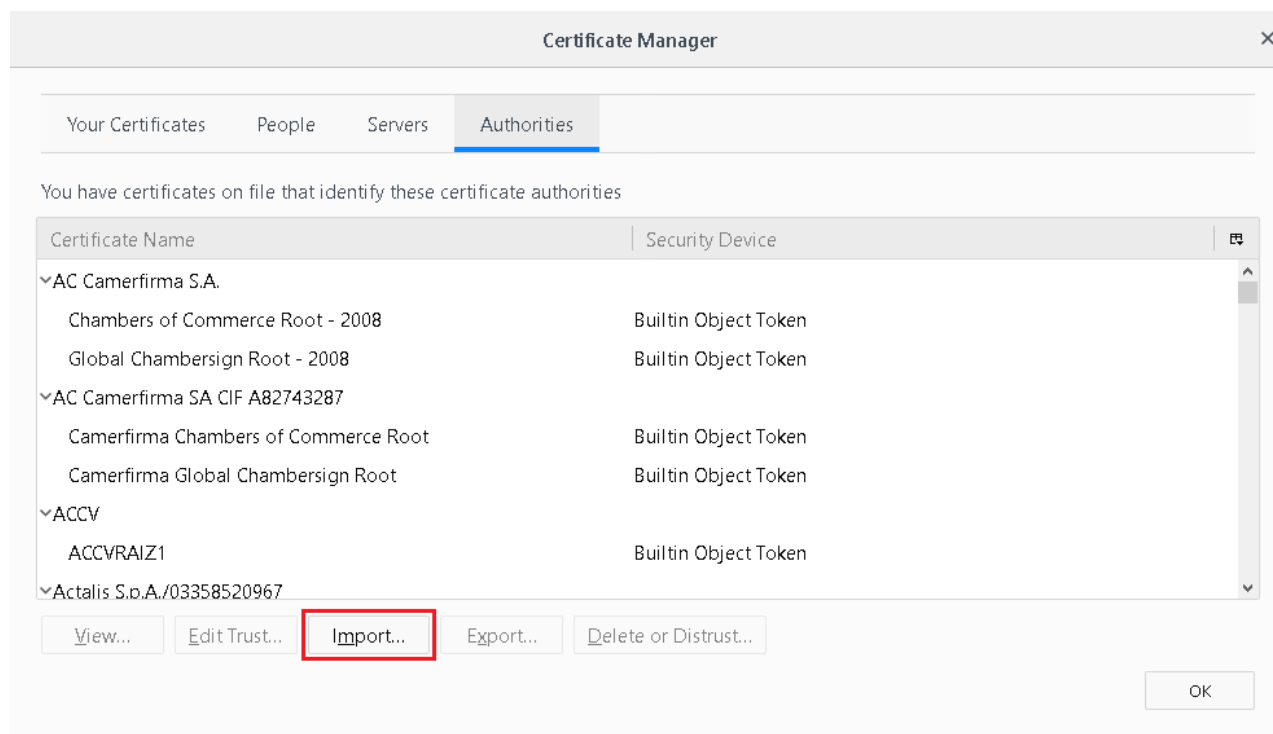


Firefox

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).

Importing and signing the CSR on the FortiAuthenticator

To import and sign the CSR:

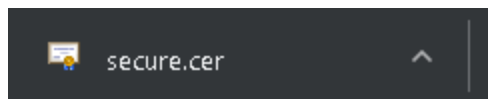
1. Back on the FortiAuthenticator, go to *Certificate Management > End Entities > Users* and import the .csr certificate created earlier.

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*.

+ Create New 📁 Import ✖ Revoke 🗑 Delete 📄 Export Certificate 📄 Export Key and Cert Search for user certificates				
✓ Certificate signing request "CN=172.25.176.127, emailAddress=joy@offworld.com" was signed with CA certificate "C=CA, ST=ON, L=Ottawa, O=Fortinet, OU=FIPS-CC, CN=Certs, emailAddress=..."				
☐	Certificate ID	Subject	Issuer	Status
☒	secure	CN=172.25.176.127, emailAddress=joy@offworld.com	C=CA, ST=ON, L=Ottawa, O=Fortinet, OU=FIPS-CC, CN=Certs, email...	Active

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



Importing the local certificate to the FortiGate

To import the local certificate:

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

Import Certificate

Type Local Certificate PKCS #12 Certificate Certificate

Certificate file + secure.cer

OK Cancel

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

Name	Status	Subject
Certificates (10)		
 secure	 OK	emailAddress = joy@offworld.com, CN = 172.25.178.127

Configuring the certificate for the GUI

To configure the certificate:

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

Administration Settings

HTTP port

80

Redirect to HTTPS



HTTPS port

8443

HTTPS server certificate

secure ▼

SSH port

22

Telnet port

23

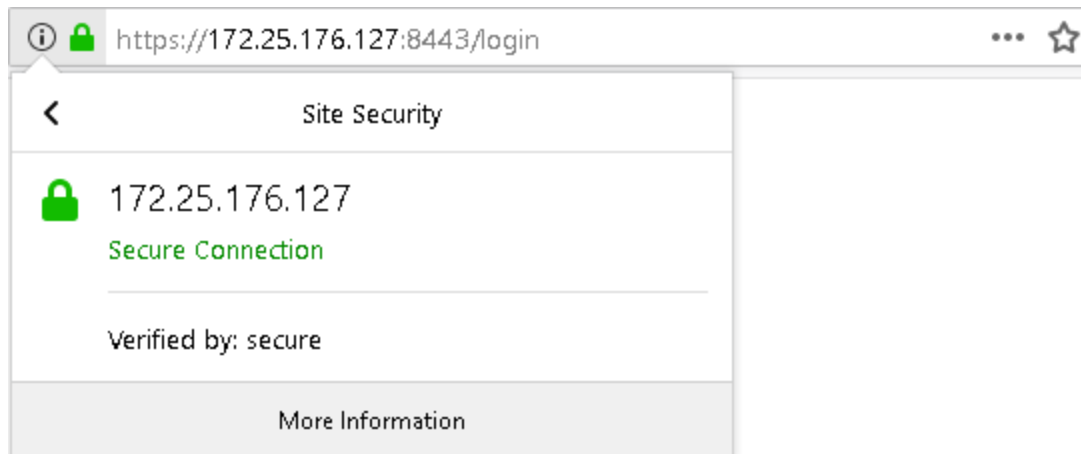
Idle timeout

45

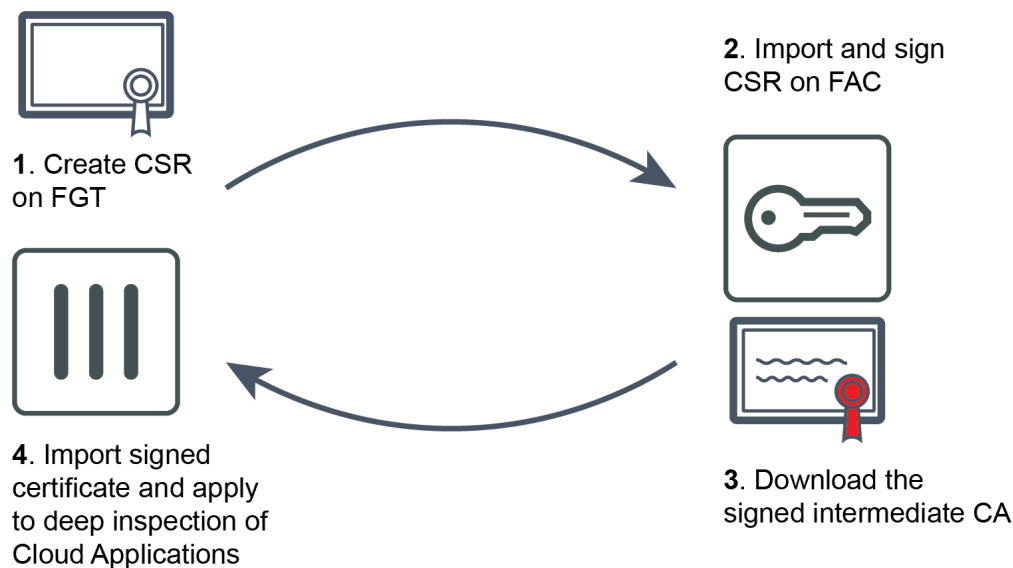
Minutes (1 - 480)

Results

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



FortiAuthenticator certificate with SSL inspection



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

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

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

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

Creating a CSR on the FortiGate

To create a CSR:

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

Certificate Name

Subject Information

ID Type ☒ Host IP ☐ Domain Name ☐ E-Mail

IP

Optional Information

Organization Unit



Organization

Locality(City)

State / Province

Country / Region ☐

E-Mail

Subject Alternative Name

Password for private key

Key Type ☒ RSA ☐ Elliptic Curve

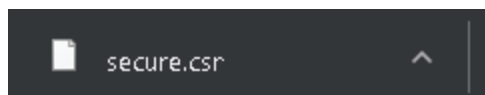
Key Size ☐ 1024 Bit ☐ 1536 Bit ☒ 2048 Bit ☐ 4096 Bit

Enrollment Method ☒ File Based ☐ Online SCEP

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

						Search	
Name	Status	Subject					
Certificates (1)							
secure	Pending						

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



Creating an Intermediate CA on the FortiAuthenticator

To create an Intermediate CA:

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

Import Signing Request or Local CA Certificate

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

Certificate ID: secure.local

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

Certificate Signing Options

Certificate authority: [dropdown]

Validity period: Set length of time Set an expiry date

3650 days

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

Subject Alternative Name

☐ Email: [text box]

☐ User Principal Name (UPN): [text box]

+ Advanced Options: Key Usages

OK Cancel

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*.

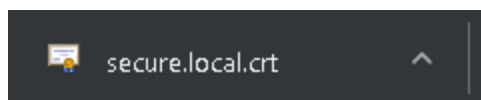
+ Create New Import Revoke Delete **Export Certificate** Export Key and Cert Search for local CA certificates

Certificate signing request "CN=172.25.176.127, emailAddress=abristow@fortinet.com" was signed with CA certificate "CN=CA, C=US, OU=Fortinet, O=Fortinet, OU=PKI-CA, OU=CA, OU=CA"

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

☐	Certificate ID	Subject	Issuer	Status	CA Type
☒	secure.local	CN=172.25.176.127, emailAddress=abristow@fortinet.com	CN=CA, C=US, OU=Fortinet, O=Fortinet, OU=PKI-CA, OU=CA, OU=CA	Active	Intermediate (non-signing) CA

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



Importing the signed certificate on the FortiGate

To import the signed certificate:

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

✕

Import Certificate

Type Local Certificate
PKCS #12 Certificate
Certificate

Certificate file + secure.local.crt

OK
Cancel

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

+ Generate ✎ Edit 🗑 Delete 📁 Import ▾ 👁 View Details ⬇ Download Search 🔍			
🔽 Name	🔽 Subject	🔽 Issuer	🔽 Status
Certificates (10)			
 my-csr	emailAddress = admin@fortinet.com , CN = 172.25.178.127	Fortinet	✔ OK

Configuring full SSL inspection

To configure full SSL inspection:

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

✕

New SSL/SSH Inspection Profile

Name

deep-inspection-cloud-apps

Comments

Write a comment...

0/255

SSL Inspection Options

Enable SSL Inspection of

Multiple Clients Connecting to Multiple Servers

Protecting SSL Server

Inspection Method

SSL Certificate Inspection

Full SSL Inspection

CA Certificate ⚠

my-csr

⬇

⬇ Download Certificate

Untrusted SSL Certificates

Allow

Block

📋 View Trusted CAs List

RPC over HTTPS

☐

- 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.

FortiAuthenticator 6.5.0 Cookbook
Fortinet Inc.

23

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

Edit Policy

Name ⓘ

internet

Incoming Interface

lan

+

✕

Outgoing Interface

wan1

+

✕

Source

all

+

✕

Destination

all

+

✕

Schedule

always

▼

Service

ALL

+

✕

Action

✓ ACCEPT

✗ DENY

IPsec

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

ON

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

OFF

Protocol Options

PRX default

✎

Security Profiles

AntiVirus

OFF

Web Filter

OFF

DNS Filter

OFF

Application Control

ON

APP default

✎

IPS

OFF

VoIP

OFF

SSL Inspection ⚠

SSL

deep-inspection-cloud-app

✎

Mirror SSL Traffic to Interfaces

OFF

Logging Options

Log Allowed Traffic

ON

Security Events

All Sessions

Comments

Write a comment...

0/1023

Enable this policy

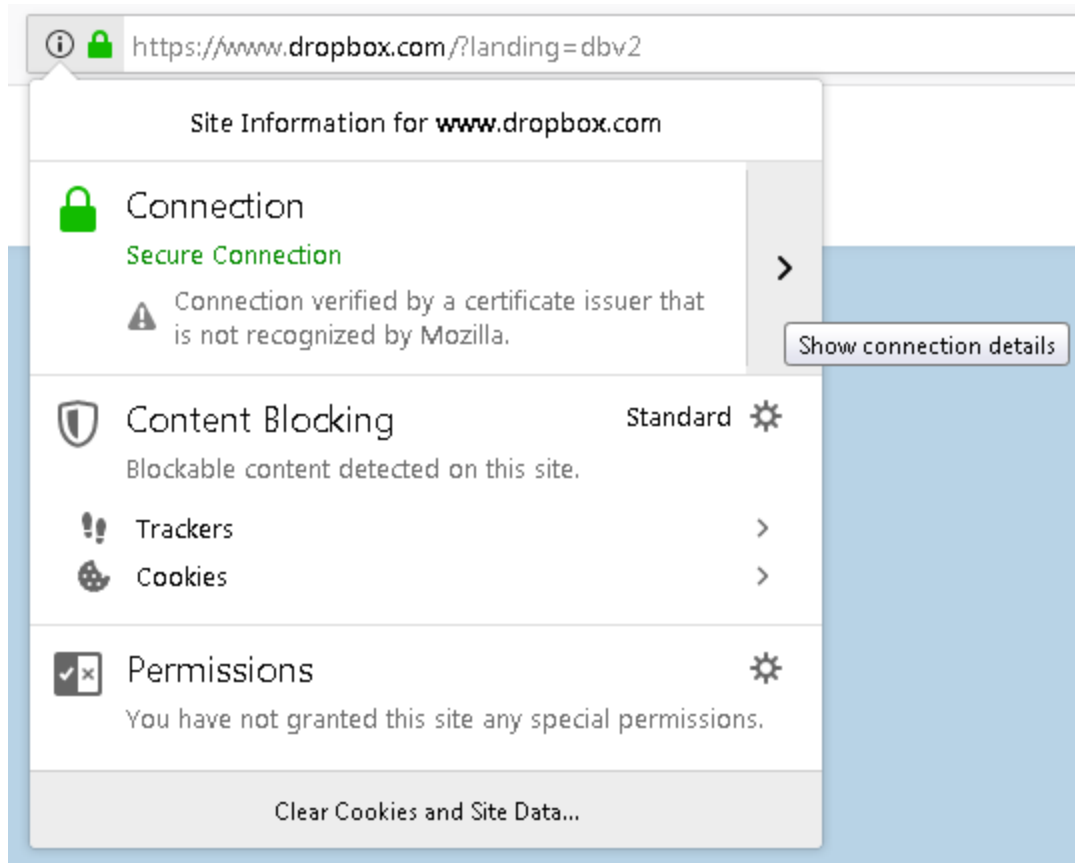
ON

FortiAuthenticator 6.5.0 Cookbook
Fortinet Inc.

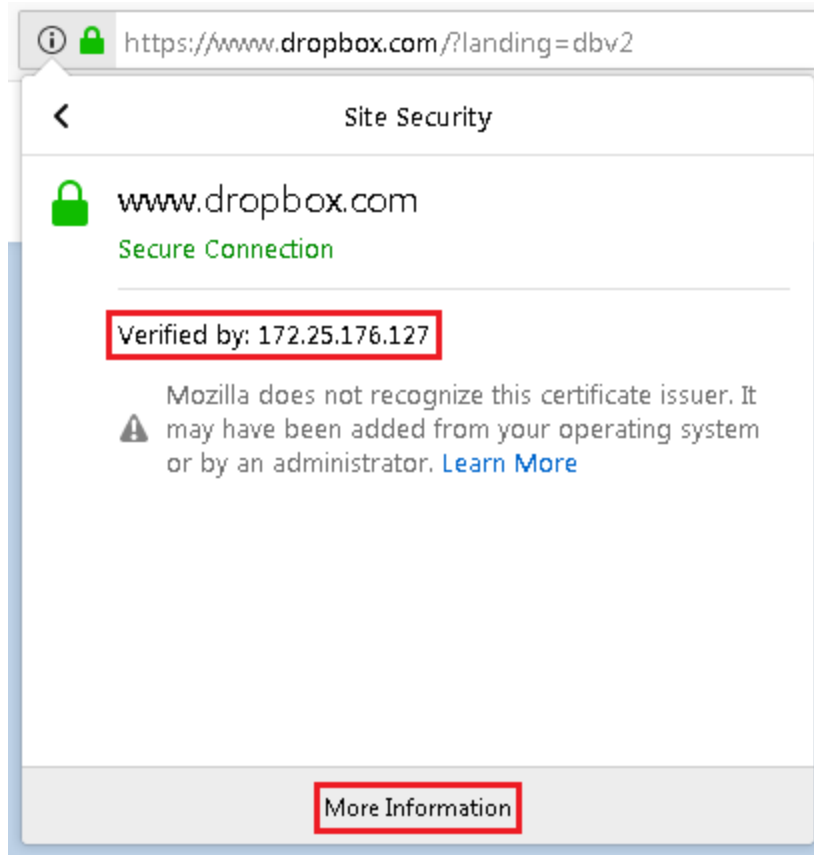
24

Results

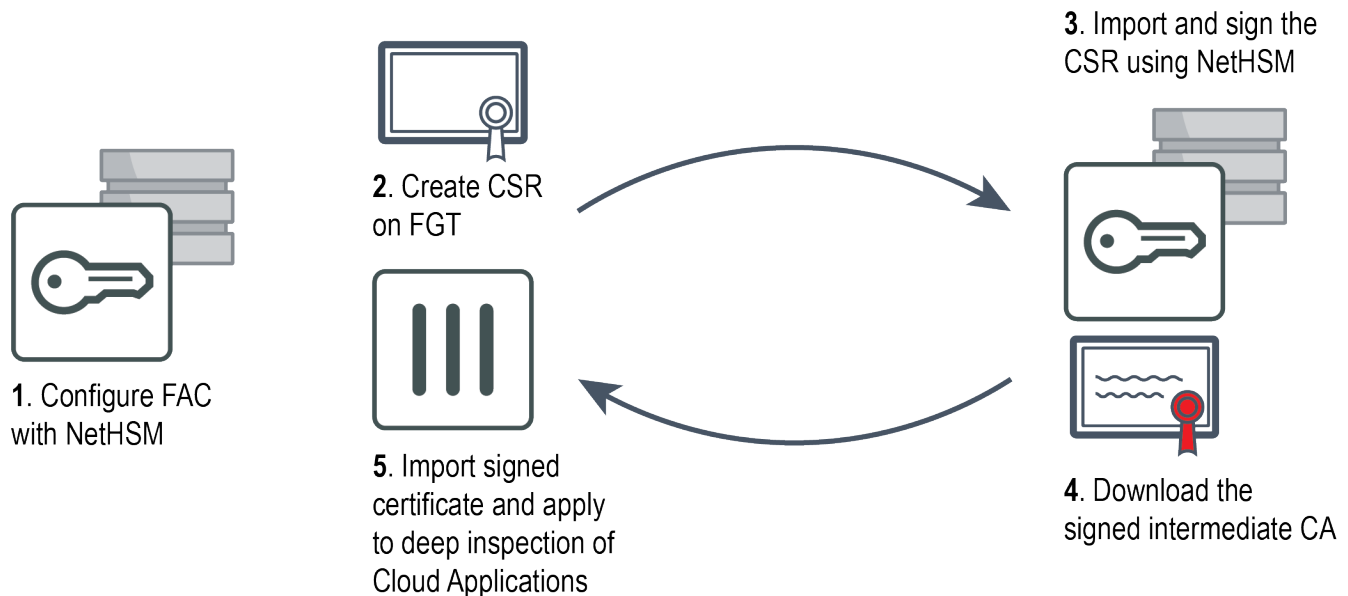
1. To test the certificate, open your web browser and attempt to navigate to an HTTPS website (in the example, <https://www.dropbox.com>).
Click on the lock icon next to the address bar and click *Show connection details*.



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

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

1. [Configuring the NetHSM profile on FortiAuthenticator on page 28](#)
2. [Creating a local CA certificate using an HSM server on page 29](#)
3. [Creating a CSR on the FortiGate on page 29](#)
4. [Creating an Intermediate CA on the FortiAuthenticator on page 31](#)
5. [Importing the signed certificate on the FortiGate on page 31](#)
6. [Configuring full SSL inspection on page 32](#)
7. [Results on page 34](#)

In order for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this recipe will not be trusted. For more information on how to do this, see [Creating a local CA certificate using an HSM server on page 29](#) 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 <i>Upload server certificate</i> to select the certificate from your HSM.

3. Click *OK* to complete the setup.

To authorize FortiAuthenticator as a Safenet Luna HSM client:

1. Make sure the FortiAuthenticator client certificate uses the `<FAC IP>.pem` naming convention. For example: `172.16.68.47.pem`
2. Upload the FortiAuthenticator client certificate to Safenet Luna HSM using SCP transfer.

```
scp [certificate filename] admin@[HSM address]:
```
3. Use SSH to connect to the HSM, then register your FortiAuthenticator, and associate it with a partition.

```
ssh -l admin [HSM address]
client register -c [client name] -ip [client address]
client assignpartition -c [client name] -p [partition name]
```
4. Confirm the status of the NetHSM client. For example:

```
client show -c my_fac
ClientID: my_fac
IPAddress: 172.16.68.47
Partitions: my_partition
```

Creating a local CA certificate using an HSM server

Once you have configured the HSM server on FortiAuthenticator, you can create a local CA certificate using the HSM server to sign requests. For more information on setting up a certificate authority, see [FortiAuthenticator as a Certificate Authority on page 10](#).

To create a new local CA certificate using HSM:

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

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

Once your CA certificate has been created, it can be exported and installed on your network. For more information on setting up a certificate authority, see [FortiAuthenticator as a Certificate Authority on page 10](#).

Creating a CSR on the FortiGate

To create a CSR:

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

Enter a *Certificate Name*, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.

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

Certificate Name

Subject Information

ID Type ☒ Host IP ☐ Domain Name ☐ E-Mail

IP

Optional Information

Organization Unit



Organization

Locality(City)

State / Province

Country / Region ☐

E-Mail

Subject Alternative Name

Password for private key

Key Type ☒ RSA ☐ Elliptic Curve

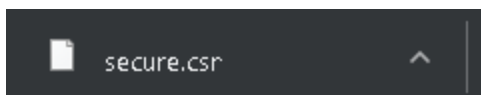
Key Size ☐ 1024 Bit ☐ 1536 Bit ☒ 2048 Bit ☐ 4096 Bit

Enrollment Method ☒ File Based ☐ Online SCEP

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

Name	Status	Subject
Certificates (1)		
secure	Pending	

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



Creating an Intermediate CA on the FortiAuthenticator

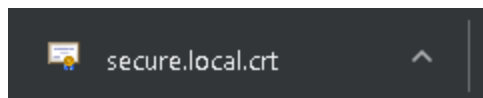
To create an Intermediate CA:

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

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

Certificate ID	Subject	Issuer	Status	CA Type
secure.local	CN=172.25.176.127, emailAddress=bristolw@fortinet.com	CN=FA, ST=0411, O=Fortinet, OU=Fortinet, CN=Fortinet, email=...	Active	Intermediate (non-signing) CA

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



Importing the signed certificate on the FortiGate

To import the signed certificate:

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

✕

Import Certificate

Type Local Certificate PKCS #12 Certificate Certificate

Certificate file + secure.local.crt

OK
Cancel

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

+ Generate ✎ Edit 🗑 Delete 📁 Import ▾ 👁 View Details 📄 Download Search 🔍			
▼ Name	▼ Subject	▼ Issuer	▼ Status
Certificates (10)			
 my-csr	emailAddress = [redacted] , CN = 172.25.178.127	Fortinet	✔ OK

Configuring full SSL inspection

To configure full SSL inspection:

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

✕

New SSL/SSH Inspection Profile

Name

deep-inspection-cloud-apps

Comments

Write a comment...

0/255

SSL Inspection Options

Enable SSL Inspection of

Multiple Clients Connecting to Multiple Servers

Inspection Method

Full SSL Inspection

CA Certificate ⚠

my-csr

Download Certificate

Untrusted SSL Certificates

Allow

RPC over HTTPS

Block
View Trusted CAs List

- 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.

FortiAuthenticator 6.5.0 Cookbook
Fortinet Inc.

32

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

Edit Policy

Name ⓘ

internet

Incoming Interface

lan

+

✕

Outgoing Interface

wan1

+

✕

Source

all

+

✕

Destination

all

+

✕

Schedule

always

▼

Service

ALL

+

✕

Action

✓ ACCEPT

✗ DENY

IPsec

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

🟢

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

🔴

Protocol Options

PRX

default

✎

Security Profiles

AntiVirus

🔴

Web Filter

🔴

DNS Filter

🔴

Application Control

🟢

APP

default

✎

IPS

🔴

VoIP

🔴

SSL Inspection ⚠

SSL

deep-inspection-cloud-app

✎

Mirror SSL Traffic to Interfaces

🔴

Logging Options

Log Allowed Traffic

🟢

Security Events

All Sessions

Comments

Write a comment...

0/1023

Enable this policy

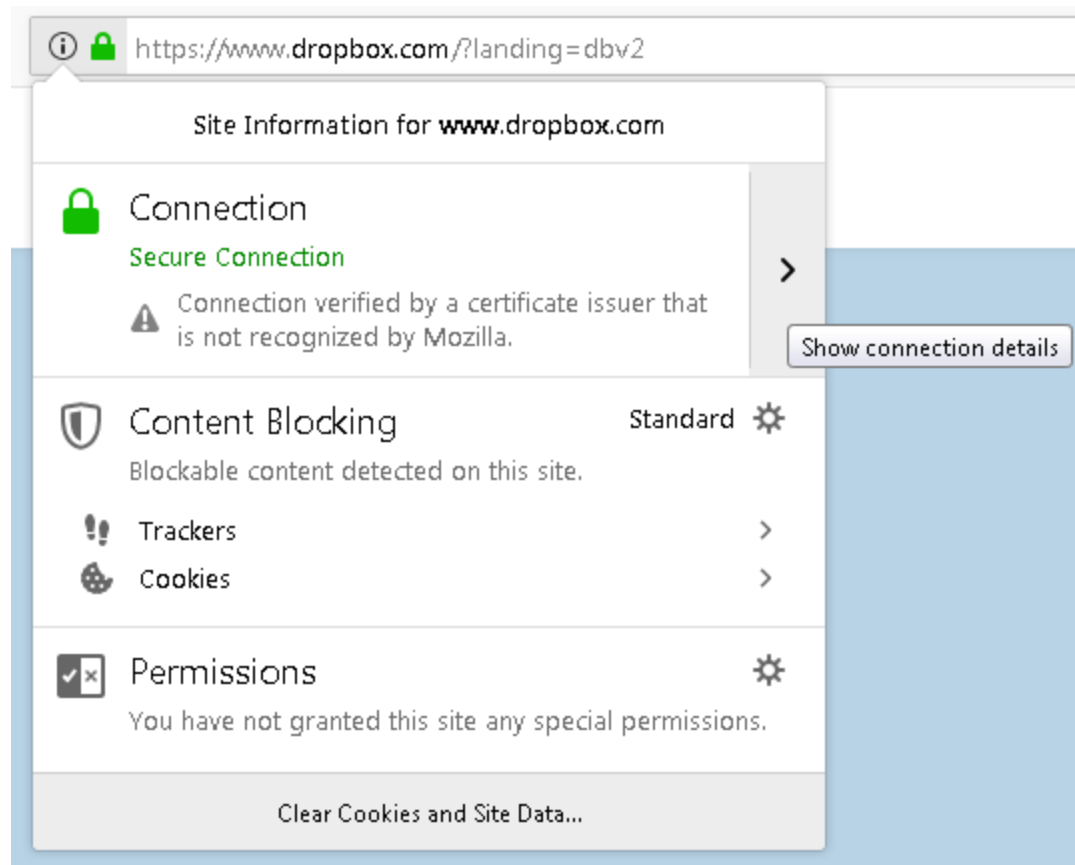
🟢

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

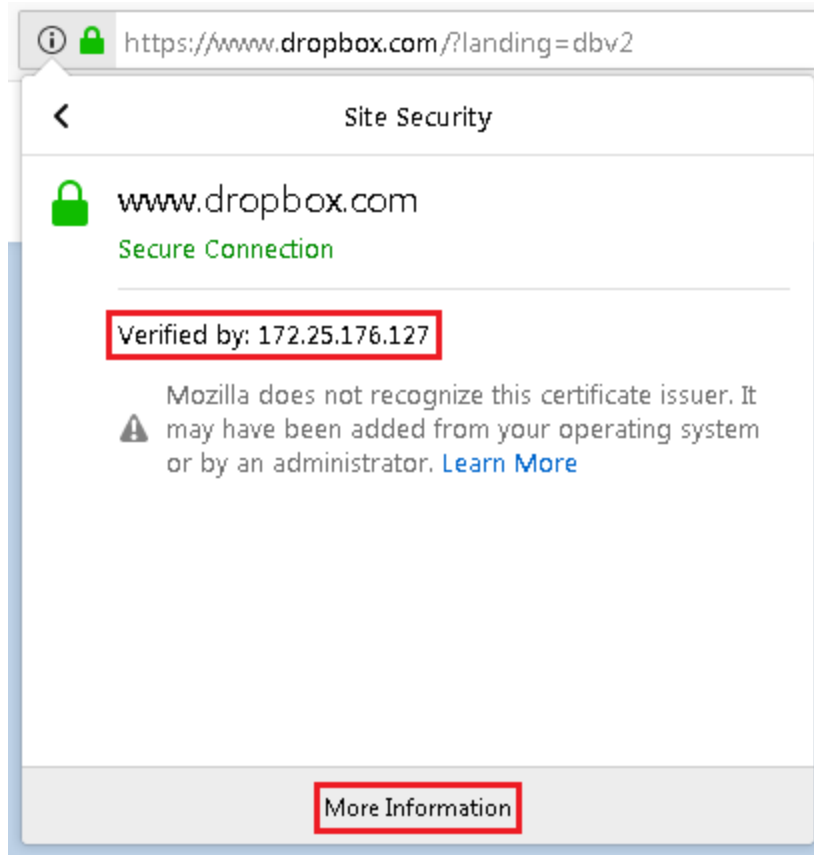
Results

1. To test the certificate, open your web browser and attempt to navigate to an HTTPS website (in the example, <https://www.dropbox.com>).

Click on the lock icon next to the address bar, and click *Show connection details*.



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*.

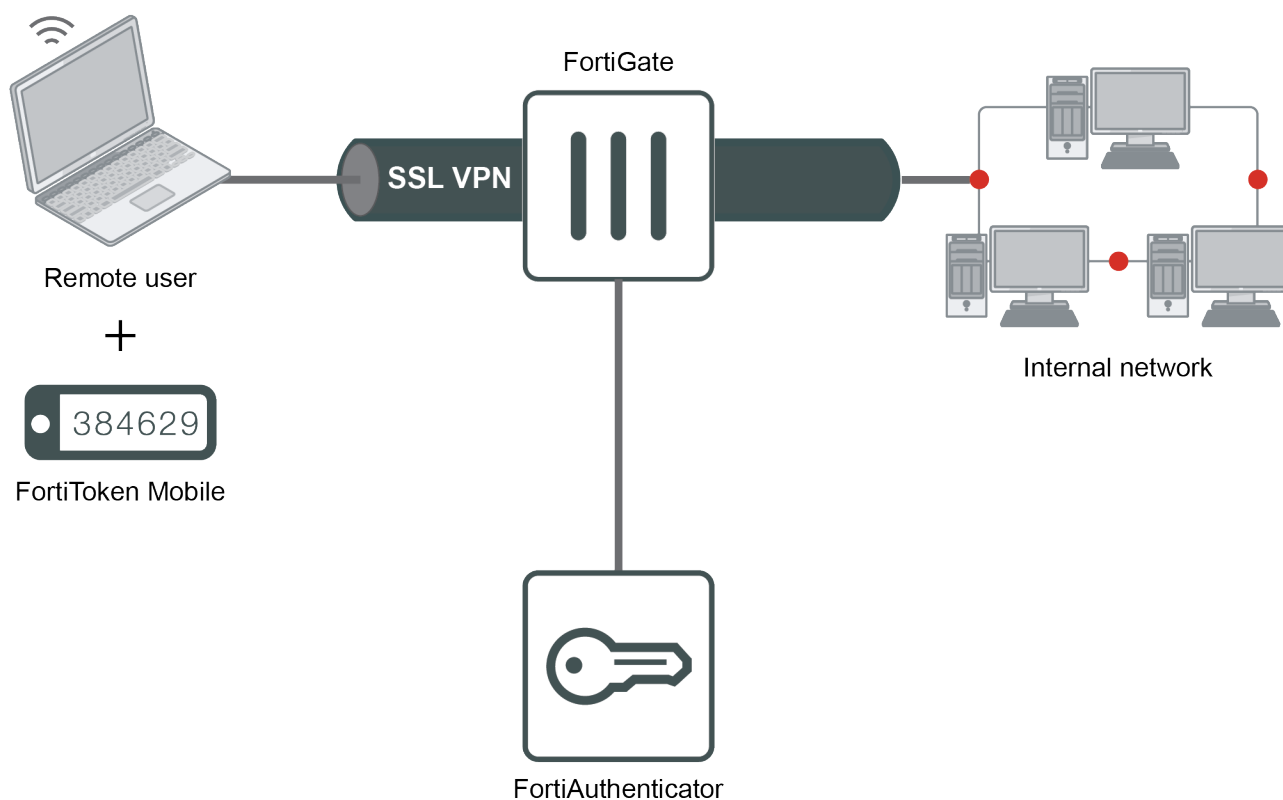


FortiToken and FortiToken Mobile

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

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

FortiToken Mobile Push for SSL VPN



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

For this configuration, you:

- Create a user on the FortiAuthenticator.
- Assign a FortiToken Mobile license to the user.

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

The following names and IP addresses are used:

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

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

- [FortiToken Mobile for Android](#)
- [FortiToken Mobile for iOS](#)

Adding a FortiToken to the FortiAuthenticator

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

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

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



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

Once configured, you can add your FortiToken.

To add a FortiToken:

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

Create New FortiToken

Token type: FortiToken Hardware FortiToken Mobile

☒ Get FortiToken Mobile free trial tokens

Activation codes: +

OK Cancel

Adding the user to the FortiAuthenticator

To add a user to FortiAuthenticator:

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

Create New Local User

Username:

Password creation: Specify a password ▼

Password:

Password confirmation:

☒ Allow RADIUS authentication

☐ Force password change on next logon

Role

Role: Administrator Sponsor User

Account Expiration

☐ Enable account expiration

OK Cancel

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

Edit Local User

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

Username: gthreepwood

☐ Disabled

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

☒ Token-based authentication

Deliver token code by:

FortiToken
Email
SMS
Dual (Email & SMS)

Hardware
Mobile
Cloud

Token:

Activation delivery method:

Email
SMS

[+ Temporary token](#)

☒ Allow RADIUS authentication

☐ Enable account expiration

☐ Force password change on next logon

User Role

Role:

Administrator
Sponsor
User

☐ Allow LDAP browsing

+ User Information

First name:
Last name:

Email:
Phone number:

Mobile number:
SMS gateway: Use default [Test SMS](#)

Street address:

City:
State/Province:

Country:

Language: Use default

Organization: [Please Select]

+ Alternative Email Addresses

+ Password Recovery Options

+ Groups

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

Create New User Group

Name: RemoteFTMUsers

Type:

Local
Remote LDAP
Remote RADIUS
Remote SAML
MAC

Users:

Available Users

Filter

admin

Selected Users

gthreepwood

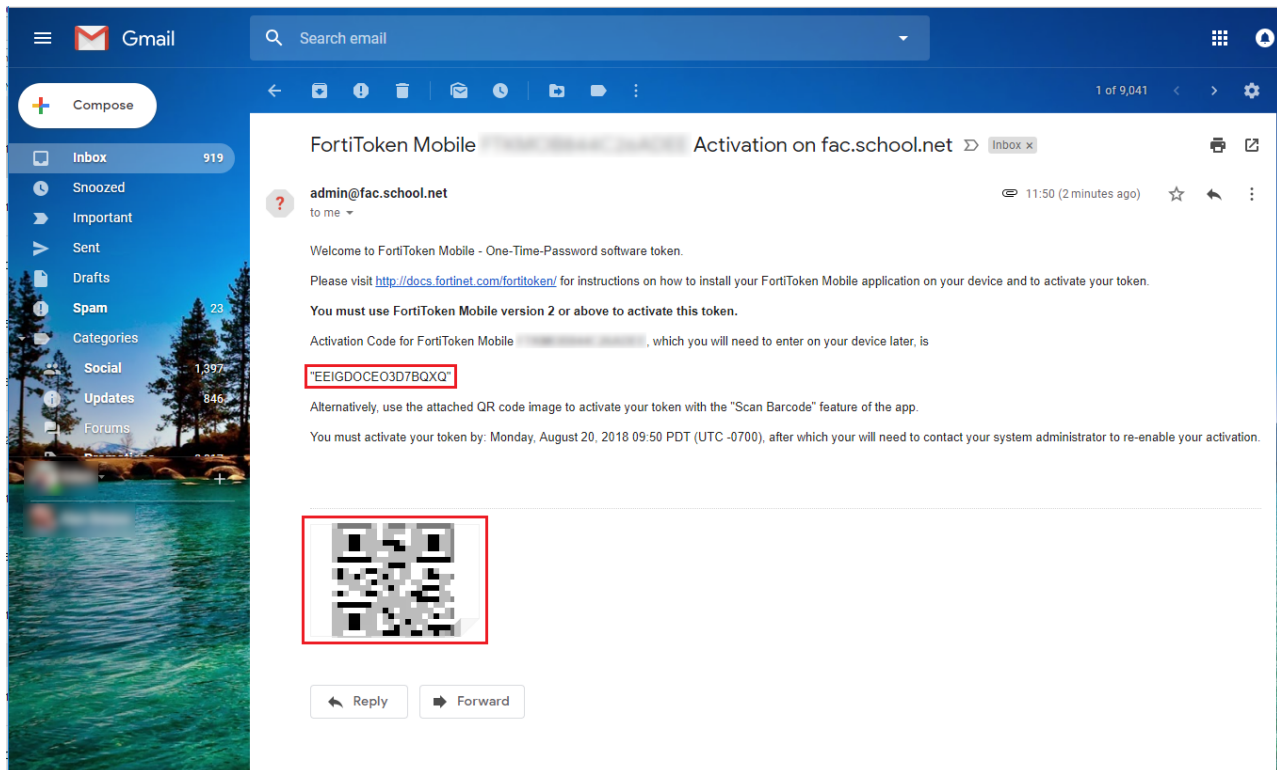
Choose all
Remove all

Password policy: Default

☐ Usage Profile [Please Select]

OK Cancel

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*.

FortiAuthenticator VM FAC-VM0000000000

System > Edit Authentication Client

Authentication > Name: FortiGate

Client address: 172.25.176.92

Secret: *****

☐ Accept RADIUS accounting messages for usage enforcement

☐ Support RADIUS Disconnect messages

OK Cancel

To create the RADIUS policy:

1. Go to *Authentication > RADIUS Service > Policies*, and select *Create New*.
2. Enter the RADIUS policy name, description, and select the FortiGate RADIUS client.
3. 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*.

FortiAuthenticator VM FAC-VM0000000000

System > Authentication > RADIUS Service > Policies > Create New

RADIUS clients > RADIUS attribute criteria > Authentication type > Identity source > Authentication factors > RADIUS response

☒ Mandatory two-factor authentication

☐ Verify all configured authentication factors

☐ Password-only authentication

☐ Token-only authentication

☒ Allow FortiToken Mobile push notifications

☐ Reject usernames containing uppercase letters

☐ Device authorization

Previous Discard and exit Update and exit Next



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

Connecting the FortiGate to the RADIUS server

To connect the FortiGate to the RADIUS server:

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

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

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

New RADIUS Server

Name

OfficeRADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.25.176.141

Secret

••••••••

Connection status

☒ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

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

New RADIUS Test User Credentials ✕

Name Username

Authentication Password

NAS IP

Include in e Connection status ✔ Successful

Primary Server User credentials ✖ More validation is required

IP/Name Server message

Secret

Connection

Secondary Server

i AVP: l=79 t=Reply-Message(18) Value: '+Enter token code or no code to send a notification to your FortiToken Mobile'; AVP: l=11 t=Vendor-Specific(26) v=Fortinet(12356) VSA: l=5 t=Fortinet-Token-Challenge(15) Value: '001'; AVP: l=3 t=State(24) Value: 31

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

- Then go to *User & Device > User Groups*, and select *Create New* to map authenticated remote users to a user group on the FortiGate.

Enter a *Name* (SSLVPNGroup) and select *Add* under *Remote Groups*.

Select *OfficeRADIUS* under the *Remote Server* drop-down menu, and leave the *Groups* field blank.

New User Group

Name

Type Firewall

Fortinet Single Sign-On (FSSO)

RADIUS Single Sign-On (RSSO)

Guest

Members

Remote Groups

Remote Server	Group Name
OfficeRADIUS	Any

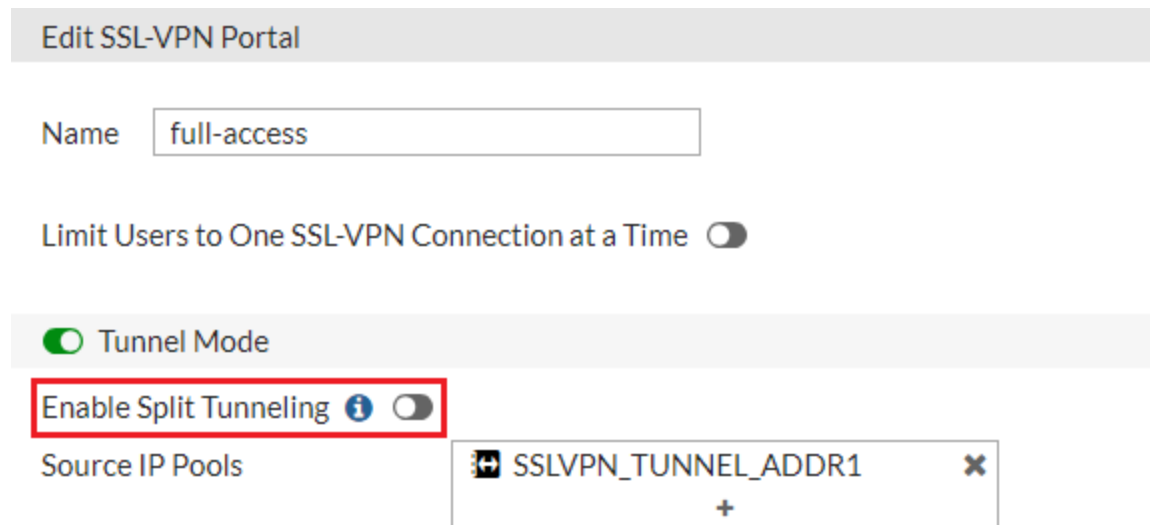
- In the FortiGate CLI, increase the remote authentication timeout to 60 seconds.
#config system global

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

Configuring the SSL-VPN

To configure the SSL-VPN:

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



Edit SSL-VPN Portal

Name

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

☒ Tunnel Mode

Enable Split Tunneling ☐

Source IP Pools

+

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

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s) wan1 + ×

Listen on Port 10443

Web mode access will be listening at <https://172.25.176.92:10443>

Redirect HTTP to SSL-VPN ☐

Restrict Access

Allow access from any host Limit access to specific hosts

Idle Logout ☒

Inactive For

300 Seconds

Server Certificate

Fortinet_Factory

 You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.

[Click here to learn more](#)

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range **Specify custom IP ranges**

IP Ranges

SSLVPN_TUNNEL_ADDR1 ×
SSLVPN_TUNNEL_IPv6_ADDR1 ×
+

DNS Server

Same as client system DNS Specify

Specify WINS Servers ☐

Allow Endpoint Registration ☐

Authentication/Portal Mapping ⓘ

+ Create New Edit Delete

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

Apply

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

New Policy

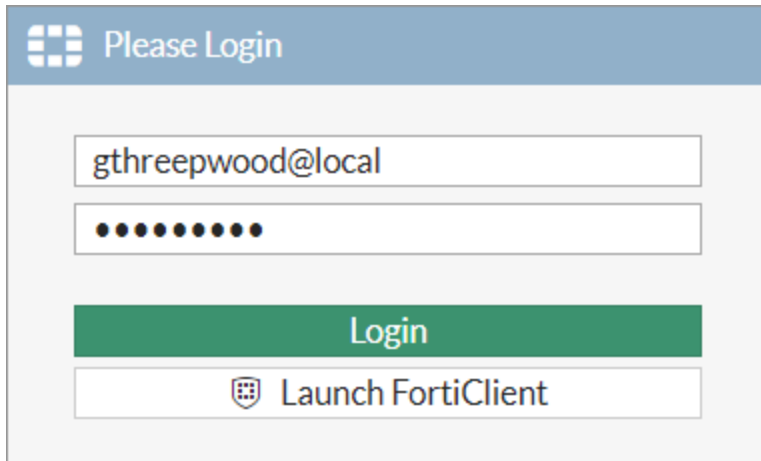
Name ⓘ	SSL-VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.root) ✕ +
Outgoing Interface	wan1 ✕ +
Source	all ✕ SSLVPNGroup ✕ +
Destination	all ✕ +
Schedule	always ▼
Service	ALL ✕ +
Action	✓ ACCEPT ✕ DENY 🎓 LEARN

Firewall / Network Options

NAT ☒

Results

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

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

Please Login

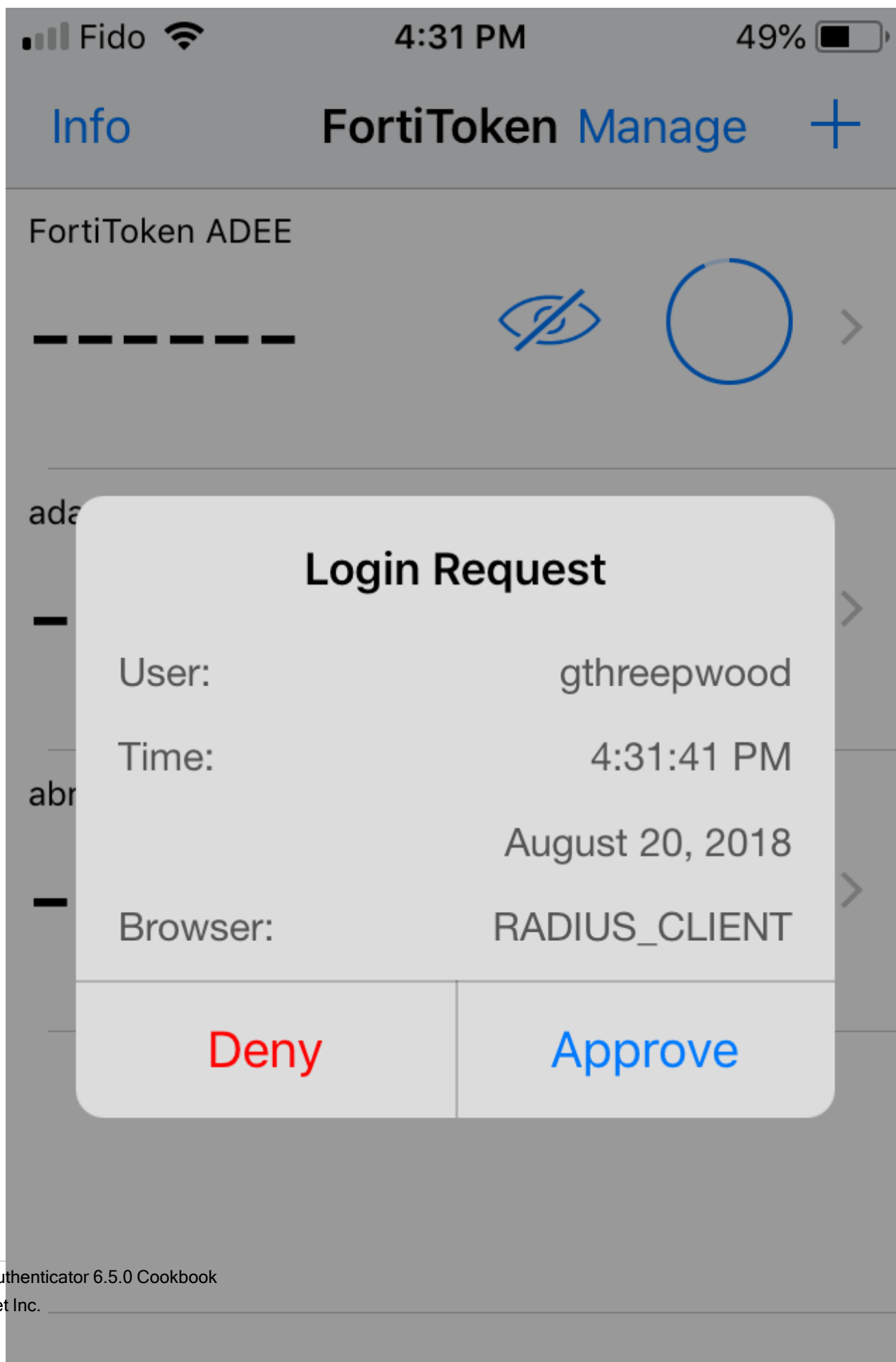
gthreepwood@local

●●●●●●●●●●

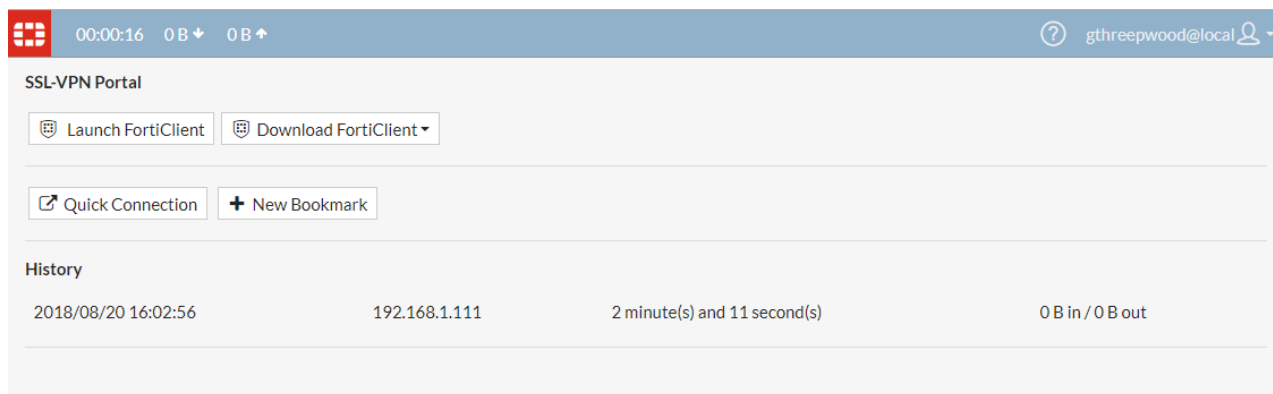
Login

Launch FortiClient

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



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



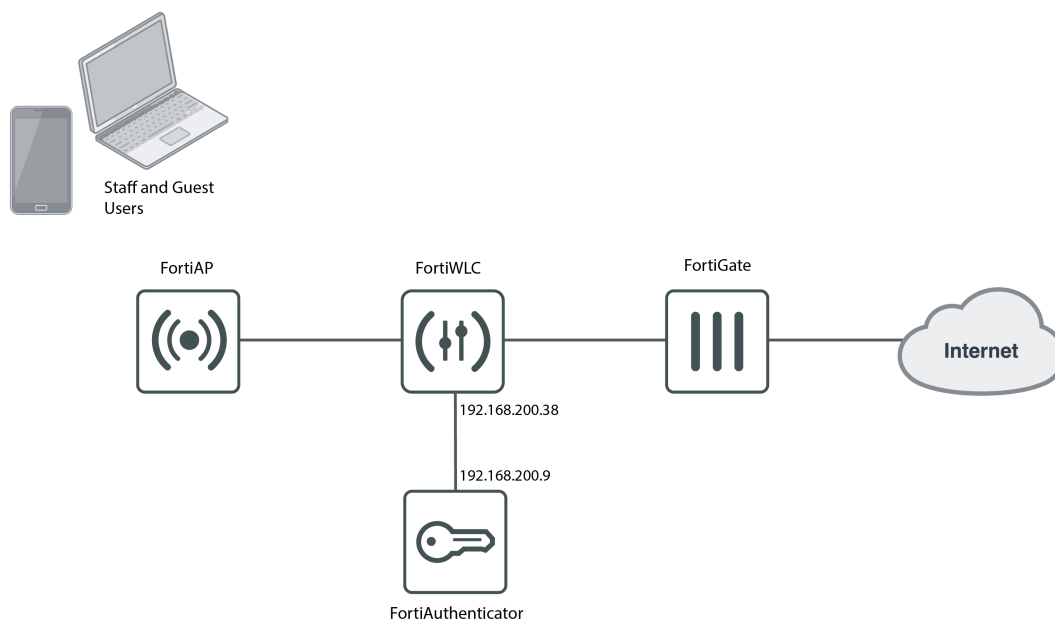
4. On the FortiGate, go to *Monitor > SSL-VPN Monitor* to confirm the user's connection.

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

Guest Portals

This section contains information about creating and using guest portals.

FortiAuthenticator as Guest Portal for FortiWLC



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

Creating the FortiAuthenticator as RADIUS server on the FortiWLC

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

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

RADIUS Profiles - Add ?

RADIUS Profile Name *	FAC-AUTH	Enter 1-16 chars.
Description	Authentication	Enter 0-128 chars.
RADIUS IP *	192.168.200.9	Enter 0-127 chars.
RADIUS Secret *	*****	Enter 1-64 chars.
RADIUS Port	1812	Valid range: [1024-65535]
Remote RADIUS Server	Off	
RADIUS Relay AP-ID	No Relay AP	
MAC Address Delimiter Calling Station	Hyphen (-)	
MAC Address Delimiter Called Station	Hyphen (-)	
Use Client IP as calling station id	No	
Password Type	Shared Key	
Called-Station-ID Type	Default	
COA	On	
RADIUS Server Timeout	2	Valid range: [1-20]
RADIUS Server Retries	3	Valid range: [1-10]
NAS IP		Enter IPv6 Address.

Creating the Captive Portal profile on the FortiWLC

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

- *Public IP of Controller*: IP address that the FortiAuthenticator can use to communicate with the FortiWLC.

Add Captive Portal Profile

CP Name *	FortiAuthenticator	Enter 1-32 chars.
-----------	--------------------	-------------------

User Authentication		
Authentication Type	radius	
Radius Authentication		
Primary Authentication	FAC-AUTH	
Secondary Authentication	No Radius	
Radius Accounting		
Primary Accounting	FAC-ACCT	
Secondary Accounting	No Radius	
Accounting Interim Interval	600	Valid range: [60-36000].

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

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

Creating the security profile on the FortiWLC

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

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

Security Profiles - Add ?

Security Profile Name *	FAC-CP	Enter 1-32 chars.
SECURITY SETTINGS		
Online Sign Up	not-configured	
Security Mode *	Open	
CAPTIVE PORTAL SETTINGS		
Captive Portal	WebAuth	
Captive Portal profile	FortiAuthenticator	
Captive Portal Authentication Method	external	
Passthrough Firewall Filter ID	FAC	Enter 0-16 chars.
MAC FILTERING SETTINGS		
MAC Filtering	Off	
FIREWALL SETTINGS		
Firewall Capability	radius-configured	
GENERAL SETTINGS		
Security Logging	Off	

Creating the QoS rule on the FortiWLC

1. On the FortiWLC, go to *Configuration > Policies > QoS* and select the *QoS and Firewall Rules* tab. Select *ADD* to create two profiles.

For the first rule, allow the wireless client to access the FortiAuthenticator guest portal.

- *ID*: Rule number (in the example, 20).
- *Destination IP*: IP address of the FortiAuthenticator, and enable *Match*.
- *Destination Netmask*: 255.255.255.255
- *Destination Port*: 443, and enable *Match*.
- *Network Protocol*: 6, and enable *Match*.
- *Firewall Filter ID*: String from the security profile, and enable *Match*.

- *QoS Protocol: Other.*

QoS and Firewall Rules - Add ?

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

2. For the second rule, allow FortiAuthenticator to reach the clients.

- *ID:* Rule number (in the example, 21).
- *Source IP:* IP address of the FortiAuthenticator, and enable *Match*.
- *Source Netmask:* 255.255.255.255
- *Source Port:* 443, and enable *Match*.
- *Network Protocol:* 6, and enable *Match*.
- *Firewall Filter ID:* Use the *Passthrough Firewall Filter ID* string from the security profile, and enable *Match*.

- *QoS Protocol: Other.*

QoS and Firewall Rules - Add ?

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

Creating the ESS Profile on the FortiWLC

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

ESS Profiles - Add ?

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

ESSID TYPE

Essid Type	Regular	
Backup ESS Profile	No Backup ESS	
Timer Profile	No Data for Timer Profile	
Primary RADIUS Accounting Server	No RADIUS	
Secondary RADIUS Accounting Server	No RADIUS	
Accounting Interim Interval (seconds)	3600	Valid range: [60-36000]
Reconnect Primary Server (minutes)	10	Valid range: [5-60]
IPv6 Forwarding	☐	
802.11r	Off	
802.11r Group	7	Valid range: [1-65535]
802.11k	Off	

DATAPLANE MODE

Dataplane Mode	Tunneled
IP Prefix Validation	On
Tunnel Interface Type	No Tunnel

VIRTUALIZATION MODE

RF Virtualization Mode	Native Cell
ACM Support	☐ ACM Voice ☐ ACM Video

Creating FortiWLC as RADIUS client on the FortiAuthenticator

To create a RADIUS client:

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

To create the RADIUS policy:

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

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

Creating the portal and access point on FortiAuthenticator

To create a portal:

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

To create an access point:

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

Creating the portal policy on FortiAuthenticator

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

The screenshot shows the FortiAuthenticator VM web interface at the URL `fac.school.net`. The left sidebar contains a navigation menu with categories like System, Authentication, and Portals. The 'Portals' category is expanded, showing sub-items like Policies, Portals, Access Points, etc. The main content area is titled 'Policy type' and shows the configuration for a new policy. The 'Name' field is set to 'FWLC Portals'. The 'Description' field is empty. The 'Type' section has two radio buttons: 'Allow captive portal access' (selected) and 'Deny captive portal access'. Under 'Allow captive portal access', there is a 'URL' field with the value `https://fac.school.net/portal/` and a 'Portal' dropdown menu set to 'WLC'. At the bottom right of the configuration area are 'Discard and exit' and 'Next' buttons.

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

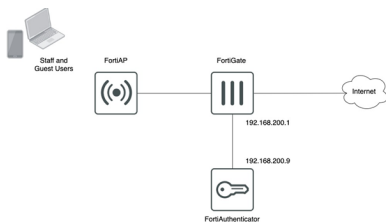
The screenshot shows the FortiAuthenticator VM web interface at the URL `fac.school.net`. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Portal selection criteria' and shows the configuration for selecting access points and RADIUS clients. There are two main sections: 'Access points' and 'RADIUS clients'. Each section has a table with columns for 'HTTP Parameter', 'Operator', 'Value', and 'Actions'. Below each table are two windows: 'Available' and 'Chosen'. In the 'Access points' section, the 'Available' window is empty, and the 'Chosen' window contains one entry: 'FAP Access Point (192.168.200.37)'. In the 'RADIUS clients' section, the 'Available' window contains one entry: 'EX2200 (10.1.2.27)', and the 'Chosen' window contains one entry: 'FWLC (192.168.200.38)'. At the bottom right of the configuration area are 'Previous', 'Discard and exit', 'Update and exit', and 'Next' buttons.

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

Results

1. Connect a client to the SSID created on the FortiWLC, then log in to the portal with the correct username and password.
On the FortiAuthenticator, you can go to *Authentication > User Management > Local Users* to create local user accounts.
2. To confirm the successful log in, on FortiAuthenticator, go to *Logging > Log Access > Logs*.
3. To confirm the successful log in, on FortiWLC, go to *Monitor > Devices > All Stations* and find the device showing the authenticated user.

FortiAuthenticator as a Wireless Guest Portal for FortiGate



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

To set up FortiAuthenticator as a wireless guest portal:

1. [Configuring FortiGate as a RADIUS client on page 60.](#)
2. [Creating a user group on FortiAuthenticator for guest users on page 60.](#)
3. [Creating a guest portal on FortiAuthenticator on page 61.](#)
4. [Configuring an access point on FortiAuthenticator on page 61.](#)
5. [Configuring a captive portal policy on FortiAuthenticator on page 62.](#)
6. [Configuring FortiAuthenticator as a RADIUS server on FortiGate on page 63.](#)
7. [Creating a guest group on FortiGate on page 64.](#)
8. [Creating a wireless guest SSID on FortiGate on page 64.](#)
9. [Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet on page 67.](#)
10. [Configuring firewall authentication portal settings on FortiGate on page 67.](#)

Configuring FortiGate as a RADIUS client

To configure FortiGate as a RADIUS client:

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

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 enter *0.0.0.0-255.255.255.255*.
4. Click *OK*.

Configuring a captive portal policy on FortiAuthenticator

To configure an allow access captive portal policy:

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

Policy type

Name: Guest-Policy

Description:

Type: ☒ Allow captive portal access
 URL: https://
 Portal: Guest-Portal
☐ Deny captive portal access

Discard and exit 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*.

Portal selection criteria

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

Portal Rule Conditions

HTTP parameter: ssid
 Operator: [string]exact_match
 Value: Guest

Previous Discard and exit 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*.

Authorized clients

Access points:

Available Access Points: 192.168.1.101
 Chosen Access Points: All (0.0.0.0-255.255.255.255)

RADIUS clients:

Available RADIUS Clients: 192.168.1.22
 Chosen RADIUS Clients: FACLAB-FGT (192.168.1.22)

Previous Discard and exit 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:
- For *Username format*, select *username@realm*.
 - 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*.
 - 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:

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

The screenshot shows the 'New User Group' configuration window in FortiGate. The 'Name' field is 'Guest'. The 'Type' dropdown is set to 'Firewall'. The 'Members' field has a '+' icon. The 'Remote Groups' section shows a table with one entry: 'FACLAB' as the Remote Server and 'Guest' as the Group Name. The 'OK' button is highlighted in blue.

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

HTTPS

PING

FMG-Access

SSH

SNMP

FTM

RADIUS Accounting

Security Fabric Connection

IPv6

HTTPS

PING

FMG-Access

SSH

SNMP

Security Fabric Connection

DHCP Server

DHCP status

Enabled

Disabled

Address range

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

Status

Enabled

Disabled

OK

Cancel

FortiAuthenticator 6.5.0 Cookbook
Fortinet Inc.

66

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:

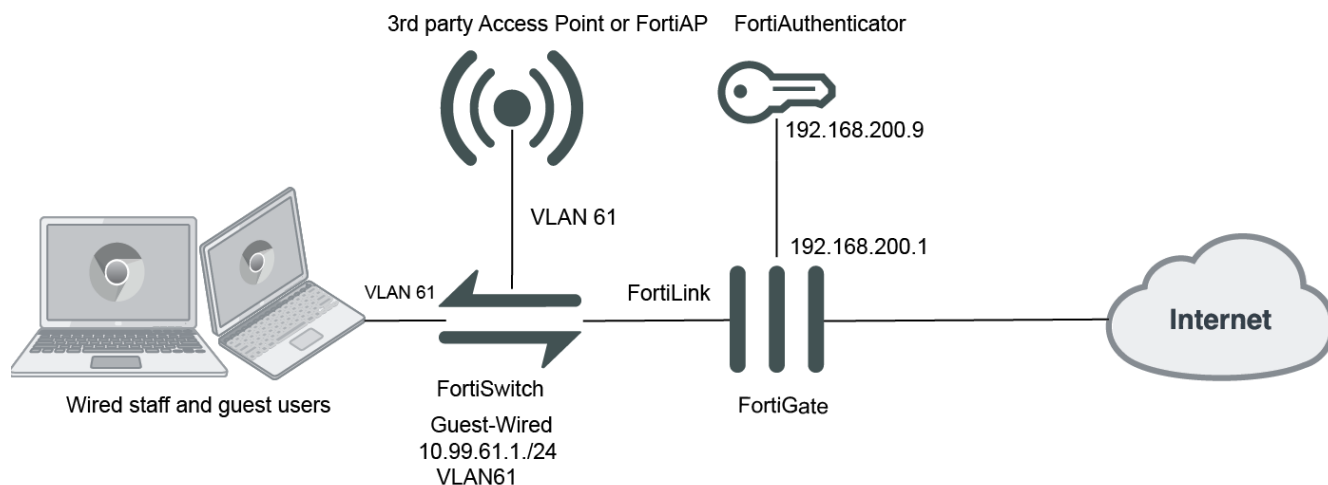
```
config firewall auth-portal
  set portal-addr <addr> #portal-addr setting must be an FQDN that resolves to the interface
  IP address of the guest SSID. The client must be able to resolve this using the DNS
  server configured in the DHCP scope.
end
```

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



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



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

To set up FortiAuthenticator as a wired guest portal:

1. [Configuring FortiGate as a RADIUS client on page 69.](#)
2. [Creating a user group on FortiAuthenticator for guest users on page 70.](#)
3. [Creating a guest portal on FortiAuthenticator on page 70.](#)
4. [Configuring an access point on FortiAuthenticator on page 71.](#)
5. [Configuring a captive portal policy on FortiAuthenticator on page 71.](#)
6. [Configuring FortiAuthenticator as a RADIUS server on FortiGate on page 73.](#)
7. [Creating a guest group on FortiGate on page 73.](#)
8. [Creating a wired guest interface on FortiSwitch on page 74.](#)
9. [Creating firewall policies for guest access to DNS, FortiAuthenticator, and internet on page 76.](#)
10. [Configuring firewall authentication portal settings on FortiGate on page 77.](#)

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*.

Create New User Group

Name:

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

☐ Guest Group

Users:

Password policy:

TACACS+ authorization rule:

RADIUS Attributes

RADIUS Attribute:

Vendor:

Attribute ID:

Value:

Type:

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 enter `0.0.0.0-255.255.255.255`.
4. Click *OK*.

Configuring a captive portal policy on FortiAuthenticator

To configure an allow access captive portal policy:

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

d. Click *Next*.

Policy type Portal selection criteria Authorized clients Authentication type

Name: Guest-Policy

Description:

Type: ☒ Allow captive portal access
 URL: https://
 Portal: Guest-Portal
☐ Deny captive portal access

Discard and exit Next

3. In the *Portal selection criteria* tab:

- In the *HTTP parameter* dropdown, select *ssid* to match.
- In the *Operator* dropdown, select *[string]exact_match*.
- In *Value*, enter the name of the interface configured on the FortiGate with captive portal authentication required. Here, *Guest-Wired*.

d. Click *Next*.

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

Portal Rule Conditions

Portal Rule Condition:

☐ Not

HTTP parameter: ssid

Operator: [string]exact_match

Value: Guest-Wired

Add Portal Rule Condition

Previous Discard and exit Next

4. In the *Authorized clients* tab:

- From *Access points*, select the access point defined in [Access points](#).
 - From *RADIUS clients*, select the FortiGate RADIUS client defined in [RADIUS clients](#).
- c. Click *Next*.

Policy type Portal selection criteria Authorized clients Authentication type

Access points:

Available Access Points

test (192.168.1.10)

Choose all Remove all

RADIUS clients:

Available RADIUS Clients

test (192.168.1.22)

Choose all Remove all

Previous Discard and exit 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*.

Policy type Portal selection criteria Authorized clients Authentication type

Authentication type:

☒ Password/OTP authentication

☒ Local/remote user

☐ Social users

☐ MAC Authorization

Previous Discard and exit Next

6. In the *Identity sources* tab:

- For *Username format*, select *username@realm*.
- 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*.

Policy type → **Portal selection criteria** → **Authorized clients** → **Authentication type** → **Identity sources** → **Authentication factors**

Local/Remote Users:
 Username format:
☒ username@realm
☐ realm.username
☐ realm/username
☐ Use default realm when user-provided realm is different from all configured realms

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	local Local users	☐	Filter: Filter local users:	
Add a realm				

[Previous](#) [Discard and exit](#) [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.

Edit RADIUS Server

Name:

Authentication method: Default Specify

NAS IP:

Include in every user group: ☐

Primary Server

IP/Name:

Secret:

Connection status: Successful

[Test Connectivity](#) [Test User Credentials](#)

Secondary Server

IP/Name:

Secret:

[Test Connectivity](#) [Test User Credentials](#)

[OK](#) [Cancel](#)

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*.

New Interface

Name: Guest-Wired

Alias:

Type: VLAN

VLAN protocol: 802.1Q 802.1AD

Interface: link (fortilink)

VLAN ID: 61

VRF ID: 0

Color: Change

Role: LAN

Address

Addressing mode: Manual DHCP Auto-managed by IPAM

IP/Netmask:

IPv6 addressing mode: Manual DHCP Delegated

IPv6 Address/Prefix: ::0

Auto configure IPv6 address: ☐

DHCPv6 prefix delegation: ☐

Create address object matching subnet: ☒

Name: Guest-Wired address

Destination:

Secondary IP address: ☐

Administrative Access

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

IPv6: ☐ HTTPS ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ Security Fabric Connection

DHCP Server

DHCP status: ☒ Enabled ☐ Disabled

Address range:

Netmask:

Default gateway: Same as Interface IP Specify

DNS server: Same as System DNS Same as Interface IP Specify

DNS server 1:

Lease time: 604800 second(s)

Advanced

Stateless Address Auto-configuration (SLAAC): ☐

DHCPv6 Server

Network

Device detection: ☒

IGMP snooping: ☐

DHCP snooping: ☐

Block intra-VLAN traffic: ☐

Security mode: Captive Portal

Authentication portal: Local External

User access: Restricted to Groups Allow all

User groups: Guest

Exempt sources:

Exempt destinations/services: FACLAB WinAD

Redirect after Captive Portal: Original Request Specific URL

https://www.fortinet.com

Traffic Shaping

Outbound shaping profile: ☐

Miscellaneous

Comments: 0/255

Status: ☒ Enabled ☐ Disabled

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

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

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Enter a name for the policy.

3. In *Incoming Interface*, select the wired guest interface created in [Wired Guest Interface](#).
4. In *Outgoing Interface*, select the interface for FortiAuthenticator and DNS access.
5. In *Source*, select an *Address* object.
6. In *Destination*, select address objects for the FortiAuthenticator and DNS servers.
7. Enable or disable *NAT* as required.
8. Optionally, enable other options including *Security Profiles* for performing inspection using the security features of FortiGate.
9. Click *OK*.

To create firewall policy for guest user internet access:

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

Configuring firewall authentication portal settings on FortiGate

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

The specific URL needs to be configured in the *Redirect after Captive Portal* option in the [New Interface](#) dialog.

To configure firewall authentication portal address from the CLI:

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

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

To configure firewall user settings from the CLI:

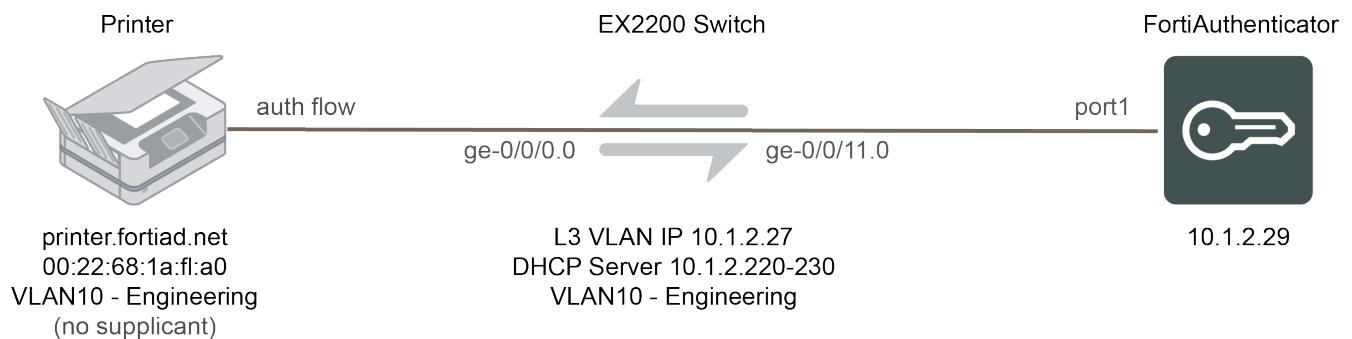
1. Enter the following commands to set to the firewall user settings:

```
config user setting
    set auth-type {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
```

MAC authentication bypass

This section describes configuring MAC address bypass with FortiAuthenticator.

MAC authentication bypass with dynamic VLAN assignment



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

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

Configuring MAC authentication bypass on the FortiAuthenticator

1. Go to *Authentication > User Management > MAC Devices* and create a new MAC-based device. Enter a name for the device along with the device's MAC address. Alternatively, you can use the *Import* option to import this information from a CSV file.

FortiAuthenticator VM fac.school.net

System > Authentication > User Account Policies > User Management > MAC Devices

Create New MAC-based Authentication Device

Name: printer-fortiad-net

MAC address: 08:00:20:08:00:08

Description:

☐ This device belongs to a user

OK Cancel

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.

FortiAuthenticator VM fac.school.net

System > Authentication > User Account Policies > User Management > User Groups

Edit User Group

Name: VLAN10

Type: Local Remote LDAP Remote RADIUS Remote SAML MAC

Mac devices:

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

Choose all Remove all

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

Add Attribute

OK Cancel



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)*.

The screenshot shows the FortiAuthenticator VM configuration interface. The left sidebar lists various system settings, with 'RADIUS Service' expanded. The main panel shows the 'Authentication type' step in a sequence of five steps: RADIUS clients, RADIUS attribute criteria, Authentication type, Identity source, and RADIUS response. Under 'Authentication type', three radio buttons are visible: 'Password/OTP authentication', 'MAC authentication bypass (MAB)' (which is selected), and 'Client Certificates (EAP-TLS)'. At the bottom of the main panel are three buttons: 'Previous', 'Discard and exit', and 'Next'.

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

The screenshot shows the 'Identity source' step in the configuration sequence. The 'Require Call-Check attribute for MAC-based authentication' checkbox is checked. Below it, the 'Authorized groups' field contains the text '*VLAN10'. The 'Blocked groups' field is empty. The 'Previous', 'Discard and exit', and 'Next' buttons are at the bottom.

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

The screenshot shows the 'RADIUS response' step. A table titled 'MAC Authentication Bypass (MAB)' defines the response for different authentication results. The table has four columns: 'MAB Authentication Result', 'RADIUS Authentication Response', 'Return Device Group Attributes', and 'Return Additional Attributes'.

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

At the bottom of the table are three buttons: 'Previous', 'Discard and exit', and '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
```



```

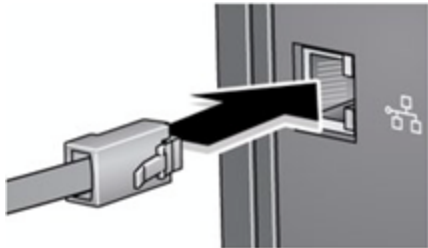
set system services dhcp pool 10.1.2.0/24 address-range high 10.1.2.230
set system services dhcp pool 10.1.2.0/24 domain-name fortiad.net
set system services dhcp pool 10.1.2.0/24 name-server 10.1.2.122
set system services dhcp pool 10.1.2.0/24 router 10.1.2.1
set system services dhcp pool 10.1.2.0/24 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 13-interface vlan.10

```

No configuration is required on the endpoint.

Results

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



2. Using tcpdump, FortiAuthenticator shows receipt of an incoming authentication request (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-f1-a0
0x0000: 3030 2032 3220 3638 2031 6120 6631 2461
0x0010: 30
Called-Station-Id Attribute (30), length: 19, Value: a8-40-e5-b0-21-80
0x0000: 6138 2464 3024 6535 2d62 302d 3231 2d38
0x0010: 30
NAS-Port-Type Attribute (61), length: 6, value: Ethernet
0x0000: 0000 000f

```

3. On the FortiAuthenticator, go to *Logging > Log Access > Logs* to verify the device authentication. The Debug Log (at <https://<fac-ip>/debug/radius>) should also confirm successful authentication.
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 -> 0x5cce1) 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 b1bb 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 dot1x interface ge-0/0/0.0
802.1X Information:
Interface Role State MAC address User
ge-0/0/0.0 Authenticator Authenticated 00:22:68:1A:F1:A0 0022681af1a0

```

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

```

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

```

Additionally, the printer shows as available on the network:

```

root# run show arp interface vlan.10
MAC Address Address Name Interface Flags
00:0c:29:5b:90:68 10.1.2.29 10.1.2.29 vlan.10 none
6c:70:9f:d6:ae:a1 10.1.2.220 10.1.2.220 vlan.10 none
b8:53:ac:4a:d5:f5 10.1.2.221 10.1.2.221 vlan.10 none
00:22:68:1a:f1:a0 10.1.2.224 10.1.2.224 vlan.10 none
a4:c3:61:24:b9:07 10.1.2.228 10.1.2.228 vlan.10 none
Total entries: 5

```

```

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

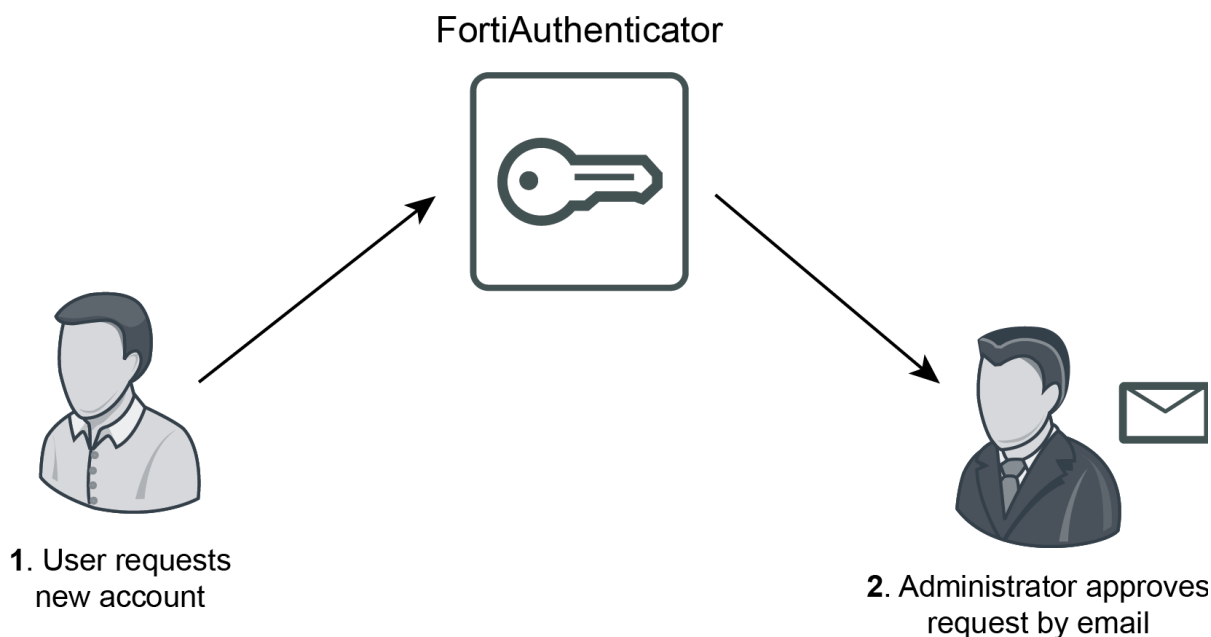
```

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

Self-service Portal

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

FortiAuthenticator user self-registration



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

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

Creating a self-registration user group

To create a self-registration user group:

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

Create New User Group

Name:

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

Users:

Available Users ?

admin
gthreepwood

Selected Users

Choose all Remove all

Password policy:

☐ Usage Profile

OK Cancel

Enabling self-registration

To enable self-registration:

1. Go to *Authentication > Self service Portal > General*.

Enter a *Site name*, add an *Email signature* that you would like appended to the end of outgoing emails, and select **OK**.

Edit General Self-service Portal Settings

Default portal language: [\[Add a Language Pack\]](#)

Site name:

Email signature:

☒ Allow users to change their password

☒ Local users

☒ Remote users

OK

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

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

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

Open the *Required Field Configuration* dropdown and enable *First name*, *Last name*, and *Email address*.

Edit Self-registration Settings

☒ Enable☒ Require administrator approval☒ Enable email to freeform addresses

Administrator email addresses:

☐ Select User Groups allowed to approve new user registrations☐ Account expires after hour(s) ▼☐ Use mobile number as username☒ Place registered users into a group ▼

Password creation:

☒ User-defined☐ Randomly generated☐ Enforce contact verification:☐ Email address☐ Mobile number☐ User's choice (email or mobile)Account delivery options
available to the user:☐ SMS☒ Email☐ Display on browser page

SMS gateway:

 ▼

Required Field Configuration

☒ First name☒ Last name☒ Email address☐ Address☐ City☐ State/Province☐ Country☐ Phone number☐ Mobile number☐ Custom field 1☐ Custom field 2☐ Custom field 3

OK

Creating a new SMTP server

To create a new SMTP server:

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

Create New SMTP Server

Name:

Server name/IP:

Port:

Sender name (optional):

Sender email address:

Connection Security and Authentication

Secure connection:

☒ Enable authentication

Account username:

Password:

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

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

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

2 SMTP servers

Results - Self-registration

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

Please enter your information below.

Username:	rdeckard
Password:	*****
Confirm password:	*****
First name:	Rick
Last name:	Deckard
Email address:	rdeckard@fortinet.com
Confirm email address:	rdeckard@fortinet.com
Address:	
City:	
State/Province:	
Country:	▼
Phone number:	
Mobile number:	

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

Registration Successful

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

[Go back to the login page](#)

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

Your account has been activated  In box x



admin@fac.school.net
to me ▾

12:52 (6 minutes ago) ☆ ↶ ⋮

Welcome to Wallace Corporation, rdeckard!

Your login information:

Username: rdeckard

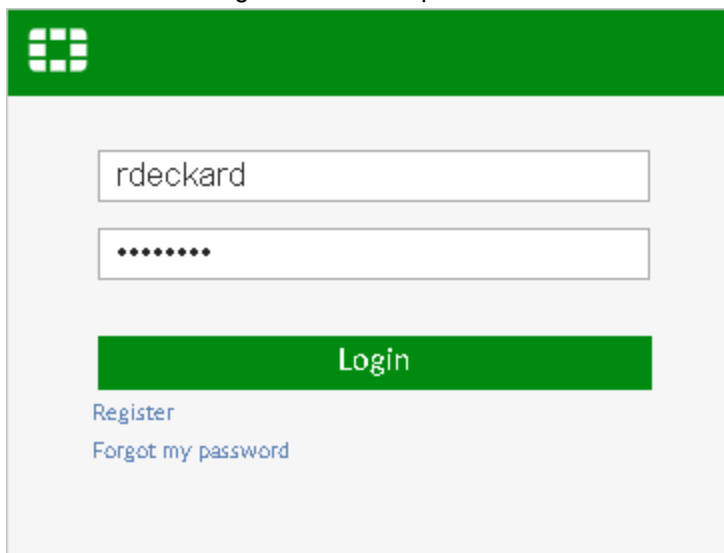
Password: *****

Please login and change your password here:

<https://fac.school.net/login/?username=rdeckard>

Niander Wallace, System Administrator

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



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

Logged in as rdeckard 

My Account 

- User 
 - Profile
 - Change Password**
 - General 

View Profile

Edit Profile

First name: Rick

Last name: Deckard

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

Phone number:

Mobile number:

Street address:

City:

State/Province:

Country:

Password Recovery Options

Email recovery: 

Security question: 

[Cancel](#)

Results - Administrator approval

- 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*.

[+ Create New](#)
[Import](#)
[Export](#)
[Edit](#)
[Delete](#)
[Disabled Users](#)

Search for local users 

☐	User	First name	Last name	Email address	Admin	Status	Token	Token Requested	Groups	Authentication Methods
☐	abriloway			abriloway@fortinet.com						RADIUS
☐	adrianus					 Expired password				RADIUS
☐	adrian									
☐	gthompson								RemoteFTMUsers	RADIUS
☐	janick									
☐	leila					 Expired password				RADIUS and LDAP
☐	rschmitt	Michael	Carmel	rschmitt@fortinet.com						RADIUS
☐	rdeckard	Rick	Deckard	adam.r.bristow@gmail.com		 Not Activated			self reg users	RADIUS

0 local users

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

Approval Required for "Rick Deckard"

abristow@fortinet.com

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

To: Adam Bristow

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

Please go to the following link to approve or deny this user:

<https://172.25.176.141/auth/register/12/approve/>

Klaus Fischer, System Administrator

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

Select *Approve*.

New User Approval

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

Username:	rdeckard
First name:	Rick
Last name:	Deckard
Email address:	adam.bristow@gmail.com
Address:	
City:	
State/Province:	
Country:	
Phone number:	
Mobile number:	

Approve

Deny

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

User Registration Completed

User Registration Completed

User "rdeckard" has been activated.

[Go back to the main page](#)

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

+ Create New Import Export Edit Delete Disabled Users Search for local users										
	User	First name	Last name	Email address	Admin	Status	Token	Token Requested	Groups	Authentication Methods
☐	abristow			abristow@fortinet.com	☒	☒		☐		RADIUS
☐	adrian				☐	Expired password		☐		RADIUS
☐	admin				☒	☒		☐		
☐	adminnew				☐	☒		☐	RemoteFTMUsers	RADIUS
☐	admin				☐	☒		☐		
☐	test				☐	Expired password		☐		RADIUS and LDAP
☐	mcsmell	Michael	Co-smell	mcsmell@fortinet.com	☒	☒		☐		RADIUS
☐	rdeckard	Rick	Deckard	adam.urbistow@gmail.com	☐	☒		☐	self reg users	RADIUS
8 local users										

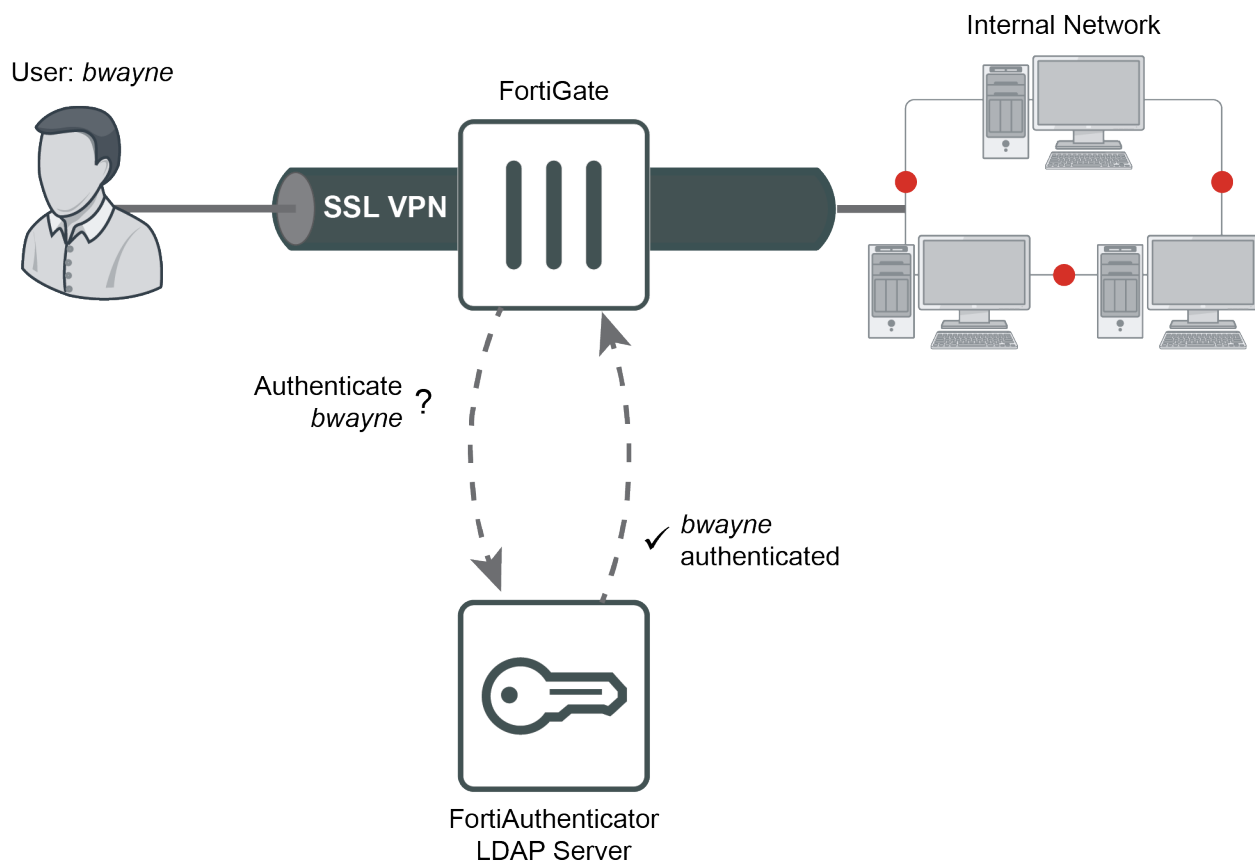
5. You can also go to **Logging > Log Access > Logs** to view the successful login of the user and more information.

Refresh Download Raw Log Log Type Reference Debug Report Search for log records										
ID	Timestamp	Level	Category	Sub category	Type Id	Action	Status	Source IP	Short message	Log Details
1858	Mon Jul 15 13:03:51 2019	Information	Event	User Portal	50001	Logout			User 'rdeckard' logged out	Log Record Detail ID 1857 Timestamp Mon Jul 15 13:00:39 2019 Level Information Action Login Status Success Source IP 172.25.181.138 Message Web access granted to 'rdeckard' User rdeckard Log Type 20994 Name Admin GUI Login Sub Category Authentication Category Event Description Logs admin GUI site login event
1857	Mon Jul 15 13:00:39 2019	Information	Event	Authentication	20994	Login	Success	172.25.181.138	Web access granted to 'rdeckard'	
1856	Mon Jul 15 13:00:39 2019	Information	Event	User Portal	50000	Login	Success		Local user authentication with no token successful	
1855	Mon Jul 15 12:52:15 2019	Information	Event	System	30908				smtp mail: send to adam.urbistow@gmail.com via localhost:25	
1854	Mon Jul 15 12:52:15 2019	Information	Event	Admin Configuration	10301				Notifying user "rdeckard" about his/her newly activated account	
1853	Mon Jul 15 12:52:15 2019	Information	Event	Admin Configuration	10301				"abristow" has approved the new account for user "rdeckard"	
1852	Mon Jul 15 12:52:15 2019	Information	Event	Admin Configuration	10002	Edit			Edited Local User: rdeckard (changed fields: active)	
1851	Mon Jul 15 12:42:26 2019	Information	Event	Admin Configuration	10301				Registration form submitted by user "rdeckard"	
1850	Mon Jul 15 12:42:26 2019	Information	Event	System	30908				smtp mail: send to adam.urbistow@gmail.com via localhost:25	
1849	Mon Jul 15 12:42:26 2019	Information	Event	Admin Configuration	10002	Edit			Edited Local User Profile: rdeckard (changed fields: email record)	
1848	Mon Jul 15 12:42:26 2019	Information	Event	Admin Configuration	10001	Add			Added Local User Profile: rdeckard	

VPNs

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

LDAP authentication for SSL VPN with FortiAuthenticator



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

Creating the user and user group on the FortiAuthenticator

To create the user and user group:

1. On the FortiAuthenticator, go to *Authentication > User Management > Local Users* and select *Create New*. Enter a name for the user, enter and confirm a password, and be sure to disable *Allow RADIUS authentication* – RADIUS authentication is not required for this recipe. Set *Role* as *User*, and select *OK*. New options will appear. Make sure to enable *Allow LDAP browsing* – the user will not be able to connect to the FortiGate otherwise.

Edit Local User

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

Username: bwayne

☐ Disabled

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

☐ Token-based authentication

☐ Allow RADIUS authentication

☐ Enable account expiration

☐ Force password change on next logon

User Role

Role: Administrator Sponsor **User**

☒ Allow LDAP browsing

+ User Information

+ Alternative Email Addresses

+ Password Recovery Options

+ Groups

+ Usage Information

+ Email Routing

+ RADIUS Attributes

+ Certificate Bindings

+ Devices

OK Cancel

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

Create New User Group

Name:

Type: Local Remote LDAP Remote RADIUS Remote SAML MAC

Users:

Available Users

admin

Selected Users

bwayne
jgarrick

Choose all Remove all

Password policy: Default

☐ Usage Profile [Please Select]

OK Cancel

Creating the LDAP directory tree on the FortiAuthenticator

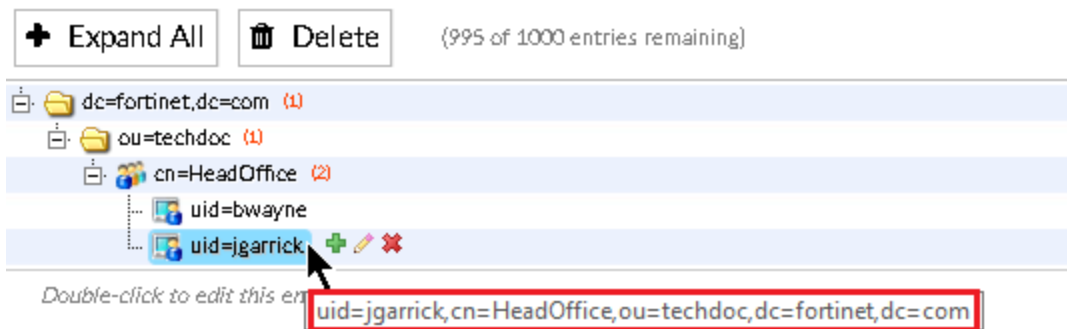
To create the LDAP directory tree:

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 *kgarrick* of the LDAP server, and enter the user's *Password*.

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

Edit LDAP Server

Name	LDAPserver		
Server IP/Name	172.25.176.141		
Server Port	389		
Common Name Identifier	uid		
Distinguished Name	dc=fortinet,dc=com	Browse	
Bind Type	Simple Anonymous <input checked="" type="button" value="Regular"/>		
Username	uid=kgarrick,cn=HeadOffice,ou=techdoc,dc=fortinet,dc=com		
Password		eye	
Secure Connection	☐		
Test Connectivity			
Test User Credentials			

2. Select *Test Connectivity* to determine a successful connection.
Then select *Test User Credentials* to query the LDAP directory using *kgarrick*'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*.

New User Group Add Group Match

Remote Server: LDAPserver

Recursive: ☒

Members: dc=fortinet,dc=com

Groups: Custom Selected

Search: [Search]

ID	Name
HeadOffice	HeadOffice

+ Add Selected

- LDAPserver has been added to the LDAP group. Select OK.

New User Group

Name: LDAPgroup

Type: Firewall

Members: +

Remote Groups

+ Add Edit Delete

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

OK Cancel

Configuring the SSL-VPN

To configure the SSL-VPN:

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

Edit SSL-VPN Portal

Name Limit Users to One SSL-VPN Connection at a Time ☐☒ Tunnel ModeEnable Split Tunneling  

Source IP Pools

 SSLVPN_TUNNEL_ADDR1 

+

2. Go to *VPN > SSL-VPN Settings*.Under *Connection Settings* set *Listen on Port* to 10443.Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and set it to `SSLVPN_TUNNEL_ADDR1`.Under *Authentication/Portal Mapping*, select *Create New*.

SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s) wan1 + ×Listen on Port 10443

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

Redirect HTTP to SSL-VPN ☐

Restrict Access

Allow access from any host

Limit access to specific hosts

Idle Logout ☒

Inactive For

300

Seconds

Server Certificate

Fortinet_Factory

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.

[Click here to learn more](#)

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addresses

Specify custom IP ranges

IP Ranges

SSLVPN_TUNNEL_ADDR1

+

DNS Server

Same as client system DNS

Specify

Specify WINS Servers ☐Allow Endpoint Registration ☐

Authentication/Portal Mapping ⓘ

+ Create New

Edit

Delete

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

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

Authentication/Portal Mapping

 Create New  Edit  Delete		
Users/Groups	Realm	Portal
 LDAPgroup	/	full-access
All Other Users/Groups	/	web-access

Apply

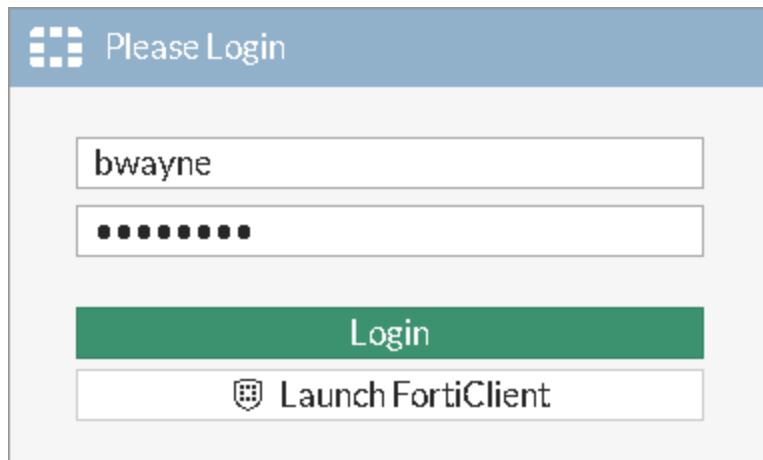
4. Select the prompt at the top of the screen to create a new SSL-VPN policy, including the *LDAPgroup*, as shown.

Edit Policy

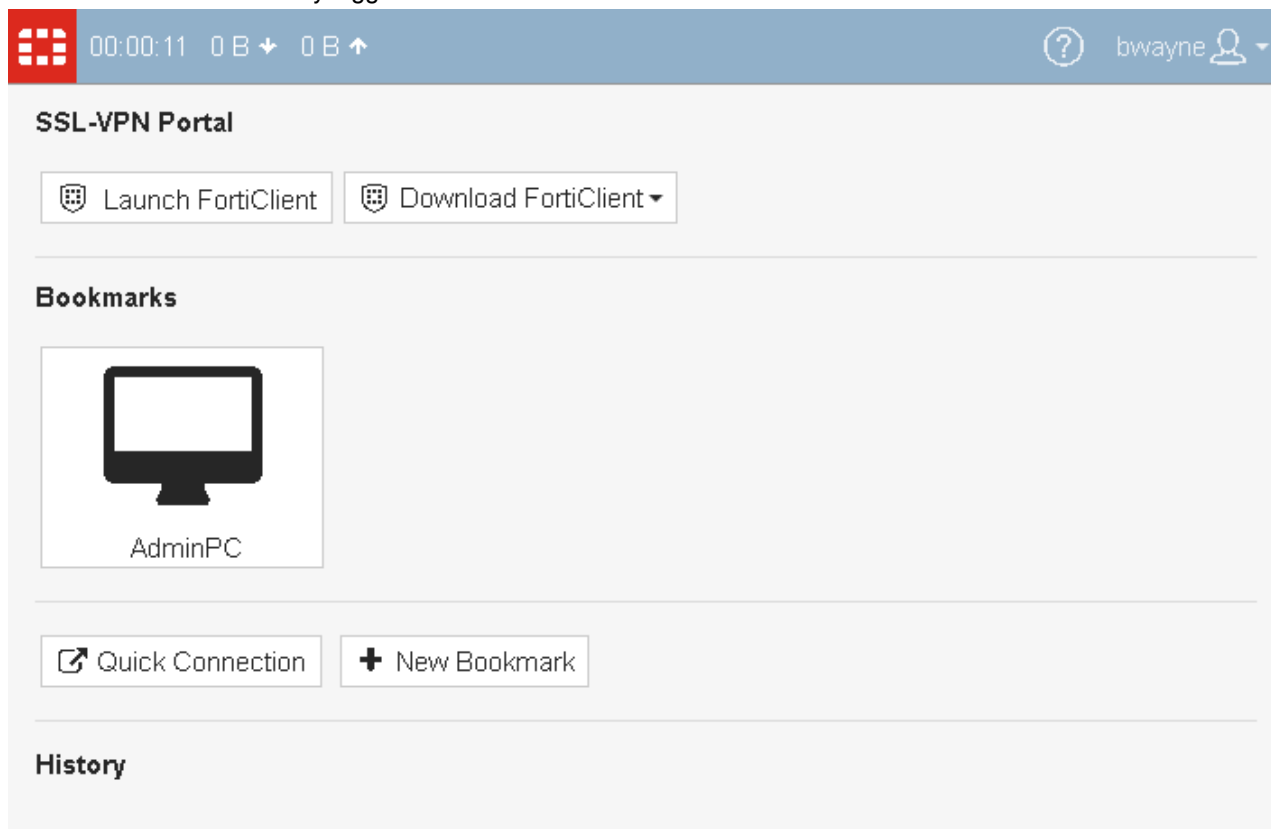
Name 	vpn-internet
Incoming Interface 	 SSL-VPN tunnel interface (ssl.roo  +
Outgoing Interface	 wan1  +
Source	 all   LDAPgroup  +
Destination	 all  +
Schedule	 always 
Service	 ALL  +
Action	 ACCEPT  DENY
Inspection Mode	Flow-based Proxy-based
Firewall / Network Options	
NAT	

Results

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



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



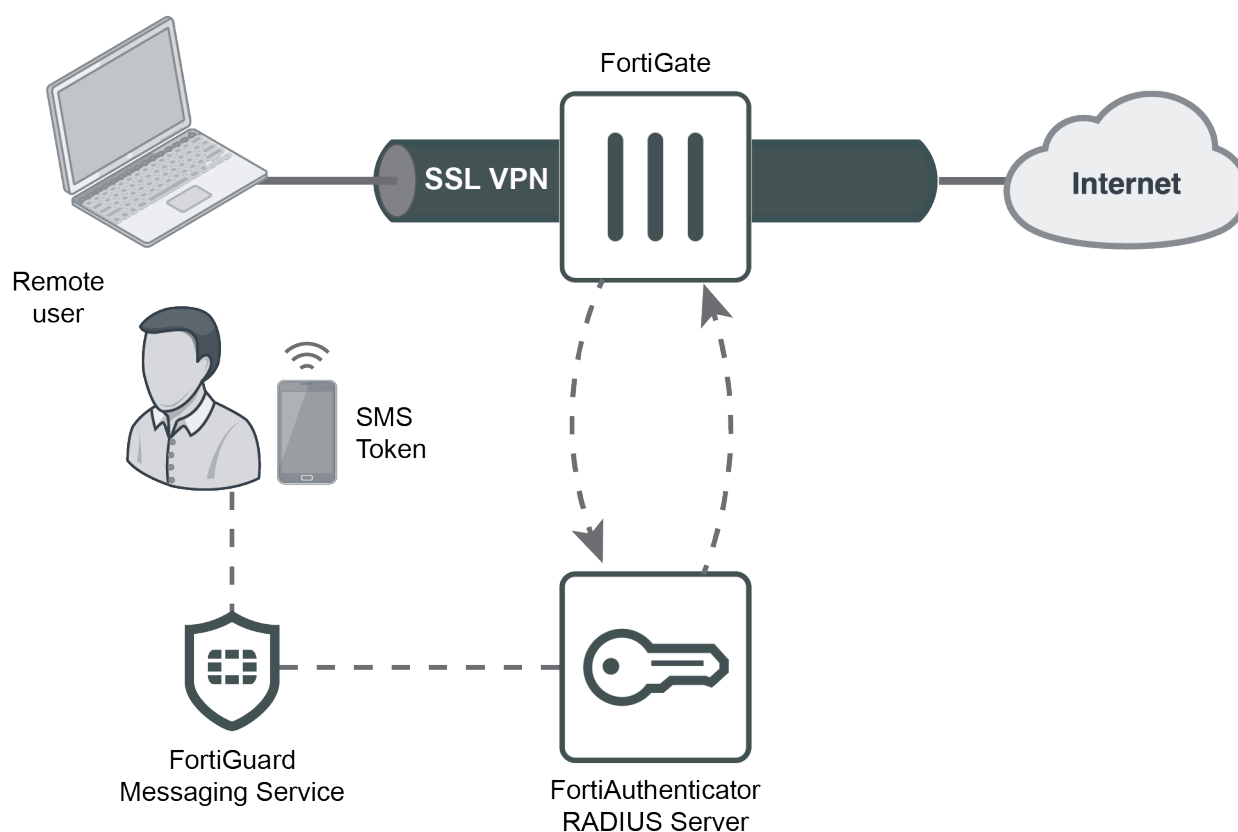
3. On the FortiGate, go to *Monitor > SSL-VPN Monitor* to confirm the connection.

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

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

										Search for log records	
ID	Timestamp	Level	Category	Sub category	Type Id	Action	Status	Source IP	Short message	Log Details	
1907	Mon Jul 15 14:53:19 2019	Information	Event	Authentication	20001	Authentication	Success	FAC_LDAP	Local user authentication(chap) with no token successful	Log Record Detail	
										ID	1907
										Timestamp	Mon Jul 15 14:53:19 2019
										Level	Information
										Action	Authentication
										Status	Success
										Source IP	FAC_LDAP
										Message	Local user authentication (chap) with no token successful
										User	bwayne
										Log Type	
										Type Id	20001
										Name	Authentication OK No FortiToken
										Sub Category	Authentication
										Category	Event
										Description	Authentication successful without FortiToken

SMS two-factor authentication for SSL VPN



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

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

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

Creating an SMS user and user group on the FortiAuthenticator

To create an SMS user and user group:

1. On the FortiAuthenticator, go to *Authentication > User Management > Local Users* and add/modify a user to include *SMS Token-based authentication* and a *Mobile number* using the preferred *SMS gateway* as shown.

The *Mobile number* must be in the following format:

+[international-number]

Enable *Allow RADIUS authentication*.

The screenshot shows the 'Edit Local User' configuration page in FortiAuthenticator. The 'Username' is 'jgarrick'. Under 'Authentication', 'Token-based authentication' is selected, and 'Deliver token code by' is set to 'SMS'. The 'Mobile number' field is highlighted in yellow, and the 'SMS gateway' dropdown is also highlighted in yellow. The 'User Role' is set to 'User'. The 'User Information' section includes fields for First name, Last name, Email, Phone number, Mobile number, Street address, City, State/Province, Country, Language, and Organization. The 'Mobile number' field is highlighted in yellow, and the 'SMS gateway' dropdown is also highlighted in yellow. The 'SMS gateway' dropdown is set to 'FortiGuard Messaging Service'.

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

Create New User Group

Name: SMSgroup

Type: Local Remote LDAP Remote RADIUS Remote SAML MAC

Users:

Available Users: admin

Selected Users: jgarrick

Choose all Remove all

Password policy: Default

Usage Profile: [Please Select]

OK Cancel

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*.

FortiAuthenticator VM FAC-VM0000000000

System > Edit Authentication Client

Authentication > RADIUS Service > Clients

Name: RADIUSclient

Client address: 172.20.121.14

Secret: *****

☐ Accept RADIUS accounting messages for usage enforcement

☐ Support RADIUS Disconnect messages

OK Cancel

To create the RADIUS policy:

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

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

The screenshot shows the FortiAuthenticator VM configuration interface. The left sidebar contains a menu with categories like System, Authentication, Policies, and Fortinet SSO Methods. The 'Authentication' section is expanded, showing 'RADIUS Service' as the selected option. The main panel displays the 'RADIUS clients' configuration page. At the top, there are tabs for 'RADIUS clients', 'RADIUS attribute criteria', 'Authentication type', 'Identity source', 'Authentication factors', and 'RADIUS response'. The 'RADIUS clients' tab is active. Below the tabs, the 'Username format' is set to 'username@realm'. The 'Realm' is set to 'local | Local users'. The 'Allow Local Users To Override Remote Users' checkbox is checked. The 'Use Windows AD Domain Authentication' checkbox is unchecked. The 'Groups' section shows 'Filter: SMSgroup' and 'Filter local users'. At the bottom, there are buttons for 'Previous', 'Discard and exit', 'Update and exit', and 'Next'.

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

Configuring the FortiGate authentication settings

To configure the FortiGate authentication settings:

- On the FortiGate, go to *User & Device > RADIUS Servers* and create the connection to the FortiAuthenticator RADIUS server, using its IP address and pre-shared secret. Use *Test Connectivity* to make sure that the FortiGate can communicate with the FortiAuthenticator.

New RADIUS Server

Name

FAC-RADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.20.121.127

Secret

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

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

New User Group

Name

RADIUSgroup

Type

Firewall

Fortinet Single Sign-On (FSSO)

RADIUS Single Sign-On (RSSO)

Guest

Members

+

Remote Groups

+ Add

Edit

Delete

Remote Server	Group Name
FAC-RADIUS	Any

OK

Cancel

Configuring the SSL-VPN

Configure the SSL-VPN settings:

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

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

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

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

SSL-VPN Settings

 **No SSL-VPN policies exist. [Click here to create a new SSL-VPN policy using these settings](#)**

Connection Settings ⓘ

Listen on Interface(s)

 wan1

+

×

Listen on Port

10443

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

Redirect HTTP to SSL-VPN ☐

Restrict Access

Allow access from any host

Limit access to specific hosts

Idle Logout



Inactive For

300

Seconds

Server Certificate

Fortinet_Factory ▾

ⓘ You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.

[Click here to learn more](#)

Require Client Certificate ☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addresses

Specify custom IP ranges

IP Ranges

 SSLVPN_TUNNEL_ADDR1

+

×

DNS Server

Same as client system DNS

Specify

Specify WINS Servers ☐Allow Endpoint Registration ☐

Authentication/Portal Mapping ⓘ

 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 SSL-VPN policy, including the *RADIUSgroup*, as shown.

New Policy

Name ⓘ	vpn-internet
Incoming Interface ⚠	 SSL-VPN tunnel interface (ssl.roo +
Outgoing Interface	 wan1 +
Source	all RADIUSgroup +
Destination	all +
Schedule	always
Service	ALL +
Action	✓ ACCEPT ✗ DENY
Inspection Mode	Flow-based Proxy-based

Firewall / Network Options

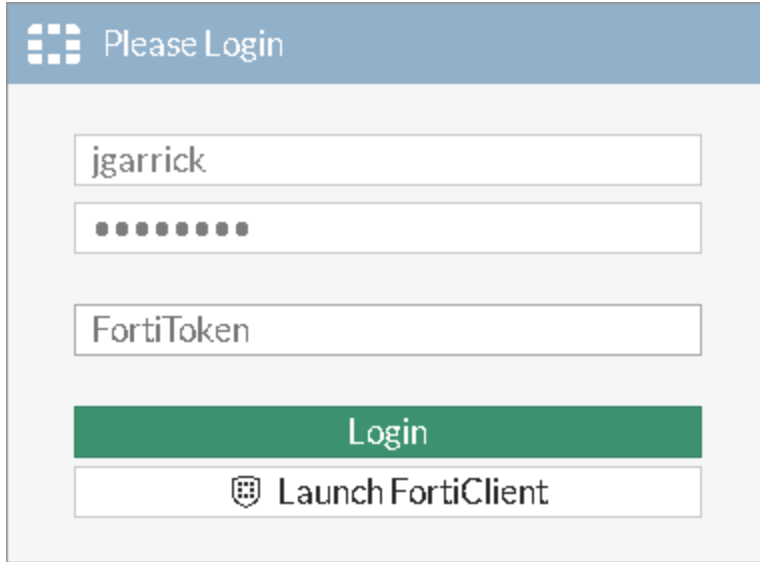
NAT ☒

Results

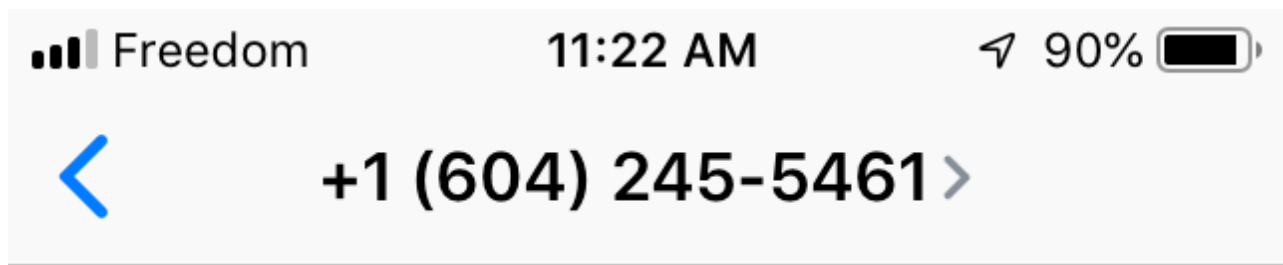
In this example, we will use the web portal to access the SSL VPN and test the two-factor authentication.

To test two-factor authentication:

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

A screenshot of the FortiAuthenticator login portal. The portal has a blue header with a grid icon and the text "Please Login". Below the header, there are four input fields: the first contains the username "jgarrick", the second contains a masked password of ten dots, the third contains the FortiToken code "FortiToken", and the fourth is empty. Below the input fields are two buttons: a green "Login" button and a white "Launch FortiClient" button with a shield icon.

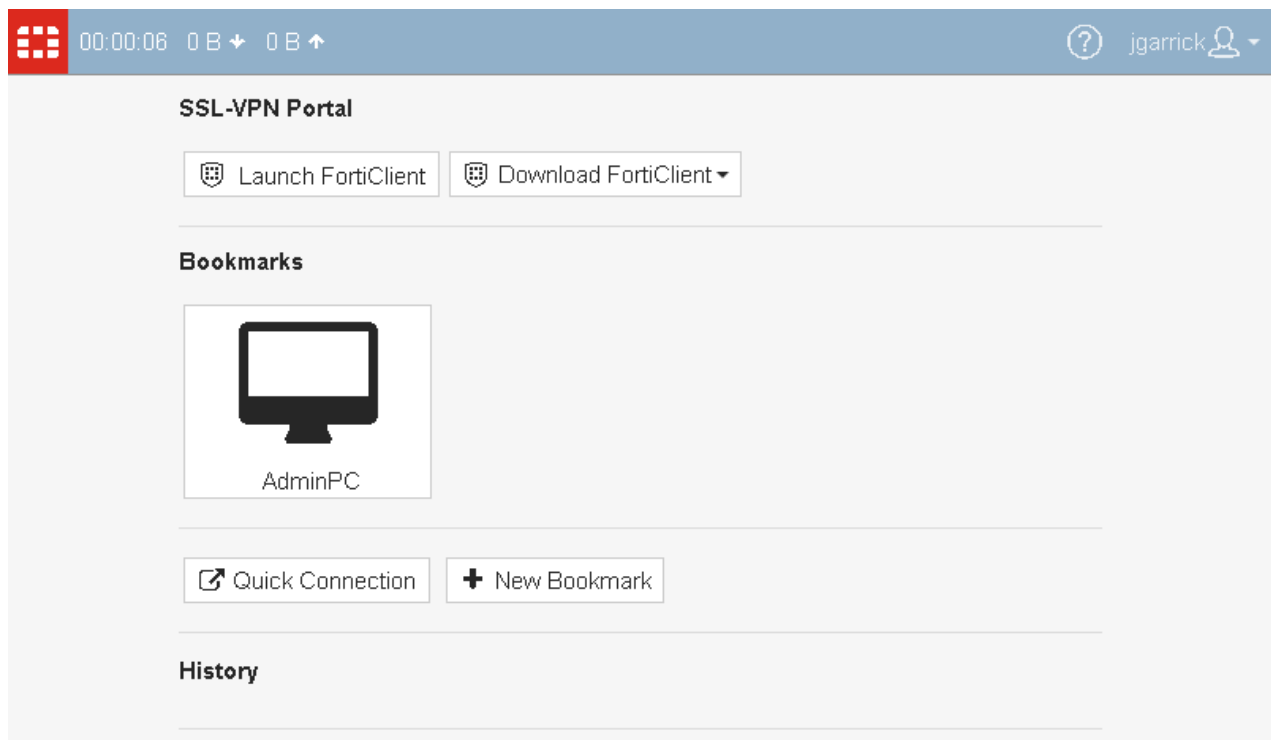
2. The *FortiToken Code* should have been sent to your mobile phone as a text message containing a 6-digit number. Enter the number into the SSL VPN login portal and select *Login*.



Text Message
Today 11:21 AM

User name: jgarrick
Token code: 297213

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



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

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

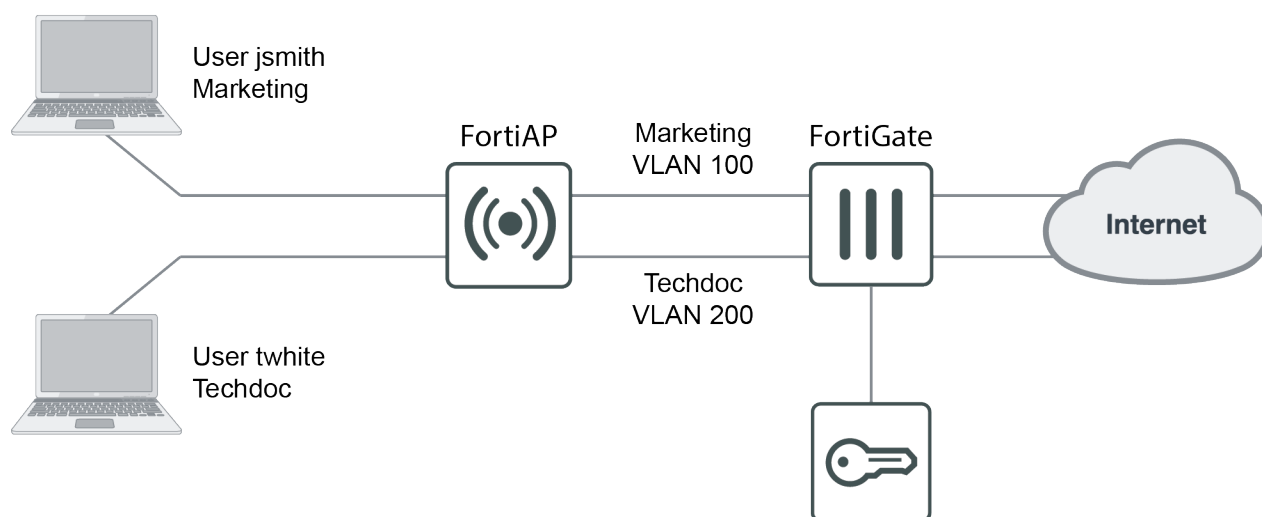
5. On the FortiAuthenticator, go to *Logging > Log Access > Logs* to confirm the user's connection.

	Download Raw Log	Log Type Reference	Debug Report	Search for log records								
ID	Timestamp	Level	Category	Sub category	Type Id	Action	Status	Source IP	Short message		Log Details	
1963	Tue Jul 16 11:24:08 2019	Information	Event	Authentication	20000	Authentication	Success	172.25.176.127	Local user authentication with SMS token successful		Log Record Detail	
1962	Tue Jul 16 11:23:57 2019	Information	Event	Authentication	20300	Authentication	Pending	172.25.176.127	Local user authentication partially done, expecting SMS token		ID	1961
1961	Tue Jul 16 11:23:57 2019	Information	Event	System	30907				FGD SMS: sent SMS to +1-6135018722 successfully		Timestamp	Tue Jul 16 11:23:57 2019
											Level	information
											Action	
											Status	
											Source IP	
											Message	FGD SMS: sent SMS to +1-6135018722 successfully
											User	admin
											Log Type	
											Type Id	30907
											Name	FortiGuard Messaging Service SMS
											Sub Category	System
											Category	Event
											Description	Logs send SMS activity from FortiGuard Messaging service

WiFi authentication

This section describes configuring WiFi authentication with FortiAuthenticator.

Assigning WiFi users to VLANs dynamically



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

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

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

Configuring the FortiAuthenticator

To create the RADIUS client:

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

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*.

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

Adding the RADIUS server to the FortiGate

To add the RADIUS server to the FortiGate:

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

New RADIUS Server

Name

facRADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.25.178.141

Secret

Connection status

☒ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

Creating an SSID with dynamic VLAN assignment

To create an SSID with dynamic VLAN assignment:

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

New

Interface Name

example-wifi

Alias

Type

WiFi SSID

Traffic Mode

Tunnel

Bridge

Mesh

Tags

Add Tag Category

Address

IP/Network Mask

10.10.12.1/255.255.255.0

IPv6 Address/Prefix

::/0

Administrative Access

IPv4

☒ HTTPS

☒ HTTP

☒ PING

☒ FMG-Access

☒ SSH

☒ SNMP

☒ FTM

☒ RADIUS Accounting

☒ FortiTelemetry

IPv6 Administrative Access

☐ HTTPS

☐ HTTP

☐ PING

☐ FMG-Access

☐ SSH

☐ SNMP

☐ FTM

DHCP Server

Address Range

Create New

Edit

Delete

Starting IP	End IP
10.10.12.2	10.10.12.254

Netmask

255.255.255.0

Default Gateway

Same as Interface IP

Specify

DNS Server

Same as System DNS

Same as Interface IP

Specify

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

WiFi Settings	
SSID	example-staff
Security Mode	WPA2 Enterprise
Client Limit	☐
Authentication	Local <input checked="" type="text" value="RADIUS Server"/> facRADIUS
Dynamic VLAN assignment 	☒
Broadcast SSID	☒
Schedule 	always
Block Intra-SSID Traffic	☐
Broadcast Suppression	☒ ARPs for known clients  DHCP Uplink  +
Filter clients by MAC Address	
RADIUS server	☐
Quarantine Host	☒
Enforce FortiClient Compliance Check	☐

- 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:

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

New

Interface Name
Alias
Type
Interface
VLAN ID

Tags

Role

Address

Addressing mode
IP/Network Mask
IPv6 Addressing mode
IPv6 Address/Prefix
Create address object matching subnet ☒
Name
Definition

Administrative Access

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

☒ DHCP Server

Address Range

Starting IP	End IP
192.168.3.2	192.168.3.254

Netmask
Default Gateway
DNS Server

- 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
☐ CAPWAP
☐ RADIUS Accounting
☐ HTTP ⓘ
☐ SSH
☐ PING
☐ SNMP
☐ FortiTelemetry
☐ FMG-Access
☐ FTM

IPv6 Administrative Access

☐ HTTPS
☐ CAPWAP
☐ HTTP ⓘ
☐ SSH
☐ PING
☐ SNMP
☐ FMG-Access
☐ 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.

New Policy

Name ⓘ

marketing-100-internet

Incoming Interface

marketing-100

+

×

Outgoing Interface

wan1

+

×

Source

all

+

×

Destination

all

+

×

Schedule

always

▼

Service

ALL

+

×

Action

✓ ACCEPT

⊘ DENY

🔒 IPsec

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

🔘

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

🔘

Protocol Options

PRX

default

▼

✎

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

Logging Options

Log Allowed Traffic

🔘

Security Events

All Sessions

Capture Packets

🔘

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

FortiAuthenticator 6.5.0 Cookbook
Fortinet Inc.

125

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

New Policy

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

Firewall / Network Options

NAT	☒
IP Pool Configuration	☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool
Preserve Source Port	☐
Protocol Options	☒ PRX ☐ default

Creating the FortiAP profile

To create the FortiAP profile:

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

New FortiAP Profile

Name

FAPS221E-dyn-vlan

Comments

Write a comment... 0/255

Platform

FAPS221E

Country / Region

Use default (United States) Specify

Canada

AP Login Password ⓘ

Set Leave Unchanged Set Empty

Administrative Access

☐ HTTPS ☐ SSH ☐ SNMP

Split Tunneling

Include Local Subnet ⓘ

☐

Split Tunneling Subnet(s)

☐

Radio 1

Mode

Disabled Access Point Dedicated Monitor

WIDS Profile

☐

Radio Resource Provision

☐

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

2.4 GHz 802.11n/g/b

Channel Width

20MHz

Short Guard Interval

☐

Channels

☒ 1 ☒ 6 ☒ 11

TX Power Control

Auto Manual

TX Power

100%

SSIDs ⓘ

Auto Manual

example-staff (example-wifi) +

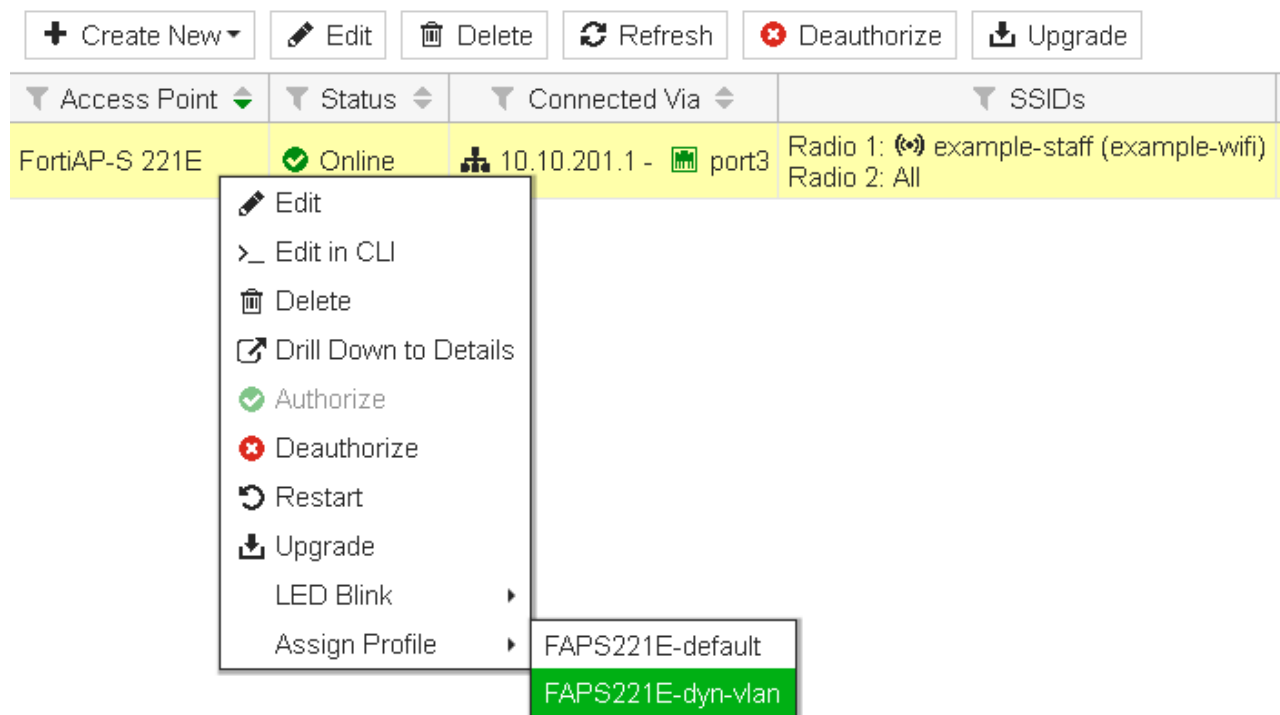
Monitor Channel Utilization

☐

Connecting and authorizing the FortiAP

To connect and authorize the FortiAP:

1. Go to *Network > Interfaces* and edit an unused interface.
Set an *IP/Network Mask* and enable *CAPWAP* under *Administrative Access > IPv4*.
Enable *DHCP Server*.
Now connect the FortiAP unit to the this interface and apply power.
2. Go to *WiFi & Switch Controller > Managed FortiAPs*.
Right-click on the FortiAP unit and select *Authorize*.
Once authorized, right-click on the FortiAP unit again and select *Assign Profile* and select the FortiAP profile created earlier.



Results

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

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

If a certificate warning message appears, accept the certificate.

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

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

Policy: marketing-100-internet (3)

Policy ID: 3

Name: marketing-100-internet

Source: marketing-100

Destination: wan1

Security Profiles: SSL

Action: ACCEPT

Log: All

First Used: 2019/07/17 08:51:39

Last Used: 9 seconds ago

Hit Count: 25

Bytes: 148.08 kB

[Edit](#) [Show in List](#)

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

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

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

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

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

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

WiFi using FortiAuthenticator RADIUS with certificates

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

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

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

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

Creating a local CA on FortiAuthenticator

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

To create the local CA:

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

Configure the fields as required.

The screenshot shows the 'Create New Local CA Certificate' configuration window in FortiAuthenticator. The fields are configured as follows:

- Certificate ID:** RootCA
- Certificate Authority Type:** Root CA (selected), Intermediate CA, Intermediate CA signing request (CSR)
- Subject Information:**
 - Subject input method:** Fully distinguished name (selected), Field-by-field
 - Name (CN):** FortiAuthenticator
 - Department (OU):** IT
 - Company (O):** Local Company
 - City (L):** Ottawa
 - State/Province (ST):** ON
 - Country (C):** Canada (CA)
 - Email address:** admin@fortinet.com
- Key And Signing Options:**
 - Validity period:** Set length of time (selected), Set an expiry date. Value: 3650 days.
 - Key type:** RSA
 - Key size:** 1024, 2048 (selected), 4096
 - Hash algorithm:** SHA-256 (selected), SHA-1
- Subject Alternative Name:**
 - Email:** (empty field)
 - User Principal Name (UPN):** (empty field)
- Advanced Options: Key Usages** (expanded)
- Certificate Revocation List (CRL):**
 - Lifetime:** 30 days (1-365)
 - Re-generate every:** 1 days

At the bottom, there are 'OK' and 'Cancel' buttons.

Creating a local service certificate on FortiAuthenticator

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

To create the local service certificate:

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

Create New Server Certificate

Certificate ID:

Certificate Signing Options

Issuer: Local CA Third-party CA

Certificate authority:

Subject Information

Subject input method: Fully distinguished name Field-by-field

Name (CN):

Department (OU):

Company (O):

City (L):

State/Province (ST):

Country (C):

Email address:

Key And Signing Options

Validity period: Set length of time Set an expiry date

days

Key type: RSA

Key size: 1024 2048 4096

Hash algorithm: SHA-256 SHA-1

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

☐ URI:

☐ DNS:

Other Extensions

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

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

+ Advanced Options: Key Usages

Configuring RADIUS EAP on FortiAuthenticator

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

To configure RADIUS EAP on FortiAuthenticator:

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

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.

The screenshot shows the 'Create New Local User' configuration form in FortiAuthenticator. The form is divided into several sections: 'Create New Local User' (header), 'Username' (text input with 'jhopper'), 'Password creation' (dropdown menu set to 'Specify a password'), 'Password' (password input field), 'Password confirmation' (password input field), 'Allow RADIUS authentication' (radio button, selected), 'Force password change on next logon' (radio button, unselected), 'Role' (section header), 'Role' (radio buttons for 'Administrator', 'Sponsor', and 'User', with 'User' selected), 'Account Expiration' (section header), and 'Enable account expiration' (radio button, unselected). At the bottom right, there are 'OK' and 'Cancel' buttons.

Configuring local user certificate on FortiAuthenticator

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

To configure the local user certificate:

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

Create New User Certificate

Certificate ID:

Certificate Signing Options

Issuer: Local CA Third-party CA

Certificate authority:

Local User (Optional):

Subject Information

Subject input method: Fully distinguished name Field-by-field

Name (CN):

Department (OU):

Company (O):

City (L):

State/Province (ST):

Country (C):

Email address:

Key And Signing Options

Validity period: Set length of time Set an expiry date

days

Key type: RSA

Key size: 1024 2048 4096

Hash algorithm: SHA-256 SHA-1

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

☐ URI:

☐ DNS:

Other Extensions

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

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

Creating RADIUS server on FortiGate

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

To create the RADIUS server on FortiGate:

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

New RADIUS Server

Name

FortiAuthenticator

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.25.176.141

Secret

.....

Connection status

 Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

Creating WiFi SSID on FortiGate

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

To create the WiFi SSID:

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

New

Interface Name

EAP-TLS

Alias

Type

WiFi SSID ▼

Traffic Mode ⓘ

Tunnel

Bridge

Mesh

Tags

+

 Add Tag Category

Address

IP/Network Mask

10.122.122.1/24

IPv6 Address/Prefix

::/0

Administrative Access

IPv4

☐ HTTPS
 ☐ HTTP ⓘ
 ☐ PING
 ☐ FMG-Access
 ☐ SSH
 ☐ SNMP
 ☐ FTM
 ☐ RADIUS Accounting
 ☐ FortiTelemetry

IPv6 Administrative Access

☐ HTTPS
 ☐ HTTP ⓘ
 ☐ PING
 ☐ FMG-Access
 ☐ SSH
 ☐ SNMP
 ☐ FTM

☒ DHCP Server

Address Range

+

 Create New

Edit

Delete

Starting IP	End IP
10.122.122.2	10.122.122.254

Netmask

255.255.255.0

Default Gateway

Same as Interface IP

Specify

DNS Server

Same as System DNS

Same as Interface IP

Specify

+

 Advanced...

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

WiFi Settings

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

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

Edit FortiAP Profile

Name: FAPS221E-default

Comments: 0/255

Platform: FAPS221E

Country / Region: United States

AP Login Password ?

Administrative Access ☐ HTTPS ☐ SSH ☐ SNMP

Split Tunneling

Include Local Subnet ? ☐

Split Tunneling Subnet(s) ☐

Radio 1

Mode:

WIDS Profile: ☐

Radio Resource Provision: ☐

Client Load Balancing: ☐ Frequency Handoff ☐ AP Handoff

Band: 2.4 GHz

Channel Width: 20MHz

Short Guard Interval: ☐

Channels: ☐ 1 ☐ 6 ☐ 11

TX Power Control:

TX Power: 100%

SSIDs ?

☒ EAP-TLS (EAP-TLS)

Monitor Channel Utilization: ☐

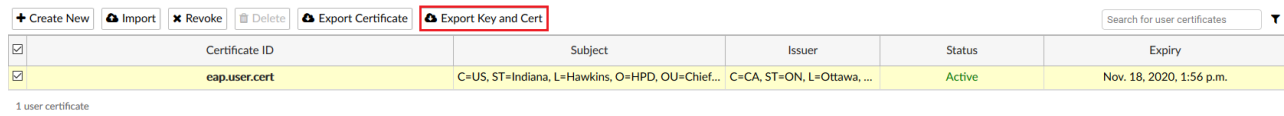
- Then go to *Policy & Objects > IPv4 Policy* and create a policy that allows outbound traffic from the *EAP-TLS* wireless interface to the Internet.

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:

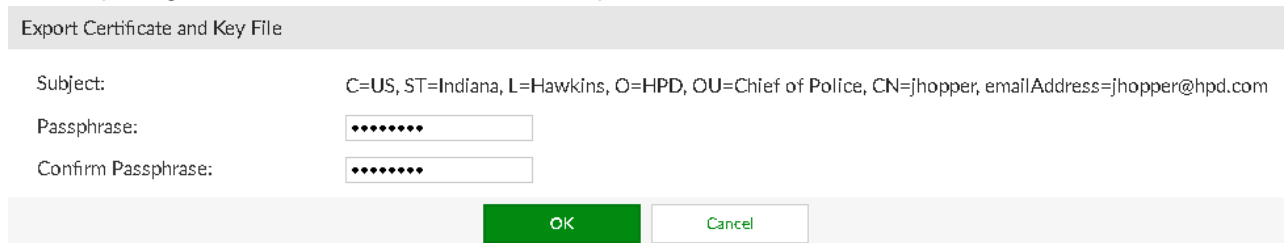
1. On the FortiAuthenticator, go to *Certificate Management > End Entities > Users*. Select the certificate and select *Export Key and Cert*.



The screenshot shows the FortiAuthenticator web interface for managing certificates. At the top, there are buttons: '+ Create New', 'Import', 'Revoke', 'Delete', 'Export Certificate', and 'Export Key and Cert' (which is highlighted with a red box). Below these buttons is a search bar labeled 'Search for user certificates'. A table lists certificates with columns: Certificate ID, Subject, Issuer, Status, and Expiry. One certificate is listed with ID 'eap.user.cert', Subject 'C=US, ST=Indiana, L=Hawkins, O=HPD, OU=Chief...', Issuer 'C=CA, ST=ON, L=Ottawa, ...', Status 'Active', and Expiry 'Nov. 18, 2020, 1:56 p.m.'. Below the table, it says '1 user certificate'.

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

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*.



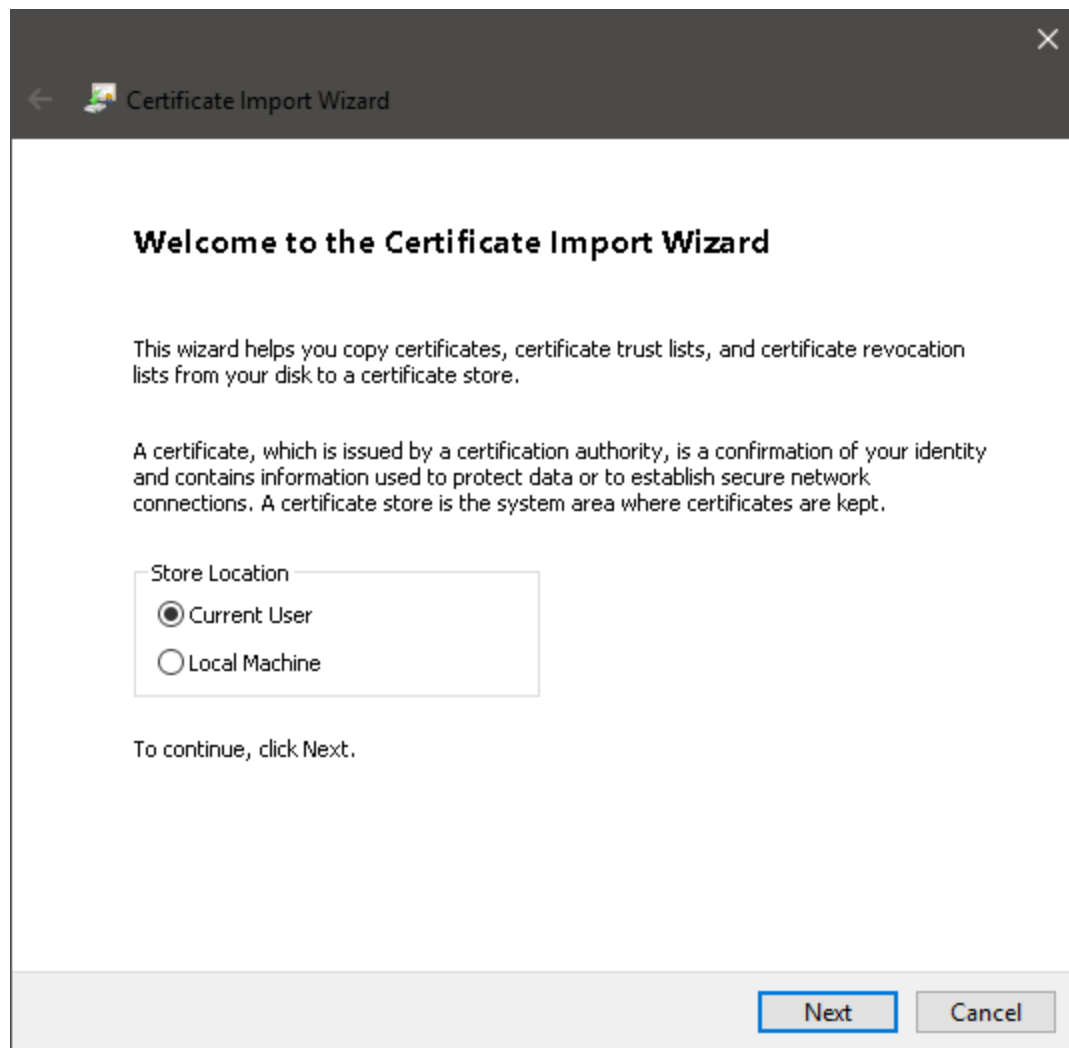
The screenshot shows the 'Export Certificate and Key File' dialog box. It has a title bar 'Export Certificate and Key File'. Below the title bar, there are three labels: 'Subject:', 'Passphrase:', and 'Confirm Passphrase:'. The 'Subject:' field contains the text 'C=US, ST=Indiana, L=Hawkins, O=HPD, OU=Chief of Police, CN=jhopper, emailAddress=jhopper@hpd.com'. The 'Passphrase:' and 'Confirm Passphrase:' fields are empty and have a password mask (dots). At the bottom of the dialog, there are two buttons: 'OK' (green) and 'Cancel' (white).

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

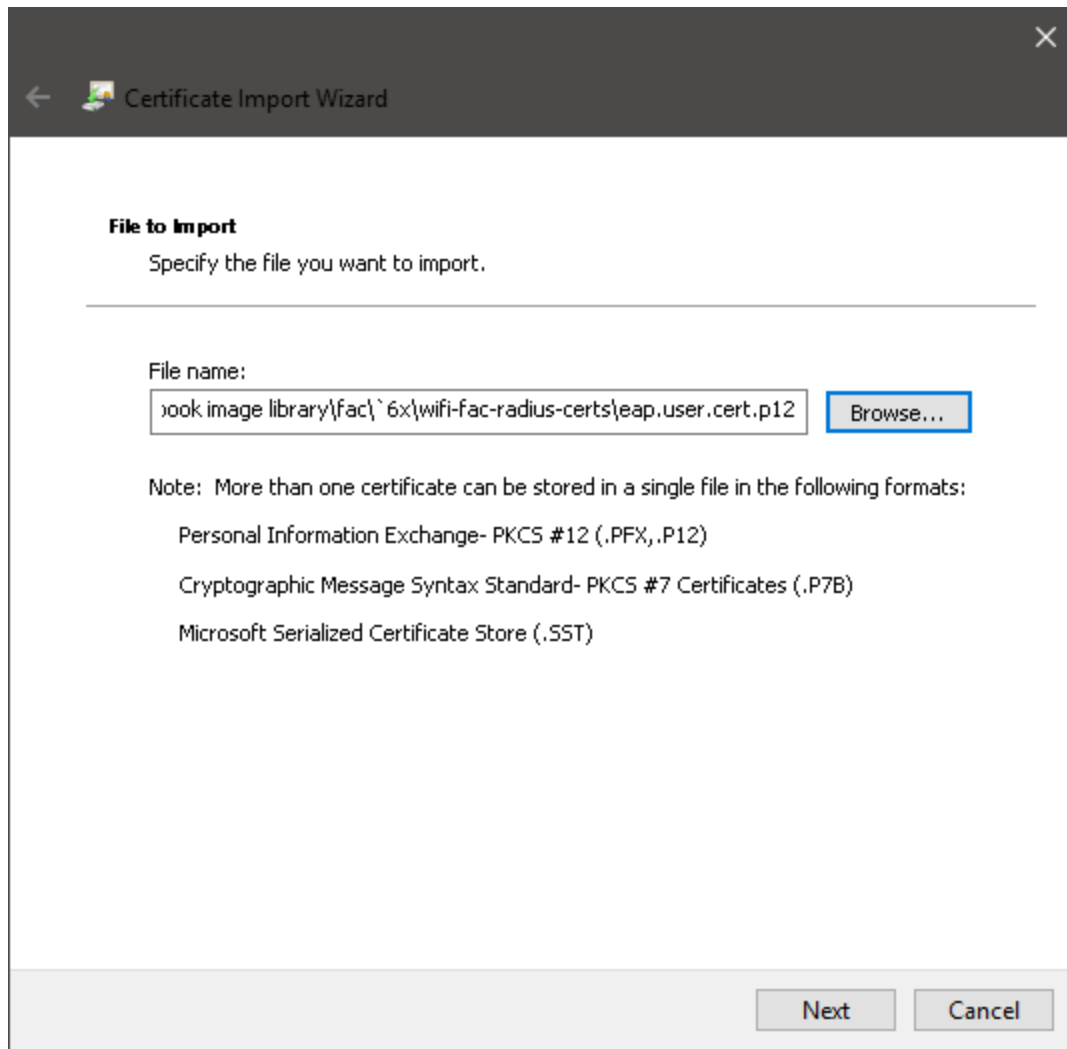
Importing user certificate into Windows 10

To import the user certificate:

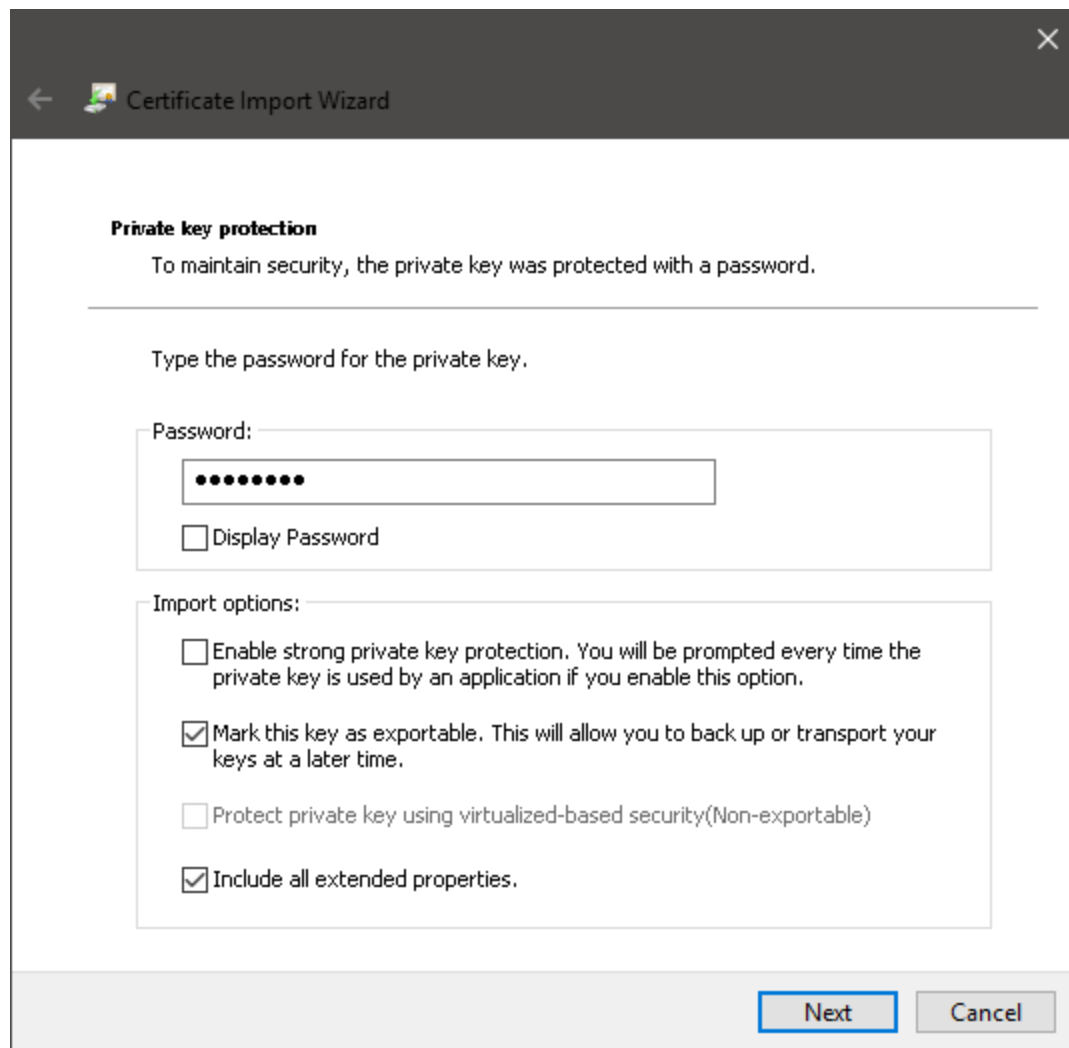
1. On the Windows 10 computer, double-click the downloaded certificate file from the FortiAuthenticator. This will launch the *Certificate Import Wizard*. Select *Next*.



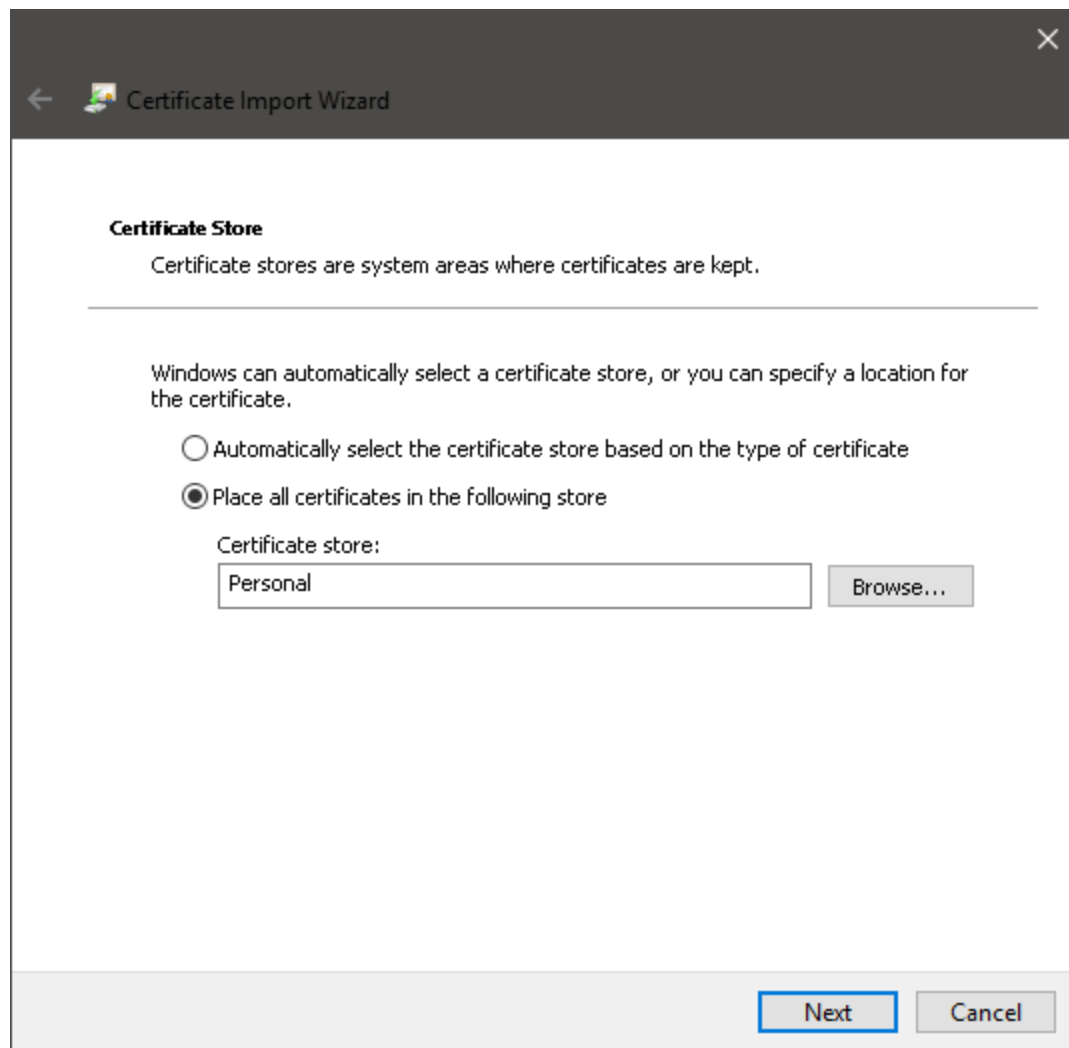
2. Make sure the correct certificate is shown in the *File name* section in the *File to Import* window. Select *Next*.



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.

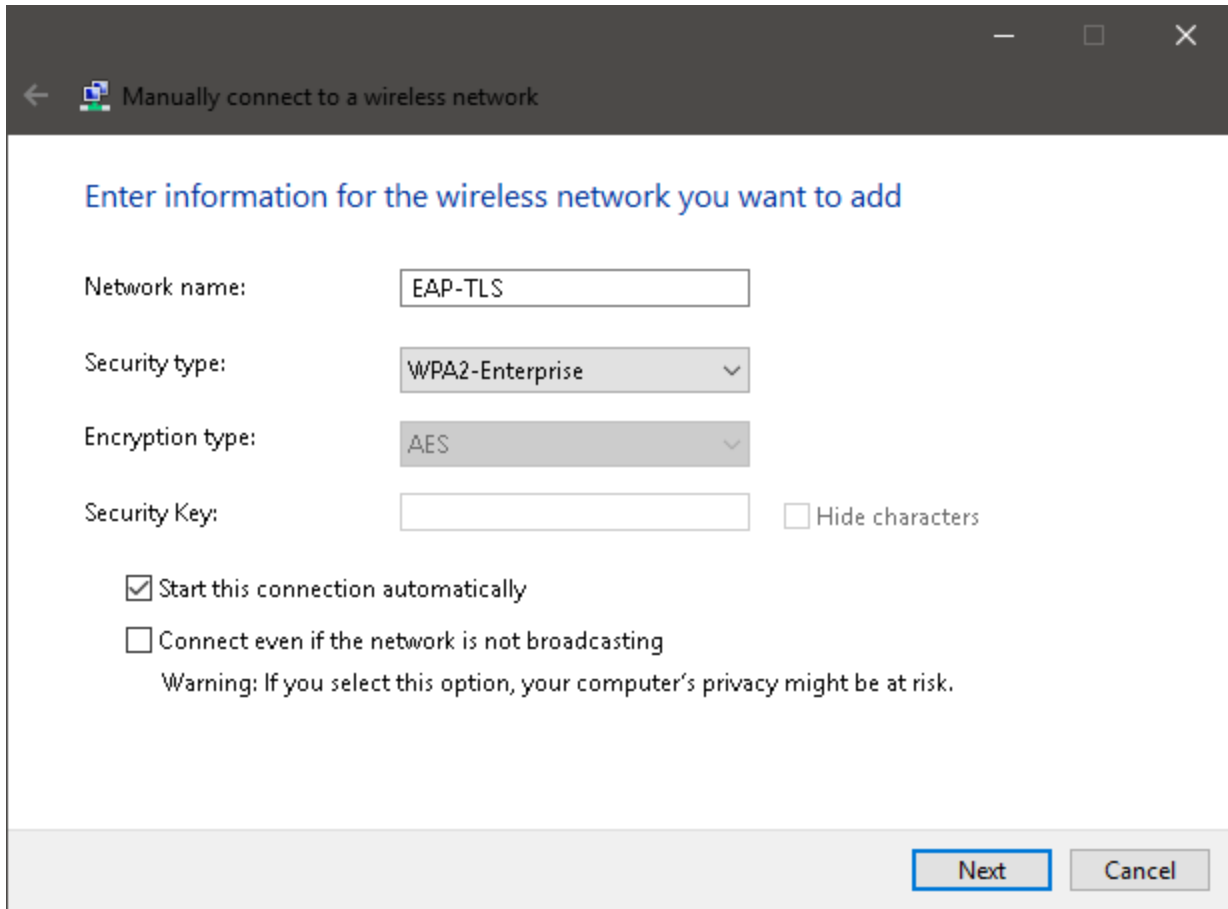


Configuring Windows 10 wireless profile to use certificate

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*.



←  Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

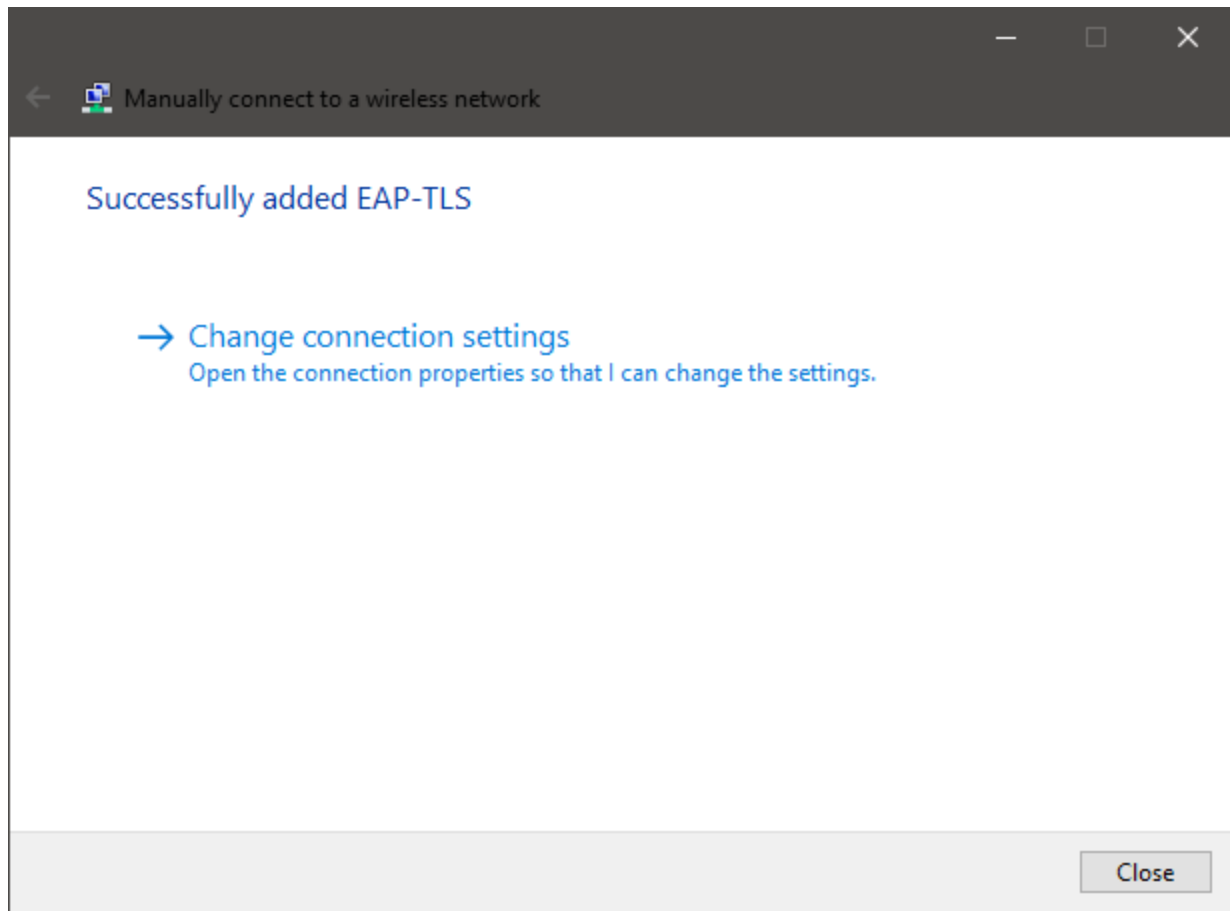
Security Key: ☐ Hide characters

☒ Start this connection automatically

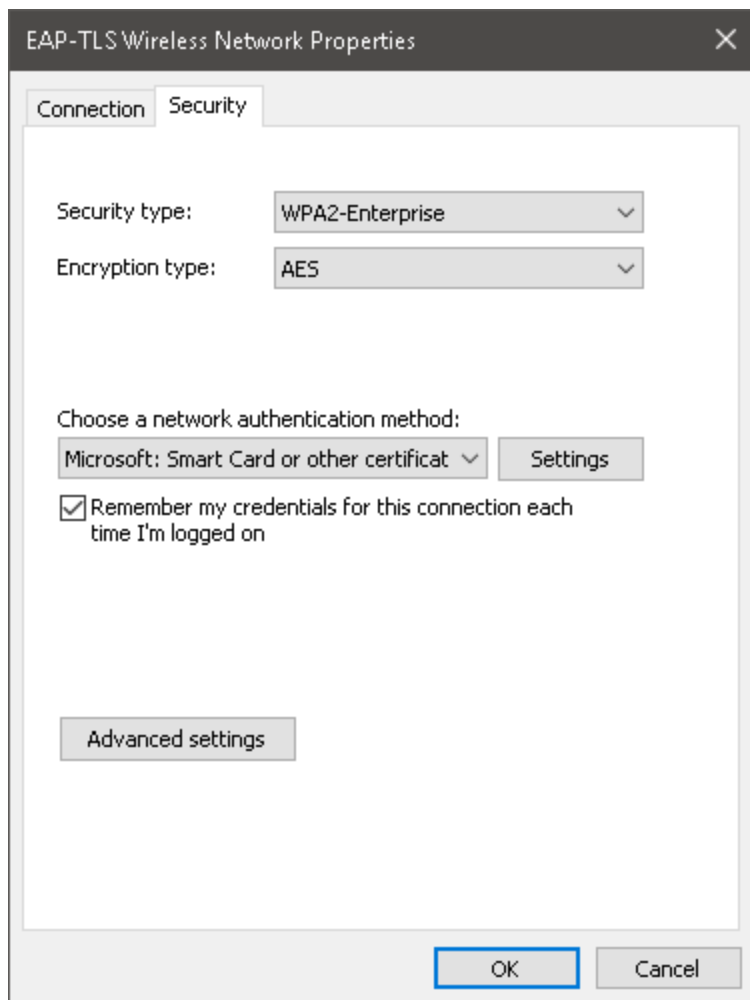
☐ Connect even if the network is not broadcasting

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

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



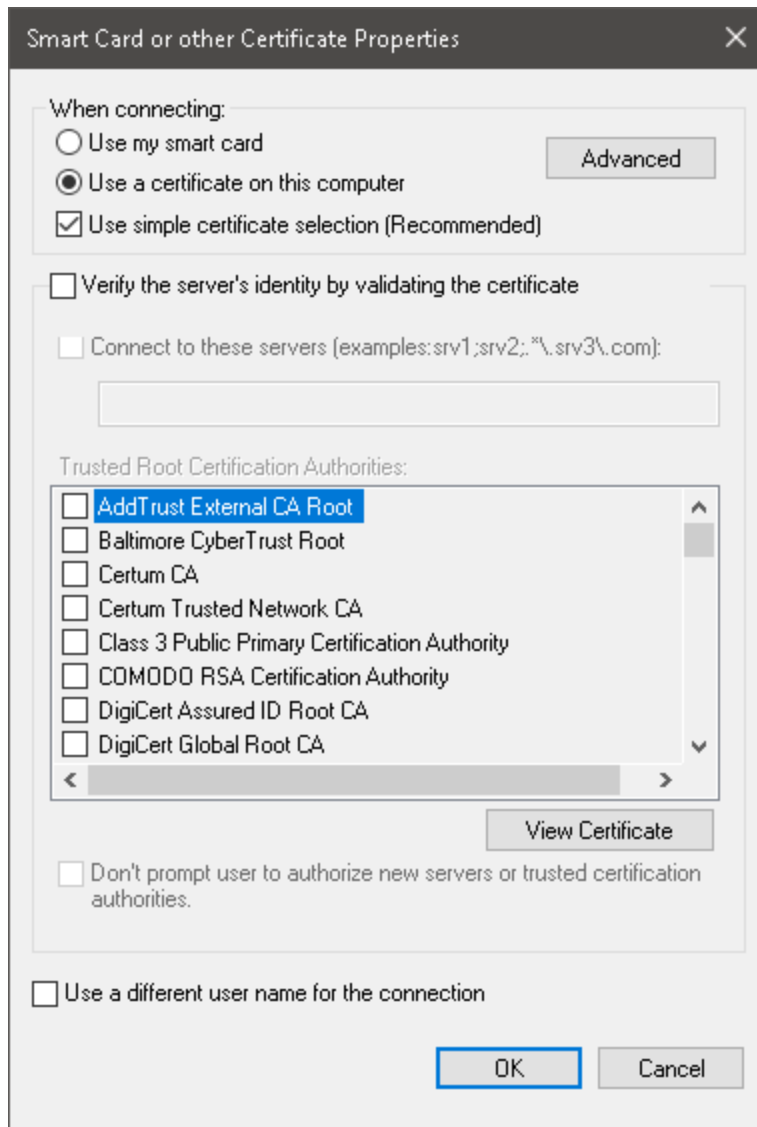
3. In the *Security* tab, set *Choose a network authentication method* to *Microsoft: Smart card or other certificates*, and select *Settings*.



4. Enable both *Use a certificate on this computer* and *Use simple certificate selection*.

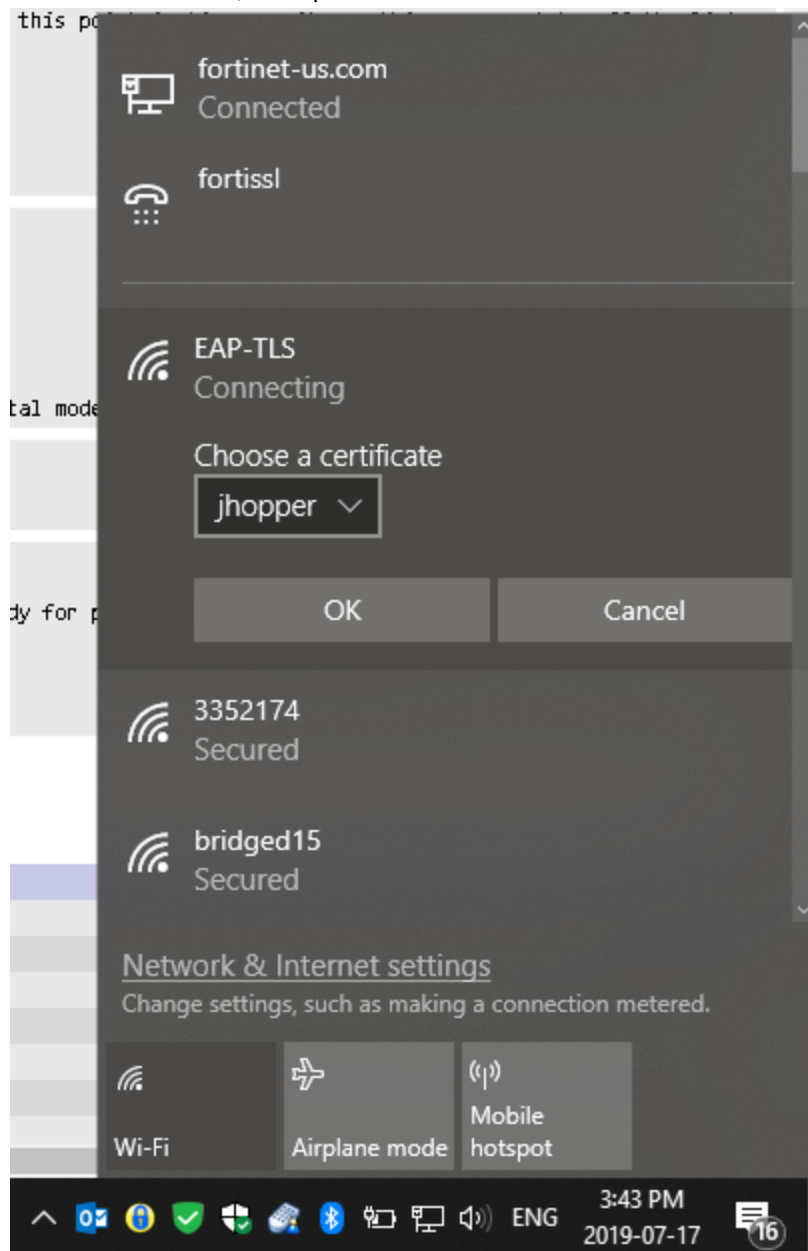
Note that, for simplification purposes, *Verify the server's identity by validating the certificate* has been disabled. However EAP--TLS allows the client to validate the server as well as the server validate the client. To enable this, you will need to import the CA from the FortiAuthenticator to the 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.



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.

Refresh	Download Raw Log	Log Type Reference	Debug Report	Search for log records						
ID	Timestamp	Level	Category	Sub category	Type Id	Action	Status	Source IP	Short message	Log Details
2173	Wed Jul 17 15:44:28 2019	Information	Event	Authentication	20420	Authentication	Success	172.25.176.37	802.1x authentication successful	Log Record Detail ID 2173 Timestamp Wed Jul 17 15:44:28 2019 Level Information Action Authentication Status Success Source IP 172.25.176.37 Message 802.1x authentication successful User jhopper Type Id 20420 Name 802.1x Authentication OK Sub Category Authentication Category Event Description 802.1x authentication successful

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

Refresh		Search		Q						
SSID	FortiAP	User	IP	MAC Address	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal Strength	Association Time
EAP-TLS	FortiAP-S 221E (PS221ETF18000452)	jhopper	10.122.122.2	10:5B:AD:32:B8:0D	ot-abristo-nb1.fortinet-us.com	112	400 bps	39dB	-88 dBm	2019/07/17 12:44:08

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

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

Log Details

General

Date2019/07/17
Time12:51:49
Duration180s
Session ID7548
Virtual Domainroot
NAT TranslationSource

Source

IP10.122.122.2
NAT IP172.25.176.37
Source Port56268
Country/RegionReserved
Primary MAC10:5b:ad:32:b8:0d
Source InterfaceEAP-TLS (EAP-TLS)
Source SSIDEAP-TLS
Host Nameot-abristo-nb1.fortinet-us.com
Device TypeUnknown
OS NameWindows
Userjhopper

Destination

IP172.16.95.16
Port53
Country/RegionReserved
Destination Interfacewan1

Application Control

Application Name
Categoryunscanned
Riskundefined
Protocol17
ServiceDNS

Data

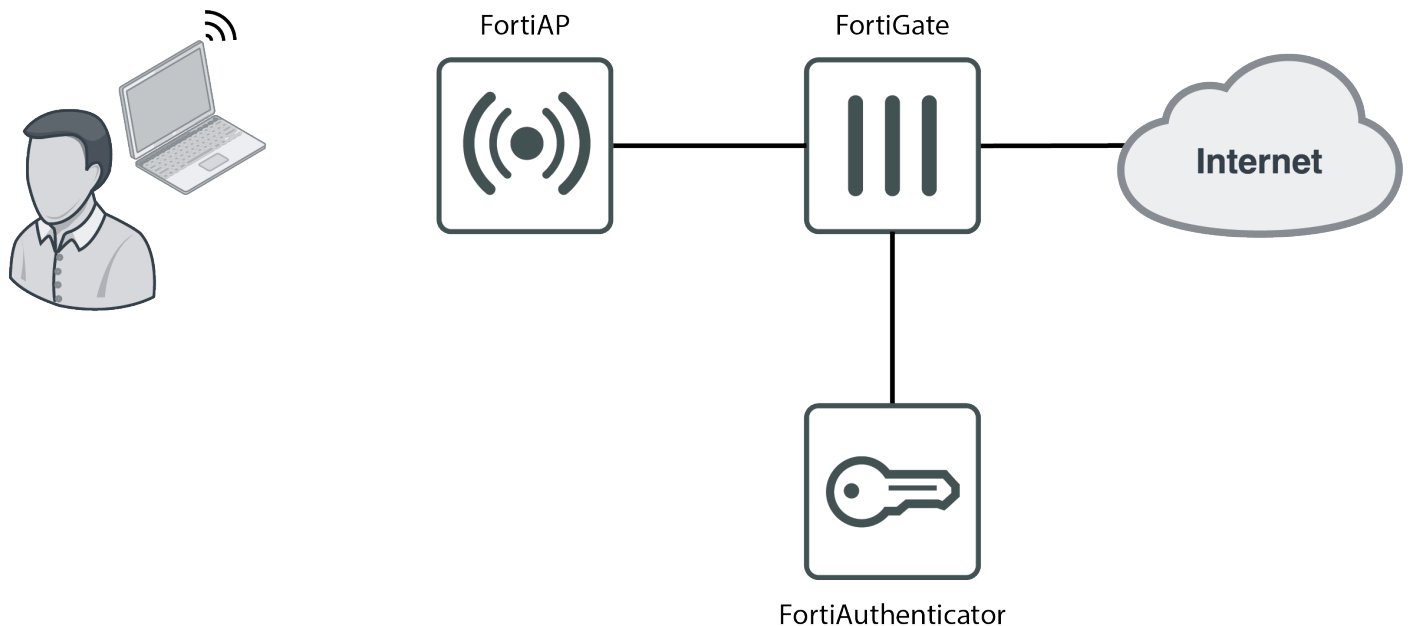
Received Bytes124 B
Received Packets1
Sent Bytes73 B
Sent Packets1

Action

ActionAccept
Policyeap-tls-internet (3)
Policy UUIDbc365144-a8ca-51e9-8fb7-7a1708be34bd
Policy Typepolicy

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 to authenticate users who belong to the employees user group.

Creating users and user groups on the FortiAuthenticator

To create users and user groups:

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

Create New Local User

Username:

Password creation:

Password:

Password confirmation:

☒ Allow RADIUS authentication

☐ Force password change on next logon

Role

Role:

Account Expiration

☐ Enable account expiration

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

Create New User Group

Name:

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

Users:

Available Users ?

Filter

admin

Selected Users

rgreen

Choose all Remove all

Password policy:

☐ Usage Profile

OK Cancel

Registering the FortiGate as a RADIUS client on the FortiAuthenticator

To create the RADIUS client:

1. On the FortiAuthenticator, go to *Authentication > RADIUS Service > Clients*, and select *Create New*.
2. Enter a *Name*, the IP address of the FortiGate, and set a *Secret*.

The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.

Create New Authentication Client

Name:

Client address:

Secret:

☐ Accept RADIUS accounting messages for usage enforcement

☐ Support RADIUS Disconnect messages

OK Cancel

To create the RADIUS policy:

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

Configuring FortiGate to use the RADIUS server

To configure FortiGate to use the RADIUS server:

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

New RADIUS Server

Name

facRADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.25.176.141

Secret

Connection status

☒ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

Creating SSID and set up authentication

To create an SSID and set up authentication:

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

New

Interface Name

example-wifi

Alias

Type

WiFi SSID

Traffic Mode

  Tunnel  Bridge  Mesh

Tags

 Add Tag Category

Address

IP/Network Mask

10.10.12.1/24

IPv6 Address/Prefix

::/0

2. Set up DHCP for your clients.

☒ DHCP Server

Address Range

 Create New

 Edit

 Delete

Starting IP	End IP
10.10.12.2	10.10.12.254

Netmask

255.255.255.0

Default Gateway

Same as Interface IP

Specify

DNS Server

Same as System DNS

Same as Interface IP

Specify

 Advanced...

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

WiFi Settings

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

Connecting and authorizing the FortiAP

To connect and authorize the FortiAP:

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

Administrative Access

IPv4	☐ HTTPS	☐ HTTP ⓘ	☒ PING	☐ FMG-Access
	☒ CAPWAP	☐ SSH	☐ SNMP	☐ FTM
	☐ RADIUS Accounting		☐ FortiTelemetry	
IPv6 Administrative Access	☐ HTTPS	☐ HTTP ⓘ	☐ PING	☐ FMG-Access
	☐ CAPWAP	☐ SSH	☐ SNMP	☐ FTM
Receive LLDP ⓘ	Use VDOM Setting	Enable	Disable	
Transmit LLDP ⓘ	Use VDOM Setting	Enable	Disable	

☒ DHCP Server

Address Range

Starting IP	End IP
10.10.201.1	10.10.201.1
10.10.201.3	10.10.201.254

Netmask

255.255.255.0

Default Gateway

Same as Interface IP Specify

DNS Server

Same as System DNS Same as Interface IP Specify

+ Advanced...

Networked Devices

Device Detection ☒

2. Connect the FortiAP unit to the interface. Then go to *WiFi & Switch Controller > Managed FortiAPs*. Notice the *Status* is showing *Waiting for Authorization*.

When the FortiAP is listed, select and *Authorize* it.

+ Create New		Edit	Delete	Refresh	<input checked="" type="button" value="Authorize"/>	Upgrade	0/32 Managed FortiAPs			AP	Radio	Group
Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Ref.				
FortiAP-S 221E	Waiting for Authorization	10.10.201.1 - port3	Radio 1: None Radio 2: None	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	PS221E-v6.2-build0232	FAPS221E-default	0				

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

+ Create New Edit Delete Refresh Upgrade						1/32 Managed FortiAPs		AP	Radio	Group
Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Ref		
FortiAP-S 221E	Online	10.10.201.1 - port3	Radio 1: None Radio 2: None	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	PS221E-v6.2-build0232	FAPS221E-default	0		

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

Radio 1

Mode

DisabledAccess PointDedicated Monitor

WIDS Profile

☐

Radio Resource Provision

☐

Client Load Balancing

☐ Frequency Handoff☐ AP Handoff

Band

2.4 GHz802.11n/g/b

Channel Width

20MHz

Short Guard Interval

☐

Channels

☒ 1☒ 6☒ 11

TX Power Control

AutoManual

TX Power

100%

SSIDs

AutoManual

example-staff (example-wifi)

Monitor Channel Utilization

☐

Creating the security policy

To create the security policy:

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

New Policy

Name ⓘ	WiFi Internet	
Incoming Interface	 example-staff (example-wifi) +	✕
Outgoing Interface	 wan1 +	✕
Source	 all +	✕
Destination	 all +	✕
Schedule	 always ▼	
Service	 ALL +	✕
Action	☒ ACCEPT ☐ DENY ☐ IPsec	
Inspection Mode	☒ Flow-based ☐ Proxy-based	

Firewall / Network Options

NAT ☒

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

Logging Options

Log Allowed Traffic ☒

Security Events
 ☒ All Sessions

Capture Packets ☐

Comments 0/1023

Enable this policy ☒

Results

1. Connect to the *example-staff* network and browse Internet sites.

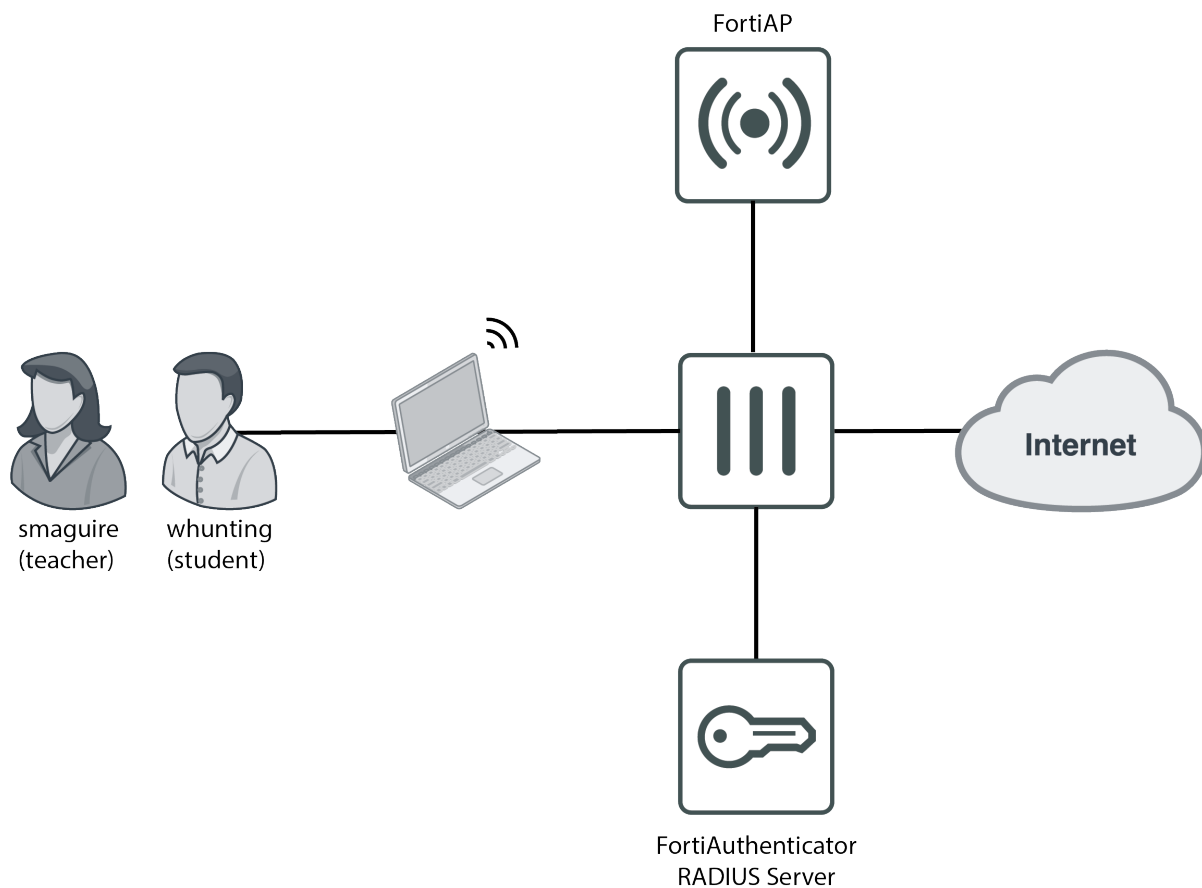
On the FortiGate, go to *Monitor > WiFi Client Monitor* to see that clients connect and authenticate.

Refresh

Search

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

WiFi with WSSO using FortiAuthenticator RADIUS and Attributes



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

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

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

Registering the FortiGate as a RADIUS client on the FortiAuthenticator

To create the RADIUS client:

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

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*).

Create New Local User

Username:

smaguire

Password creation:

Specify a password

Password:

••••••••

Password confirmation:

••••••••

☒ Allow RADIUS authentication

☐ Force password change on next logon

Role

Role:

Administrator

Sponsor

User

Account Expiration

☐ Enable account expiration

OK

Cancel

Create New Local User

Username:

whunting

Password creation:

Specify a password

Password:

••••••••

Password confirmation:

••••~•~•~

☒ Allow RADIUS authentication

☐ Force password change on next logon

Role

Role:

Administrator

Sponsor

User

Account Expiration

☐ Enable account expiration

OK

Cancel

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

Edit Local User

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

Username: whunting

☐ Disabled

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

☐ Token-based authentication

☒ Allow RADIUS authentication

☐ Enable account expiration

☐ Force password change on next logon

User Role

Role: Administrator Sponsor **User**

☐ Allow LDAP browsing

+ User Information

+ Alternative Email Addresses

+ Password Recovery Options

+ Groups

+ Usage Information

+ Email Routing

RADIUS Attributes

Attribute	Value	Vendor	Actions
Add Attribute			

+ Certificate Bindings

+ Devices

OK Cancel

Creating user groups on the FortiAuthenticator

To create user groups:

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

Create New User Group

Name: students

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

Users:

Available Users ?

Filter

admin
smaguire

Choose all

Selected Users

whunting

Remove all

Password policy: Default

☐ Usage Profile [Please Select]

OK Cancel

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.

The screenshot shows the 'Edit User Group' interface in FortiAuthenticator. The 'Name' field is set to 'students'. The 'Type' is 'Local'. The 'Users' list shows 'admin', 'john.doe', 'rgreen', and 'smaguire'. A modal window titled 'Create New User Group RADIUS Attribute' is open, showing 'Vendor' as 'Fortinet', 'Attribute ID' as 'Fortinet-Group-Name', 'Type' as 'String', and 'Value' as 'students'. The 'Add Attribute' button is visible at the bottom left of the modal.

Configuring the FortiGate to use the FortiAuthenticator as the RADIUS server

To configure the FortiGate to use the FortiAuthenticator RADIUS server:

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

New RADIUS Server

Name

fac-radius

Authentication method

Default

Specify

NAS IP

Include in every user group

☐

Primary Server

IP/Name

172.25.176.141

Secret

.....

Connection status

✓

 Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name

Secret

Test Connectivity

Test User Credentials

OK

Cancel

Configuring user groups on the FortiGate

To configure user groups on the FortiGate:

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

New User Group

Name

students

Type

Firewall

Fortinet Single Sign-On (FSSO)

RADIUS Single Sign-On (RSSO)

Guest

Members

+

Remote Groups

+ Add

Edit

Delete

Remote Server	Group Name
No matching entries found	

OK

Cancel

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:

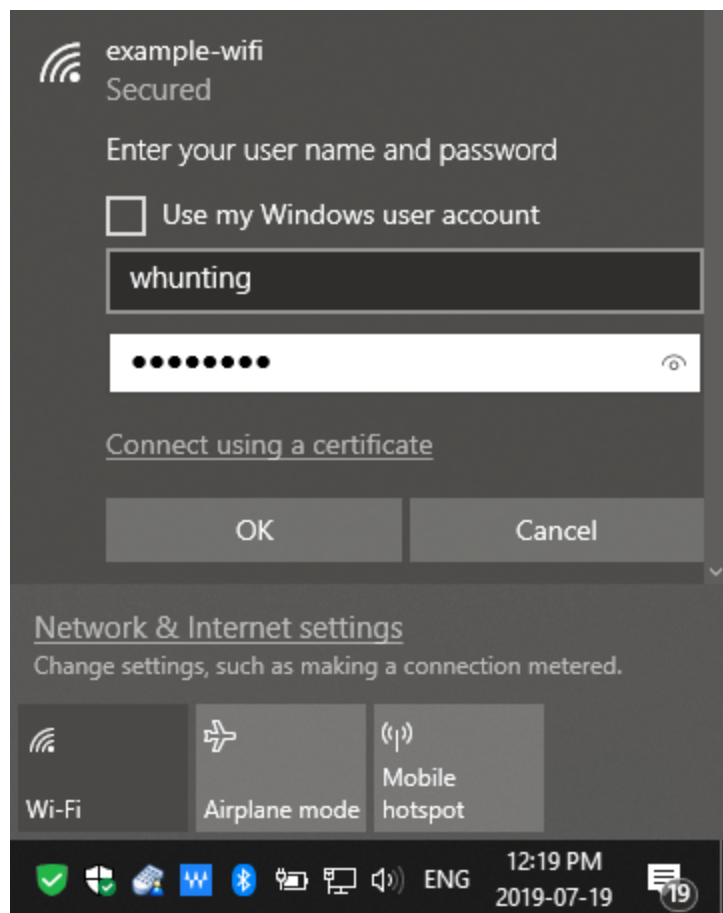
1. Go to *WiFi & Switch Controller > SSID* and edit your pre-existing SSID interface.
Under *WiFi Settings*, set *Security Mode* to *WPA2 Enterprise*, set *Authentication* to *RADIUS Server*, and add the RADIUS server configured on the FortiGate earlier from the dropdown menu.

WiFi Settings

SSID	example-wifi
Security Mode	WPA2 Enterprise
Client Limit	☐
Authentication	Local RADIUS Server  fac-radius

Results

1. Connect to the WiFi network as a student.



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.

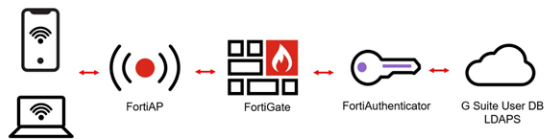
Refresh	Deauthenticate	Show all FSSO Logons	Search		
User Name ⇅	User Group ⇅	Duration ⇅	IP Address ⇅	Traffic Volume ⇅	Method ⇅
whunting	students	1 minute(s) and 24 second(s)	10.10.12.2	0 B	WiFi Single Sign-On

802.1X authentication using FortiAuthenticator with Google Workspace User Database

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

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

Topology



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

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

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

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

1. [Configuring FortiGate as a RADIUS client on page 169.](#)
2. [Configuring Google Workspace as an LDAP server. See \[Google Workspace integration using LDAP on page 175.\]\(#\)](#)
3. [Creating a realm and RADIUS policy with EAP-TTLS authentication on page 170.](#)
4. [Configuring FortiAuthenticator as a RADIUS server in FortiGate on page 171.](#)
5. [Configuring a WPA2-Enterprise with FortiAuthenticator as the RADIUS server on page 171.](#)
6. [Configuring Windows or macOS to use EAP-TTLS and PAP on page 173.](#)

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.

New RADIUS Server

Name: FortiAuthenticator_Server

Authentication method: Default Specify

NAS IP: PAP

Include in every user group: ☐

Primary Server

IP/Name: 192.168.1.100

Secret:

Test Connectivity

Test User Credentials

Connection status: ✔ Successful

Secondary Server

IP/Name:

Secret:

Test Connectivity

Test User Credentials

OK Cancel

Configuring a WPA2-Enterprise with FortiAuthenticator as the RADIUS server

To configure a WPA2-Enterprise WLAN:

1. Go to *WiFi & Switch Controller > SSIDs*.
2. From the *Create New* dropdown, select *SSID*.
3. Enter a *Name* for the interface. Optionally, you can enter an alias.
4. In *Traffic mode*, select *Bridge*.
5. In the *WiFi settings* pane:
 - a. Enter a name in the *SSID* field.
 - b. Enable *Broadcast SSID*.

- c. In *Security mode* dropdown, select *WPA2 Enterprise*.
 - d. In *Authentication*, select *RADIUS Server*, and from the dropdown select the FortiAuthenticator RADIUS server you created.
 - e. Optionally, enable *Dynamic VLAN assignment*.
 - f. For *Schedule*, select *always*.
 - g. Optionally, enable *Block intra-SSID traffic*.
 - h. Optionally, enable *Broadcast suppression*, and select *ARPs for known clients*, *DHCP unicast*, *DHCP uplink*, *IPv6*, *ALL other broadcast*, and *All other multicast*.
6. Click *OK* to save changes.

Edit Interface

Name
Alias
Type
WiFi SSID
VRF ID
0
Traffic mode
Bridge

WiFi Settings
SSID
CORP
Client limit
Broadcast SSID

Security Mode Settings
Security mode
WPA2 Enterprise
Authentication
Local
RADIUS Server
FortiAuthenticator_Server

Client MAC Address Filtering
RADIUS server

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

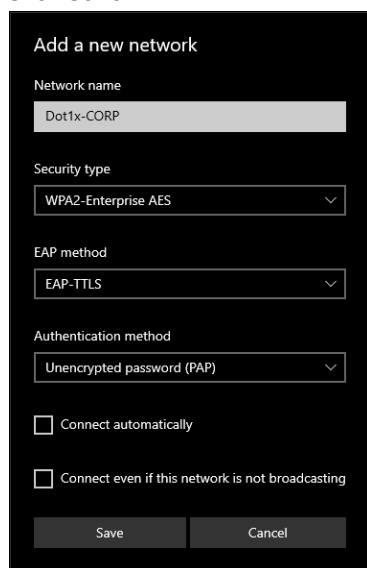
Miscellaneous
Comments
0/255
Status
Enabled Disabled

OK
Cancel

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*.



The screenshot shows the 'Add a new network' dialog box in Windows. It has a title bar 'Add a new network'. Below it are four dropdown menus: 'Network name' with the text 'Dot1x-CORP', 'Security type' with 'WPA2-Enterprise AES', 'EAP method' with 'EAP-TTLS', and 'Authentication method' with 'Unencrypted password (PAP)'. Below these are two checkboxes: 'Connect automatically' and 'Connect even if this network is not broadcasting', both of which are unchecked. At the bottom are two buttons: 'Save' and 'Cancel'.

To configure macOS to use EAP-TTLS and PAP:

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

4. Click *Create*.

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

Dot1x-CORP

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

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

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

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

Proxy Setup
Configures proxies to be used with this network

None

Security Type
Wireless network encryption to use when connecting

WPA2 Enterprise (iOS 8 or later except Apple TV)

Enterprise Settings
Configuration of protocols, authentication, and trust

Protocols Trust

Accepted EAP Types
Authentication protocols supported on target network

☐ TLS	☐ LEAP	☐ EAP-FAST	☐ EAP-AKA
☒ TTLS	☐ PEAP	☐ EAP-SIM	

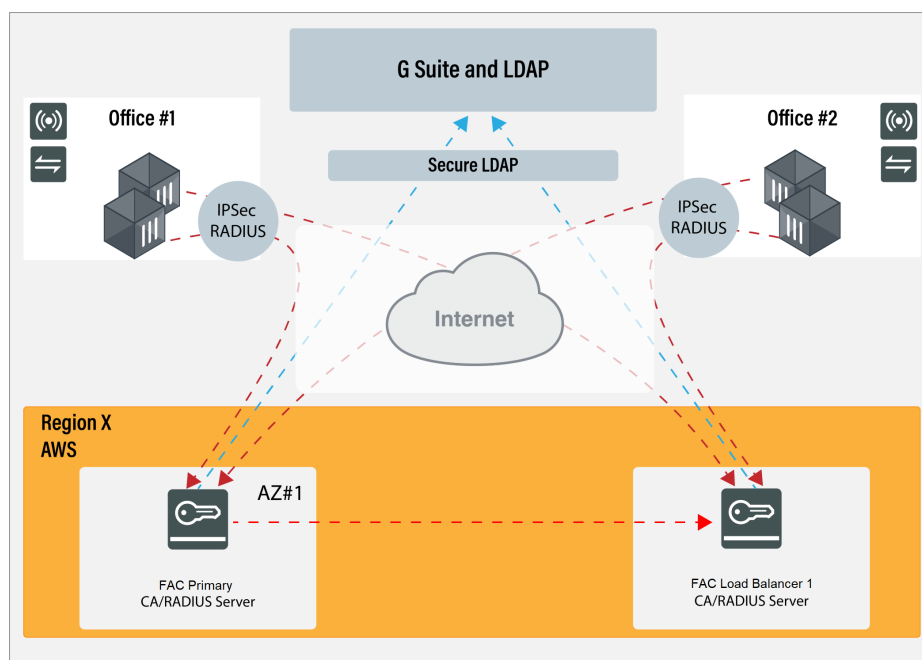
LDAP Authentication

This section describes configuring LDAP authentication.

Google Workspace integration using LDAP

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

1. [Generating the Google Workspace certificate on page 175](#)
2. [Importing the certificate to FortiAuthenticator on page 177](#)
3. [Configuring LDAP on the FortiAuthenticator on page 178](#)
4. [Troubleshooting on page 178](#)



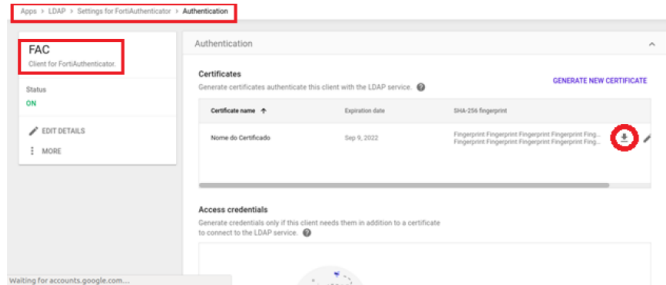
Generating the Google Workspace certificate

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.

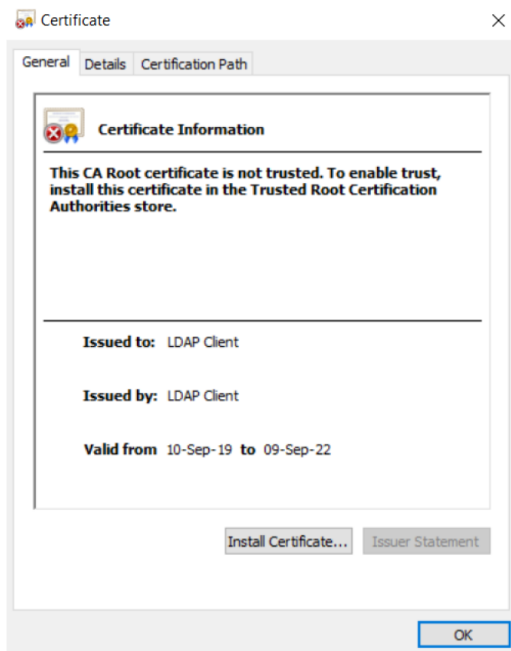
3. Click the *Authentication* card.
 4. Click *GENERATE NEW CERTIFICATE*, then click the download icon to download the certificate.
 5. Upload the certificate to your client, and configure the application.
- Depending on the type of LDAP client, configuration may require LDAP access credentials. See [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/>.

- Download CA certificates
- [Expand all](#)
- 

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

Name	Public Key	Fingerprint (SHA256)	Valid Until
GlobalSign R4	ECDSA	b0:85:d7:0b:96:4f:19:1a:73:e4:af:0d:54:ae:7a:0e:07:aa:fd:af:9b:71:db:08:62:13:8a:b7:32:5a:24:a2	2038-01-19 Action
GTS Root R1	RSA	d9:47:43:2a:bde:7b:7f:90:fc:2e:6b:59:10:1b:12:80:e0:e1:c7:e4:e4:0fa:3:c6:88:7f:ff:57:a7:4f:c1	2036-06-22 Action
GTS Root R2	RSA	8d:25:cd:97:22:db:bf:70:35:6b:da:4e:b3:cc:73:40:31:e2:4c:0f:0f:acf:d3:2dc:c7:6e:b5:84:1c:7e:a8	2036-06-22 Action
GTS Root R3	ECDSA	34:d8:a7:3e:08:2e:d9:bc:db:0d:95:65:20:93:4b:4e:40:e6:94:82:59:6e:8b:6f:73:c8:42:6b:01:0a:6f:48	2036-06-22 Action
GTS Root R4	ECDSA	34:9d:fa:40:58:e5:e2:63:12:3b:39:8a:e7:95:57:3c:4e:13:13:c8:3f:e6:8f:93:55:6c:d5:e8:03:1b:3c:7d	2036-06-22 Action

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

Results:

4 trusted CA certificates.

1. Go to *Certificate Management > End Entities > Local Services > Import.*

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 OK Cancel

+ Create New Import Revoke Delete Export Certificate Search for server certificates					
Certificate ID	Subject	Issuer	Status	Expiry	
Fortinet_CA1_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuth...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active	Jan. 19, 2038, 1:14 a.m.	
Fortinet_CA2_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=FortiAuth...	Remote CA: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=C...	Active	Jan. 19, 2056, 1:14 a.m.	
Gsuite_LDAP	O=Google Inc., L=Mountain View, CN=LDAP Client, OU=GSuite, C=...	Remote CA: O=Google Inc., L=Mountain View, CN=LDAP Client, OU=...	Active	Sept. 9, 2022, 5:06 p.m.	

Configuring LDAP on the FortiAuthenticator

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

- Go to *Authentication > Remote Auth. Servers > LDAP > Create New*, and enter the following information:
 - Enter a name.
 - For *Primary server name/IP* enter `ldap.google.com`, and set the port to 636.
 - Enter the base distinguished name.
 - For the *Username attribute*, enter `uid`.
 - Select the option to obtain group memberships from *Group attribute*.
 - Enable *Secure Connection* and select either *LDAPS* or *STARTTLS* as the *Protocol*, and select *All Trusted* in the *Trusted CA* option.
 - Enable *Use Client Certificate for TLS Authentication*, and select the LDAP certificate.

Create New LDAP Server

Name: GoogleLDAP

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

☐ Use secondary server

Base distinguished name: [Browse]

Bind type: Simple Regular

Server type: Microsoft Active Directory OpenLDAP/GSuite Novell eDirectory/Others Apply template

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

Query Elements

User object class: person

Username attribute: uid

Group object class: group

Obtain group memberships from: User attribute Group attribute

Group membership attribute: memberOf

☒ Force use of administrator account for group membership lookups

Secure Connection

☒ Enable

Protocol: LDAPS STARTTLS

Trusted CA: Single All Trusted

CA certificate: [Please Select]

☒ Use Client Certificate for TLS Authentication

Client certificate: [Please Select]

Windows Active Directory Domain Authentication

☐ Enable

OK Cancel

- Select *OK*.

If required, you can now import users by selecting *Import users* when editing the LDAP server, selecting the LDAP server from the *Remote LDAP server* dropdown, and clicking the *Go* button next to the *Import users* dropdown. This is not a required step, but can be done in cases where you want to include additional information to their accounts or assign FortiTokens.

Import Remote LDAP Users

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

Action: Import users Go

OK Cancel

Troubleshooting

Missing option to use client certificate for TLS authentication

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

The screenshot shows the FortiAuthenticator VMXEN configuration interface. The left sidebar lists various system settings, with 'Remote Auth. Servers' selected. The main panel is titled 'Edit LDAP Server' and contains the following fields:

- Name:** GoogleLDAP
- Primary server name/IP:** ldap.google.com
- Port:** 636
- Bind type:** Simple (selected), Regular
- Query Elements:**
 - Pre-defined templates:** (Dropdown menu)
 - User object class:** person
 - Username attribute:** uid
 - Group object class:** group
 - Obtain group memberships from:** User attribute (selected), Group attribute
 - Group membership attribute:** memberOf
 - Force use of administrator account for group membership lookups:** (Checked)
- Secure Connection:**
 - Enable:** (Checked)
 - Protocol:** LDAPS (selected), STARTTLS
 - CA certificate:** Google CA | OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign
 - Use Client Certificate for TLS Authentication:** (Checked)
 - Client certificate:** Google LDAP | O=Google Inc., L=Mountain View, CN=LDAP Client, OU=GSuite, C=US, ST=California

At the bottom, there is a section for 'Windows Active Directory Domain Authentication'.

Certificate error messages

The following is an example of an incorrect Trusted CA certificate entry. Please verify that you have followed the steps included in [Generating the Google Workspace certificate on page 175](#).

The first screenshot shows the 'Import Remote LDAP Users - Google Chrome' window. The URL bar indicates a connection to 'ldap.google.com:636'. The 'LDAP server' field is set to 'ldap.google.com:636'. The 'Filter' field is '(objectClass=person)'. The 'Distinguished name' field is 'dc=ldap,dc=com,dc=br'. The 'Organization' field is '[Please Select]'. A red box highlights the error message: 'Query failed: ldap_search_ext_s connection failed: Can't connect LDAP server error:5416f08655L routines:tls_process_server_certificate:certificate verify failed: unable to get local issuer certificate'.

The second screenshot shows a Wireshark packet capture of the LDAP connection. The packet list shows a '73 Alert (Level: fatal, Description: Unknown CA)' at the bottom. The packet details pane shows the 'Alert Message' with the description 'Unknown CA (48)'. The packet bytes pane shows the raw data of the alert message.

SAML Authentication

This section describes configuring SAML authentication.

SAML IdP proxy for Azure

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

To configure FortiAuthenticator as a SAML IdP proxy for Azure:

1. [Configuring OAuth settings on page 180](#)
2. [Configuring the remote SAML server on page 181](#)
3. [Creating a remote SAML user synchronization rule on page 182](#)
4. [Configuring an Azure realm on page 183](#)
5. [Configuring SAML IdP settings on page 183](#)
6. [Configuring SP settings on FortiAuthenticator on page 183](#)
7. [Configuring the login page replacement message on page 184](#)
8. [Results on page 185](#)

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 181](#) and [Creating a remote SAML user synchronization rule on page 182](#).

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 180](#).
5. At the top of the page, select *Proxy* as the *Type*, and copy the *Portal URL* to be used later when customizing the replacement message.

6. Click **OK** to save changes.

Creating a remote SAML user synchronization rule

To create a SAML synchronization rule:

1. Go to **Authentication > User Management > Remote User Sync Rules**.
2. In the **Remote User Sync Rules** tab, select **SAML**, and then select **Create New**. The **Create New Remote SAML User Synchronization Rule** window opens.
3. Enter a name for the synchronization rule.
4. In **Remote SAML server**, select the remote SAML server created in [Configuring the remote SAML server on page 181](#).
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)**.

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

Configuring an Azure realm

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

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

Configuring SAML IdP settings

To configure general settings:

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

Edit SAML Identity Provider Settings

☒ Enable SAML Identity Provider portal

Device FQDN:

Server address:

IdP-initiated login URL:

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

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

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	addip Local users	☐	Filter:	☒

Login session timeout: minutes (5-1440)

Default IdP certificate:

☒ Automatically switch IdP certificate before its expiry time

Default signing algorithm:

☒ Get nested groups for user

☒ IAM login

- Click *OK* to save changes.

Configuring SP settings on FortiAuthenticator

To configure service provider settings:

- 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.
- Enter the following information:
 - SP name:** Enter a name for the SP device.
 - IdP prefix:** Select *+*, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
 - Server certificate:** Select the same certificate as the default IdP certificate used in *Authentication > SAML IdP > General*. See [Configuring SAML IdP settings on page 183](#).
- Click *Save*.
- 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*.

The screenshot shows the FortiAuthenticator VM configuration interface. The left sidebar lists various configuration categories: System, Authentication, User Account Policies, User Management, Portals, Remote Auth. Servers, RADIUS Service, TACACS+ Service, LDAP Service, OAuth Service, SAML IdP, Replacement Messages, Service Providers, FAC Agent, Fortinet SSO Methods, Monitor, Certificate Management, and Logging. The main panel is titled 'Edit SAML Service Provider' and shows configuration for 'fac.school.net'. The 'SAML IdP' section is expanded, showing 'General' and 'Service Providers' tabs. The 'Service Providers' tab is active, showing configuration for 'samlSP'. The 'SP Metadata' section includes fields for 'SP entity ID', 'SP ACS (login) URL', 'SP SLS (logout) URL', and 'SAML request must be signed by SP'. The 'Authentication' section includes 'Authentication method' (Mandatory password and OTP, All configured password and OTP factors, Password-only, OTP-only, FIDO-only) and 'Adaptive Authentication' (Configure substrate). The 'Assertion Attribute Configuration' section includes 'Subject NameID' (Username), 'Format' (urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified), 'Include realm name in subject NameID' (checked), and 'Realm Format' (username@realm). The 'Assertion Attributes' section includes 'SAML attribute' (memberid) and 'User attribute' (SAML_username). The 'Debugging Options' section includes 'Do not return to service provider automatically after successful authentication, wait for user input' and 'Disable this service provider'. The bottom of the panel has buttons for 'Import SP metadata', 'OK', and 'Cancel'.

10. Click *OK* to save changes.

Configuring the login page replacement message

To configure the login page replacement message:

1. Go to *Authentication > SAML IdP > Replacement Messages*.
2. On the *Login Page* replacement message, click the *Restore Defaults* dropdown and choose *idp-server-and-proxy*.
3. In the text/html editor, scroll down until you see the `[proxy_porta1_ur1]` placeholder and replace it with the previously saved proxy portal URL.

FortiAuthenticator VM FAC-IdP

System

- Authentication
 - User Account Policies
 - User Management
 - Self-service Portal
 - Portals
 - Remote Auth. Servers
 - RADIUS Service
 - LDAP Service
 - OAuth Service
 - SAML IdP**
 - General
 - Replacement Messages**
 - Service Providers
 - FAC Agent
 - Fortinet SSO Methods
 - Monitor
 - Certificate Management
 - Logging

Manage Images

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

Save Restore Default Toggle Tag List

Please enter correct credentials.

Example message

John

Password

Login

Or Sign in using a cloud server

```

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

```

4. Click **Save**.

Results

To test Azure login through the SP:

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

SAML IdP proxy for Google Workspace

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

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

1. Configuring OAuth settings on page 186
2. Configuring the remote SAML server on page 186
3. Creating a remote SAML user synchronization rule on page 187
4. Configuring a Google Workspace Realm on page 188
5. Configuring IdP settings on page 188
6. Configuring SP settings on FortiAuthenticator on page 189
7. Configuring the login page replacement message on page 190
8. Results on page 190

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 186](#) and [Creating a remote SAML user synchronization rule on page 187](#).

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 186](#).
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 186](#).
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. Enable the SAML identity provider portal and enter the following:
 - a. **Server address:** Enter the FortiAuthenticator FQDN.
 - b. **Realms:** Add the realm associated with the remote server for Google Workspace.
 - c. **Default IdP certificate:** Select a default certificate to use.

3. Click *OK* to save your changes.

Configuring SP settings on FortiAuthenticator

To configure service provider settings:

1. Go to *Authentication > SAML IdP > Service Providers* and create a new reference for the service provider that you will be using as your SAML client.
2. Enter the following information:
 - a. **SP name:** Enter a name for the SP device.
 - b. **IdP prefix:** Select *+*, enter an IdP prefix in the *Create Alternate IdP Prefix* dialog or select *Generate prefix*, and click *OK*.
 - c. **Server certificate:** Select the same certificate as the default IdP certificate used in *Authentication > SAML IdP > General*. See [Configuring IdP settings on page 188](#).
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*.

The screenshot shows the FortiAuthenticator VM configuration interface for a SAML Service Provider. The left sidebar lists various configuration categories, with 'SAML IdP' selected. The main panel is titled 'Edit SAML Service Provider' and contains several sections:

- General:** Includes fields for 'IdP address' (fac.school.net), 'SP name' (samlsp), 'IdP prefix' (3dtkw@v9h1174gjh), 'IdP entity id' (http://fac.school.net/saml-idp/3dtkw@v9h1174gjh/metadata/), 'IdP single sign-on URL' (https://fac.school.net/saml-idp/3dtkw@v9h1174gjh/login/), 'IdP single logout URL' (https://fac.school.net/saml-idp/3dtkw@v9h1174gjh/logout/), 'Server certificate' (Default Server Certificate | CN=Default Server Certificate-38A870E), and 'IdP signing algorithm' (Use default signing algorithm in SAML IdP General page).
- SP Metadata:** Includes an 'Import SP metadata' button and fields for 'SP entity ID' (http://129ip.org/saml-sp/samlServer128/metadata/), 'SP ACS (login) URL' (https://129ip.org/saml-sp/samlServer128/saml/acs), and 'SP SLS (logout) URL' (https://129ip.org/saml-sp/samlServer128/saml/sls). There is also an 'Alternative ACS URLs' field.
- Authentication:** Includes a checkbox for 'Support IdP-initiated assertion response', a checkbox for 'Participate in single logout', and a section for 'Authentication method' with radio buttons for 'Mandatory password and OTP', 'All configured password and OTP factors' (selected), 'Password-only', 'OTP-only', and 'FIDO-only'. There is also a 'Configure subnets' button.
- Adaptive Authentication:** Includes a checkbox for 'Adaptive Authentication' and a section for 'Application name for FTM push notification'.
- Assertion Attribute Configuration:** Includes a dropdown for 'Subject NameID' (Username), a dropdown for 'Format' (urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified), a checkbox for 'Include realm name in subject NameID', and a 'Realm Format' field (realm/username).
- Assertion Attributes:** Includes a section for 'Assertion attribute' with a dropdown for 'SAML attribute' (memberof) and a dropdown for 'User attribute' (SAML_username). There is an 'Add Assertion Attribute' button.
- Debugging Options:** Includes checkboxes for 'Do not return to service provider automatically after successful authentication, wait for user input.' and 'Disable this service provider'.

At the bottom of the interface, there are buttons for 'IdP metadata', 'OK', and 'Cancel'.

- Click *OK* to save changes.

Configuring the login page replacement message

To configure the login page replacement message:

- Go to *Authentication > SAML IdP > Replacement Messages*.
- On the *Login Page* replacement message, click the *Restore Defaults* dropdown and choose *idp-server-and-proxy*.
- 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.

The screenshot shows the FortiAuthenticator VM FAC-IdP configuration interface. On the left, the 'SAML IdP' menu is expanded, and 'Replacement Messages' is selected. The main table lists several replacement messages, with 'Login Page' highlighted. Below the table, the 'Restore Default' dropdown is set to 'idp-server-and-proxy'. The HTML editor on the right shows the replacement of the `[proxy_portal_url]` placeholder with the actual proxy portal URL.

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

The HTML editor shows the following code snippet:

```
<div class="login" style="width:100%;>
  <div id="id_saml_login_link" class="login_link">
    <a href="[proxy_portal_url]" >Sign in</a>
  </div>
  <div class="login_msg_bar">
    <p class="error">[[!error]]</p>
  </div>
  <script type="text/javascript">
    var username_field = document.getElementById("id_username");
    var username_display = document.getElementById("id_username_display");
    var fixed_username = "[fixed_username]";
    if (fixed_username) {
      document.getElementById("id_login_title").style.fontStyle = "italic";
      username_field.style.display = "none";
      username_display.style.display = "none";
      document.getElementById("id_password").focus();
    }
    else {
      username_field.focus();
    }
  </script>
</div>
</html>
```

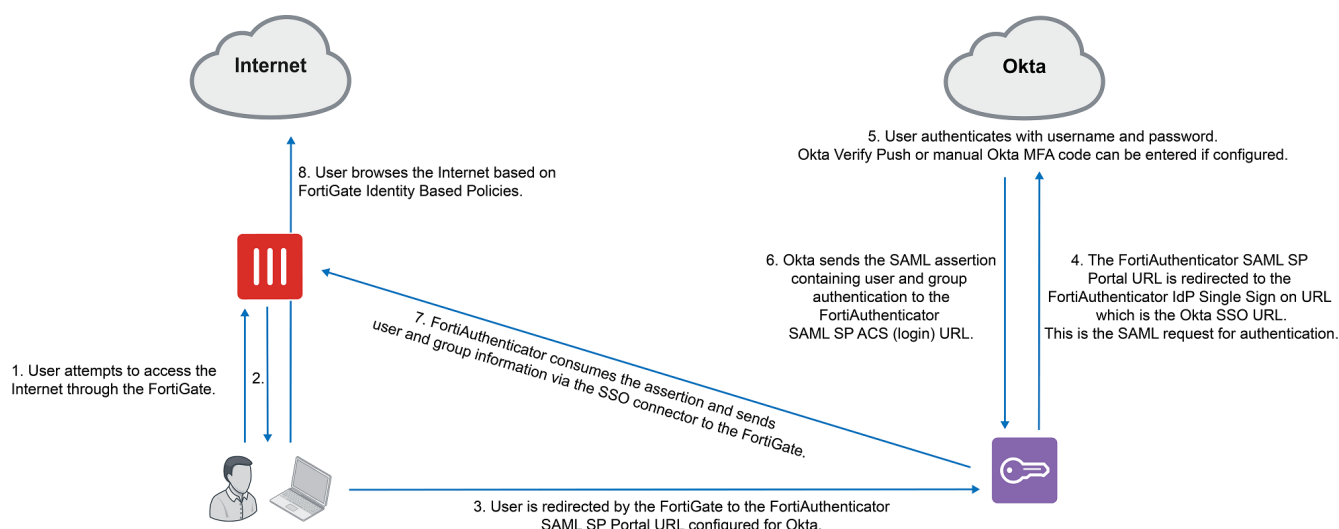
- Click *Save*.

Results

To test Google Workspace login through the SP:

- 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.
- 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.

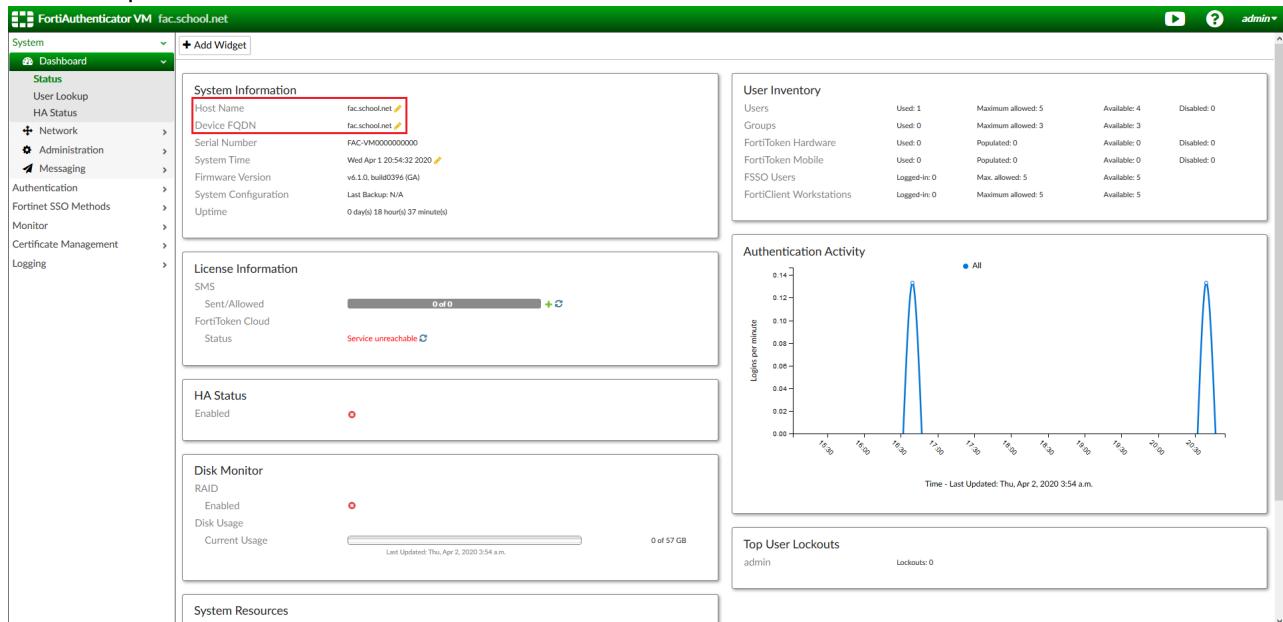
In this example configuration, the FortiGate has a DMZ IP address of 192.168.50.1, and the FortiAuthenticator has the Port1 IP address of 192.168.50.100. Note that, for testing purposes, the FortiAuthenticator's IP and FQDN have been added to the host's file of trusted host names; this is not necessary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

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

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.

FortiAuthenticator VM fac.school.net

- System > Edit SSO Configuration
- Authentication > FortiGate
- Fortinet SSO Methods > SSO
 - General
 - Listening port: 8000
 - ☒ Enable authentication
 - Secret key: [Redacted]
 - Login expiry: 480 minutes
 - Extend user session beyond logoff by: 0 seconds (0-3600)
 - ☐ Enable NTLM authentication
 - Fortinet Single Sign-On (FSSO)
 - Maximum concurrent user sessions: 0 [Configure Per User/Group]
 - Log level: [Error] [Warning] **[Info]** [Debug] [Configure Log Filter]
 - ☐ Enable Windows event log polling (e.g. domain controllers/Exchange servers)
 - ☐ Enable FortiNAC SSO
 - ☐ Enable RADIUS Accounting SSO clients
 - ☐ Enable Syslog SSO [Configure syslog sources]
 - ☐ Enable FortiClient SSO Mobility Agent Service
 - ☐ Enable hierarchical FSSO tiering
 - ☐ Enable DC/TS Agent Clients
 - ☐ Restrict auto-discovered domain controllers to configured Windows event log sources and remote LDAP servers
 - ☐ Enable Windows Active Directory workstation IP verification
 - ☒ Disable NTLMv1 in client authentication to Windows AD server
 - ☒ Disable SMB1 in client connection to Windows AD server

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

FortiAuthenticator VM fac.school.net

- System > Edit Portal Services Settings
- Authentication > User Portal
- Fortinet SSO Methods > SSO
 - General
 - Portal Services**
 - ☐ Enable SSO on login portal
 - Kerberos User Portal
 - ☐ Enable Kerberos login for SSO [Import keytab and enable]
 - Kerberos Principal:
 - SAML Portal
 - ☒ Enable SAML portal
 - SSO Web Service
 - ☐ Enable SSO Web Service

OK

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 > Create New Remote SAML Server

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 >

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

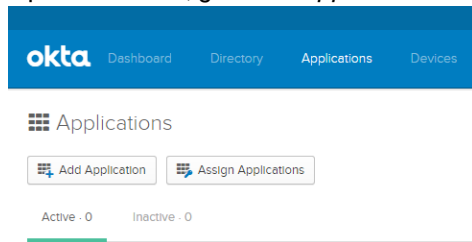
Obtain group membership from: ☒ SAML assertions
☒ "In-group" boolean assertions
☐ Text-based list
☐ LDAP lookup
☐ Cloud

☐ Implicit group membership

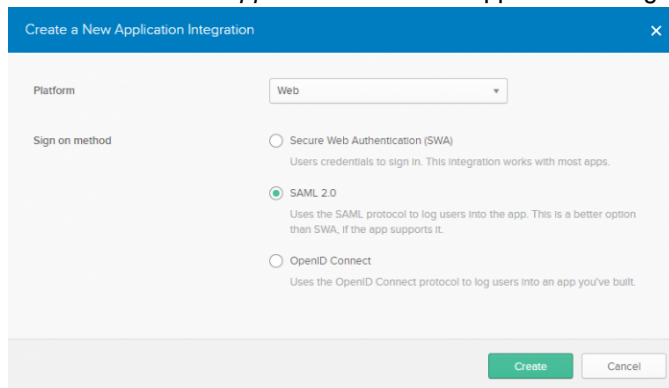
OK Cancel

Configuring the Okta developer account IdP application

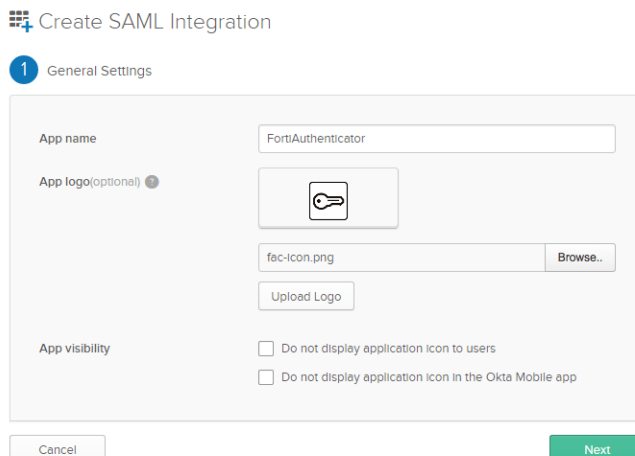
1. Open a browser, go to the *Applications* tab and select *Add Application*.



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.

SAML Settings

GENERAL

Single sign on URL

☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Application username

[Show Advanced Settings](#)

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

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

[Add Another](#)

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

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

Okta Certificate
 Import the Okta certificate to your Identity Provider if required.
[Download Okta Certificate](#)

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

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

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

[Add Another](#)

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

3 Help Okta Support understand how you configured this application

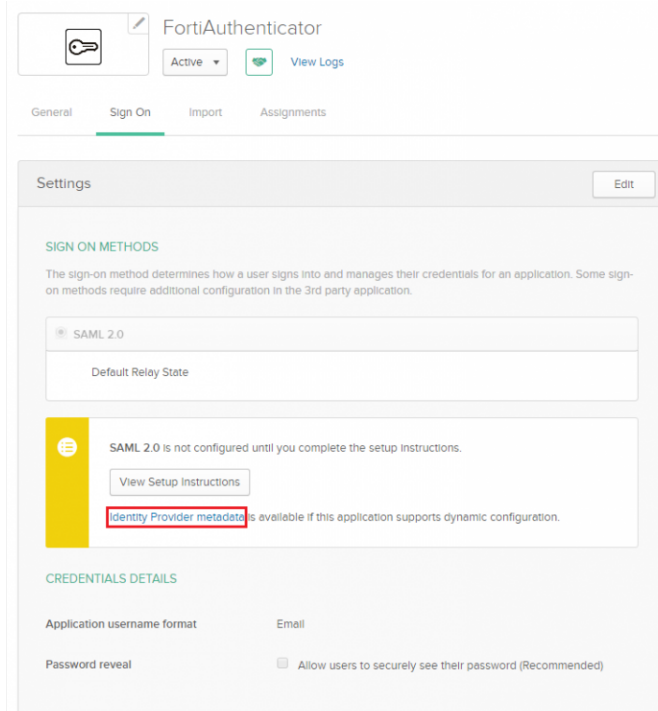
Are you a customer or partner? ☒ I'm an Okta customer adding an internal app
☐ I'm a software vendor. I'd like to integrate my app with Okta

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

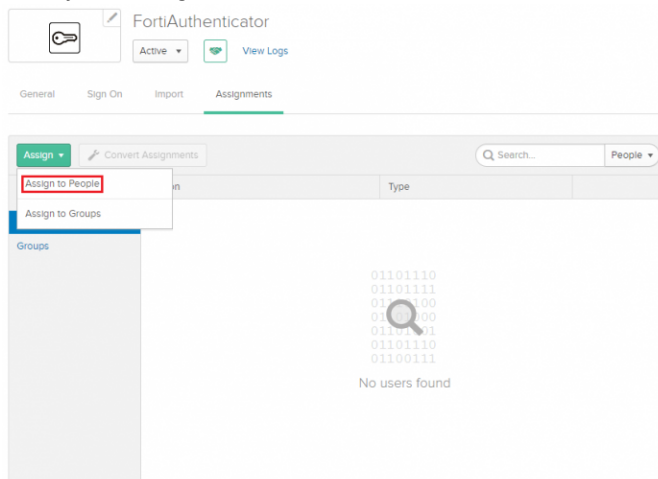
App type ☒ This is an internal app that we have created

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

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.

FortiAuthenticator VM fac.school.net

System > Edit Remote SAML Server

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 >

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: http://www.okta.com/exkar3wdtyGkleriK0h7

IdP single sign-on URL: https://dev-241684.oktapreview.com/app/fortinetdev241684_fortiauthenticator_1/exkar3wdtyGkleriK0h7/sso/saml

IdP certificate fingerprint: 218087c3d42f153f8ae55c7715afe0eae1beb099ee07635656fb3e841dccc8

Fingerprint algorithm: sha256

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

☐ Enable IdP-initiated assertion response

☐ Sign SAML requests with a local certificate

Single Logout

☐ Enable SAML single logout

Username

Obtain username from: ☒ Subject NameID SAML assertion ☐ Text SAML assertion

Group Membership

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

☐ Implicit group membership

OK Cancel

2. Enable SAML single logout and add the *IdP single logout URL* under the *Single Logout* section of the Okta Remote SAML Server.

For example, if your Okta organization is "facschool" then the *IdP single logout URL*: entry would be `https://facschool.okta.com/login/default`.

Single Logout

☒ Enable SAML single logout

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

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

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

FortiAuthenticator VM fac.school.net

System > Edit FortiGate Filter

Authentication >

Fortinet SSO Methods >

SSO >

General

Portal Services

SAML Authentication

Windows Event Log Sources

RADIUS Accounting Sources

Syslog Sources

Fine-grained Controls

SSO Users

SSO Groups

Domain Groupings

FortiGate Filtering

IP Filtering Rules

Tiered Architecture

Accounting Proxy >

Monitor >

Certificate Management >

Logging >

Name: Okta

FortiGate name/IP: 192.168.50.1

Description:

IP Filtering

☐ Enable IP filtering for this service.

Domain Grouping Filtering

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

Fortinet Single Sign-On (FSSO)

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

SSO Filtering Objects

Name/DN	Type	Actions
Okta_group1	Group	

Create New Import OK Cancel



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*.

FortiGate 100EF FortiGate_100EF

Dashboard >

Security Fabric >

Physical Topology

Logical Topology

Security Rating

Automation

Settings

Fabric Connectors ☆

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

Log & Report >

Monitor >

Edit Fabric Connector

SSO/Identity

Fortinet Single Sign-On Agent

Connector Settings

Name: fac.school.net

Primary FSSO agent: 192.168.50.100 - [password field]

Enable SSL/TLS connection ☐

User group source: Collector Agent Local

Users/Groups: 1 View

Apply & Refresh OK Cancel

Public SDN Connector Setup Guides

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Oracle Cloud Infrastructure

Private SDN Connector Setup Guides

- Cisco Application Centric Infrastructure
- Nuage Virtualized Services Platform
- OpenStack Connector
- VMware NSX

Documentation

- Online Help
- Video Tutorials

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*.

FortiGate 100EF FortiGate_100EF

Dashboard > New User Group

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

User Definition >

User Groups ☆

Guest Management

Device Inventory

LDAP Servers

RADIUS Servers

Authentication Settings

FortiTokens

Log & Report >

Monitor >

Name: Okta_group1

Type: Firewall

Fortinet Single Sign-On (FSSO)

RADIUS Single Sign-On (RSSO)

Guest

Members: OKTA_GROUP1

OK Cancel

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.

The screenshot shows the FortiGate 100EF web interface. The left sidebar has a green header with 'FortiGate 100EF' and 'FortiGate_100EF'. Below it is a navigation menu with items: Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects (expanded), IPv4 Policy, Authentication Rules, Addresses (selected), Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Security Profiles, and VPN. The main panel is titled 'Edit Address' and contains the following fields: Name (fac.school.net), Color (Change), Type (Subnet), IP/Netmask (192.168.50.100/32), Interface (dmz), Show in address list (checked), Static route configuration (unchecked), and Comments (Write a comment...). At the bottom right are OK and Cancel buttons.

2. Create the FQDN objects below.

- *.okta.com
- *.mtls.okta.com
- *.oktapreview.com
- *.mtls.oktapreview.com
- *.oktacdn.com
- *.okta-emea.com
- *.mtls.okta-emea.com
- *.kerberos.okta.com
- *.kerberos.okta-emea.com
- *.kerberos.oktapreview.com

As these are FQDNs, make sure to set *Type* to *FQDN*.

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

Edit Policy

Name ⓘ

FortiAuthenticator

Incoming Interface

 lan ▼

Outgoing Interface

 dmz ▼

Source

 lan ×

+

Destination

 fac.school.net ×

+

Schedule

 always ▼

Service

 HTTPS ×

+

Action

 ACCEPT

 DENY

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT



Add the following three policies in order:

Edit Policy

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

Firewall / Network Options

NAT 

Edit Policy

Name ⓘOkta_Bypass

Incoming Interface🔌 lan

Outgoing Interface🏠 wan1

Source🏠 lan

Destination🏠 Okta_Bypass

Schedule🕒 always

Service🏠 HTTPS

Action✔️ ACCEPT❌ DENY

Inspection ModeFlow-basedProxy-based

Firewall / Network Options

NAT🔴

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

Edit Policy

Name ⓘ

SSO_Internet_Access

Incoming Interface

 lan

Outgoing Interface

 wan1

Source

 lan

 Guest-group

 OKTA_GROUP1

+

Destination

 all

+

Schedule

 always

Service

 ALL

+

Action

 ACCEPT

 DENY

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

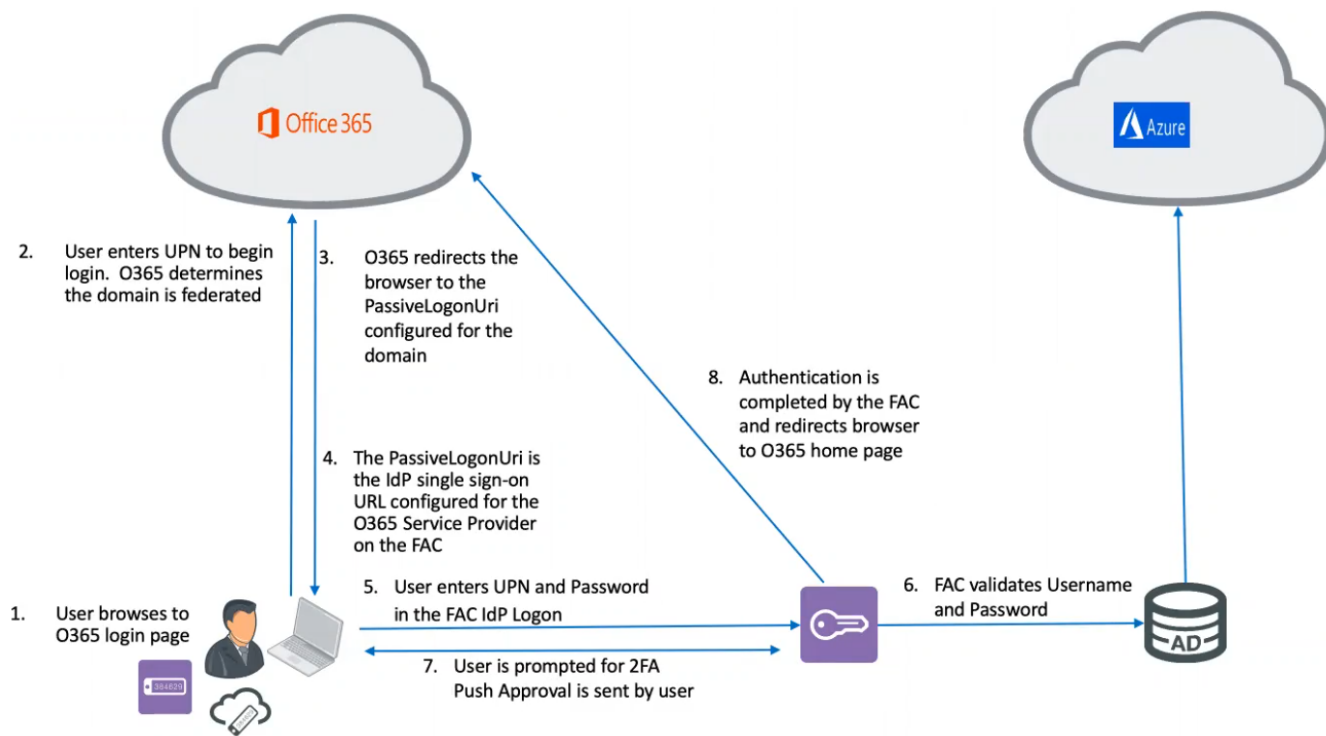
NAT



Office 365 SAML authentication using FortiAuthenticator with 2FA

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

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



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

1. [Configure the remote LDAP server on FortiAuthenticator on page 207](#)
2. [Configure SAML settings on FortiAuthenticator on page 208](#)
3. [Configure two-factor authentication on FortiAuthenticator on page 209](#)
4. [Configure the domain and SAML SP in Microsoft Azure AD PowerShell on page 210](#)
5. [Configure Microsoft Azure AD Connect on page 213](#)

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.

FortiAuthenticator VMAZURE fac1

System > Edit SAML Identity Provider Settings

Authentication > Enable SAML Identity Provider portal

Device FQDN: fac1.ftnt.xyz

Server address: fac1.ftnt.xyz

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

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

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	ad AD (172.16.10.6)	☒	☐ Filter: X	X

Login session timeout: 480 minutes (5-1440)

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

3. Click *OK* to save your changes.

To configure the service provider settings on FortiAuthenticator:

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

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

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.

Configure the domain and SAML SP in Microsoft Azure AD PowerShell

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

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

1. Launch the Microsoft Azure Active Directory Module for Windows PowerShell.
2. Enter the following command in PowerShell:

```
Install-Module -Name MSOnline.
```

Accept the next two default ("Y") prompts for installing the NuGet Provider and installing from PSGallery.



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

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

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

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

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

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

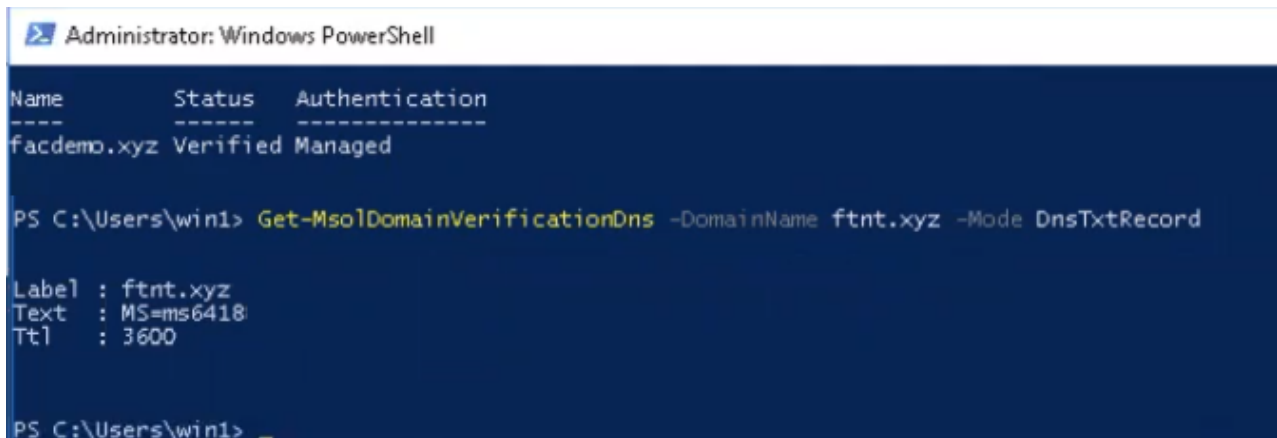
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

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

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

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

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



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



- ## 6. Configure the domain as a SAML service provider.

You can create these variables inside a text editor and then copy and paste them into a PowerShell window.

```
$domain = "<your domain>"
```

```
$cert = "<your certificate. This can be obtained by downloading your certificate from FortiAuthenticator and opening it with a text editor.>"
```

```
$protocol = "SAML"
```

```
$IssuerUrl = "<The IdP entity ID from FortiAuthenticator>"
```

```
$LogonUrl = "<The IdP single sign-on URL from FortiAuthenticator>"
```

```
$LogoffUrl = "<The IdP single logout URL from FortiAuthenticator>"
```

```
PS C:\Users\win1> $domain = "fntt.xyz"
PS C:\Users\win1> $cert = "MIIDWjCCAgqgAwIBAgIDAyAiMAOGCSqGSIb3DQEBCwUAMBgxFjAUBGNVBAAMDDWzhYzEuZnRudC54eX
> owHicNMjYwMzYMDIzOTAxWhcNMjYwMzYMDIzOTAxWjAUMYRyYwFAYDVQQDDA1mYWMxLmZvb2NueH16
> MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5nM3c7Kt0t1gXXeLCgd9VvCPAUqfLqyy5SRK
> qj/2kt0svtAeArEJYbP7MvTRhQJzL1sTuAwQHuFcfBF12aLCVwofIqb0CvNqK7L2bEVdAnpgR3
> tgt/gkbu8u32h1whufgjyftzVEWweyoHobxkrF+kpoZdf1cldYNGkoFI4nU4K1rY9WcwXUSG7N0VRu
> 1TwePwbEjG8FCG10+Zg8dZ28oPa0izp64vp2ygH2DJhGBc1vns0n/abkLHsdeuV3tL0FhmWQIDRAX
> HcbAwj1o41Cj+bbQJ1K2HMuDKvMr6TbpY8AP,4ACWf31NqvqdpPZQ9Jqf5Tn0tjBE1v0g7mWQIDAQ
> AB04IBezCCAQ8u0AYDVROTAQH,KAIwADAD8gNVH04EFgQU9MatJmk118vOS9vq+6iE5jtCw1MwRwYD
> VR0jBEAw8KwJ75E3oBj1xKLIMvZM0DX+siHHKQAMBgxFjAUBGNVBAAMDDWzhYzEuZnRudC54eX
> qCCDZzabeMTt0eMBUGA1UdeEQQOMayCCiouZnRudC54eXowEwYDVR01BAwwCgYIKwYBBQUHAEwNQYI
> KwYBBQUHAEQEK1tHnMCUGCSqGSIb3DQEBAHh1odHRwOi8vZmFjM55mdG50Lnhs5ejoyNTYwMDQQA1UdHw
> qKtMcswKAanoCQK12h0dHA6Ly9mYWMxLmZvb2NueH16L2NlcnQvY3JzLzAuzY3jSMAOGCSqGSIb3DQEBC
> wUAA41BAQArjEzkfVfcszTHB1kbo1+AA8F1yq80LSEdw9amtAyvo2T1HHZVpBU0Xj2w5u2zSF59NsPs
> oImFarq5Scmhhs3IId3fNPyM4V0979w1aKq/V00iuxL3OCfeq90+ZT9uZ50s41tiFK/BJ1dAxUxPRd
> bD8BZ3HFZqp0UCvYpaUB1YVUHTbx+keMp8dZ5HTbrmSWQ89TN/VNYKRBBgZfTxSEf83CHbozoqur
> +esrq0YgP6s3urr3pxfERNT8D3J9SJA2efgzioHj3gXcXAoss+/Ibbg+bNskusbtQ8VkbxfBDpCmD
> AjFuBTCTCB8pjF1g6W7FngfK0aJhCr1cs5mK/yabY"
PS C:\Users\win1> $protocol = "SAML"
PS C:\Users\win1> $issuerUrl = "https://fac1.fntt.xyz/saml-idp/8d95in490xe6g1bu/metadata/"
PS C:\Users\win1> $loginUrl = "https://fac1.fntt.xyz/saml-idp/8d95in490xe6g1bu/login/"
PS C:\Users\win1> $logoutUrl = "https://fac1.fntt.xyz/saml-idp/8d95in490xe6g1bu/logout/"
PS C:\Users\win1>
```

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

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

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

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

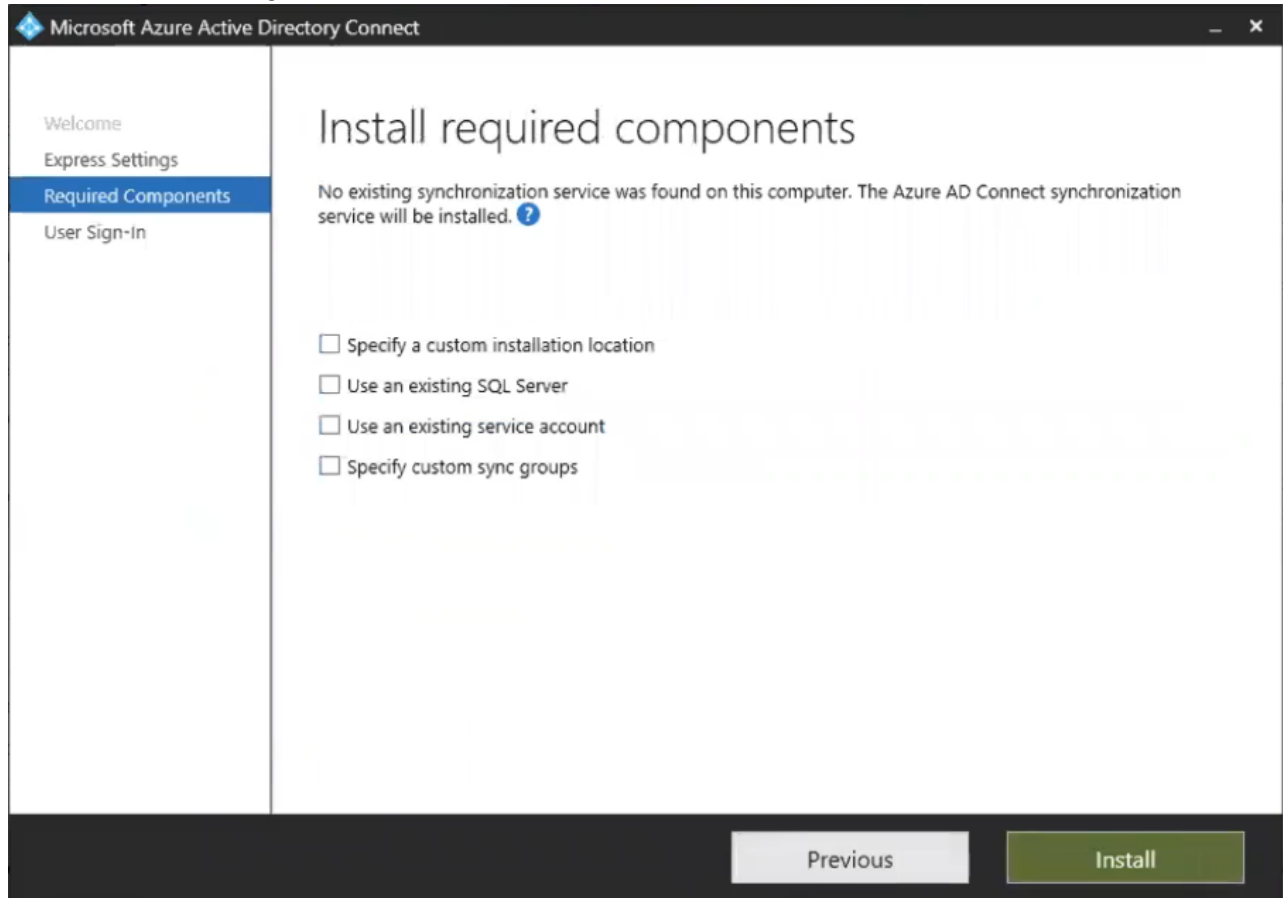
The return text from the above command should read "AvailableImmediately The domain has been successfully verified for your account."

Configure Microsoft Azure AD Connect

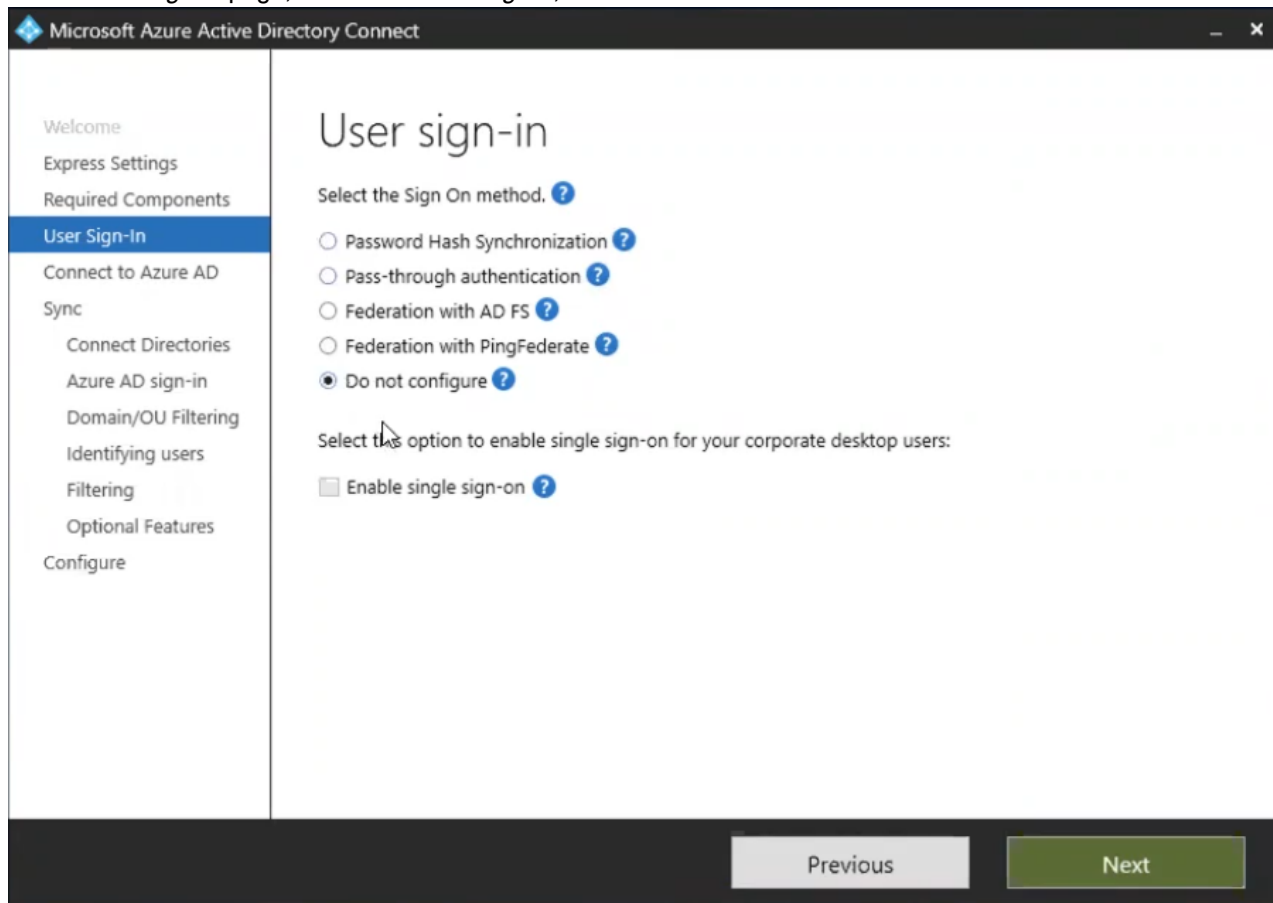
You will first need to download Azure AD Connect from Microsoft on your Active Directory Domain Controller.

To configure Microsoft Azure AD Connect:

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



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

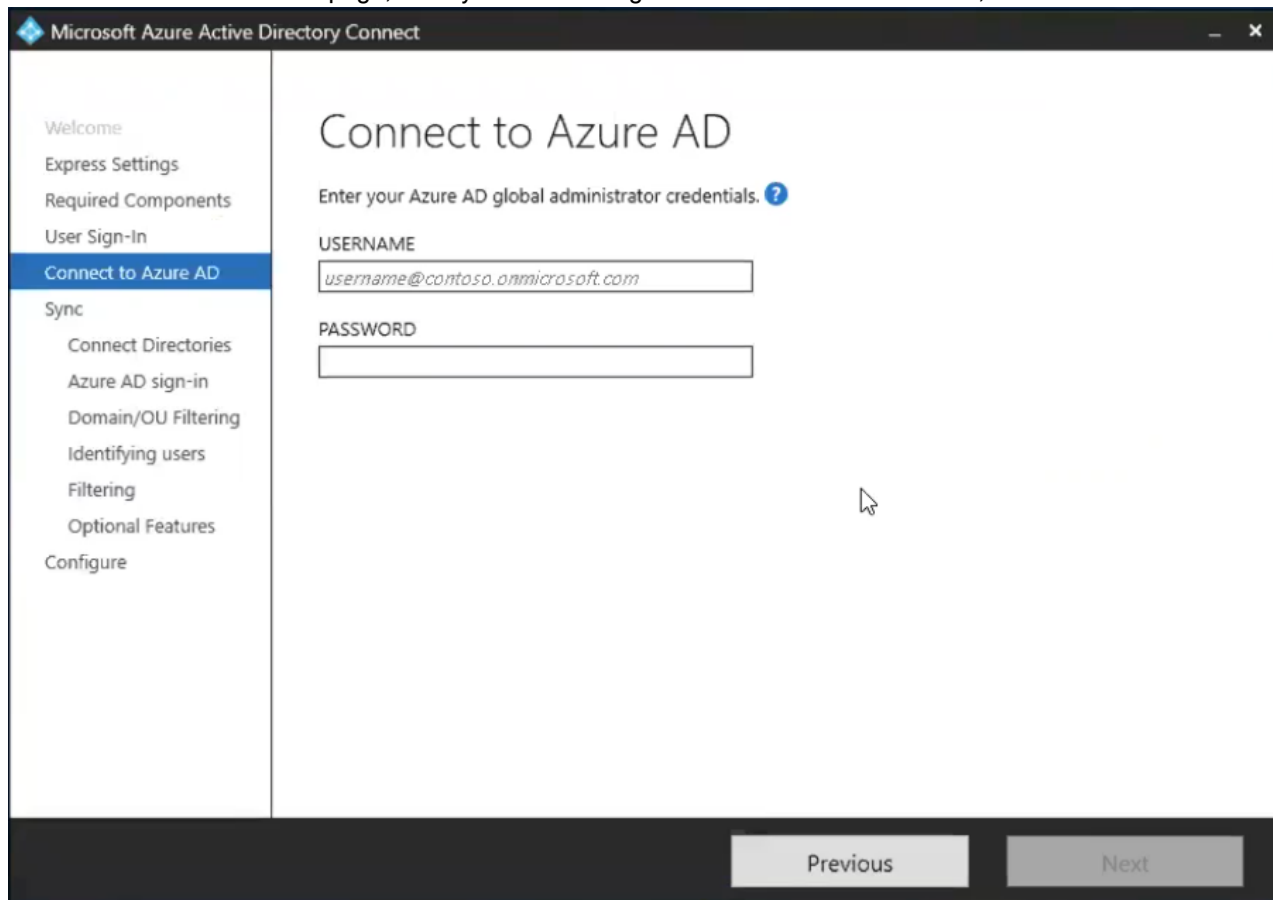


The screenshot shows the 'User sign-in' configuration window in Microsoft Azure Active Directory Connect. The window has a dark title bar with the Microsoft Azure logo and the text 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with a blue header 'User Sign-In' and several menu items: 'Welcome', 'Express Settings', 'Required Components', 'Connect to Azure AD', 'Sync', 'Connect Directories', 'Azure AD sign-in', 'Domain/OU Filtering', 'Identifying users', 'Filtering', 'Optional Features', and 'Configure'. The main content area is titled 'User sign-in' and contains the following options:

- 'Select the Sign On method.' with a help icon (?). Below it are five radio button options:
 - ☐ Password Hash Synchronization ?
 - ☐ Pass-through authentication ?
 - ☐ Federation with AD FS ?
 - ☐ Federation with PingFederate ?
 - ☒ Do not configure ?
- 'Select this option to enable single sign-on for your corporate desktop users:' with a help icon (?). Below it is a checkbox option:
 - ☐ Enable single sign-on ?

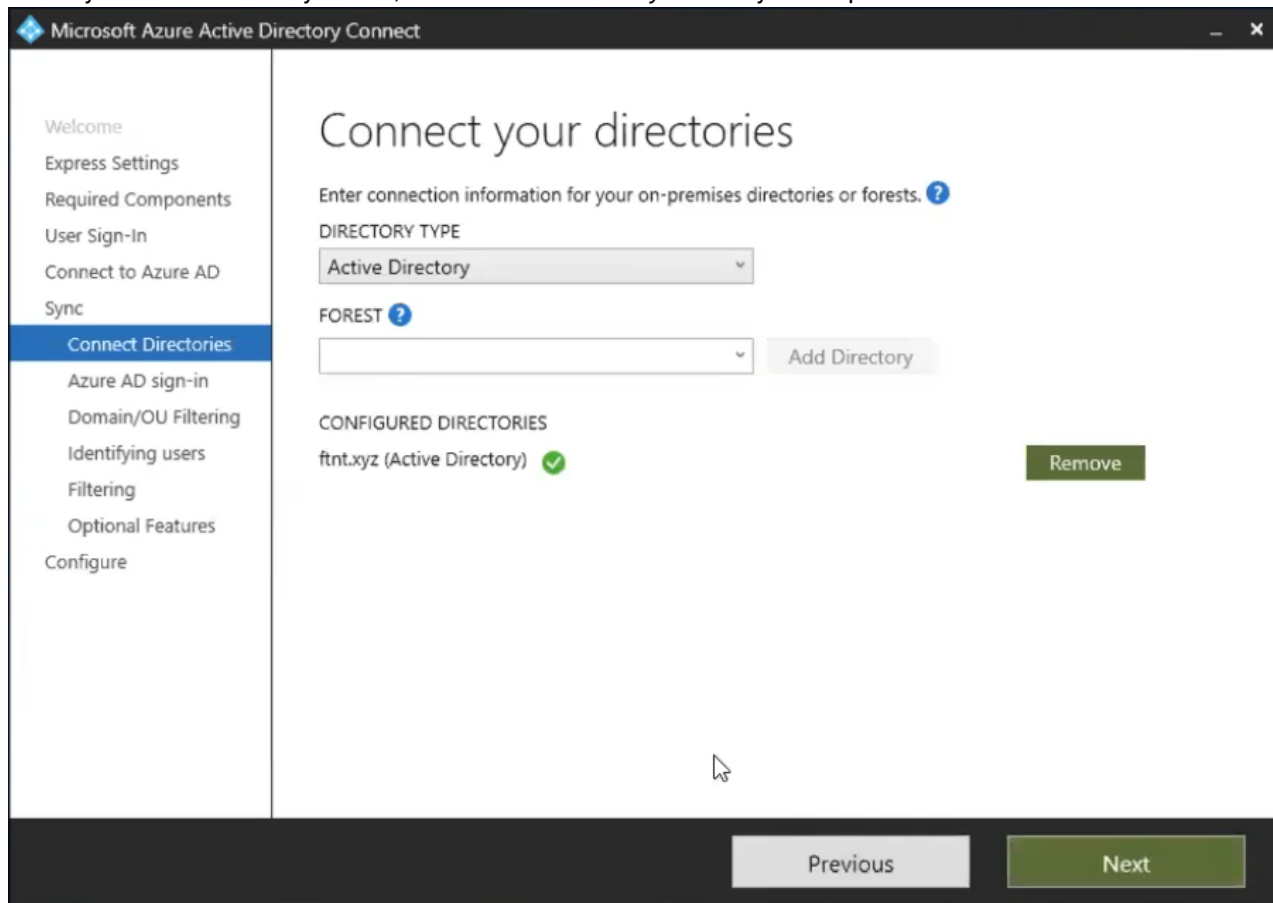
At the bottom right of the window are two buttons: 'Previous' (disabled) and 'Next' (active).

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



The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar reads 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with the following items: 'Welcome', 'Express Settings', 'Required Components', 'User Sign-In', 'Connect to Azure AD' (highlighted in blue), 'Sync', 'Connect Directories', 'Azure AD sign-in', 'Domain/OU Filtering', 'Identifying users', 'Filtering', 'Optional Features', and 'Configure'. The main content area is titled 'Connect to Azure AD' and contains the instruction 'Enter your Azure AD global administrator credentials.' with a help icon. Below this are two input fields: 'USERNAME' containing 'username@contoso.onmicrosoft.com' and 'PASSWORD' which is empty. At the bottom right are two buttons: 'Previous' and 'Next'.

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



The screenshot shows the 'Microsoft Azure Active Directory Connect' window. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, **Connect Directories** (highlighted), Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, and Configure. The main content area is titled 'Connect your directories' and includes the instruction 'Enter connection information for your on-premises directories or forests. ?'. Below this, there are two dropdown menus: 'DIRECTORY TYPE' (set to 'Active Directory') and 'FOREST ?' (empty). An 'Add Directory' button is to the right of the 'FOREST' dropdown. Under the 'CONFIGURED DIRECTORIES' section, 'fnt.xyz (Active Directory)' is listed with a green checkmark, and a 'Remove' button is to its right. At the bottom of the window, there are 'Previous' and 'Next' buttons.

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

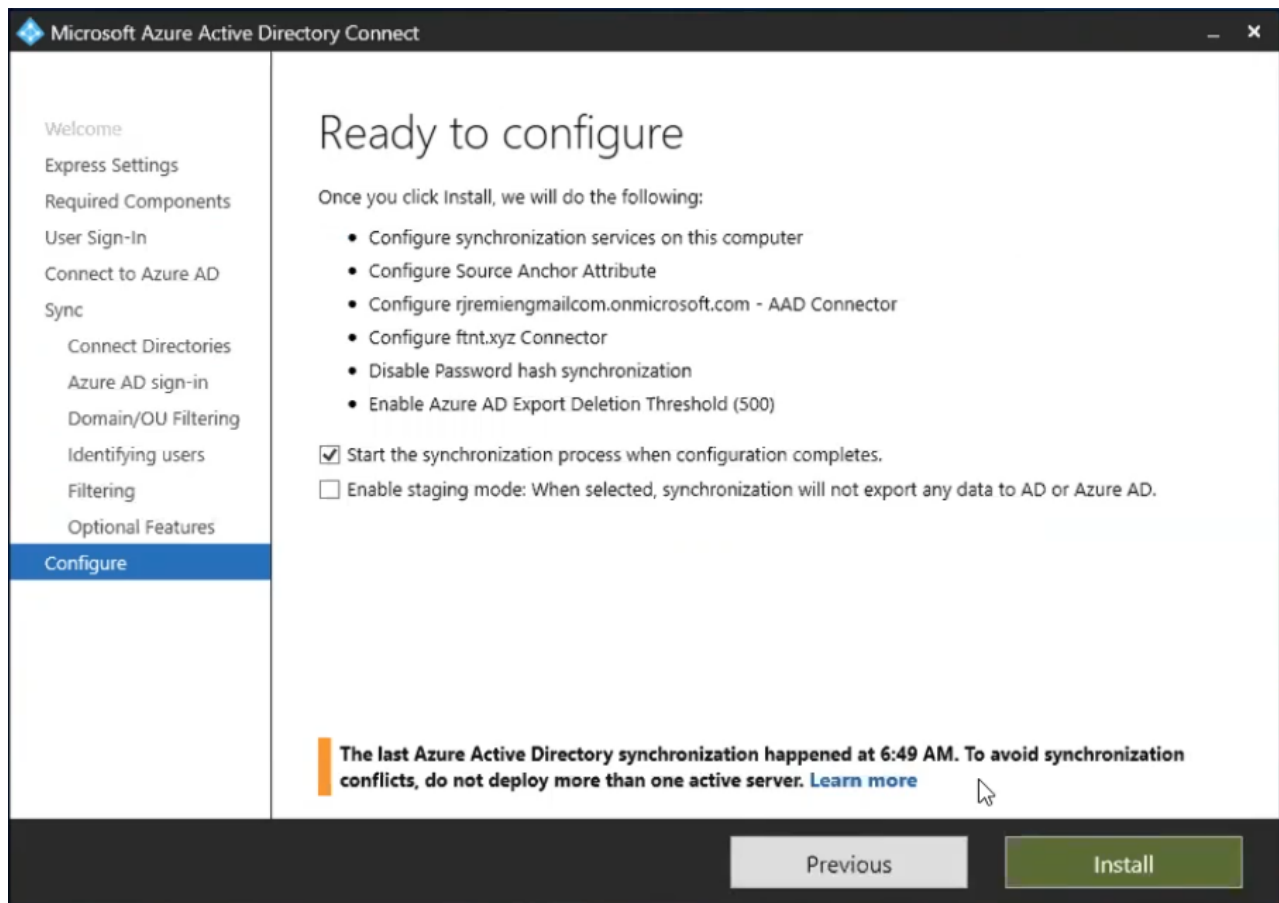
Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME ?

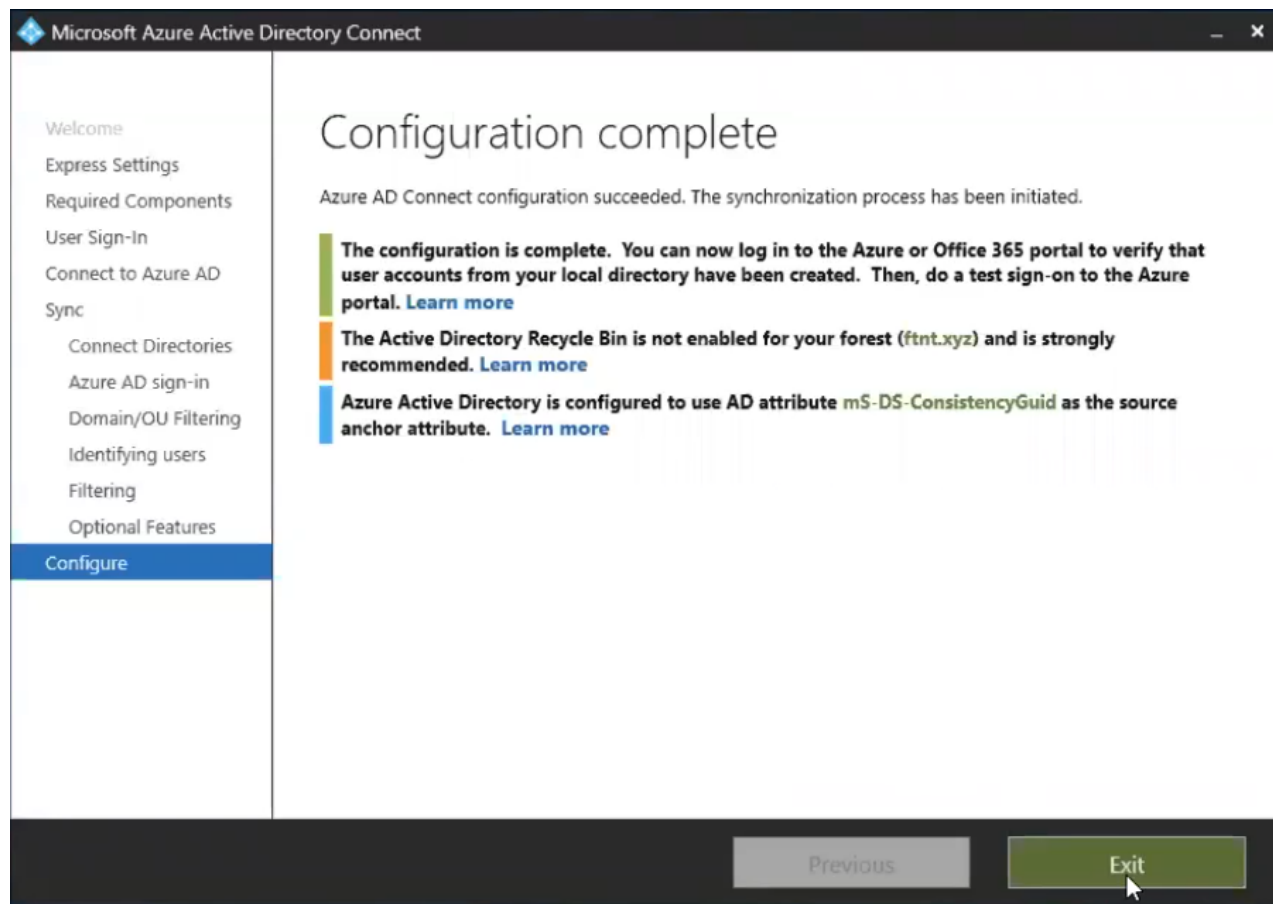
userPrincipalName

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.

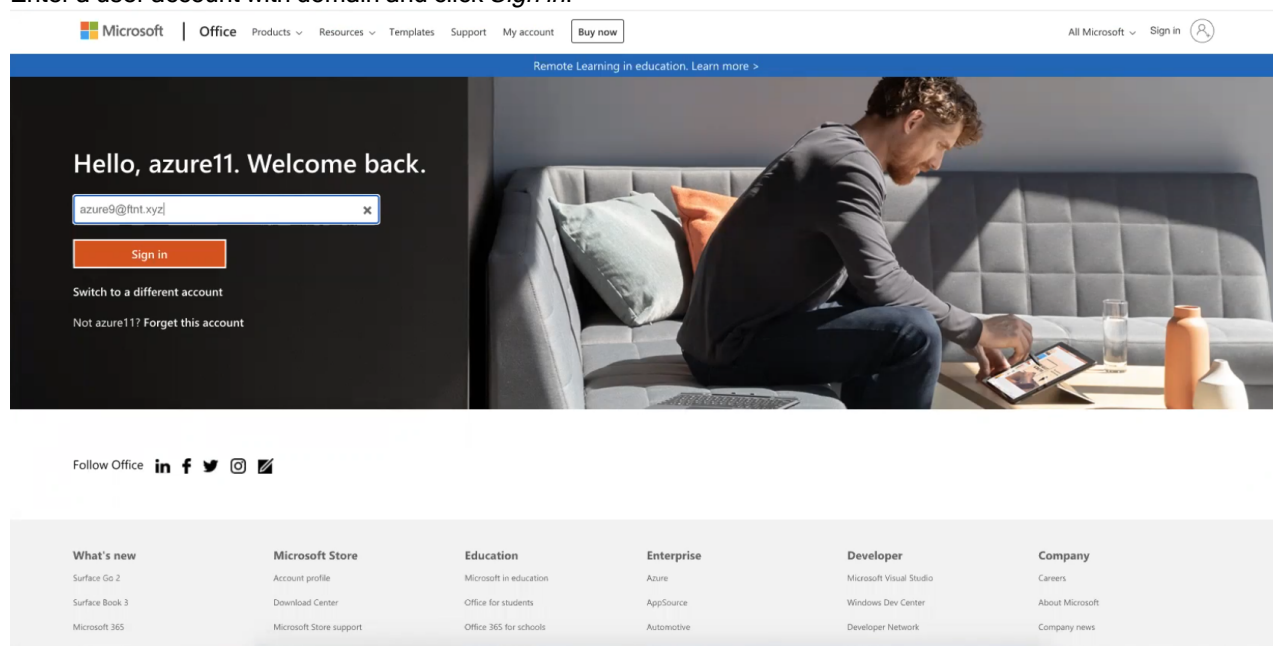


Results

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:

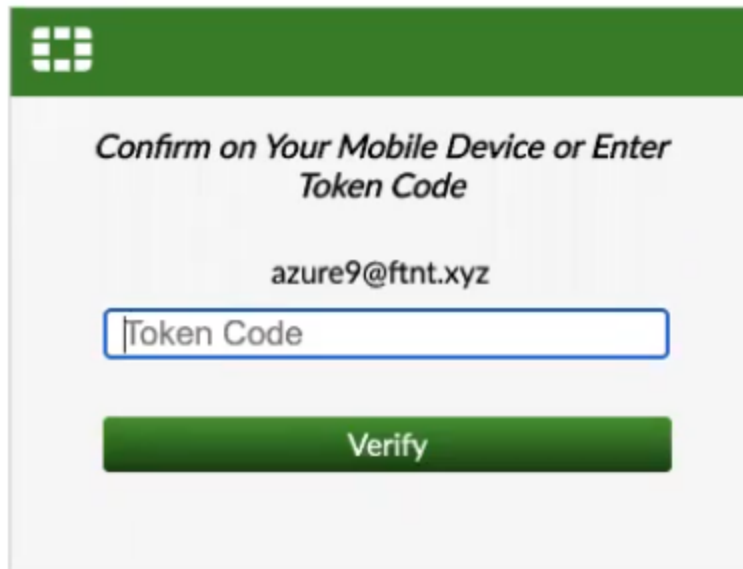
1. Navigate to Office 365 and click *Sign in* or *Switch to a different account*.
2. Enter a user account with domain and click *Sign in*.



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

A screenshot of the FortiAuthenticator login page. It has a green header with a white grid icon. The main area is light gray and contains a 'Username' input field, a 'Password' input field, and a green 'Login' button. Below the button, there is a link that says 'Or Sign in using a cloud server'.

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



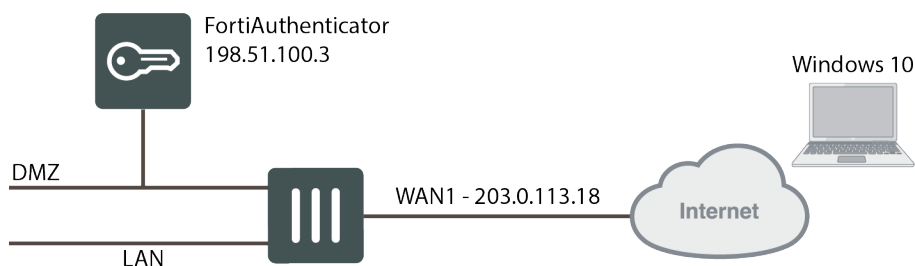
Not azure9@ftnt.xyz? [Sign in as a different user](#)

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

FortiGate SSL VPN with FortiAuthenticator as the IdP proxy for Azure

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

This configuration uses the following topology:



To configure FortiAuthenticator as the IdP proxy for Azure:

1. [Configuring Azure on page 223](#)
2. [Configuring FortiAuthenticator on page 226](#)
3. [Configuring FortiGate on page 230](#)
4. [Results on page 232](#)



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

Configuring Azure

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

Validation passed.

* Basics * Configuration **Review + create**

Summary

Basics

Directory type	Azure Active Directory
----------------	------------------------

Configuration

Organization name	MyDomainHere
Initial domain name	MyDomainHere.onmicrosoft.com
Country/Region	United States
Datacenter location	United States

Create < Previous Next >

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

Create your own application

What's the name of your app?

Azure_fac_as_idproxy

What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
☐ Register an application you're working on to integrate with Azure AD
☒ Integrate any other application you don't find in the gallery

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

to match your FortiAuthenticator's configuration.

Basic SAML Configuration

Identifier (Entity ID)

https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idp
proxy/metadata

Reply URL (Assertion Consumer Service URL)

https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idp
proxy/saml/?acs

Sign on URL

https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idp
proxy/login/

Relay State

Optional

Logout Url

https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_idp
proxy/saml/?sls

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

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

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

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

Additional claims

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

Group Claims

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

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

☐ None
 ☒ All groups
 ☐ Security groups
 ☐ Directory roles
 ☐ Groups assigned to the application

Source attribute *

Group ID

Advanced options

☐ Customize the name of the group claim

Name (required)

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

SAML Signing Certificate

Status

Active

Thumbprint

9714E28E4C0F75BA38E8E38C2878DEEA6B274E

Expiration

6/15/2023, 4:37:22 PM

Notification Email

facmills@fortinet-us.com

App Federation Metadata Url

https://login.microsoftonline.com/07368711-a8...

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

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

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Users and groups

Single sign-on

« + Add user Edit Remove Update Credentials Columns Got feedback?

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

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

Display Name	Object Type
No application assignments found	

FortiAuthenticator 6.5.0 Cookbook
Fortinet Inc.

224

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

saml-fac-as-idproxy | Properties
Enterprise Application

« Save Discard Delete Got feedback?

Overview

- Deployment Plan
- Diagnose and solve problems

Manage

- Properties**
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins

Enabled for users to sign-in? ☒ Yes ☐ No

Name ✓

Homepage URL

Logo

User access URL

Application ID ✓

Object ID

Terms of Service URL

Privacy Statement URL

Reply URL

User assignment required? ☒ Yes ☐ No

Visible to users? ☒ Yes ☐ No

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

Home > cselatam | Roles and administrators >

Directory readers | Assignments
All roles

« + Add assignments X Remove assignments Refresh Manage in PIM Got feedback?

Search Type

Name Username

No role assignments found

Add assignments

Search

saml-fac-as-idproxy
7429d49e-b802-7429d49e-b802-7429d49e-b802
Selected

Selected items

saml-fac-as-idproxy
7429d49e-b802-7429d49e-b802-7429d49e-b802 Remove

Add

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

Home > cselatam | App registrations >

saml-fac-as-idproxy | Certificates & secrets

Search (Cmd+F)

Add a client secret

Description

Expires

- ☒ In 1 year
- ☐ In 2 years
- ☐ Never

Add Cancel

Client secrets

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

+ New client secret



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

Configuring FortiAuthenticator

Configure the remote servers

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

To configure the remote OAuth server:

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

Create New Remote OAuth Server

Name:

OAuth source:

Client ID:

Client Key:

3. Click *OK*.

To configure the remote SAML server:

1. Go to *Authentication > Remote Auth. Servers > SAML*, and click *Create New*.
2. Under *Remote SAML Server*, configure the following:
 - **Name:** Enter a name for the server. This name must match the server name configured in Azure. In this example, the server name is *Azure_fac_as_idpproxy*.
 - **Type:** *Proxy*.
 - **Entity ID:** Select the Azure IdP option.
 - **Import IdP metadata/certificate:** Import the certificate that you previously exported from Azure.
 - **IdP entity ID:** Enter the *Azure AD Identifier* from your Azure configuration.
 - **IdP single sign-on URL:** Enter the *Login URL* from your Azure configuration.
3. Under *Single Logout*, configure the following:
 - **Enable SAML single logout:** Optionally, you can enable this setting to enable SAML single logout.
 - **IdP single logout URL:** Enter the *Logout URL* from your Azure configuration.
4. Under *Username*, configure the following:
 - **Obtain username from:** Select *Text SAML assertion* and use the configured username claim URL from your Azure configuration.

5. In *Group Membership*, configure the following:

- **Obtain group membership from:** Select *Cloud* and choose your remote OAuth server. Group membership of a particular user will be retrieved dynamically through OAuth upon authentication.

Edit Remote SAML Server

Name:

Description:

Device FQDN:

Type: ☐ FSSO ☒ Proxy

URL Nomenclature: ☒ Individualize ☐ Legacy

Portal URL:

Entity ID:

ACS (login) URL:

IdP entity ID:

IdP single sign-on URL:

IdP certificate fingerprint:

Fingerprint algorithm:

Authentication context:

☐ Enable IdP-initiated assertion response

☐ Sign SAML requests with a local certificate

Single Logout

☒ Enable SAML single logout

SLS (logout) URL:

IdP single logout URL:

Username

Obtain username from: ☐ Subject NameID SAML assertion ☒ Text SAML assertion

Group Membership

Obtain group membership from: ☐ SAML assertions ☐ LDAP lookup ☒ Cloud

OAuth server:

Groups field:

☐ Implicit group membership

6. Click *OK*.

Configure the SAML IdP settings on FortiAuthenticator

To create the Azure realm:

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

Create New Realm

Name:

User source:

3. Click *OK*.

To enable SAML IdP on FortiAuthenticator:

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

Edit SAML Identity Provider Settings

☒ Enable SAML Identity Provider portal

Device FQDN: fac.fortilab.local

Server address: fac.fortilab.local

IdP-initiated login URL: https://fac.fortilab.local/saml-idp/portal/

Username input format:

- ☒ username@realm
- ☐ realm\username
- ☐ realm/username

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

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	azurecse Azure_fac_as_idpproxy	☐	☐ Filter: ☐ Filter local users:	
+ Add a realm				

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: fac.fortilab.local | CN=fac.fortilab.local

☐ Get nested groups for user

OK

- 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:

- Go to *Authentication > SAML IdP > Service Providers*, and click *Create New*.
- 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.
- Under *Assertion Attributes*, configure the following:
 - Subject NameID:** *Remote SAML Server > Subject NameID*.
 - Format:** *urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified*.
- 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 231](#).
 - Attribute 1: SAML attribute: *groups*, User attribute: *SAML Group membership*.
 - Attribute 2: SAML attribute: *username*, User attribute: *SAML Username*.

5. Click **Save**.

Edit SAML Service Provider

IdP address: fac.fortilab.local
SP name: fgt1sslvn
IdP prefix: fgt1sslvn [Generate prefix](#)
Server certificate: Use default setting in SAML IdP General page
IdP entity id: http://fac.fortilab.local/saml-idp/fgt1sslvn/metadata/ [🔗](#)
IdP single sign-on URL: https://fac.fortilab.local/saml-idp/fgt1sslvn/login/ [🔗](#)
IdP single logout URL: https://fac.fortilab.local/saml-idp/fgt1sslvn/logout/ [🔗](#)
☐ Support IdP-initiated assertion response
☐ Participate in single logout

SP Metadata

[Import SP metadata](#)
SP entity ID:
SP ACS (login) URL: [Alternative ACS URLs](#)
SP SLS (logout) URL:
☐ SAML request must be signed by SP

Authentication

Authentication method:
☐ Mandatory two-factor authentication
☒ Verify all configured authentication factors
☐ Password-only authentication
☐ Token-only authentication
☐ Bypass FortiToken authentication when user is from a trusted subnet [Configure subnets](#)
Client application name for FortiToken Mobile push notification:

Assertion Attributes

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

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

[Create New Assertion](#)



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

To update the SAML replacement message:

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

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

Name	Description	Modified
SAML IdP		
Login Page	HTML page for SAML IdP user login	✓
Token Login Page	HTML page for SAML IdP two factor authentication	✗
SAML IdP Login Success Page	HTML page presented when user is successfully authenticated	✗
SAML IdP Request Expired Page	HTML page presented when SAML assertion request is expired	✗

Save

Restore Default

Toggle Tag List

idp-server

idp-server-and-proxy

idp-proxy

Please enter correct credentials.

Example message

Redirecting to remote identity provider in 3 seconds.

If you were not redirected click here

```
width: 30px;
height: 30px;
}
#header {
margin-left: -40px;
margin-right: -40px;
background: #008b10;
padding: 5px 10px;
}
</style>
</head>
<body>
<div id="login_wrapper">
<div id="login">
<div id="header" class="title logo">

</div>
<!-- All the [proxy_portal_url] in this page should be replaced with desirable remote
saml server proxy URL. In order to find it, go to the remote saml server
in [Authentication] -> [Remote Auth. Servers] -> [SAML] select the desirable server and then
click show IDP urls. Replace [proxy_portal_url] with the Portal URL -->
</div>
<div class="login_msg_bar">
<p class="error">{::errors}</p>
{::msgs}
</div>
<div id="redir_text">
<p>Redirecting to remote identity provider in 3 seconds.</p>
<p>If you were not redirected click <a href="https://fac.fortilab.local/saml-idp/proxy/Azure_fac_as_id">
</div>
</div>
<script>
if ( {::errors} ) == '' && {::msgs} == '' {
var timer = setTimeout(function() {
window.location='[[proxy_portal_url]]';
}, 3000);
} else {
var redirObj=document.getElementById("redir_text");
redirObj.innerHTML=<p>to login click <a href="[[proxy_portal_url]]">here</a></p>
}
</script>
<body>
</html>
</div>

```

3. Click **Save**.

Configure FortiToken

To include tokens in a user's authentication:

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

Configuring FortiGate

Import the certificate

To import the FortiAuthenticator IdP certificate:

- Go to *System > Certificates*, and click *Import > Remote Certificate*.
- Click *Upload* and select your FortiAuthenticator IdP certificate.

3. Click *OK*.

FortiGate will choose a name by default. You can rename the certificate for easier management with the following CLI commands:

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

Configure the SAML user

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

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

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

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

To configure a SAML user:

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

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



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

See [To add FortiGate as a SAML service provider: on page 228](#)



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 227](#).

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

To configure a SAML group:

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

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

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

To increase the remote authentication timeout:

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

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

Configure the SSL VPN

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

To add a portal to your SSL VPN:

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

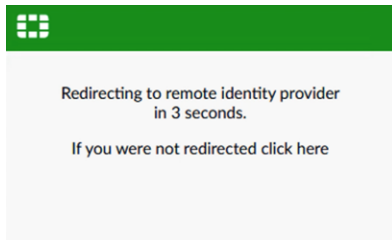
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
SSLVPN to LAN1	samlproxy-sslvpn	lan1_net	always	ALL	ACCEPT	Enabled	No-Inspection	All	0 B

For more information on configuring SSL VPN on FortiGate, see the [FortiGate Administration Guide](#).

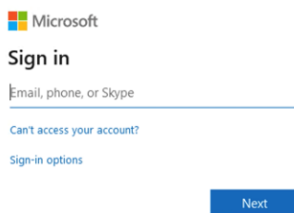
Results

To sign in to your SSL VPN:

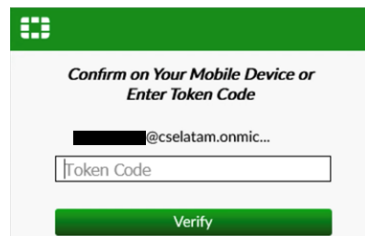
1. Once the user tries to connect to the SSL VPN web portal, FortiGate will redirect the user to FortiAuthenticator.



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

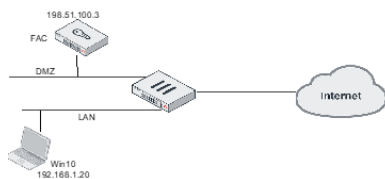


3. After entering their credentials, if the user has a token assigned they will be requested to enter it for two factor authentication.



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

SAML FSSO with FortiAuthenticator and Microsoft Azure AD



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

To configure SAML FSSO with FortiAuthenticator and Microsoft Azure AD:

1. Microsoft Azure related configurations:
 - a. [Creating a tenant in Azure Portal on page 234.](#)
 - b. [Creating an enterprise application in Azure Portal on page 235.](#)

- c. [Setting up single sign-on for an enterprise application on page 236](#)
 - i. [Adding a user group SAML attribute to the enterprise application on page 238.](#)
 - ii. [Adding users to an enterprise application on page 238.](#)
 - d. [Adding the enterprise application as an assignment on page 239.](#)
 - e. [Registering the enterprise application with Microsoft identity platform and generating authentication key on page 239.](#)
2. FortiAuthenticator related configurations:
 - a. [Creating a remote OAuth server with Azure application ID and authentication key on page 240.](#)
 - b. [Creating a remote SAML server on page 240.](#)
 - c. [Setting up SAML SSO in FortiAuthenticator on page 241.](#)
3. FortiGate related configurations:
 - a. [Adding an FSSO agent on page 242.](#)
 - 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 243.](#)
 - d. [Creating an exempt policy to allow users to access the captive portal on page 244.](#)
4. [Results on page 244.](#)

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.

The screenshot shows the Azure Active Directory Overview page. The left sidebar contains navigation links for Overview, Preview features, Diagnose and solve problems, and Manage. The main content area displays basic information about the Default Directory, including the number of users (1,863), groups (42), applications (911), and devices (19). It also displays alerts, such as the upcoming TLS 1.0, 1.1, and 3DES deprecation, and a 'My feed' section with a secure score for identity (26.53%) and Azure AD Connect status.

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

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

Home > Default Directory > Switch tenant >

Create a tenant ...

Azure Active Directory

* Basics * Configuration Review + create

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

Tenant type

Select a tenant type *

☒ Azure Active Directory

☐ Azure Active Directory (B2C)

[Help me choose...](#)

[Review + create](#) < Previous Next: Configuration >

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

Home > Default Directory > Switch tenant >

Create a tenant ...

Azure Active Directory

* Basics * Configuration Review + create

Directory details

Configure your new directory

Organization name *

MyDomainHere

Initial domain name *

MyDomainHere

Country/Region

United States

Datacenter location - United States

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

[Review + create](#) < Previous Next: Review + create >

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*.

Home > Enterprise applications

Enterprise applications | All applications ...

Default Directory - Azure Active Directory

+ New application Columns Preview features Got feedback?

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

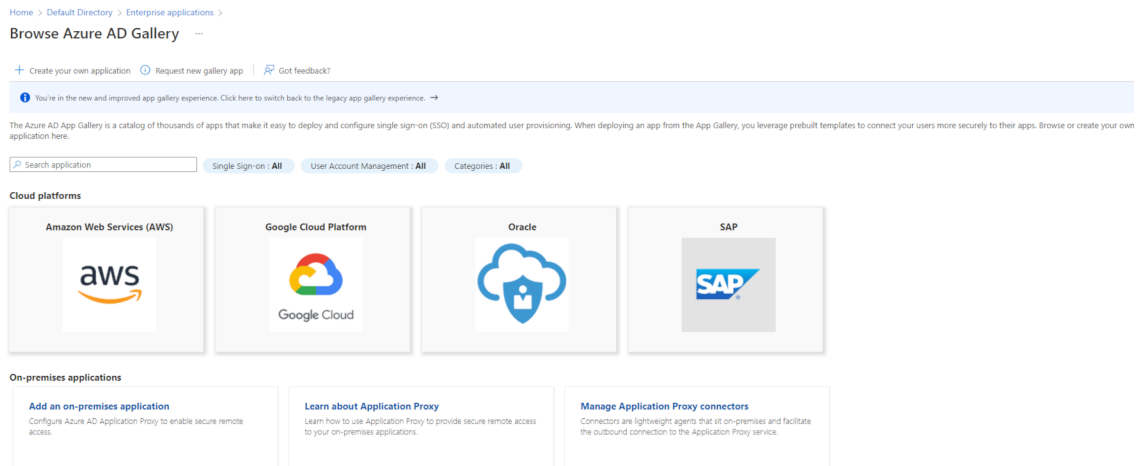
View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their identity Provider.

Application type Applications status Application visibility Apply Reset

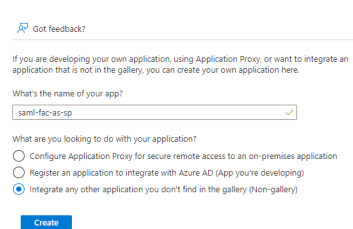
First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID	Application ID
APAC-TU-08-API-APP	https://localhost/APAC-TU-08-API-APP	72252649-32b0-4ce0-b236-70638ea2d093	e3a38a98-fa2a-4b6f-9a54-a8748cd0fb33
asp-fgt	https://forti.io/aspfgt	bc98c977-3c5f-49cd-963b-edd554efa7e0	59f08e75-9b22-4226-acd4-dc3ed3ef1fc
azure.github.io	http://azure.github.io	2fb1db9c-5554-4a4f-b2cc-b990943fda9	fb6c7a71-256b-454a-b2f2-12162630e6a
AzureSDNConnector	http://AzureSDNConnector	a51449b9-1686-41e4-afcc-98ec2b4162ca	f0c49805-f260-4c93-8b11-03f28262d29d
checkpoint	https://localhost/vsec-controller	456f751e-90c2-449d-8287-95618f5e940	99abc472-ad3b-49fd-9c0b-b95b3e74b041
CloudynAzureCollector	https://azureaccountcloudyn.microsoft.com/cloudynazurecollector	15efb372-ed86-46a6-9603-a847639df1e2	83e638ef-7885-479f-bb6b-9150acc0b3d
dmurAADApp	http://dmurAADApp	51f3d077-b646-4d8b-8b5a-5d2c4d6d2be7	afa3b281-08f2-4e8f-9387-e52807673324
fgbanew	https://www.fortinet.com	0480837f-2931-4482-6c08-1fe732eca8b0	ab65a6fa-810f-4362-93b1-5133080427e
FGT	https://wiki.fortinet.fr	af9e953c-3680-465d-a31f-0a838765319e	7d6ca80-2a71-4b0c-8021-6e685799b87
fgtha	http://localhost	806a1967-f02f-43a3-9c27-fac1dc1bf243	483e78ce-0ad5-4bdc-befc-be5b6332d89
FortiCASB	https://www.forticab.com	37f9eac9-cfa5-4548-9ae5-42202d3c8afb	6ef19c36-5655-4f1d-9e7f-e3ca381bd426
Fortigate	http://www.fortigate.com	9f09088-aa82-4b46-99c9-3f5eacdcf3c6	4b7ad08b-2143-475a-90cd-d76158256917
FortiGate-Failover	https://www.fortinet.com	696db64c-9721-402f-9181-e215d544ad2a	b36d7492-8e58-45d5-988a-f15955a4e9d7
FortigateVM	https://13.78.51.154/	855db7cf-873b-41c3-abd1-6eab23bd633	11d87131-495d-4525-a076-baacbd77b4d5
fsaAPI		5edeadd1-223b-46a1-aaa2-527347d6329	104e3e8b-a2a8-49fc-be88-b7f8b596880
fsaminint	https://192.168.56.51/fsaminint	c8e991a-3a4f-4cfd-99d4-d6b039fe118	7891ed5b-7d5e-4d6b-b41c-131659e4923

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 235](#).

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:

- In *Identifier (Entity ID)*, enter the SP entity ID.
- In *Reply URL (Assertion Consumer Service URL)*, enter the URL where the application receives the authentication token.

- c. In *Sign on URL*, enter the URL for the sign-in page for the application.
- d. In *Relay State*, enter the URL to which the user is redirected to by the SP after a successful assertion response.
- e. In *Logout Url*, enter the URL used to send the SAML logout response back to the application.
- f. Click **Save**.

Basic SAML Configuration Edit	
Identifier (Entity ID)	https://fac.fortilab.local/local/saml-sp/Azure_fac_as_sp/metadata
Reply URL (Assertion Consumer Service URL)	https://fac.fortilab.local/local/saml-sp/Azure_fac_as_sp/saml/facs
Sign on URL	https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/login
Relay State	Optional
Logout URL	https://fac.fortilab.local/saml-sp/Azure_fac_as_sp/logout

See [Adding a user group SAML attribute to the enterprise application on page 238](#) and [Adding users to an enterprise application on page 238](#).

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 236](#), 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.

Attributes & Claims

+ Add new claim + Add a group claim Columns Get feedback?	
Required claim	
Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname (nameid-for...
Additional claims	
Claim name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups (All) ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.email ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***

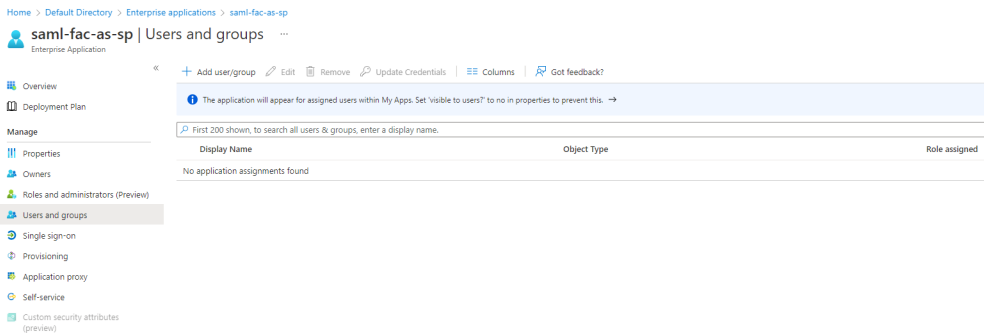


In the *SAML Signing Certificate* pane, download the certificate file (base64) needed to configure the [remote SAML server](#).

Adding users to an enterprise application

To add users:

1. In the *SAML-based Sign-on* window that opens after [step 4 in Setting up single sign-on for an enterprise application on page 236](#), 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 238](#).
5. In *Client Key*, enter the authentication key created in [Registering the enterprise application with Microsoft identity platform and generating authentication key on page 239](#).
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 240](#)
11. Click *OK*.

The following shows the relation between the Microsoft Azure AD 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 240](#).

3. In the *Domain Membership* pane, enable *Get SSO domain name from*, and select *Username prefix/suffix* to obtain the domain name specified in the username.
4. Click *OK* to create the new SAML SP portal.

To enable FSSO for FortiGate and define a password:

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

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

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

Adding an FSSO agent

To add an FSSO agent:

1. Go to *Security Fabric > External Connectors* and select *Create New*.
The *New External Connector* window opens.
2. In the *Endpoint/Identity* pane, select *FSSO Agent on Windows AD*.
3. In the *Connector Settings* pane:
 - a. Enter a name for the FSSO agent.
 - b. In *Primary FSSO agent*, enter the FortiAuthenticator SP IP address, and enter a password.



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

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

Configuring an interface to use an external captive portal

To configure an interface:

1. Go to *Network > Interfaces*.
2. Select *Create New > Interface*.
The *New Interface* window opens.
3. Enter a name for the interface. Optionally, enter an alias.

4. In *Type*, select *802.3ad Aggregate*.
5. In the *Role* dropdown, select *LAN*.
6. In the *Address* pane:
 - a. In *Addressing mode*, select *Manual*.
 - b. In *IP/Netmask*, enter an IP address/netmask for the interface.
 - c. In *IPv6 addressing mode*, select *Manual*.
 - d. Disable *Create address object matching subnet*.
7. In the *Network* pane:
 - a. Enable *Device detection*.
 - b. Enable *Security mode*, and from the dropdown, select *Captive Portal*.
 - c. In *Authentication portal*, select *External*, and enter the captive portal URL.



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

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

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

To configure a policy:

1. Go to *Policy & Objects > Firewall Policy* and select *Create New*.
2. Enter a name for the policy.
3. In *Incoming Interface*, select the interface created to [use an external captive portal](#).
4. In *Outgoing Interface*, select the interface for virtual WAN.
5. In *Source*:
 - a. Select *+* to open the *Select Entries* window.
 - b. In *Address*, search and select *all*.
 - c. Select *Close*.
6. In *Destination*:
 - a. Select *+* to open the *Select Entries* window.
 - b. In *Internet Service*, search and select *Microsoft-Azure*.
 - c. Select *Close*.
7. In *Advanced* pane, enable *Exempt Captive Portal* to exempt this policy from the captive portal.



To make the *Advanced* pane visible:

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

8. Click *OK*.

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

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

To create an exempt policy:

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



To make the *Advanced* pane visible:

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

10. Click *OK*.

Results

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

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

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

The configuration outlined in this guide assumes that you have already configured your FortiAuthenticator with FortiToken Cloud, and that ADFS is set up as a SAML IdP.

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

1. [Configure FortiAuthenticator as an SP in ADFS on page 245](#)
2. [Configure the remote SAML server on FortiAuthenticator on page 245](#)
3. [Configure SAML settings on FortiAuthenticator on page 246](#)
4. [Configure two-factor authentication on FortiAuthenticator on page 248](#)
5. [Configure FortiAuthenticator replacement messages on page 249](#)
6. [Results on page 249](#)

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.

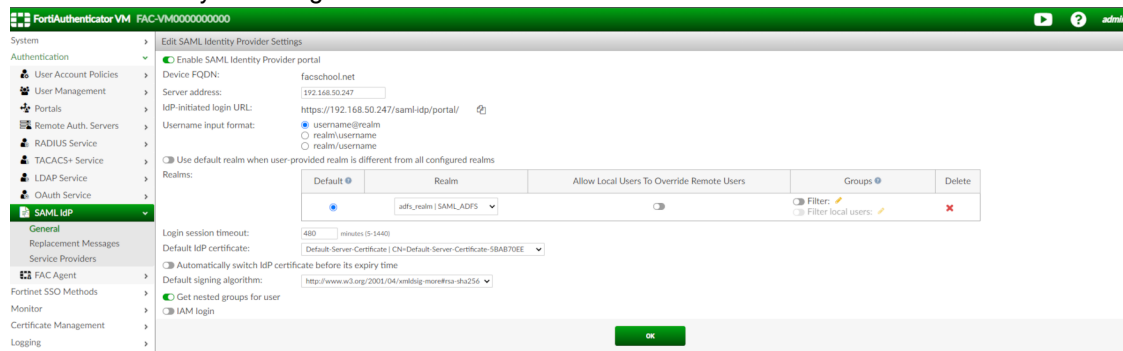
To configure the ADFS realm:

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.

The screenshot displays the FortiAuthenticator VM configuration window for a SAML Service Provider (SP). The left sidebar shows the navigation menu with categories like System, Authentication, and SAML SP. The main panel is titled 'Edit SAML Service Provider' and contains several sections:

- SP Metadata:** Includes fields for SP entity ID, SP ACS (login) URL, and SP SLS (logout) URL. There is an 'Import SP metadata' button.
- Authentication:** Includes an 'Authentication method' section with radio buttons for 'Mandatory password and OTP', 'All configured password and OTP factors' (selected), 'Password-only', 'OTP-only', and 'FIDO-only'. There is also an 'Adaptive Authentication' section with a 'Configure subnets' button.
- Assertion Attribute Configuration:** Includes a 'Subject NameID' dropdown menu and a 'Format' dropdown menu.
- Assertion Attributes:** Includes a table for 'Assertion attribute' with columns for 'SAML attribute', 'User attribute', and 'Custom field'. The 'SAML attribute' is set to 'IDPEmail'.

At the bottom of the window, there are buttons for 'Import SP metadata', 'OK', and 'Cancel'.

Configure two-factor authentication on FortiAuthenticator

To configure a remote user sync rule:

1. Go to *Authentication > User Management > Remote User Sync Rules*, choose *SAML* and then click *Create New*.
2. Configure the following settings:
 - a. **Name:** Enter a name for the sync rule (e.g. SAML Users).
 - b. **Remote SAML server:** Select the previously configured remote SAML server.
3. Configure the token-based sync priority settings under *Synchronization Attributes* by enabling and ordering the authentication sync priorities.
This example scenario uses FortiToken Cloud for two-factor authentication, so the priority is *FortiToken Cloud* followed by *None (users are synced explicitly with no token-based authentication)*.
4. Select or create a user group to associate users with from the dropdown menu.
5. In *SAML User Mapping Attributes*, set the *Username* field to *sAMAccountName*.
6. The remaining settings can be configured to your preference or left in their default state.
7. Click *OK* to save your changes when completed.

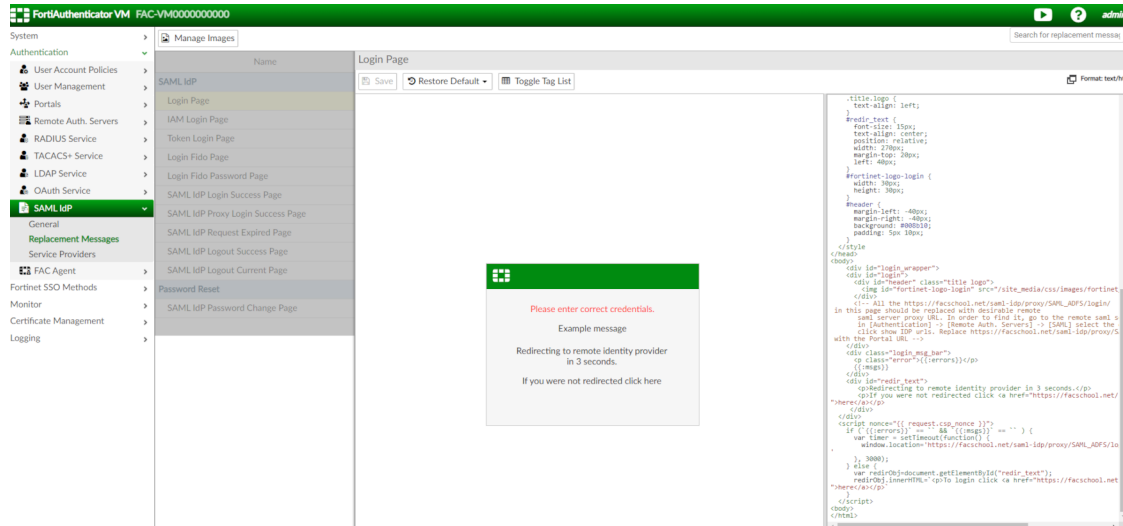
To configure remote users with two-factor authentication:

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

Configure FortiAuthenticator replacement messages

To configure the FortiAuthenticator replacement messages:

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

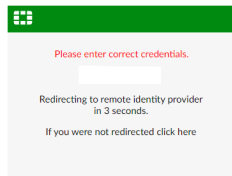


Results

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

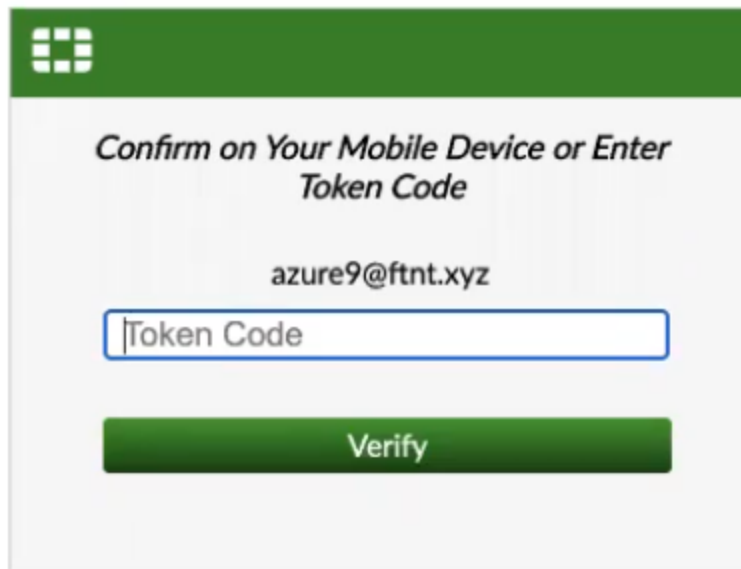
To sign in to Office 365 using FortiAuthenticator with two-factor authentication:

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.



Not azure9@ftnt.xyz? [Sign in as a different user](#)

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

SSL VPN SAML authentication using FortiAuthenticator with OneLogin as SAML IdP

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



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

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

In this example:

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



User validation is done using OneLogin user database.

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



VPN user authentication requests are sent to FortiAuthenticator for validation.

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

Prerequisites and scope of the recipe

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

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

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

1. OneLogin related configurations:
 - a. [Creating an OneLogin application on page 252](#)
 - b. [Configuring an application on OneLogin on page 252](#)
 - i. [Configuring application parameters on OneLogin on page 254](#)
 - ii. [Configuring SSO on OneLogin on page 255](#)
 - c. [Granting user access to the application on page 256](#)
2. FortiAuthenticator related configurations:
 - a. [Configuring a remote SAML server on page 257](#)
 - b. [Configuring an OneLogin realm on page 259](#)
 - c. [Creating remote SAML users on page 259](#)
 - d. [Configuring SAML IdP settings on page 260](#)
 - e. [Configuring FortiAuthenticator replacement message on page 261](#)
 - f. [Configuring FortiGate SP settings on FortiAuthenticator on page 261](#)
3. FortiGate related configurations:
 - a. [Uploading SAML IdP certificate to the FortiGate SP on page 263](#)
 - b. [Creating SAML user and server on page 264](#)
 - c. [Mapping SSL VPN authentication portal on page 266](#)
 - d. [Increasing remote authentication timeout using FortiGate CLI on page 267](#)
 - e. [Configuring a policy to allow users access to allowed network resources on page 267](#)

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 252](#), [Configuring application parameters on OneLogin on page 254](#), and [Configuring SSO on OneLogin on page 255](#).

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 252](#), 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 257](#).

The screenshot displays the 'SAML Custom Connector (Advanced)' configuration page in the OneLogin console. The left sidebar contains navigation tabs: Info, Configuration (selected), Parameters, Rules, SSO, Access, Users, Privileges, and Setup. The main content area is titled 'Application details' and contains the following configuration fields:

- RelayState**: Text input field.
- Audience (EntityID)**: Text input field with the value `http://fac.cselab.ca/saml-idp/proxy/OneLogin/metadata/`.
- Recipient**: Text input field.
- ACS (Consumer) URL Validator***: Text input field with the value `*https://fac.cselab.ca/saml-idp/proxy/OneLogin/saml/?acs$`.
- ACS (Consumer) URL***: Text input field with the value `https://fac.cselab.ca/saml-idp/proxy/OneLogin/saml/?acs`.
- Single Logout URL**: Text input field with the value `https://fac.cselab.ca/saml-idp/proxy/OneLogin/saml/?sls`.
- Login URL**: Text input field with the value `https://fac.cselab.ca/saml-idp/proxy/OneLogin/login/`.
- SAML not valid before**: Text input field with the value `5`.
- SAML not valid on or after**: Text input field with the value `5`.
- SAML initiator**: Dropdown menu with the value `OneLogin`.
- SAML nameID format**: Dropdown menu with the value `Email`.
- SAML issuer type**: Dropdown menu with the value `Specific`.
- SAML signature element**: Dropdown menu with the value `Both`.
- Encrypt assertion**: Checkbox (unchecked).
- SAML encryption method**: Dropdown menu with the value `TRIPLEDES-CBC`.
- Send NameID Format in SLO Request**: Checkbox (unchecked).
- Generate Attribute/Value tag for empty values**: Checkbox (unchecked).
- SAML sessionNotOnOrAfter**: Text input field with the value `1440`.
- Sign SLO Request**: Checkbox (unchecked).
- Sign SLO Response**: Checkbox (unchecked).

Configuring application parameters on OneLogin

To configure an email application parameters on OneLogin:

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

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

New Field

Field name

email

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

Flags

☒ Include in SAML assertion

☐ Multi-value parameter

Cancel Save

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

onelogin Users Applications Devices Authentication Activity Security Settings Developers Getting Started Guide

Applications / SAML Custom Connector (Advanced)

More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Credentials are

☒ Configured by admin

☐ Configured by admins and shared by all users

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

To configure a *MemberOf* application parameter on OneLogin:

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

onelogin Users Applications Devices Authentication Activity Security Settings Developers Getting Started Guide

Applications / SAML Custom Connector (Advanced)

More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Credentials are

☒ Configured by admin

☐ Configured by admins and shared by all users

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

Configuring SSO on OneLogin

To configure SSO on OneLogin:

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

4. Click *Save*.

Clicking *View Details* in *X.509 Certificate* shows the certificate assigned to the application by OneLogin that includes the fingerprint information. Ensure that *SHA fingerprint* is *SHA256*.

Select a format from the dropdown and download the certificate.

The screenshot shows the OneLogin SAML Custom Connector (Advanced) configuration page. The left sidebar contains a navigation menu with options: Info, Configuration, Parameters, Rules, SSO, Access, Users, Privileges, and Setup. The main content area is titled 'Enable SAML2.0' and includes the following sections:

- Sign on method:** SAML2.0
- X.509 Certificate:** Standard Strength Certificate (2048-bit). A 'View Details' link is available.
- SAML Signature Algorithm:** A dropdown menu showing 'SHA-256'.
- Issuer URL:** https://app.onelogin.com/saml/metadata/12094046-5c1e-44f5-812b-d1e8e9d1db2f
- SAML 2.0 Endpoint (HTTP):** https://testfint.onelogin.com/trust/saml2/http-post/12094046-5c1e-44f5-812b-d1e8e9d1db2f
- SLO Endpoint (HTTP):** https://testfint.onelogin.com/trust/saml2/http-redirect/slo/1678744
- Login Hint:** A checkbox 'Enable login hint' is checked. A note states: 'When enabled, the username will auto-populate during login if a login hint is provided.'
- Login Connection Display:** A checkbox 'Disable Login Connection Display' is unchecked. A note states: 'When selected, the login field won't display the app name the user is attempting to access. Example: "Connecting to Salesforce".'
- Assumed Sign-In:** A checkbox 'Allow assumed users to sign into this app' is unchecked. A note states: 'When enabled, admins who assume users can sign into this app with their identity. This setting can only be changed by the account owner. Note that the account owner can also completely disable the assume feature under Account -> Settings.'

Granting user access to the application

To grant user access to the application:

1. Go to *Users > Users*.

The screenshot shows the OneLogin Users page. At the top, there is a search bar and a 'Show filters' link. Below is a table with the following columns: Name, User Information, Last Logged In, and Status.

Name	User Information	Last Logged In	Status
Mark Almond testfint@fortinet.com	Default account owner	Last logged in about 7 hours ago	Active

At the bottom right, there is a 'Results per page' dropdown menu set to 20.

2. Select the desired user from the list.

The *Users* window opens.

3. Go to the *Applications* tab and select *+*.

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



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

Assign new login to *Fortis Almond*

This login will override any apps assigned via roles.

Select application

[Cancel](#) [Continue](#)

5. In the new dialog that appears:
- Ensure that *Allow the user to sign in* is selected.
 - In *NameID value*, enter the user email address.
 - 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 261](#) and [Configuring a policy to allow users access to allowed network resources on page 267](#).

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

Edit FortiAuthenticator Demo login for *Fortis Almond*

☒ Allow the user to sign in
☐ Hide this app in Portal

NameID value

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

group

email

[Reset login \(What's this? \)](#)

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

[Cancel](#) [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 255](#) and [Configuring application parameters on OneLogin on page 254](#).

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 configuration.
 - b. In *IdP single sign-on URL*, enter *SAML 2.0 Endpoint (HTTP)* from the *SSO* tab in OneLogin application configuration.
 - 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 257](#).
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 257](#).

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 *System > Dashboard > Status*.

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

3. Ensure that *Username input format* is set as *username@realm*.
4. In the *Realms* dropdown, select the OneLogin realm configured in [Configuring an OneLogin realm on page 259](#). 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 263](#).
To export the IdP certificate, see [Exporting the IdP certificate](#).
7. Ensure that *Get nested groups for user* is disabled.
8. Click *OK*.

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	onelogin.com OneLogin	☐	☐ Filter: Filter local users:	

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*.

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

3 / 3 server certificates



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

Configuring FortiAuthenticator replacement message

To configure a replacement message:

1. Go to *Authentication > SAML IdP > Replacement Messages*, and click the *Login Page* replacement message.
2. In *Restore Default* dropdown, select *idp-proxy* to automatically redirect users to the IdP proxy login page after 3 seconds.
Alternatively, select *idp-server-and-proxy*, and then select *Or Sign in using a cloud server* to go to the IdP proxy login page.
3. On the right side of the screen, you can edit the replacement message in HTML. Replace all instances of *[proxy_portal_url]* with *Portal URL* in [Configuring a remote SAML server on page 257](#).
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 FortiGate 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 260](#).
 - 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 264](#).
 - b. **SP ACS (login) URL:** Enter the *SP single sign-on URL* from [Creating SAML user and server on page 264](#).
 - c. **SP SLS (logout) URL:** Enter the *SP single logout URL* from [Creating SAML user and server on page 264](#).



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 264](#).

9. Click *OK* to save changes.

Edit SAML Service Provider

IdP address: fac.cselab.ca
 SP name: Onelogin-FortiGate SSO VPN
 IdP prefix: 7ynjdtza10saf1
 IdP entity id: http://fac.cselab.ca/saml-idp/7ynjdtza10saf1/metadata/
 IdP single sign-on URL: https://fac.cselab.ca/saml-idp/7ynjdtza10saf1/login/
 IdP single logout URL: https://fac.cselab.ca/saml-idp/7ynjdtza10saf1/logout/
 Server certificate: FAC_Main | CN=cselab.ca
 IdP signing algorithm: Use default signing algorithm in SAML IdP General page
☐ Support IdP-initiated assertion response
☐ Participate in single logout

SP Metadata

SP entity ID: http://192.168.1.14443/remote/saml/metadata/
 SP ACS (login) URL: https://192.168.1.14443/remote/saml/login/
 SP SLS (logout) URL: https://192.168.1.14443/remote/saml/logout/
☐ SAML request must be signed by SP

Authentication

Authentication method:
☐ Mandatory password and OTP
☒ All configured password and OTP factors
☐ Password-only
☐ OTP-only
☐ FIDO-only
☐ Adaptive Authentication
 Application name for FTM push notification: Onelogin
☐ Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

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

Assertion Attributes

Assertion attribute:
 SAML attribute: group
 User attribute: SAML assertion
 Custom field: group
 Assertion attribute:
 SAML attribute: email
 User attribute: Username
 + Add Assertion Attribute

Debugging Options

Import metadata OK Cancel

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*.

+ Create/Import + Edit Delete View Details Download Search Q						
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 unl...	DigiCert Inc	2022/11/04 16:59:59	Valid	Factory
Remote CA Certificate						
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						
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 264](#).



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 264](#).

Creating SAML user and server

To create a new SAML server:

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



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

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



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

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

See [Configuring FortiGate SP settings on FortiAuthenticator on page 261](#).

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 260](#).
- c. In *Prefix*, enter the *IdP prefix* from [Configuring FortiGate SP settings on FortiAuthenticator on page 261](#).
- d. In the *IdP certificate* dropdown, select the certificate from [Uploading SAML IdP certificate to the FortiGate SP on page 263](#).

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 261](#).

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 SSL VPN authentication portal

To map SSL VPN authentication portal:

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

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



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

- d. Click *OK*.

3. Click *Apply*.

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:

- 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:

- Go to *Policy & Objects > Firewall Policy* and select *Create New*.
- Enter a name for the policy.
- In *Incoming Interface*, select *SSL-VPN tunnel interface (ssl.root)*.
- In *Outgoing Interface*, select a destination interface.
- In *Source*:
 - Select *+* to open the *Selected Entries* window.
 - In *User*, search and select the SAML user group created in [Creating a SAML group](#) and the SSL VPN pool range object.
 - Select *Close*.

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



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

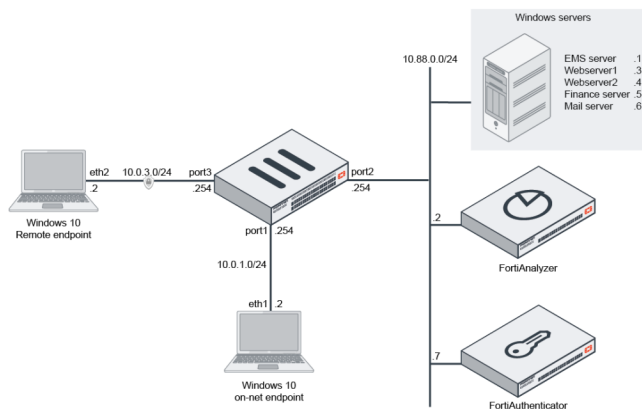
FortiGate SSL VPN with FortiAuthenticator as SAML IdP

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

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

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

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



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

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



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

Assumptions

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

Certificate management

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

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

Configuring the local CA on FortiAuthenticator

To configure a local CA on FortiAuthenticator:

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

To export the created local CA:

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

Generating the certificates on FortiAuthenticator

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

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

6. Click **OK**.

Create New User Certificate

Certificate ID:

Certificate Signing Options

Issuer: (Third party CA)

Certificate authority: (C-CA, ST-BC, L-Burlington, O-Fortinet, OU-technics, CN-Fortinet)

Local User (Optional):

Subject Information

Subject input method: (Field by field)

Name (CN):

Department (OU):

Company (C):

City (L):

State/Province (ST):

Country (C):

Email address:

Key and Signing Options

Validity period: (Set length of time) (Set an expiry date)

Key type:

Key size: (2048) (4096)

Hash algorithm: (SHA-256) (SHA-1)

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

☐ URI:

☐ DNS:

Other Extensions

☐ Add CRL Distribution Points extension (Location: http://fac.ctrademo.com/cert/crl/FortiADInfo_RootCA.crl) (Edit device FQDN)

☐ Add OCSP Responder URL (Location: <http://fac.ctrademo.com/2560>) (Edit device FQDN)

☐ Use certificate for Smart Card logon

To export the user certificate:

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

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

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

Create New Server Certificate

Certificate ID:

Certificate Signing Options

Issuer: (Third party CA)

Certificate authority: (C-CA, ST-BC, L-Burlington, O-Fortinet, OU-technics, CN-Fortinet)

Local User (Optional):

Subject Information

Subject input method: (Field by field)

Name (CN):

Department (OU):

Company (C):

City (L):

State/Province (ST):

Country (C):

Email address:

Key and Signing Options

Validity period: (Set length of time) (Set an expiry date)

Key type:

Key size: (2048) (4096)

Hash algorithm: (SHA-256) (SHA-1)

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

☐ URI:

☐ DNS:

Other Extensions

☐ Add CRL Distribution Points extension (Location: http://fac.ctrademo.com/cert/crl/FortiADInfo_RootCA.crl) (Edit device FQDN)

☐ Add OCSP Responder URL (Location: <http://fac.ctrademo.com/2560>) (Edit device FQDN)

☐ Use certificate for Smart Card logon

[Advanced Options: Key Users](#)

To export the server certificate:

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

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

1. On FortiGate, go to *System > Certificate*, and from the *Create/Import* dropdown, select *Generate CSR*.
2. 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*.

Name	Subject	Comments	Issuer	Expires	Status
F01-SSLVPN	C=CA, ST=BC, L=Burnaby, O=Fortinet, OU=Technology, CN=F01-SSLVPN		Fortinet	2023/12/31 22:58:33	Valid

To import the SAML IdP remote certificate:

1. On FortiGate, go to *System > Certificates*, and from the *Create/Import* dropdown, select *Remote Certificate*.
2. Select *Upload* to locate and upload the .cer remote certificate from your computer.
3. Click *OK*.

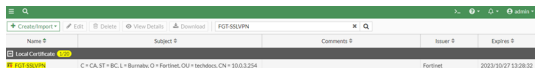
On the certificates list page, the new certificate is now available in *Remote Certificate*.



To import the user certificate for the FortiGate SSL VPN portal

1. On FortiGate, go to *System > Certificates*, and from the *Create/Import* dropdown, select *Certificate*.
2. Select *Import Certificate* to locate the .cer user certificate file from your computer.
3. Click *Create*.

On the certificates list page, the new certificate is now available in *Local Certificate*.



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.

The screenshot shows the 'Create New LDAP Server' configuration page. Fields include: Name (FortiAD), Primary server name/IP (10.88.0.1), Port (389), Base distinguished name (DC=fortiad,DC=info), Bind type (Regular), Username (facadmin@fortiad.com), Password (masked), Server type (Microsoft Active Directory), Query Elements (User object class: person, Username attribute: sAMAccountName, Group object class: group, Obtain group memberships from: User attribute, Group membership attribute: memberOf), Secure Connection (disabled), and Windows Active Directory Domain Authentication (disabled). OK and Cancel buttons are at the bottom.

3. Click *OK*.

To configure a user realm on FortiAuthenticator:

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

To configure user groups on FortiAuthenticator:

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



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

SAML IdP and SP configurations



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

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

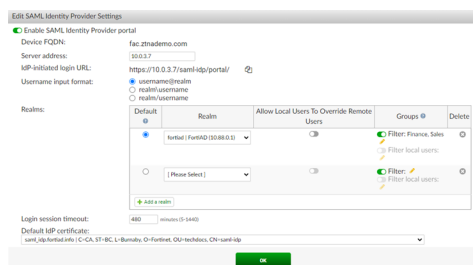
- **FortiAuthenticator (IdP)** - 10.0.3.7:443
- **FortiGate (SP)** - 10.0.3.254:10443 (10443 is used for access related to SSL VPN based on the default listening port for SSL VPN. Change this accordingly when listening on a different port)

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

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

To configure general SAML IdP settings on FortiAuthenticator:

1. Go to *Authentication > SAML IdP > General*.
2. Enable *SAML Identity Provider portal*.
3. Enter the server address. This address must be accessible by the client endpoint.
4. In *Realms*, select *Add a realm* and select the recently created realm from the dropdown.
5. In *Groups*, enable *Filter*, and choose the **Finance** and **Sales** user groups that you recently created.
6. In *Default IdP certificate* dropdown, select the IdP certificate created in *Certificate Management > End Entities > Local Services*. See [Generating a server certificate](#).
7. Click *OK*.



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*.

SAML Service Provider

IP address: 10.0.3.7
 SP name:
 IP profile:
 IP entity id: https://10.0.3.7/saml/idp/fg2/metadata/
 IP single sign on URL: https://10.0.3.7/saml/idp/fg2/signon/
 IP single logout URL: https://10.0.3.7/saml/idp/fg2/signon/
 Server certificate:
 IP signing algorithm:
☐ Support IP-initiated assertion request
☐ Participate in single logout

SP Metadata

SP entity ID:
 SP ACS (Sign) URL:
 SP SLS (Sign) URL:
☐ SAML request must be signed by SP

Authentication

Authentication method:
 ☐ Mandatory password and OTP
☒ All configured password and OTP factors
☐ Password only
☐ OTP only
☐ FIDO only

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

Assertion Attribute Configuration

Subject NameID:

☐ Include real name in subject NameID

Assertion Attributes

Assertion attribute:
 SAML attribute:
 User attribute:
 Assertion attribute:
 SAML attribute:
 User attribute:

Debugging Options

To configure SAML Single Sign-On settings on the FortiGate:

SAML settings can be configured from the GUI, but the default SP URLs must be changed after they are created. Therefore, the following instructions show how to configure the SAML settings from CLI instead.

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

```
config user saml
  edit "fac_saml_idp-sslvpn"
    set cert "saml_sp.fortiad.info"
    set entity-id "http://10.0.3.254:10443/remote/saml/metadata/"
    set single-sign-on-url "https://10.0.3.254:10443/remote/saml/login/"
    set single-logout-url "https://10.0.3.254:10443/remote/saml/logout/"
    set idp-entity-id "http://10.0.3.7/saml-idp/fgt2/metadata/"
    set idp-single-sign-on-url "https://10.0.3.7/saml-idp/fgt2/login/"
    set idp-single-logout-url "https://10.0.3.7/saml-idp/fgt2/logout/"
    set idp-cert "saml_idp.fortiad.info"
    set user-name "username"
    set group-name "group"
    set digest-method sha1
  next
end
```



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

FortiGate user management

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

To configure user groups for Finance and Sales in FortiGate:

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

The screenshot shows the 'Edit User Group' configuration window in FortiGate. The 'Name' field is set to 'Sales' and the 'Type' is 'Firewall'. The 'Members' field is empty with a '+' button. The 'Remote Groups' section has a table with one entry: Remote Server 'fac_saml_idp-sslvpn' and Group Name 'CN=Sales,CN=Users,DC=fortiad,DC=info'. The 'Add' button is highlighted in green.

3. To create a user group for **Finance**:
 - a. In *Name*, enter *Finance*.
 - b. In *Remote Groups*, click *Add*.
 - c. Choose the SAML SSO settings as the *Remote Server*.
 - d. Set *Groups* to *Specify*.

The group name is the result of the output of the LDAP query for the **memberOf** attribute. In the example, this is `CN=Finance,CN=Users,DC=fortiad,DC=info`.

e. Click **OK**.

Edit User Group

Name: Finance

Type: Firewall

Members: +

Remote Groups

Remote Server	Group Name
fac_saml_idp-sslvpn	CN=Finance,CN=Users,DC=fortiad,DC=info

OK Cancel

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

Edit User Group

Name: sslvpn_group

Type: Firewall

Members: ljames, pparker

Remote Groups

No results

OK Cancel

FortiGate SSL VPN configurations

Configure SSL VPN portals and settings for **Finance** and **Sales** users to have remote network access. Firewall policies also need to be put into place for access control.

To configure SSL VPN portals for Finance and Sales users:

1. Go to *VPN > SSL-VPN Portals* and click *Create New*.
2. To create a profile named **Finance-portal**:
 - a. In *Name*, enter *Finance-portal*.
 - b. Enable *Tunnel Mode* with split tunneling set to *Enabled Based on Policy Destination*.
 - c. Set *Source IP Pools* to a desired pool.
 - d. Enable *Web Mode* and in *Portal Message*, enter *Finance SSL-VPN Portal*.
 - e. In *Predefined Bookmarks*, select *Create New* to create a new bookmark called *Finance Server*. In our example, a *Finance server* is available on `https://10.88.0.5:9443`.

f. Click **OK**.

Edit SSL-VPN Portal

Name: Finance-portal

Limit Users to One SSL-VPN Connection at a Time: ☒

Tunnel Mode

Split tunneling: ☒ Tunnel Mode

☐ Disabled
All client traffic will be directed over the SSL-VPN tunnel.

☒ **Enabled Based on Policy Destination**
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

☐ Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override: +

Source IP Pools: SSLVPN_TUNNEL_ADDR1 x

Tunnel Mode Client Options

Allow client to save password: ☒

Allow client to connect automatically: ☒

Allow client to keep connections alive: ☒

DNS Split Tunneling: ☒

☒ Host Check

☒ Restrict to Specific OS Versions

Web Mode

Portal Message: Finance SSL-VPN Portal

Theme: Neutrino

Show Session Information: ☒

Show Connection Launcher: ☒

Show Login History: ☒

User Bookmarks: ☒

Rewrite Content IP/URI: ☒

RDP/VNC clipboard: ☒

Predefined Bookmarks

+ Create New Edit Delete Search

Name	Type	Location	Description
Finance Server	HTTP/HTTPS	https://10.88.0.5:9443	

FortiClient Download

Download Method: Direct SSL-VPN Proxy

Customize Download Location: ☒

OK Cancel

3. To create a profile named **Sales-portal**:

- a. In *Name*, enter *Sales-portal*.
- b. Enable *Tunnel Mode* with split tunneling set to *Enabled Based on Policy Destination*.
- c. Set *Source IP Pools* to a desired pool.
- d. Enable *Web Mode* and in *Portal Message*, enter *Sales SSL-VPN Portal*.
- e. In *Pre-defined Bookmarks*, create a new bookmark called *Sales Server*. In our example, a *Sales server* is available on `https://10.88.0.3:9443`.

f. Click **OK**.

Edit SSL-VPN Portal

Name: Sales-portal

Limit Users to One SSL-VPN Connection at a Time: ☐

Tunnel Mode

Split tunneling: ☒ Enabled Based on Policy Destination
 Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

☐ Disabled
 All client traffic will be directed over the SSL-VPN tunnel.

☐ Enabled for Trusted Destinations
 Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override:

Source IP Pools: ☒ SSLVPN_TUNNEL_ADDR1

Tunnel Mode Client Options

Allow client to save password: ☐

Allow client to connect automatically: ☐

Allow client to keep connections alive: ☐

DNS Split Tunneling: ☐

☐ Host Check

☐ Restrict to Specific OS Versions

Web Mode

Portal Message: Sales SSL-VPN Portal

Theme: Neutrino

Show Session Information: ☒

Show Connection Launcher: ☒

Show Login History: ☒

User Bookmarks: ☒

Rewrite Content IP/UI: ☐

RDP/VNC clipboard: ☒

Predefined Bookmarks

Name	Type	Location	Description
Sales Webserver	HTTP/HTTPS	https://10.88.0.3:9443	

FortiClient Download

Download Method:

Customize Download Location: ☐

To configure SSL VPN settings:

1. Go to **VPN > SSL-VPN Settings** and enable SSL-VPN.
2. Set **Listen on Interface(s)** to **WAN (port3)**.
3. Set **Listen on Port** to **10443**.
4. Set the **Server Certificate** to **FGT-SSLVPN**.
5. In **Authentication/Portal Mapping**, configure user groups to portal mappings.
 - a. Select **Create New** and create a new Finance mapping:
 - i. Set **Users/Groups** to **Finance**.
 - ii. Set **Portal** to **Finance-portal**.
 - iii. Click **OK**.
 - b. Select **Create New** and create a new Sales mapping:
 - i. Set **Users/Groups** to **Sales**.
 - ii. Set **Portal** to **Sales-portal**.
 - iii. Click **OK**.
 - c. Select **Create New** and create a new placeholder mapping:
 - i. Set **Users/Groups** to **sslvpn_group**.
 - ii. Set **Portal** to **no-access**.
 - iii. Click **OK**.

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

SSL-VPN Settings

Connection Settings

Enable SSL-VPN ☒

Listen on Interface(s) WAN (port3)

Listen on Port 10443

Web mode access will be listening at <https://10.0.3.254:10443>

Server Certificate FGT-SSLVPN

Redirect HTTP to SSL-VPN ☒

Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout ☒

Inactive For 300 Seconds

Require Client Certificate ☐

Tunnel Mode Client Settings

Address Range Automatically assign addresses Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server Same as client system DNS Specify

Specify WINS Servers ☐

Web Mode Settings

Language Browser preference System

Authentication/Portal Mapping

Create New Edit Delete Send SSL-VPN Configuration

Users/Groups	Portal
Finance	Finance-portal
Sales	Sales-portal
sslvpn_group	no-access
All Other Users/Groups	no-access

Apply

To configure firewall policies for access control:

- Go to *Policy & Objects > Firewall Policy* and click *Create New*.
- Create a policy named *SSLVPN-Finance*.
 - Set *Incoming Interface* to *SSL-VPN tunnel interface (ssl.root)*.
 - Set *Outgoing Interface* to *port2*.
 - Set *Source* to *all* and *User* to *Finance*.
 - Set *Destination* to the *Finance* address object. If needed, create this object with the IP address *10.88.0.5/32*.
 - Set *Service* to *ALL*.
 - Configure other settings as needed.

g. Click **OK**.

The screenshot shows the 'Edit Policy' configuration window in FortiGate. The policy is named 'SSLVPN-Finance'. The configuration is as follows:

- Name:** SSLVPN-Finance
- Incoming Interface:** SSLVPN tunnel interface (ssl.root)
- Outgoing Interface:** DMZ (port2)
- Source:** all, Finance
- Destination:** Finance
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall/Network Options:**
 - NAT: enabled
 - IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool
 - Preserve Source Port: disabled
 - Protocol Options: default
- Security Profiles:**
 - AntiVirus: disabled
 - Web Filter: disabled
 - DNS Filter: disabled
 - Application Control: disabled
 - IPS: disabled
 - File Filter: disabled
 - SSL Inspection: no-inspection
- Logging Options:**
 - Log Allowed Traffic: Security Events (selected), All Sessions
 - Generate Logs when Session Starts: disabled
- Comments:** Write a comment... (0/1023)
- Enable this policy:** enabled

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

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

g. Click **OK**.

The screenshot shows the 'Edit Policy' configuration window in FortiGate. The policy is named 'SSLVPN-Sales'. The configuration is as follows:

- Name:** SSLVPN-Sales
- Incoming Interface:** SSLVPN tunnel interface (ssl.root)
- Outgoing Interface:** DMZ (port2)
- Source:** all, Sales
- IP/MAC Based Access Control:** (disabled)
- Destination:** Webserver1
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall/Network Options:**
 - NAT:** (checked)
 - IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool
 - Preserve Source Port:** (checked)
 - Protocol Options:** (none)
- Security Profiles:**
 - AntiVirus: (checked)
 - Web Filter: (checked)
 - DNS Filter: (checked)
 - Application Control: (checked)
 - IPS: (checked)
 - File Filter: (checked)
 - SSL Inspection: (checked), no-inspection
- Logging Options:**
 - Log Allowed Traffic: (checked), Security Events (selected), All Sessions
 - Generate Logs when Session Starts: (checked)
- Comments:** (Copy of SSLVPN-Finance) 25/1023
- Enable this policy:** (checked)

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

4. Create a placeholder policy named *SSLVPN-placeholder*.
 - a. Set *Incoming Interface* to *SSL-VPN tunnel interface (ssl.root)*.
 - 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**.

The screenshot shows the 'Edit Policy' configuration window for an SSLVPN policy. The policy is named 'SSLVPN-placeholder'. The configuration is as follows:

- Name:** SSLVPN-placeholder
- Incoming Interface:** SSLVPN tunnel interface (ssl.roo)
- Outgoing Interface:** Clients_LAN (port1)
- Source:** all, sslvpn_group
- IP/MAC Based Access Control:** none
- Schedule:** always
- Service:** ALL_ICMP
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall/Network Options:**
 - NAT:** enabled
 - IP Pool Configuration:** Use Outgoing interface Address, Use Dynamic IP Pool
 - Preserve Source Port:** disabled
 - Protocol Options:** default
- Security Profiles:**
 - AntiVirus: disabled
 - Web Filter: disabled
 - DNS Filter: disabled
 - Application Control: disabled
 - IPS: disabled
 - File Filter: disabled
 - SSL Inspection: no-inspection
- Logging Options:**
 - Log Allowed Traffic: Security Events (selected), All Sessions
 - Generate Logs when Session Starts: disabled
- Comments:** Write a comment... (0/1023)
- Enable this policy:** enabled

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

FortiClient configurations

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

To configure an SSL VPN remote access profile on FortiClient:

1. Go to the *Remote Access* tab.
2. Click the hamburger icon beside the *VPN Name* dropdown and select *Add a new connection*.
3. Set the *VPN* to *SSL-VPN*.
4. Set the *Connection Name* to *SAML_SSLVPN*.
5. Set *Remote Gateway* to *10.0.3.254*.
6. Select *Customize port* and set it to *10443*.
7. Select *Enable Single Sign On (SSO) for VPN Tunnel*.
8. Optionally, select *Use external browser as user-agent for saml user authentication* if you wish to use an external browser instead of the embedded module for authentication.

9. Click **Save**.

New VPN Connection

VPN: **SSL VPN** | IPsec VPN | XLS

Connection Name: SAML_SSLVPN

Description:

Remote Gateway: 10.0.3.254

+Add Remote Gateway

☒ Customize port: 10443

☒ Enable Single Sign On (SSO) for VPN Tunnel

☒ Use external browser as user-agent for saml user authentication

☐ Enable auto-login with Azure Active Directory

Cancel Save

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

1. Go to *Endpoint Profiles > Remote Access*.
2. Select an existing profile such as *Default* and click *Edit*.
3. In *VPN Tunnels*, add *Add Tunnel*.
4. In *VPN Type*, select *Manual* and click *Next*.
5. In *Basic Settings*:
 - a. Set *Name* to *EMS_SAML_SSLVPN*.
 - b. Set *Remote Gateway* to *10.0.3.254*.
 - c. Set *Port* to *10443*.
6. In *Advanced Settings*:
 - a. Enable *SAML Login*.
 - b. b. Optionally, enable *Use external browser as user-agent for saml user authentication* if you wish to use an external browser instead of the embedded module for authentication.
7. Click *Save* to save the VPN profile.
8. Click *Save* again to save the changes to the *Remote Access Profile*.

FortiClient Endpoint Management Server

Remote Access Profile

Name: Default

DNS Cache Service Control: Disable discache service

Prefer SSL VPN DNS: ☒

Do Not Accept Invalid Server Certificate: ☐

Register the Address in DNS: Register both physical adapter and tunnel IP's to DNS server

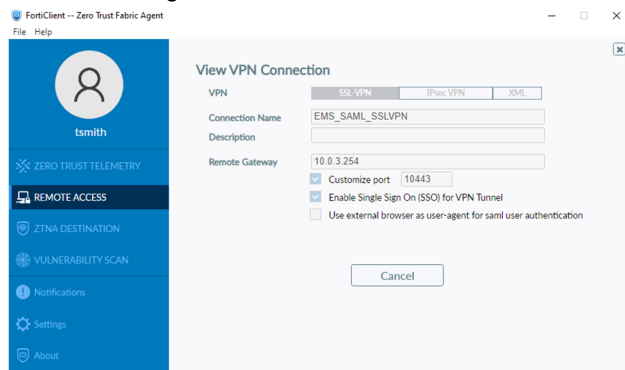
VPN Tunnels

Name	Type	Remote Gateway
EMS_SAML_SSLVPN	SSL	10.0.3.254

Save Discard Changes Revert To Default

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

10. View the settings on FortiClient.



Testing and verification

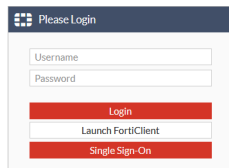
The following demonstrates connection via Web mode and Tunnel mode using SAML authentication. Review the authentication process at the beginning of this deployment scenario to understand how the process works.

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 SSL VPN web portal.

Web mode SSL VPN

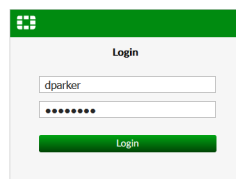
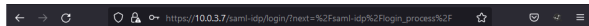
To verify a Web mode SSL VPN connection with the Finance user Dan Parker (dparker):

1. Open a browser, and enter `https://10.0.3.254:10443`.
2. Click *Single Sign-On* to sign in.



Your sign-on request will be redirected by the FortiGate SAML SP to the FortiAuthenticator SAML IdP.

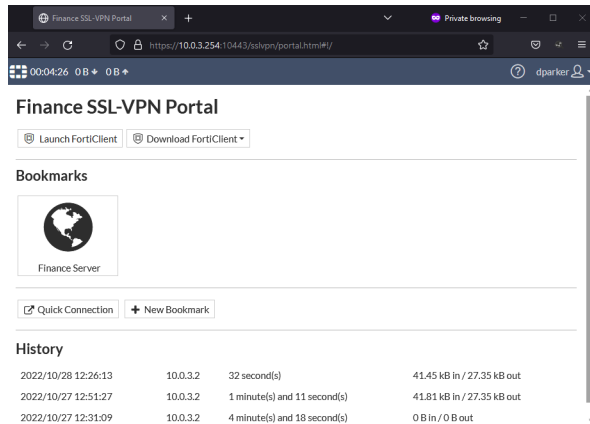
3. Enter the user credentials for the user and click *Login*.



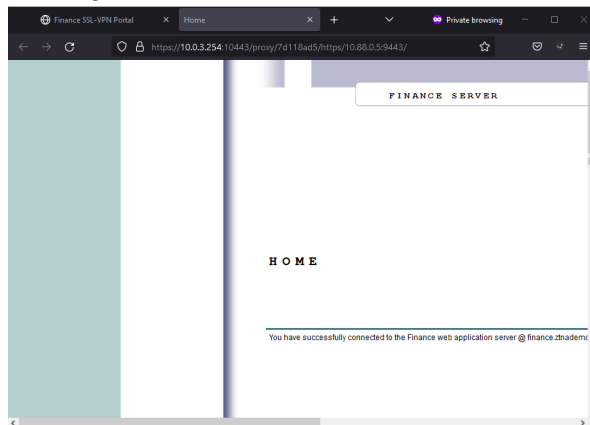
In the background, the FortiAuthenticator authenticates this user over the LDAP connection to the Windows AD. If the authentication succeeds and matches a user group on FortiAuthenticator, FortiAuthenticator sends a SAML assertion back to the browser containing the username and group information.

The browser redirects the SAML assertion to the FortiGate SAML SP, which matches the username and group information to a user group. Based on this user group, access is granted.

The Finance user can now see the Finance SSL-VPN Portal.

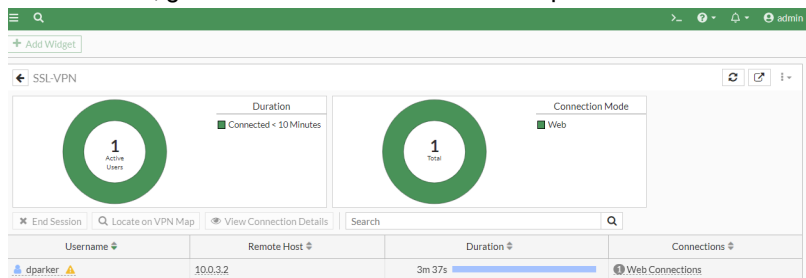


- Clicking on the Finance Server bookmark, the user can access the Finance server.



To verify the login status on the FortiGate and FortiAuthenticator:

- On FortiGate, go to *Dashboard > Network* and expand the *SSL-VPN* widget.



- 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"
```

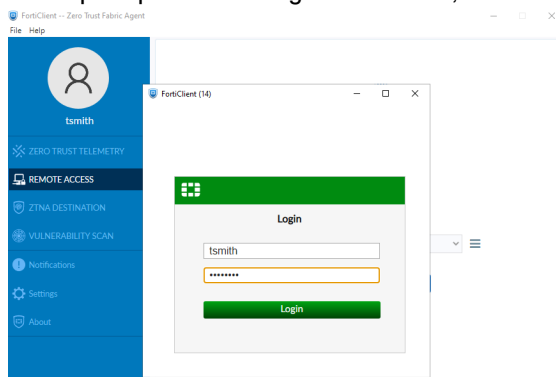
- On FortiAuthenticator, go to *Logging > Log Access > Logs*.
The SAML IdP authentication for dparker will be displayed.

ID	Timestamp	Level	Category	Sub Category	Log Type ID	Action	Status	Source IP	Short Message	User
242	Fri Oct 28 14:19:34 20...	Information	Event	Authentication	20001	Authentication	Success	SAML IdP	Remote LDAP user authentica...	dparker
241	Fri Oct 28 14:19:02 20...	Information	Event	Authentication	20502				SAML logout request from SP '...	dparker
240	Fri Oct 28 14:19:02 20...	Information	Event	User Portal	50008				SAML IdP user 'dparker' logged...	dparker
239	Fri Oct 28 14:13:58 20...	Information	Event	Authentication	20502				SAML assertion request from S...	dparker
238	Fri Oct 28 14:13:57 20...	Information	Event	User Portal	50007				SAML IdP user 'dparker' logged...	dparker
237	Fri Oct 28 14:13:47 20...	Information	Event	Authentication	20001	Authentication	Success	SAML IdP	Remote LDAP user authentica...	dparker
236	Fri Oct 28 14:08:34 20...	Information	Event	Authentication	20502				SAML logout request from SP '...	dparker

Tunnel mode SSL VPN

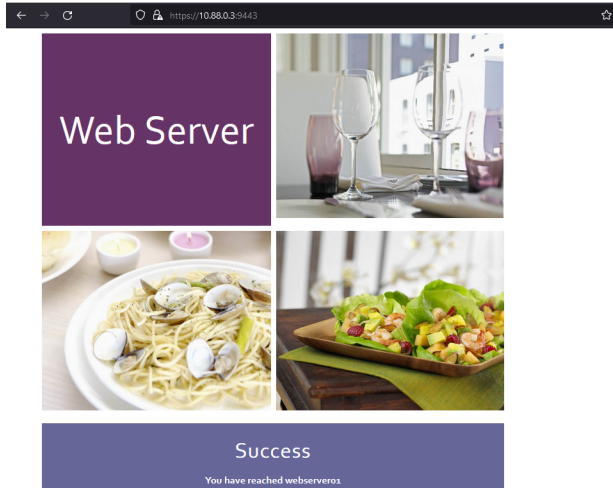
To verify a Tunnel mode SSL VPN connection with the Sales user Tom Smith (tsmith):

- On the client desktop, open FortiClient and go to the *Remote Access* tab.
- Select the VPN tunnel created earlier and click *SAML Login*.
- When prompted for the login credentials, enter the username and password and click *Login*.



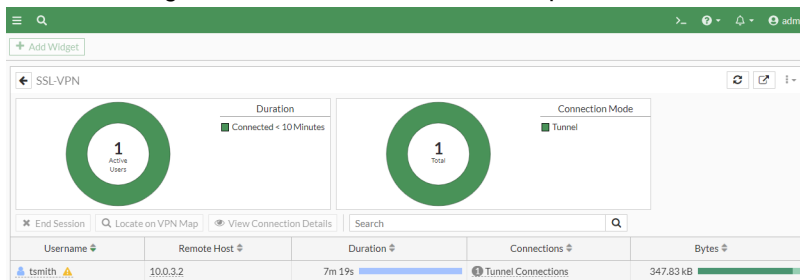
Again, in the background, the SAML login request gets processed by FortiAuthenticator. Upon a successful match, it sends a SAML assertion back to the FortiClient. The FortiClient forwards this to the FortiGate which matches a corresponding user group.

- Once connected, the user can open a browser and browse to `https://10.88.0.3:9443` to access the Sales webserver.

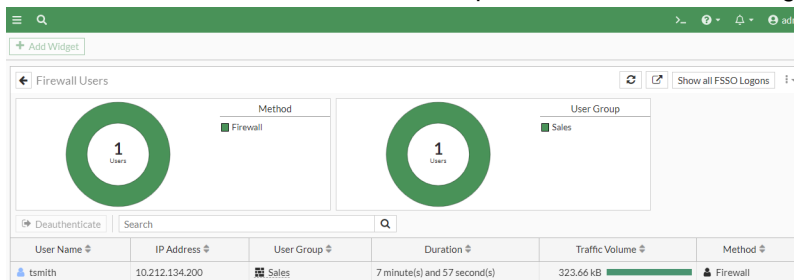


To verify the login status on the FortiGate and FortiAuthenticator:

1. On FortiGate, go to *Dashboard > Network* and expand the *SSL-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
	Fri Oct 28 14:48:00 20...	information	Event	Authentication	20502				SAML assertion request from S...	tsmith
251	Fri Oct 28 14:48:00 20...	information	Event	User Portal	50007				SAML IdP user 'tsmith' logged i...	tsmith
250	Fri Oct 28 14:48:00 20...	information	Event	Authentication	20001	Authentication	Success	SAML IdP	Remote LDAP user authentica...	tsmith
249	Fri Oct 28 14:24:48 20...	information	Event	Authentication	20502				SAML logout request from SP '...	dparker
248	Fri Oct 28 14:24:48 20...	information	Event	User Portal	50008				SAML IdP user 'dparker' logged...	dparker
247	Fri Oct 28 14:23:32 20...	information	Event	Authentication	20994	Login	Success	172.16.7.254	Web access granted to 'admin'	admin

Computer Authentication

This section describes configuring computer authentication.

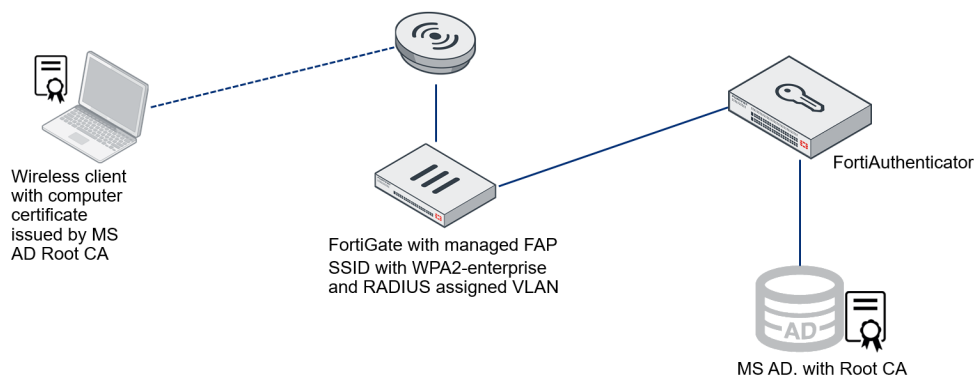
- [Computer authentication using FortiAuthenticator with MS AD Root CA on page 291](#)

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:

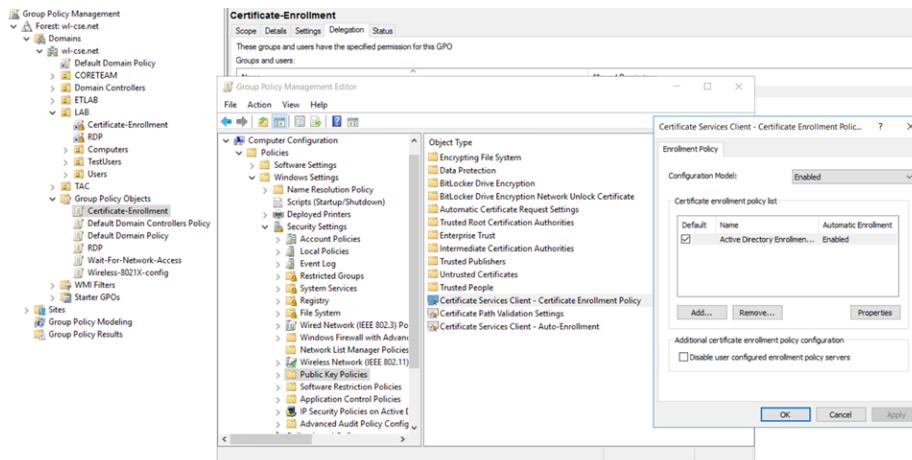
1. [Configure the certificates and Root CA on page 292](#)
2. [Configure LDAP users on FortiAuthenticator on page 293](#)
3. [Configure RADIUS authentication on page 296](#)
4. [Configure the SSID and interface objects on page 301](#)
5. [Results on page 303](#)

Configure the certificates and Root CA

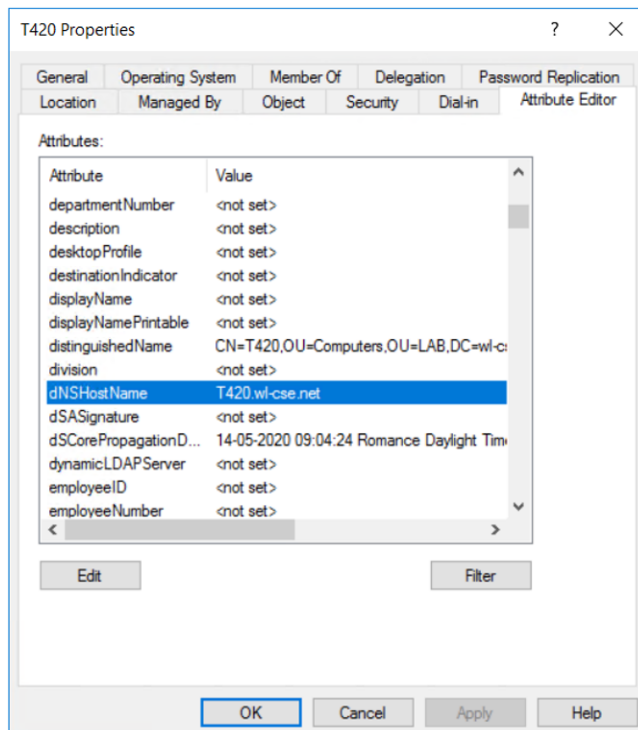
With Microsoft Active Directory as the Root CA, use Group Policy Management to deploy client certificates to domain computers. This is the certificate that will be used to validate RADIUS requests.

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 293](#)
2. [Creating a user realm on page 294](#)
3. [Creating a user group on page 295](#)
4. [Importing users with a remote user sync rule on page 295](#)

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.w1-cse.net` using *Port 636*.
 - c. **Base distinguished name:** Enter the base distinguished name, for example: `DC=w1-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=w1-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=w1-cse,DC=net))*.
3. Under *Synchronization Attributes*, set the following:
 - a. **Token-based authentication sync priorities:** Select *None*.
 - b. **Sync every:** Select the sync frequency based on your preferences, for example: *1 hour(s)*.
 - c. **Sync as:** *Remote LDAP User*.
 - d. **User role for new user imports:** *User*.
 - e. **Group to associate users with:** Select your remote LDAP user group.
 - f. **Certificate binding CA:** Select your CA for certificate binding.

4. Under *LDAP User Mapping Attributes*, set the following:

- a. **Username:** `dNSHostName`.
- b. **Certificate binding common name:** `dNSHostName`.

Create New Remote LDAP User Synchronization Rule

Name:

Remote LDAP:  

Base distinguished name:

LDAP filter:

Synchronization Attributes

Token-based authentication sync priorities:

☒ None (users are synced explicitly with no token-based authentication)

☐ FortiToken Hardware (assign if serial number is provided)

☐ FortiToken Hardware (assign an available token)

☐ FortiToken Mobile (assign an available token)

☐ FortiToken Cloud

☐ Email

☐ SMS

☐ Dual (Email and SMS)

Sync every:

Sync as: ☒ Remote LDAP User ☐ Local User

User role for new user imports: ☐ Administrator ☐ Sponsor ☒ User

Group to associate users with:   

Organization:  

Certificate binding CA:

☐ Email password recovery

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

☐ Proceed with rule even when response empty.

LDAP User Mapping Attributes

Username:

First name:

Last name:

Email:

Phone number:

Mobile number:

FTK-200 serial number:

Certificate binding common name:

Debugging Settings

User Fields Format 

The following user fields will be synchronized:

- Username:
 - maximum length: 255 characters
- First name:
 - maximum length: 30 characters
- Last name:
 - maximum length: 30 characters
- Email address:
 - maximum length: 254 characters
 - must be a valid email address
- Phone number:
 - maximum length: 64 characters

Please note that user fields will be truncated if their values exceed the maximum length.

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 297](#)
2. [Configuring the RADIUS client on page 297](#)
3. [Configuring the EAP server certificate on page 298](#)
4. [Creating a RADIUS policy on page 298](#)

5. Configuring the RADIUS server on FortiGate on page 300

Adding RADIUS attributes

RADIUS attributes can be added to the previously configured LDAP user group.

To add RADIUS attributes to the LDAP user group:

1. Go to *Authentication > User Management > User Groups*, and edit the user group associated with the remote LDAP users.
2. Under *RADIUS Attributes*, add the RADIUS attributes required by your configuration. In this example, the following attributes are required:
 - Tunnel-Type: VLAN.
 - Tunnel-Medium-Type: IEEE-802.
 - Tunnel-Private-Group-Id: 240.
 - Fortinet-Group-Name: FTNT_LAB_Computers.

Edit User Group

Name:

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

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

Remote LDAP:

LDAP users:

Selected LDAP Users: t420.wl-cse.net @ AD_Computers (dc01.wl-cse.net), win10a.wl-cse.net @ AD_Computers (dc01.wl-cse.net)

Usage Profile:

TACACS+ Authorization:

TACACS+ authorization rule:

Attribute	Value	Vendor	Actions
Tunnel-Type	VLAN (13)	Default	edit delete
Tunnel-Medium-Type	IEEE-802 (6)	Default	edit delete
Tunnel-Private-Group-Id	240	Default	edit delete
Fortinet-Group-Name	FTNT_LAB_Computers	Fortinet	edit delete

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.

RADIUS clients | RADIUS attribute criteria | Authentication type | Identity source | Authentication factors | RADIUS response

Policy name:

Description:

RADIUS clients:

Available RADIUS Clients:

Chosen RADIUS Clients:

Choose all | Remove all

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

RADIUS clients | **RADIUS attribute criteria** | Authentication type | Identity source | Authentication factors | RADIUS response

☒ RADIUS authentication request must contain specific attributes

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

RADIUS clients | **RADIUS attribute criteria** | **Authentication type** | Identity source | Authentication factors | RADIUS response

Authentication type:

☐ Password/OTP authentication

☐ MAC authentication bypass (MAB)

☒ Client Certificates (EAP-TLS)

5. Under *Identity source*, configure the following, and click *Next*.

- a. **Username format:** Select your preferred username format, for example: *realm\username*.
- b. **Realms:** In the *Realms* table, select your AD realm.
You can additionally apply a group filter if required.

RADIUS clients | **RADIUS attribute criteria** | **Authentication type** | **Identity source** | Authentication factors | RADIUS response

[Understanding the Client Certificates \(EAP-TLS\) workflow](#)

Username format:

☒ username@realm

☐ realm\username

☐ realm/username

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

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	host AD_Computers (dc01.wl-cse.net)	☐	☐ Filter: Filter local users:	X
+ Add a realm				

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

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

Certificate Verification Result	RADIUS Authentication Response	Return User Attributes	Return User Group Attributes
Valid	Access-Accept	✓	✗
Invalid	Access-Reject	✗	✗

Configuring the RADIUS server on FortiGate

Finally, you can configure the RADIUS server settings (FortiAuthenticator) on FortiGate.

To configure the RADIUS server on FortiGate:

1. On FortiGate, go to *User & Authentication > RADIUS Servers*, and click *Create New*.
2. Under *New RADIUS Server*, set the following:
 - a. **Name:** Enter a name for the RADIUS server, for example: *FAC*.
 - b. **Authentication method:** *Default*.

3. Under *Primary Server*, set the following:

- a. **IP/Name:** Enter the IP address of the FortiAuthenticator.
- b. **Secret:** Enter the RADIUS server secret created on FortiAuthenticator.

New RADIUS Server

Name: FAC

Authentication method: **Default** Specify

NAS IP:

Include in every user group: ☒

Primary Server

IP/Name: 192.168.200.9

Secret:

Connection status:

Test Connectivity

Test User Credentials

Secondary Server

IP/Name:

Secret:

Test Connectivity

Test User Credentials

OK Cancel

4. Click *OK*.

Configure the SSID and interface objects

To configure the SSID and interface objects:

1. [Creating the SSID on page 302](#)
2. [Creating interfaces on page 303](#)

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*.

The screenshot displays the FortiGate SSID configuration interface. The configuration is organized into several sections:

- Name:** FGT-FAC-8021X (FGT-8021X)
- Alias:** Used for 802.1X
- Type:** WiFi SSID
- VRF ID:** 0
- Traffic mode:** Tunnel
- Address:**
 - IP/Netmask: 0.0.0.0/0.0.0.0
 - Create address object matching subnet: ☐
 - Secondary IP address: ☐
- Administrative Access:**
 - IPv4: ☐ HTTPS, ☐ FMG-Access, ☐ FTM, ☐ HTTP, ☐ SSH, ☒ RADIUS Accounting, ☐ PING, ☐ SNMP, ☐ Security Fabric Connection
- DHCP Server:** ☐
- Network:**
 - Device detection: ☒
- WiFi Settings:**
 - SSID: FGT-FAC-8021X
 - Client limit: ☐
 - Broadcast SSID: ☒
- Security Mode Settings:**
 - Security mode: WPA2 Enterprise
 - Authentication: Local, **RADIUS Server**, FAC
- Client MAC Address Filtering:**
 - RADIUS server: ☐
- Additional Settings:**
 - Dynamic VLAN assignment: ☒
 - Schedule: always

Creating interfaces

You can now create interfaces as required.

To create additional interfaces:

1. Go to *Network > Interfaces*, and click *Create New > Interface*.
2. Configure your VLAN interface. In this example, the DomainComputers VLAN is created with the following settings:
 - a. **Name:** DomainComputers.
 - b. **Type:** VLAN.
 - c. **Interface:** The configured SSID, FGT-FAC-8021X (FGT-FAC-8032X).
 - d. **VLAN ID:** 240
 - e. **Role:** LAN.

Interface	 DomainComputers
Link	
Port Speed	Auto-Negotiation
Type	 VLAN
Role	LAN
IPv4 Addresses	10.10.240.1/24
VLAN ID	240
Base Interface	 FGT-FAC-8021X (FGT-FAC-8021X)

Results

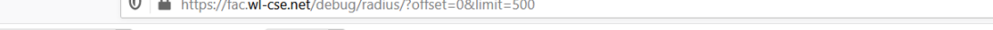
Once the configuration is complete, you should now be able to authenticate your computer using FortiAuthenticator with a Microsoft AD Root CA.

To confirm computer authentication is working as intended:

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

System	Refresh Download Raw Log Log Type Reference Debug Report Search for log records 480113 results (386530 total)										
Authentication											
Fortinet SSO Methods											
Monitor											
Certificate Management											
Logging											
Log Access											
Logs											
Log Config											
Audit Reports											
	ID	Timestamp	Level	Category	Sub Category	Log Type ID	Action	Status	Source IP	Log Details	
	480...	Thu Sep 24 14:15...	informati...	Event	Authentication	20420	Authenticat...	Success	192.168.200.1	Log Record Detail	
	480...	Thu Sep 24 14:15...	informati...	Event	System	30350				Id 480113	
	480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success	192.168.190.108	Jd Timestamp Thu Sep 24 14:15:37 2020	
	480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success		V Level Information	
	480...	Thu Sep 24 14:14...	informati...	Event	Authentication	20994	Login	Success		A Action Authentication Success	
	480...	Thu Sep 24 14:14...	informati...	Event	System	30350				S Source IP 192.168.200.1	
	480...	Thu Sep 24 14:13...	informati...	Event	System	30350				L Message 802.1x authentication successful	
	480...	Thu Sep 24 14:12...	informati...	Event	System	30350				J User host/7420.wl-ess.net	
	480...	Thu Sep 24 14:12...	informati...	Event	System	30350				Log Type	
	480...	Thu Sep 24 14:11...	informati...	Event	System	30350				Type Id 20420	
	480...	Thu Sep 24 14:10...	informati...	Event	System	30350				Name 802.1x Authentication in GDC	
	480...	Thu Sep 24 14:09...	informati...	Event	System	30350				Sub Category Authentication	
	480...	Thu Sep 24 14:08...	informati...	Event	System	30350				Category Event	
	480...	Thu Sep 24 14:07...	informati...	Event	System	30350				Description 802.1x authentication successful	

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



Service: **RADIUS Authentication** Max. log file size: **1 MB** Enter debug mode

```

2020-09-24T14:17:35.572936+02:00 PAC radiusd[1571]: (262) # Executing group from file /usr/etc/raddb/sites-enabled/default
2020-09-24T14:17:35.572946+02:00 PAC radiusd[1571]: (262) eap: Expiring EAP session with state 0x7949ede7d0c9386
2020-09-24T14:17:35.572951+02:00 PAC radiusd[1571]: (262) eap: Finished EAP session with state 0x7949ede7d0c9386
2020-09-24T14:17:35.572956+02:00 PAC radiusd[1571]: (262) eap: Previous EAP request found for state 0x7949ede7d0c9386, released from the list
2020-09-24T14:17:35.574169+02:00 PAC radiusd[1571]: rlm_eap_tls: Certificate passed CRL check.
2020-09-24T14:17:35.574832+02:00 PAC radiusd[1571]: fn_eap_tls_c: Verifying remote LDAP user cert binding (user: t420.wl-cse.net, ldap net: 2)
2020-09-24T14:17:35.575344+02:00 PAC radiusd[1571]: rlm_eap_tls: Certificate binding check succeeded. (CN=T420.wl-cse.net, Issuer=/DC=net/DC=wl-cse/CN=wl-cse-DC01-CA)
2020-09-24T14:17:35.575626+02:00 PAC radiusd[1571]: rlm_eap_tls: Certificate passed CRL check.
2020-09-24T14:17:35.577125+02:00 PAC radiusd[1571]: (262) eap: EAP session adding eap=1:state= 0x7949ede7d0c9386

```

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

Dashboard

Status

Security

Network

Users & Devices

WiFi

FortiView Sources

FortiView Destinations

FortiView Applications

FortiView Web Sites

FortiView Policies

FortiView Sessions

Security Fabric

Network

Add Widget

←

Clients By FortiAP

FortiAP

PU421E3X16003...

Technology

Diagnostics and Tools

Search

IP	MAC Address	User	Device	SSID	
2.4 GHz	10.10.240.2	8C:A9:82:AE:4E:D6	host/T420-wl-cse.net	8ca9:82:ae:4e:d6	FGT-FAC-80212

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

14	0.122548	192.168.200.9	192.168.200.1	RADIUS	304 Access-Accept id=111
----	----------	---------------	---------------	--------	--------------------------

```

Authenticator: 960d1fd1eb07285343c9710b9886a250
[This is a response to a request in frame 13]
[Time from request: 0.016899000 seconds]
  Attribute Value Pairs
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
    > AVP: t=EAP-Message(79) l=6 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=c0dc18c09834985ce1a3f6ce03c1c71b
    > AVP: t=User-Name(1) l=22 val=host/T420.wl-cse.net
    > AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x00 val=IEEE-802(6)
    > AVP: t=Tunnel-Type(64) l=6 Tag=0x00 val=VLAN(13)
    > AVP: t=Tunnel-Private-Group-Id(81) l=5 val=240
  
```

WiFi onboarding using FortiAuthenticator Smart Connect

This example demonstrates how to configure WiFi onboarding using FortiAuthenticator Smart Connect with either Google Workspace or Microsoft Azure.

This configuration assumes that you have already configured your FortiAuthenticator following the initial configuration steps available within the FortiAuthenticator Administration Guide. FortiAuthenticator must be version 6.1.1 or higher.

Before starting, you should already have the following available:

- A registered domain name and functional DNS. This example uses fortixpert.com.
- A publicly signed wildcard certificate for your domain (for example *.fortixpert.com used to sign MS Azure DS Secure LDAP Connector).
- A publicly signed host/server certificate for FortiAuthenticator.
- An active Google Workspace Enterprise or MS Azure subscription, depending on your chosen configuration.
 - Please note: Secure LDAP is not supported using Google Workspace Business or Google Workspace Basic subscriptions.
 - An active MS Azure subscription requires AD Directory Services to be provisioned in order to support Secure LDAP.
- Have the appropriate Fortinet infrastructure in place, for example, Fortigate running FOS 6.2.4GA+, FortiSwitch running 6.2.4GA+, FortiAP/FortiAP-U running latest GA and FortiAuthenticator 6.1.1 and above.

To configure WiFi onboarding using Smart Connect:

1. [Initial settings on FortiAuthenticator on page 305](#)
2. Select either the Google Workspace or Azure configuration:
 - a. [Option A - WiFi onboarding with Smart Connect and Google Workspace on page 309](#)
 - b. [Option B - WiFi onboarding with Smart Connect and Azure on page 319](#)
3. [FortiGate configuration on page 328](#)
4. [Results on page 338](#)

Initial settings on FortiAuthenticator

To set up the initial configuration on FortiAuthenticator:

1. [Install certificates on page 306](#)
2. [Configure the RADIUS client settings on page 307](#)
3. [Configure the local root CA on page 308](#)
4. [Configure the EAP server certificate and CA for EAP-TLS on page 309](#)

Install certificates

To install a wildcard certificate on FortiAuthenticator:

1. Go to *Certificate Management > Certificate Authorities > Trusted CA*.
Import a trusted root/intermediate public CA certificate in order to support your wildcard certificate.

Import Trusted CA Certificate

Certificate ID:

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*.

Import Certificate

Type: PKCS12 Certificate **Certificate and Private Key** Local certificate

Certificate ID:

Certificate file (.cer):

Private key file:

Passphrase:

To generate a Certificate Signing Request (optional):

The following steps are optional and can be done if the server certificate matching the FortiAuthenticator FQDN is not yet available.

1. In *Certificate Management > End Entities > Local Services*, select the *Create New* button.
Configure the following settings:
 - a. Under *Create New Server Certificate*, set the *Certificate ID* to your certificate name, for example, *fac.fortixpert.com*.
 - b. Under *Subject Information*, configure the *Name*, *Department*, *Company*, *City*, *State/Province*, *Country* and *Email Address* for your certificate.
 - c. (Optional) If you are using a self-signed certificate on FortiAuthenticator, add a Subject Alternative Name (SAN) matching the FQDN under *Subject Alternative Name*.
 - d. (Optional) Under *Advanced Options: Key Usages*, choose all *Key Usages* and *Extended Key Usages*.

- e. All other fields can be left in their default state. Click *OK* to save your changes.

- 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.
- Import the signed certificate file from the public CA by selecting *Import* and uploading the `certificatename.cer` file.

To install local service certificates:

- Go to *Certificate Management > Certificate Authorities > Trusted CA*. Upload the trusted root/intermediate public CA certificates in order to support your host/server certificate.
- 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.
- Under *System > Administration > System Access > GUI Access*, configure the following:
 - For *HTTPS Certificate*, select the server certificate matching the device FQDN from the dropdown box.
 - For *CA Certificate*, select the Root CA certificate that was used to sign the host/server certificate selected above.
- Select *OK*.

Configure the RADIUS client settings

To configure the RADIUS client:

- 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.
- Under *System > Dashboard > Status*, edit and set the hostname and FQDN for FortiAuthenticator so that it matches the DNS host record.
- 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).

The screenshot shows the 'Edit EAP Certificates' configuration window. It has a 'Server Settings' section with 'EAP Server Certificate' set to 'fac.fortixpert.com | OU=Domain Control Validated, CN=fac.fortixpert.com'. Below this is the 'EAP-TLS Authentication' section, which includes a 'Local CAs' list with 'FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney' selected, and an empty 'Trusted CAs' field. At the bottom right is a green 'OK' button.

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 310](#)
2. [Configure Smart Connect and the captive portal on page 315](#)
3. [Configure RADIUS settings on FortiAuthenticator on page 318](#)

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 310](#)
2. [Configure certificates on FortiAuthenticator on page 312](#)
3. [Configure the remote LDAP server and users on page 313](#)

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*.

Step 1 of 2: Client details

Client details

LDAP client name *

FAC

Description

Secure LDAP Client for FAC

* Required field

CANCEL CONTINUE

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

5. Click *Add LDAP Client*.

Verify user credentials
Specify client's access level for verifying user credentials. Changes can take up to 24 hours to take effect. ?

☒ Entire domain (fortixpert.com)
☐ Selected organizational units
☐ No access

Read user information
Specify client's access level for reading user information. Some clients need additional information before authenticating users. ?

☒ Entire domain (fortixpert.com)
☐ Selected organizational units
☐ No access

Read group information
Client can read group information. Some clients need additional information before authenticating users. ?

☒ On

BACK 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.

✓ FAC added

Next, connect your client to the LDAP service

1. Download the generated certificate (it might take a few minutes to generate).

Want to do this later? You can generate and download a certificate at any time from the client's details page.

Google_2023_05_15_9640
Expires May 15, 2023
[Download certificate](#)

2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials.
[Learn more](#)

CONTINUE TO CLIENT DETAILS

Unzip the certificate file to a local folder. Contained within will be a public certificate along with a private key.

7. Select *Continue to Client Details*. Select Service status and change the status to *On*.

Service status

☒ ON for everyone

☐ OFF for everyone

 Changes may take up to 24 hours to propagate to all users.

1 unsaved change

CANCEL

SAVE

8. Click *Save*.

Configure certificates on FortiAuthenticator

To download Google Root CA Certificate:

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

To import the Google Certificates into FortiAuthenticator:

1. In FortiAuthenticator, go to *Certificate Management > Certificate Authorities > Trusted CAs*, and click *Import*.
2. Enter a *Certificate ID* and then upload the Google Root CA certificate previously downloaded.

Import Trusted CA Certificate

Certificate ID:

Google_RootCA_GSR2

Certificate:

 GSR2.crt

OK

Cancel

3. Go to *Certificate Management > End Entities > Local Services*, and click *Import*.
4. Under *Import Certificate*, select *Certificate and Private Key* as the *Type*. Enter a *Certificate ID*, and select the *Certificate file* and *Private key file* from the file you unzipped previously. A *Passphrase* is not required. Click *OK*.

Import Certificate

Type:

PKCS12 Certificate

Certificate and Private Key

Local certificate

Certificate ID:

GSuite_LDAP

Certificate file (.cer):

 Google_2023_05_15_9640.crt

Private key file:

 Google_2023_05_15_9640.key

Passphrase:

OK

Cancel

Configure the remote LDAP server and users

To provision the remote LDAP server:

1. In FortiAuthenticator, go to *Authentication > Remote Auth. Servers > LDAP*, and click *Create New*.
2. Under *Create New LDAP Server*, set the following:
 - a. **Name**: Enter a name for the remote LDAP server, for example *google.fortixpert.com*.
 - b. **Primary server name/IP**: *ldap.google.com*.
 - c. **Base distinguished name**: Enter the base LDAP search directory, for example the Google Workspace domain: *dc=fortixpert,dc=com*.
 - d. **Bind type**: *Simple*.
3. Under *Query Elements*, set the following:
 - a. **Pre-defined templates**: Select *OpenLDAP/G Suite* from the dropdown box, and click *Apply*.
4. Under *Secure Connection*, enable the secure connection function, and set the following:
 - a. **Protocol**: *LDAPS*.
 - b. **CA Certificate**: Select the *Google_RootCA_GSR2* certificate from the dropdown box.
 - c. **Use Client Certificate for TLS Authentication**: *Enabled*.
 - d. **Client certificate**: Select the *G Suite_LDAP* client certificate from the dropdown box.
5. At the top of the page under Base distinguished name, select the directory lookup icon.
Once the LDAPS connection is established you'll see the Directory of Groups and Users within Google Workspace.

Select *OK*.

Create New LDAP Server

Name: google.fortixpert.com

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

☐ Use secondary server

Base distinguished name: dc=fortixpert,dc=com

Bind type: Simple Regular

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

Query Elements

Pre-defined templates: OpenLDAP/GSuite Apply

User object class: person

Username attribute: uid

Group object class: group

Obtain group memberships from: User attribute Group attribute

Group membership attribute: member

☐ Force use of administrator account for group membership lookups

Secure Connection

☒ Enable

Protocol: LDAPS STARTTLS

CA certificate: Google_RootCA_GSR2 | OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign

☒ Use Client Certificate for TLS Authentication

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

Windows Active Directory Domain Authentication

☐ Enable

OK Cancel

6. Select *OK* again to save the LDAP server settings.

To import remote user accounts:

1. Go to *Authentication > User Management > Remote Users*, and confirm that *LDAP* is selected at the top right of the page.
2. Click *Import*.
3. Under *Import Remote LDAP Users*, set the following:
 - a. **Remote LDAP server:** Select your connector bound to ldap.google.com from the dropdown box.
 - b. **Action:** *Import Users*.
4. Click *Go*. A list of all the users within your Google Workspace directory will be displayed.
5. Select the users you want to be able to connect to the wireless network using their Google Workspace account, and select *OK* to import the relevant user accounts.
6. Under *Synchronization Attributes*, set the following:
 - a. **Token-based authentication sync priorities:** *None*.
 - b. **Sync every:** Select the sync frequency. In production environments, this should be set to 30 minutes or more depending on the number of users being synchronized.
 - c. **Sync as:** *Remote LDAP User*.
 - d. **User role for new user imports:** *User*.

7. Leave all other settings in their default state, and click *OK*.

To create a new realm:

1. Go to *Authentication > User Management > Realms*, and click *Create New*.
2. Configure the following settings:
 - a. **Name:** Enter a name for your realm, for example fortixpert.com.
 - b. **User source:** Select the remote LDAP service from the dropdown box.
3. Click *OK*.

Configure Smart Connect and the captive portal

This section outlines the configuration required on FortiAuthenticator to provision a captive portal using Smart Connect authenticating against Google Workspace.

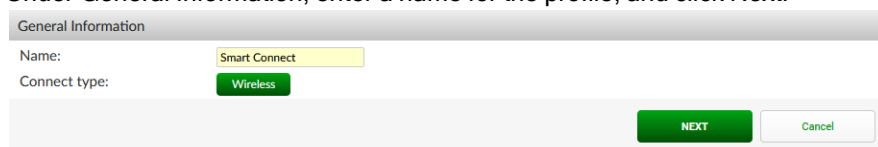
To configure Smart Connect and portals on FortiAuthenticator:

1. [Create the Smart Connect profile on page 315](#)
2. [Create the captive portal on page 316](#)
3. [Create the self-service portal policy on page 317](#)

Create the Smart Connect profile

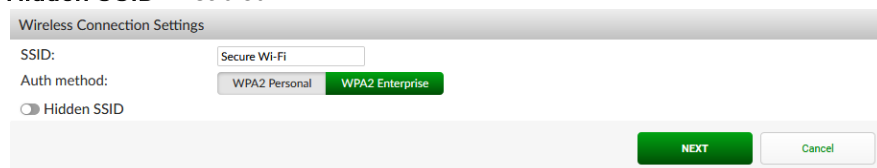
To create Smart Connect profiles:

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*.



The screenshot shows the 'General Information' tab of the Smart Connect profile configuration. The 'Name' field is set to 'Smart Connect' and the 'Connect type' is set to 'Wireless'. At the bottom right, there are 'NEXT' and 'Cancel' buttons.

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*.



The screenshot shows the 'Wireless Connection Settings' tab. The 'SSID' field is set to 'Secure Wi-Fi', the 'Auth method' is set to 'WPA2 Enterprise', and the 'Hidden SSID' checkbox is unchecked. At the bottom right, there are 'NEXT' and 'Cancel' buttons.

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

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

EAP General Settings

EAP Type: **TLS** TTLS PEAP

Signing CA: FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney, O=FortiXpert, OU=IT, CN=fac.fortixpert.com, emailAddress=admin@fortixpert.com

Username Format:

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

NEXT Cancel

5. Under *Certificate Installation Settings*, set the following and then click *OK*.

- a. **Install local CA certificates:** Choose to install the local Root_CA certificate.
- b. **Install trusted CA certificates:** Choose to install any certificate that is required for all relevant certificate chains to be fully trusted.

Certificate Installation Settings

Install local CA certificates:

Available Install Local CA Certificates

Filter

Choose all

Selected Install Local CA Certificates

FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney,

Remove all

Install trusted CA certificates:

Available Install Trusted CA Certificates

Filter

Choose all

Selected Install Trusted CA Certificates

Fortinet_CA1_Root | C=US, ST=California, L=Sunr
 Fortinet_CA2_Intermediate | C=US, ST=California
 Fortinet_CA2_Root | C=US, ST=California, L=Sunr
 Go_Daddy_Class_2_CA | C=US, O=The Go Dadd
 Go_Daddy_Root_CA_G2 | C=US, ST=Arizona, L=5
 Go_Daddy_Secure_CA_G2 | C=US, ST=Arizona, L=5
 Google_RootCA_GSR2 | OU=GlobalSign Root CA
 Sectigo_RSA_DV_Secure_Server_CA | C=GB, ST=I
 Sectigo_Root_CA | C=US, ST=New Jersey, L=Jerse

Remove all

OK Cancel

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

Create the captive portal

To create a captive portal:

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

4. Select *OK*.

Create 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.

FortiAuthenticator VM FAC-VM0000000000

System > Authentication > Policy type > Identity sources > Authentication factors

Local/Remote Users:

Username format:

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

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	fortixpert.com azure.fortixpert.com (13.75.227.41)	☐	Filter:	Filter local users

[Add a realm](#)

[Previous](#) [Discard and exit](#) [Update and exit](#) [Next](#)

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:

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

RADIUS clients > RADIUS attribute criteria > Authentication type > Identity source > Authentication factors > RADIUS response

Policy name:

Description:

RADIUS clients:

Available RADIUS Clients:

Chosen RADIUS Clients:

[Choose all](#) [Remove all](#)

[Discard and exit](#) [Next](#)

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

RADIUS clients > RADIUS attribute criteria > Authentication type > Identity source > Authentication factors > RADIUS response

Authentication type:

- ☐ Password/OTP authentication
- ☐ MAC authentication bypass (MAB)
- ☒ Client Certificates (EAP-TLS)

[Previous](#) [Discard and exit](#) [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 Azure AD Directory Services via Secure Lightweight Directory Access Protocol

To configure WiFi Onboarding with Azure:

1. [Configure Azure AD DS LDAPS integration on page 319](#)
2. [Configure Smart Connect and the captive portal on page 324](#)
3. [Configure RADIUS settings on FortiAuthenticator on page 328](#)

Configure Azure AD DS LDAPS integration

This guide does not include information on how to provision Azure AD DS. Please refer to [Microsoft's support site](#) for instructions on how to do this.

To configure Azure AD DS LDAPS integration:

1. [Provision the LDAPS connector in Azure AD DS on page 320](#)
2. [Provision the remote LDAP server on FortiAuthenticator on page 321](#)

Provision the LDAPS connector in Azure AD DS

To provision the LDAP connector in Azure AD DS:

1. Login to the Azure admin portal using an Azure admin account.
2. Select *Active Directory Domain Services*.
3. Select *View*.
4. Select your AD DS instance, for example fortixpert.com.
5. Within the AD DS menu for your domain, select *Secure LDAP* under *Settings*.
6. In the Secure LDAP window, perform the following:
 - a. Set *Secure LDAP* to *Enable*.
 - b. Set *Allow secure LDAP access over the internet* to *Enable*.
 - c. Upload your domain wildcard certificate, for example *.fortixpert.com, in .PFX format.
 - d. Enter the password to decrypt the PFX file.

Save Discard Change Certificate

Secure LDAP Disabled	Allow secure LDAP access over the internet Disabled
Thumbprint Not available	Certificate expires Not available

Secure LDAP

Disable Enable

Allow secure LDAP access over the internet

Disable Enable

Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain

.PFX file with secure LDAP certificate *

"star.fortixpert.com.p12.pfx"

Password to decrypt .PFX file *

7. Select the *Save* button at the top of the page, and wait for Azure to configure Secure LDAP. This process takes approximately five minutes.
8. Once provisioning is complete, you must now allow inbound access for the secure LDAP protocol (port 636) to your AD DS instance.
9. Browse to the network security group linked in your Secure LDAP connector.
10. Select the network security 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.

Save Discard Change Certificate

Secure LDAP Enabled	Allow secure LDAP access over the internet Enabled
Thumbprint 3E2973752E953750A07102AA7B305DACC22FAB5E	Certificate expires Tue, 25 Jan 2022 23:59:59 GMT

Secure LDAP ⓘ

Allow secure LDAP access over the internet ⓘ

⚠ Your subnet is protected by network security group **aadds-nsg-01**. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.

🔒 Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory.

- [Instructions for cloud-only user accounts](#)
- [Instructions for synced user accounts](#)

To create an Azure inbound firewall policy:

1. Within the network security group, go to *Settings > Inbound Security Rules*, and click *Add*.
2. In *Add inbound security rule*, set the following:
 - a. **Source:** IP Address.
 - b. **Source IP address/CIDR ranges:** Set as the IP address/range that the inbound request will be originating from.
 - c. **Destination port ranges:** 636.
 - d. **Name:** Enter the name, for example AllowSecureLDAP.
 - e. **Description:** Add an optional description.
3. Leave all other settings as their default values, and click *Add*.

To obtain the LDAPS IP address:

1. Go to Azure AD Directory Services, and select the Azure domain.
2. Go to *Settings > Properties*. Note down the Secure LDAP external IP address.

Provision the remote LDAP server on FortiAuthenticator

To provision the remote LDAP server:

1. In FortiAuthenticator, go to *Authentication > Remote Auth. Servers > LDAP*, and click *Create New*.
2. In the *Create New LDAP Server* window, set the following:
 - a. **Name:** Enter a name, for example azure.fortixpert.com.
 - b. **Primary server name/IP:** Enter the Secure LDAP IP.
 - c. **Bind type:** *Regular*.
 - d. **Username/Password:** Enter a username and password that can access MS Azure DS to perform directory lookups.

- e. **Base distinguished name:** Leave blank.
3. In the *Query Elements* section, set the following:
 - a. **Pre-defined templates:** Select *Microsoft Active Directory* and click *Apply*.
 - b. **Force use of administrator account for group membership lookups:** Enabled.
4. In the *Secure Connection* section, set the following
 - a. **Secure Connection:** Enabled.
 - b. **Protocol:** *LDAPS*.
 - c. **CA Certificate:** Select the Root CA certificate for the wildcard certificate that was uploaded to MS Azure to use with the Secure LDAP connector.
5. Select the lookup icon next to *Base distinguished name*. Choose the base DN for your user accounts, for example *DC=fortixpert,DC=com*. Click *OK*.

Name: azure.fortixpert.com

Primary server name/IP: 13.75.227.41 Port: 636

☐ Use secondary server

Base distinguished name: DC=fortixpert,DC=com

Bind type: Simple Regular

Username: ldapservice@fortixpert.com Password:

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

Query Elements

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

User object class: person

Username attribute: sAMAccountName

Group object class: group

Obtain group memberships from: User attribute Group attribute

Group membership attribute: memberOf

☒ Force use of administrator account for group membership lookups

Secure Connection

☒ Enable

Protocol: LDAPS STARTTLS

CA certificate: Sectigo_Root_CA | C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority

☐ Use Client Certificate for TLS Authentication

Windows Active Directory Domain Authentication

☐ Enable

Remote LDAP Users

Username	Token	Actions
Import users	Go	

OK Cancel

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

To import remote user accounts:

1. Go to *Authentication > User Management > Remote Users*. Confirm *LDAP* is selected at the top of the page, and click *Import*.
2. Under *Import Remote LDAP User*, complete the following:
 - a. **Remote LDAP Server:** Select the Azure remote LDAP server.
 - b. **Action:** Select *Import users*, and click *Go* to view a list of users within your Azure directory.

- c.** Select the users you wish to be able to connect to the wireless network using their Azure based account.

Import Remote LDAP Users

LDAP server: 13.75.227.41:636

Filter: (&(objectClass=user)(objectCategory=person))

☒ Filter child nodes and show number of children

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

- [-] CN=Users (3)
 - [+] CN=Guest Username=Guest
 - [+] CN=dcaasadmin Username=dcaasadmin
 - [+] CN=krbtgt Username=krbtgt
- [-] OU=AADDC Users (7)
 - [+] CN=Brian Andersen First name=Brian, Last name=Andersen, Username=bandersen
 - [+] CN=Eric Mouque First name=Eric, Last name=Mouque, Username=emouque
 - [+] CN=John Battam (87B7184F) First name=John, Last name=Battam, Username=jbattam (87B7184F)
 - [+] CN=Vincent Ribiere First name=Vincent, Last name=Ribiere, Username=vribiere
 - [+] CN=jbattam@fortinet.com Battam First name=jbattam@fortinet.com, Last name=Battam, Username=jbattam (0BF202CE)
 - [+] CN=labb1 First name=Lob, Last name=1, Username=labb1
 - [+] CN=ldap First name=ldap, Last name=service, Username=ldapservice

Distinguished name: DC=fortixpert,DC=com

Organization: [Please Select]

- 3.** Click *OK*.

To set up a remote user sync rule:

1. Go to *Authentication > User Management > Remote User Sync Rule*, and click *Create New*.
2. Under *Create New Remote LDAP User Synchronization Rule*, set the following:
 - a. **Name**: Enter a name, for example *Azure_Remote_Sync*.
 - b. **Remote LDAP**: Select your Azure remote LDAP server.
 - c. **Base distinguished name**: This setting can be left as the default, for example *DC=fortixpert,DC=com*.
3. Under *Synchronization Attributes*, set the following:
 - a. **Token-based authentication sync priorities**: Enable *None*.
 - b. **Sync every**: Select the sync frequency. In production environments, this should be set to 30 minutes or more depending on the number of users being synchronized.
 - c. **Sync as**: *Remote LDAP User*.
 - d. **User role for new user imports**: *User*.
4. Leave all other settings in their default states, and click *OK*.

To create a new realm:

1. Go to *Authentication > User Management > Realms*, and click *Create New*.
2. Under *Create New Realm*, set the following:
 - a. **Name**: Enter the realm name, for example fortixpert.com.
 - b. **User source**: Select the remote LDAP service from the dropdown box.
3. Click *OK*.

Configure Smart Connect and the captive portal

This section outlines the configuration required on FortiAuthenticator to provision a Captive Portal using Smart Connect authenticating against MS Azure AD DS.

To configure Smart Connect and portals on FortiAuthenticator:

1. [Create the Smart Connect profile on page 325](#)
2. [Create the captive portal on page 326](#)
3. [Create the self-service portal policy on page 327](#)

Create the Smart Connect profile

To create Smart Connect profiles:

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

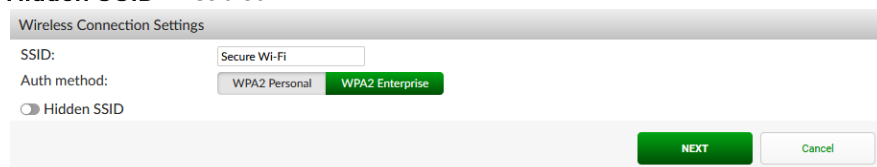


General Information

Name:

Connect type: ☒ Wireless

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



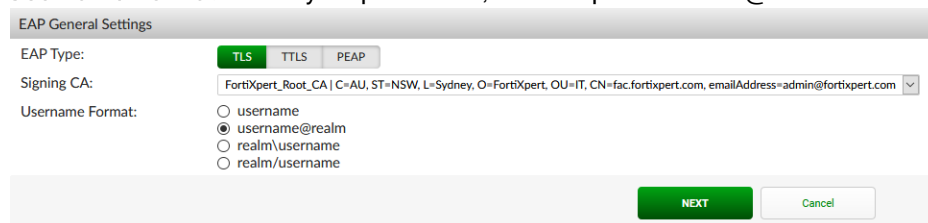
Wireless Connection Settings

SSID:

Auth method: ☐ WPA2 Personal ☒ WPA2 Enterprise

☐ Hidden SSID

4. Under *EAP General Settings*, set the following and then click *Next*.
 - a. **EAP Type:** *TLS*.
 - b. **Signing CA:** Select the local Root CA configured earlier.
 - c. **Username Format:** Select your preference, for example *username@realm*.



EAP General Settings

EAP Type: ☒ TLS ☐ TTLS ☐ PEAP

Signing CA:

Username Format: ☐ username ☒ username@realm ☐ realm\username ☐ realm/username

5. Under *Certificate Installation Settings*, set the following and then click *OK*.
 - a. **Install local CA certificates:** Choose to install the local *Root_CA* certificate.
 - b. **Install trusted CA certificates:** Choose to install any certificate that is required for all relevant certificate chains to be fully trusted.

Certificate Installation Settings

Install local CA certificates:

Available Install Local CA Certificates

Filter

Choose all

Selected Install Local CA Certificates

FortiXpert_Root_CA | C=AU, ST=NSW, L=Sydney

Remove all

Install trusted CA certificates:

Available Install Trusted CA Certificates

Filter

Choose all

Selected Install Trusted CA Certificates

Fortinet_CA1_Root | C=US, ST=California, L=Sunr
 Fortinet_CA2_Intermediate | C=US, ST=California, L=Sunr
 Fortinet_CA2_Root | C=US, ST=California, L=Sunr
 Go_Daddy_Class_2_CA | C=US, O="The Go Dadd
 Go_Daddy_Root_CA_G2 | C=US, ST=Arizona, L=S
 Go_Daddy_Secure_CA_G2 | C=US, ST=Arizona, L=S
 Google_RootCA_GSR2 | OU=GlobalSign Root CA
 Sectigo_RSA_DV_Secure_Server_CA | C=GB, ST=I
 Sectigo_Root_CA | C=US, ST=New Jersey, L=Jerse

Remove all

OK Cancel

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

Create the captive portal

To create a captive portal:

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

FortiAuthenticator VM FAC-VM000000000000

System > Create New Portal

Authentication > User Account Policies > User Management > Self-service Portal > Portals

Name: Smart Connect Portal

Description: Captive Portal to be used for Smart Connect user onboarding.

General

SMS gateway: Use default

Pre-login Services

☐ Disclaimer

☐ Password Reset

☐ Account Registration

☐ Token Revocation

☐ Usage Extension Notifications

Post-login Services

☐ Profile

☐ Password Change

☐ Token Registration

☒ Smart Connect

Smart connect profile: Smart Connect | Add a smart connect profile

☐ Device Tracking and Management

OK Cancel

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.

The screenshot shows the FortiAuthenticator VM web interface. The left sidebar has a tree view with 'Authentication' expanded, then 'Portals', and finally 'Policies'. The main content area is titled 'Policy type' and shows the following configuration:

- Name:** SmartConnect
- Description:** Smart Connect Portal - User Onboarding Policy
- URL:** https://fac.fortixpert.com/portal/selfservice/SmartConnect/
- Portal:** Smart Connect Portal

At the bottom of the configuration area are three buttons: 'Discard and exit', 'Update and exit', and 'Next'.

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.

The screenshot shows the FortiAuthenticator VM web interface with the 'Identity sources' tab selected. The configuration is as follows:

- Local/Remote Users:**
 - ☒ Local/Remote Users
 - ☐ Username format: username@realm
 - ☐ realm/username
 - ☐ realm/username
- Realms:**

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	fortixpert.com azure.fortixpert.com (13.75.227.41)	☐		

Below the table is a button: '+ Add a realm'.

At the bottom are four buttons: 'Previous', 'Discard and exit', 'Update and exit', and 'Next'.

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 329](#)
2. [Create the user group for cloud-based directory user accounts on page 329](#)
3. [Provision the Onboarding and Secure WiFi networks on page 330](#)

Configure the RADIUS server on FortiGate

To configure the RADIUS server:

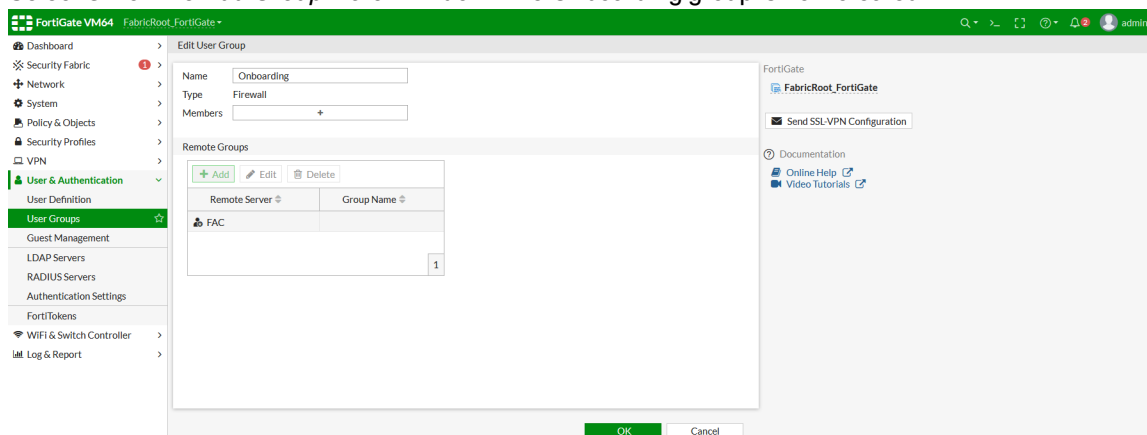
1. In FortiGate, go to *User & Authentication > RADIUS Servers*, and click *Create New*.
2. Under *New RADIUS Server*, set the following:
 - a. **Name:** Enter a name for the RADIUS server, for example FAC.
 - b. **NAS IP:** Enter the Network Access Server (NAS) IP. This should ideally be the IP from 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.

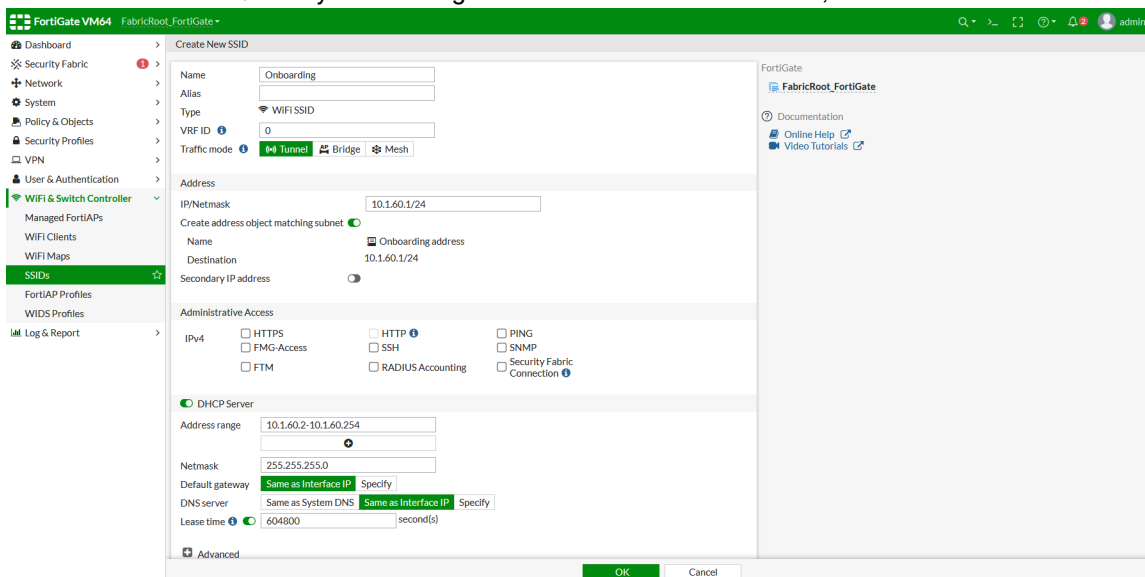
3. Select *OK* on the *Add Group Match* window. The Onboarding group is now created.



Provision the Onboarding and Secure WiFi networks

To provision the Smart Connect enabled "Onboarding" SSID:

- Go to *Wi-Fi & Switch Controller > SSID*, and click *Create New*.
- Under *Create New SSID*, set the following:
 - Profile name:** Enter a name for the profile, for example Onboarding.
 - Traffic mode:** *Tunnel*.
- Under *Address*, set the following:
 - IP/Netmask:** Enter the interface IP address for the Onboarding SSID.
- Under *DHCP Server*, enable the DHCP Server setting and set the following:
 - Leave *Address range*, *Netmask*, *Gateway*, and *Lease time* in their default states.
 - 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.

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar shows the navigation menu with 'WiFi & Switch Controller' selected. The main panel displays the 'Create New SSID' dialog for 'Onboarding'. The settings are as follows:

- SSID:** Onboarding
- Client limit:** Off
- Broadcast SSID:** On
- Security Mode Settings:**
 - Security mode:** Captive Portal
 - Portal type:** Authentication
 - Authentication portal:** External (URL: https://fac.fortixpert.com/portal/selfser)
 - User groups:** Onboarding
 - Exempt sources:** (empty)
 - Exempt destinations/services:** FortiAuthenticator
 - Redirect after Captive Portal:** Original Request
- Client MAC Address Filtering:**
 - RADIUS server:** Off
- Additional Settings:**
 - Schedule:** always
 - Block Intra-SSID traffic:** Off
 - Broadcast suppression:** On
 - ARPs for known clients: Off
 - DHCP unicast: Off
 - DHCP uplink: Off
 - Quarantine host:** On
 - VLAN pooling:** Off
- Traffic Shaping:**
 - Outbound shaping profile:** Off
- Miscellaneous:**
 - Comments:** (empty)
 - Status:** Enabled

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

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.

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar contains a navigation menu with options like Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, and WiFi & Switch Controller. The main area displays the 'Edit Interface' configuration for 'Secure Wi-Fi (Secure Wi-Fi)'. The configuration is organized into several sections: General (Name, Alias, Type, VRF ID, Traffic mode), WiFi Settings (SSID, Client limit, Broadcast SSID), Security Mode Settings (Security mode, Authentication, Client MAC Address Filtering), Additional Settings (Local standalone, Dynamic VLAN assignment, Schedule, Block Intra-SSID traffic, Optional VLAN ID, Security profile group, Broadcast suppression, VLAN pooling), and Miscellaneous (Comments, Status). The 'Status' is currently 'Enabled'.

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: 0/255
 Platform: FAPU422EV
 Country / Region: Australia
 AP login password:
 Administrative access: ☒ HTTPS ☒ SSH ☒ SNMP
 Client load balancing: ☒ Frequency Handoff ☐ AP Handoff

Radio 1

Mode:
 WIDS profile: ☐
 Radio resource provision: ☒
 Band: 2.4 GHz
 Channel width: 20MHz
 Short guard interval: ☒
 Channels: ☒ 1 ☐ 6 ☐ 11
 TX power control:
 TX power: - dBm
 SSIDs:

 Monitor channel utilization: ☒

Radio 2

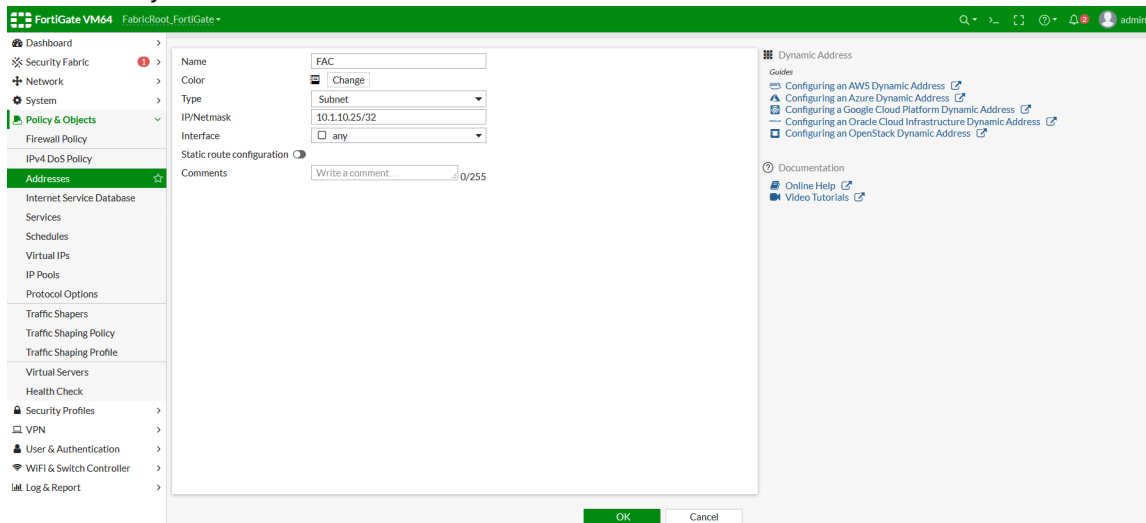
Mode:
 WIDS profile: ☐
 Radio resource provision: ☒
 Band: 5 GHz
 Channel width:
 Short guard interval: ☒
 Channels:

☐ 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

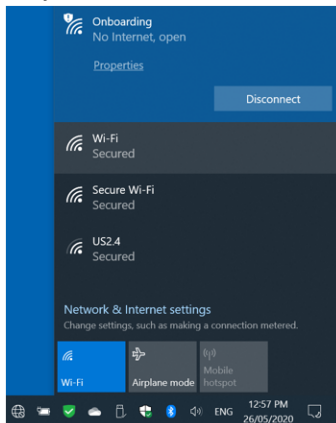
You can now connect your device to the Onboarding SSID and proceed with the Smart Connect onboarding process:

- [Smart Connect Windows device onboarding process on page 338](#)
- [Smart Connect iOS device onboarding process on page 340](#)

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.

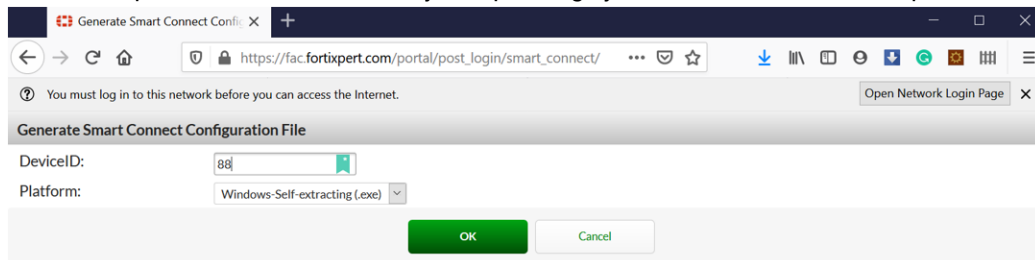
2. Enter either your Google Workspace or Azure login credentials, and select *Login*. Once logged in, select *Smart Connect*.

FORTINET

Welcome to FortiAuthenticator Guest Portal
Logged in as: labuser

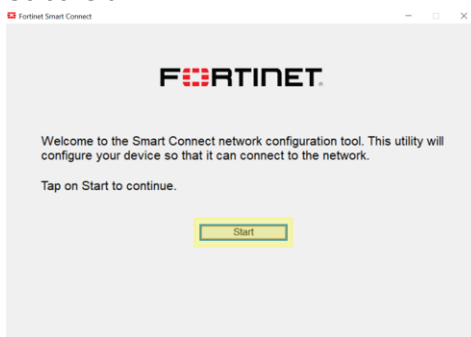


3. Enter a unique *Device ID* and choose your operating system from the *Platform* dropdown. Click *OK*.



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.

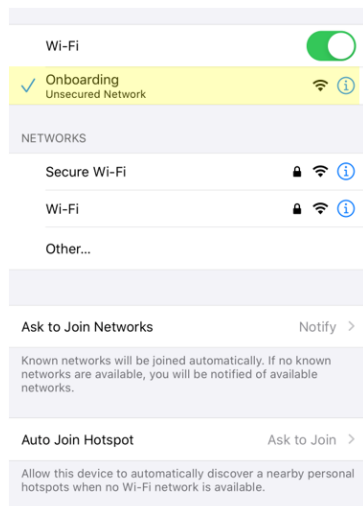
6. Once provisioning is complete, click *Connect*. Your device will now connect to the Secure Wi-Fi network using WPA2 and EAP-TLS.

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.



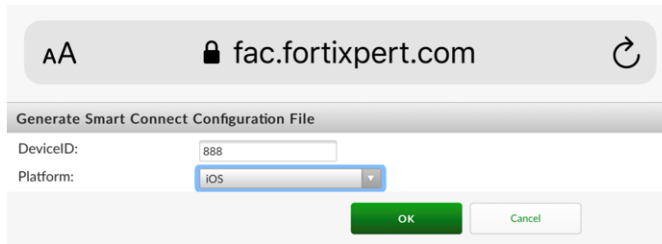
The FortiAuthenticator login screen is displayed.

2. Enter either your Google Workspace or Azure login credentials, and select *Login*. Once logged in, select *Smart Connect*.

FORTINET.



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



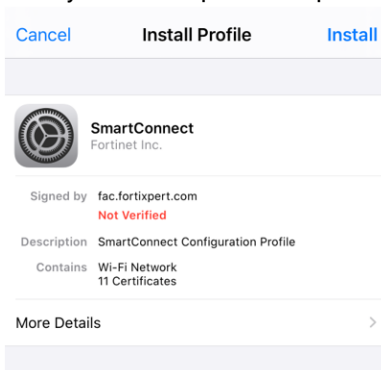
Generate Smart Connect Configuration File

DeviceID: 888

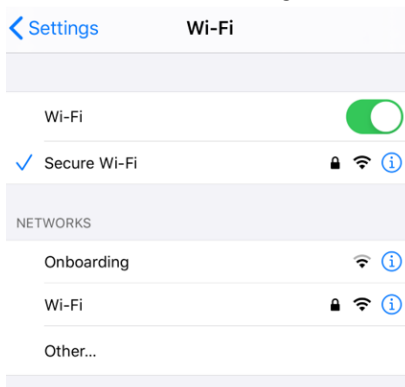
Platform: IOS

OK Cancel

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.



ZTNA

This section describes configuring ZTNA using FortiAuthenticator.

Setting up a zero trust tunnel

A zero trust tunnel allows FortiAuthenticator to securely access TCP-based-on-premise services from the public internet. Further, using zero trust tunnels, you can access an on-premise LDAP/AD server.

In this example, FortiAuthenticator forms a zero trust tunnel to a remote ZTNA server, i.e., a FortiGate device.

To set up a zero trust tunnel:

1. [Configuring a zero trust tunnel on FortiAuthenticator on page 342](#)
2. [Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator on page 343](#)
3. [Configuring certificate authentication for FortiAuthenticator on page 343](#)
4. [Configuring a ZTNA server on page 346](#)
5. [Configuring a ZTNA rule on page 347](#)
6. [Debugging on page 348](#)

Configuring a zero trust tunnel on FortiAuthenticator

To configure a zero trust tunnel:

1. Go to *System > Network > Zero Trust Tunnels*.
2. Select *Create New*.
The *Create New Zero Trust Tunnel* window opens.
3. In *Name*, enter a name for the zero trust tunnel.
4. In *URL*, enter a URL specifying the IP/FQDN and port for the ZTNA server, e.g., `https://fac.school.net:8443/`.
5. In the *Client certificate* dropdown, select a certificate.
This certificate is used to authenticate to the ZTNA server. In this example, it is generated by the FortiAuthenticator CA. See [Server Certificate](#).
6. Click *OK*.



Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator

To configure an LDAP server:

1. Go to *Authentication > Remote Auth. Servers > LDAP*, and select *Create New*.
2. In *Create New LDAP server*:
 - a. In *Name*, enter a name.
 - b. Enable *Use Zero Trust tunnel* and from the dropdown select the zero trust tunnel configured in [Configuring a zero trust tunnel on FortiAuthenticator on page 342](#).
 - c. In *Primary Server IP*, enter the IP address/FQDN of the LDAP server.
 - d. In *Port*, enter the port number of the LDAP server.
 - e. In *Base distinguished name*, enter a base distinguished name.
 - f. In *Bind Type*, select *Regular*.

Enter the username and password for the LDAP server administrator account.

3. Click *OK*.

Configuring certificate authentication for FortiAuthenticator

To configure a local root CA:

1. Go to *Certificate Management > Certificate Authorities > Local CAs*, and select *Create New*.
The *Create New Local CA Certificate* window opens.
2. In *Certificate ID*, enter a unique ID for the CA.
3. Ensure that the *Certificate type* is *Root CA*.
4. In *Name(CN)*, enter the subject name, e.g., a domain name.
5. Click *OK*.

To export the local root CA:

1. Go to *Certificate Management > Certificate Authorities > Local CAs*.
2. From the local CA certificate list, select the local root CA created in [Configuring a local root CA](#), and select *Export Certificate*.

The public certificate for the CA is downloaded to your computer, and the certificate is later imported to FortiGate. See [Importing local root CA](#).

To create a server certificate for FortiAuthenticator signed by the CA:

1. Go *Certificate Management > End Entities > Local Services*, and select *Create New*.
The *Create New Server Certificate* window opens.
2. In *Certificate ID*, enter a unique ID for the certificate.
3. In the *Certificate Signing Options* pane, ensure that the *Issuer* is *Local CA* and the *Certificate authority* is the local CA created in [Configuring a local root CA](#).
4. In the *Subject Information* pane, for *Name(CN)*, enter the FQDN of the FortiAuthenticator.
The certificate is used when configuring the zero trust tunnel. See [Configuring a zero trust tunnel on FortiAuthenticator on page 342](#).

To import the local root CA to FortiGate:

1. Go to *System > Certificates*, and from the *Create/Import* dropdown, select *CA Certificate*.
The *Import CA Certificate* window opens.
2. In *Type*, select *File*.
3. Select *Upload*, and locate the local root certificate created in [Configuring a local root CA](#) on your computer.
4. Click *OK*.



The imported root CA is available with the name `CA_Cert_X` where X denotes the number of certificates imported.

The *Issuer* field for the imported root CA is the *Name(CN)* you gave it.



To rename the root CA on FortiGate:

In the CLI console, enter the following commands:

```
config vpn certificate ca
  rename <cert> to <new name>
```

To create an address object on FortiGate for FortiAuthenticator and the LDAP server:

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



For FortiTrust Identity, 154.52.4.227 is the fixed WAN IP address for FortiAuthenticator Cloud to build zero trust tunnels into an on-prem environment.

Use the IP address with its subnet mask.

4. Click *OK*.
The address is used when [Configuring an authentication rule](#).
5. Go to *Policy & Objects > Addresses*, and from the *Create New* dropdown, select *Address*.
The *New Address* window opens.
6. In *Name*, enter a name for the address, e.g., lab-ad-address.

7. In *IP/Netmask*, enter the private IP address of the LDAP server with its subnet mask.
8. Click *OK*.

To configure an authentication scheme with user-cert enabled:

1. Go to *Policy & Objects > Authentication Rules*.
2. From the *Create New* dropdown, select *Authentication Schemes*.
The *New Authentication Scheme* window opens.
3. In *Name*, enter a name for the authentication scheme.
4. In *Method*:
 - a. Select *+* to open the *Select Entries* window.
 - b. Select *Certificate*.
 - c. Select *Close*.
5. Click *OK*.

Alternatively, in the CLI console, enter the following commands:

```
config authentication scheme
  edit "test_scheme" #The authentication scheme name
    set method cert
    set user-cert enable
  next
end
```

To configure an authentication rule that uses the authentication scheme:

1. Go to *Policy & Objects > Authentication Rules*.
2. From the *Create New* dropdown, select *Authentication Rules*.
The *Add New Rule* window opens.
3. In *Name*, enter a name for the authentication rule.
4. In *Source Address*:
 - a. Select *+* to open the *Select Entries* window.
 - b. Search and select the address object for FortiAuthenticator. See [Address object for FortiAuthenticator](#).
 - c. Select *Close*.
5. In *Incoming interface*:
 - a. From the dropdown, select the external interface used in [Configuring a ZTNA server on page 346](#).
6. Enable *Authentication Scheme* and from the dropdown select the authentication scheme created in [Creating an authentication scheme](#).
7. Set *IP-based Authentication* as *Disable*.
8. Click *OK*.

Alternatively, in the CLI console, enter the following commands:

```
config authentication rule
  edit "Cert-Auth-Rule" #The authentication rule name
    set srcintf "port1"
    set srcaddr "fac"
    set ip-based disable
    set active-auth-method "test_scheme" #The authentication scheme
  next
end
```


To configure authentication setting to use the CA that issued the client certificate as the user-cert-ca:

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


```
config authentication setting
  set user-cert-ca "FAC_Cloud" #The CA certificate being used for client certificate
  verification
end
```

Configuring a ZTNA server

To configure a ZTNA server:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Servers* tab.
2. Select *Create New*.
The *New ZTNA Server* window opens.
3. In *Type* select *IPv4*.



Once set up, *Type* cannot be changed when editing the ZTNA server.

4. In *Name*, enter a name for the server.
5. In the *Network* pane:
 - a. In *External interface* dropdown, select an external interface.
Select *Create* to create a new interface.
 - b. In *External IP*, enter the external IP address that the ZTNA clients, e.g., FortiAuthenticator, connect to.
 - c. In *External port*, enter the port number that the ZTNA clients, e.g., FortiAuthenticator, connect to, e.g., 8443.
6. In *Services and Servers* pane:
 - a. In *Default certificate* dropdown, select *Fortinet_Factory*.
Clients are presented with this certificate when they connect to the access proxy VIP.
 - b. In *Service/server mapping*, select *Create new*.
The *New Service/Server Mapping* window opens.
 - i. In *Type*, select *IPv4*.



All hosted servers must be the same address type. The address type cannot be changed after the mapping is created.

- ii. In *Service*, select *TCP Forwarding*.
 - iii. In the *Servers* pane, add a server by selecting *Create new*.
Select an address and enter a port number for the LDAP server, e.g., lab-ad-address and 389.
-



The address and the port number must match the *Primary Server IP* and *Port* when [Configuring an LDAP server with zero trust tunnel enabled on FortiAuthenticator on page 343](#).



By default, LDAP uses port 389.

Click *OK*.

iv. Click *OK*.

7. Click *OK*.

The screenshot shows the 'New ZTNA Server' configuration window. The 'Type' is set to 'IPv4'. The 'Name' is 'zserver'. The 'Network' section shows 'External Interface' as 'port1', 'External IP' as '192.168.1.1', and 'External port' as '8443'. The 'SAML' section is disabled. The 'Services and Servers' section shows 'Default certificate' as 'Fortinet_Factory'. The 'Service/server mapping' section contains a table with one entry: 'TCP Forwarding' with URL '/tcp', Type 'IPv4', and # Real Servers '1'. The 'OK' button is highlighted.

Configuring a ZTNA rule

To configure a ZTNA rule:

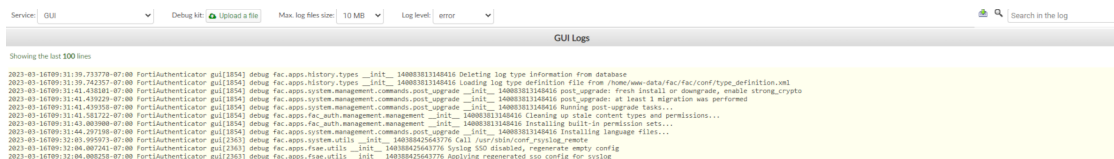
1. Go to *Policy & Objects > ZTNA* and select *ZTNA Rules* tab.
2. Select *Create New*.
The *New ZTNA Rule* window opens.
3. In *Name*, enter a name for the ZTNA rule.
4. In *Incoming Interface*, select the same interface as selected in [Configuring a ZTNA server on page 346](#).
5. In *Source*, select *+*, and from the *Select Entries* list, select the address object for FortiAuthenticator. See [Address object for FortiAuthenticator](#), and select *Close*.
6. In *ZTNA Server*, select the server created in [Configuring a ZTNA server on page 346](#).
7. In *Destination*, select *+*, and from the *Select Entries* list, either select or create a destination.

8. Click **OK**.

Debugging

Go to <https://<FortiAuthenticator-IP-Address>/debug> and select **GUI** from the **Service** dropdown to see extended FortiAuthenticator debug logs.

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



To access WAD debug categories and set them to the maximum level in a FortiGate ZTNA server, use `diagnose wad debug enable all` CLI command.

- cert-status: failure**

```
wad_vs_ssl_access_proxy_on_clt_certs:11553 1:ZTNA-LDAP: received certs from the client.
wad_ssl_cert_auth_find      :60  find wad_ssl_cert_auth_info fail by timeout 1654239602
wad_ssl_cert_auth_find      :78  Can't find auth_info!
wad_vs_ssl_access_proxy_on_clt_certs:11557 1:ZTNA-LDAP: cert cache cert(0x343ab124) authi(0x336054c0)
wad_vs_ssl_access_proxy_on_clt_certs:11562 1:ZTNA-LDAP: vs, Found the cert, and issued by:trusted root!
wad_ssl_cert_check_auth_status_with_ca_store:305  authi(0x336054c0) status(0)
wad_ssl_validate_cert_by_ca_store :3193  !OK, cur(cert(0x3375943c)) err(20)
wad_vs_ssl_access_proxy_on_clt_certs: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:ww.fortinet.com, cert-status:failure
```

- cert-status: success**

```
wad_vs_ssl_access_proxy_on_clt_certs:11553 1:Terminator-ZTNA: received certs from the client.
__wad_ssl_cert_open_cert    :655  https server uses key_len 4096
wad_vs_ssl_access_proxy_on_clt_certs:11557 1:Terminator-ZTNA: cert cache cert(0x343beb28) authi(0x336bfa5c)
wad_vs_ssl_access_proxy_on_clt_certs:11580 1:Terminator-ZTNA: Empty EMS CAs!
wad_ssl_cert_check_auth_status_with_ca_store:305  authi(0x336bfa5c) status(0)
wad_ssl_validate_cert_by_ca_store :3275  Certificate verified!
wad_vs_ssl_access_proxy_on_clt_certs:11601 1:Terminator-ZTNA: Cert auth success. issued_by: cert-auth-case
```



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.