FortiAuthenticator - Cookbook

Version 6.0.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

October 25, 2019
FortiAuthenticator 6.0.0 Cookbook
23-600-570505-20191025

TABLE OF CONTENTS

Change Log **5**
Certificate management **6**
FortiAuthenticator as a Certificate Authority 6
Creating a new CA on the FortiAuthenticator 6
Installing the CA on the network 8
Creating a CSR on the FortiGate 12
Importing and signing the CSR on the FortiAuthenticator 13
Importing the local certificate to the FortiGate 14
Configuring the certificate for the GUI 14
Results 15
FortiAuthenticator Certificate with SSL Inspection 16
Creating a CSR on the FortiGate 16
Creating an Intermediate CA on the FortiAuthenticator 18
Importing the signed certificate on the FortiGate 18
Configuring full SSL inspection 19
Results 21
FortiToken and FortiToken Mobile **23**
FortiToken Mobile Push for SSL VPN 23
Adding a FortiToken to the FortiAuthenticator 24
Adding the user to the FortiAuthenticator 24
Creating the RADIUS client on the FortiAuthenticator 28
Connecting the FortiGate to the RADIUS server 29
Configuring the SSL VPN 32
Results 34
Self-service Portal **38**
FortiAuthenticator user self-registration 38
Creating a self-registration user group 38
Enabling self-registration 39
Creating a new SMTP server 42
Results - Self-registration 42
Results - Administrator approval 45
VPNs **48**
LDAP authentication for SSL VPN with FortiAuthenticator 48
Creating the user and user group on the FortiAuthenticator 48
Creating the LDAP directory tree on the FortiAuthenticator 50
Connecting the FortiGate to the LDAP server 50
Creating the LDAP user group on the FortiGate 51
Configuring the SSL VPN 53
Results 56
SMS two-factor authentication for SSL VPN 57
Creating an SMS user and user group on the FortiAuthenticator 58
Configuring the FortiAuthenticator RADIUS client 59
Configuring the FortiGate authentication settings 60
Configuring the SSL VPN 62

Creating the security policy for VPN access to the Internet ... 64
Results ... 64
WiFi authentication ... 68
Assigning WiFi users to VLANs dynamically ... 68
Configuring the FortiAuthenticator ... 69
Adding the RADIUS server to the FortiGate ... 70
Creating an SSID with dynamic VLAN assignment ... 71
Creating the VLAN interfaces ... 73
Creating security policies ... 77
Creating the FortiAP profile ... 78
Connecting and authorizing the FortiAP ... 80
Results ... 80
WiFi using FortiAuthenticator RADIUS with certificates ... 82
Creating a local CA on FortiAuthenticator ... 82
Creating a local service certificate on FortiAuthenticator ... 83
Configuring RADIUS EAP on FortiAuthenticator ... 84
Configuring RADIUS client on FortiAuthenticator ... 85
Configuring local user on FortiAuthenticator ... 86
Configuring local user certificate on FortiAuthenticator ... 87
Creating RADIUS server on FortiGate ... 88
Creating WiFi SSID on FortiGate ... 89
Exporting user certificate from FortiAuthenticator ... 93
Importing user certificate into Windows 10 ... 93
Configuring Windows 10 wireless profile to use certificate ... 97
Results ... 102
WiFi RADIUS authentication with FortiAuthenticator ... 105
Creating users and user groups on the FortiAuthenticator ... 106
Registering the FortiGate as a RADIUS client on the FortiAuthenticator ... 107
Configuring FortiGate to use the RADIUS server ... 108
Creating SSID and set up authentication ... 110
Connecting and authorizing the FortiAP ... 111
Creating the security policy ... 114
Results ... 115
WiFi with WSSO using FortiAuthenticator RADIUS and Attributes ... 115
Registering the FortiGate as a RADIUS client on the FortiAuthenticator ... 115
Creating users on the FortiAuthenticator ... 116
Creating user groups on the FortiAuthenticator ... 118
Configuring the FortiGate to use the FortiAuthenticator as the RADIUS server ... 120
Configuring user groups on the FortiGate ... 121
Creating security policies ... 122
Configuring the SSID to RADIUS authentication ... 124
Results ... 124
LDAP Authentication ... 126
G Suite integration using LDAP ... 126
Generating the G Suite certificate ... 126
Importing the certificate to FortiAuthenticator ... 127
Configuring LDAP on the FortiAuthenticator ... 129
Troubleshooting ... 131

Change Log

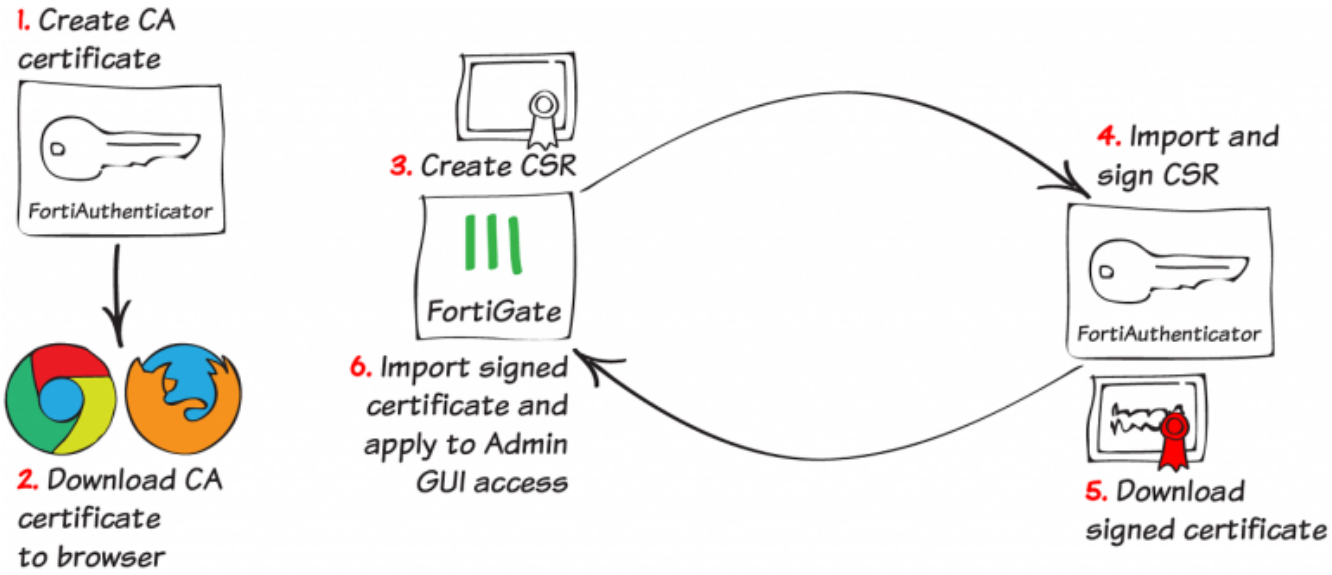
Date	Change Description
2019-09-05	Initial release.
20109-10-25	Added G Suite integration using LDAP on page 126.

Certificate management

This section describes managing certificates with the FortiAuthenticator device.

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

FortiAuthenticator as a Certificate Authority



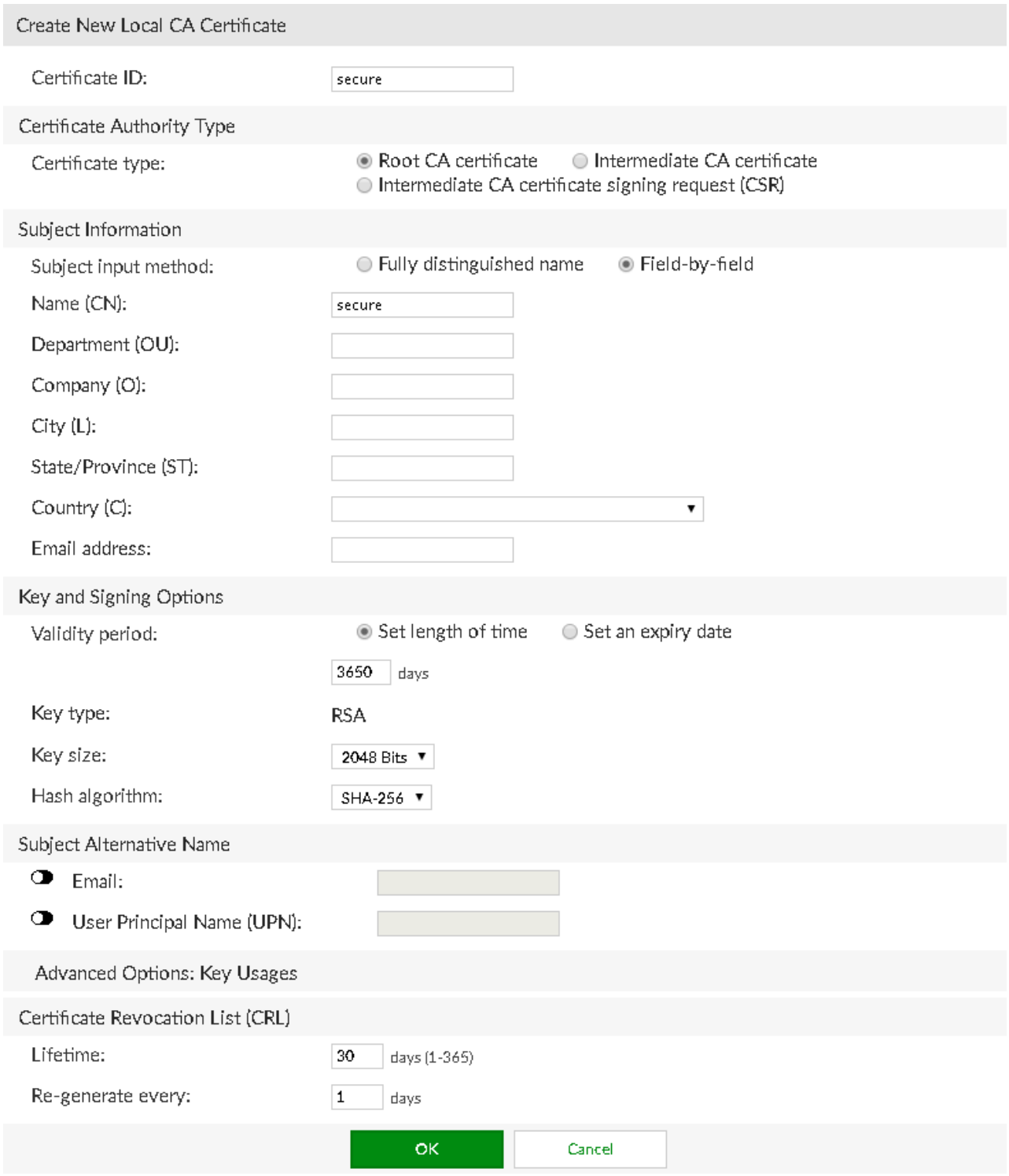
For this recipe, you will configure the FortiAuthenticator as a Certificate Authority (CA). This will allow the FortiAuthenticator to sign certificates that the FortiGate will use to secure administrator GUI access.

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.

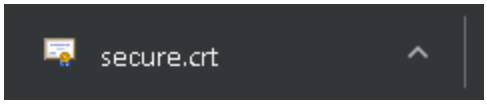
Creating a new CA on the FortiAuthenticator

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



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

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

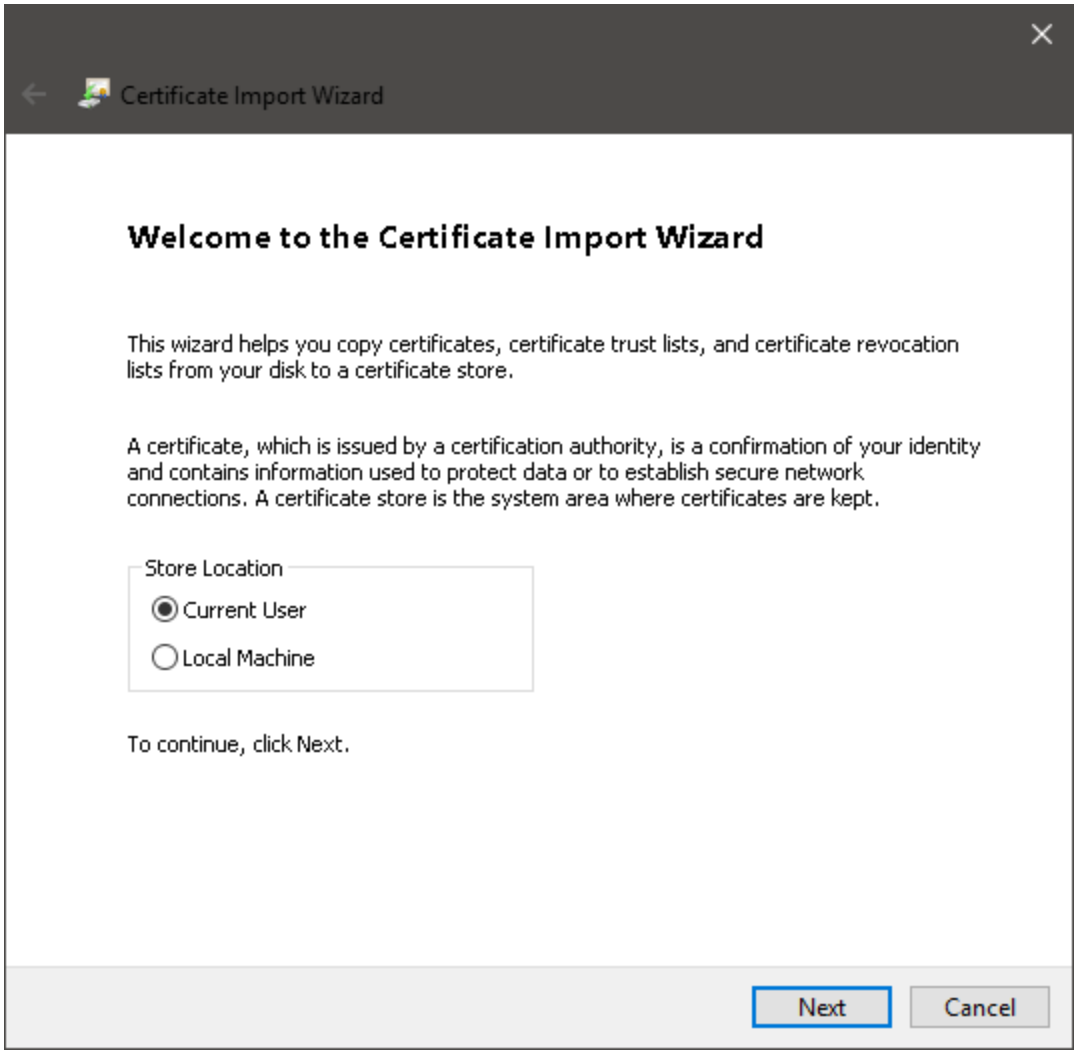


Installing the CA on the network

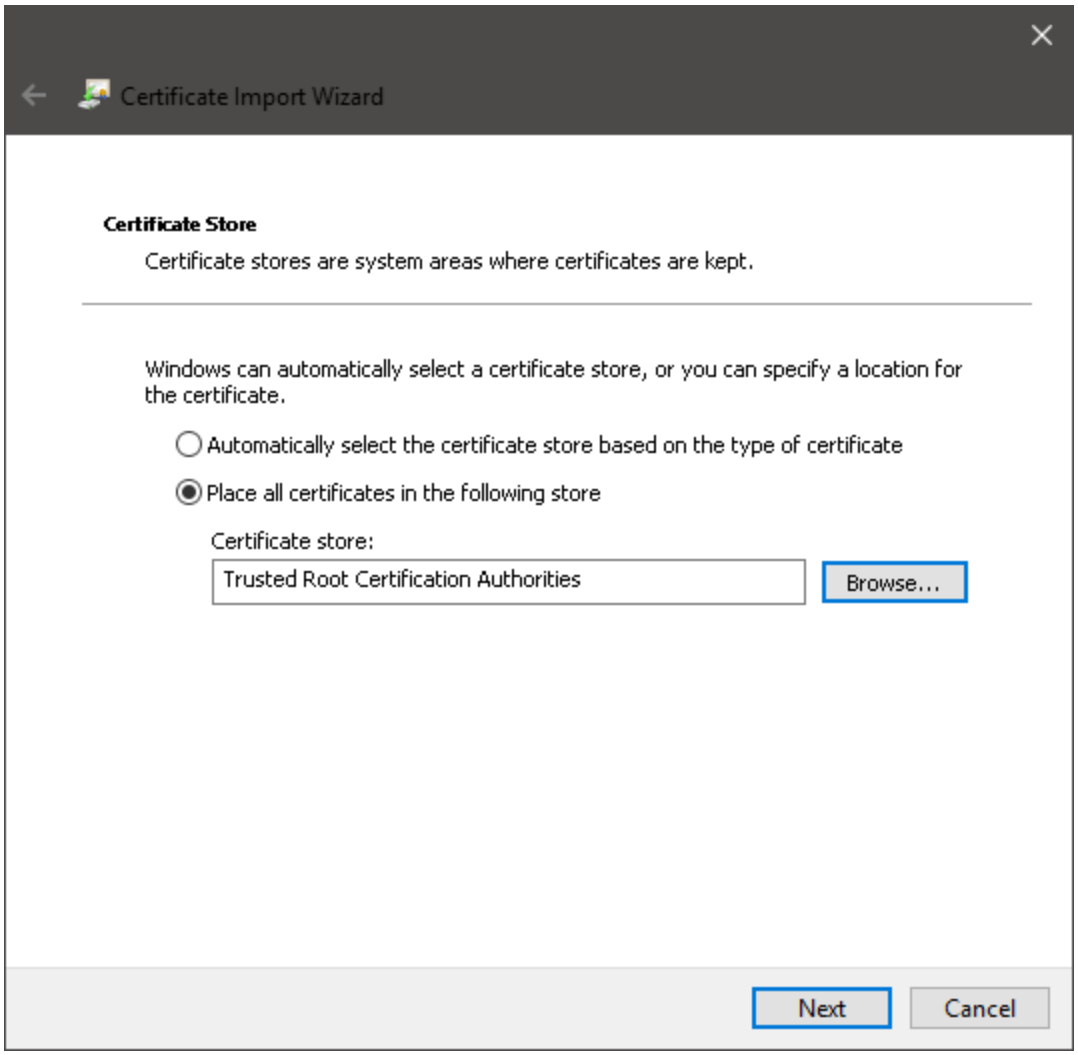
The certificate must now be installed on the computers in your network as a trusted root CA. The steps below show different methods of installing the certificate, depending on your browser.

Internet Explorer and Chrome

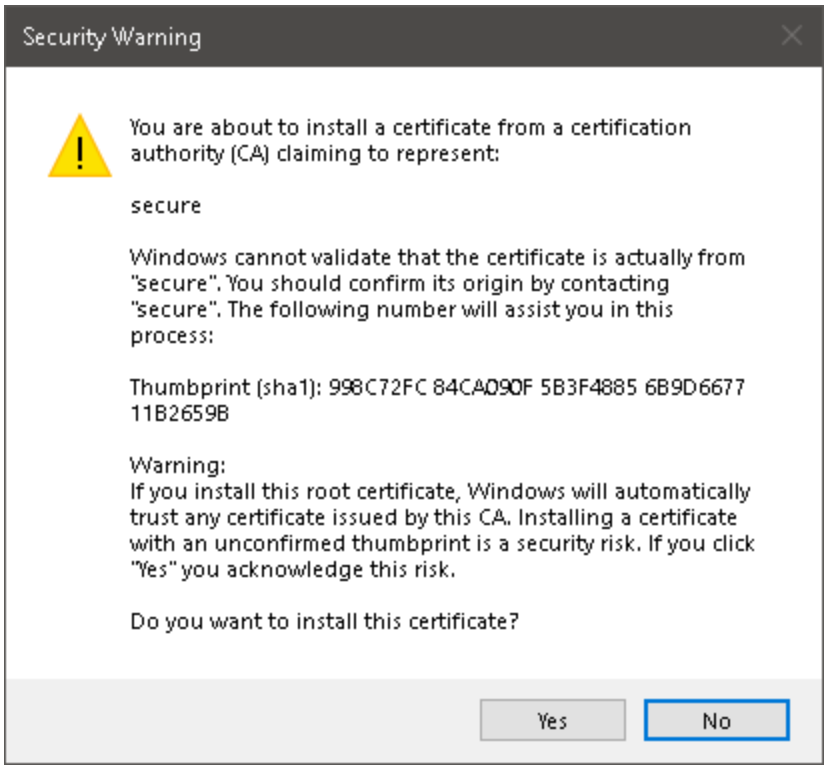
1. In Windows Explorer, right-click on the certificate and select **Install Certificate**. Open the certificate and follow the **Certificate Import Wizard**.



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

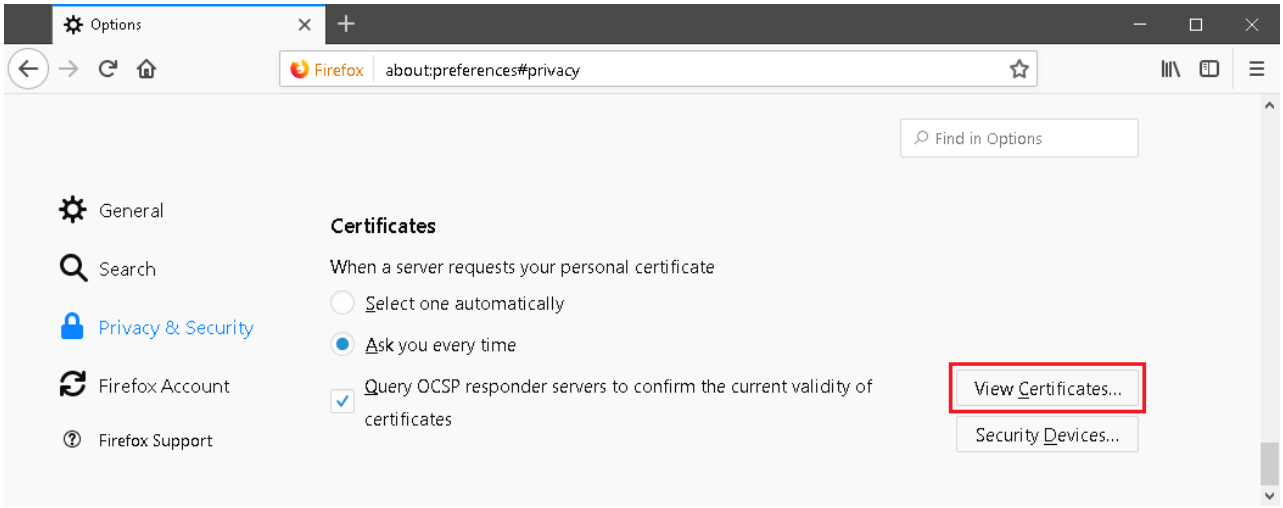


3. Finish the Wizard and select **Yes** to confirm and install the certificate.

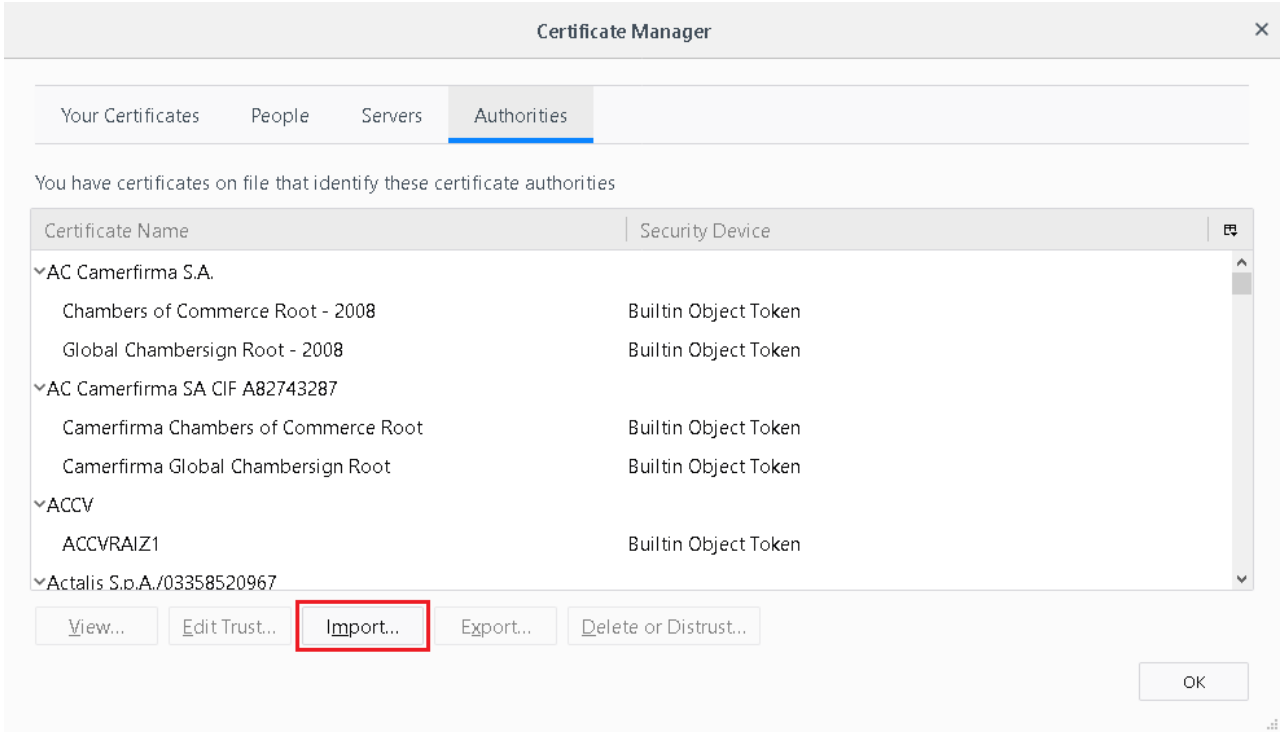


Firefox

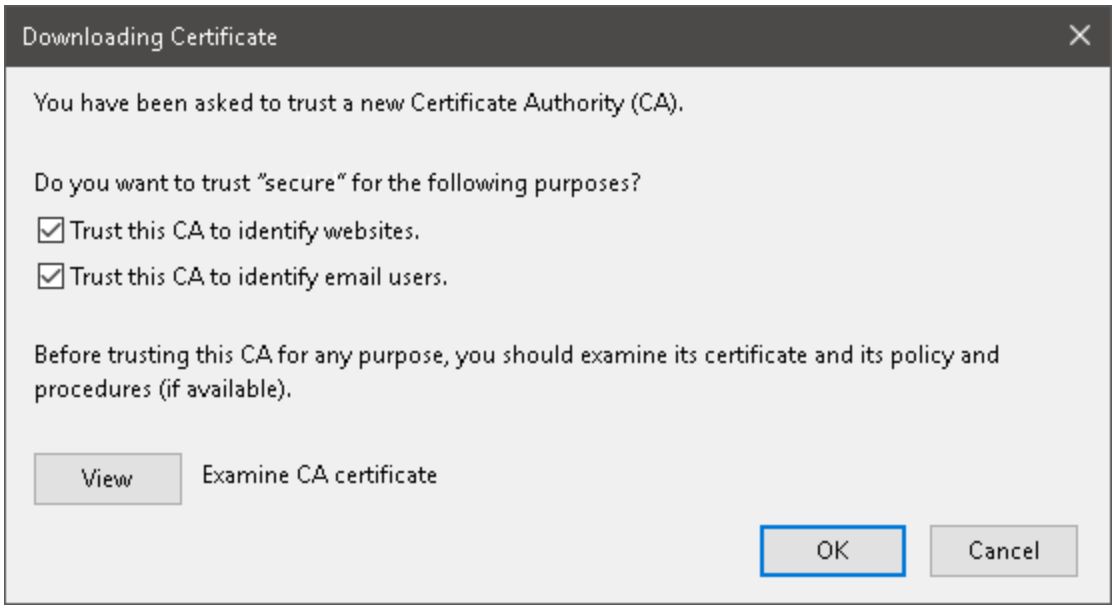
1. In the web browser, go to **Options > Privacy & Security > Certificates** and select **View Certificates**.



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

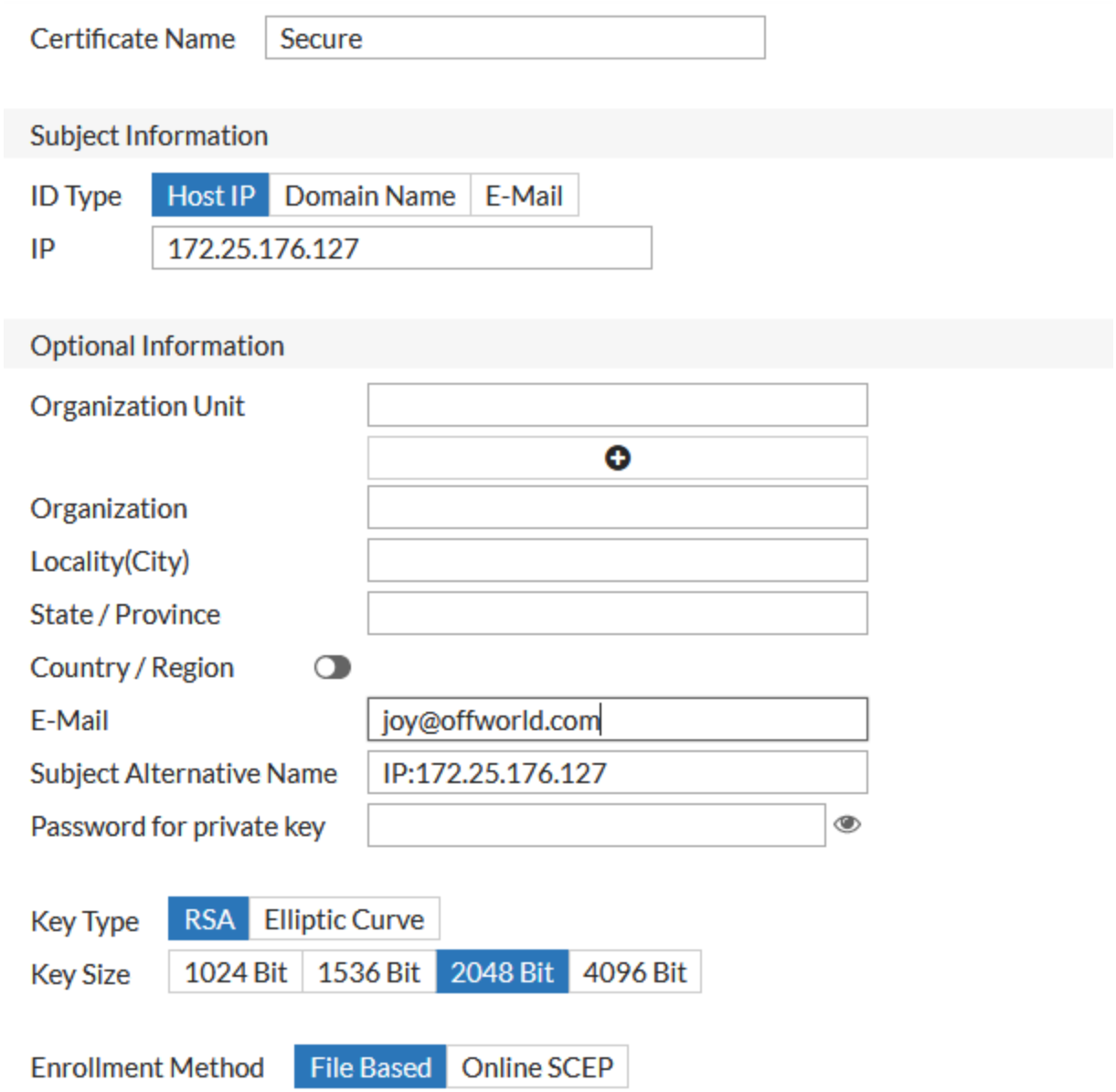


3. Find and open the root certificate.
   You will be asked what purposes the certificate will be trusted to identify. Select all options and select **OK**.

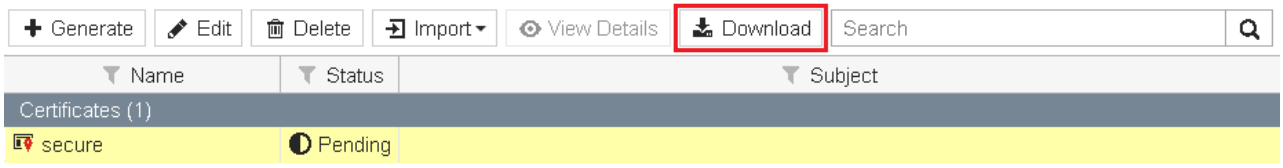


Creating a CSR on the FortiGate

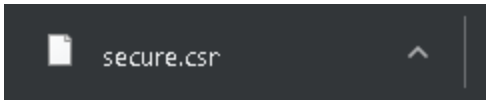
1. On the FortiGate, go to **System > Certificates** and select **Generate** to create a new certificate signing request (CSR).
   Enter a **Certificate Name**, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.
   The **Subject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



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

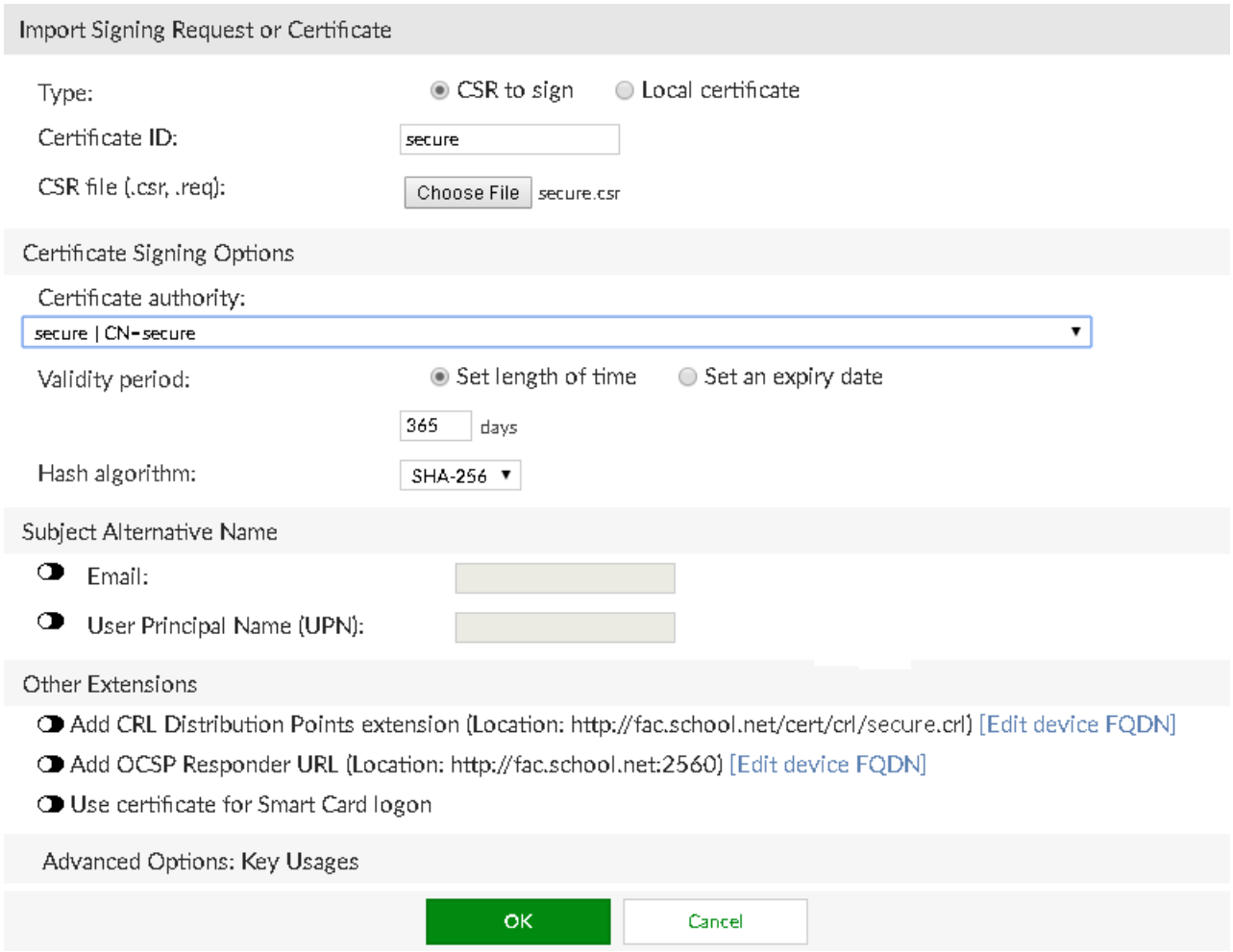


This will save a **.csr** file to your local drive.

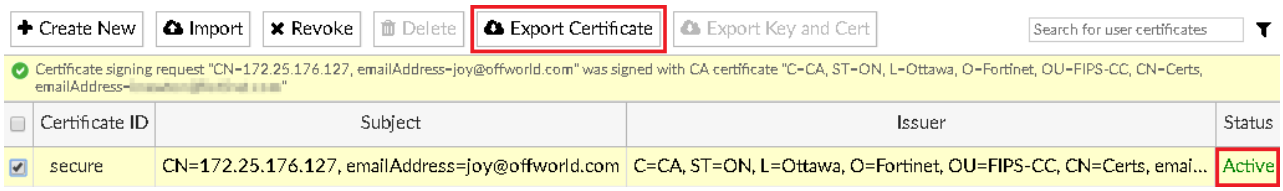


Importing and signing the CSR on the FortiAuthenticator

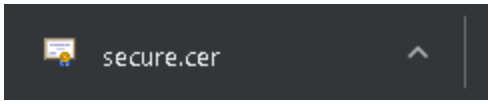
1. Back on the FortiAuthenticator, go to **Certificate Management > End Entities > Users** and import the **.csr** certificate created earlier.
   Make sure to select the **Certificate authority** from the drop-down menu and set the **Hash algorithm** to **SHA-256**, as configured earlier.



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

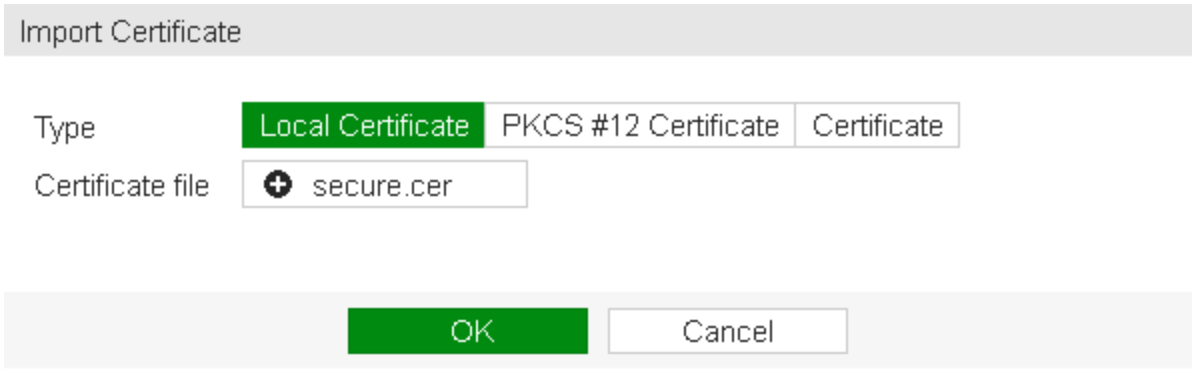


This will save a **.cer** file to your local drive.

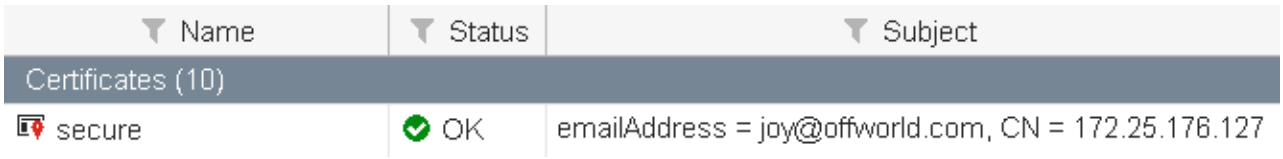


Importing the local certificate to the FortiGate

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



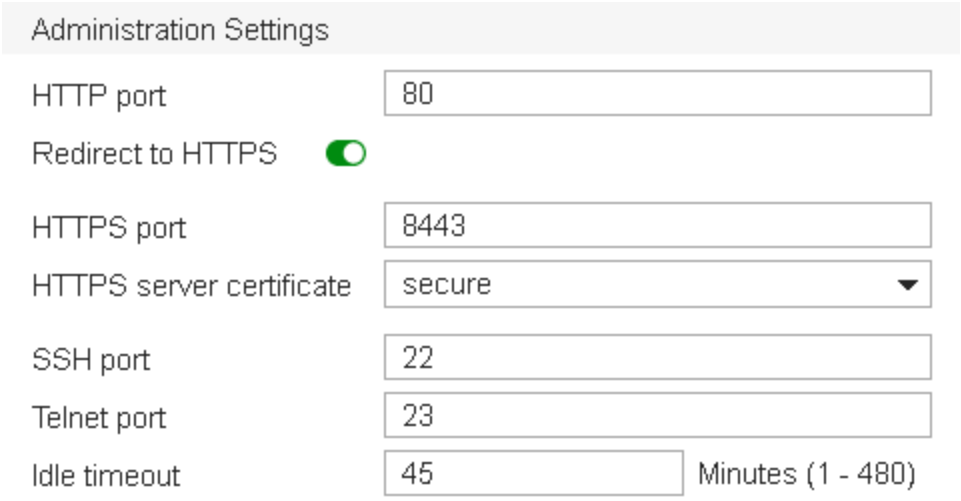
You should now see that the certificate's **Status** has changed from **Pending** to **OK**. You may have to refresh your page to see the status change.



Configuring the certificate for the GUI

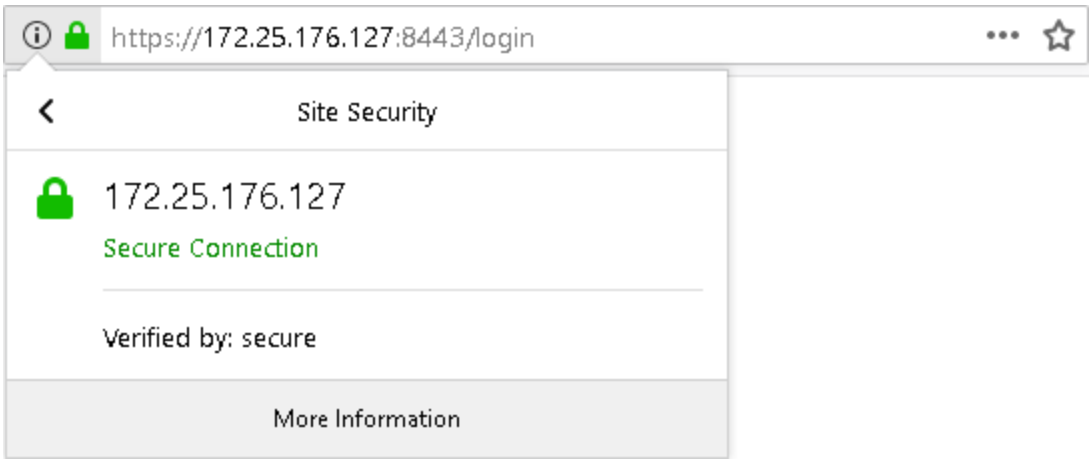
1. On the FortiGate, go to **System > Settings**.
   Under **Administration Settings**, set **HTTPS server certificate** to the certificate created/signed earlier, then

select **Apply**.

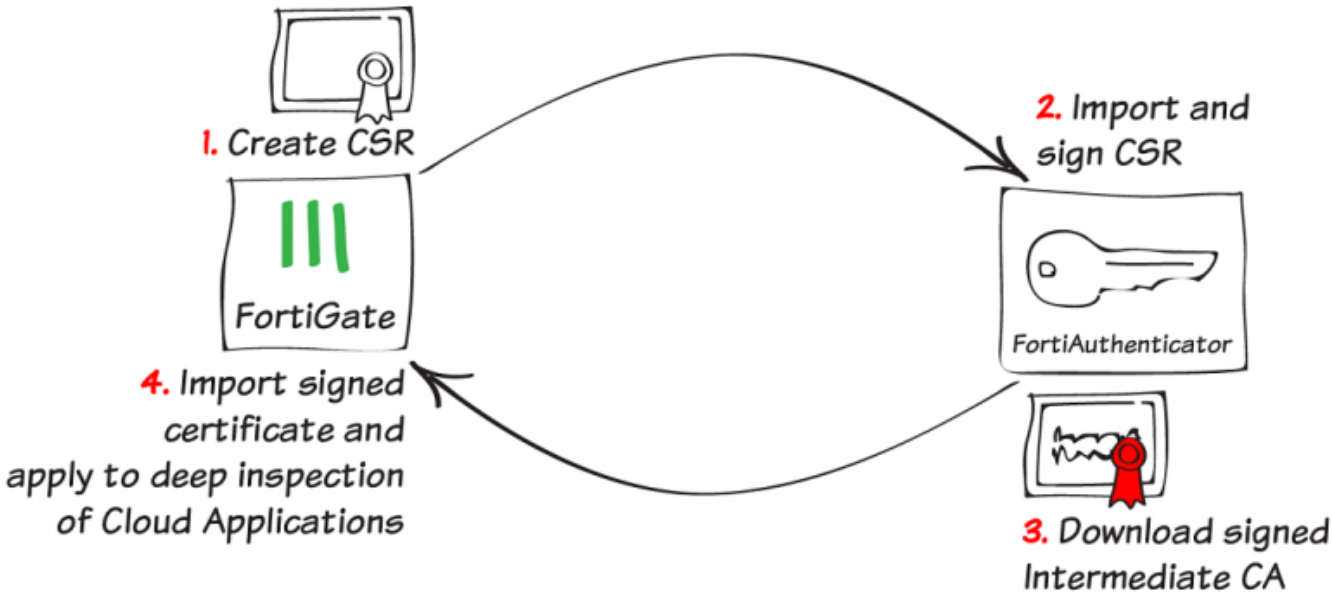


Results

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



FortiAuthenticator Certificate with SSL Inspection



For this 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.

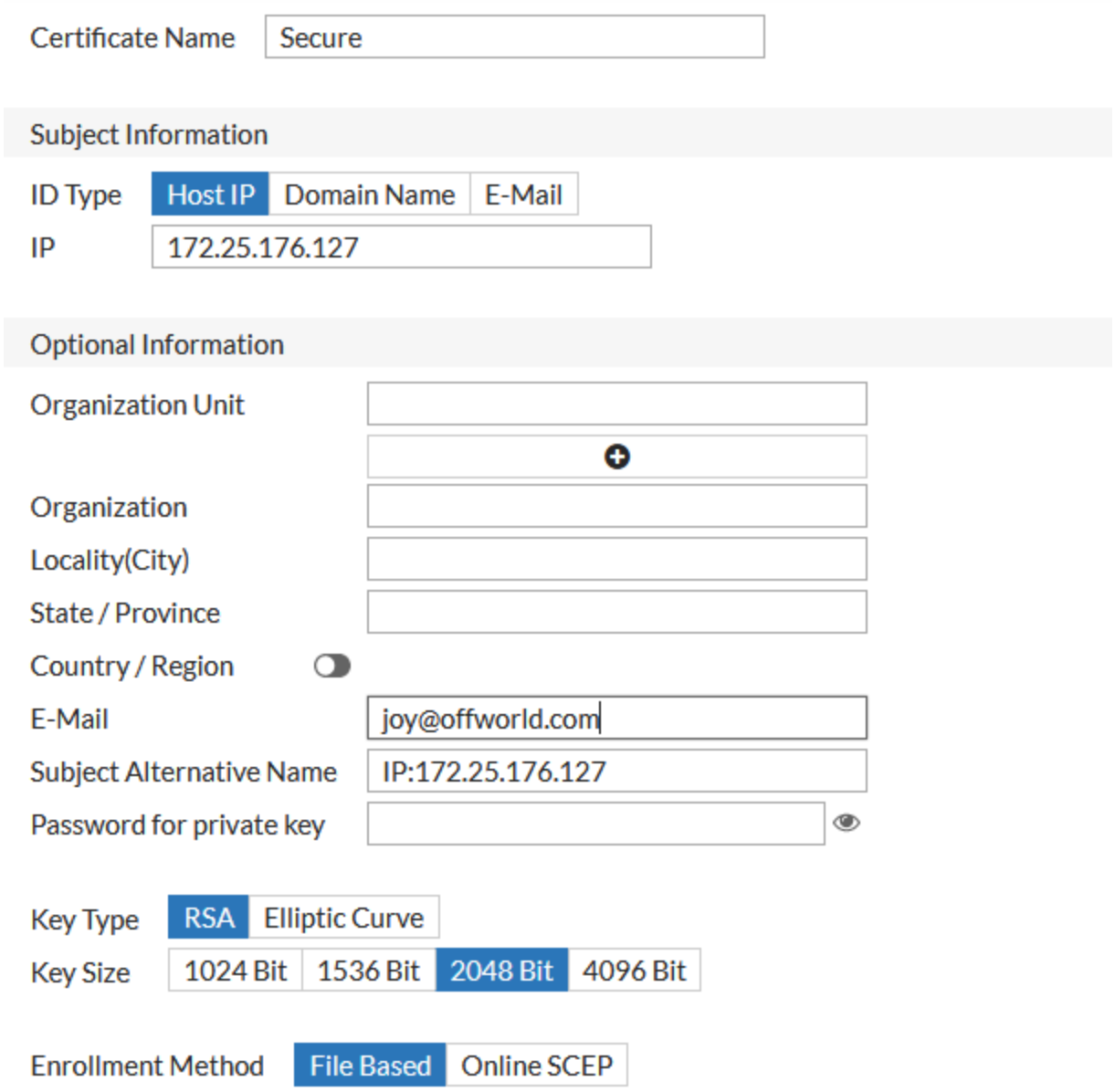
Note that, for this configuration to work correctly, the FortiAuthenticator must be configured as a certificate authority (CA), otherwise the certificate created in this recipe will not be trusted. For more information on how to do this, see FortiAuthenticator as a Certificate Authority.

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.

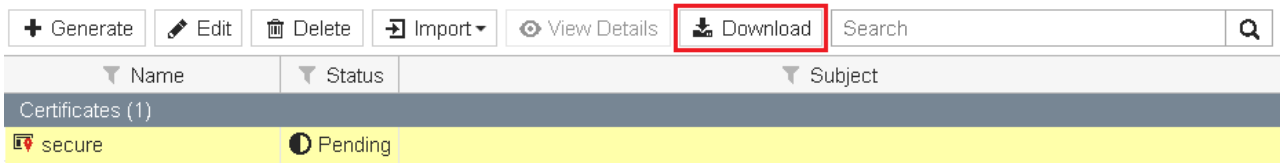
As an example, you will also have **Application Control** with **Deep Inspection of Cloud Applications** enabled. This will apply inspection to HTTPS traffic. Note that you may use another security profile instead of **Application Control**.

Creating a CSR on the FortiGate

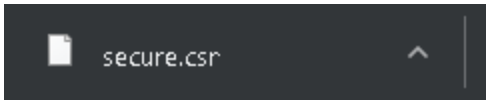
1. On the FortiGate, go to **System > Certificates** and select **Generate** to create a new certificate signing request (CSR).
   Enter a **Certificate Name**, the Internet facing IP address of the FortiGate, and a valid email address, then configure the key options as shown in the example.
   The **Subject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



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

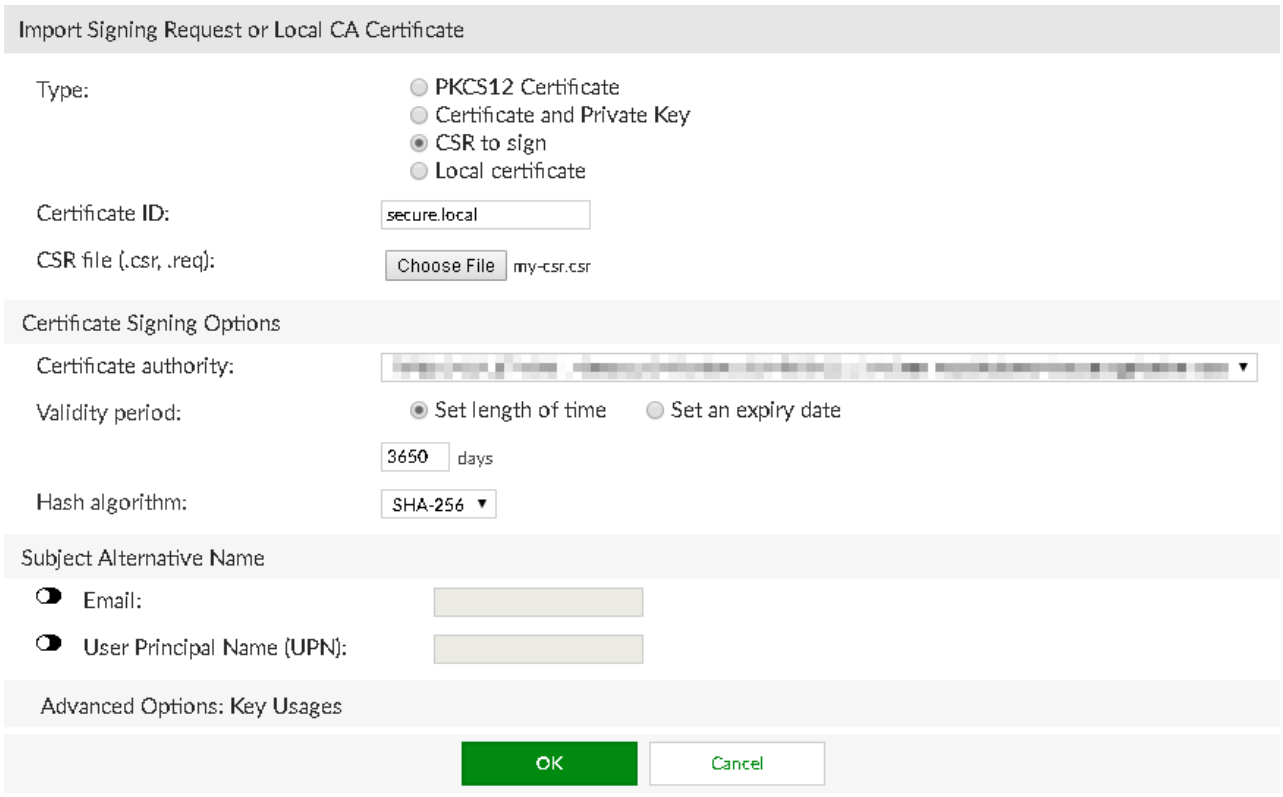


This will save a **.csr** file to your local drive.

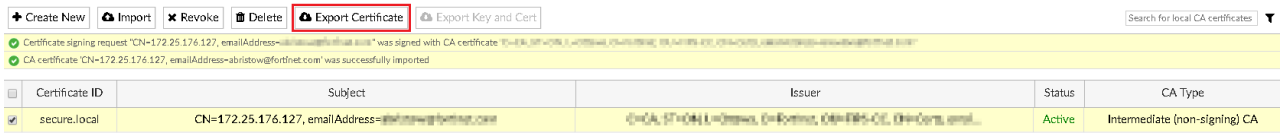


Creating an Intermediate CA on the FortiAuthenticator

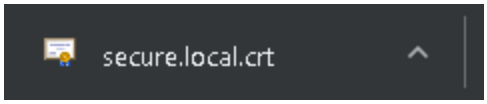
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and select **Import**.
   Set **Type** to **CSR to sign**, enter a **Certificate ID**, and import the CSR file. Make sure to select the **Certificate authority** from the drop-down menu and set the **Hash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



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

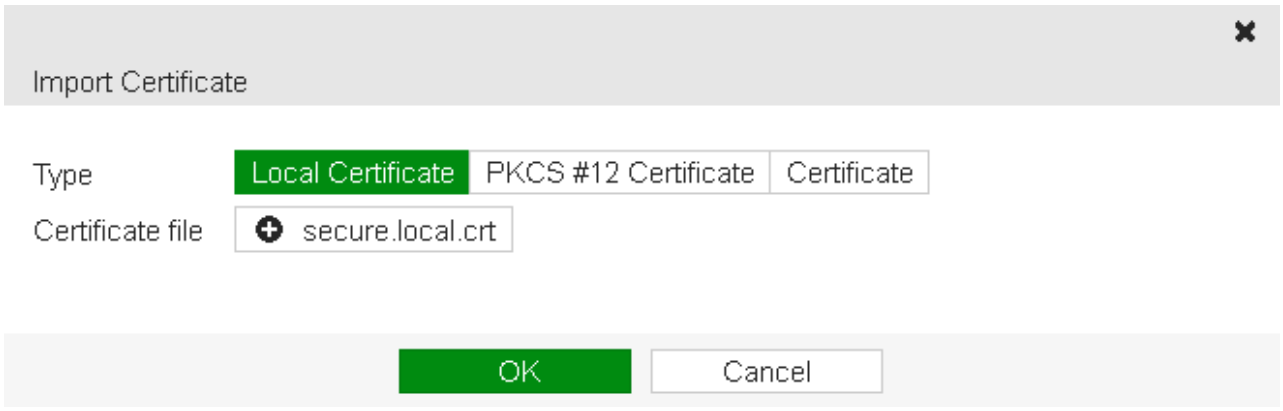


This will save a **.crt** file to your local drive.

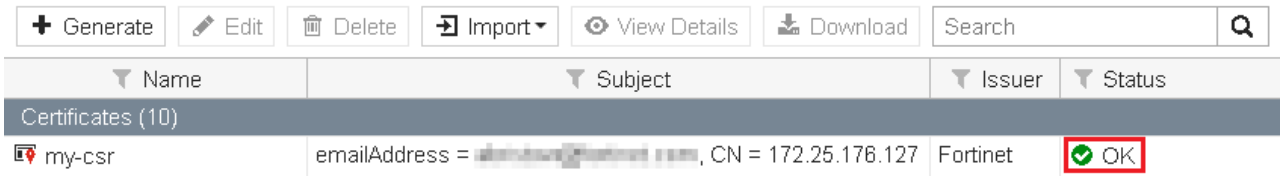


Importing the signed certificate on the FortiGate

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

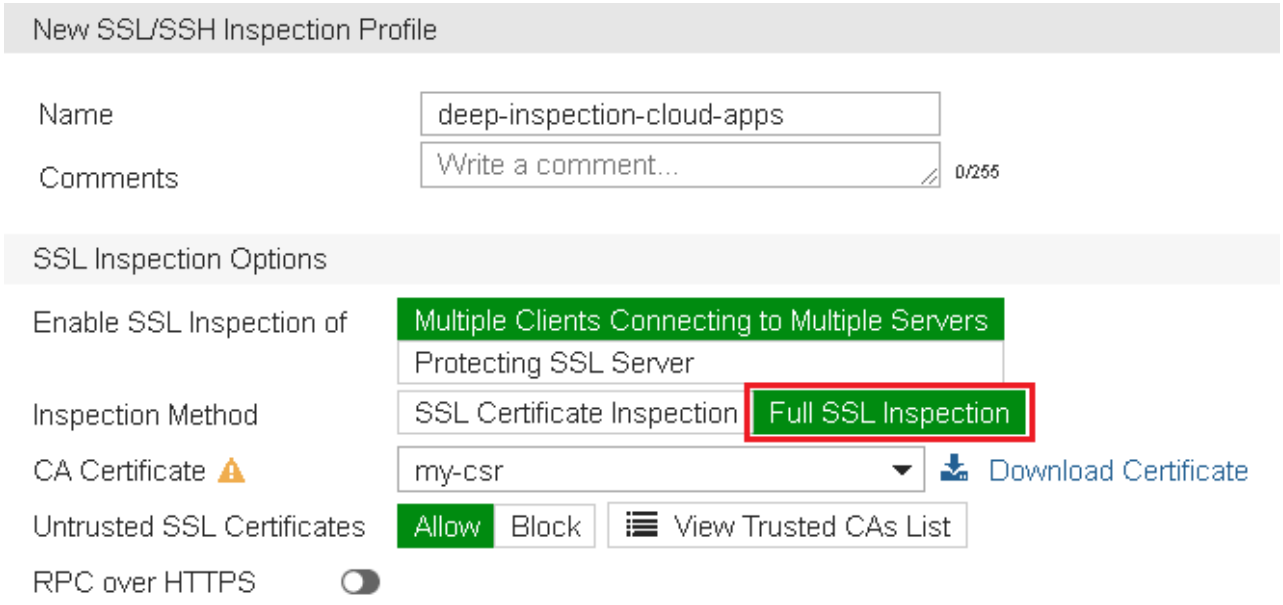


2. You should now see that the certificate has a **Status** of **OK**.

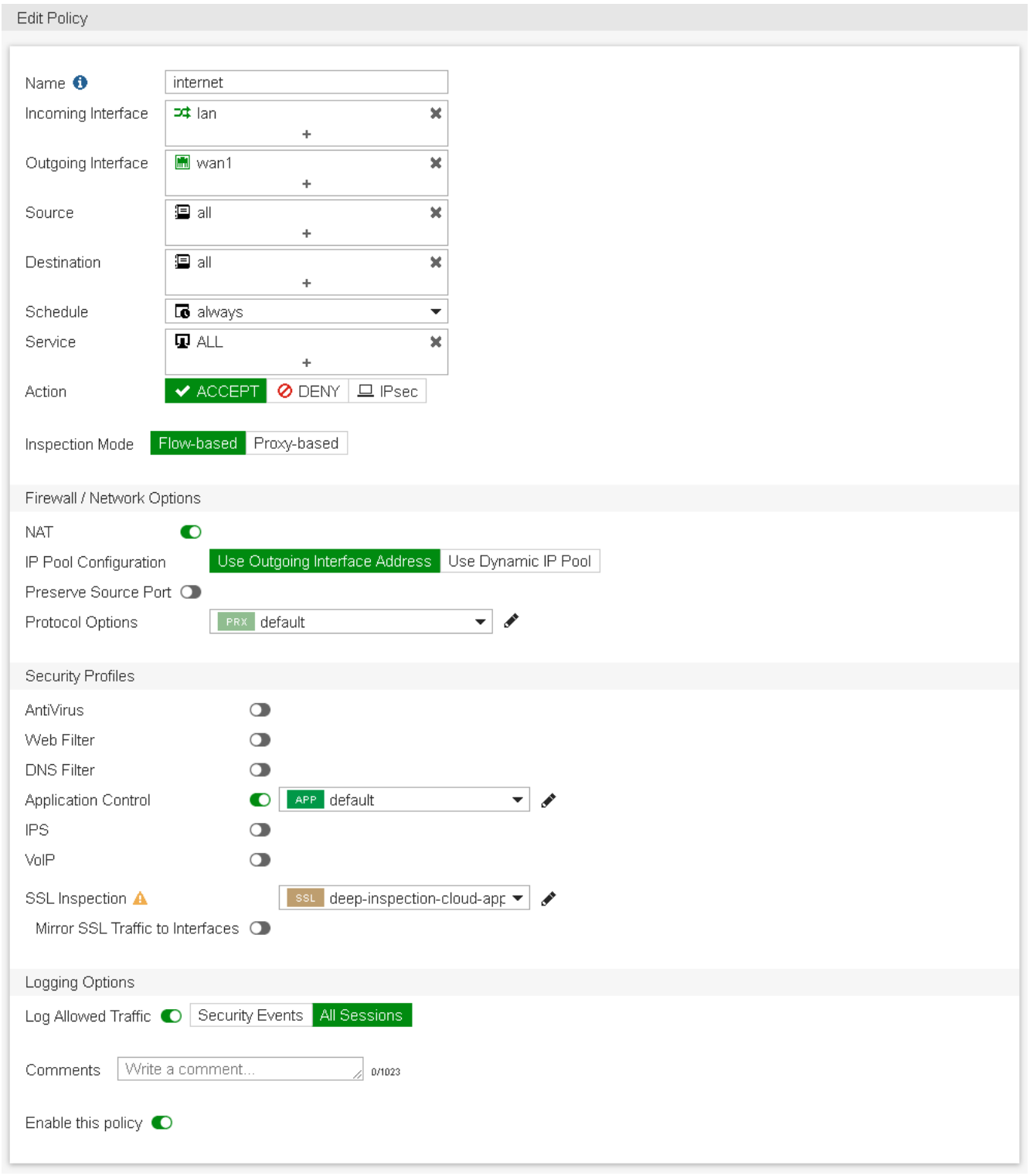


Configuring full SSL inspection

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

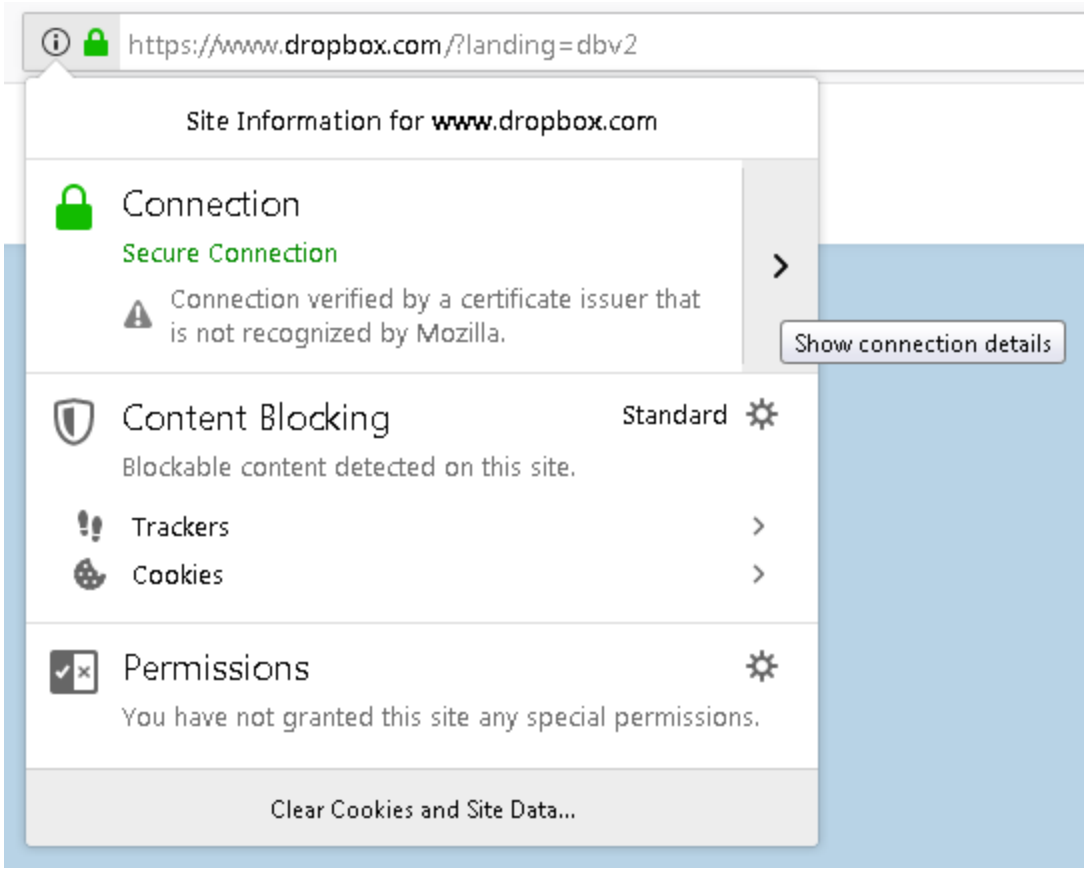


2. Add the certificate to your web browser's list of trusted certificates. End users will likely see certificate warnings unless the certificate is installed in their browser.
3. Next go to **Policy & Objects > IPv4 Policy** and edit the policy that allows Internet access.
   Under **Security Profiles**, enable **SSL/SSH Inspection** and select the custom profile created earlier.
   Enable **Application Control** and set it to **default**.


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

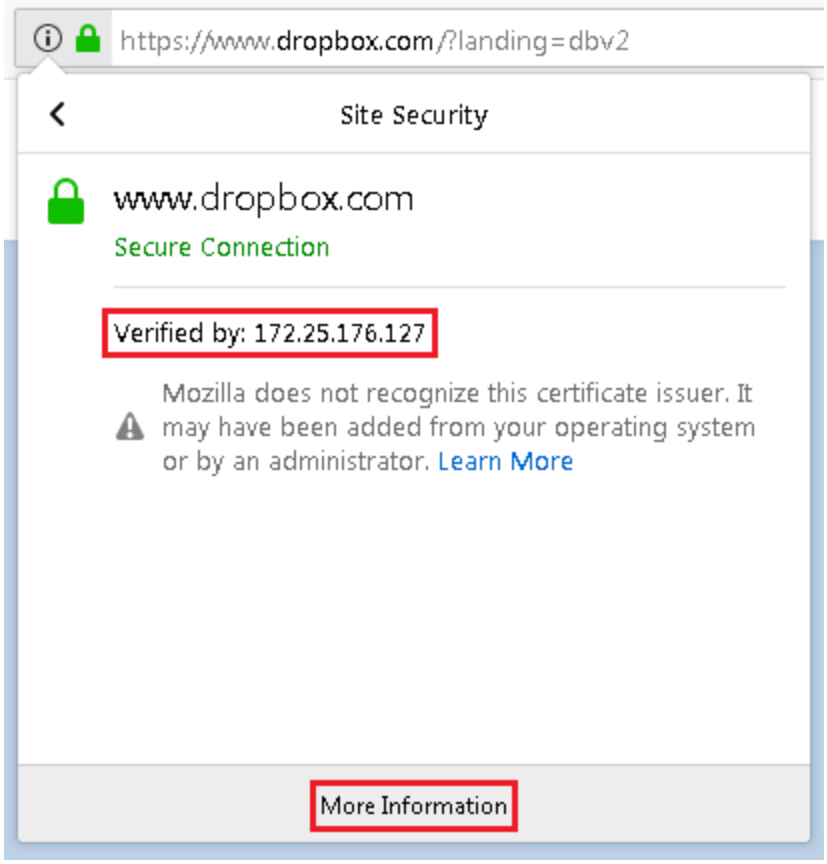
Results

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**.

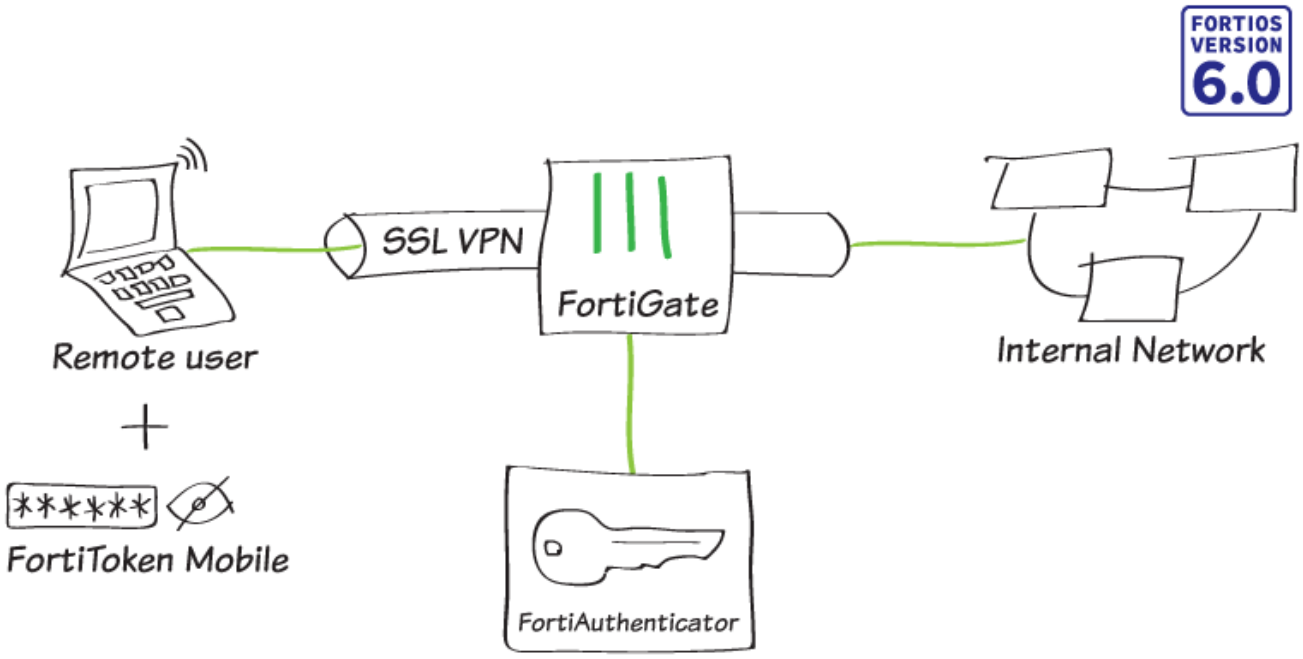


FortiToken and FortiToken Mobile

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

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

FortiToken Mobile Push for SSL VPN



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

For this configuration, you:

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

The following names and IP addresses are used:

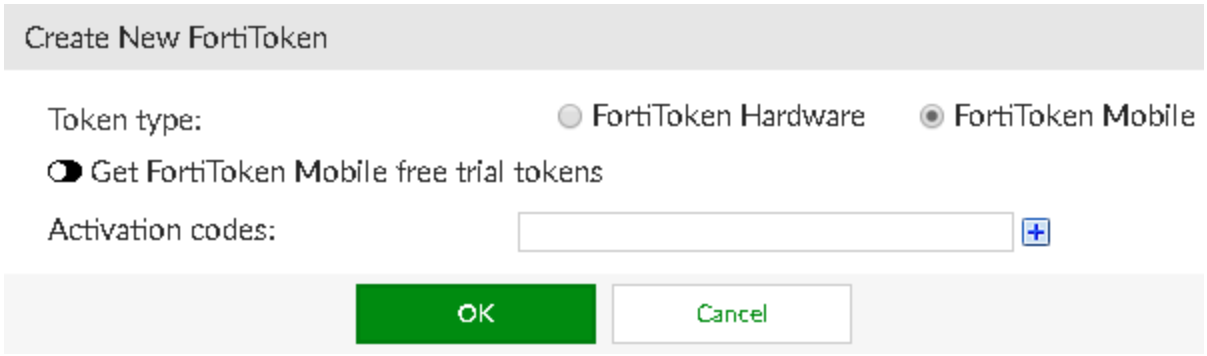
- Username: gthreepwood
- User group: RemoteFTMGroup
- RADIUS server: OfficeRADIUS
- RADIUS client: OfficeServer
- SSL VPN user group: SSLVPNGroup
- FortiAuthenticator: 172.25.176.141
- FortiGate: 172.25.176.92

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

- FortiToken Mobile for Android
- FortiToken Mobile for iOS

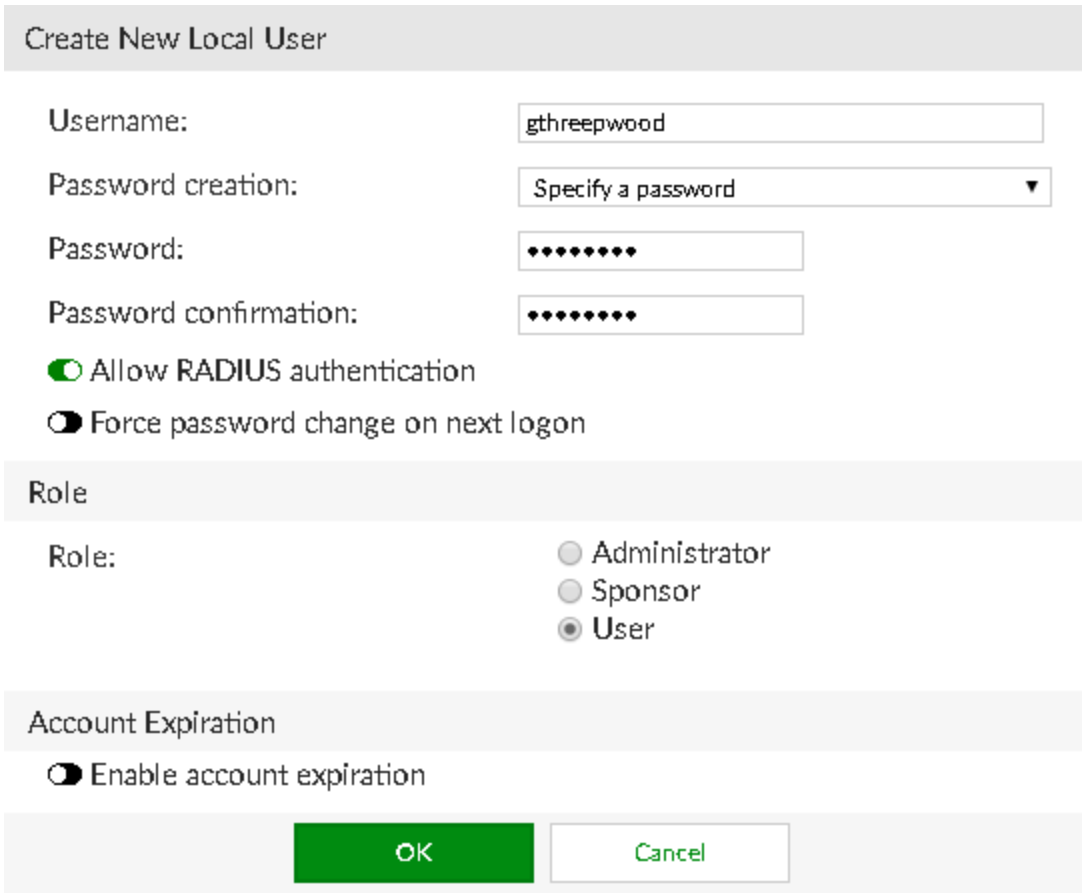
Adding a FortiToken to the FortiAuthenticator

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

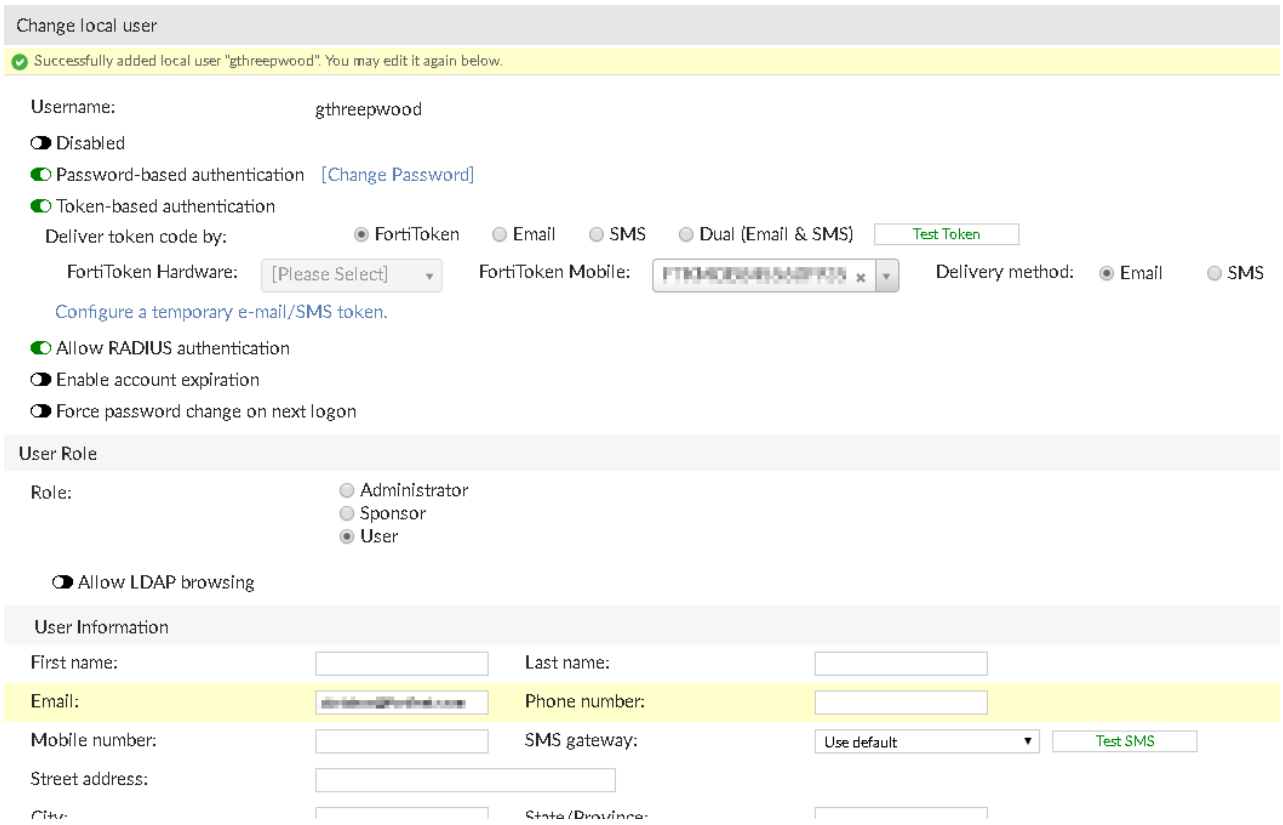


Adding the user to the FortiAuthenticator

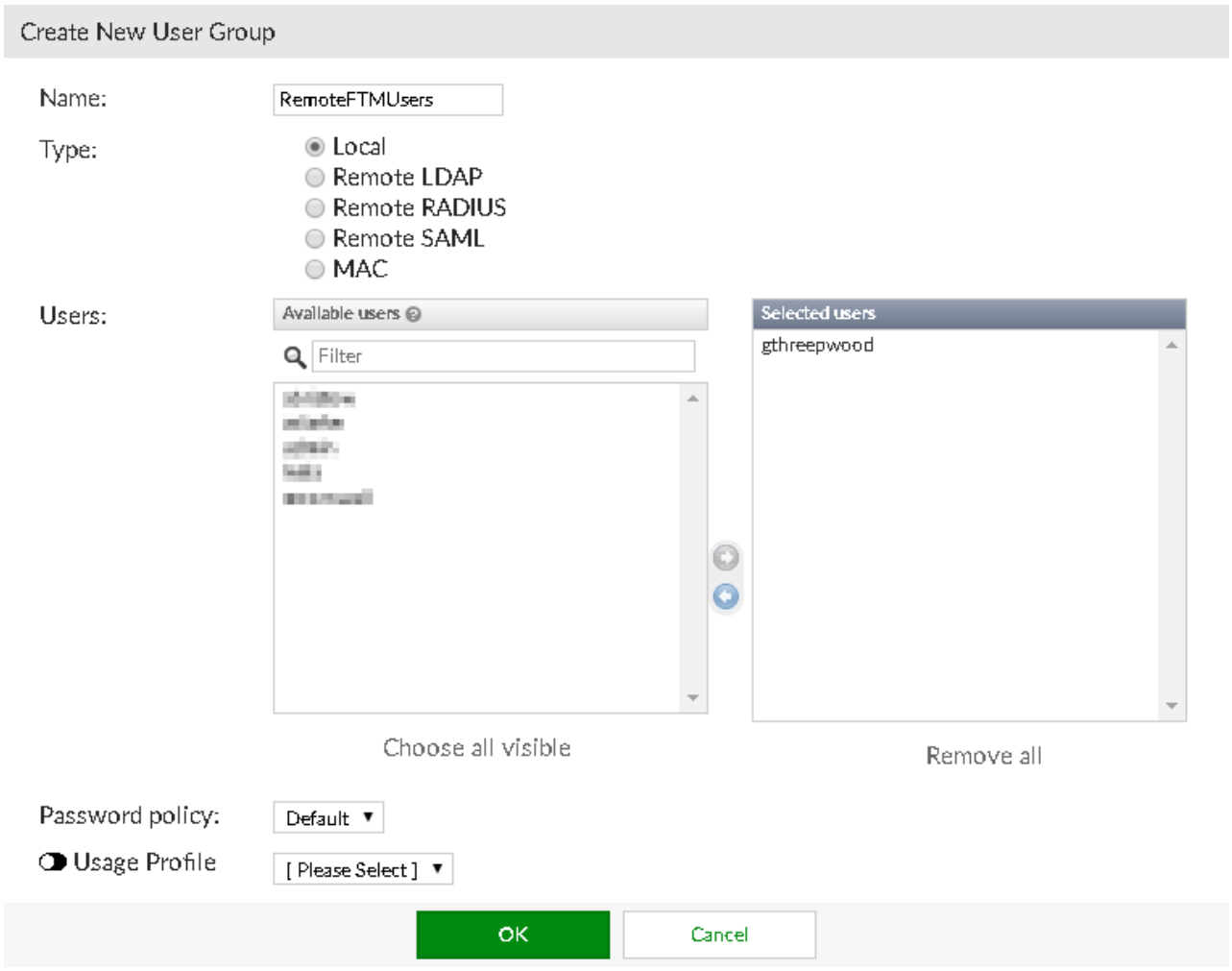
1. On the FortiAuthenticator, go to **Authentication > User Management > Local Users**, and select **Create New**. Enter a **Username** (*gthreepwood*) and enter and confirm the user password.
   Enable **Allow RADIUS authentication**, and select **OK** to access additional settings.



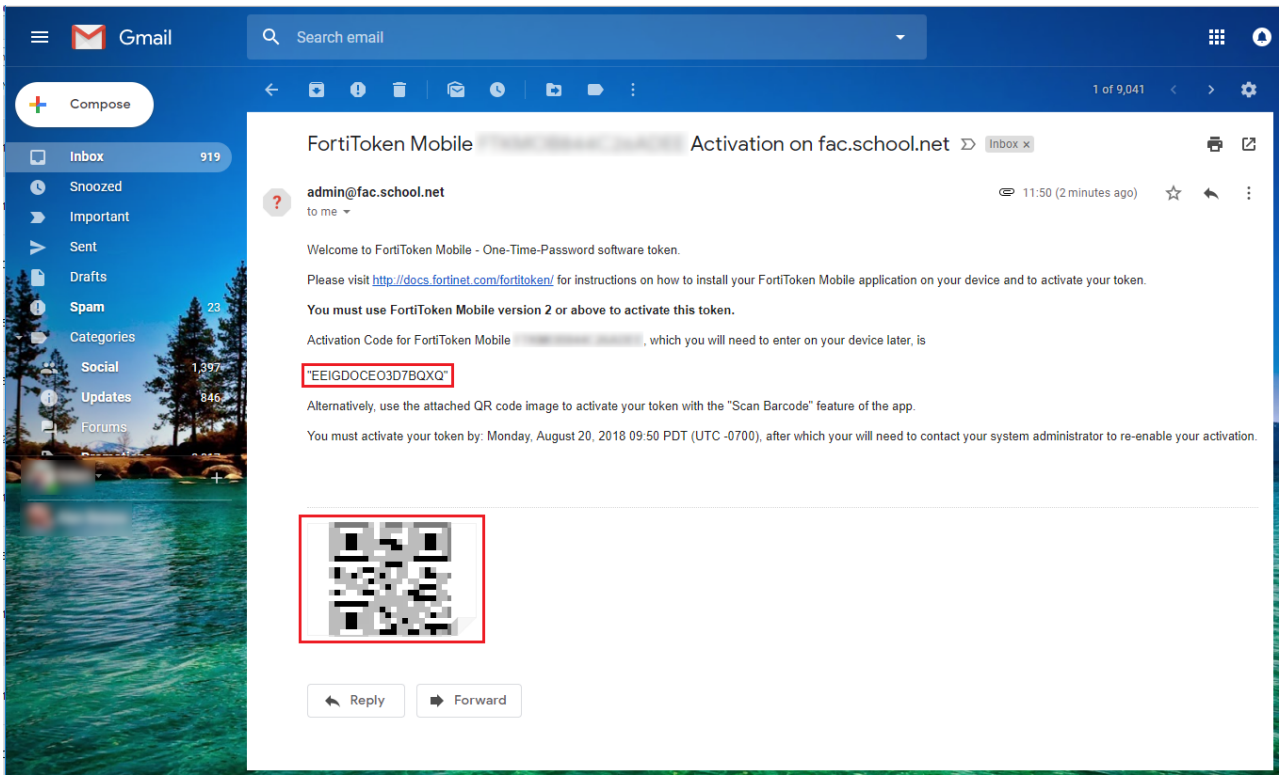
2. Enable **Token-based authentication** and select to deliver the token code by **FortiToken**. Select the FortiToken added earlier from the **FortiToken Mobile** drop-down menu.
   Set **Delivery method** to **Email**. This will automatically open the **User Information** section where you can enter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



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



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



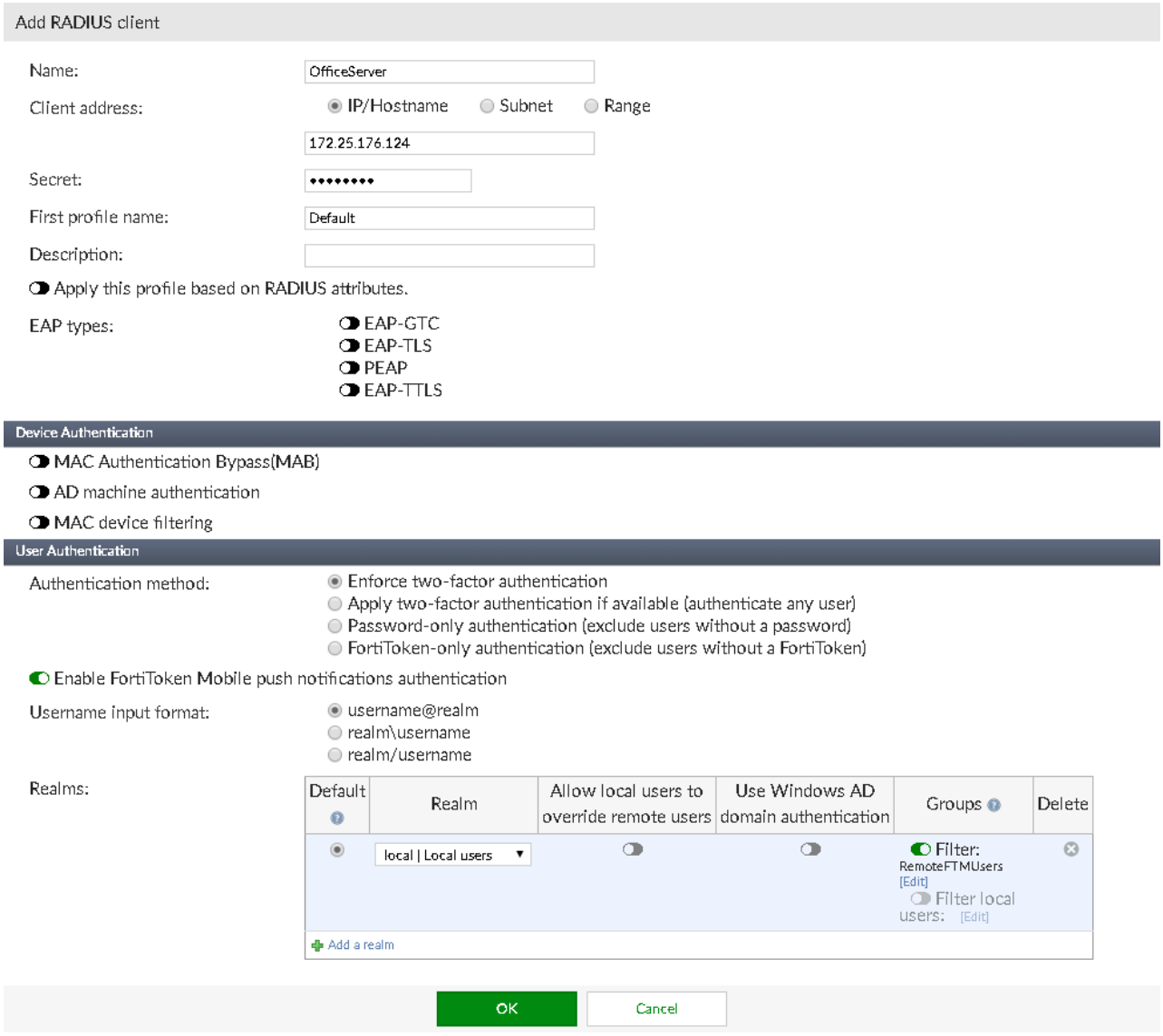
For more information, see the FortiToken Mobile user instructions.

Creating the RADIUS client on the FortiAuthenticator

1. On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients**, and select **Create New** to add the FortiGate as a RADIUS client.
2. Enter a **Name** (*OfficeServer*), the IP address of the FortiGate, and set a **Secret**. The secret is a pre-shared secure password that the FortiGate will use to authenticate to the FortiAuthenticator.
3. Set **Authentication method** to **Enforce two-factor authentication** and check the **Enable FortiToken Mobile push notifications authentication** checkbox.

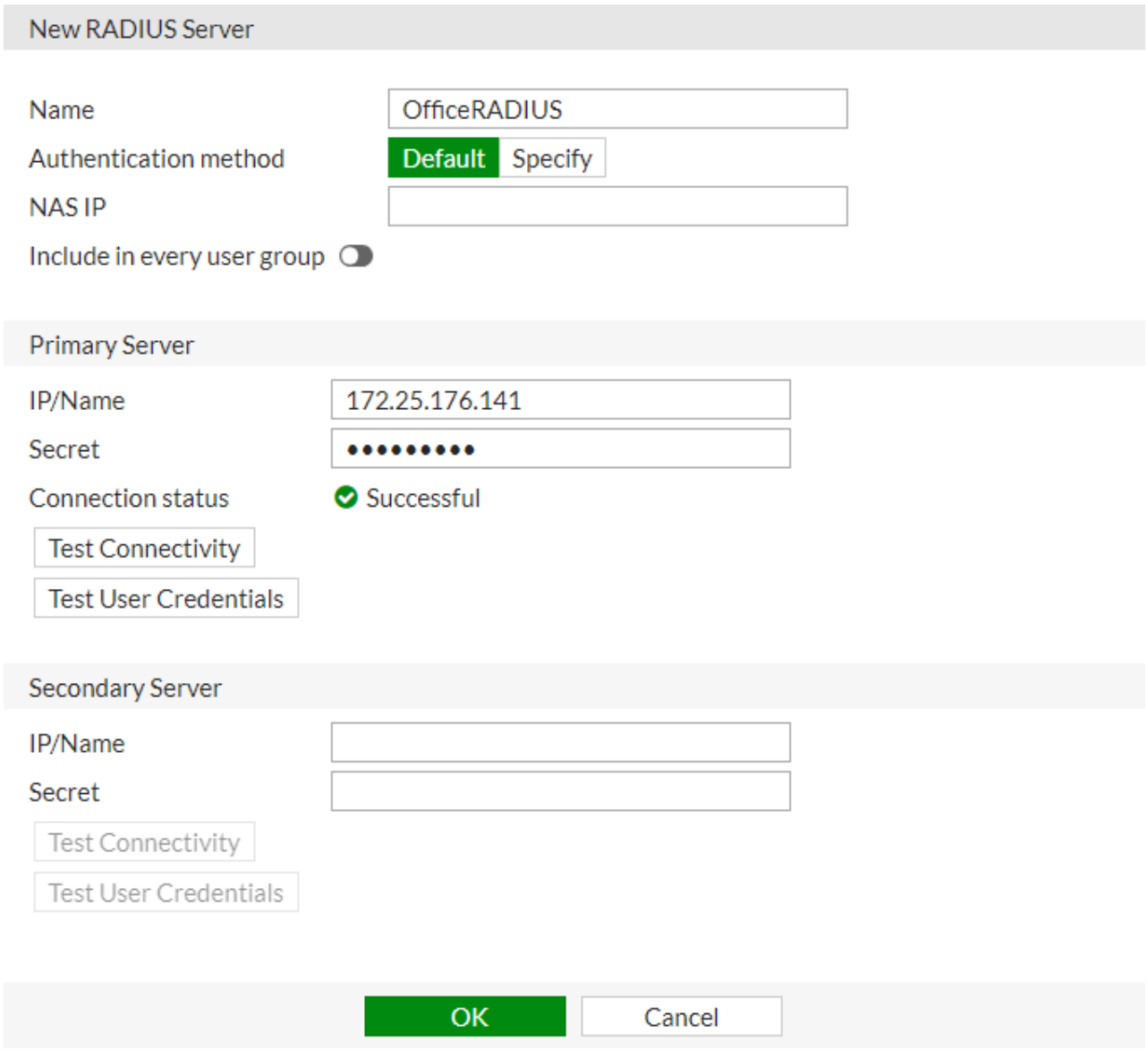
4. Set **Realms** to **local | Local users**, and add **RemoteFTMUsers** to the **Groups** filter.

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

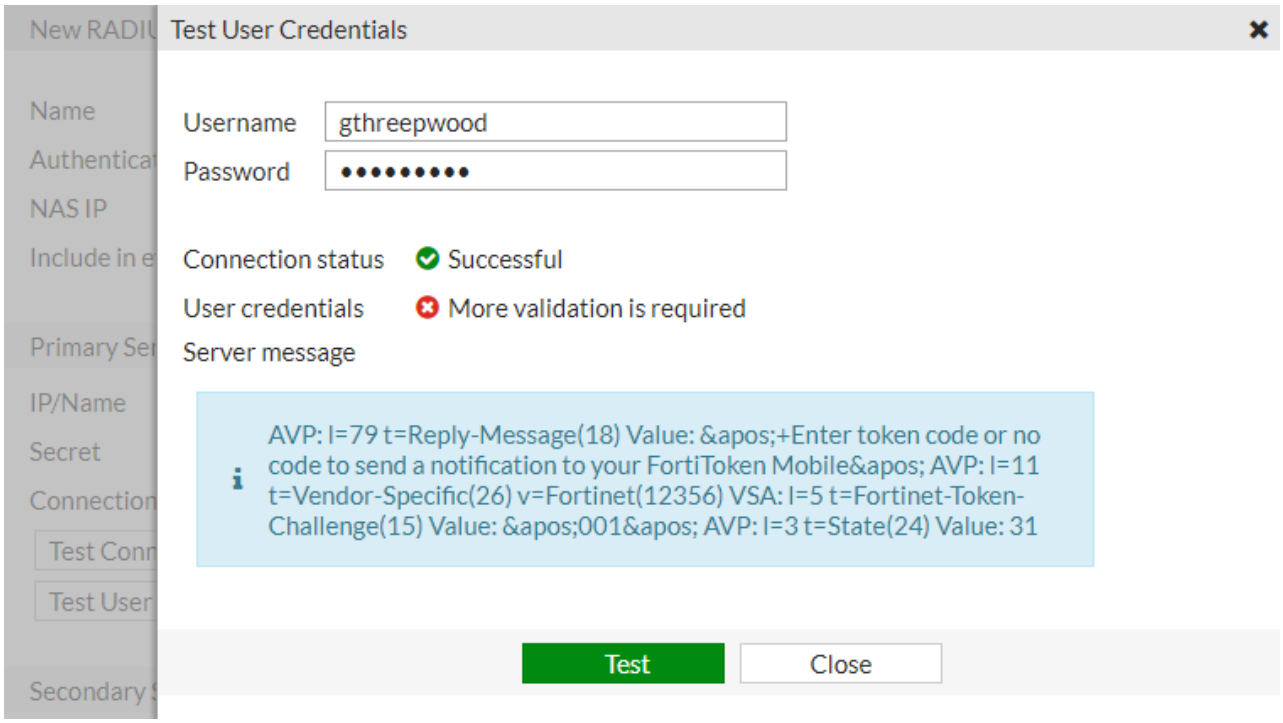


Connecting the FortiGate to the RADIUS server

1. On the FortiGate, go to **User & Device > RADIUS Servers**, and select **Create New** to connect to the RADIUS server (FortiAuthenticator).
   Enter a **Name** (*OfficeRADIUS*), the IP address of the FortiAuthenticator, and enter the **Secret** created before.
   Select **Test Connectivity** to be sure you can connect to the RADIUS server. Then select **Test User Credentials** and enter the credentials for **gthreepwood**.

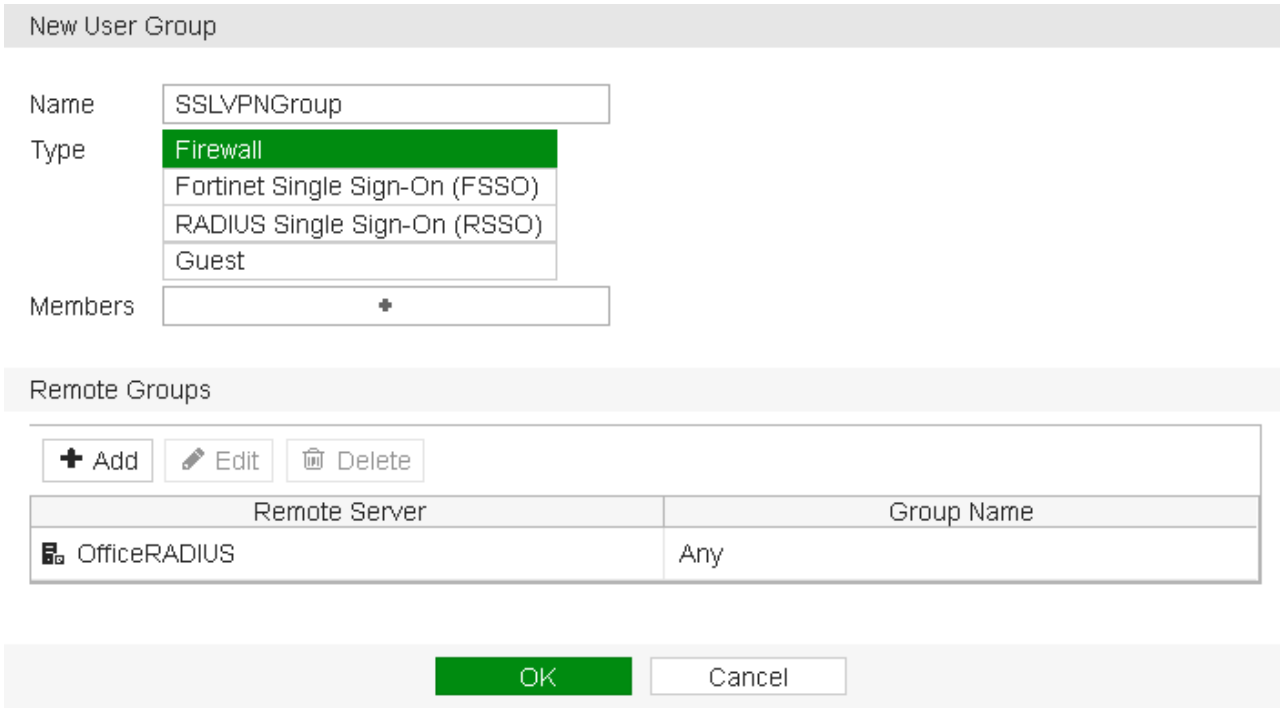


Because the user has been assigned a FortiToken, the test should return stating that **More validation is required**.



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

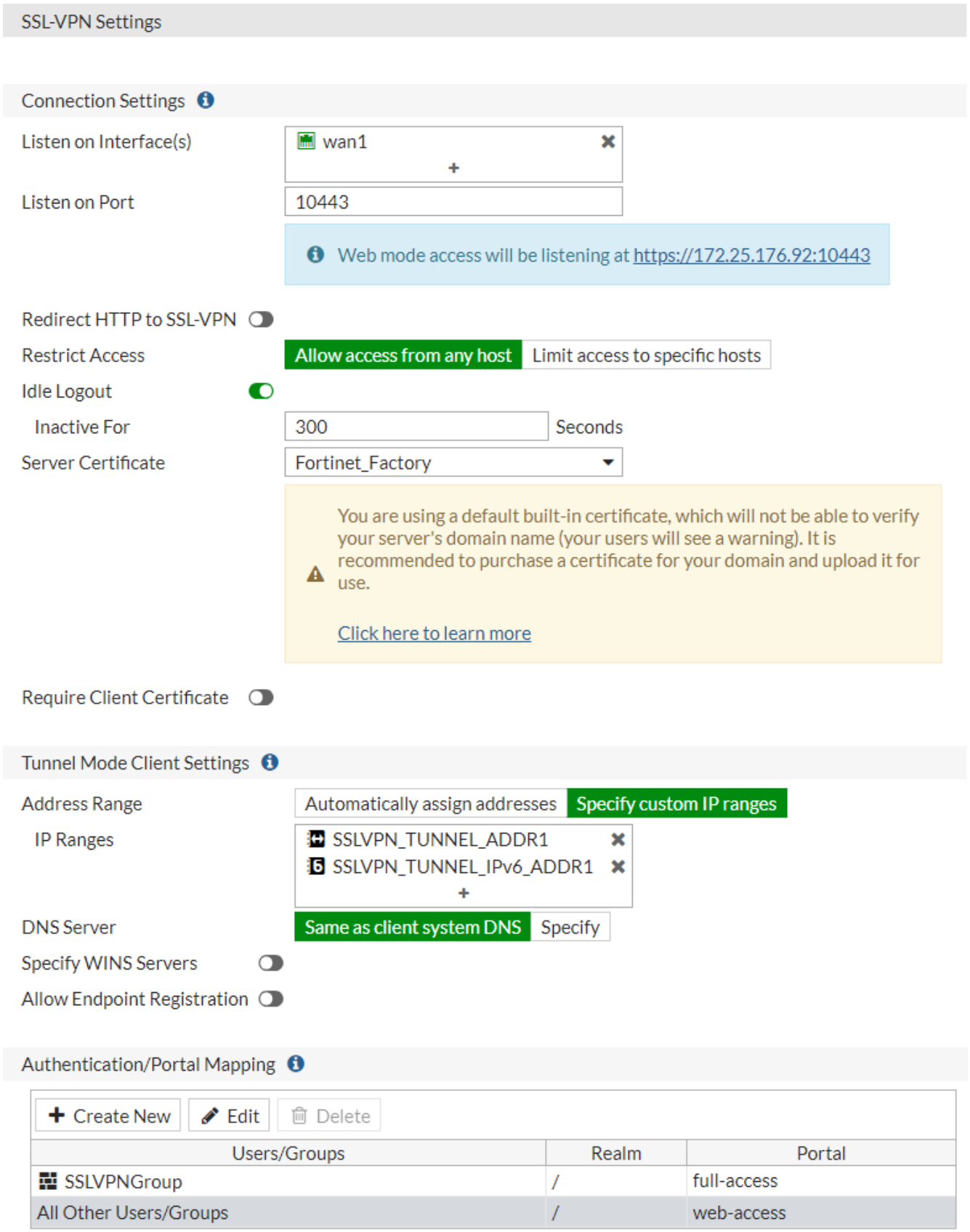
2. Then go to **User & Device > User Groups**, and select **Create New** to map authenticated remote users to a user group on the FortiGate.
   Enter a **Name** (*SSLVPNGroup*) and select **Add** under **Remote Groups**.
   Select **OfficeRADIUS** under the **Remote Server** drop-down menu, and leave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



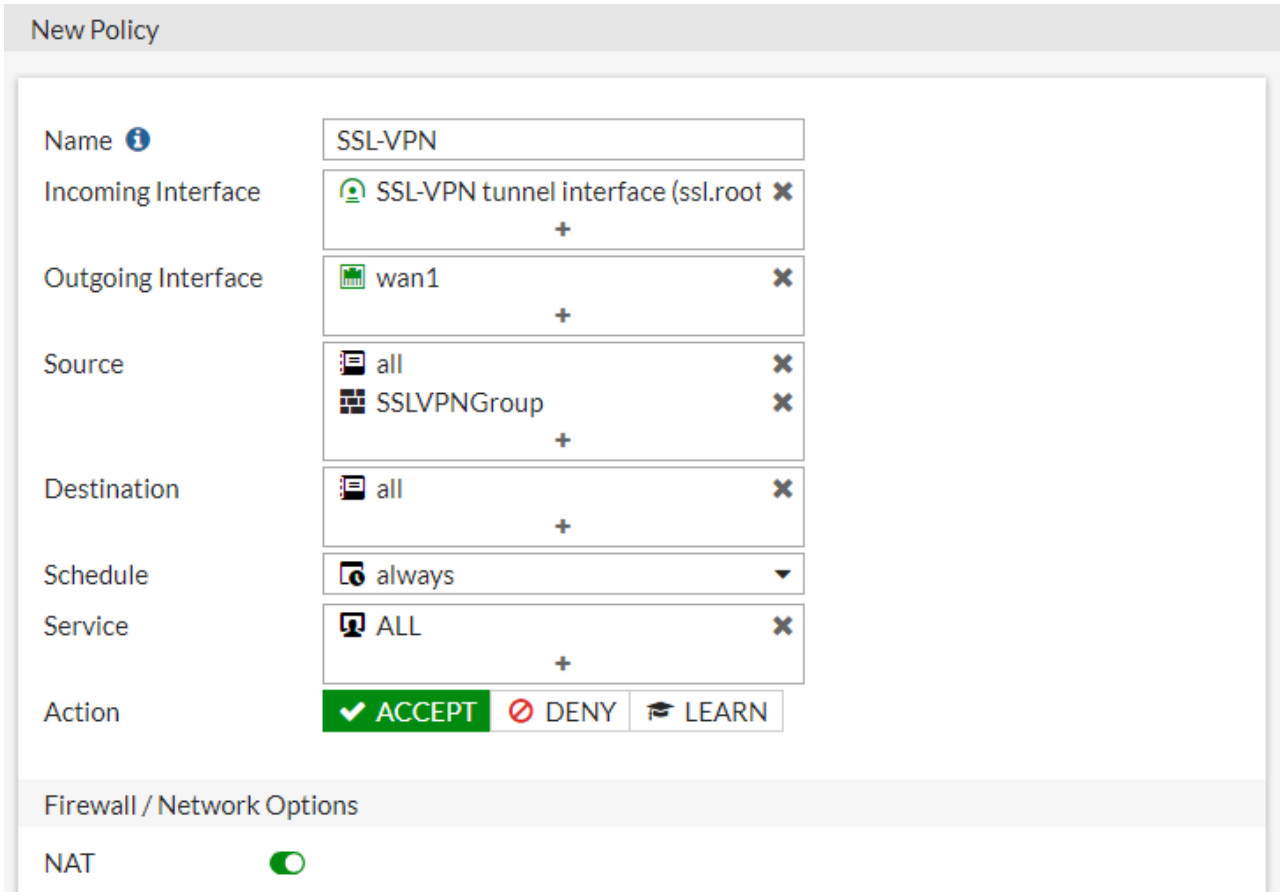
Configuring the SSL VPN

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

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

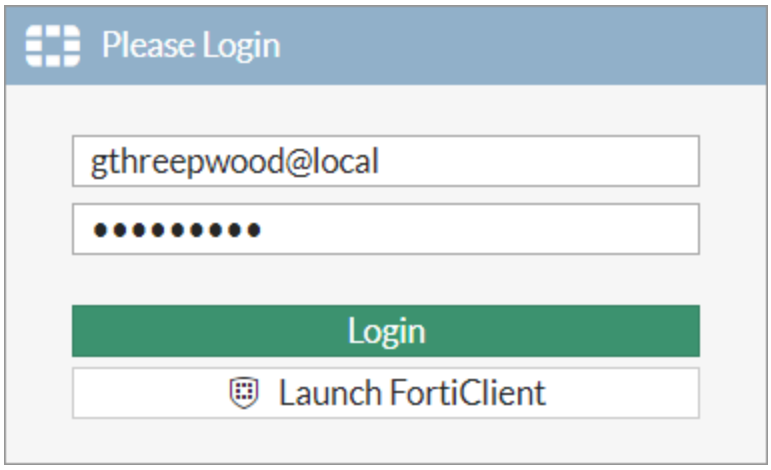

SSL-VPN Settings
Connection Settings
Listen on Interface(s)
wan1
Listen on Port
10443
Web mode access will be listening at https://172.25.176.92:10443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate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

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

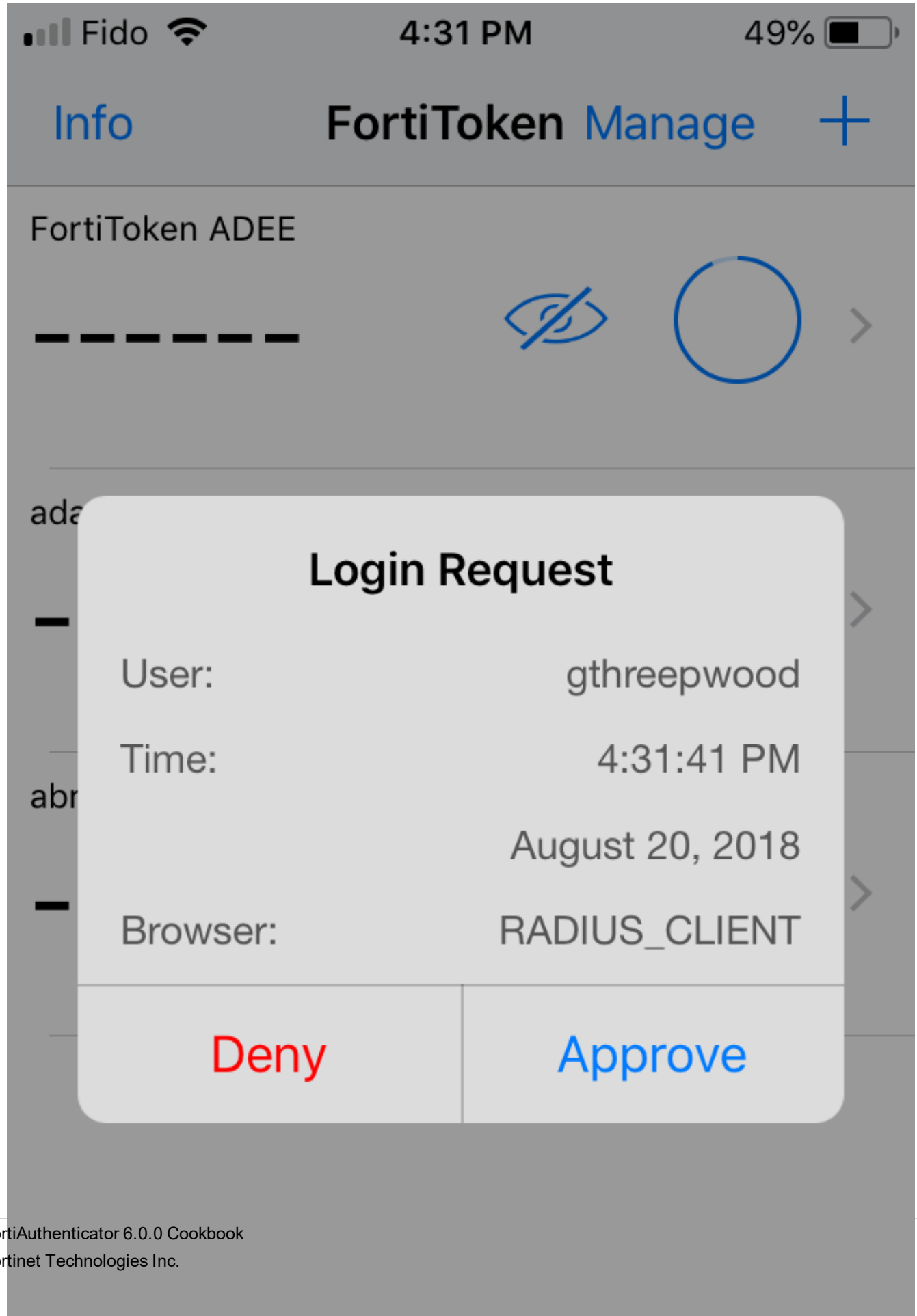


Results

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

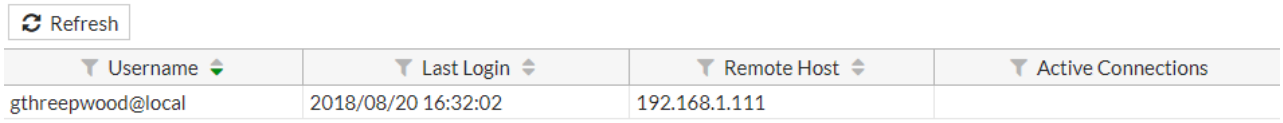


3. The FortiAuthenticator will then push a login request notification through the FortiToken Mobile application. Select **Approve**.


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

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

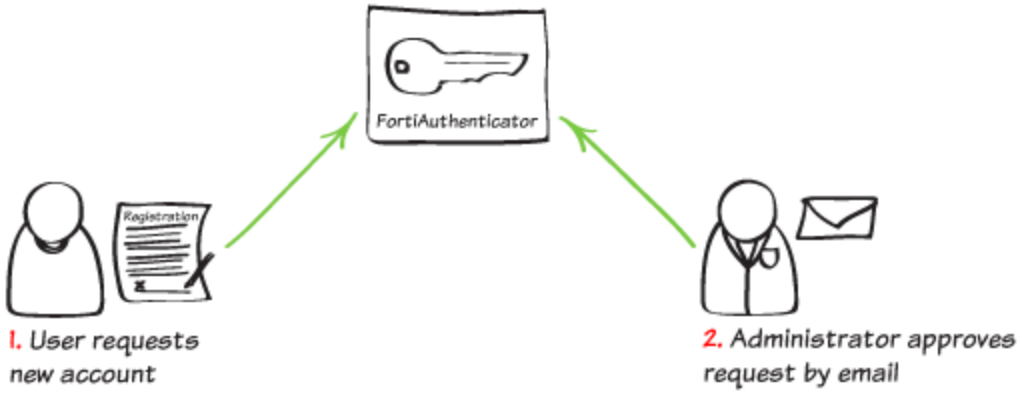
3. On the FortiGate, go to **Monitor > SSL-VPN Monitor** to confirm the user's connection.



Self-service Portal

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

FortiAuthenticator user self-registration



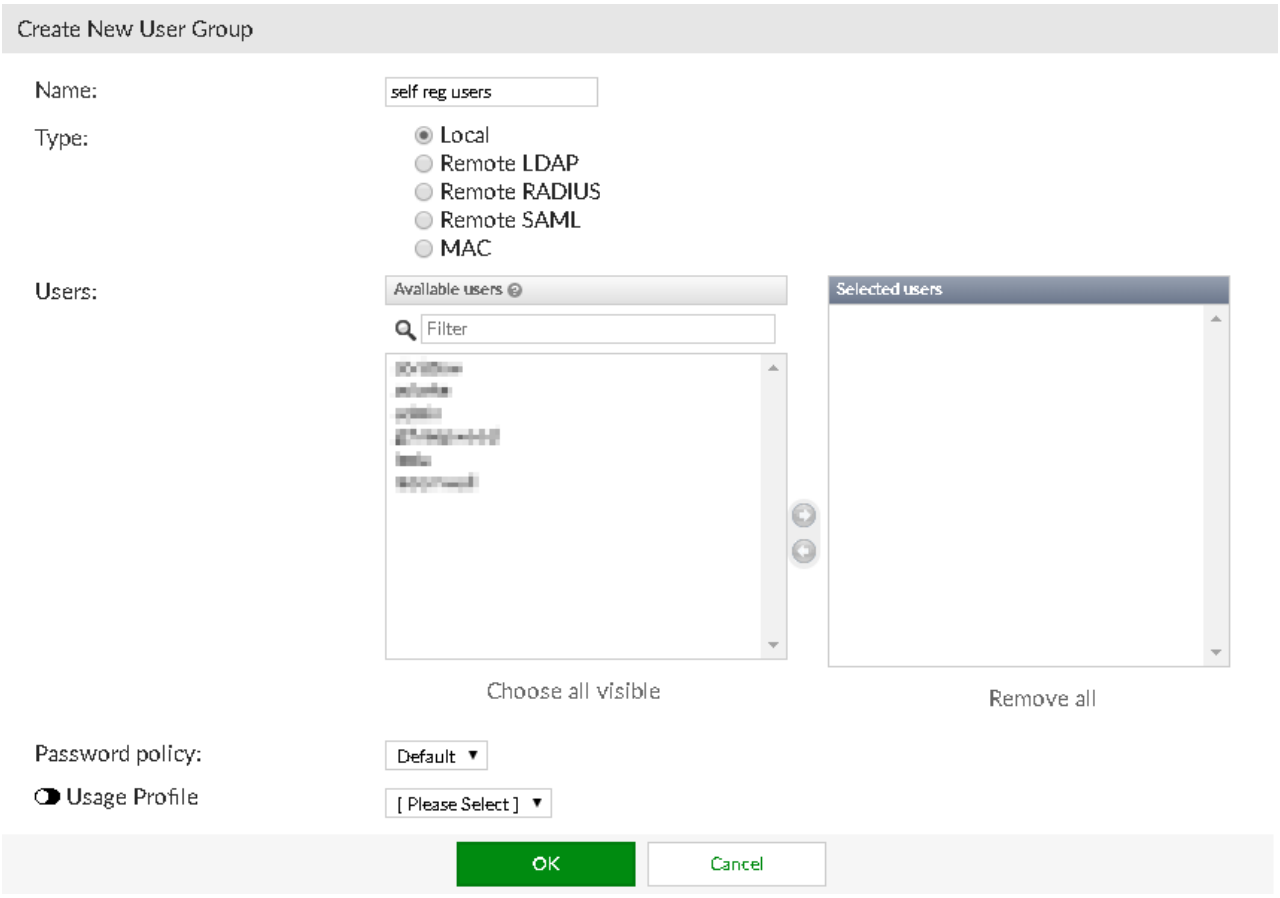
For this recipe, you will configure the FortiAuthenticator self-service portal to allow users to add their own account and create their own passwords.

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

Creating a self-registration user group

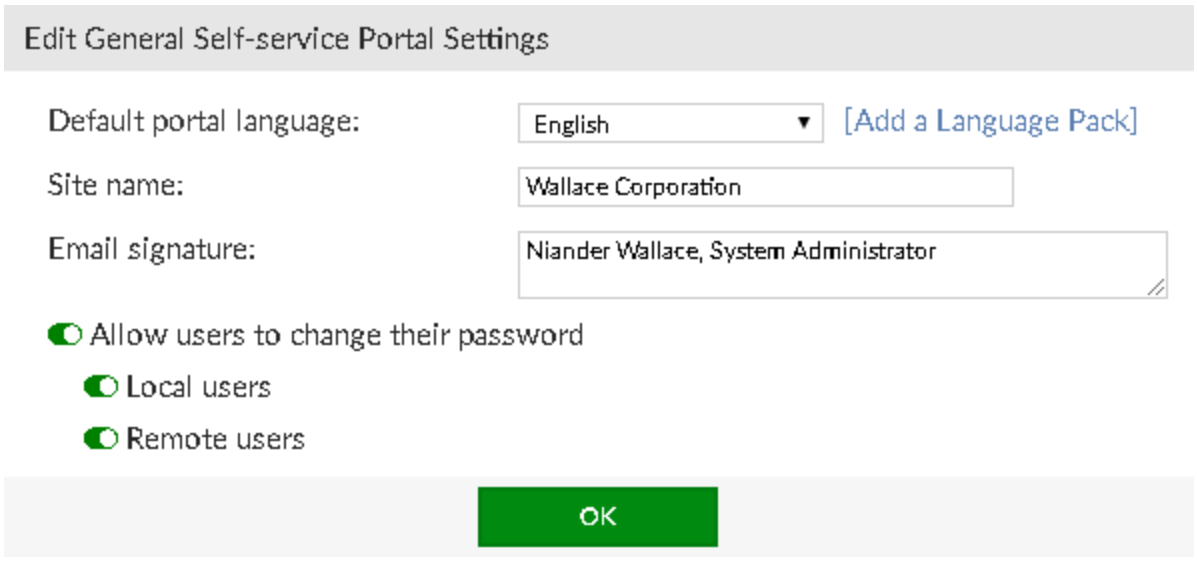
1. Go to **Authentication > User Management > User Groups** and create a new user group for self-registering users.
   Enter a **Name** and select **OK**. Users will be added to this group once they register through the self-registration

portal.

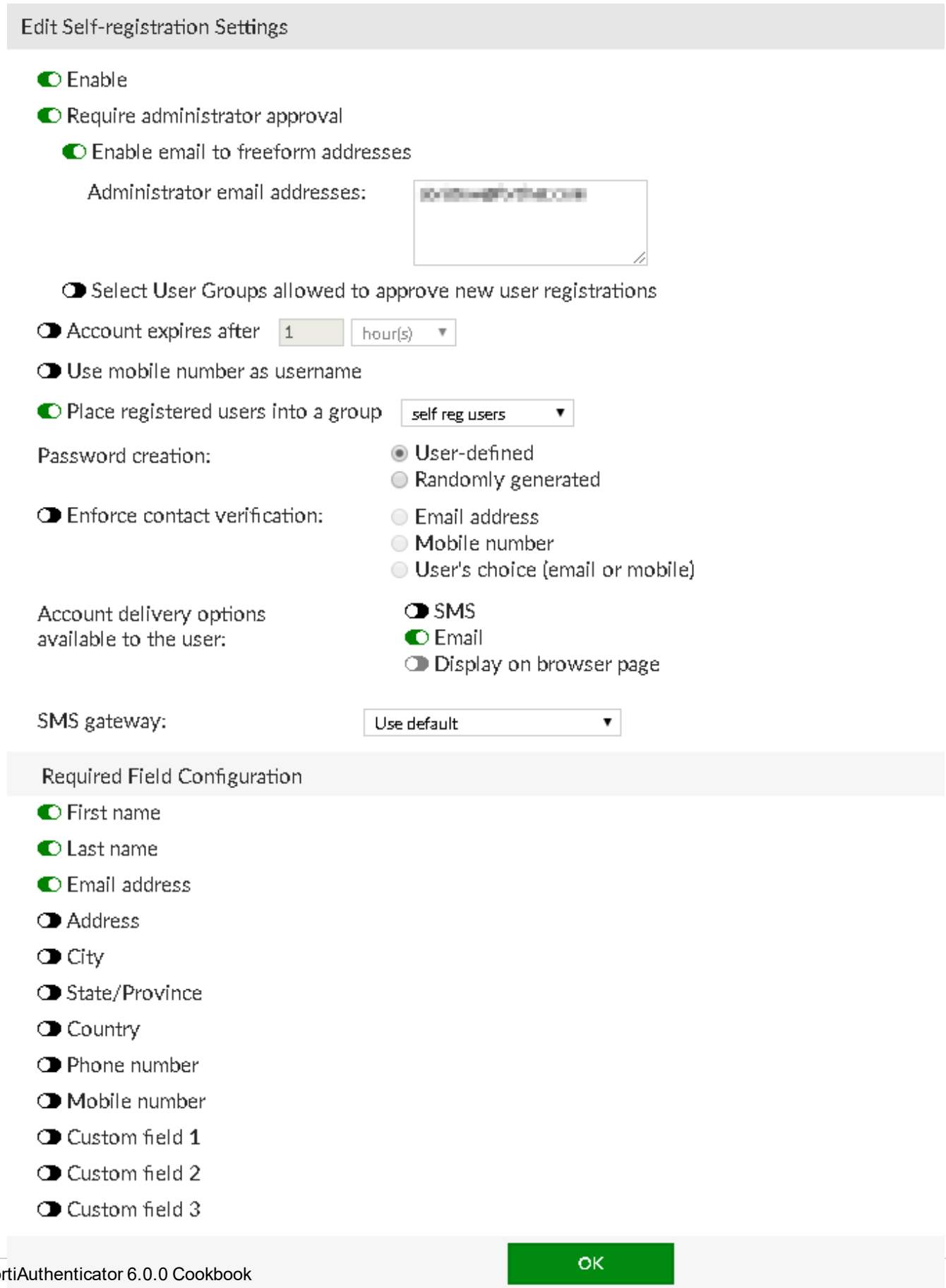


Enabling self-registration

1. Go to **Authentication > Self-service Portal > General**.
   Enter a **Site name**, add an **Email signature** that you would like appended to the end of outgoing emails, and select **OK**.

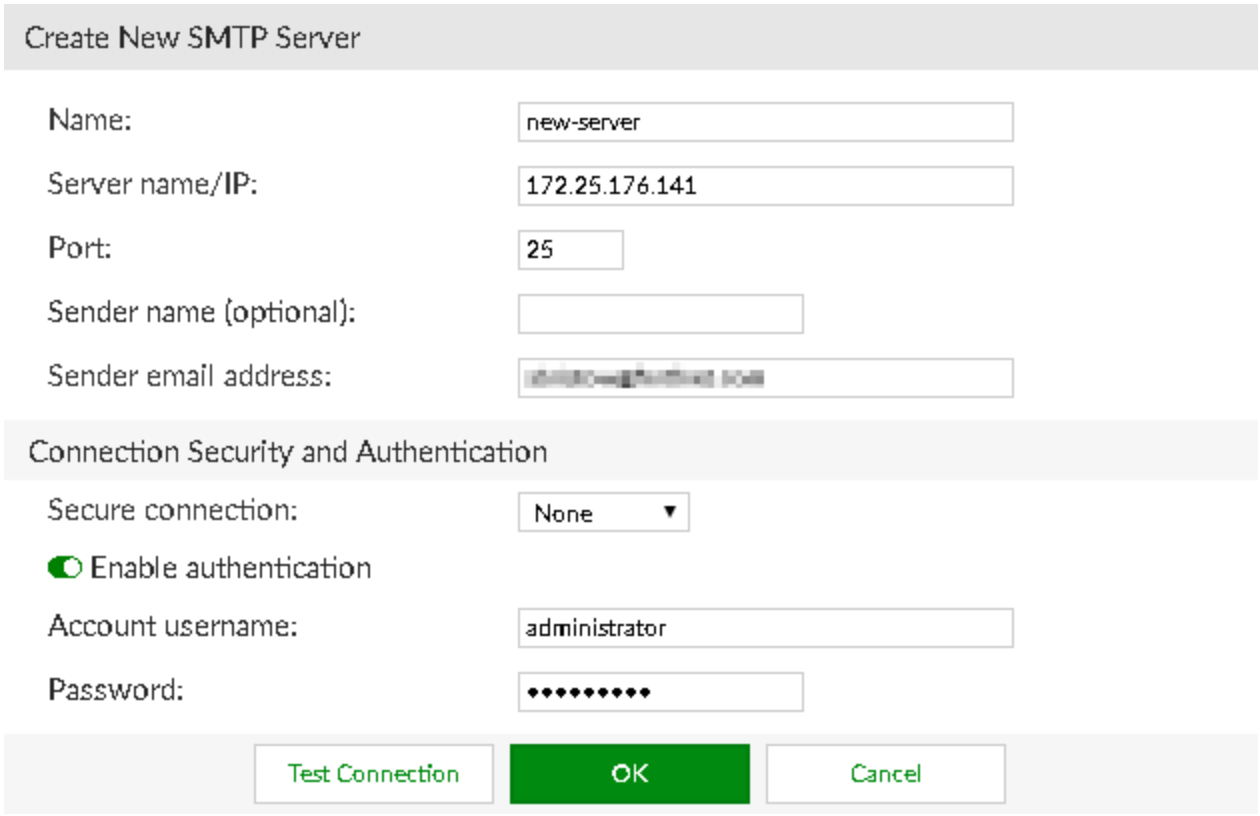


2. Then go to **Authentication > Self-service Portal > Self-registration** and select **Enable**.
   Enable **Require administrator approval** and **Enable email to freeform addresses**, and enter the administrator's email address in the field provided.
   Enable **Place registered users into a group**, select the user group created earlier, and configure basic account information to be sent to the user by **Email**.
   Open the **Required Field Configuration** drop-down and enable **First name**, **Last name**, and **Email address**.

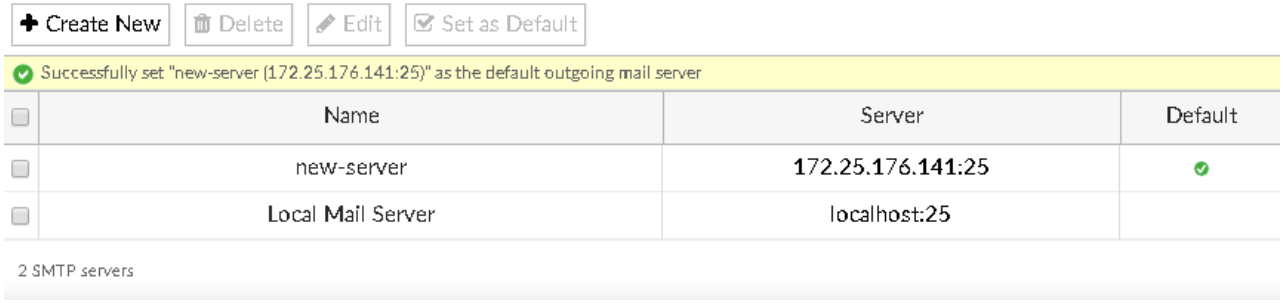

Edit Self-registration Settings
Enable
Require administrator approval
Enable email to freeform addresses
Administrator email addresses:
Select User Groups allowed to approve new user registrations
Account expires after
1
hour(s)
Use mobile number as username
Place registered users into a group
self reg users
Password creation:
User-defined
Randomly generated
Enforce contact verification:
Email address
Mobile number
User's choice (email or mobile)
Account delivery options available to the user:
SMS
Email
Display on browser page
SMS gateway:
Use default
Required Field Configuration
First name
Last name
Email address
Address
City
State/Province
Country
Phone number
Mobile number
Custom field 1
Custom field 2
Custom field 3
OK

Creating a new SMTP server

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



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

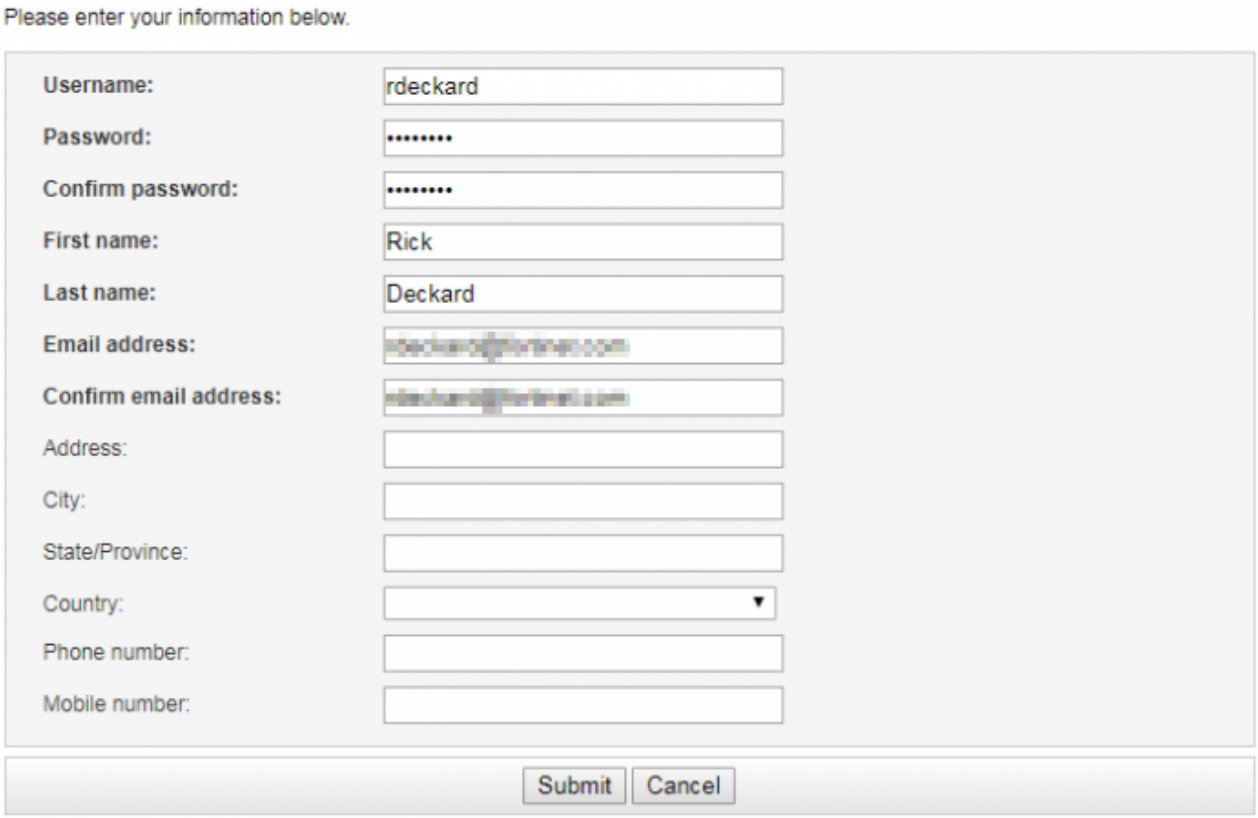


Results - Self-registration

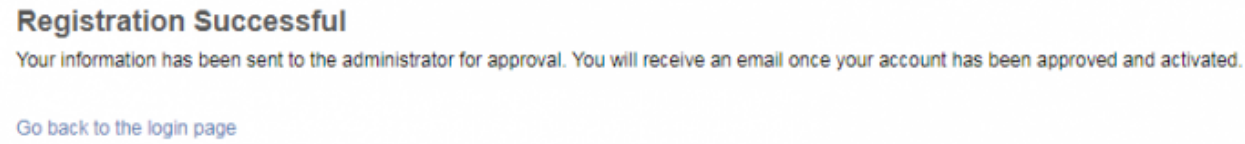
1. When the user visits the login page, *https://<FortiAuthenticator-IP>/auth/register/*, they can click the **Register** button, where they will be prompted to enter their information.

They will need to enter and confirm a **Username**, **Password**, **First name**, **Last name**, and **Email address**. These are the only required fields, as configured in the FortiAuthenticator earlier.

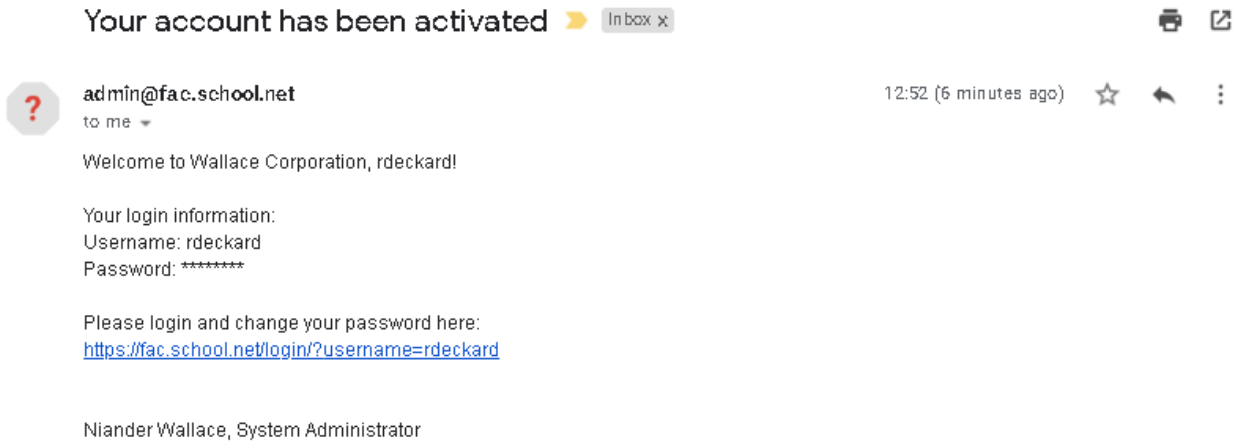
Select **Submit**.



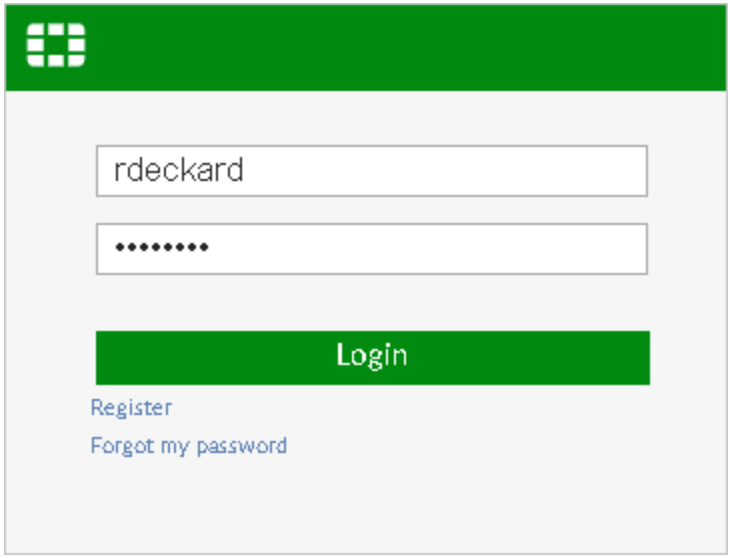
2. The user's registration is successful, and their information has been sent to the administrator for approval.



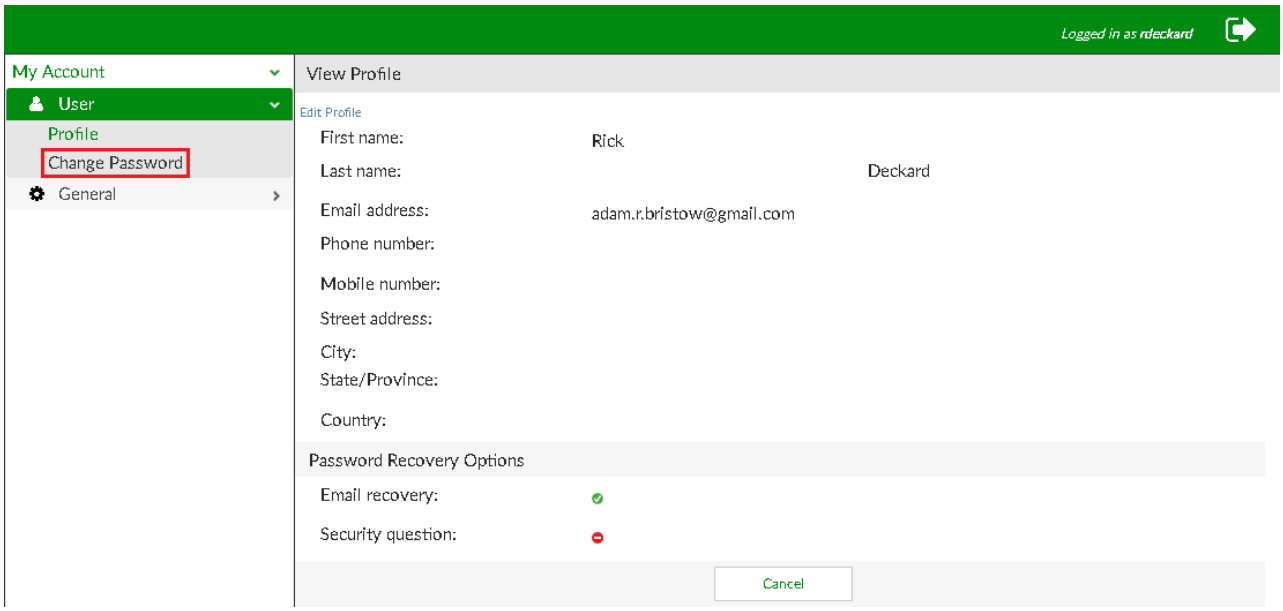
3. When the administrator has enabled the user's account, the user will receive an activation welcome email. The user's login information will be listed.



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

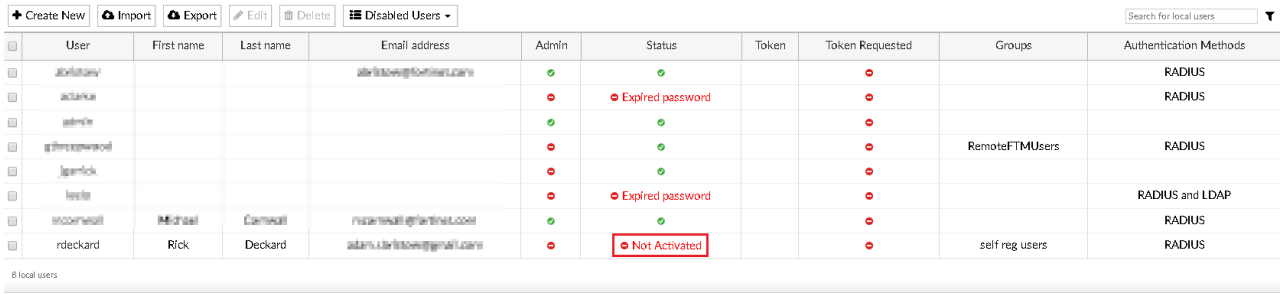


5. The user is now logged into their account where they can review their information.
As recommended in the user's welcome email, the user may change their password. However, this is optional.

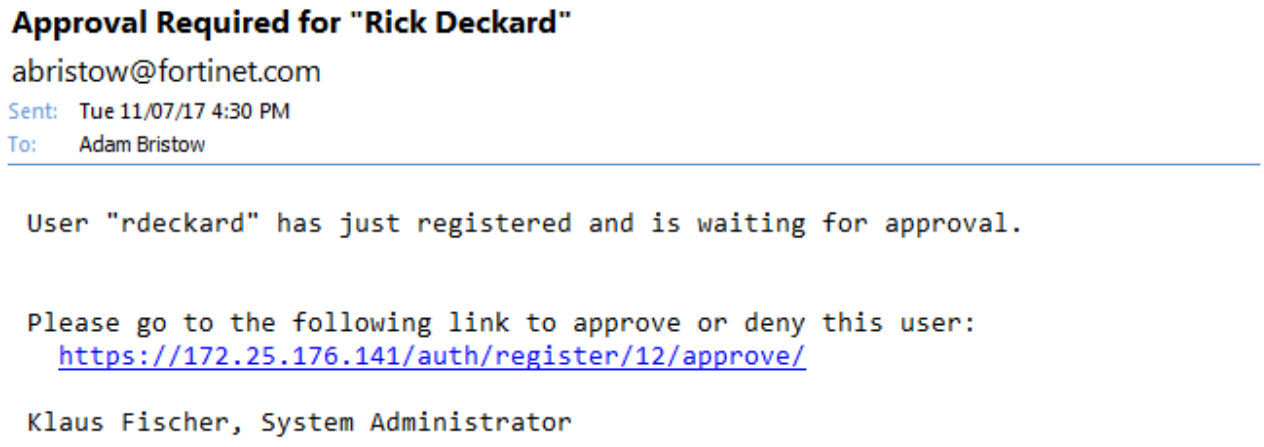


Results - Administrator approval

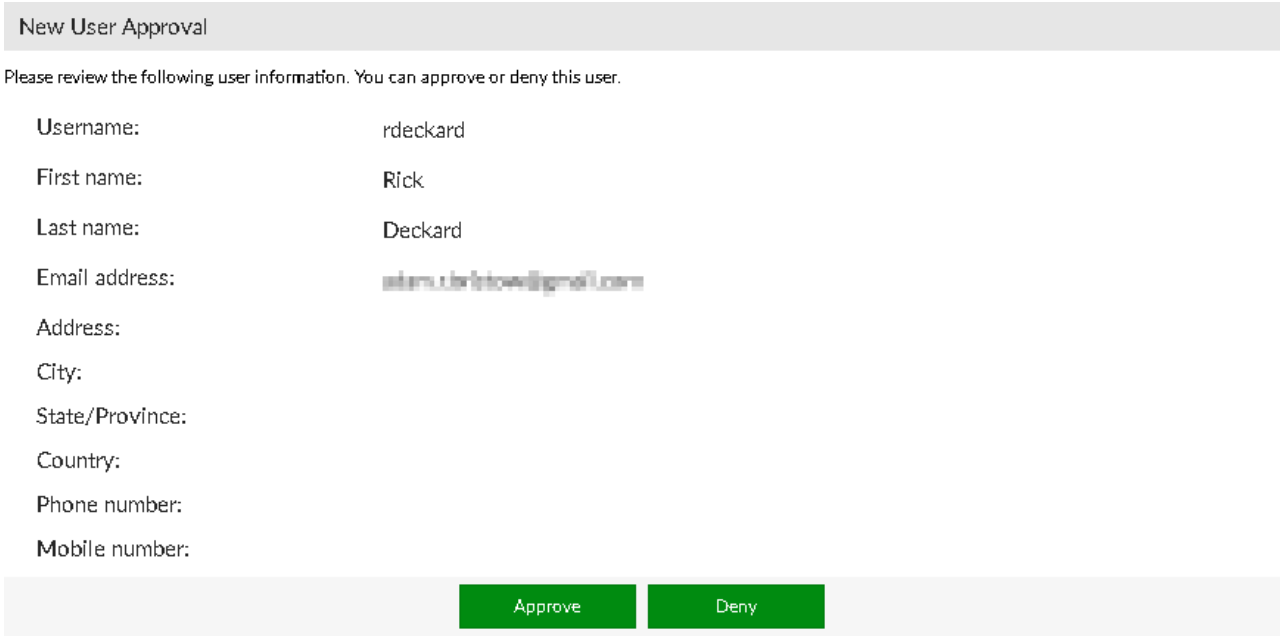
1. After receiving the user's registration request, in the FortiAuthenticator as the administrator, go to **Authentication > User Management > Local Users**. The user has been added, but their **Status** is listed as **Not Activated**.



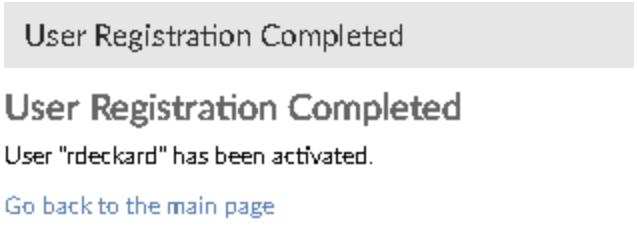
2. In the administrator's email account, open the user's **Approval Required** email. The user's full name will appear in the email's subject, along with their username in the email's body.
Select the link to approve or deny the user.



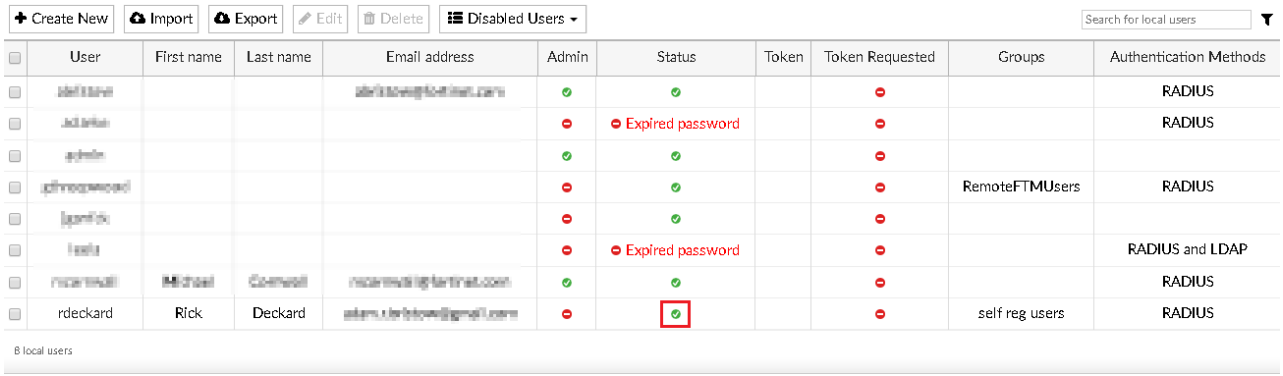
3. The link will take you to the **New User Approval** page, where you can review the user's information and either approve or deny the user's full registration.
Select **Approve**.



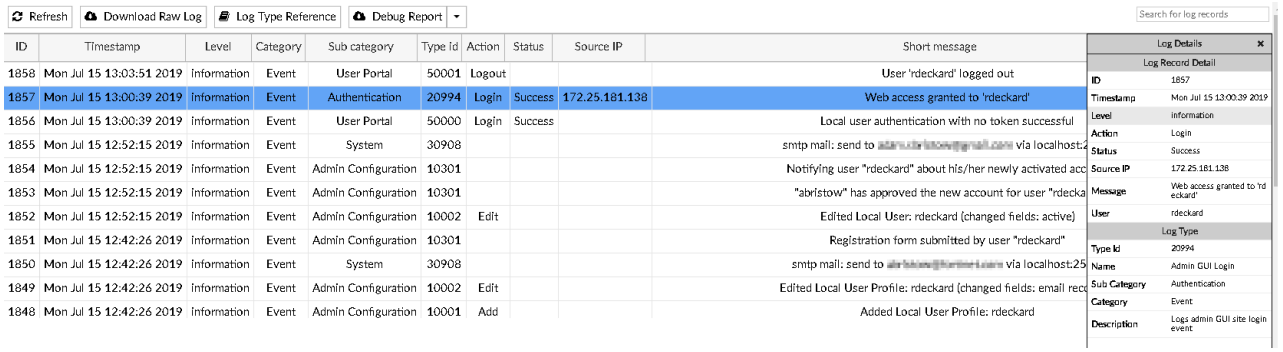
4. The user has now been approved and activated by the administrator.



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



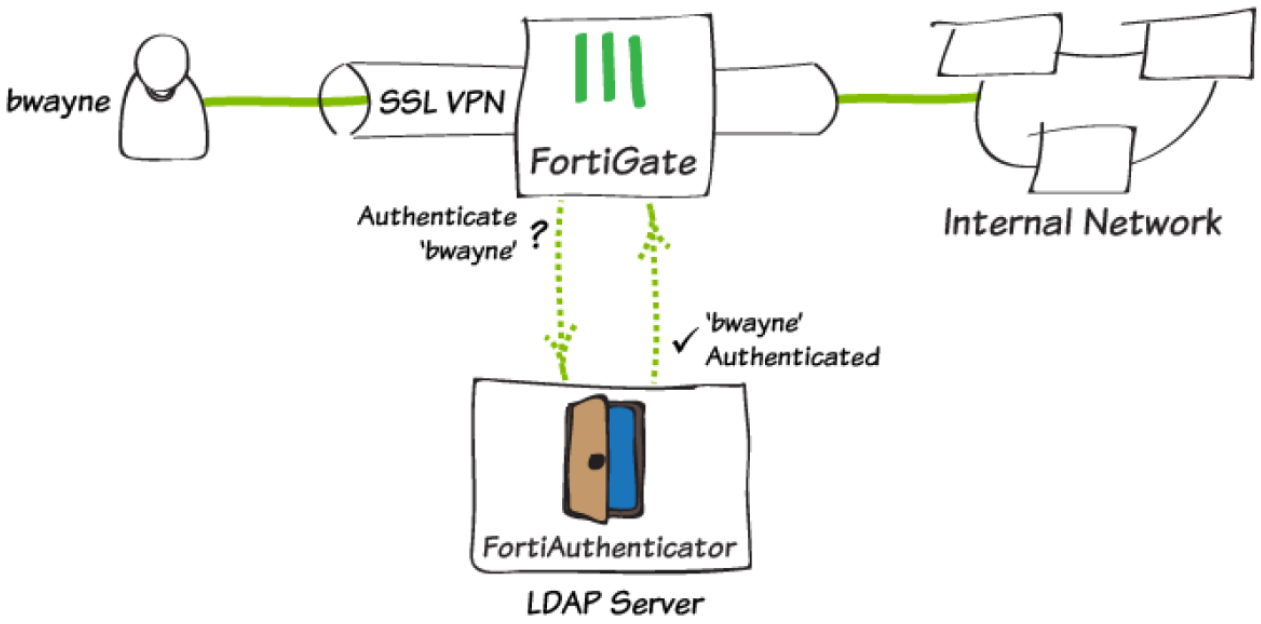
5. You can also go to **Logging > Log Access > Logs** to view the successful login of the user and more information.



VPNs

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

LDAP authentication for SSL VPN with FortiAuthenticator



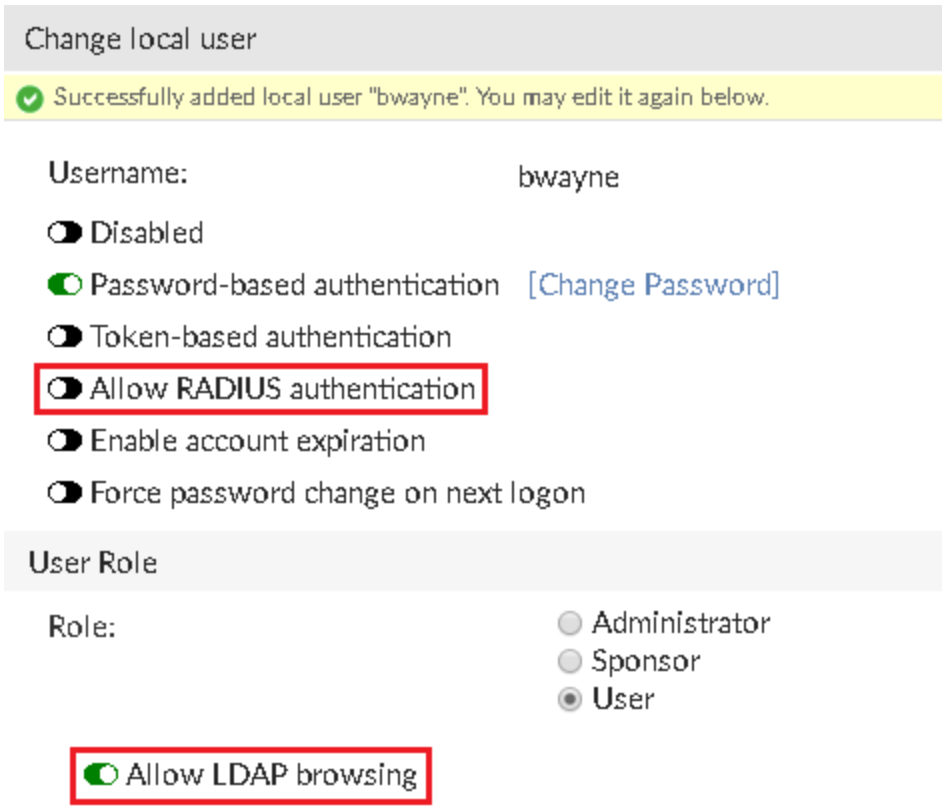
This recipe describes how to set up FortiAuthenticator to function as an LDAP server for FortiGate SSL VPN authentication. It involves adding users to FortiAuthenticator, setting up the LDAP server on the FortiAuthenticator, and then configuring the FortiGate to use the FortiAuthenticator as an LDAP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

Creating the user and user group on the FortiAuthenticator

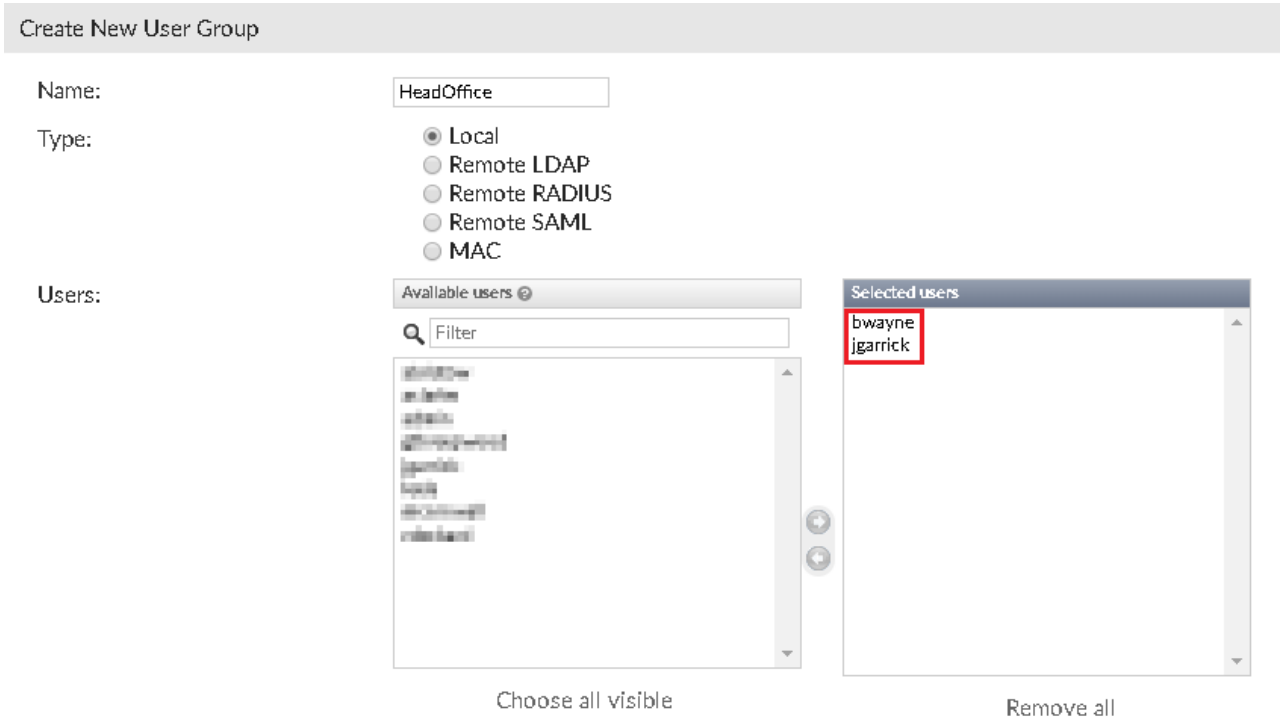
1. On the FortiAuthenticator, go to **Authentication > User Management > Local Users** and select **Create New**. Enter a name for the user, enter and confirm a password, and be sure to disable **Allow RADIUS authentication** — RADIUS authentication is not required for this recipe.

   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.

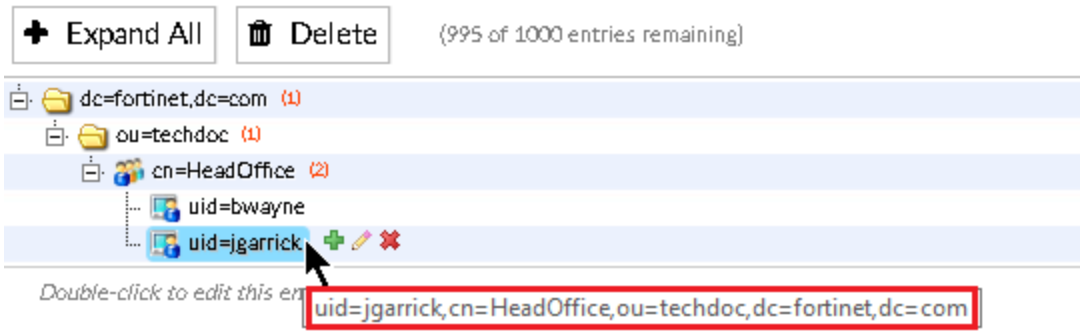


2. Create another user with the same settings. Later, you will use **jgarrick** on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use **bwayne** credentials to connect to the VPN tunnel.
3. Next go to **Authentication > User Management > User Groups**, and create a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



Creating the LDAP directory tree on the FortiAuthenticator

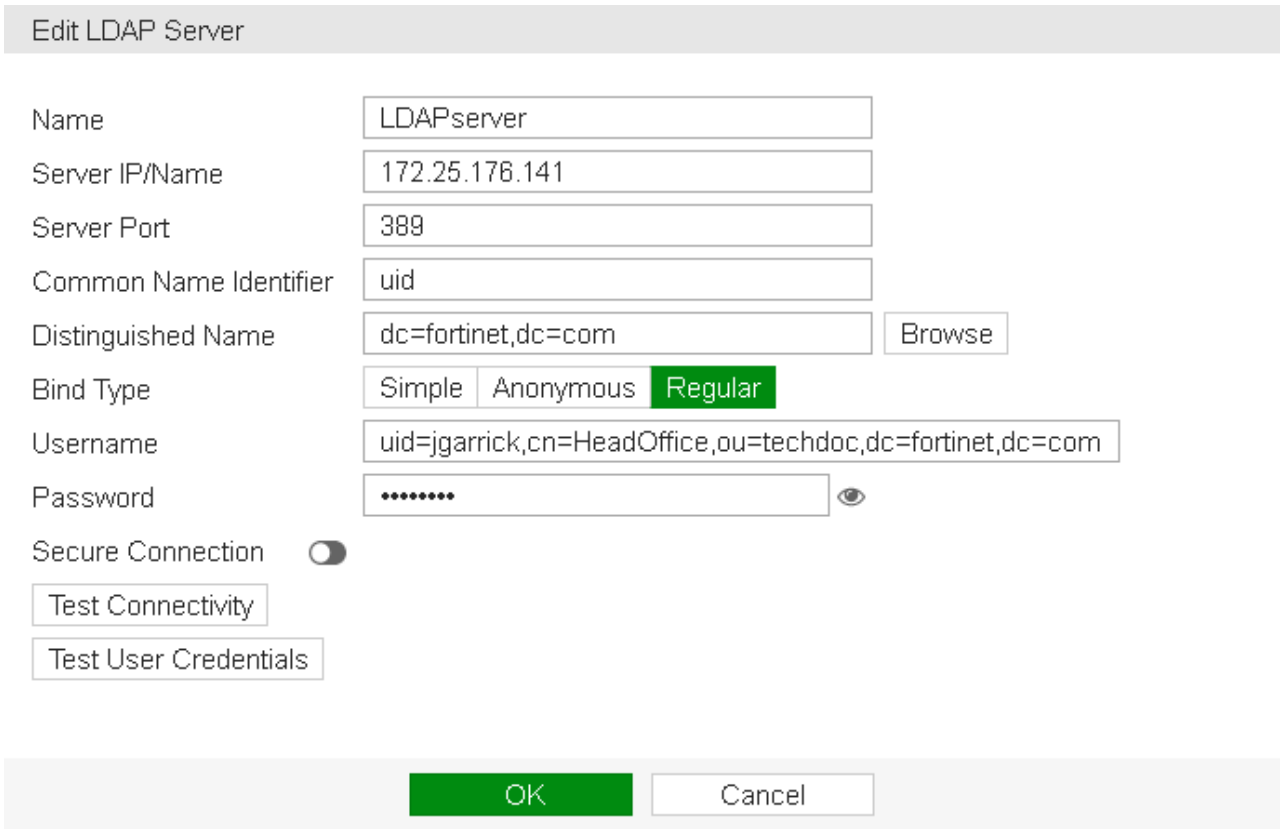
1. Go to **Authentication > LDAP Service > Directory Tree**, and create a Distinguished Name (DN). A DN is made up of Domain Components (DC).
   Both the users and user group created earlier are the User ID (UID) and the Common Name (CN) in the LDAP Directory Tree.
   Create an Organizational Unit (OU),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



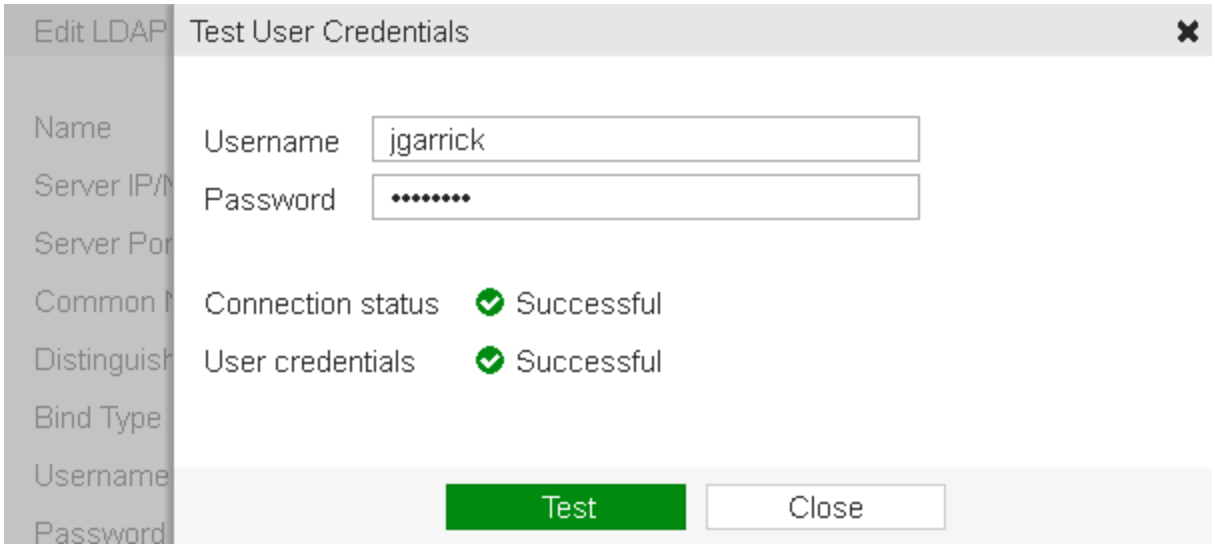
   Later, you will use **jgarrick** on the FortiGate to query the LDAP directory tree on FortiAuthenticator, and you will use **bwayne** credentials to connect to the VPN tunnel.

Connecting the FortiGate to the LDAP server

1. On the FortiGate, go to **User & Device > LDAP Servers**, and select **Create New**.
   Enter a name for the LDAP server connection.
   Set **Server IP/Name** to the IP of the FortiAuthenticator, and set the **Common Name Identifier** to **uid**.
   Set **Distinguished Name** to *dc=fortinet,dc=com*, and set the **Bind Type** to **Regular**.
   Enter the user DN for **jgarrick** of the LDAP server, and enter the user's **Password**.
   The DN is an account that the FortiGate uses to query the LDAP server.

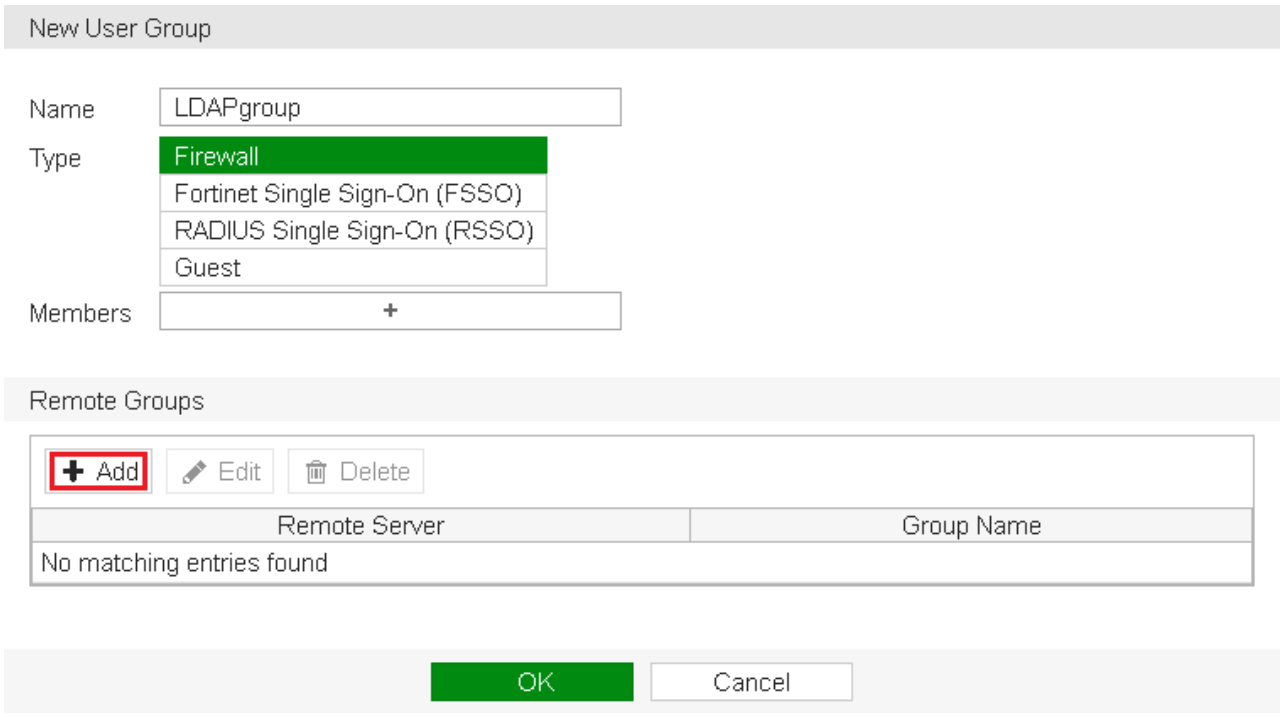


2. Select **Test Connectivity** to determine a successful connection.
Then select **Test User Credentials** to query the LDAP directory using **jgarrick**'s credentials. The query is successful.

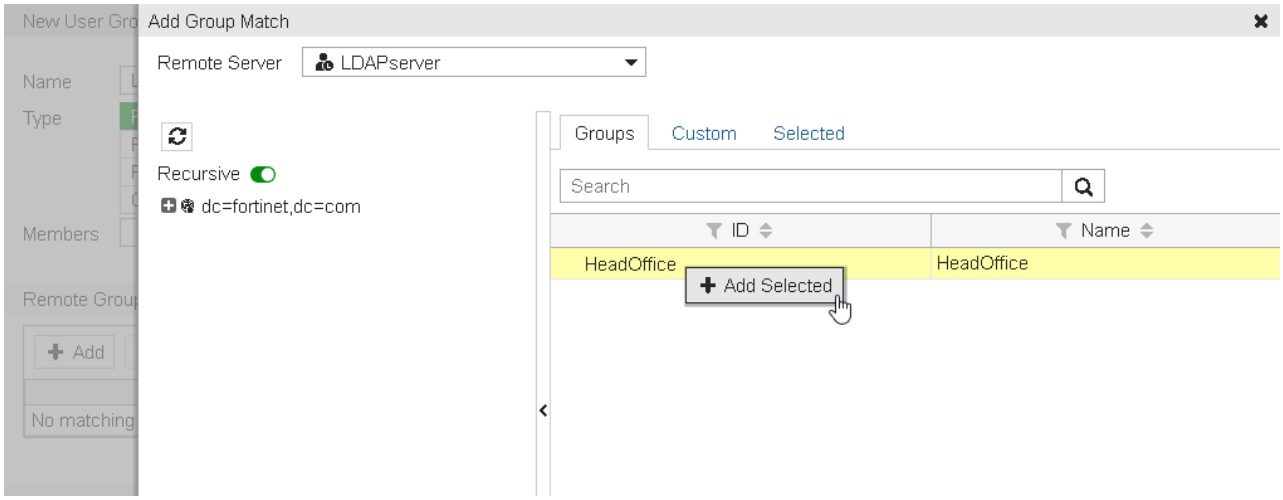


Creating the LDAP user group on the FortiGate

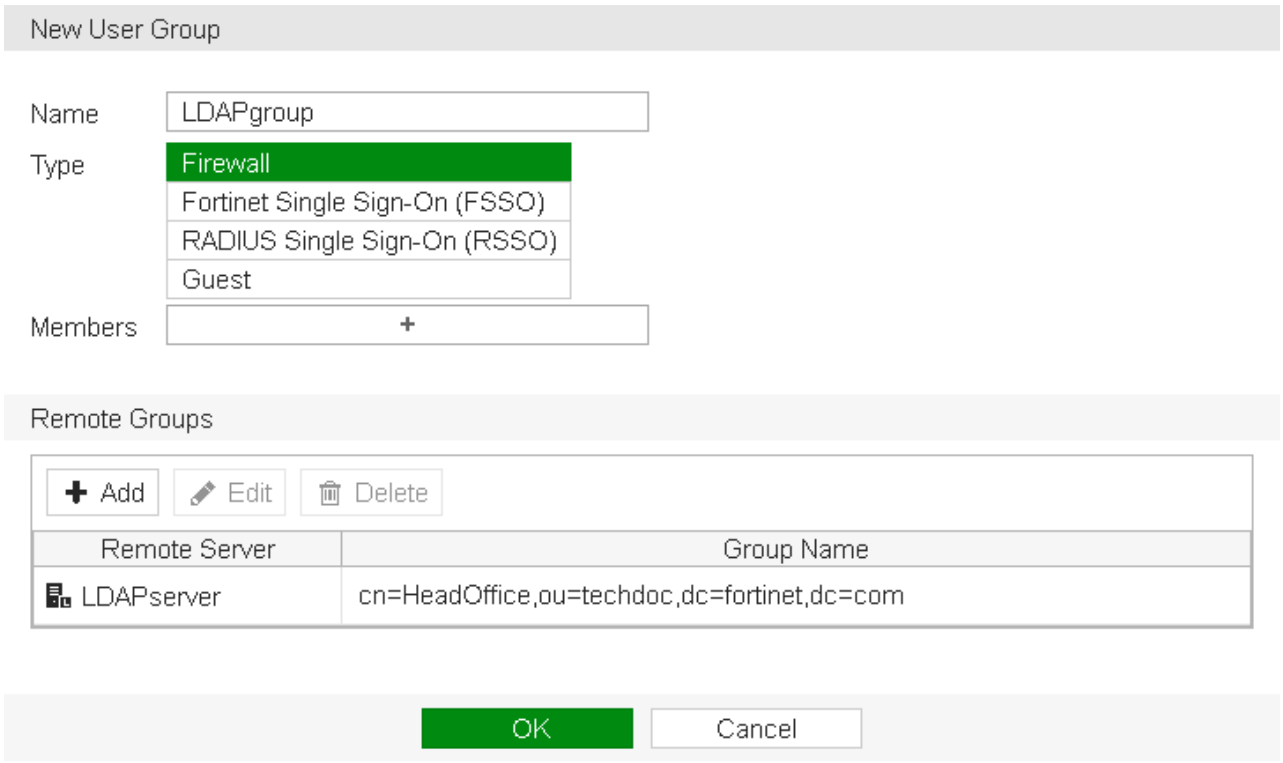
1. Go to **User & Device > User Groups**, and select **Create New**.
Enter a name for the user group. Under **Remote Groups** select **Add**.



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



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



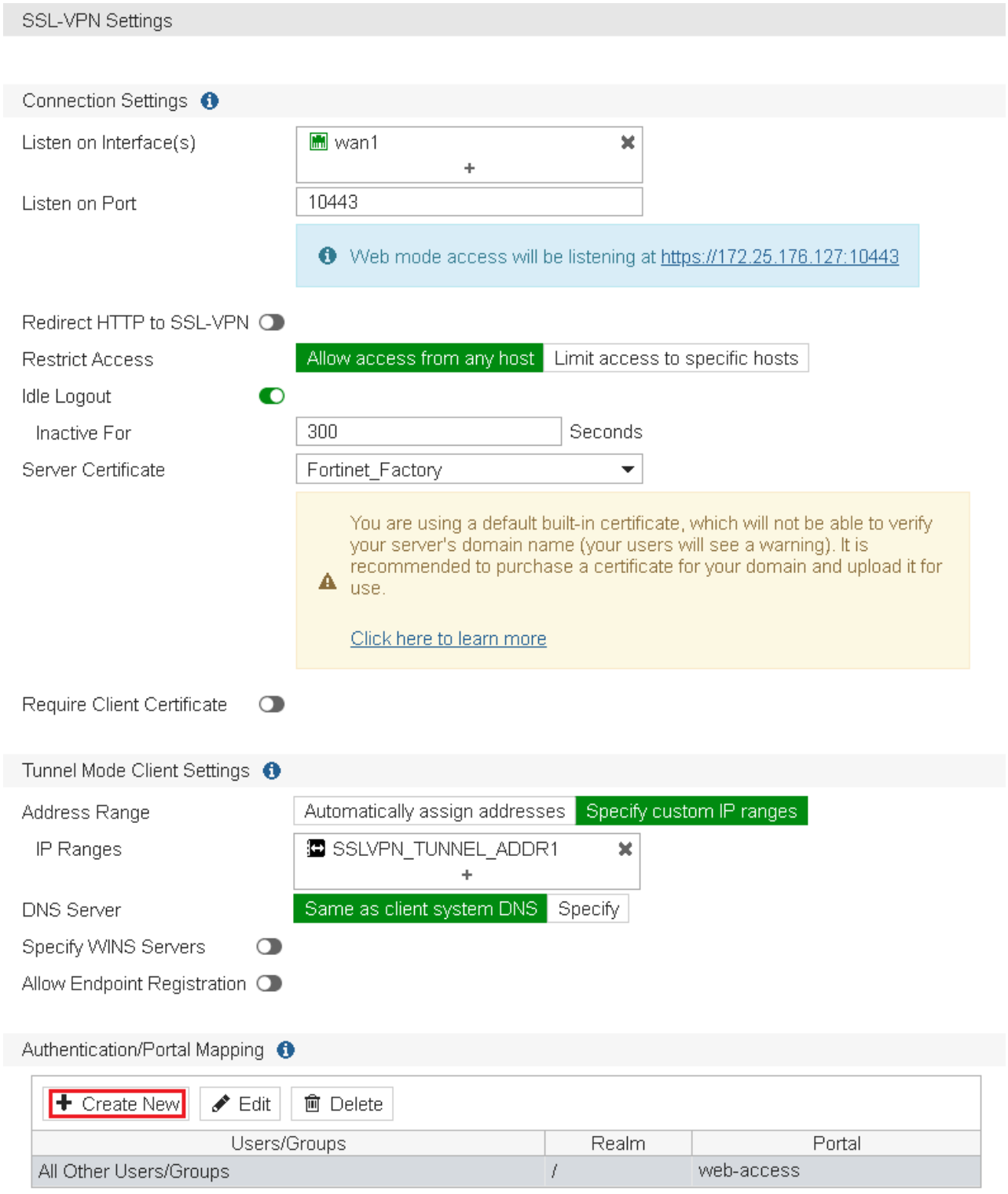
Configuring the SSL VPN

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

2. Go to **VPN > SSL-VPN Settings**.
   Under **Connection Settings** set **Listen on Port** to **10443**.

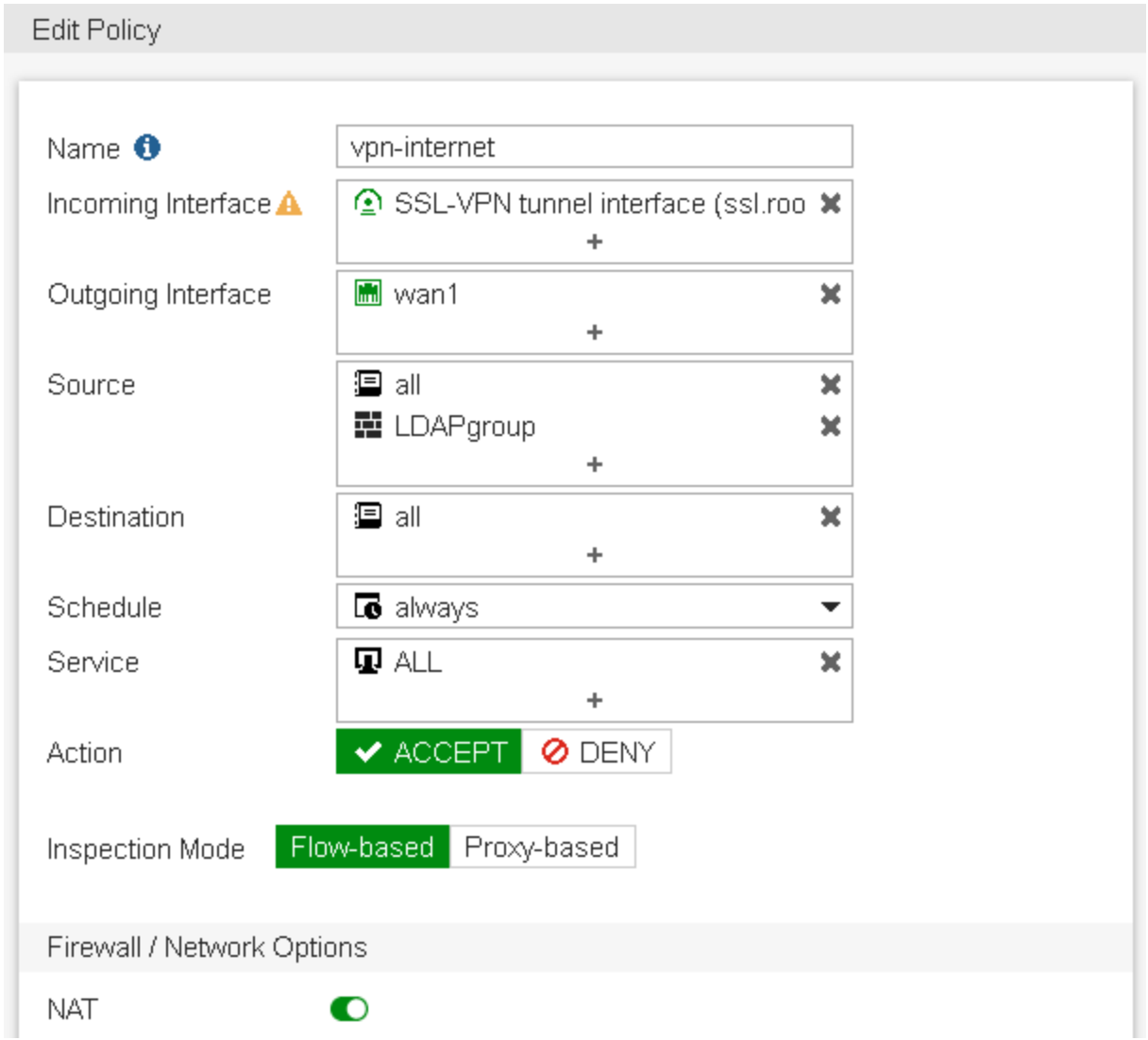
Under **Tunnel Mode Client Settings**, select **Specify custom IP ranges** and set it to **SSLVPN_TUNNEL_ADDR1**.

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



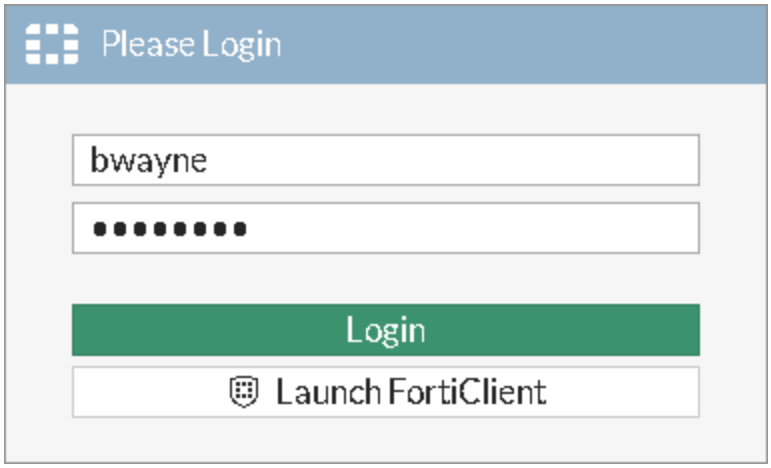
3. Assign the **LDAPgroup** user group to the **full-access** portal, and assign **All Other Users/Groups** to the desired portal. Select **Apply**.

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

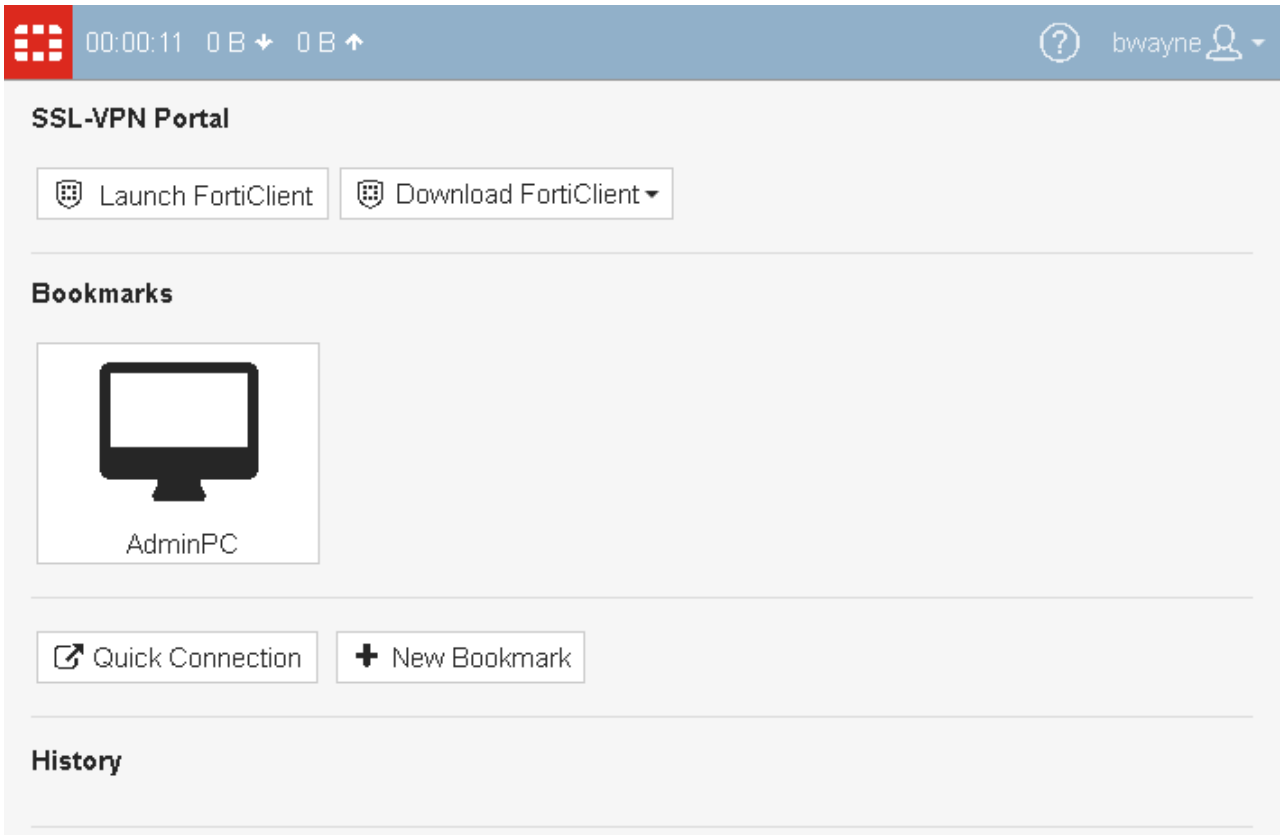


Results

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



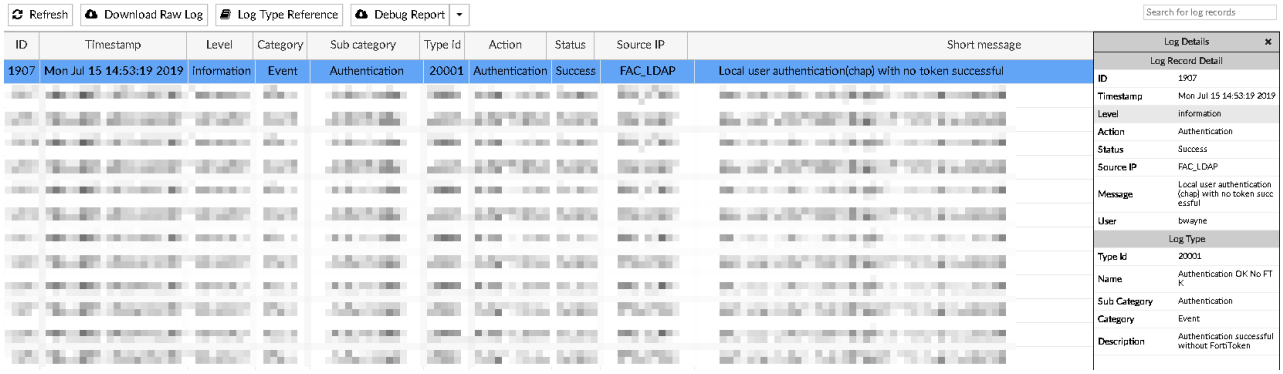
2. The user is now successfully logged into the SSL VPN Portal.



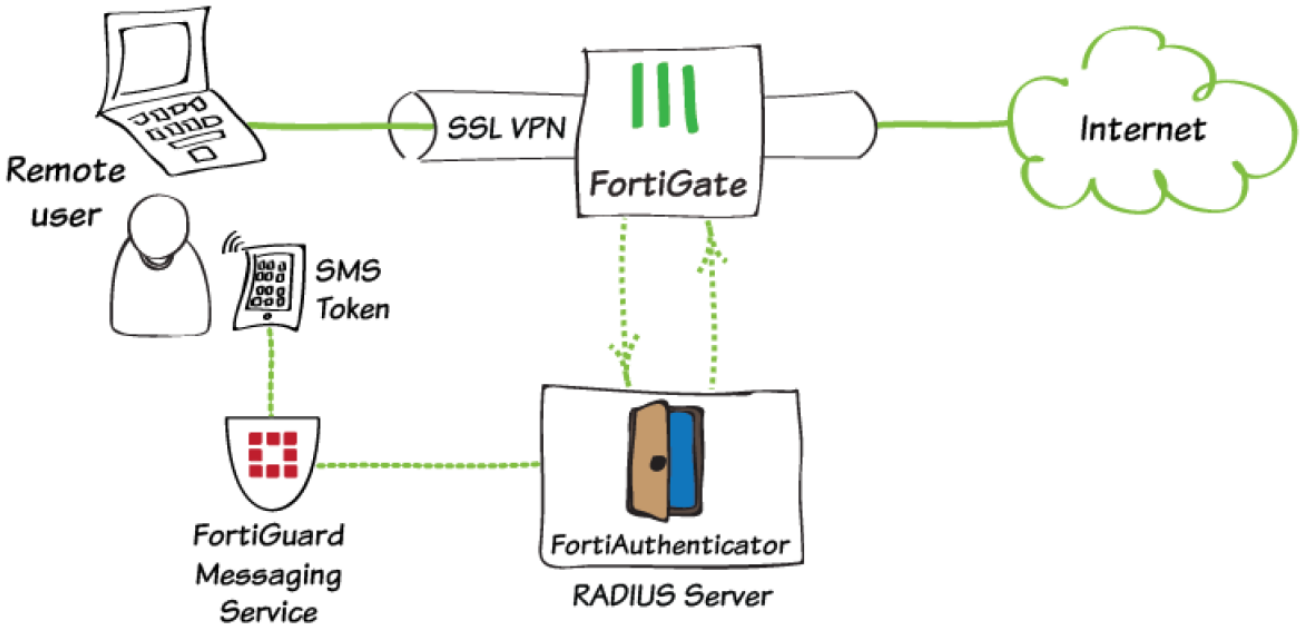
3. On the FortiGate, go to **Monitor > SSL-VPN Monitor** to confirm the connection.

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.



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.

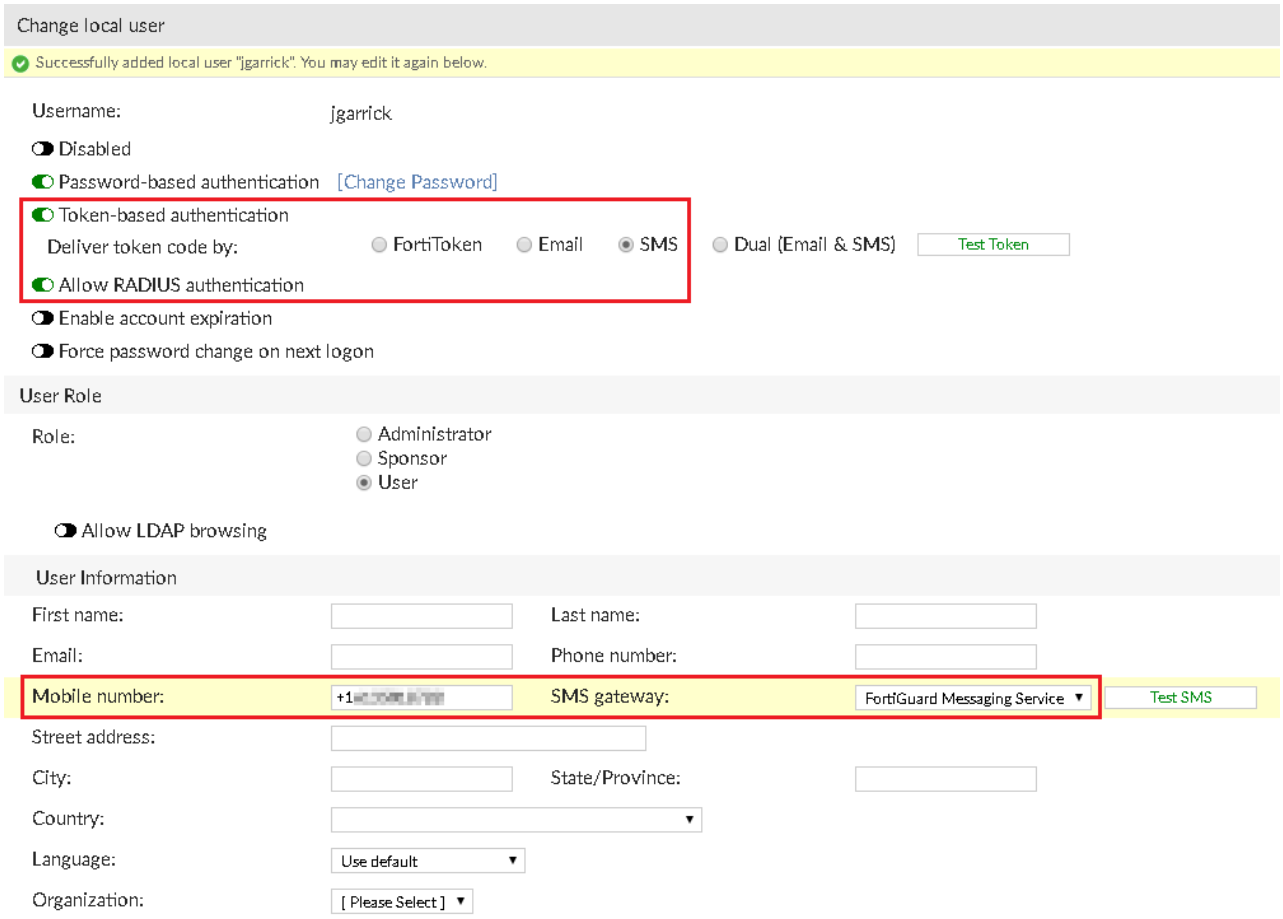
Although this recipe uses the FortiGuard Messaging Service, it will also work with any compatible SMS service you configure as an SMS Gateway.

Creating an SMS user and user group on the FortiAuthenticator

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

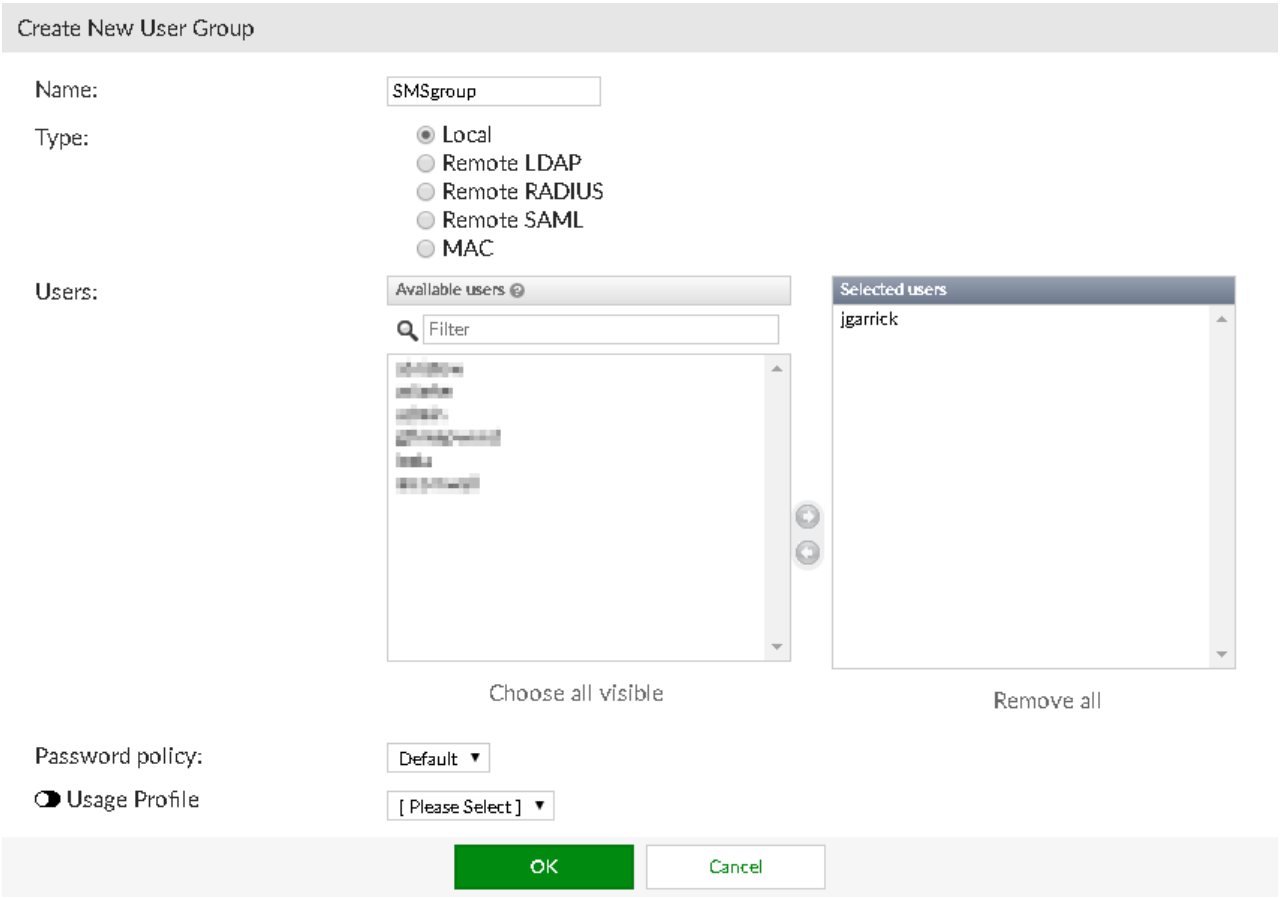
   `+[international-number]`

   Enable **Allow RADIUS authentication**.



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

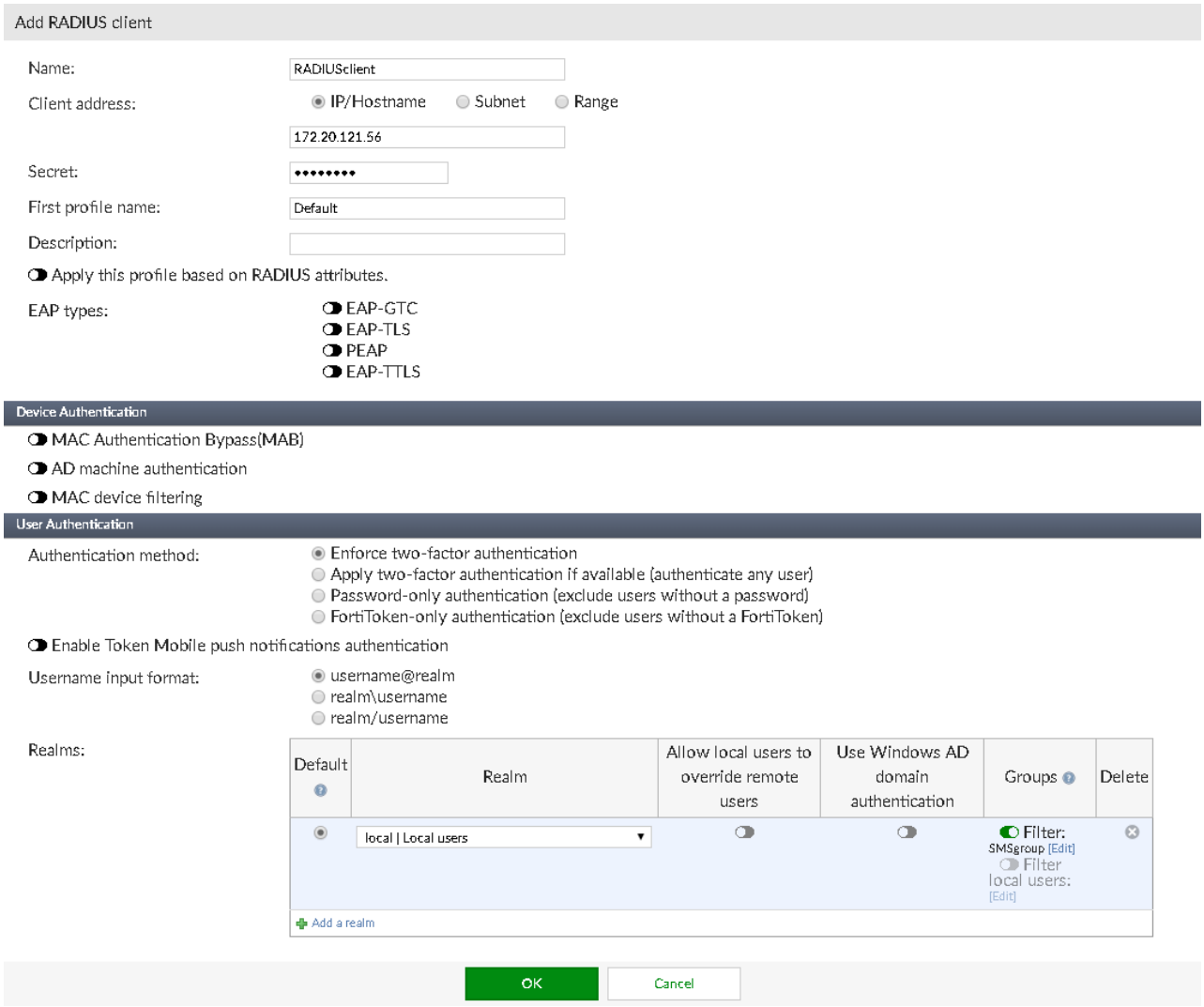
(in the example, *SMSgroup*).



Configuring the FortiAuthenticator RADIUS client

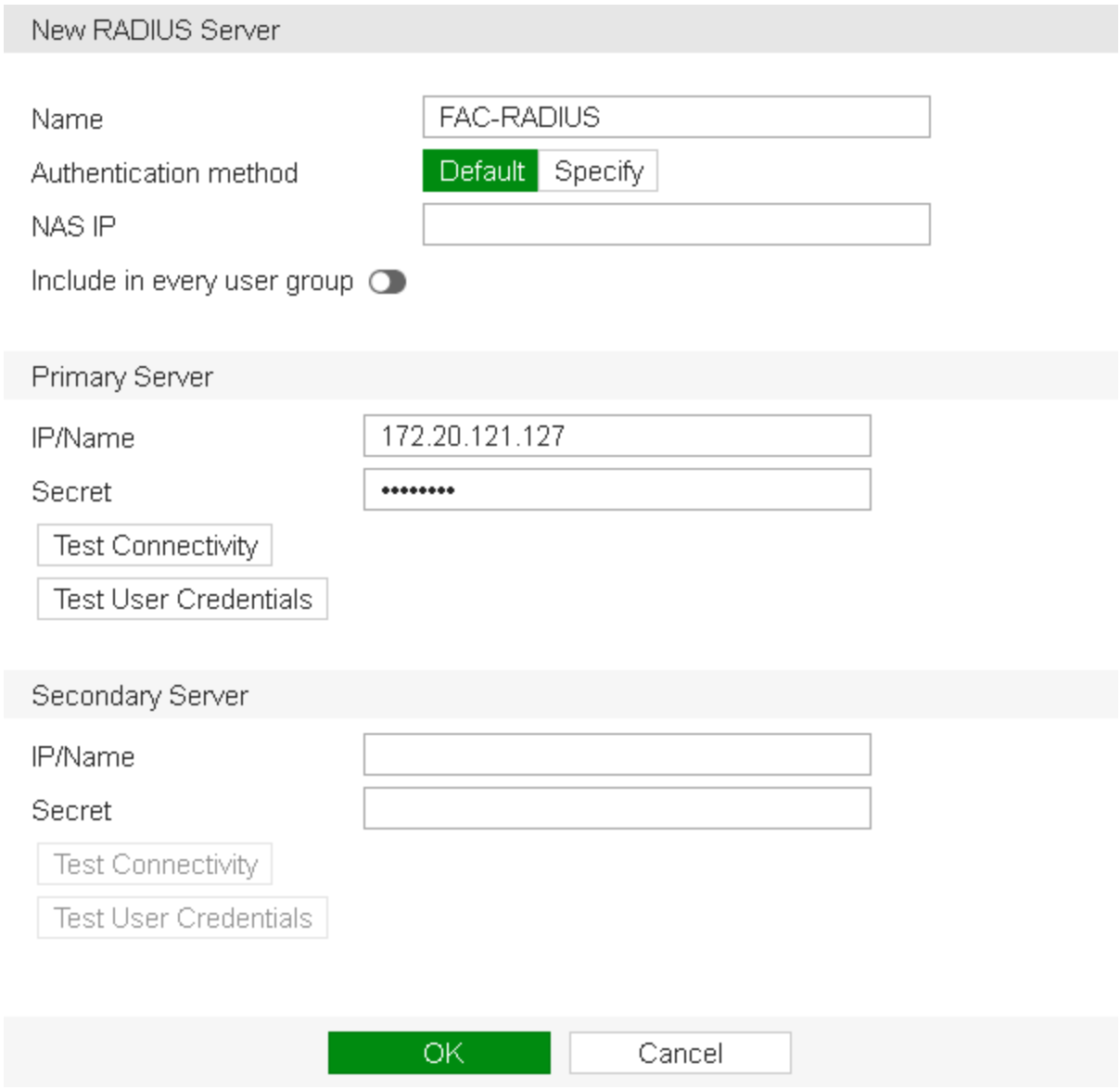
1. Go to **Authentication > RADIUS Service > Clients** and create a new RADIUS client.
   Enter a **Name** for the RADIUS client (the FortiGate) and enter its IP address (in the example, *172.20.121.56*).

Choose to **Enforce two-factor authentication** and add the SMS user group to the **Realms** group filter as shown.

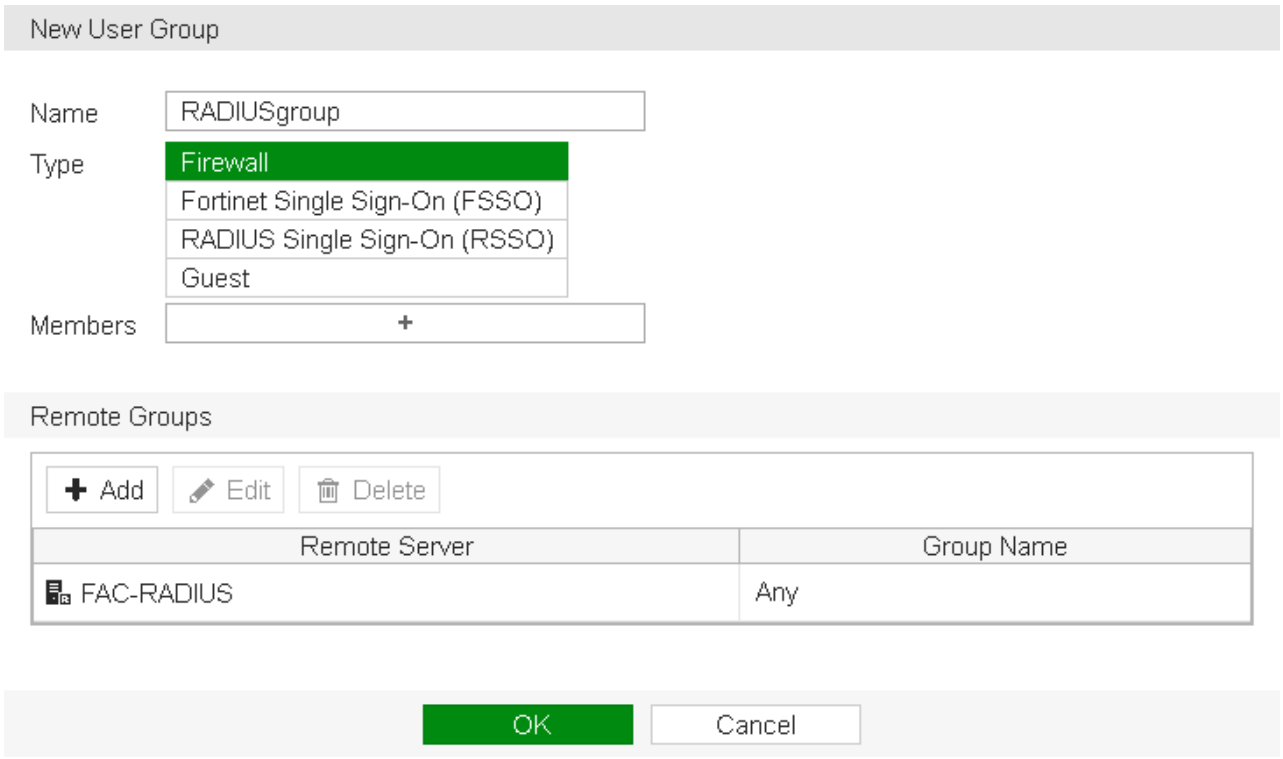


Configuring the FortiGate authentication settings

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

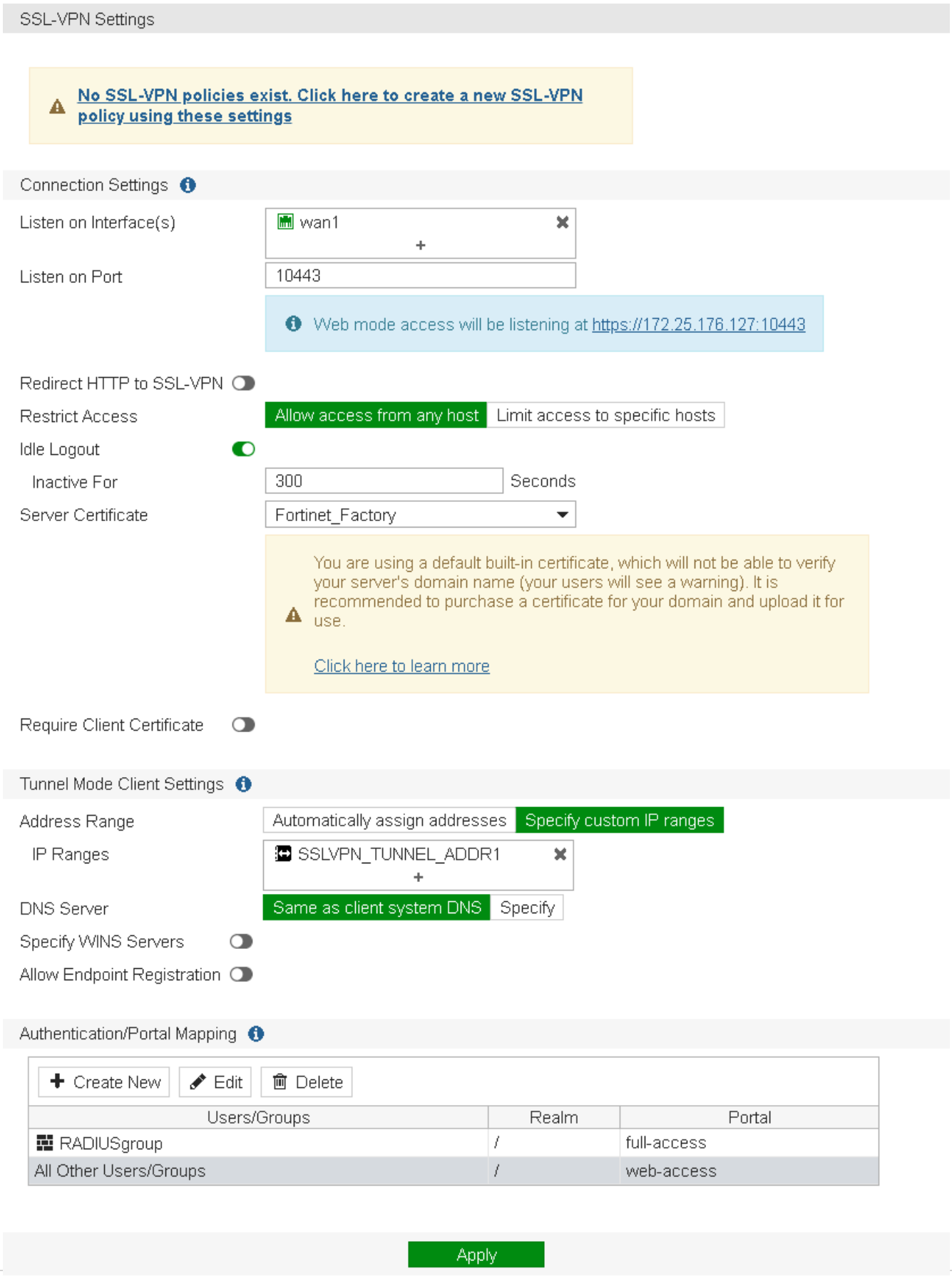


2. Next, go to **User & Device > User Groups** and create a RADIUS user group called **RADIUSgroup**. Set the **Type** to **Firewall** and add the RADIUS server to the **Remote groups** table.



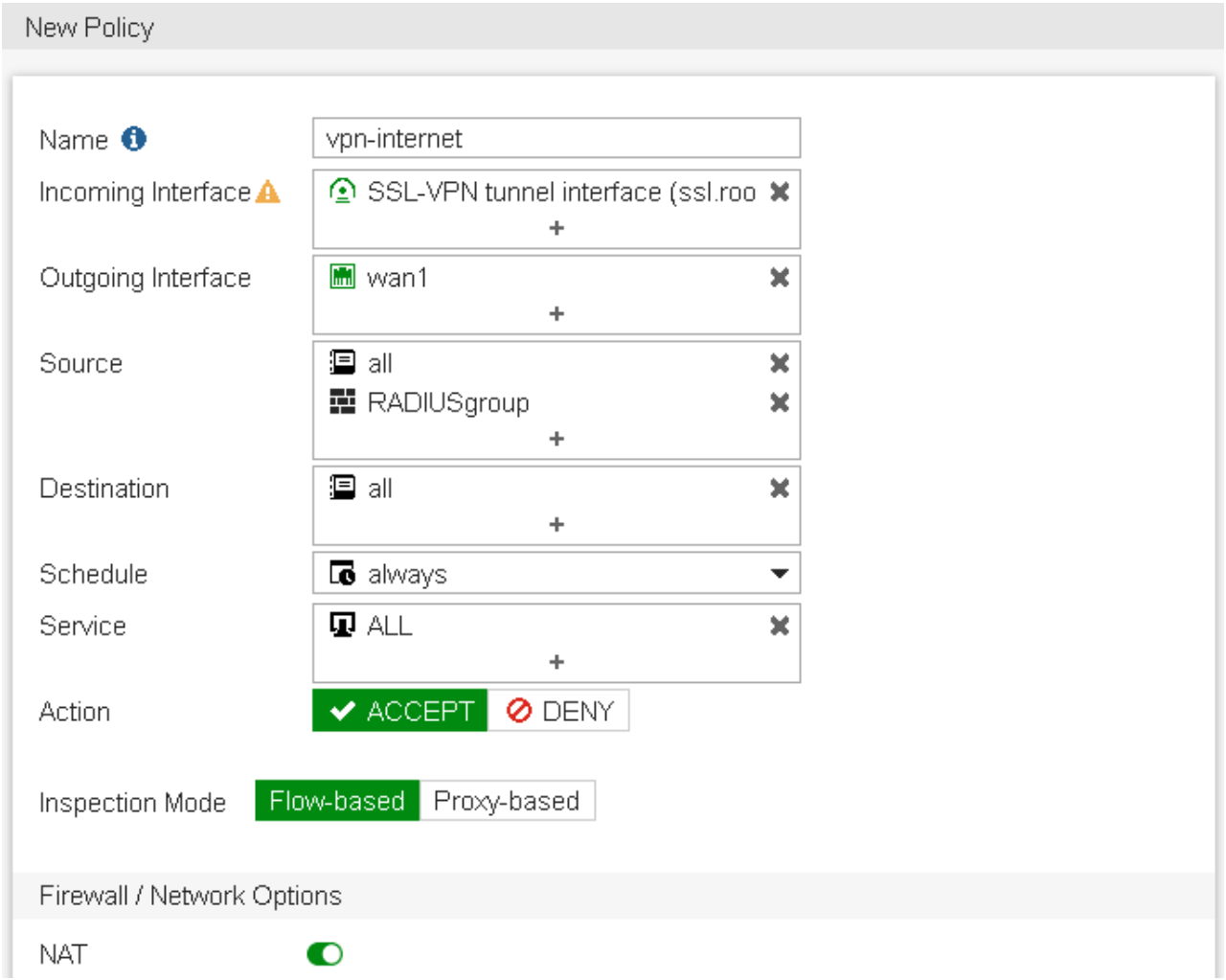
Configuring the SSL VPN

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

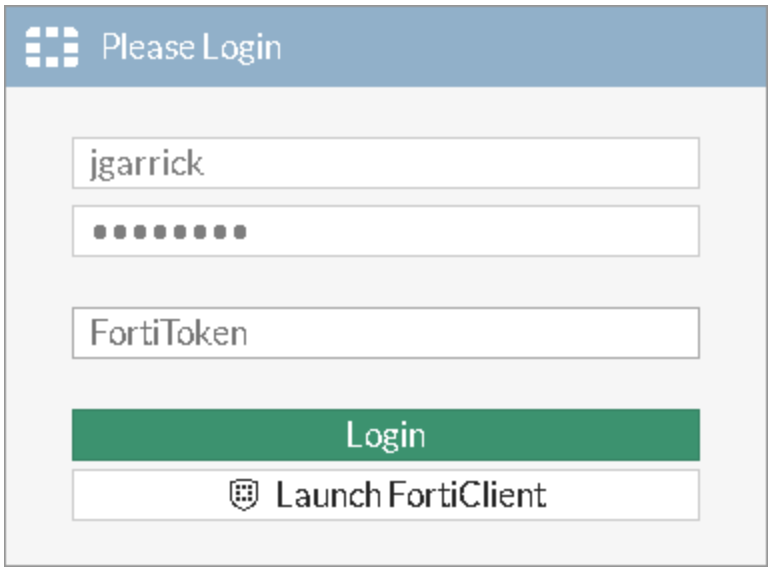
1. Go to **Policy & Objects > IPv4 Policy** and create a new SSL-VPN policy, including the **RADIUSgroup**, as shown.



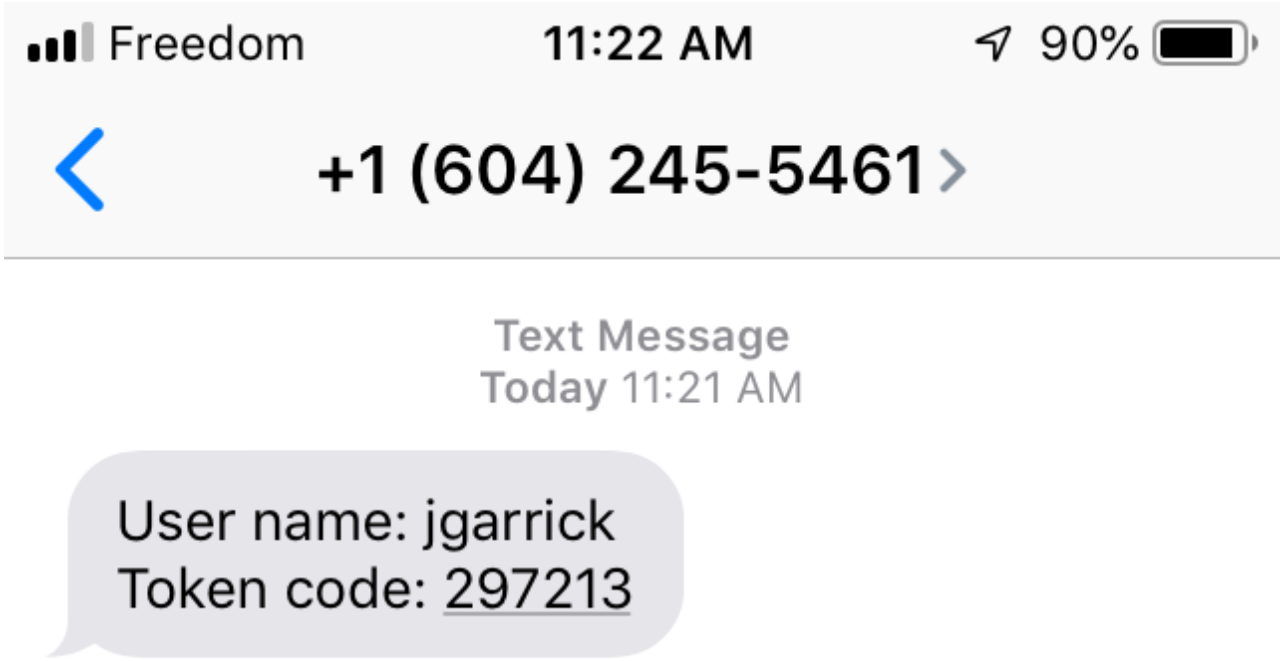
Results

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

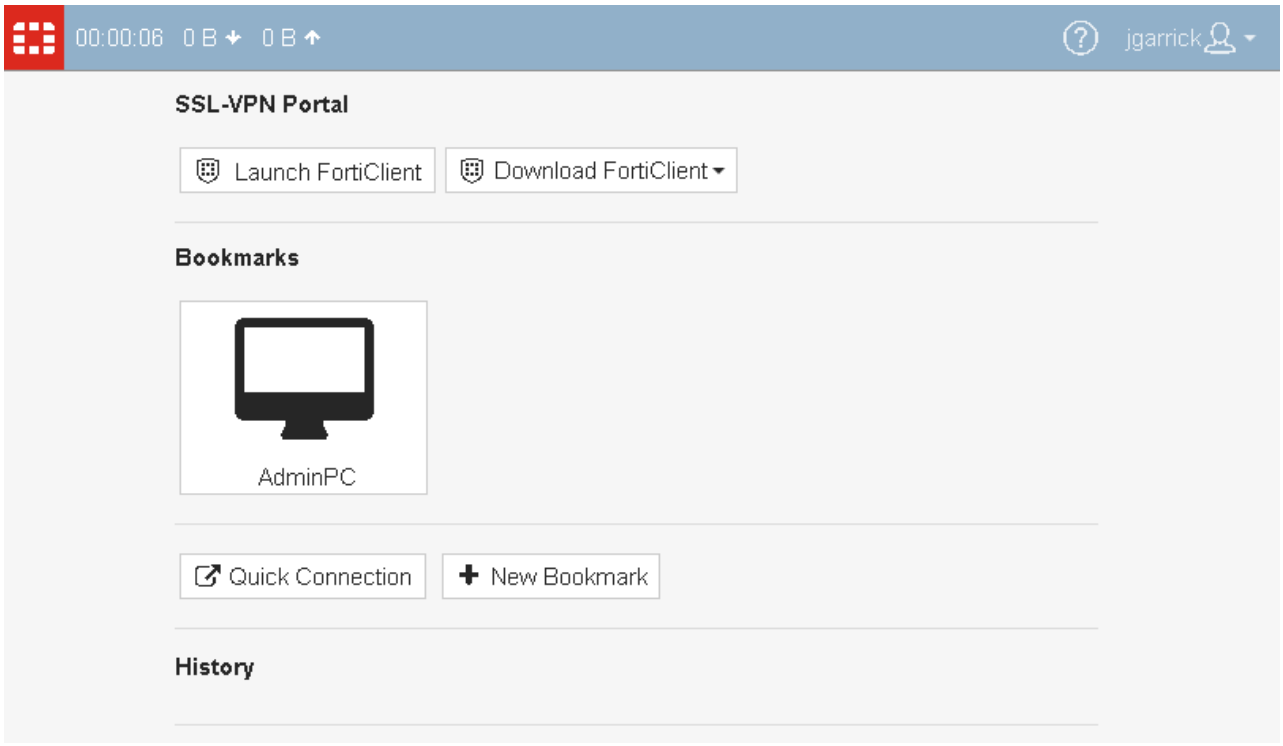
1. Open a browser and navigate to the SSL VPN web portal, in this case *https://172.25.176.127:10443*.
   Enter a valid username and password and select **Login**. You should be prompted to enter a **FortiToken Code**.



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**.

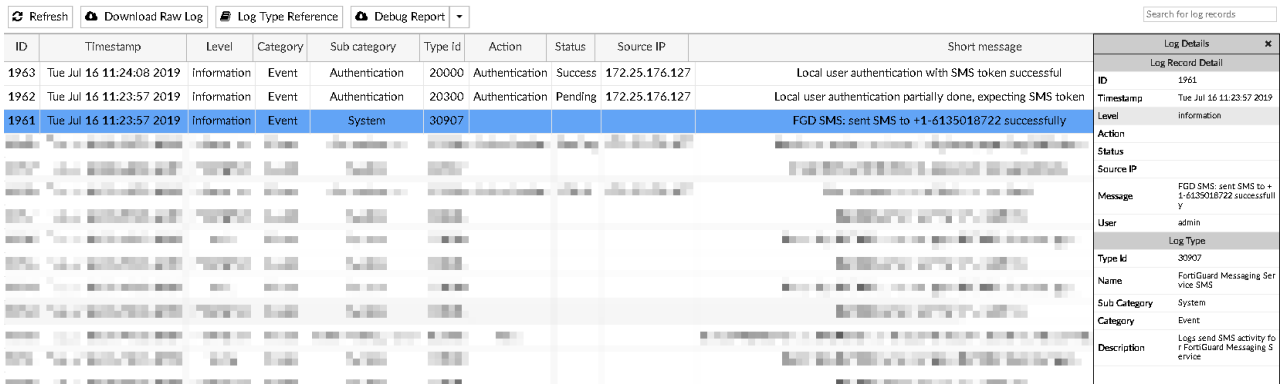

Freedom
11:22 AM
90%
+1 (604) 245-5461
Text Message
Today 11:21 AM
User name: jgarrick
Token code: 297213

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



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

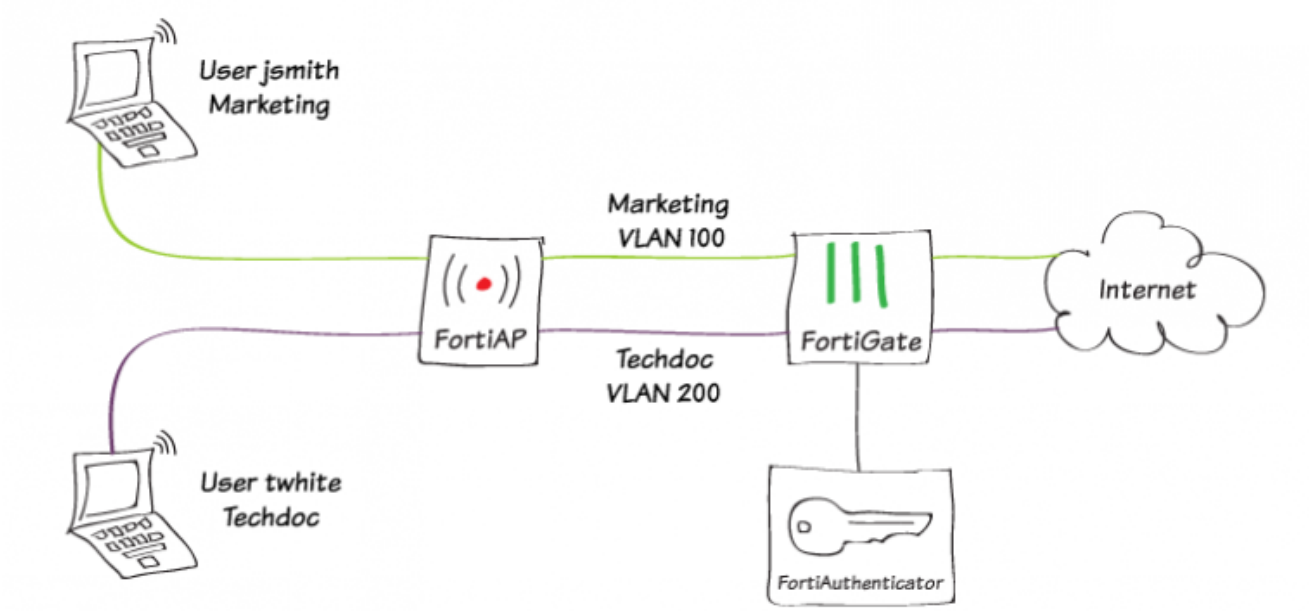
5. On the FortiAuthenticator, go to **Logging > Log Access > Logs** to confirm the user's connection.



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.

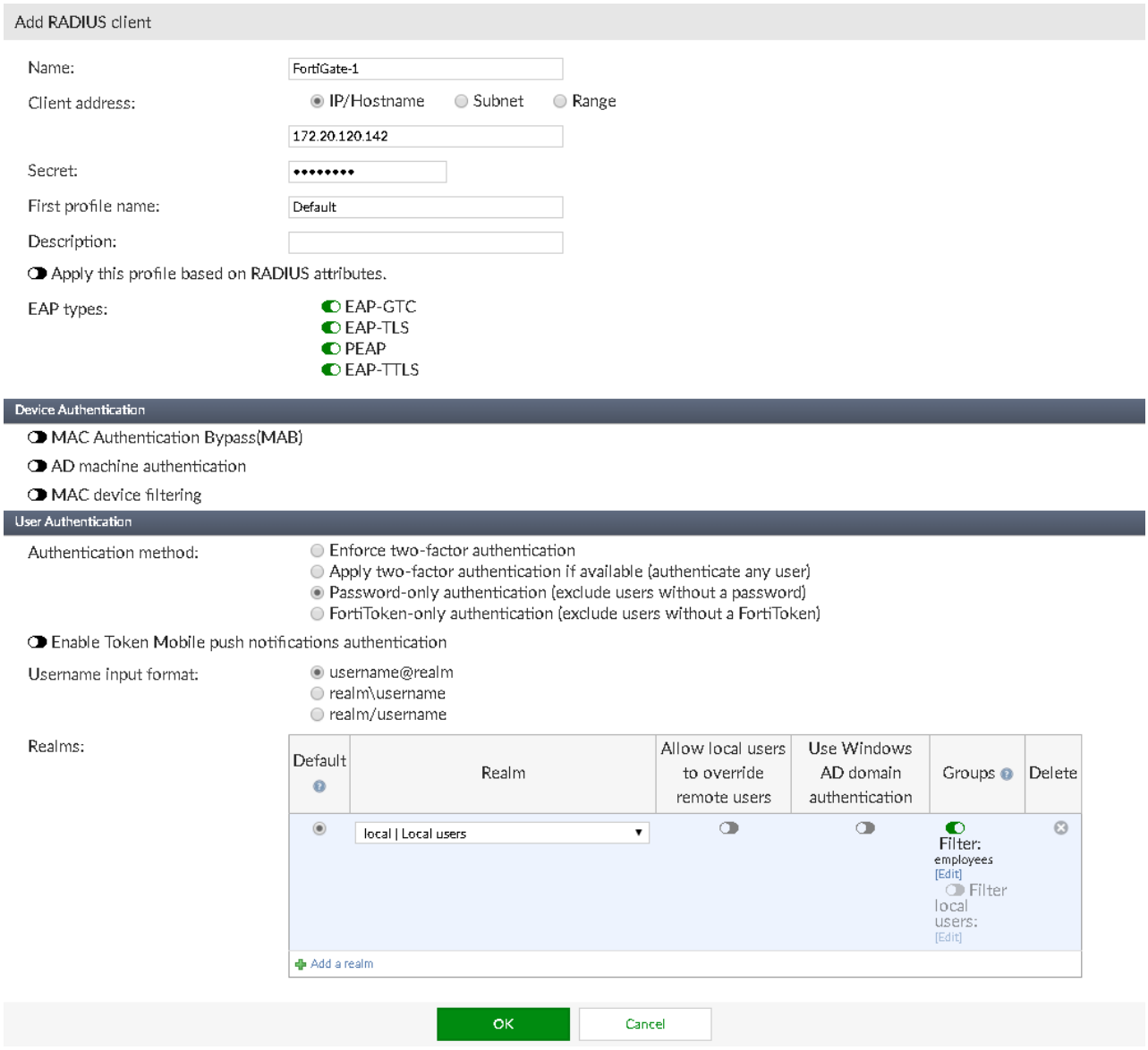
This example creates dynamic VLANs for the **Techdoc** and **Marketing** departments. The RADIUS server is a FortiAuthenticator. It is assumed a user group on the FortiAuthenticator has already been created (in this example, **employees**).

```
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 cer-
tificate.
                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]
```

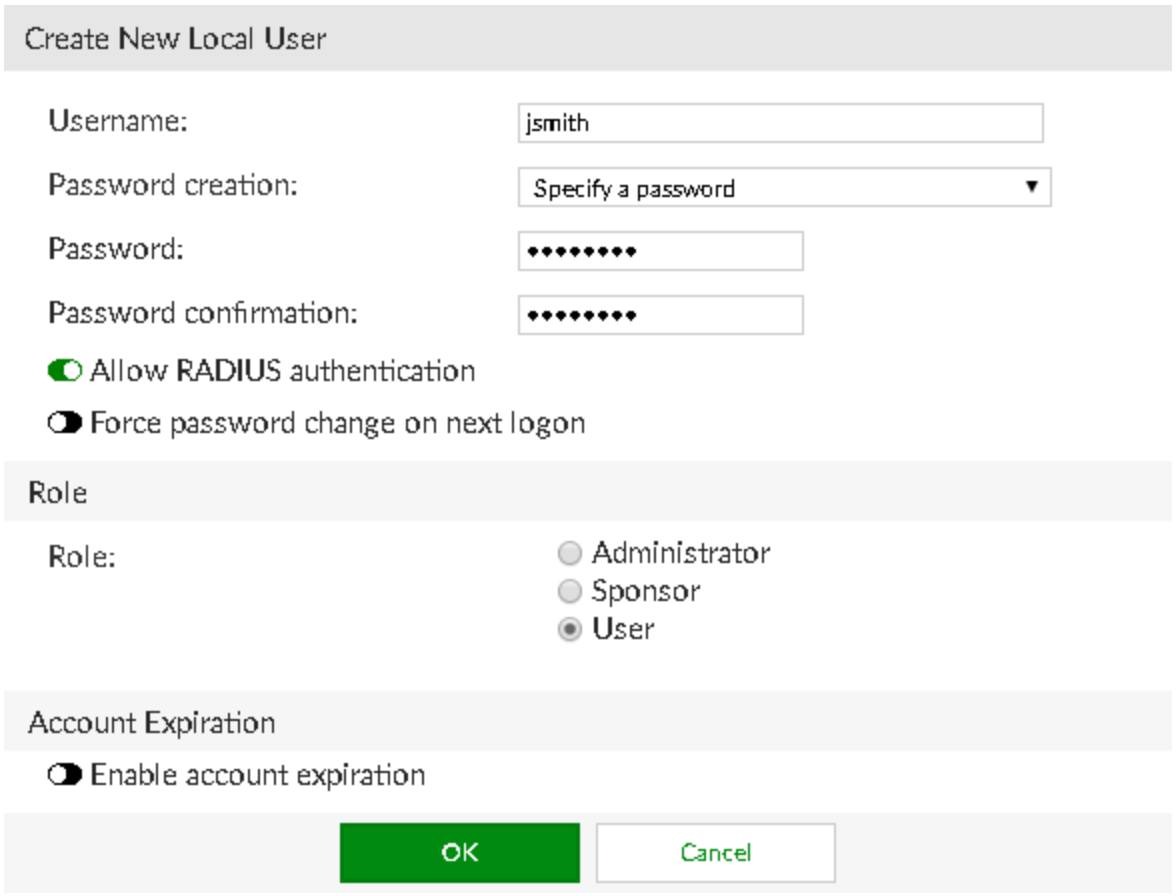
```
        set auto-update-days {integer}   Number of days to wait before requesting an updated
CA certificate (0 - 4294967295, 0 = disabled). range[0-4294967295]
```

Configuring the FortiAuthenticator

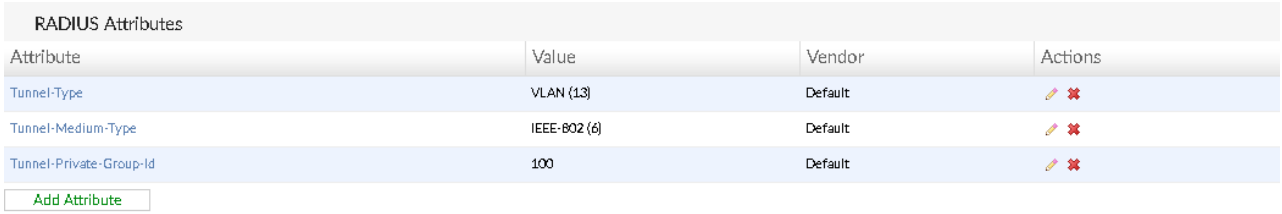
1. On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients** and register the FortiGate as a client.
   Enable all **EAP types**, set **Realm** to **local**, and apply the **employees** user group.



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



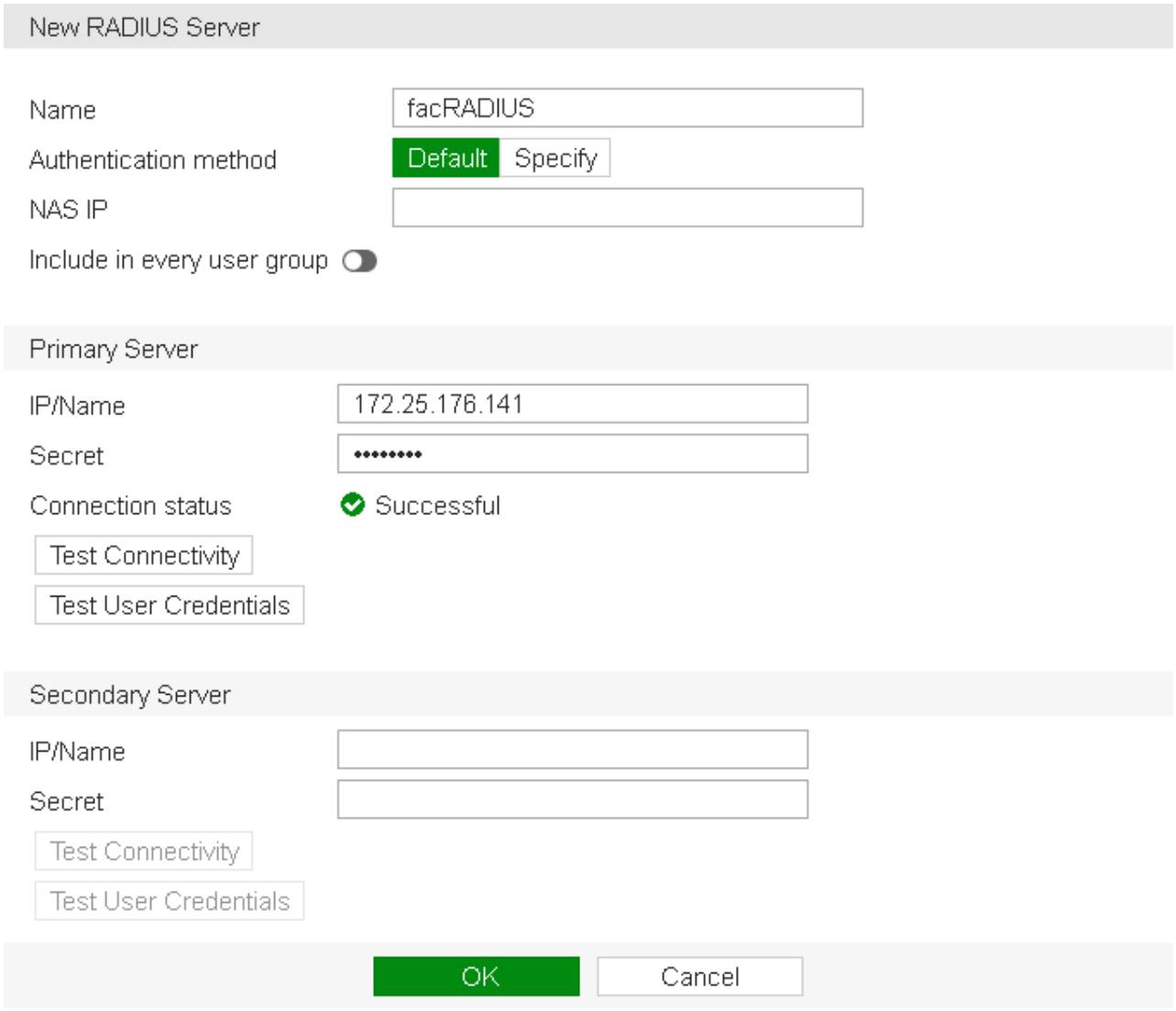
3. For each user, add the following RADIUS attributes which specify the VLAN information to be sent to the FortiGate. The **Tunnel-Private-Group-Id** attribute specifies the VLAN ID.
   In this example, **jsmith** is assigned VLAN **100** and **twhite** is assigned VLAN **200**.



Adding the RADIUS server to the FortiGate

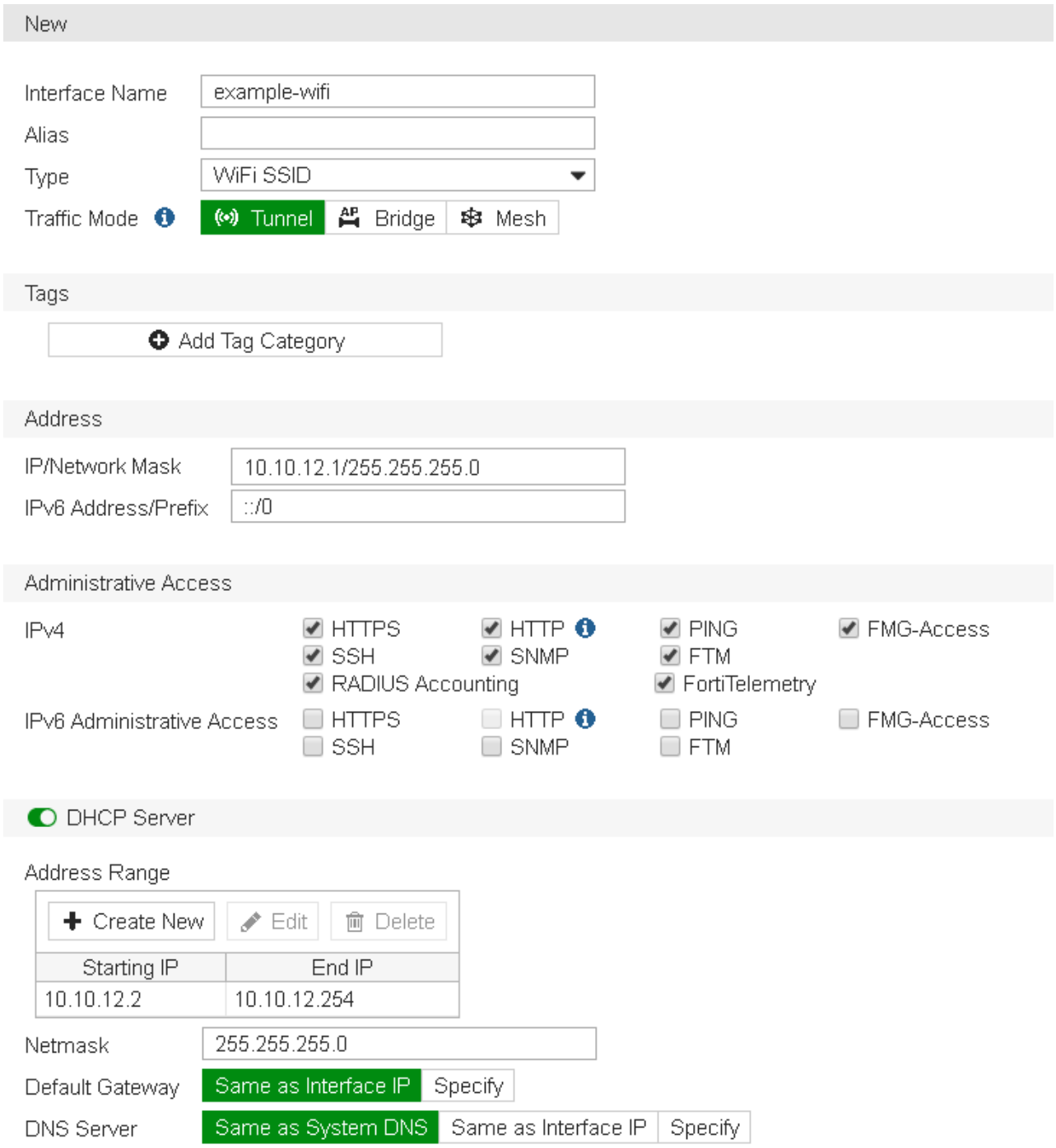
1. On the FortiGate, go to **User & Device > RADIUS Servers** and select **Create New**.
   Enter the FortiAuthenticator IP address and the server **Secret** entered on the FortiAuthenticator earlier.

Select **Test Connectivity** to confirm the successful connection.

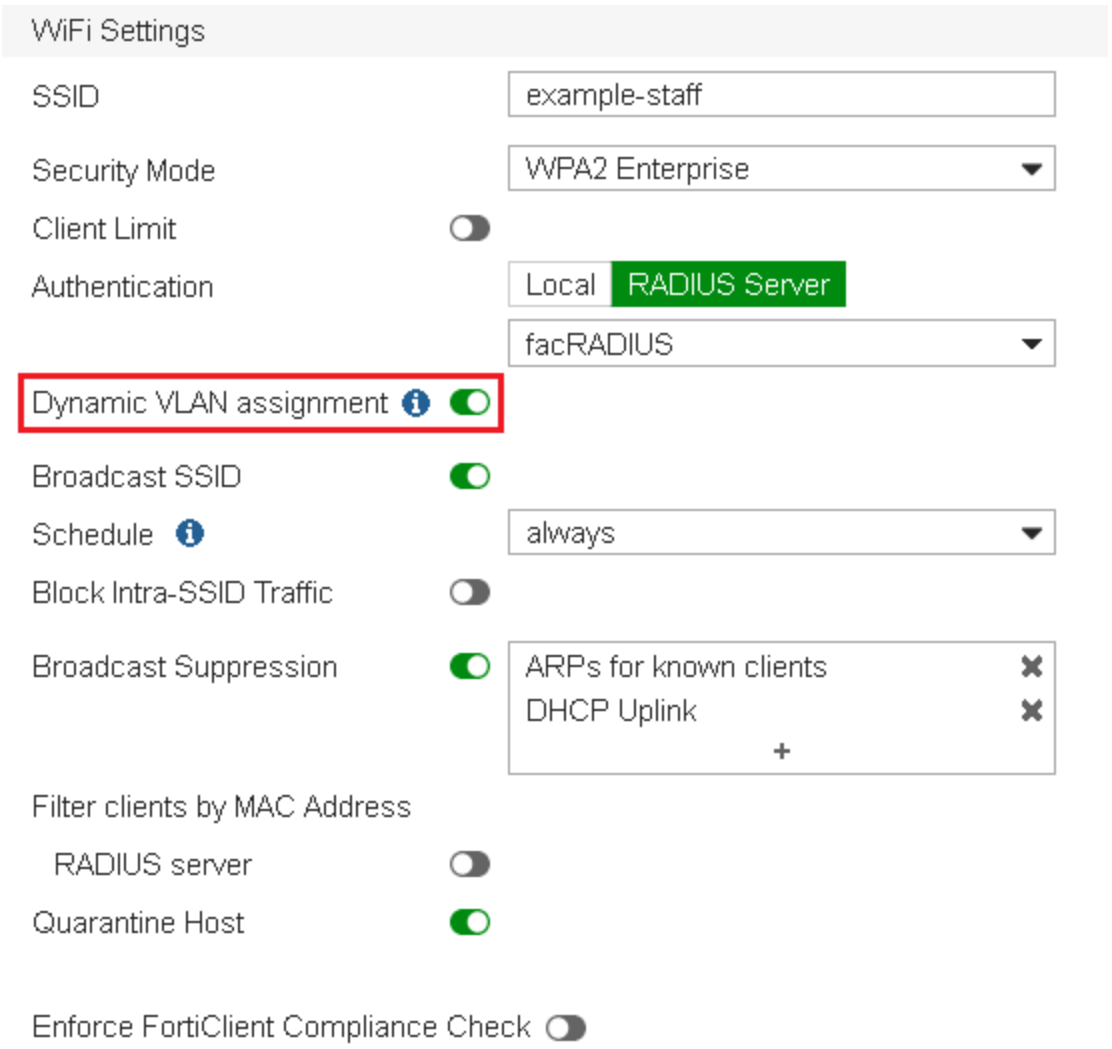


Creating an SSID with dynamic VLAN assignment

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



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

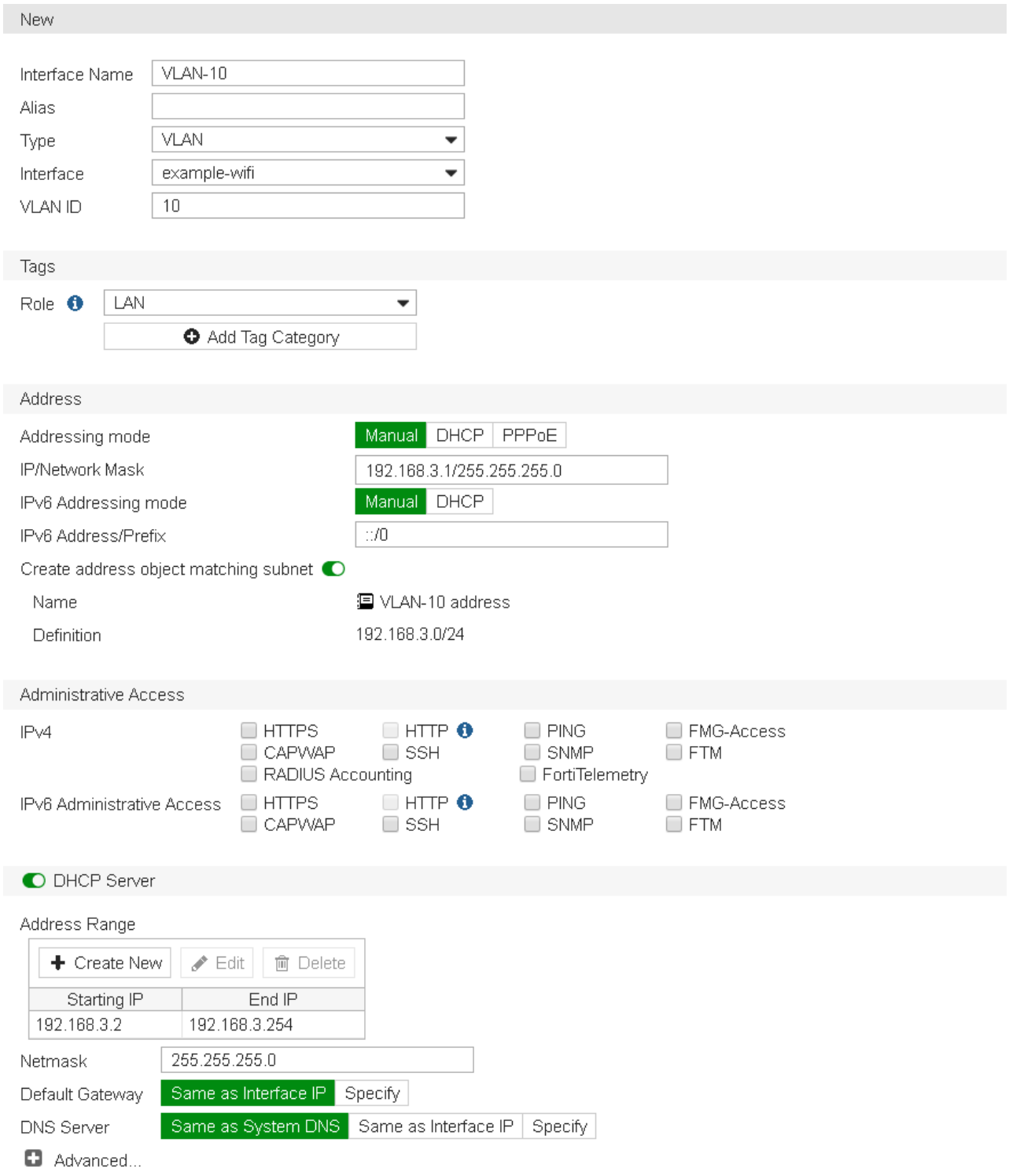


3. Then open the **CLI Console** and enter the following command to assignment and set the VLAN ID to **10**. This VLAN is used when RADIUS does not assign a VLAN:

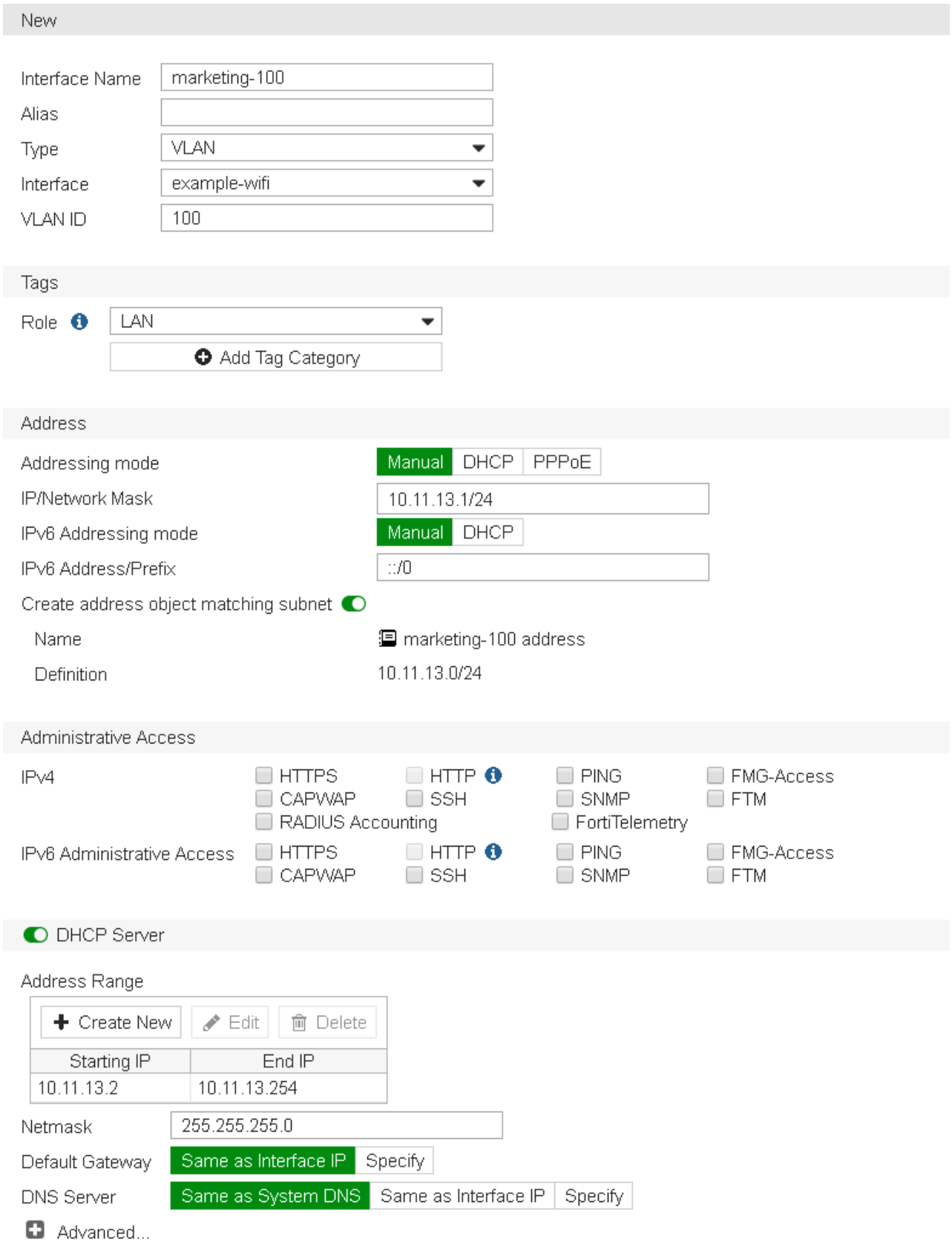
```
config wireless-controller vap
   edit example-wifi
      set vlanid 10
   next
end
```

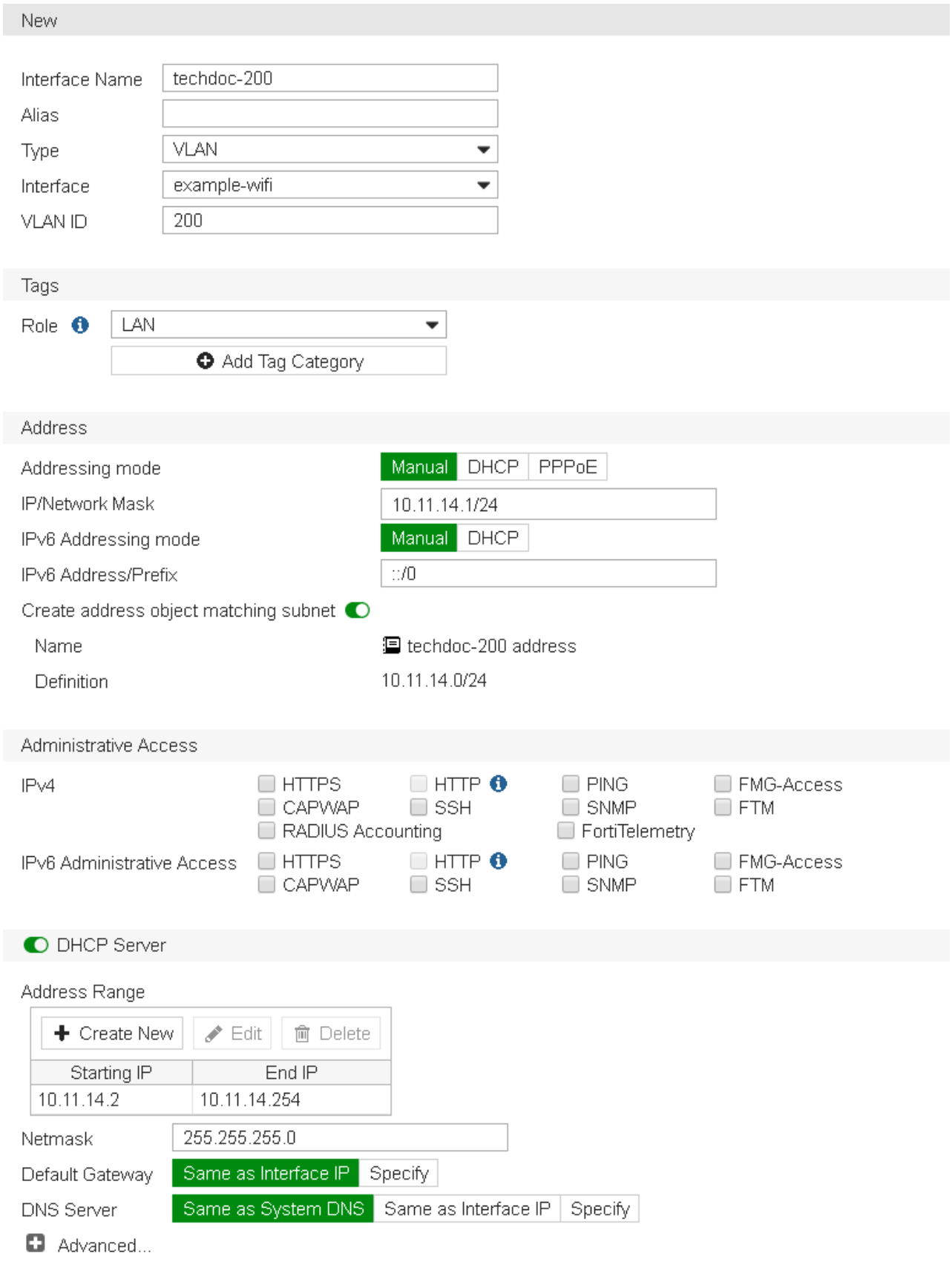
Creating the VLAN interfaces

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



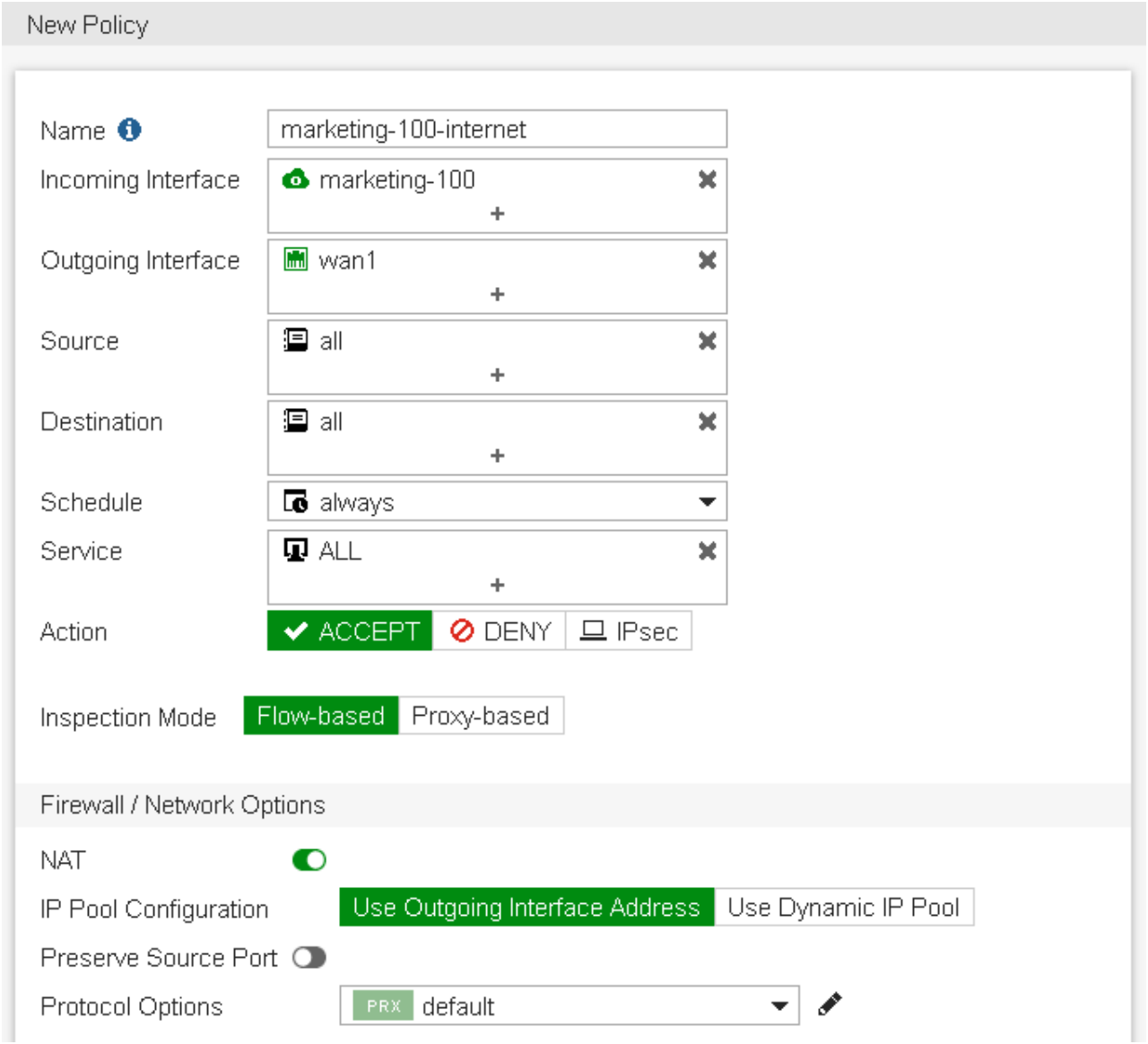
2. Then create two more VLAN interfaces: one for **marketing-100** and another for **techdoc-200**, both with DHCP service.


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


New
Interface Name
techdoc-200
Alias
Type
VLAN
Interface
example-wifi
VLAN ID
200
Tags
Role
LAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
PPPoE
IP/Network Mask
10.11.14.1/24
IPv6 Addressing mode
Manual
DHCP
IPv6 Address/Prefix
::/0
Create address object matching subnet
Name
techdoc-200 address
Definition
10.11.14.0/24
Administrative Access
IPv4
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry
IPv6 Administrative Access
HTTPS
HTTP
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
DHCP Server
Address Range
Create New
Edit
Delete
Starting IP
End IP
10.11.14.2
10.11.14.254
Netmask
255.255.255.0
Default Gateway
Same as Interface IP
Specify
DNS Server
Same as System DNS
Same as Interface IP
Specify
Advanced...

Creating security policies

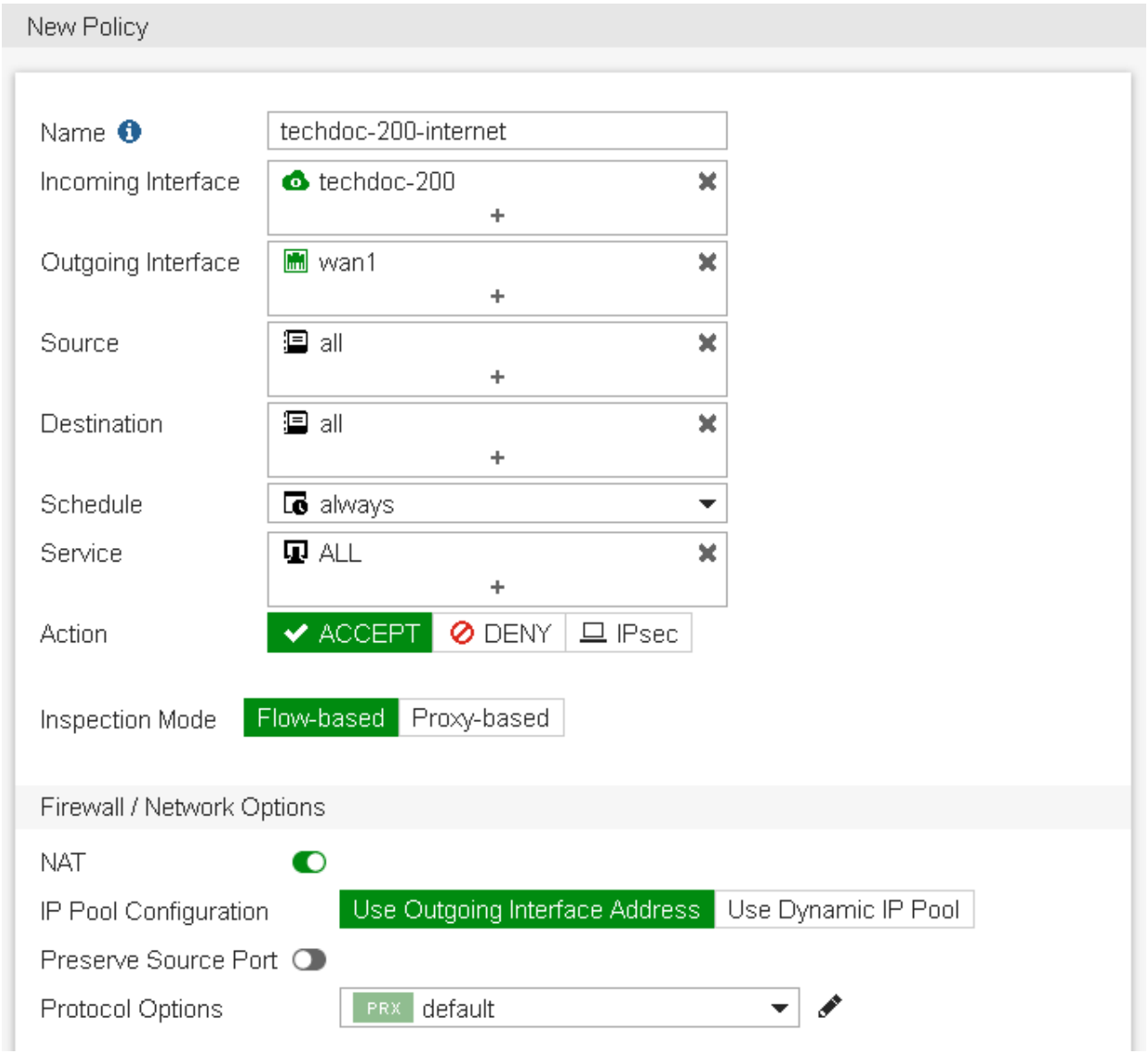
1. Go to **Policy & Objects > IPv4 Policy**.
   Create a policy that allows outbound traffic from **marketing-100** to the Internet.



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

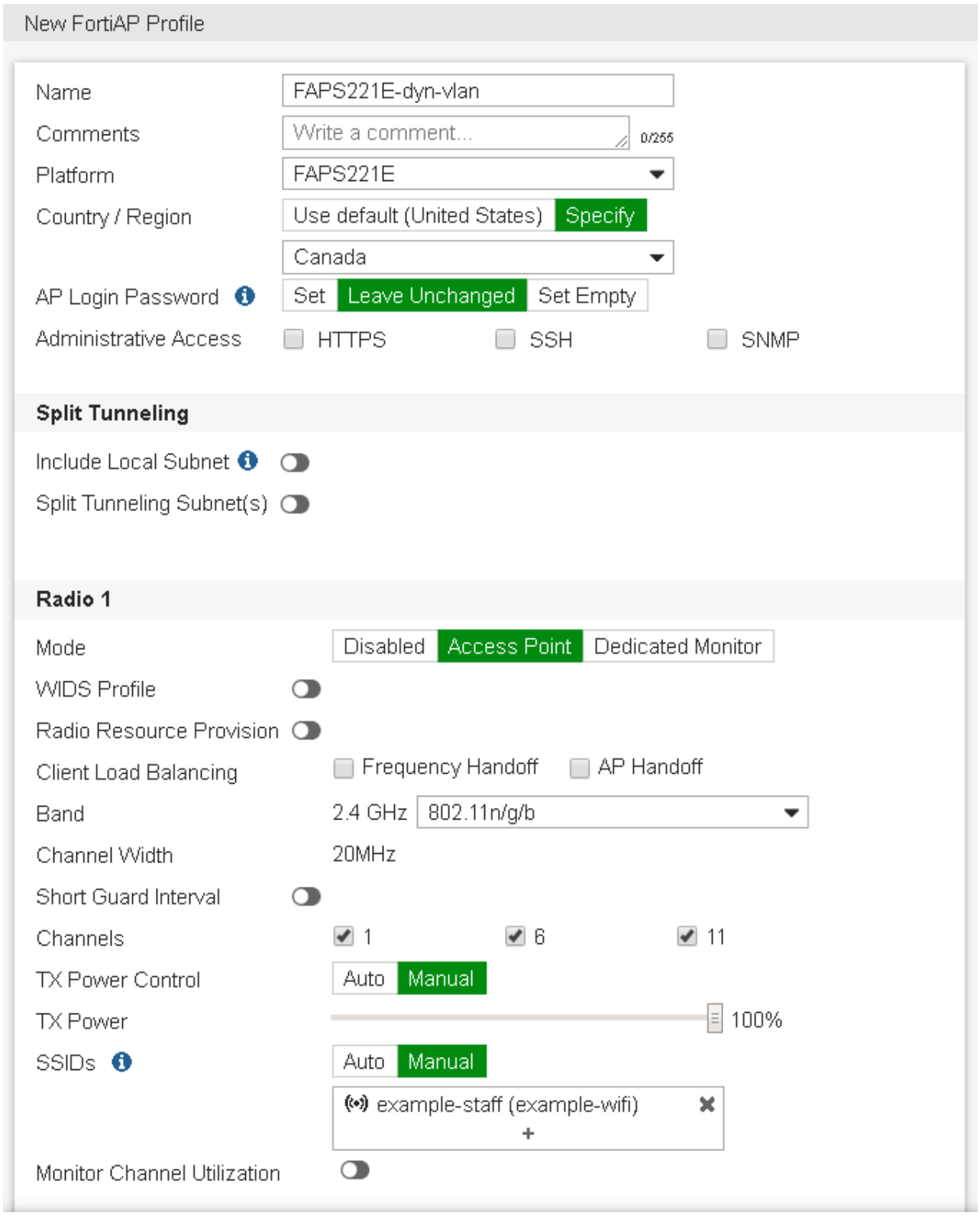
3. Create another policy that allows outbound traffic from **techdoc-200** to the Internet.

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



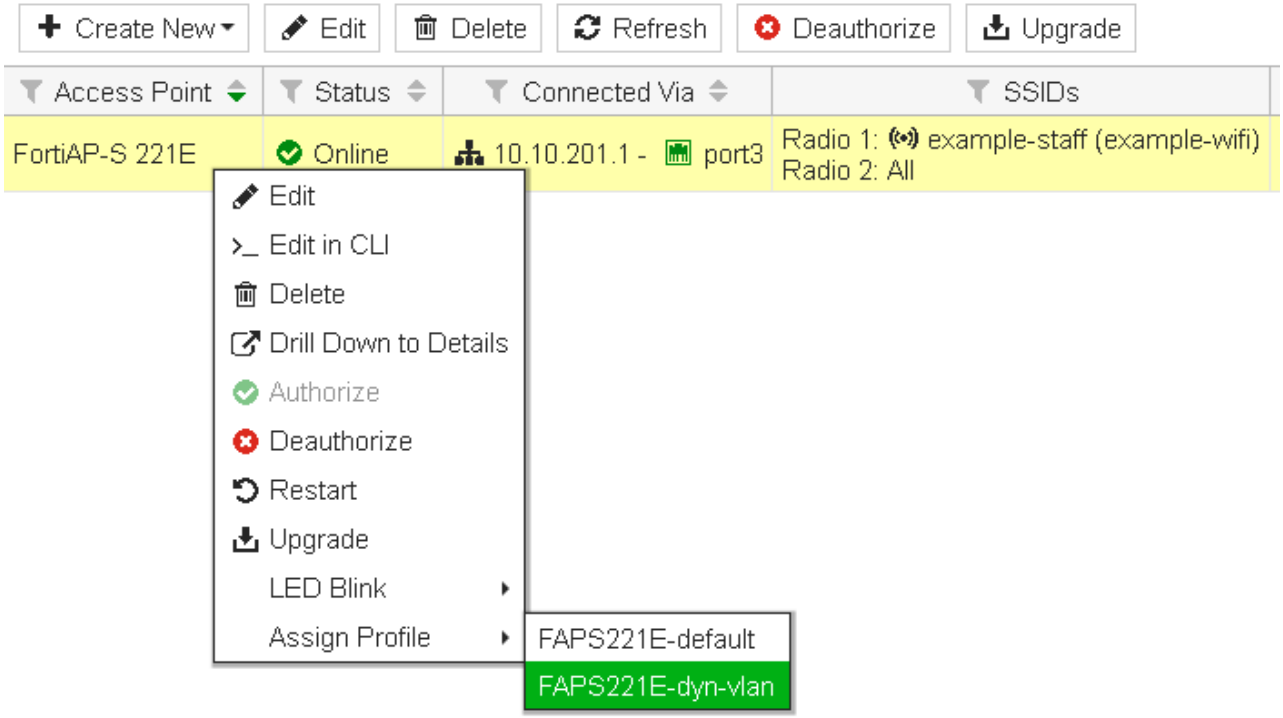
Creating the FortiAP profile

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

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



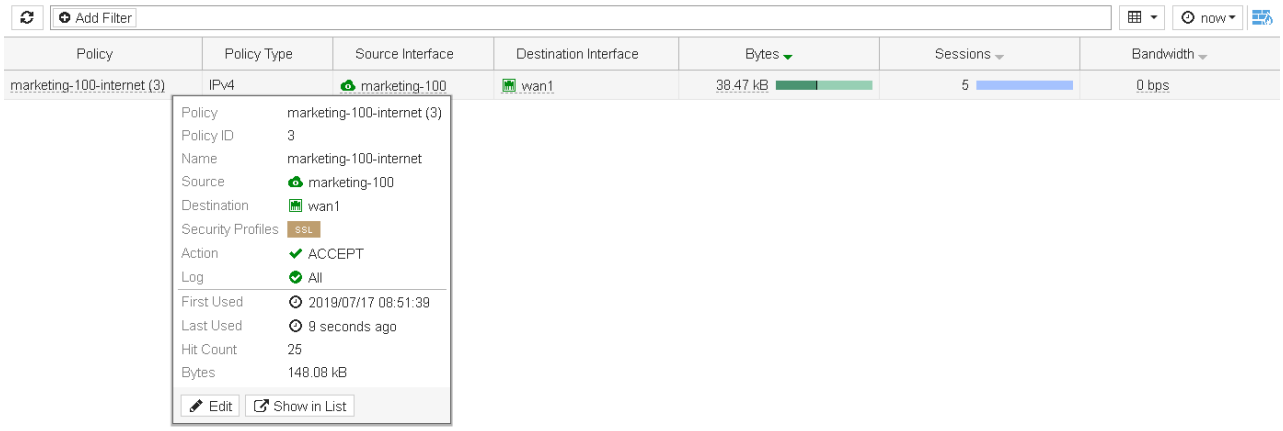
Results

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

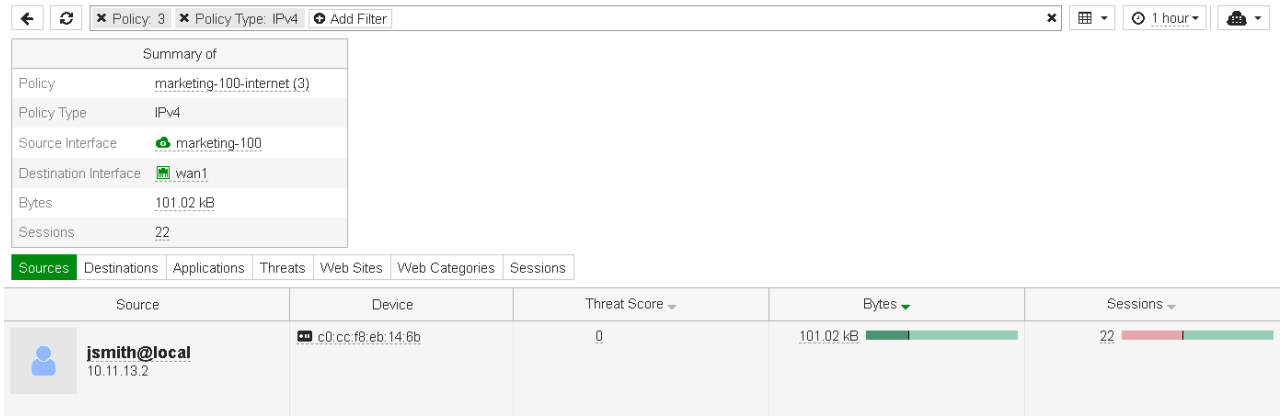
Both **twhite** and **jsmith** can connect to the SSID with their credentials and access the Internet.

If a certificate warning message appears, accept the certificate.

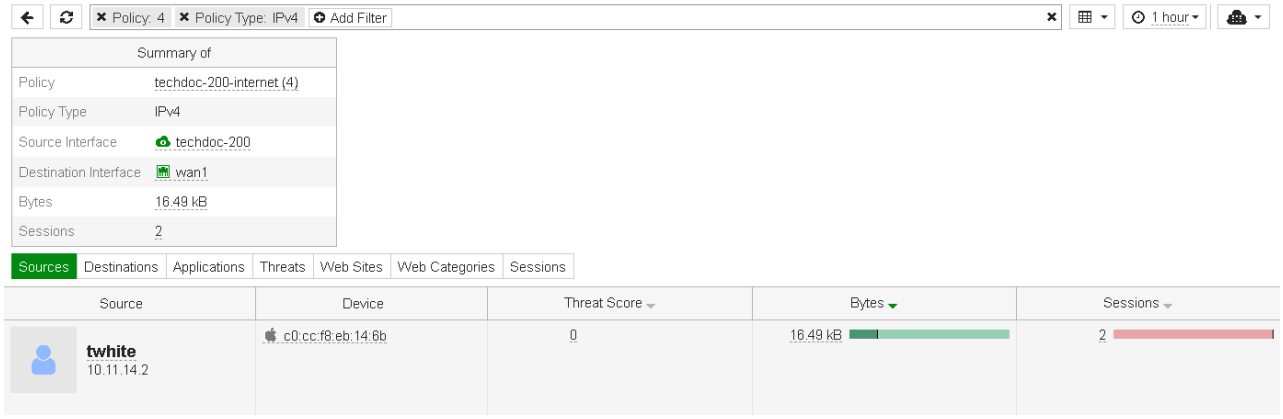
1. Go to **FortiView > Policies**.
   Note that traffic for **jsmith** and **twhite** will pass through different policies. In this example, the **marketing-100-internet** policy is displayed, indicating that **jsmith** has connected to the WiFi.



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



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



WiFi using FortiAuthenticator RADIUS with certificates

This 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:

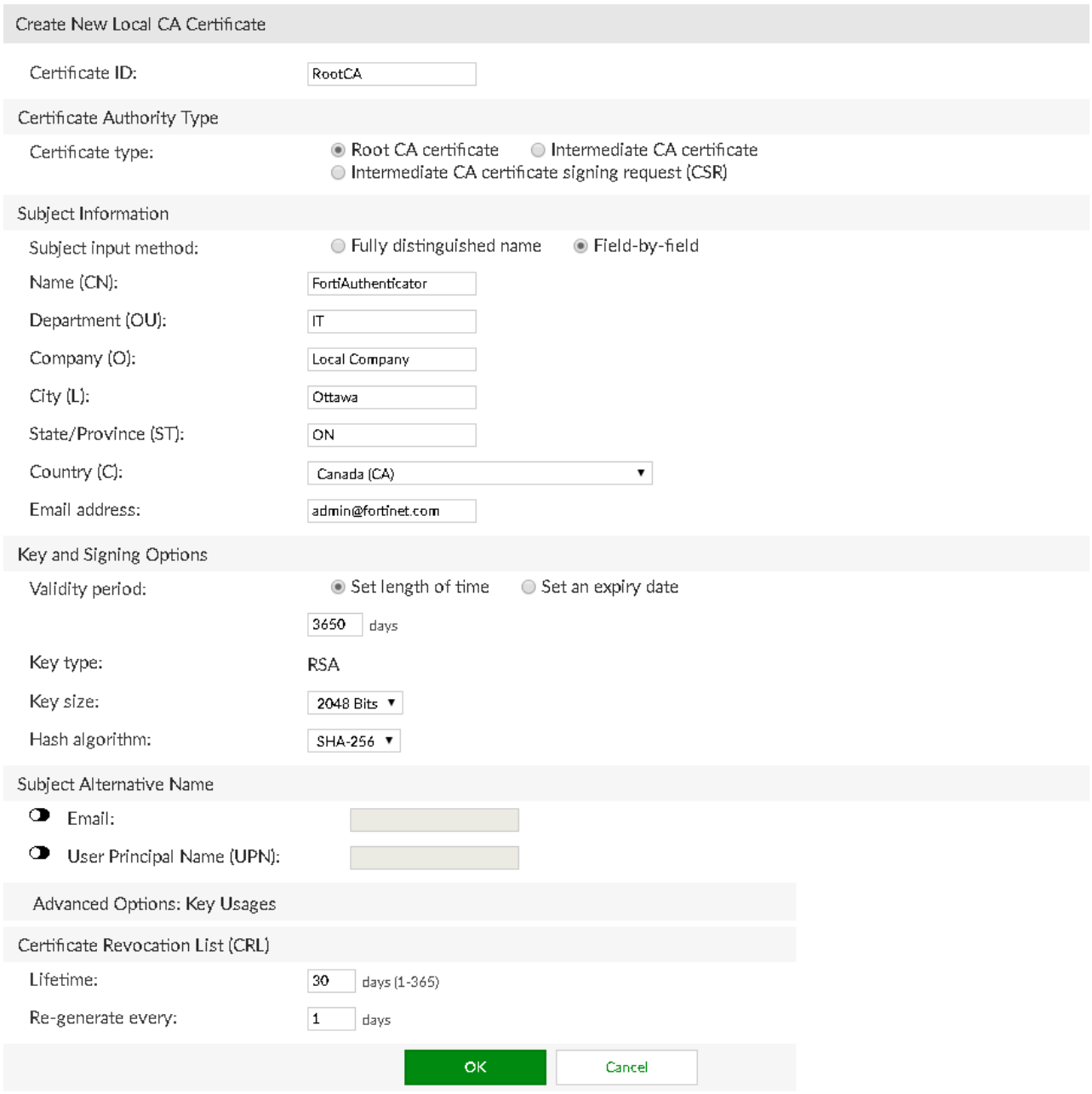
1. A client certificate signed by the certificate authority (CA)
2. A copy of the CA root certificate.

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.

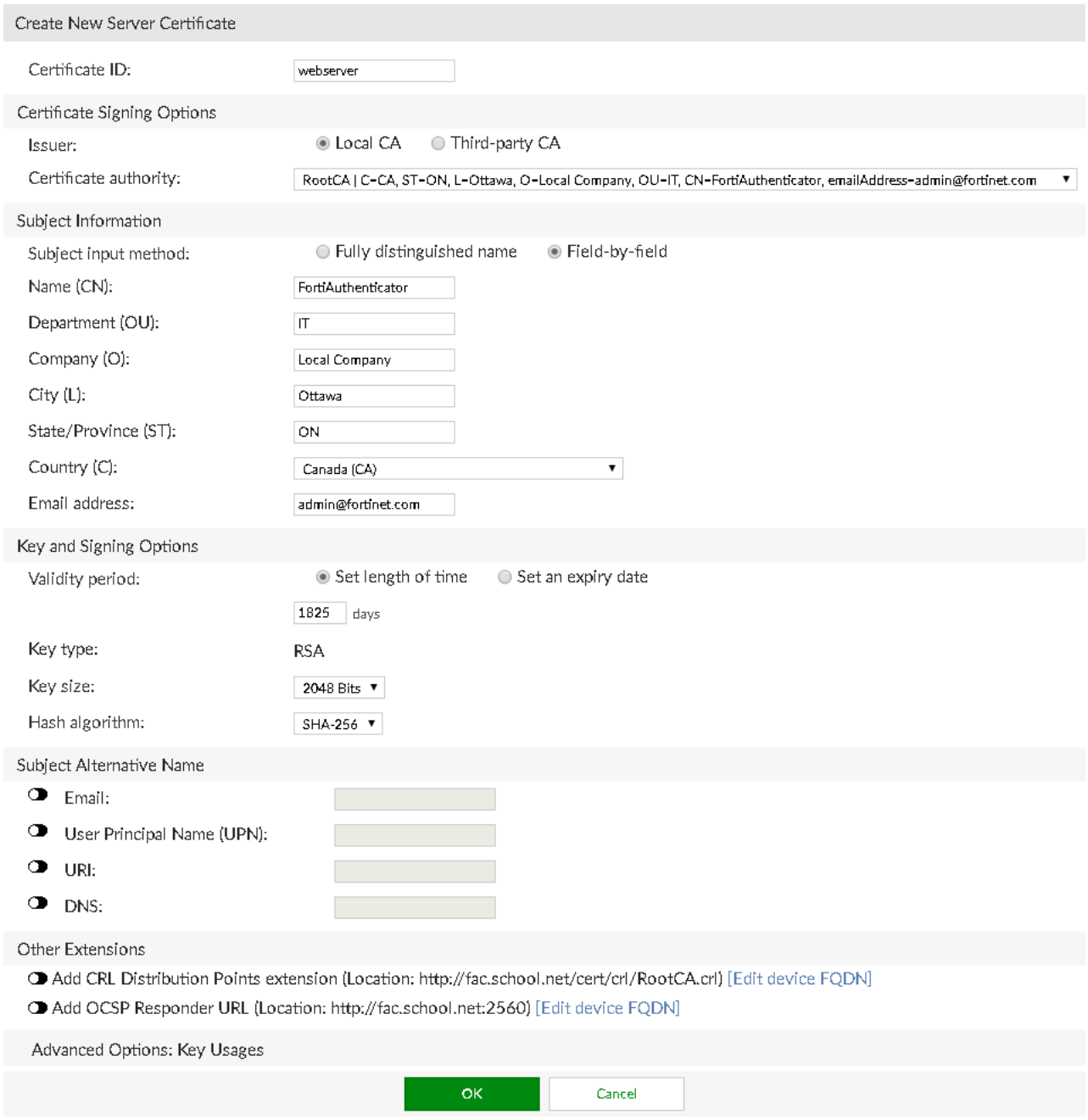
1. On the FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and select **Create New**. Configure the fields as required.



Creating a local service certificate on FortiAuthenticator

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

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

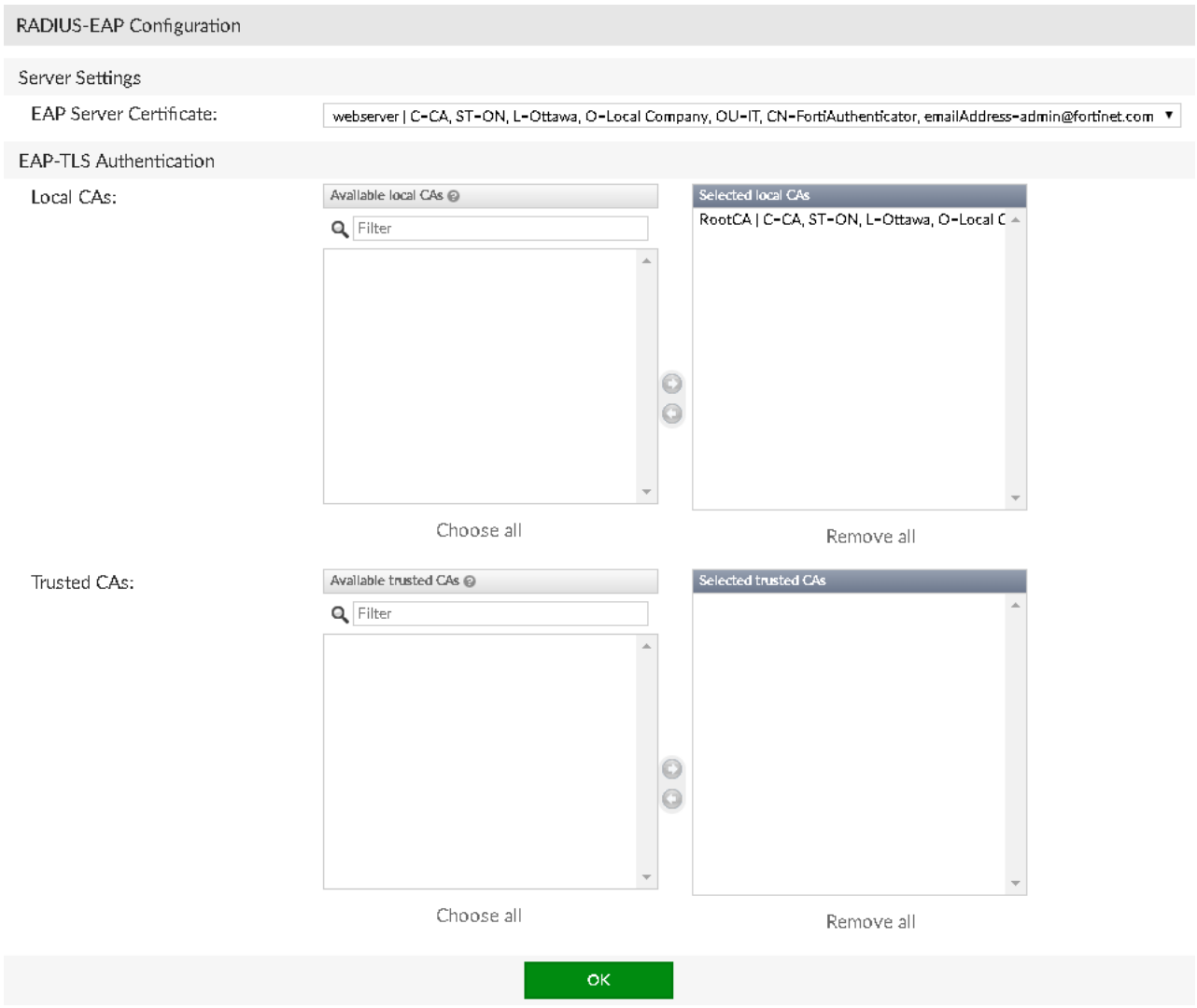


Configuring RADIUS EAP on FortiAuthenticator

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

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

Local CAs section.

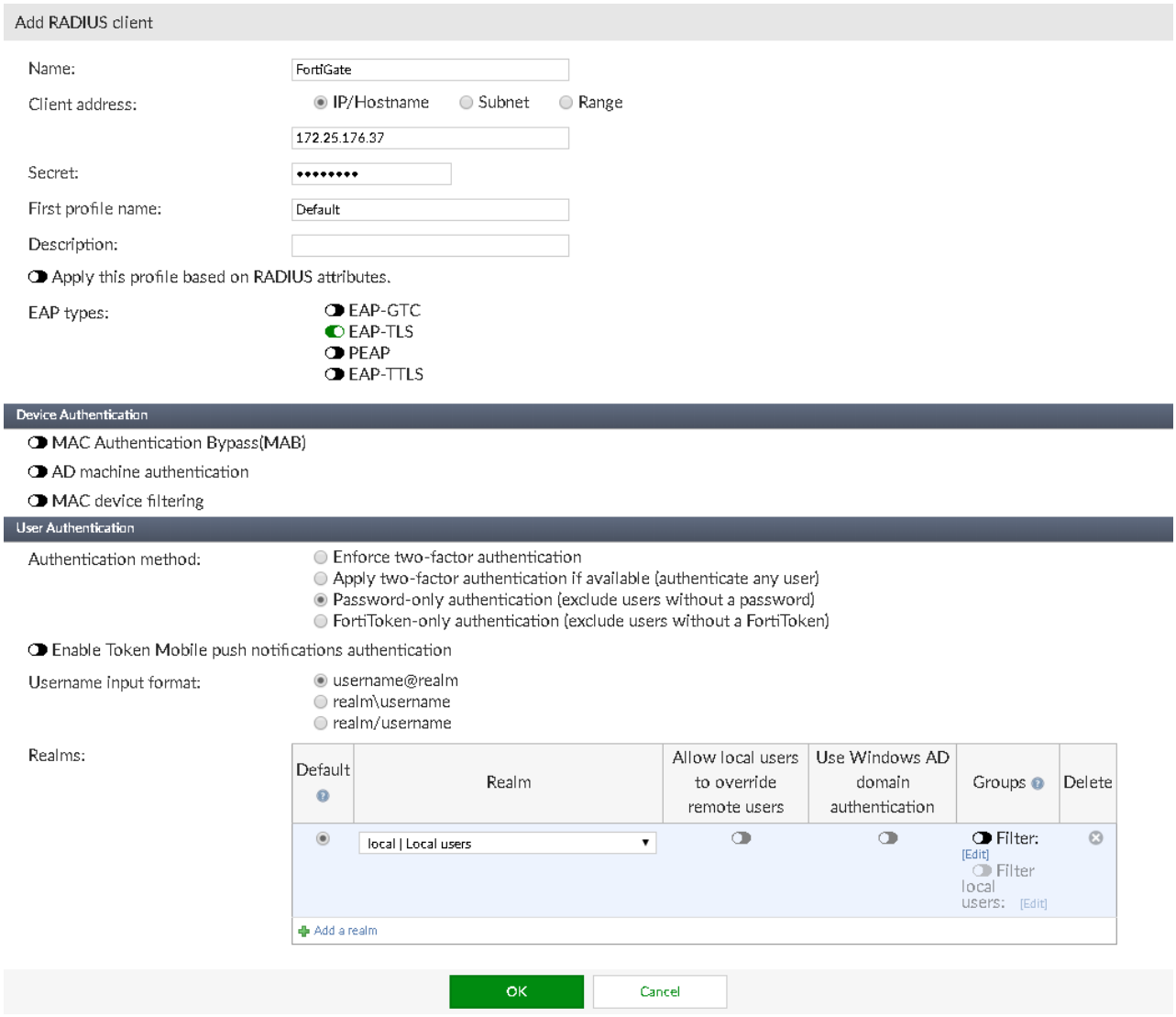


Configuring RADIUS client on FortiAuthenticator

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

1. Go to **Authentication > RADIUS Service > Clients** and select **Create New**.
   Enter a **Name**, enter the FortiGate's IP address, and enter a **Secret**. Set the **Authentication method** to **Password-only authentication** and set **Username input format** to **username@realm**.
   EAP-TLS should be the only EAP type selected to prevent fallback to a less secure version of authentication if a

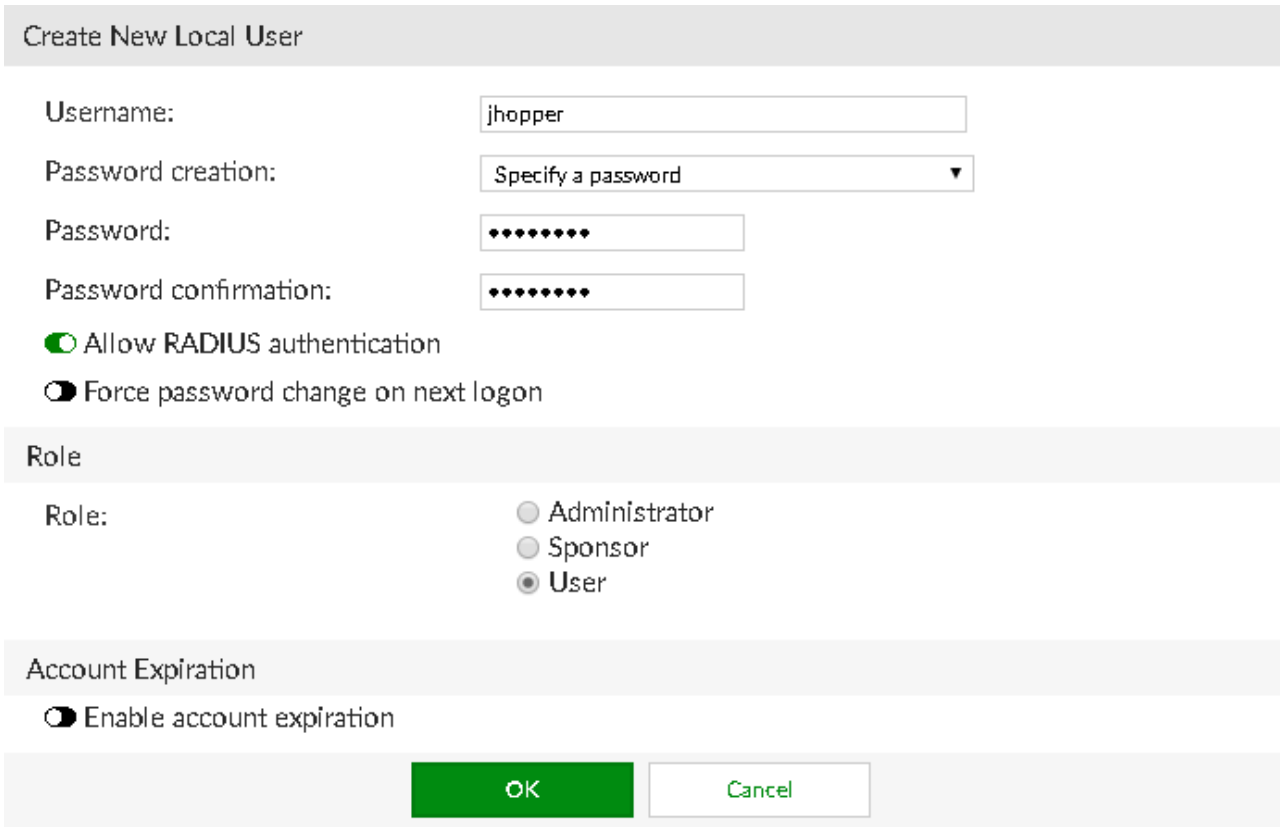
certificate is not presented by the WiFi client.



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.

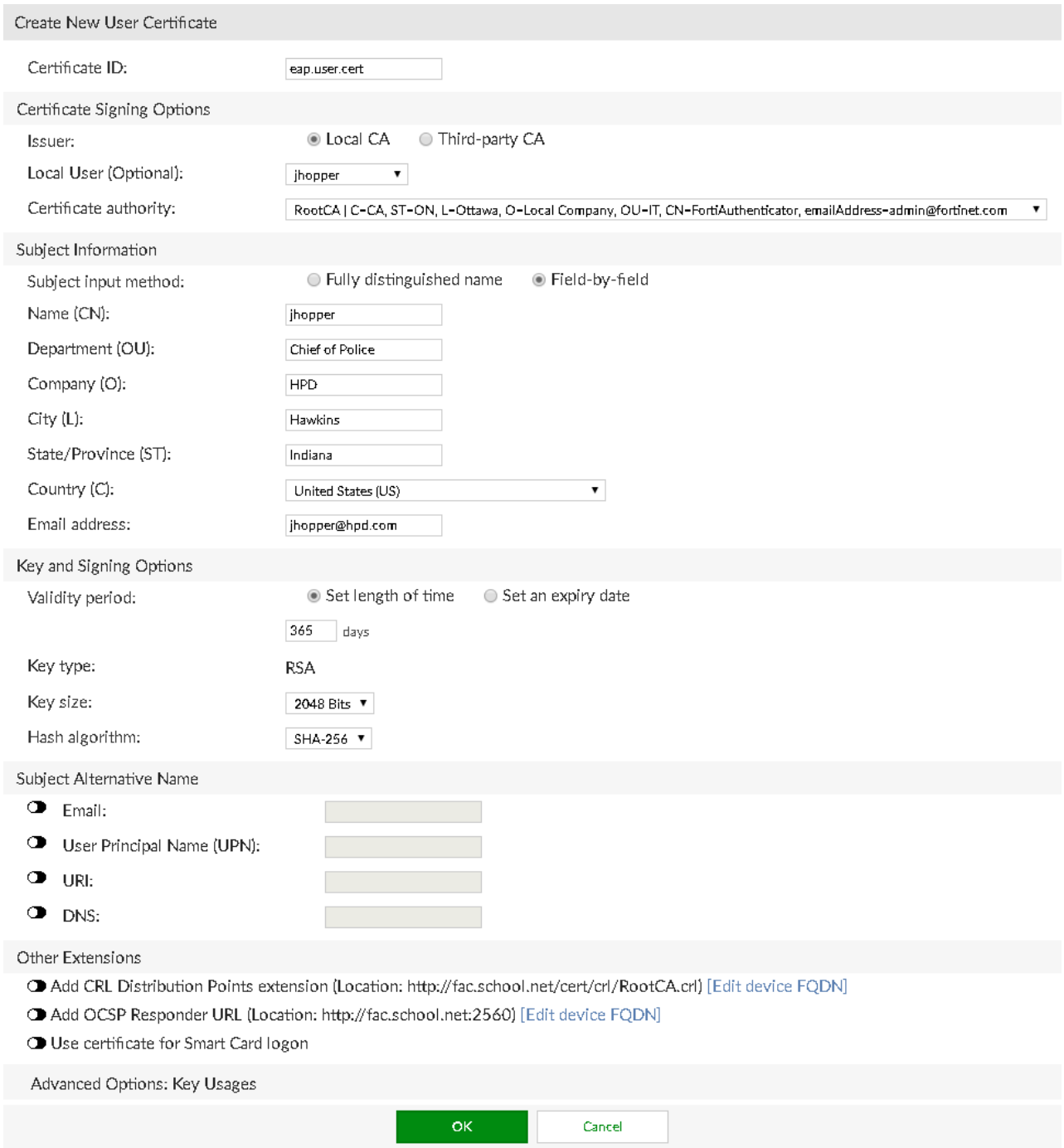
1. Go to **Authentication > User Management > Local Users** and select **Create New**. Fill out applicable user information.



Configuring local user certificate on FortiAuthenticator

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

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

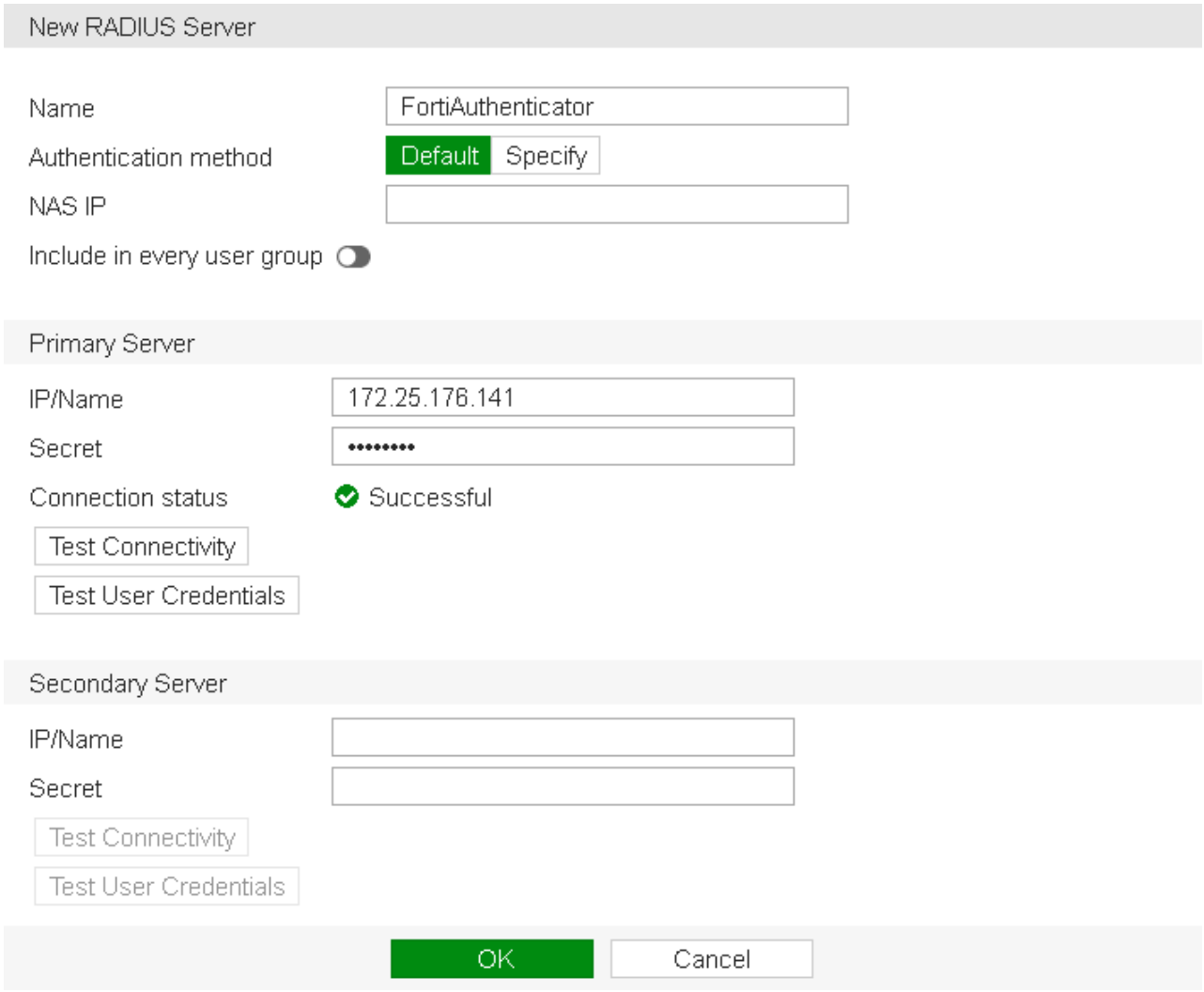


Creating RADIUS server on FortiGate

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

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

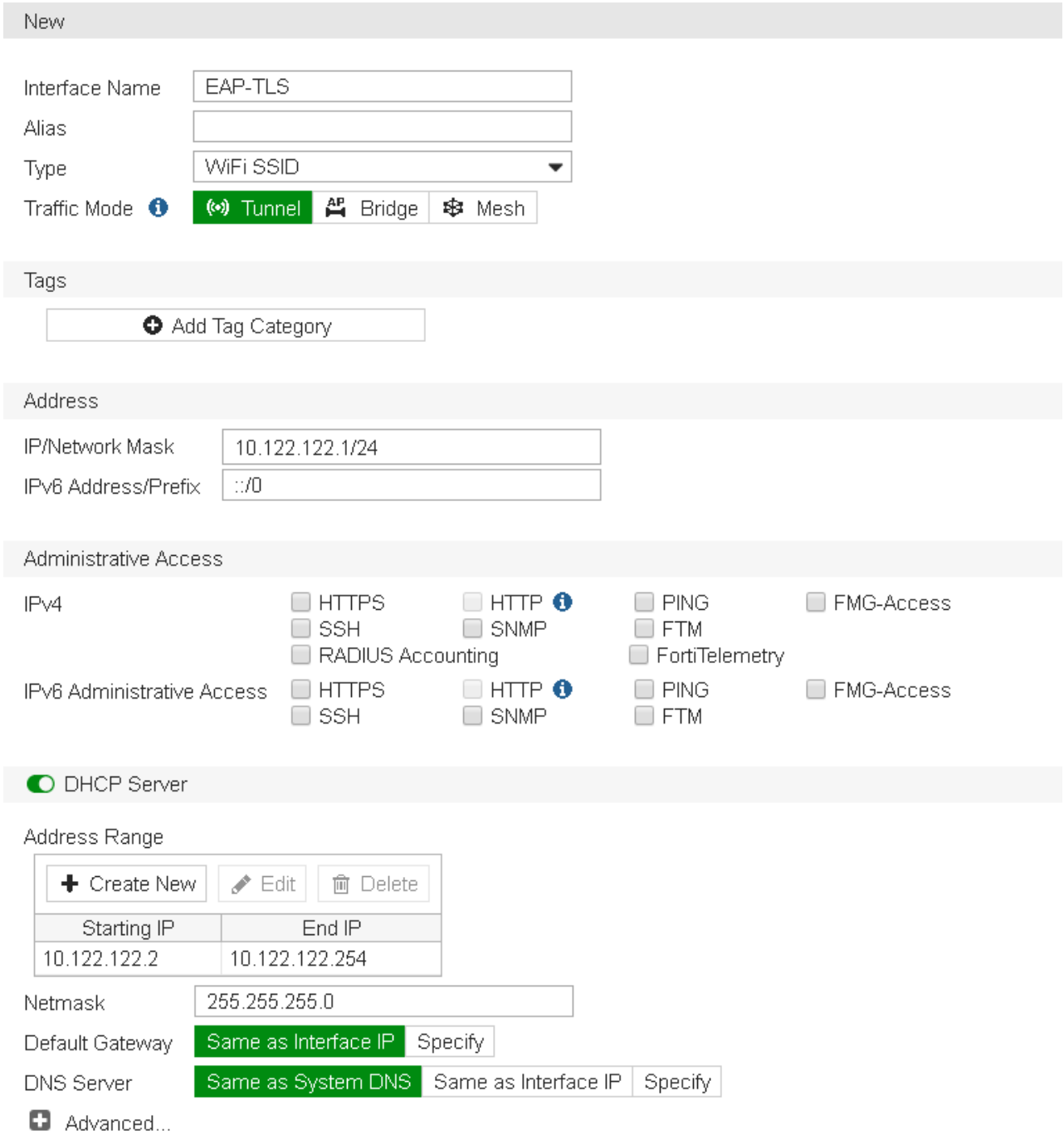
Select **Test Connectivity** to confirm the successful connection.



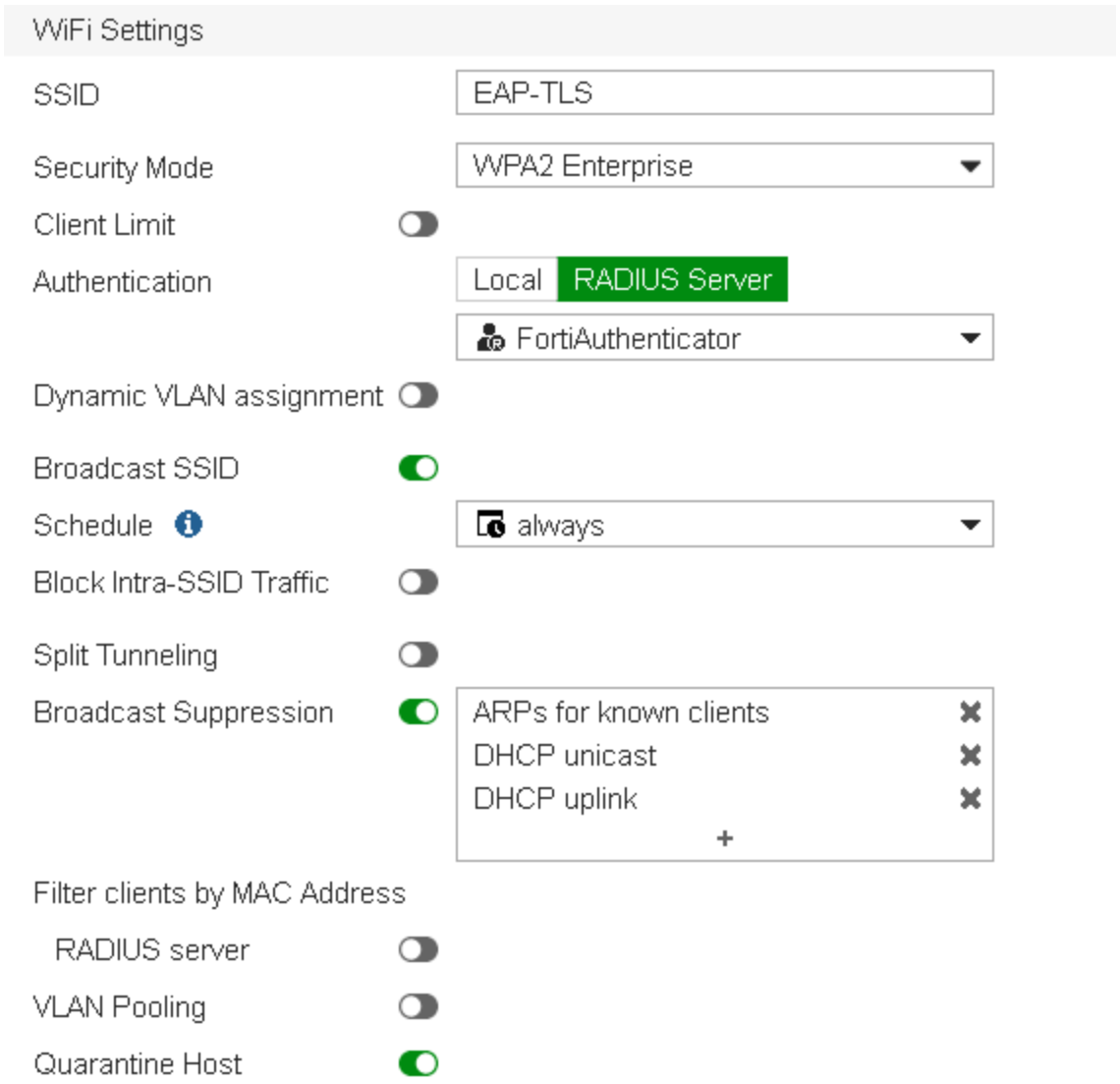
Creating WiFi SSID on FortiGate

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

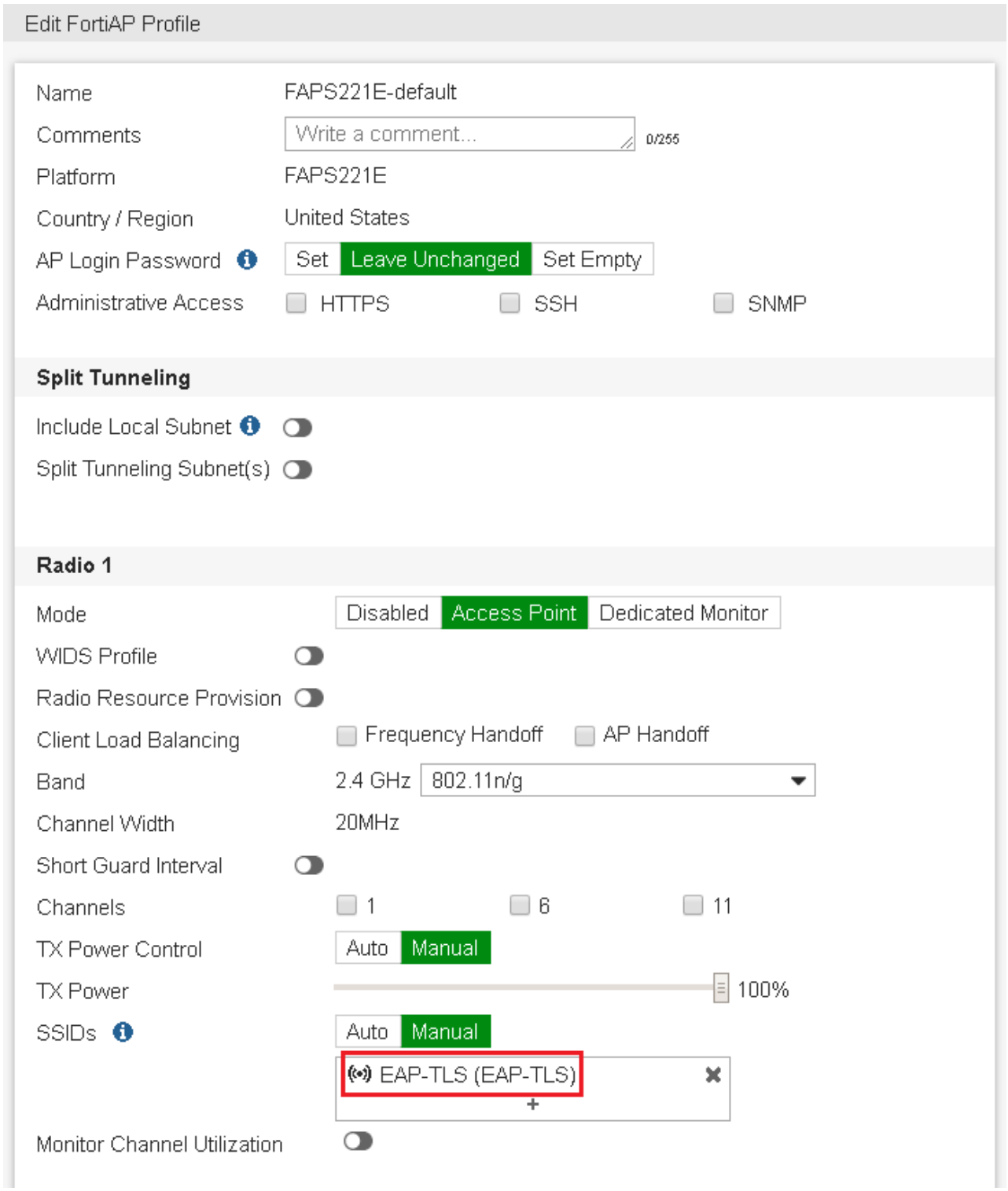
1. Go to **WiFi & Switch Controller > SSID** and create an SSID with DHCP for clients.



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



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

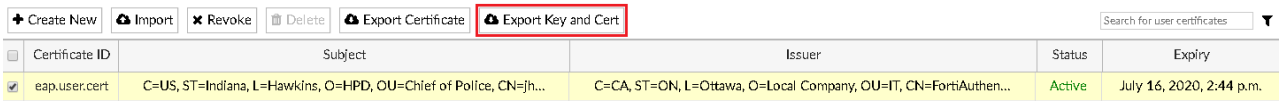


4. Then go to **Policy & Objects > IPv4 Policy** and create a policy that allows outbound traffic from the **EAP-TLS** wireless interface to the Internet.

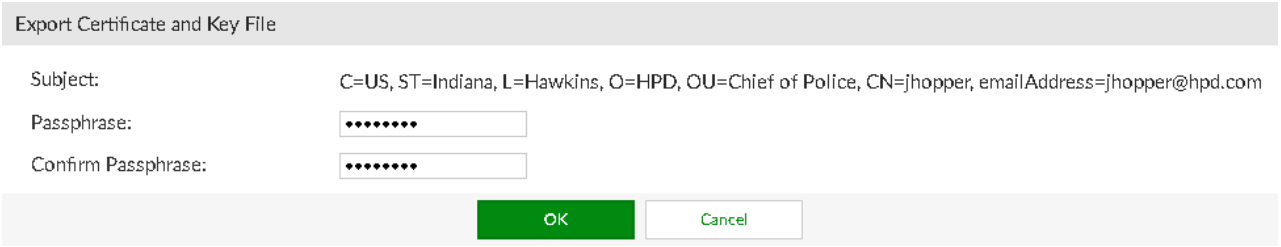
Exporting user certificate from FortiAuthenticator

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

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



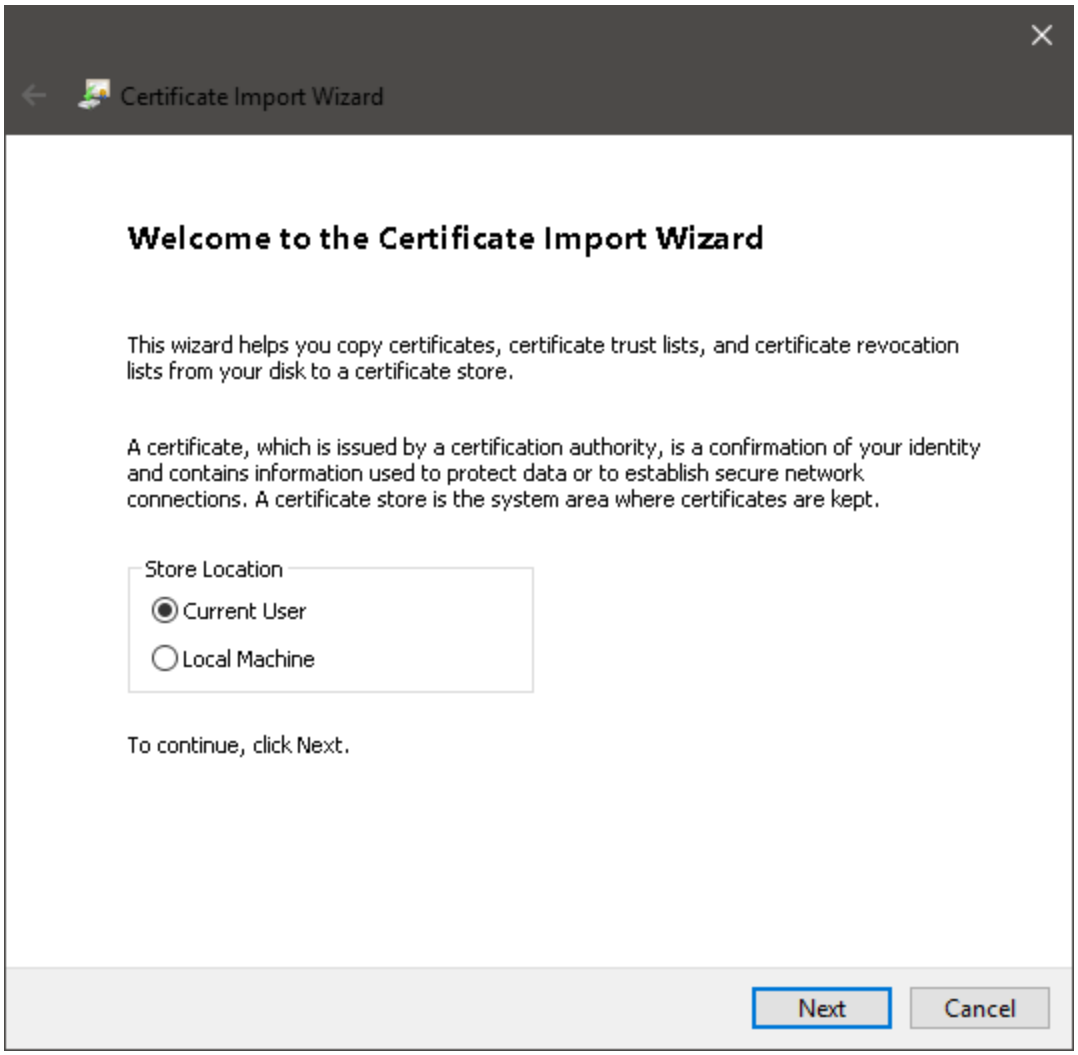
2. In the **Export User Certificate and Key File** dialog, enter and confirm a **Passphrase**. This password will be used when importing the certificate into a Windows 10 computer. Select **OK**.



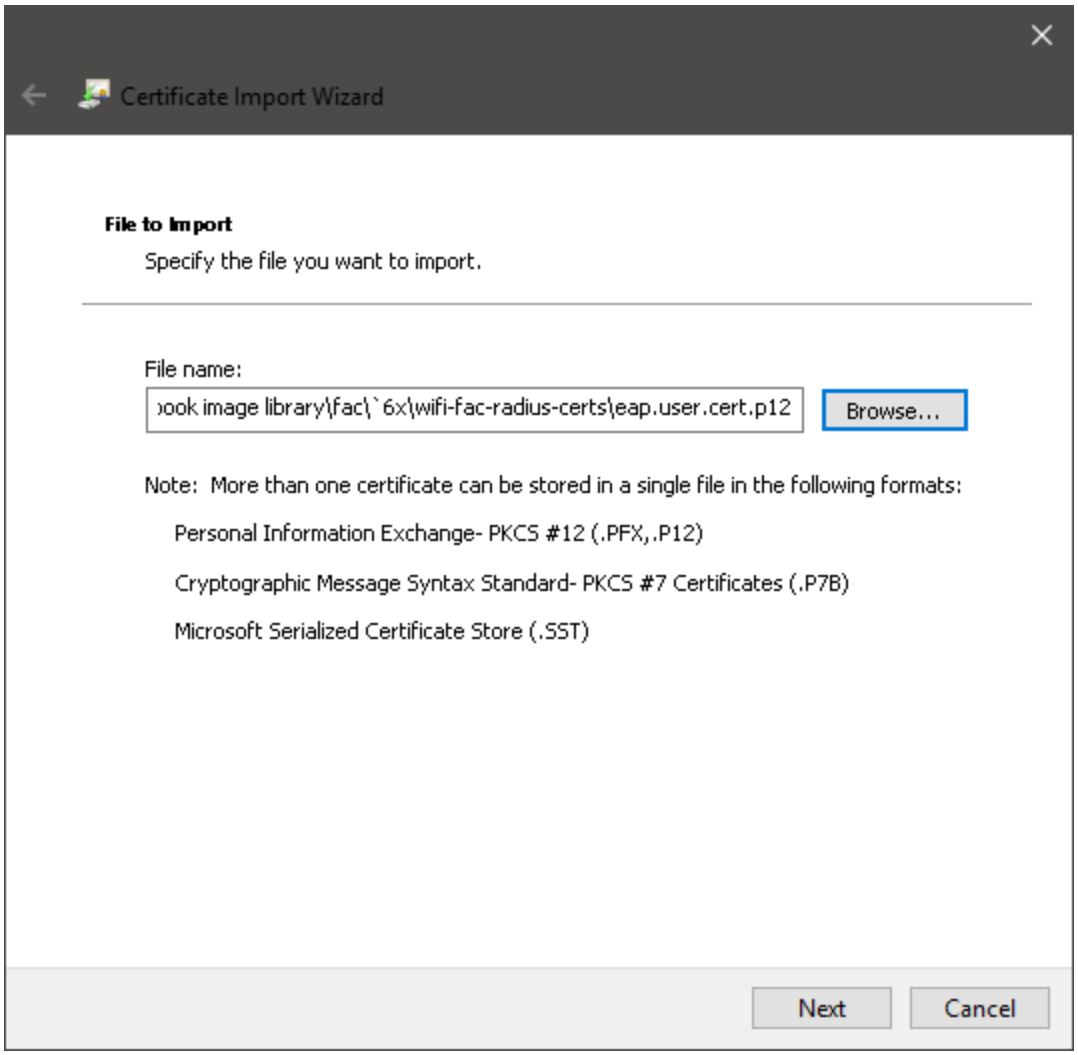
3. Select **Download PKCS#12 file** to pull this certificate to the Widows 10 computer. Select **Finish**.

Importing user certificate into Windows 10

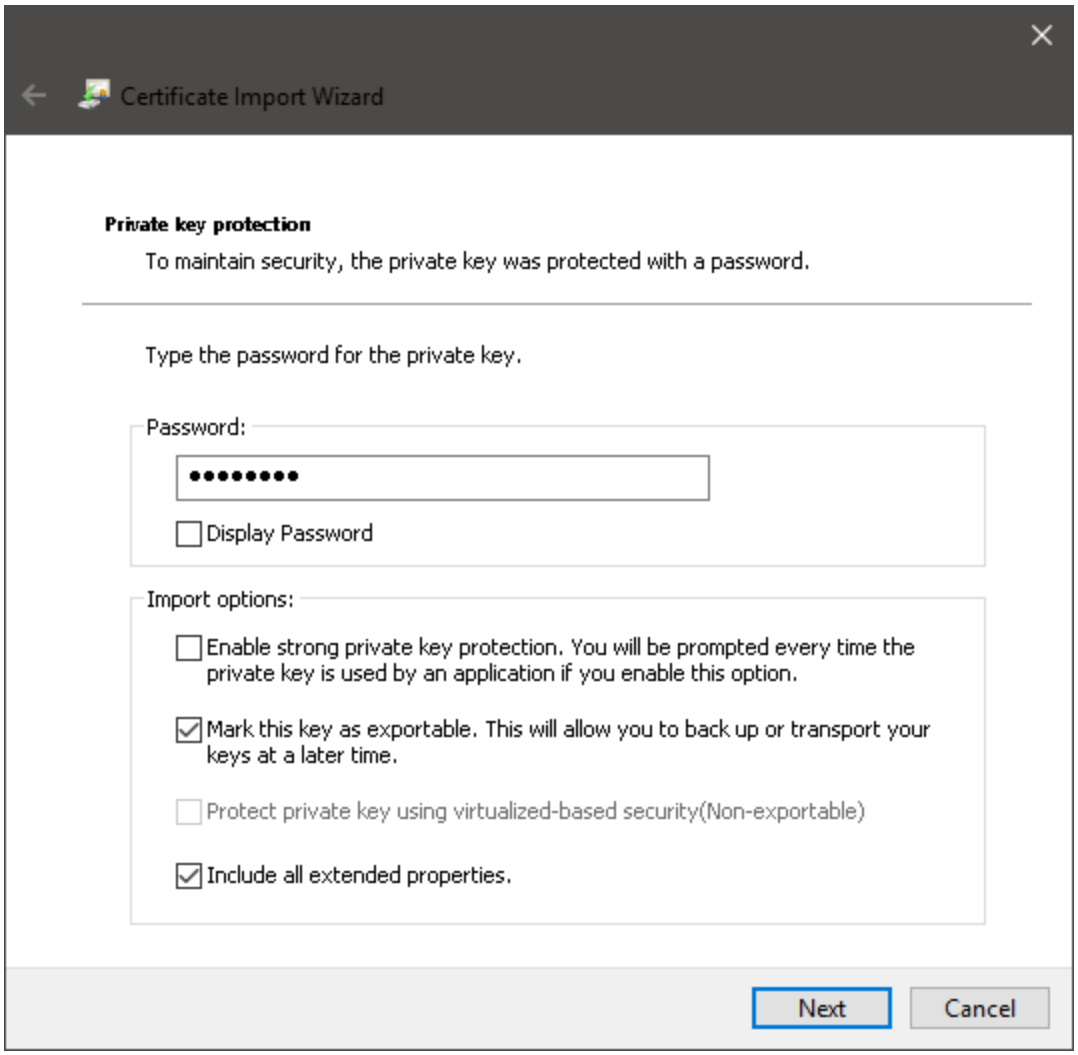
1. On the Windows 10 computer, double-click the downloaded certificate file from the FortiAuthenticator. This will launch the **Certificate Import Wizard**. Select **Next**.



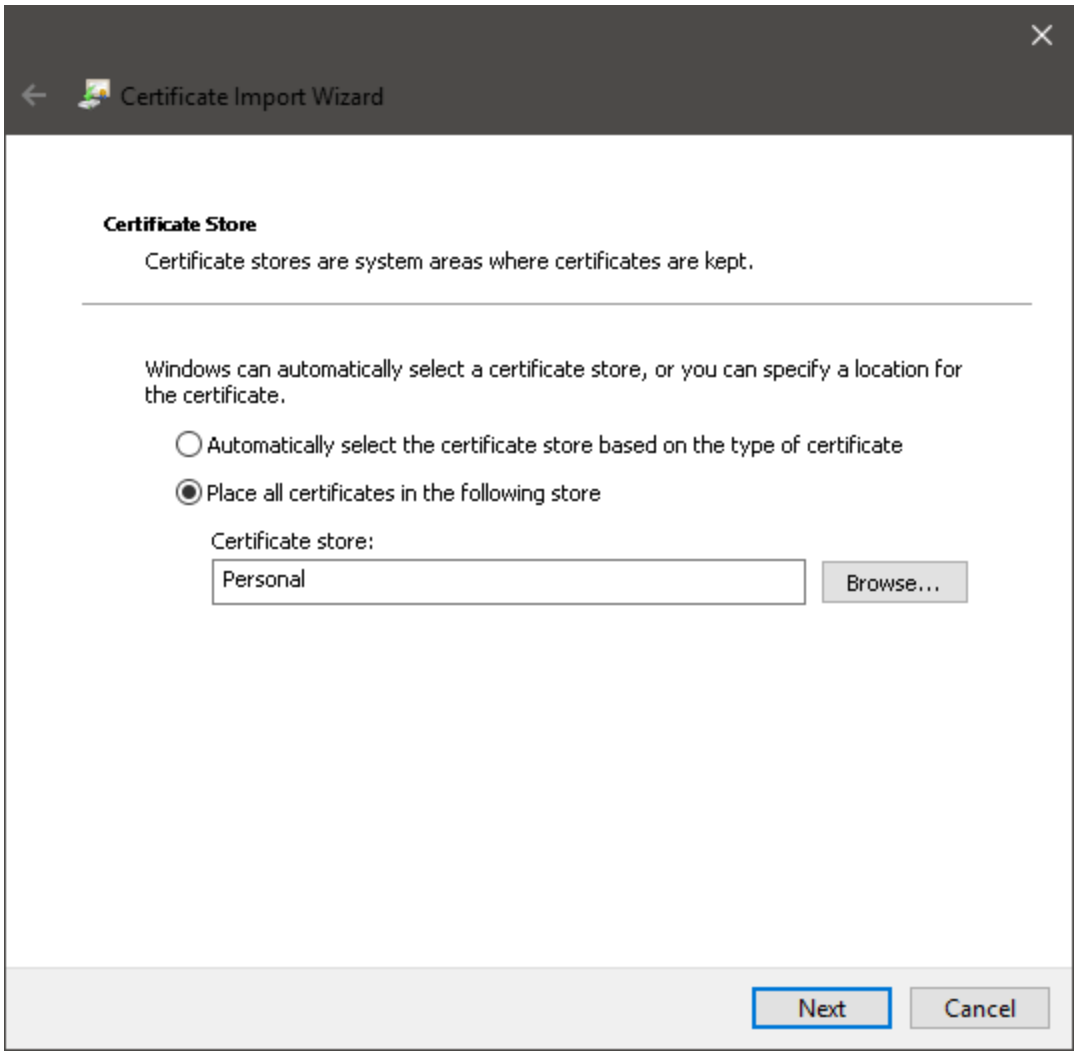
2. Make sure the correct certificate is shown in the **File name** section in the **File to Import** window. Select **Next**.



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**.



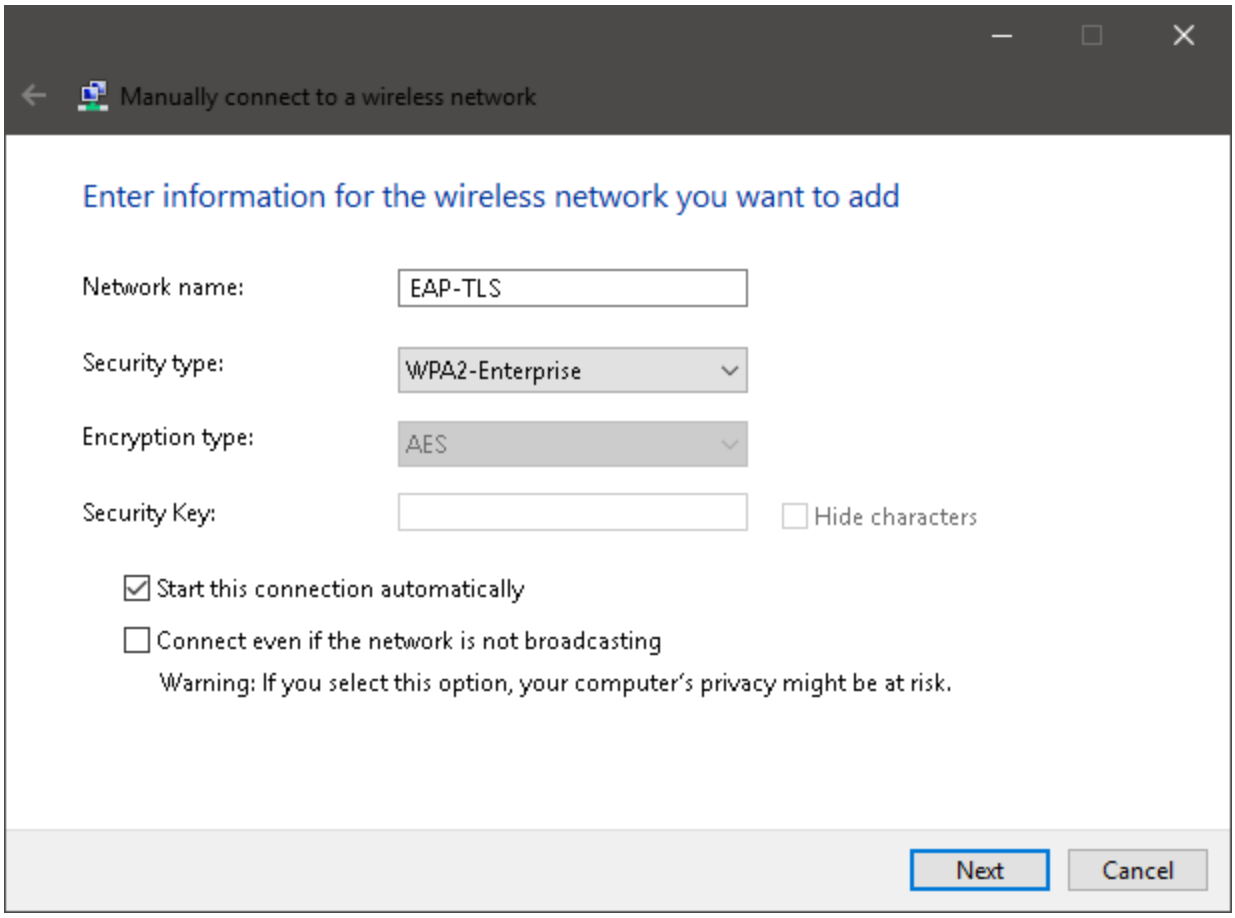
4. In the **Certificate Store**, choose the **Place all certificates in the following store**. Select **Browse** and choose **Personal**. Select **Next**, and then **Finish**. A dialog box will show up confirming the certificate was imported successfully.



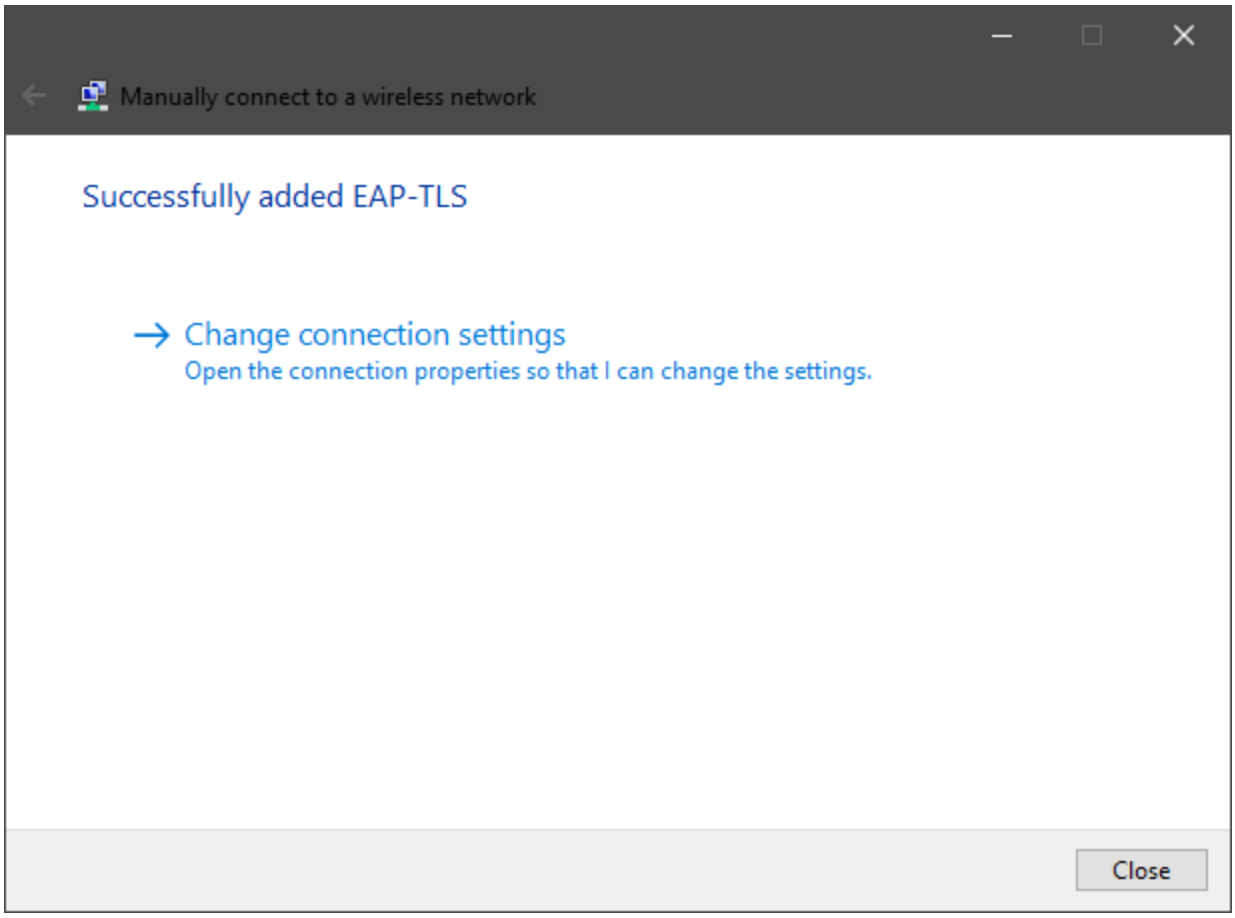
Configuring Windows 10 wireless profile to use certificate

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

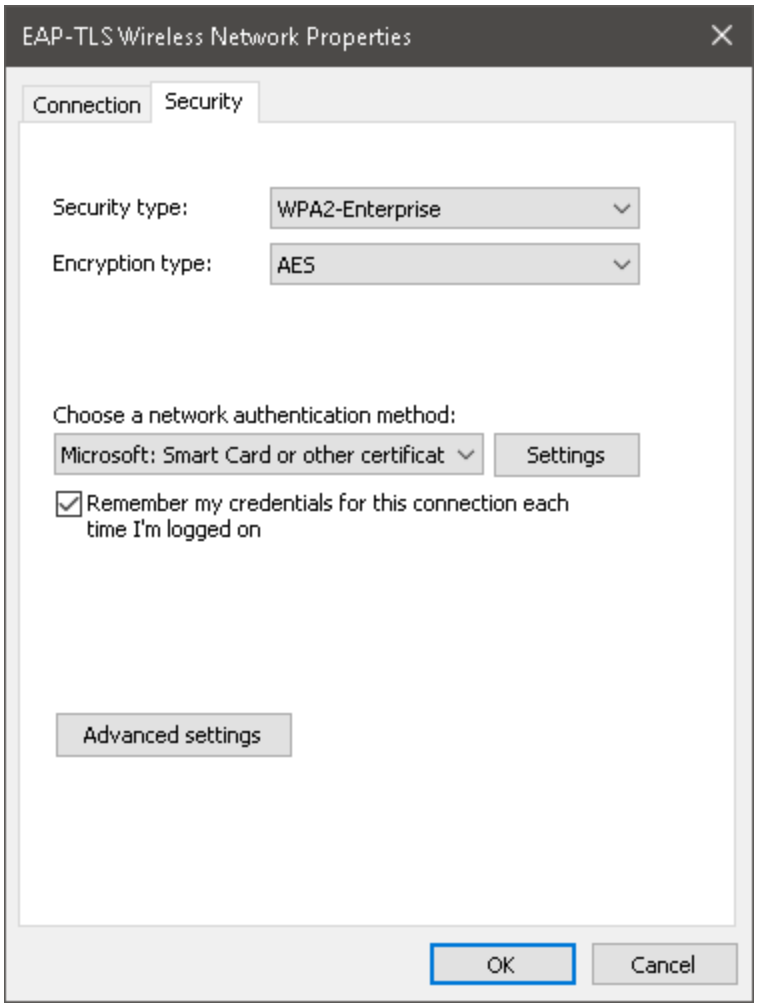
1. On Windows 10, got to **Control Panel > Network and Sharing Center > Set up a new connection or network > Manually connect to a wireless network**. Enter a **Network name** and set **Security type** to **WPA2-Enterprise**. The **Encryption type** is set to **AES**.



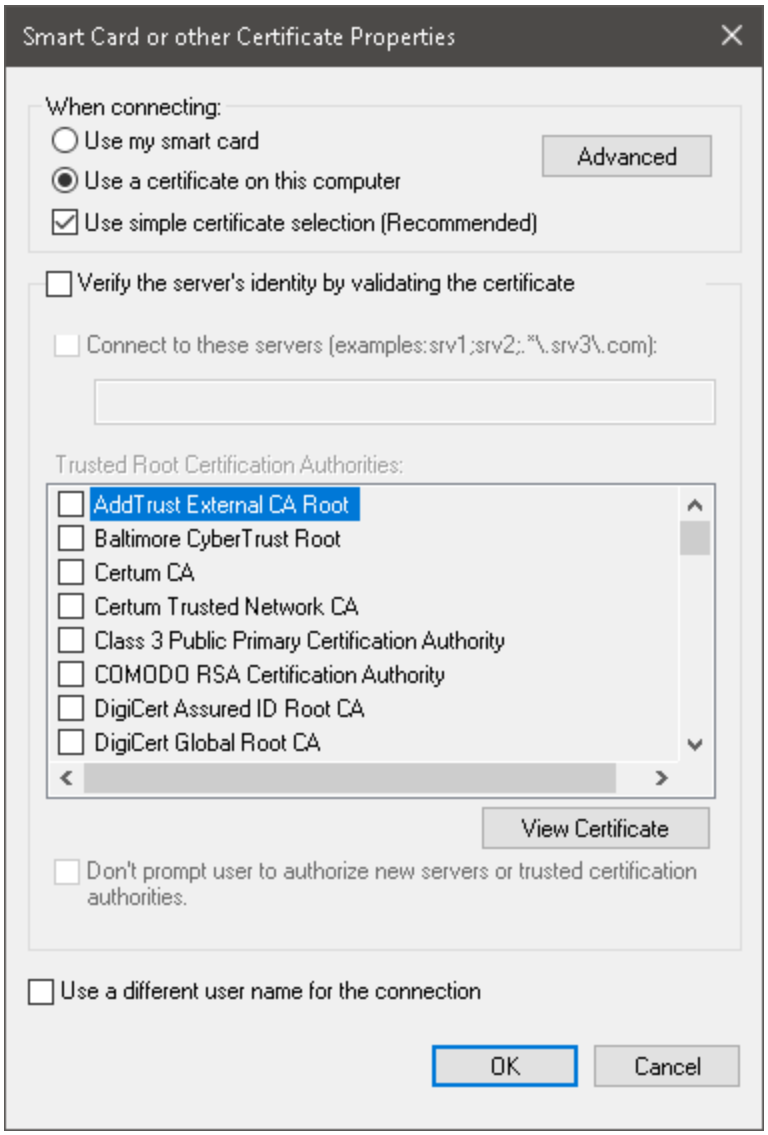
2. Once created, you have the option to modify the wireless connection. Select **Change connection settings**.



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

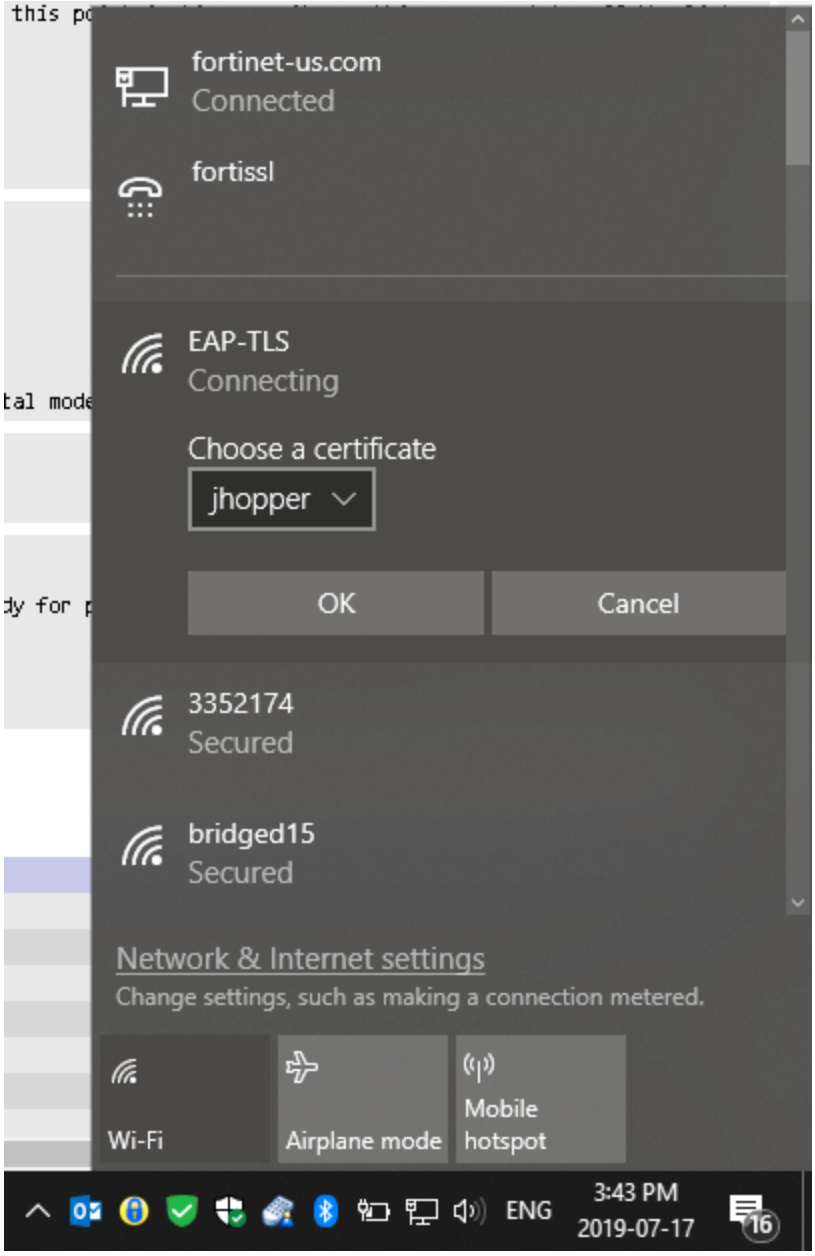


4. Enable both **Use a certificate on this computer** and **Use simple certificate selection**.
   Note that, for simplification purposes, **Verify the server's identity by validating the certificate** has been disabled. However EAP- TLS allows the client to validate the server as well as the server validate the client. To enable this, you will need to import the CA from the FortiAuthenticator to the Windows 10 computer and make sure that it is enabled as a Trusted Root Certification Authority.
   Select **OK** for all dialog windows to confirm all settings. The configuration for the Windows 10 computer has been completed and the user should be able to authenticate to WiFi via the certificate without using their username and password.

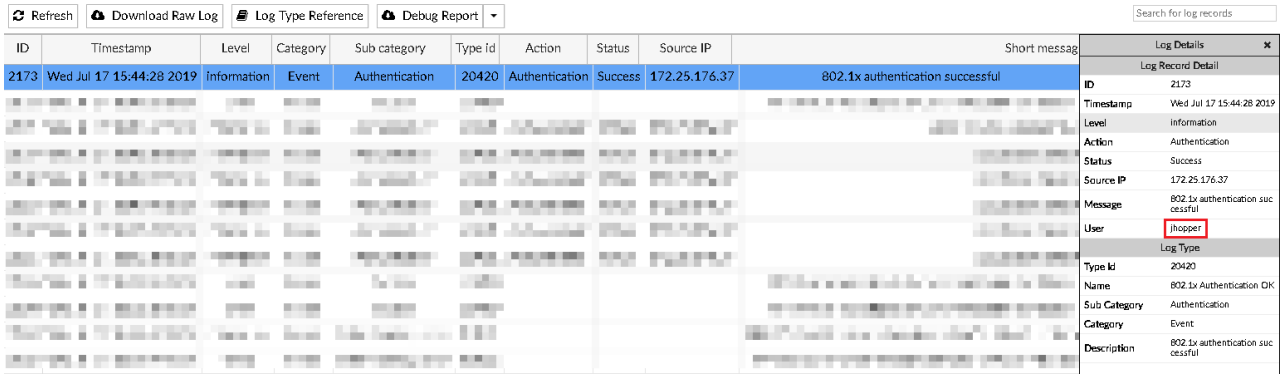

Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Advanced
Use simple certificate selection (Recommended)
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AddTrust External CA Root
Baltimore CyberTrust Root
Certum CA
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
View Certificate
Don't prompt user to authorize new servers or trusted certification authorities.
Use a different user name for the connection
OK
Cancel

Results

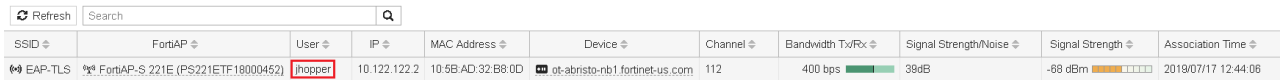
1. On the user's device, attempt to connect to the WiFi. Select the user's certificate and select **OK**.



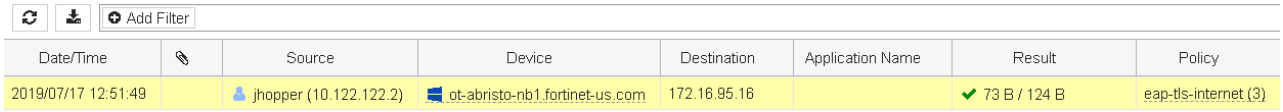
2. On the FortiAuthenticator, go to **Logging > Log Access > Logs** to confirm the successful authentication.

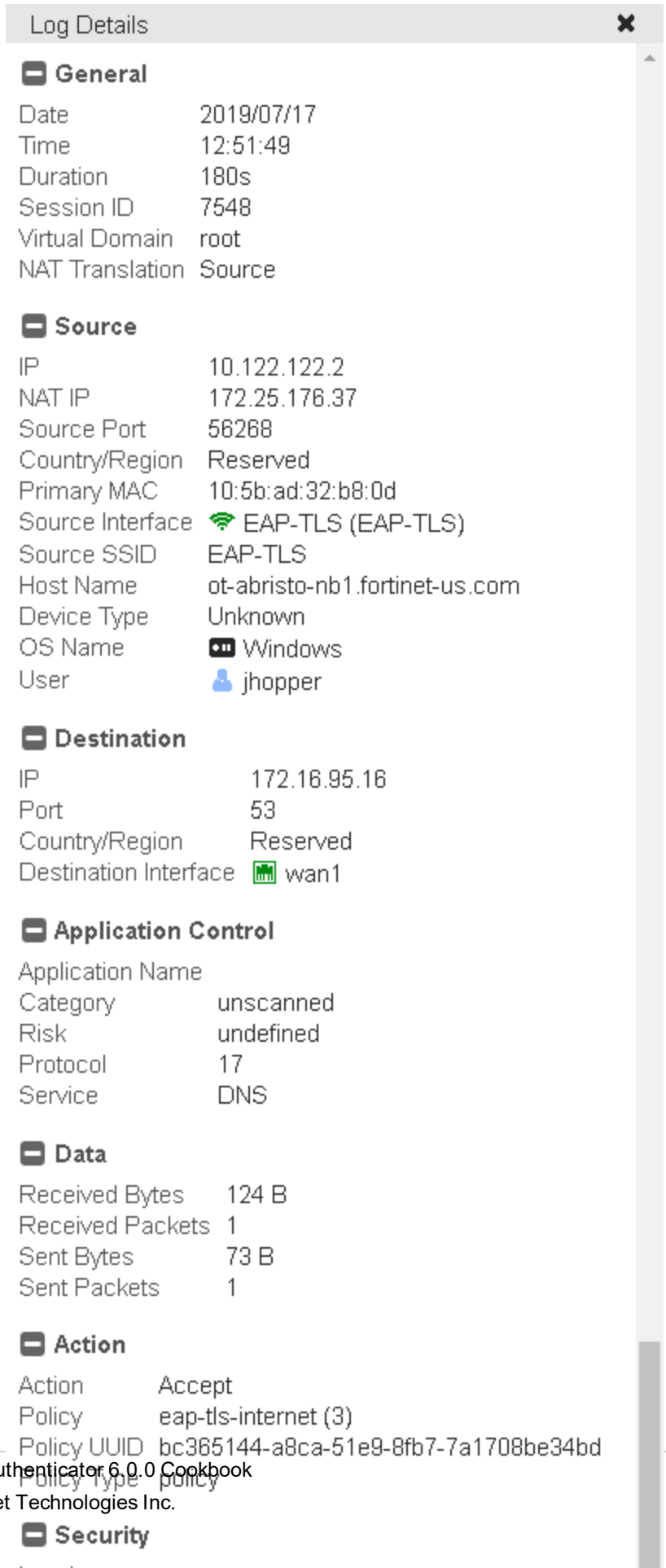


3. On the FortiGate, go to **Monitor > WiFi Client Monitor** to view various information about the client.

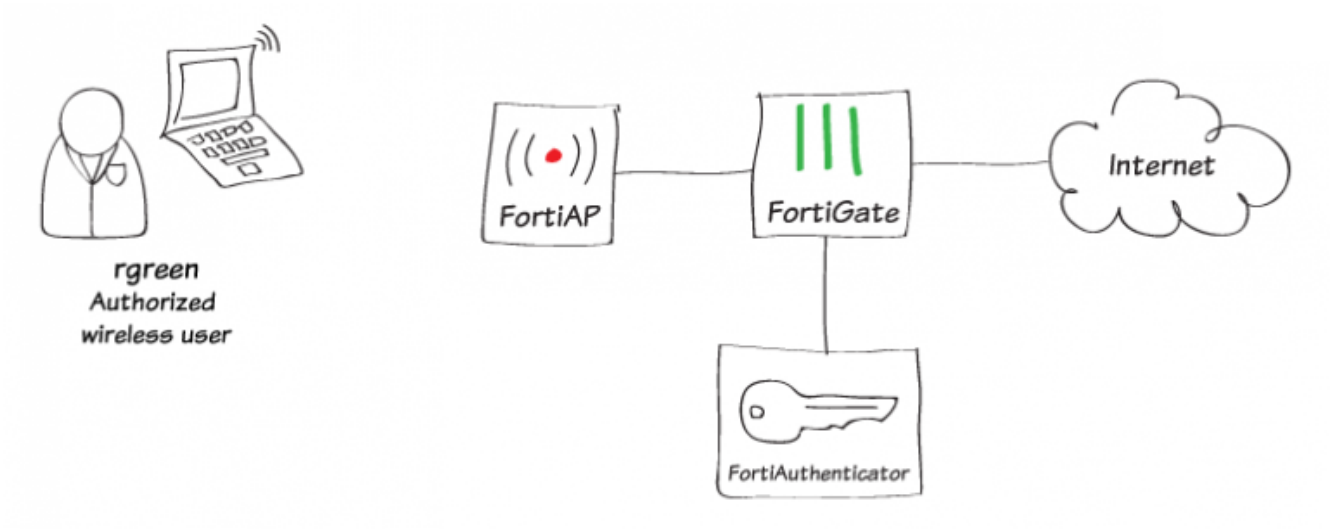


You can also go to **Log & Report > Forward Traffic** to view more log details.




Log Details
General
Date 2019/07/17
Time 12:51:49
Duration 180s
Session ID 7548
Virtual Domain root
NAT Translation Source
Source
IP 10.122.122.2
NAT IP 172.25.176.37
Source Port 56268
Country/Region Reserved
Primary MAC 10:5b:ad:32:b8:0d
Source Interface EAP-TLS (EAP-TLS)
Source SSID EAP-TLS
Host Name ot-abristo-nb1.fortinet-us.com
Device Type Unknown
OS Name Windows
User jhopper
Destination
IP 172.16.95.16
Port 53
Country/Region Reserved
Destination Interface wan1
Application Control
Application Name
Category unscanned
Risk undefined
Protocol 17
Service DNS
Data
Received Bytes 124 B
Received Packets 1
Sent Bytes 73 B
Sent Packets 1
Action
Action Accept
Policy eap-tls-internet (3)
Policy UUID bc365144-a8ca-51e9-8fb7-7a1708be34bd
Policy Type policy
Security

WiFi RADIUS authentication with FortiAuthenticator

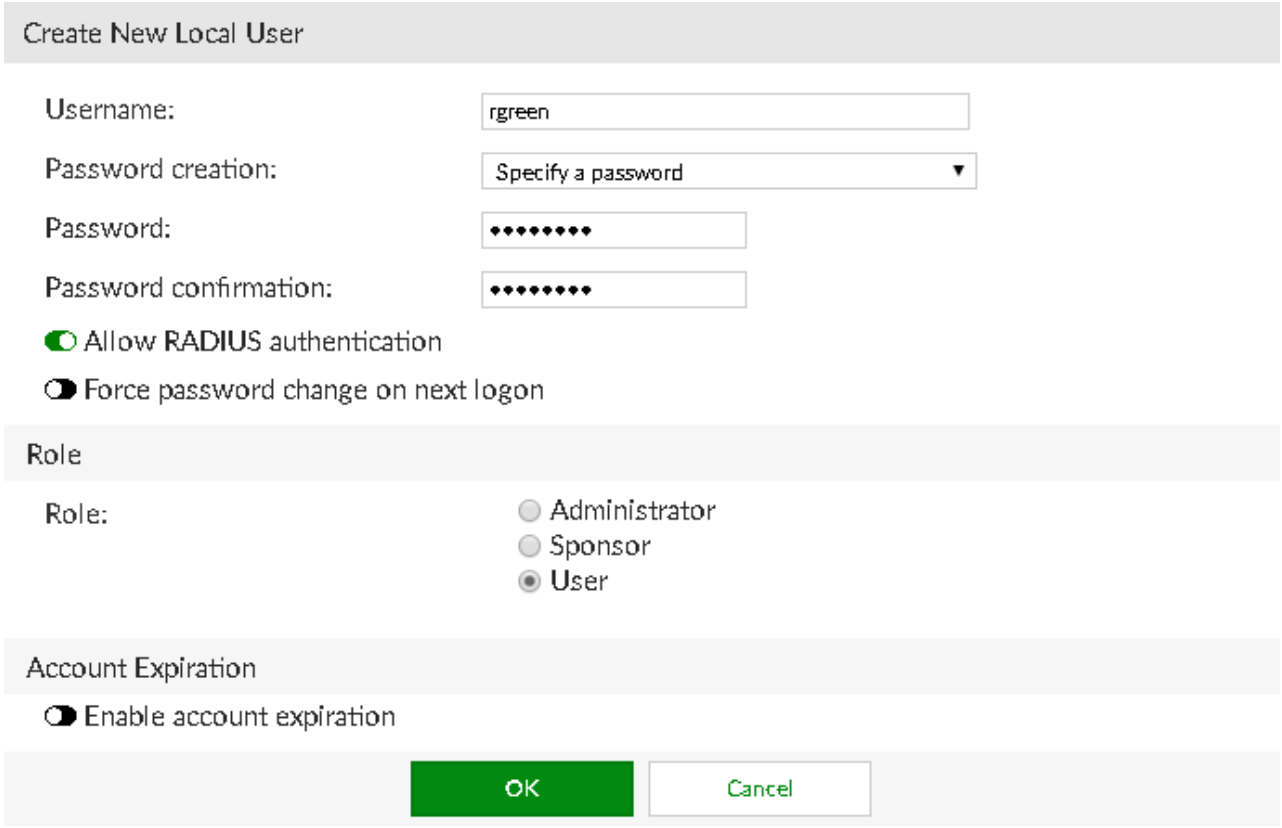


In this example, you use a RADIUS server to authenticate your WiFi clients.

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

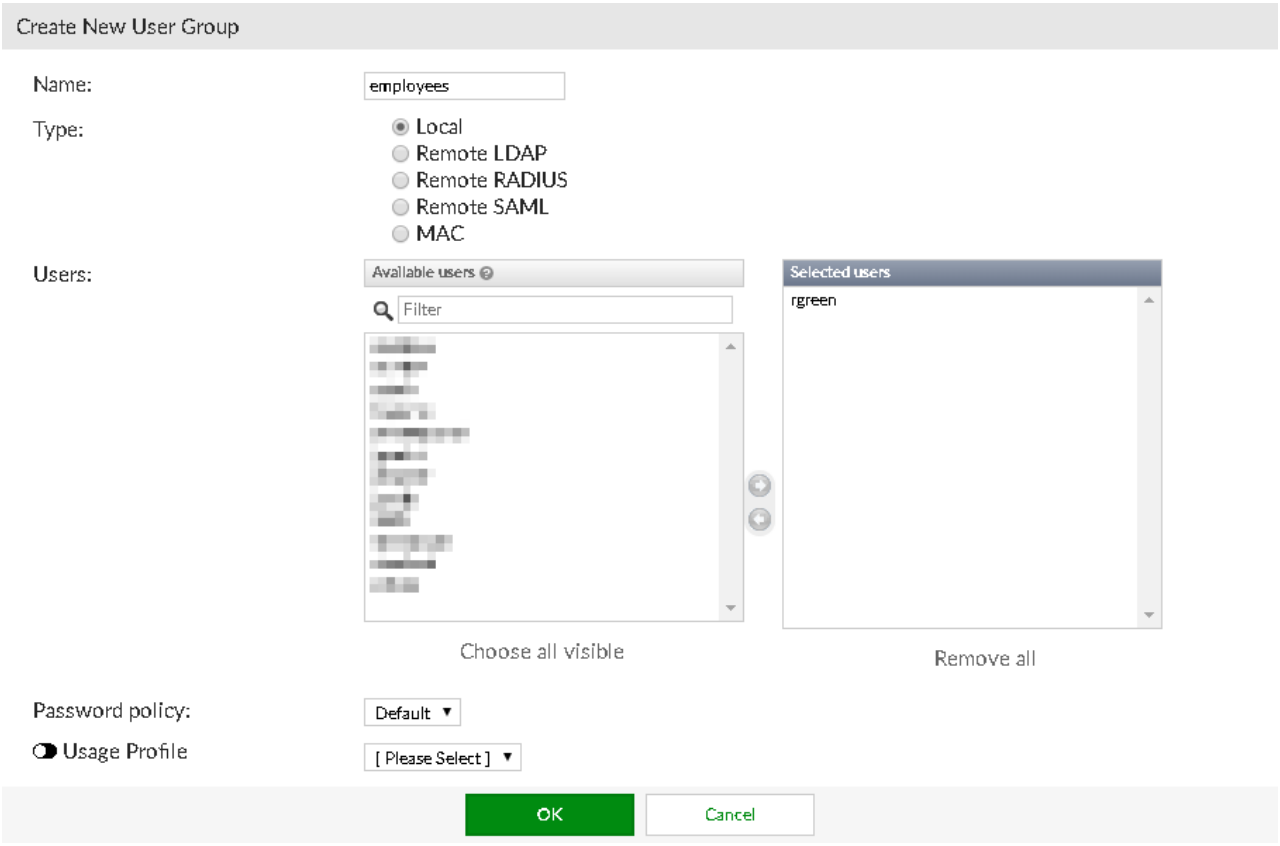
Creating users and user groups on the FortiAuthenticator

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



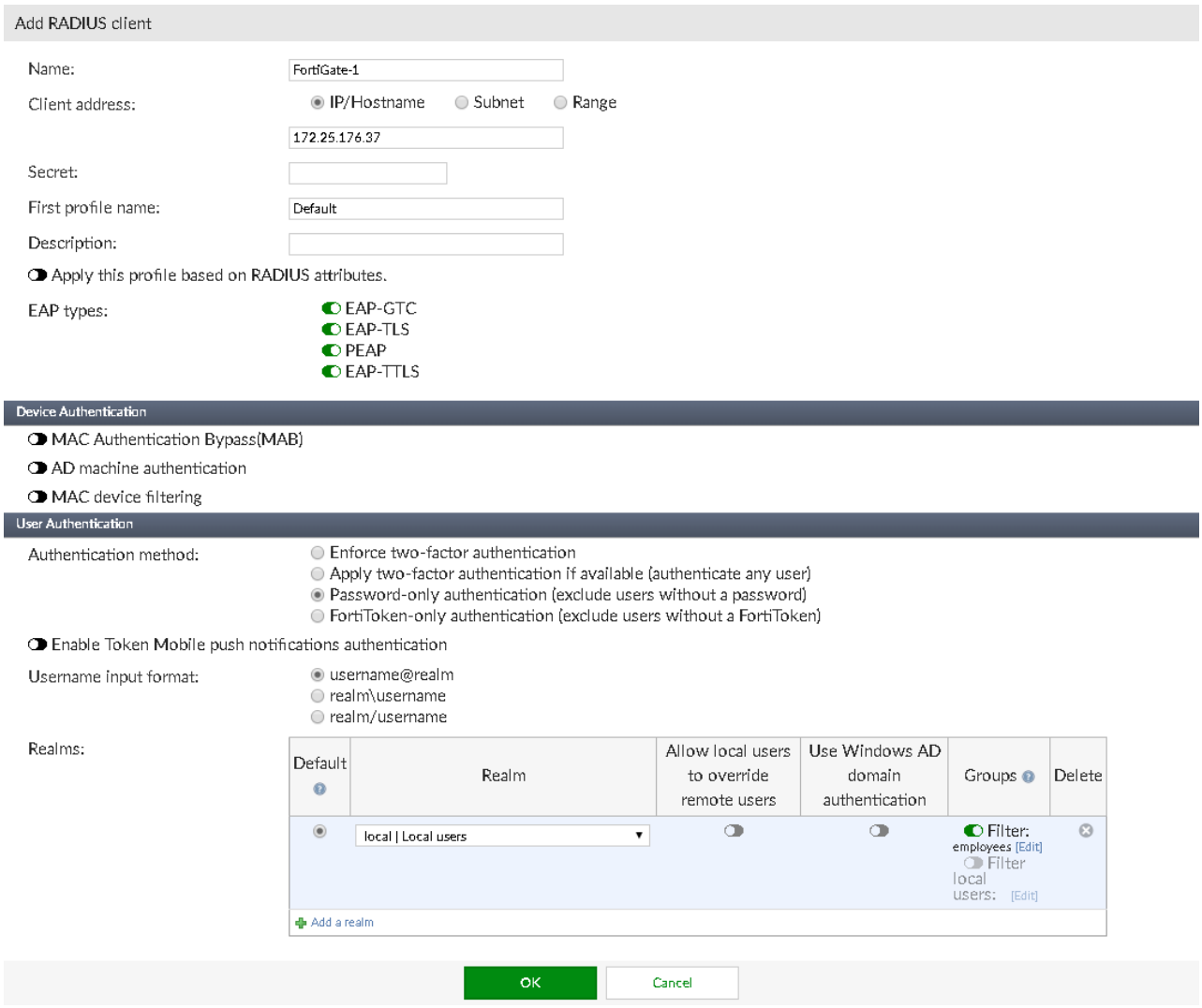
2. Then go to **Authentication > User Management > User Groups** and create a local user group (**employees**),

adding the newly created user.



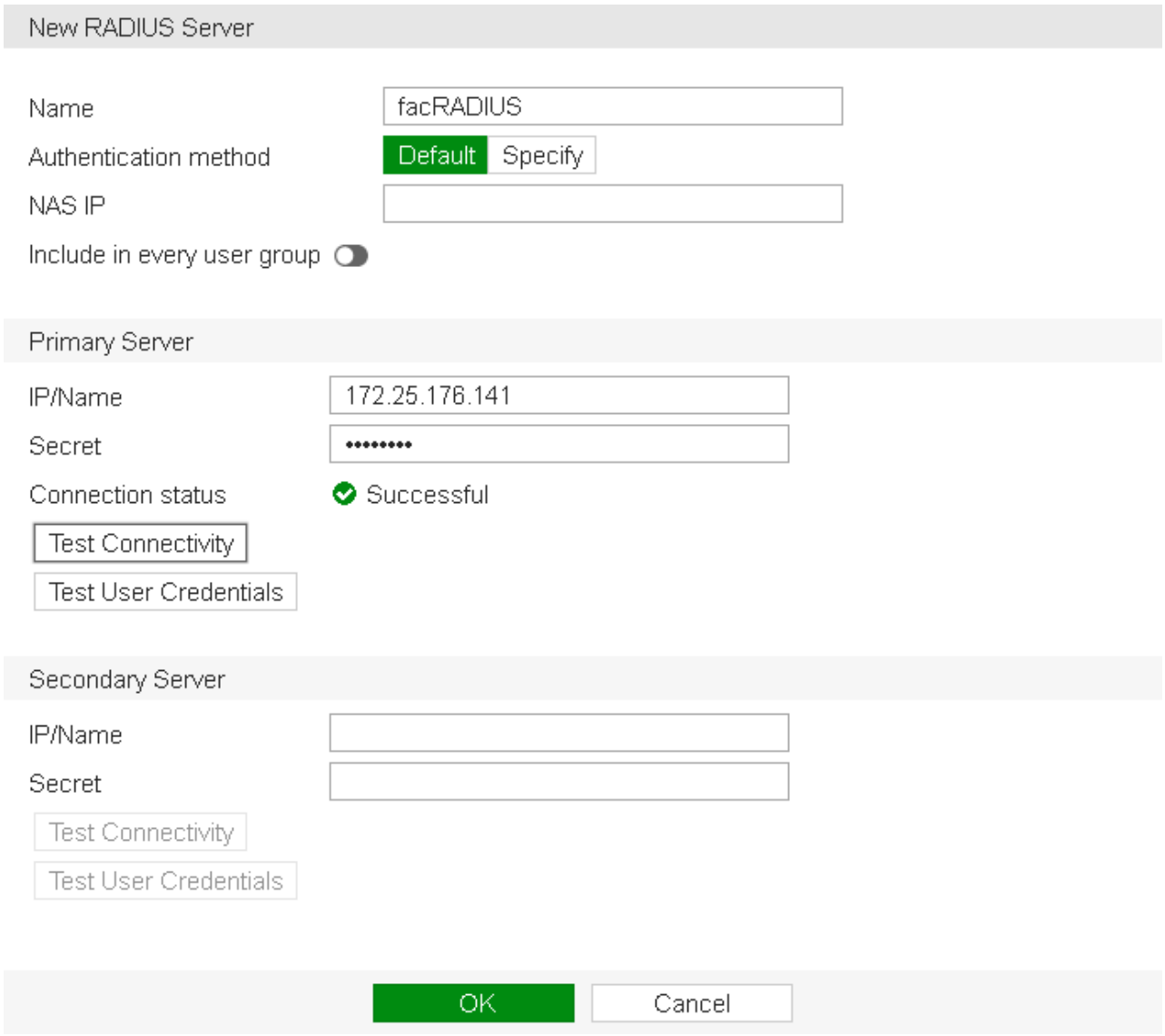
Registering the FortiGate as a RADIUS client on the FortiAuthenticator

1. Go to **Authentication > RADIUS Service > Clients** and create a client account. Enable all **EAP types**, set **Realm** to **local**, and apply the **employees** user group.



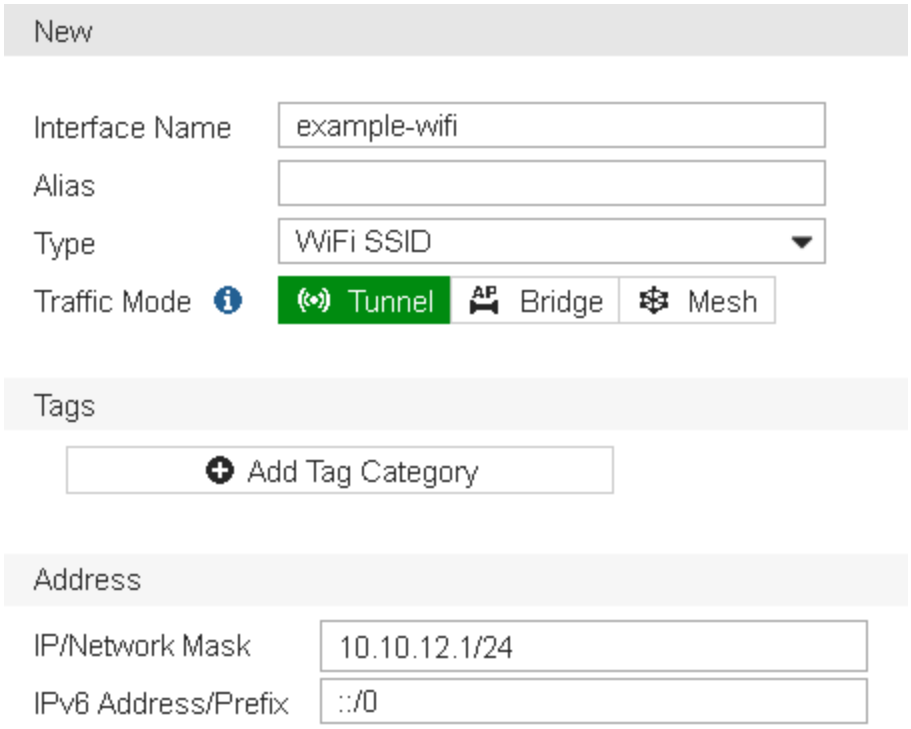
Configuring FortiGate to use the RADIUS server

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

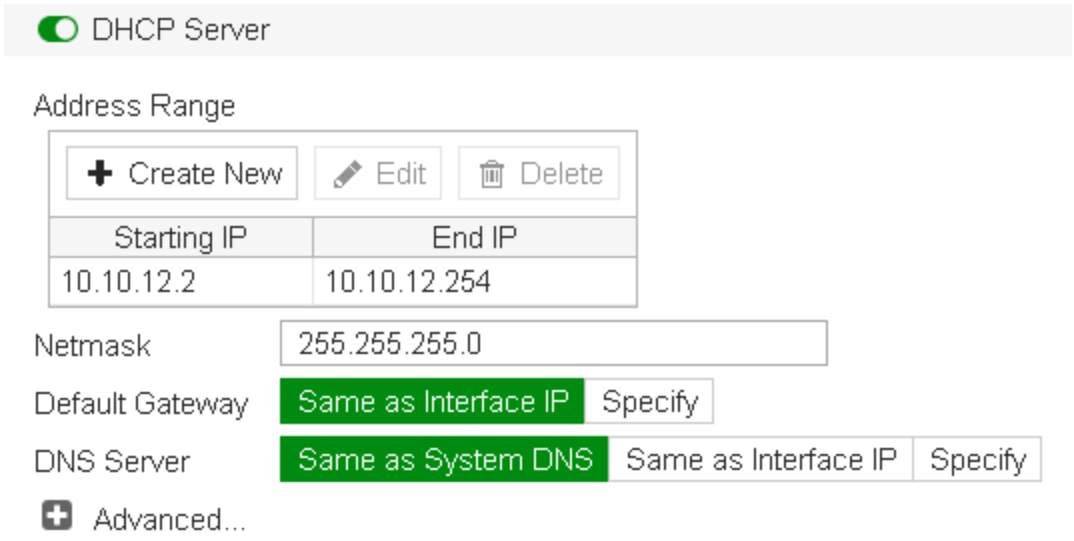

New RADIUS Server
Name
facRADIUS
Authentication method
Default
Specify
NAS IP
Include in every user group
Primary Server
IP/Name
172.25.176.141
Secret
Connection status
Successful
Test Connectivity
Test User Credentials
Secondary Server
IP/Name
Secret
Test Connectivity
Test User Credentials
OK
Cancel

Creating SSID and set up authentication

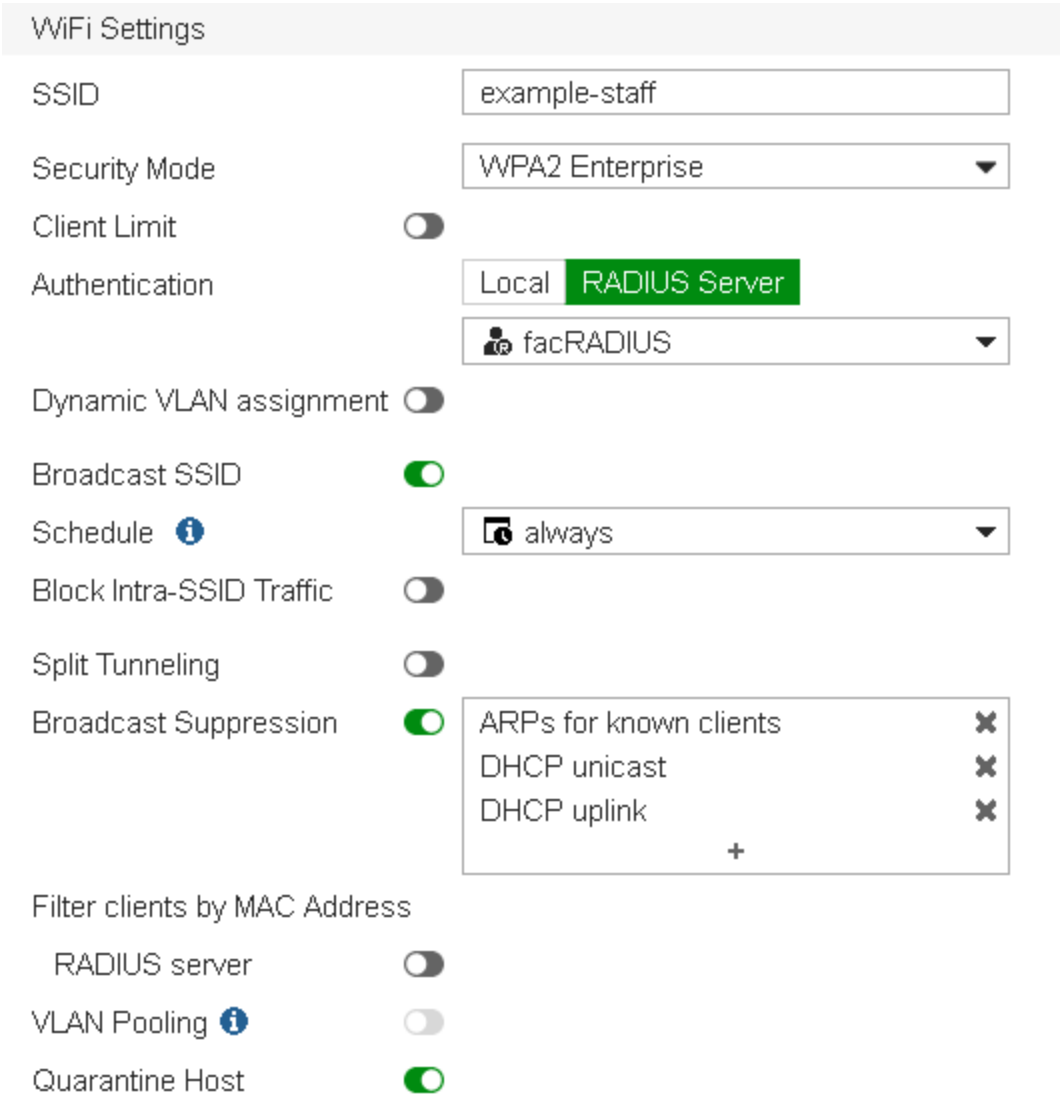
1. Go to **WiFi & Switch Controller > SSID** and define your wireless network.



2. Set up DHCP for your clients.

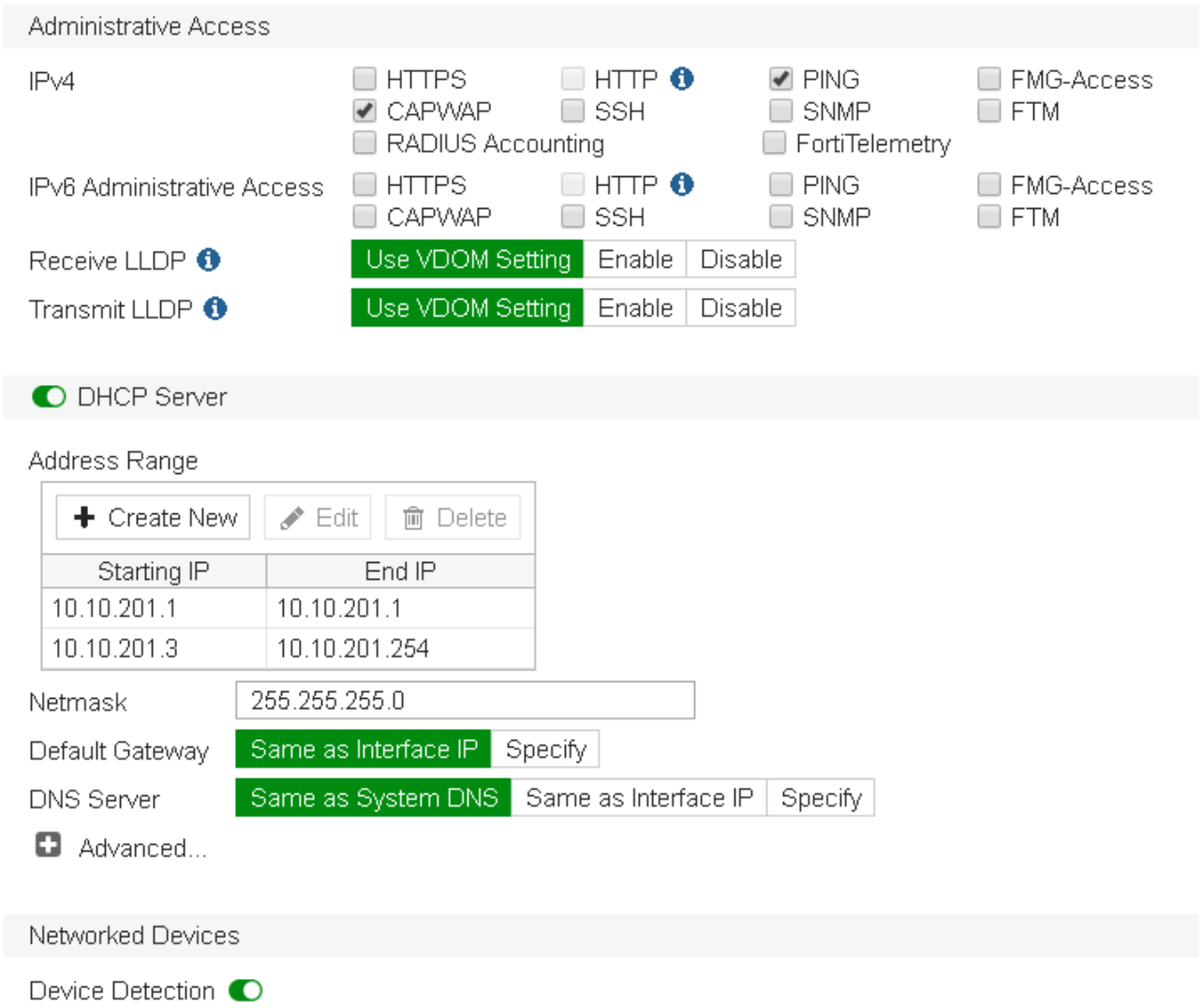


3. Configure WPA2 Enterprise security that uses the RADIUS server.

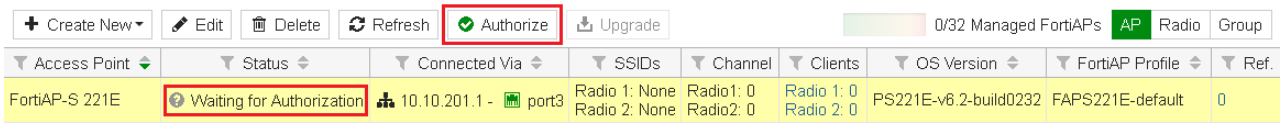


Connecting and authorizing the FortiAP

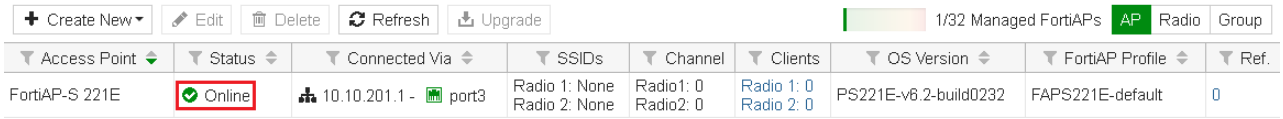
1. Go to **Network > Interfaces** and configure a dedicated interface for the FortiAP.
   Under **Administrative Access**, enable **PING** and **CAPWAP**, and enable **DHCP Server**.
   Under **Networked Devices**, enable **Device Detection**.



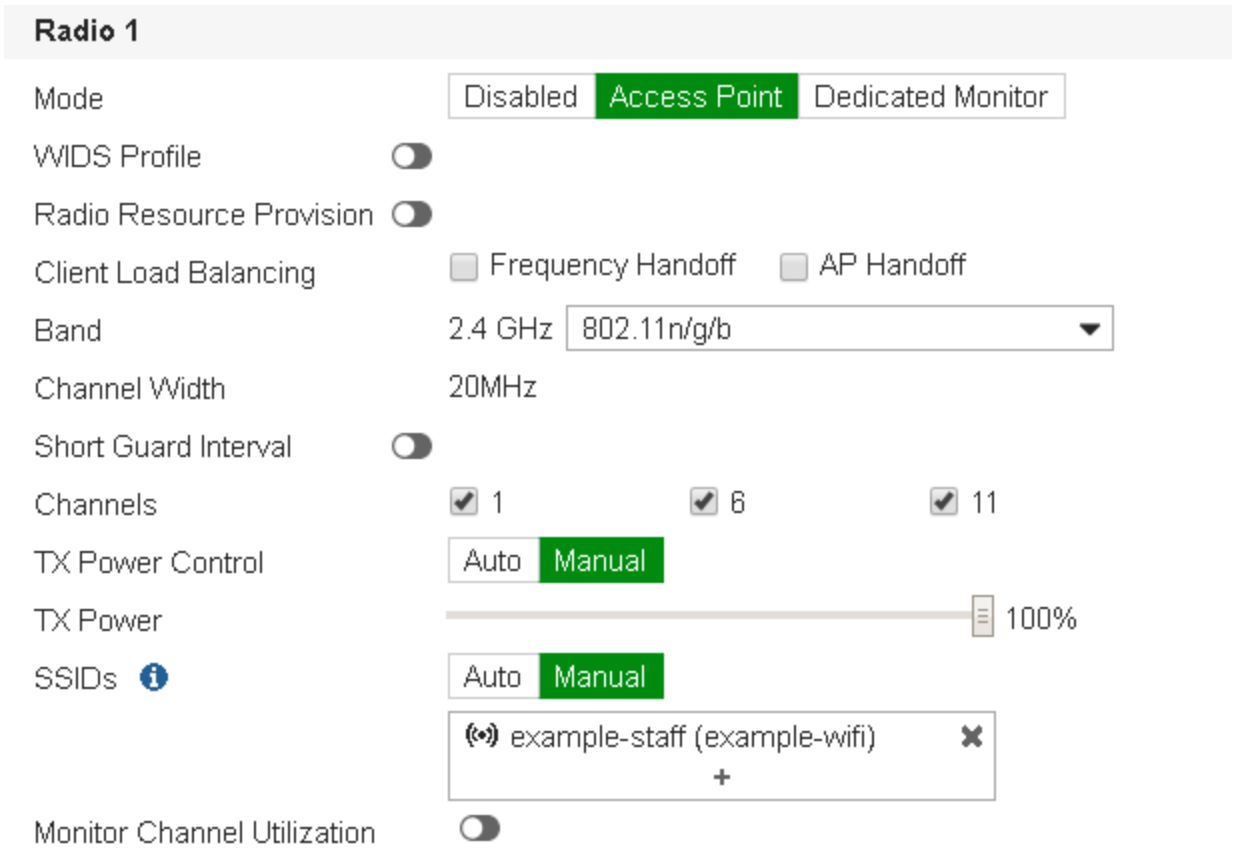
2. Connect the FortiAP unit to the interface. Then go to **WiFi & Switch Controller > Managed FortiAPs**. Notice the **Status** is showing **Waiting for Authorization**.
When the FortiAP is listed, select and **Authorize** it.



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

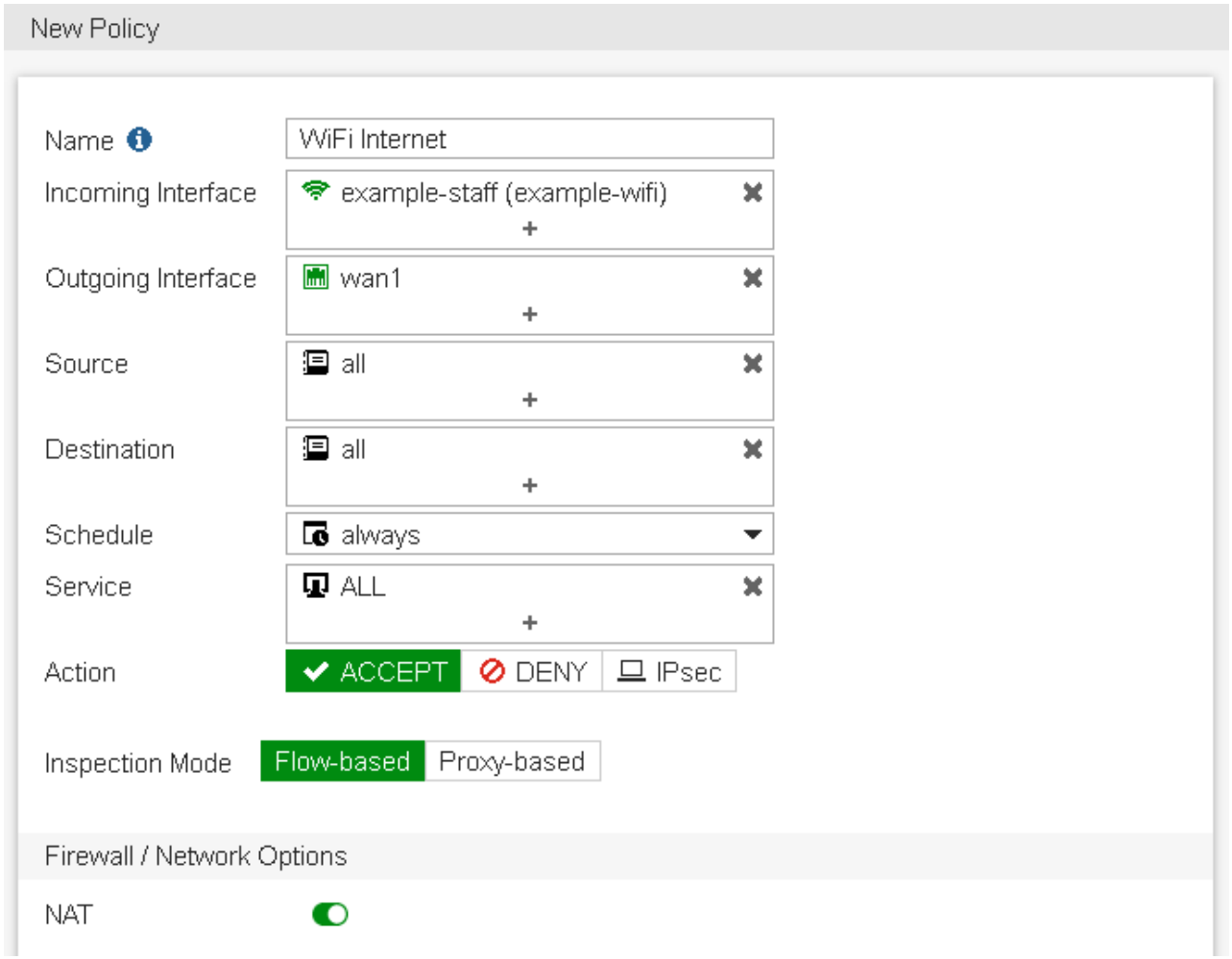


4. Go to **WiFi & Switch Controller > FortiAP Profiles** and edit the profile.
This example uses a FortiAP-S 221E, so the **FAPS221E-default** profile applies.
For each radio, make sure to select your **SSID**.

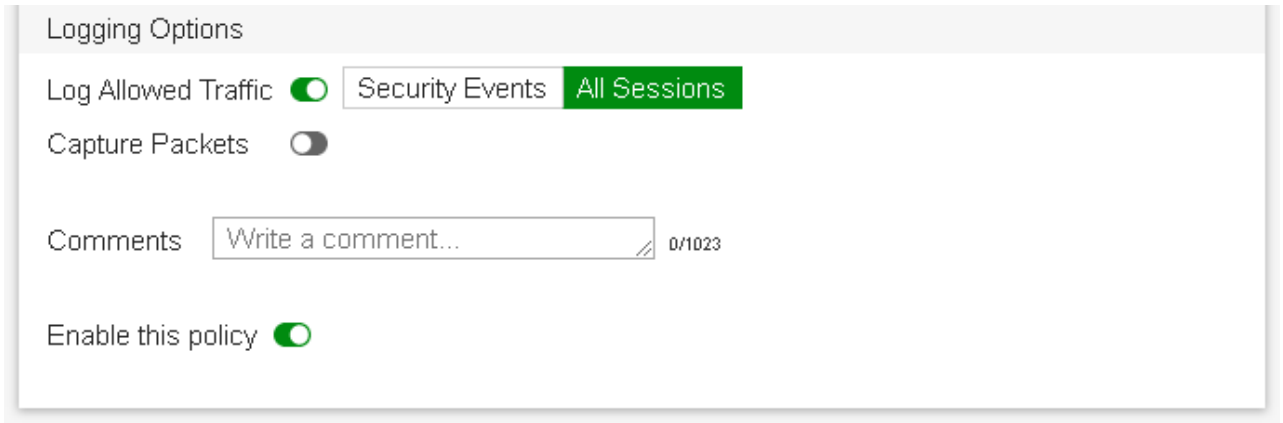

Radio 1
Mode
Disabled
Access Point
Dedicated Monitor
WIDS Profile
Radio Resource Provision
Client Load Balancing
Frequency Handoff
AP Handoff
Band
2.4 GHz
802.11n/g/b
Channel Width
20MHz
Short Guard Interval
Channels
1
6
11
TX Power Control
Auto
Manual
TX Power
100%
SSIDs
Auto
Manual
example-staff (example-wifi)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

Creating the security policy

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

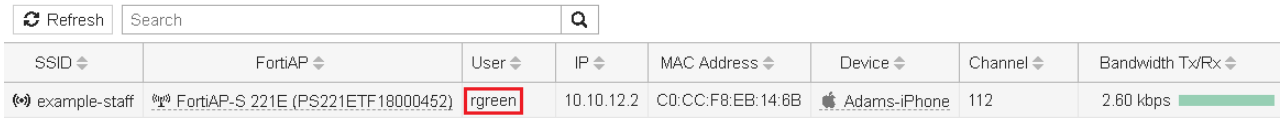


2. Under **Logging Options**, enable **Log Allowed Traffic** and **All Sessions**.

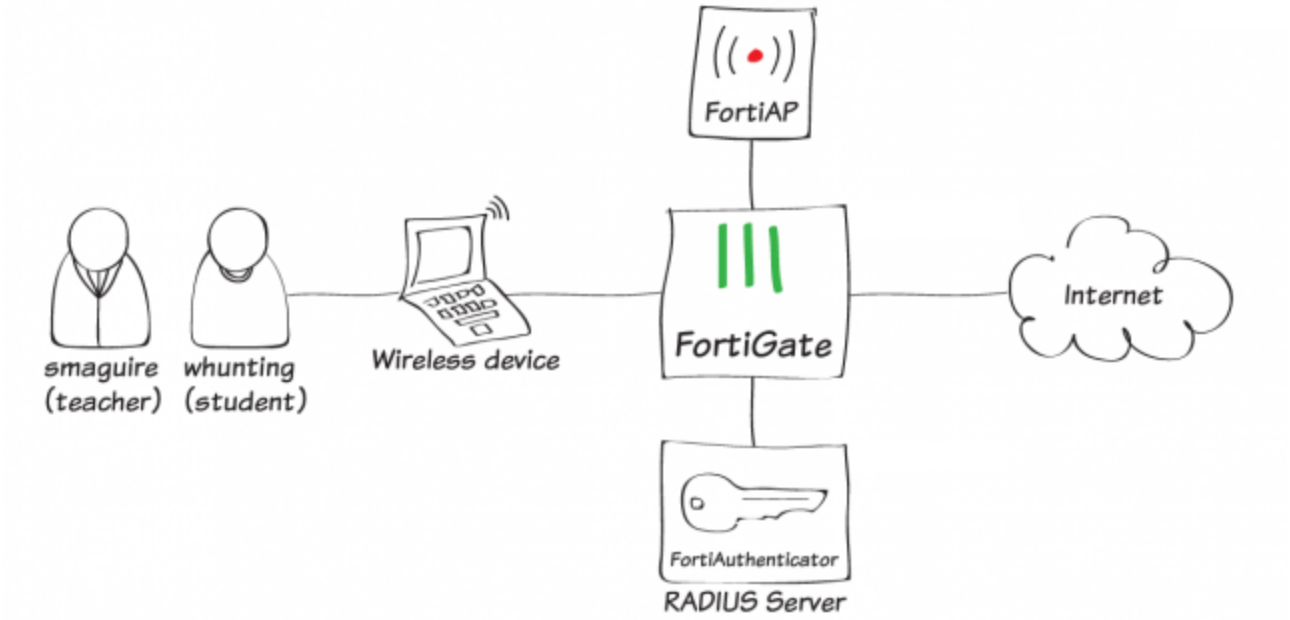


Results

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



WiFi with WSSO using FortiAuthenticator RADIUS and Attributes



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

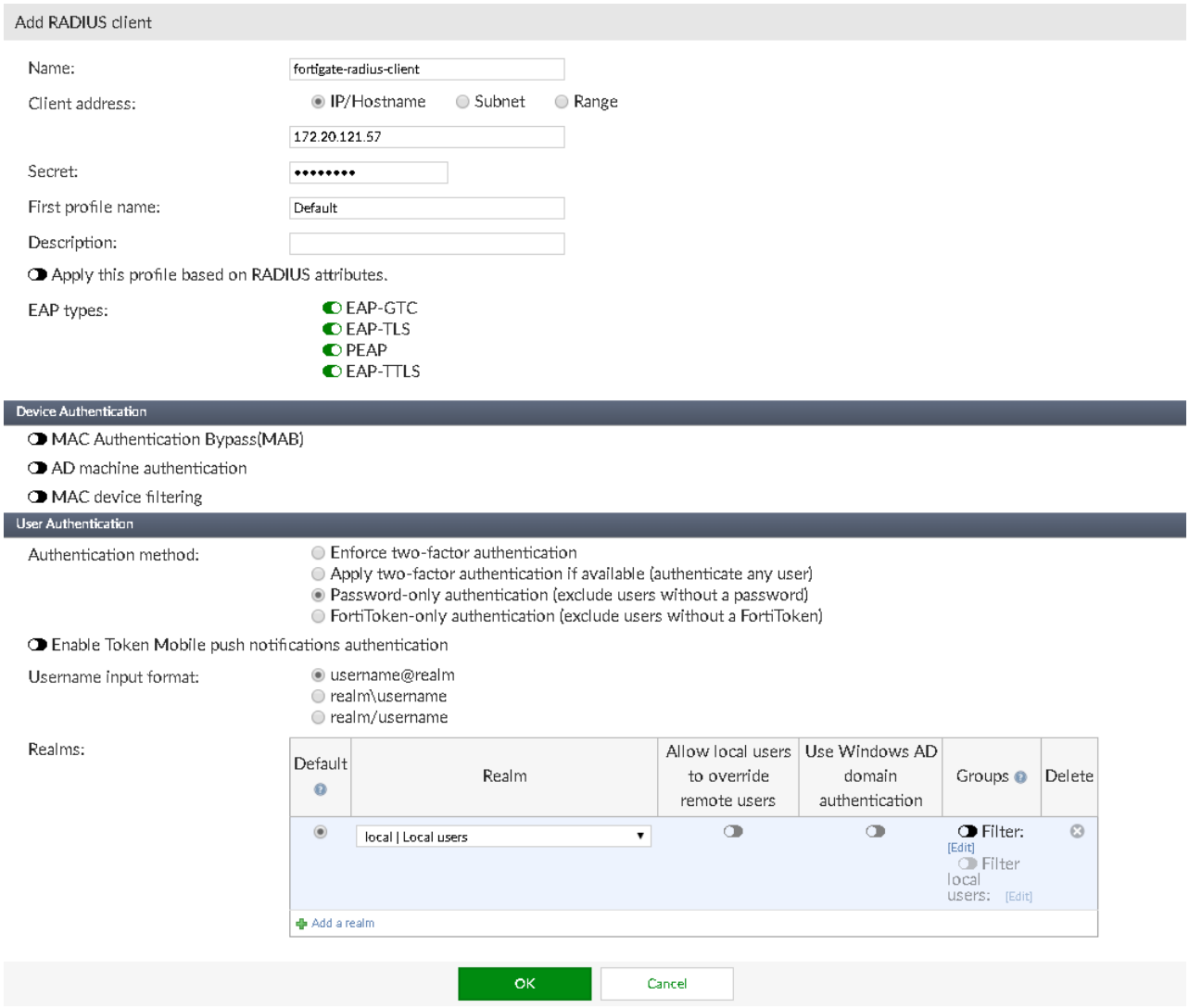
This recipe assumes that an SSID and a FortiAP are configured on the FortiGate unit. In this configuration, you will be changing the existing SSID's WiFi settings so authentication is provided by the RADIUS server.

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

Registering the FortiGate as a RADIUS client on the FortiAuthenticator

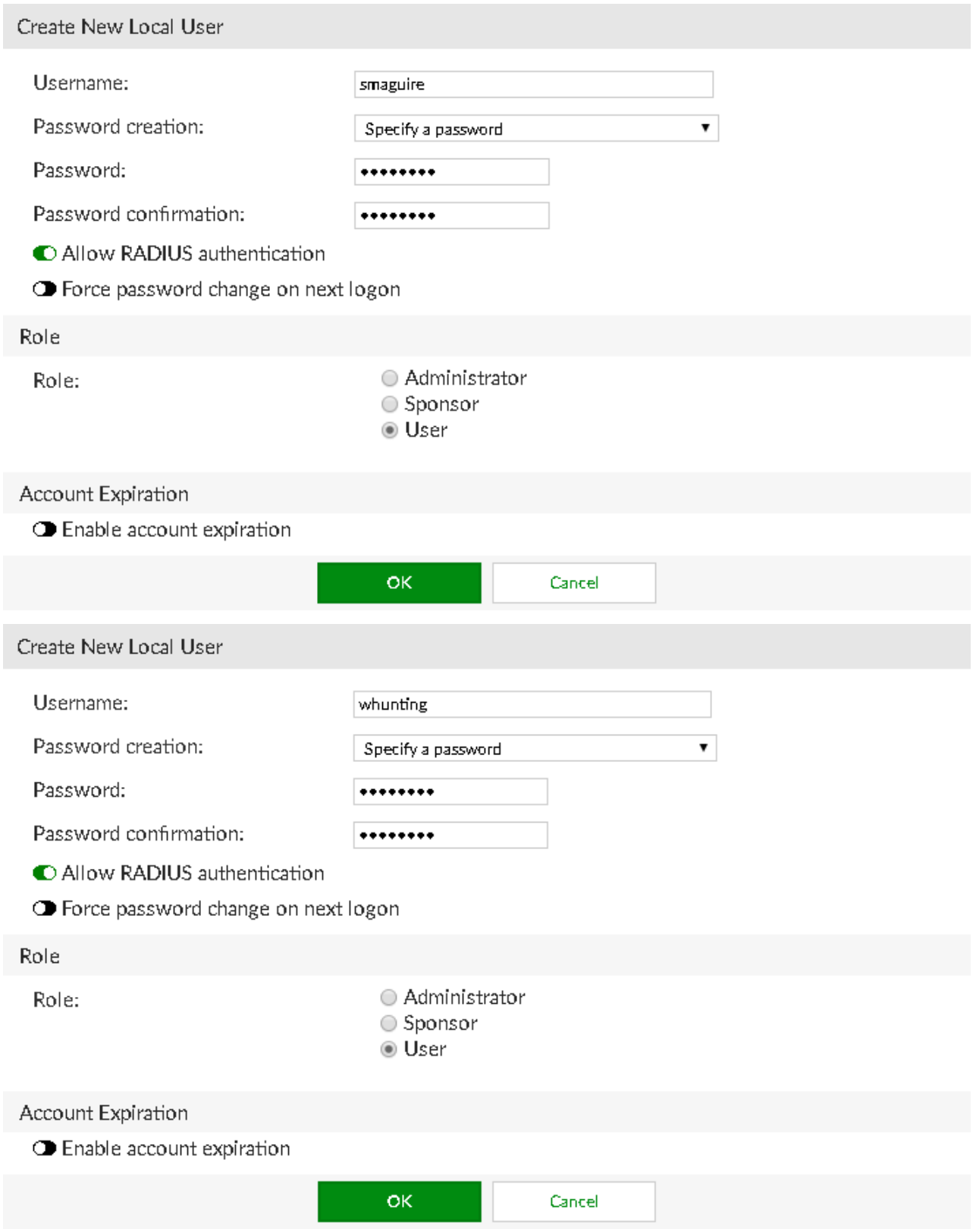
1. On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients** and select **Create New**.
   Enter a **Name**, the Internet-facing IP address of the FortiGate, and a **Secret**.

Select the **Password-only authentication** method, select the **Local** users realm, and enable all **EAP types**.



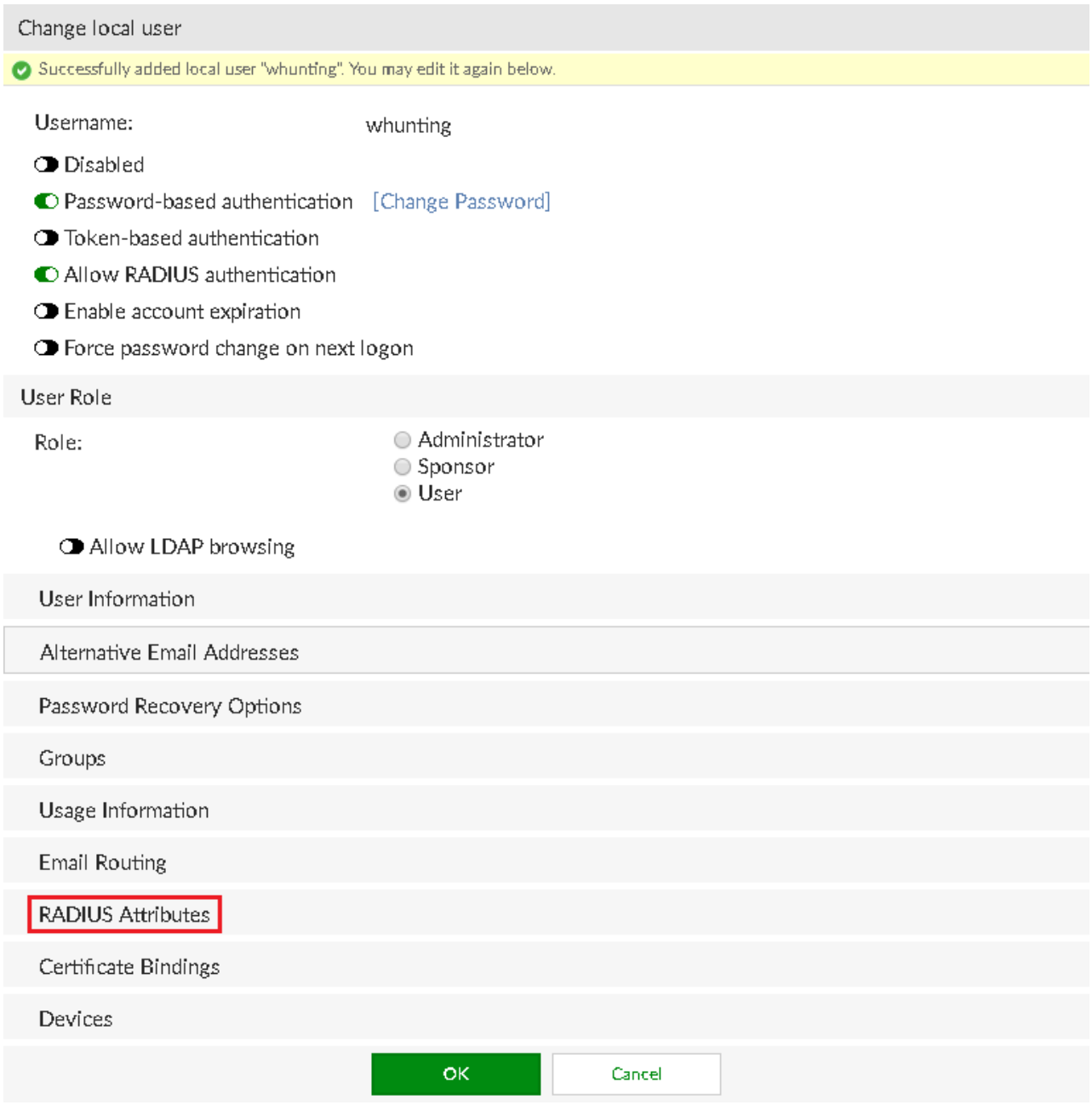
Creating users on the FortiAuthenticator

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



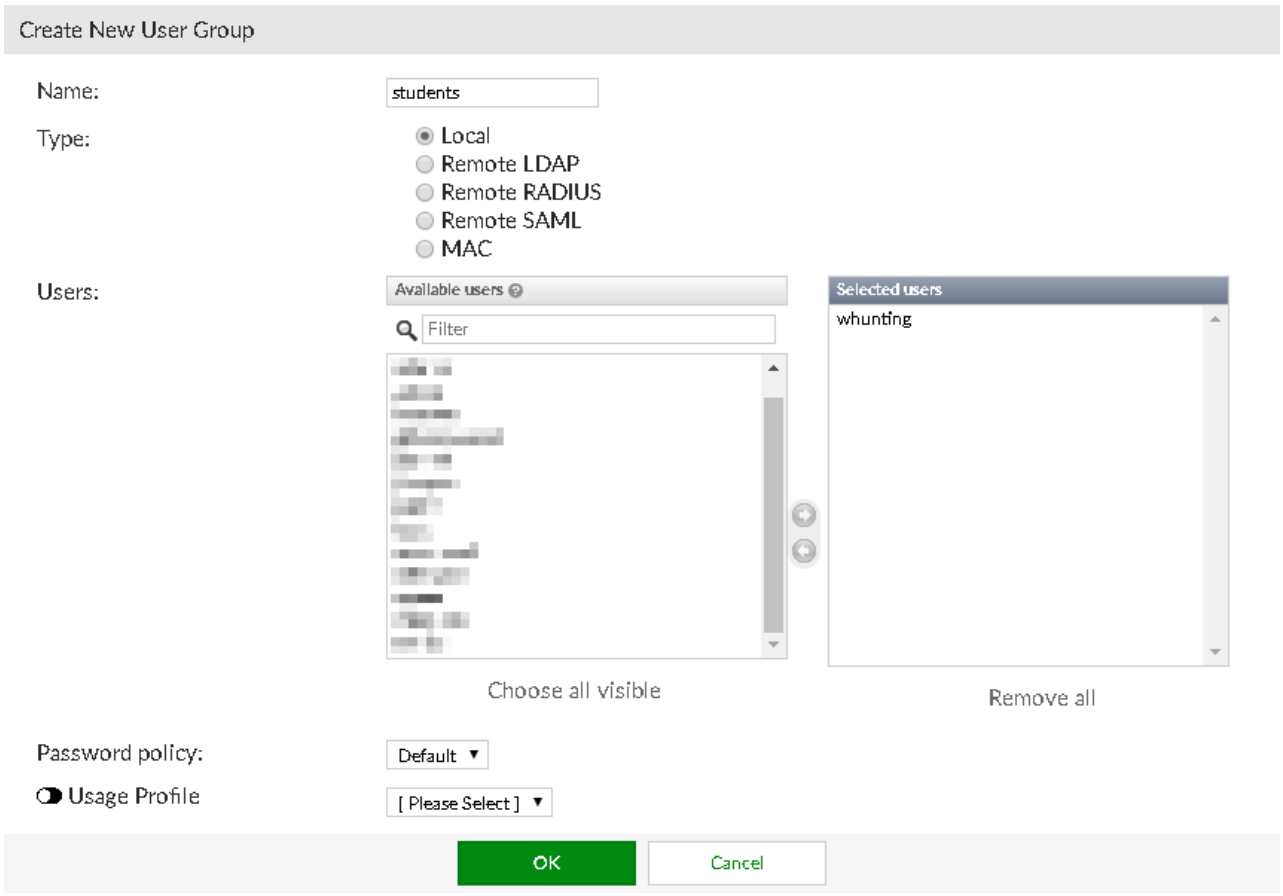
2. Note that, after you create the users, **RADIUS Attributes** appears as an option.

If your configuration involves multiple users, it is more efficient to add RADIUS attributes in their respective user groups, in the next step.

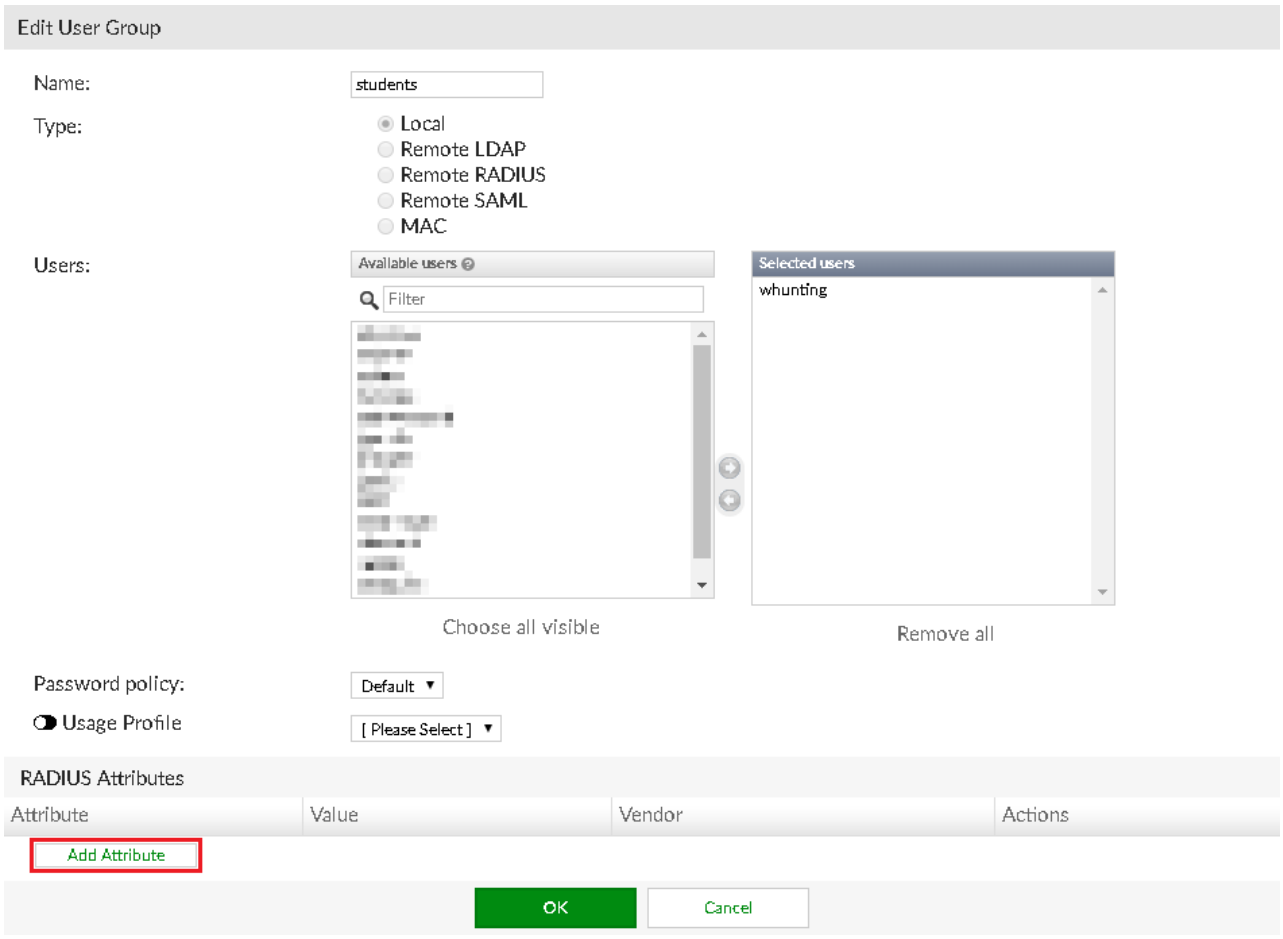


Creating user groups on the FortiAuthenticator

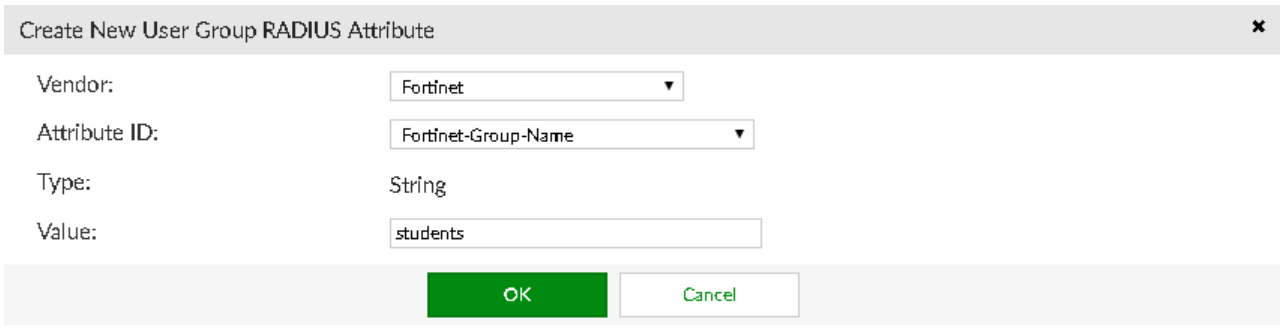
1. Go to **Authentication > User Management > User Groups** and create two user groups: **teachers** and **students**.
   Add the users to their respective groups.



2. Once created, edit both user groups and select **Add Attribute**.



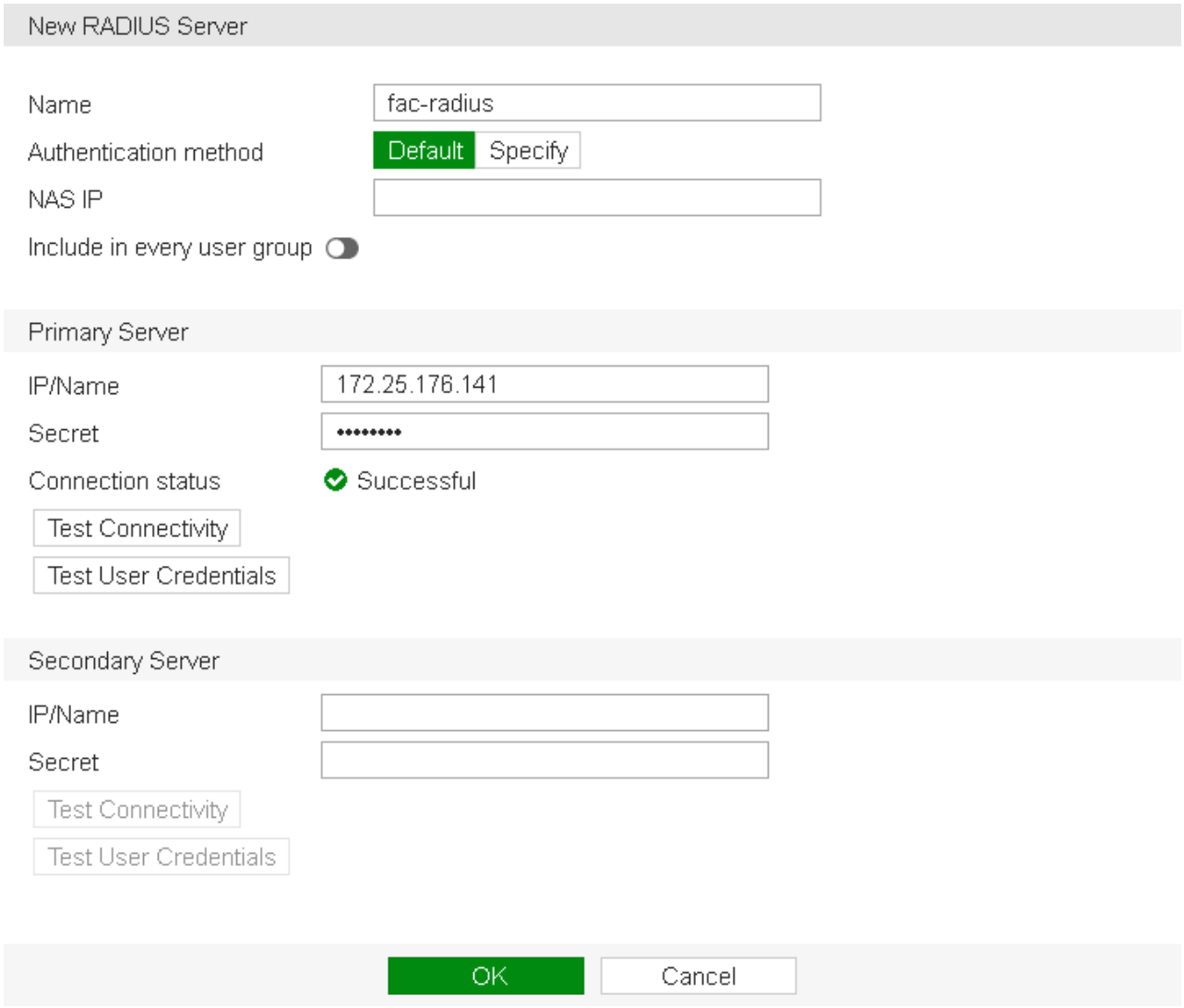
3. Add the **Fortinet-Group-Name** RADIUS attribute to each group, which specifies the user group name to be sent to the FortiGate.



Configuring the FortiGate to use the FortiAuthenticator as the RADIUS server

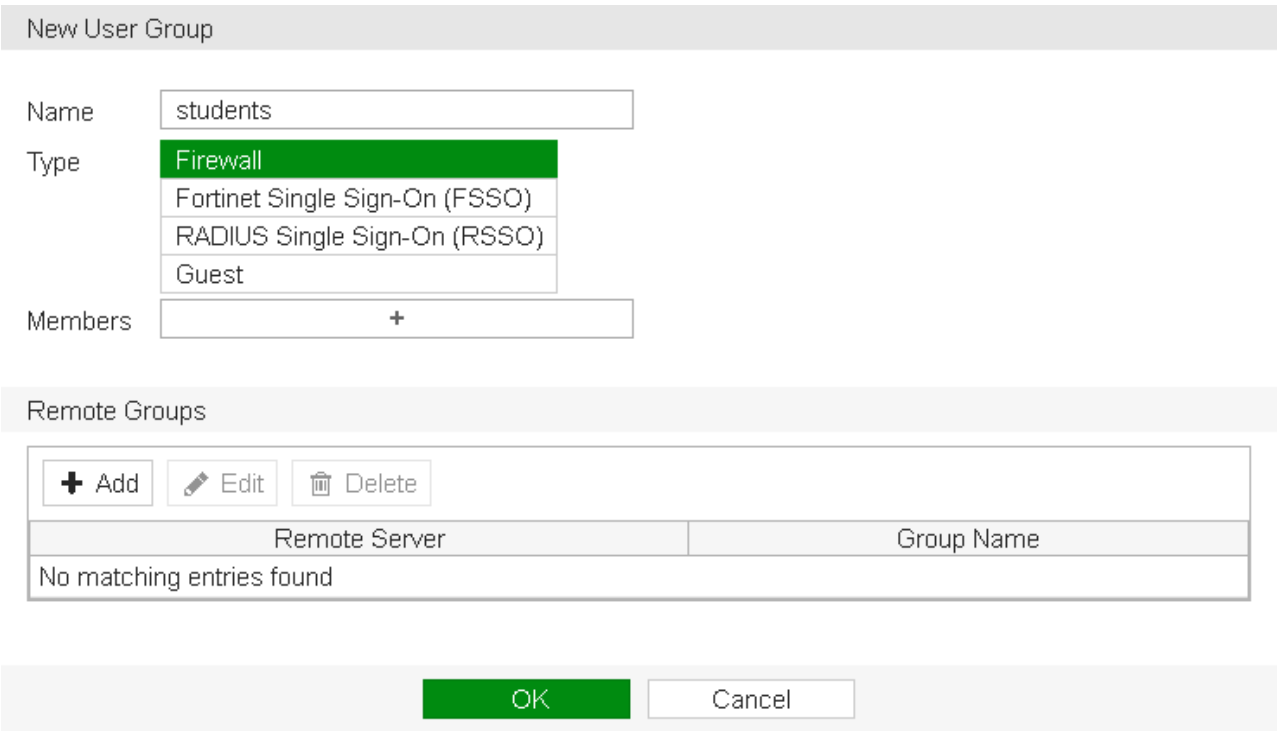
1. On the FortiGate, go to **User & Device > RADIUS Servers** and select **Create New**.
   Enter a **Name**, the Internet-facing IP address of the FortiAuthenticator, and enter the same **Primary Server Secret** entered on the FortiAuthenticator.

Select **Test Connectivity** to confirm the successful connection.



Configuring user groups on the FortiGate

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

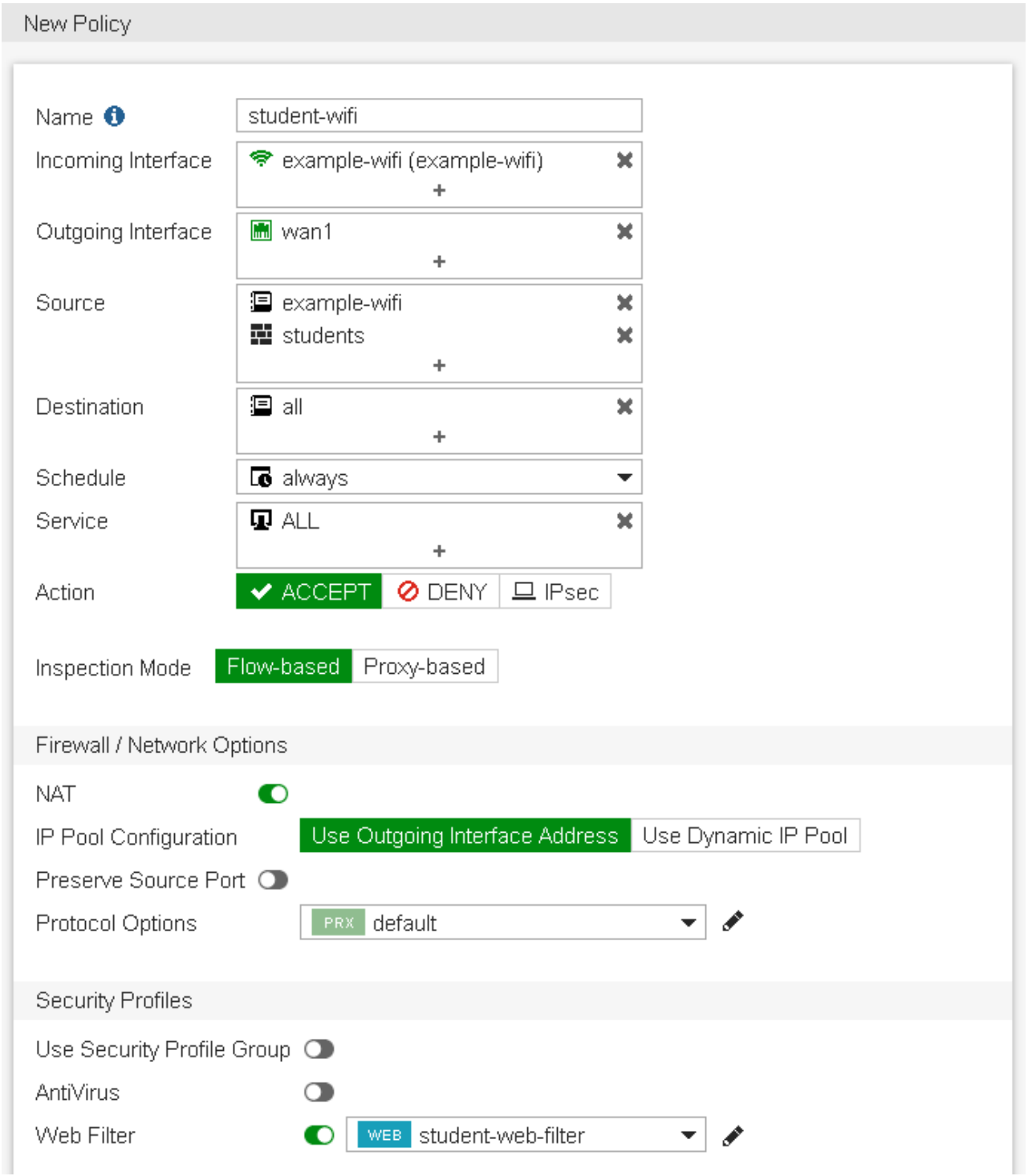


Do not add any members to either group.

Creating security policies

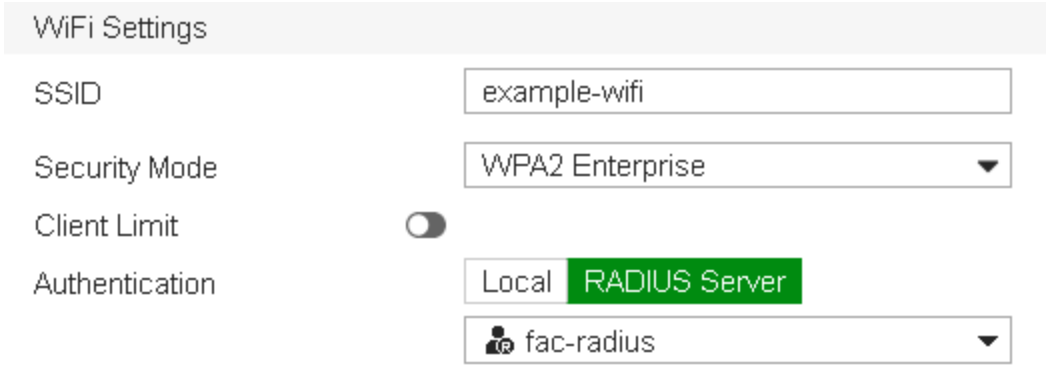
1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
   Create two policies (**student-wifi** and **teacher-wifi**) with WiFi-to-Internet access: one policy with **Source** set to the **students** user group, and the other set to **teachers**. Make sure to add the SSID address (*example-wifi*)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

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



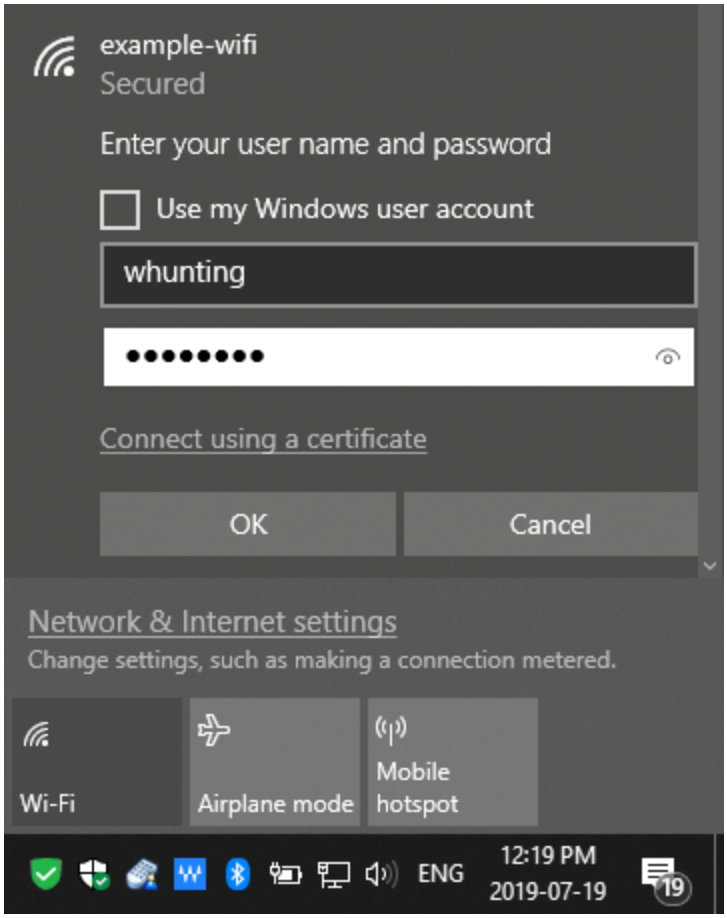
Configuring the SSID to RADIUS authentication

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

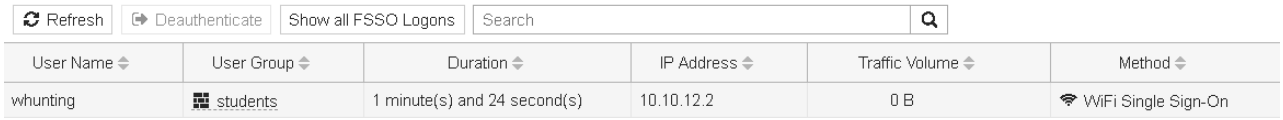


Results

1. Connect to the WiFi network as a student.



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



LDAP Authentication

This section describes configuring LDAP authentication.

- G Suite integration using LDAP on page 126

G Suite integration using LDAP

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

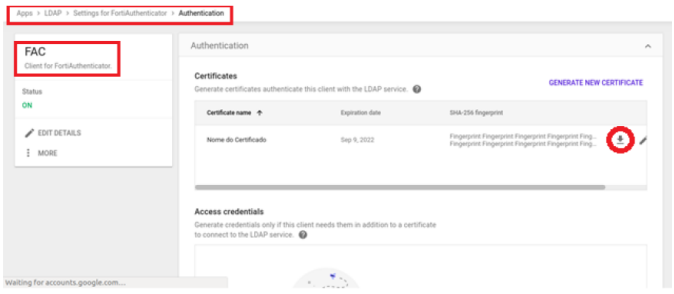
1. Generating the G Suite certificate on page 126
2. Importing the certificate to FortiAuthenticator on page 127
3. Configuring LDAP on the FortiAuthenticator on page 129
4. Troubleshooting on page 131

Generating the G Suite certificate

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

To generate certificate authentication:

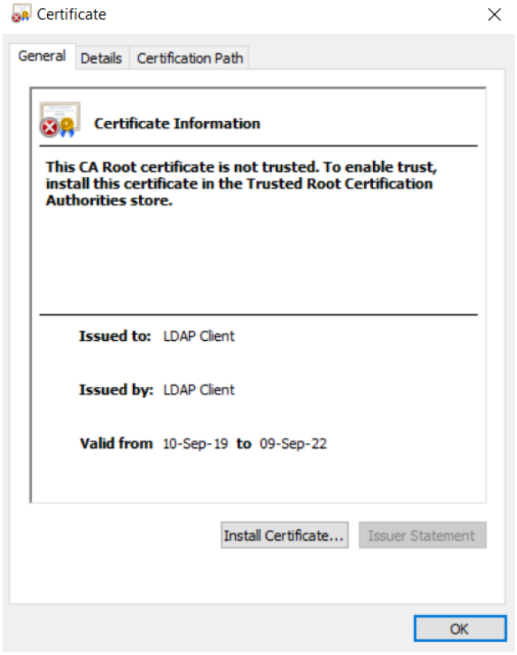
1. From the Google Admin console, go to **Apps** > **LDAP**.
2. Select one of the clients in the list.
3. Click the **Authentication** card.
4. Click **GENERATE NEW CERTIFICATE**, then click the download icon to download the certificate.
5. Upload the certificate to your client, and configure the application.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



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

Example:

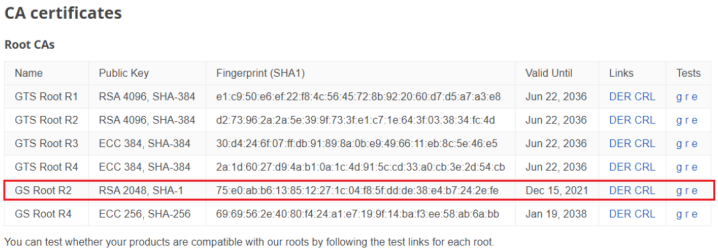
- Cert: *Google_2022_09_09_72372.crt*
- Key: *Google_2022_09_09_72372.key*



Store the certificate and key in a safe place.

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

- *GS Root R2*



CA certificates

Root CAs

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

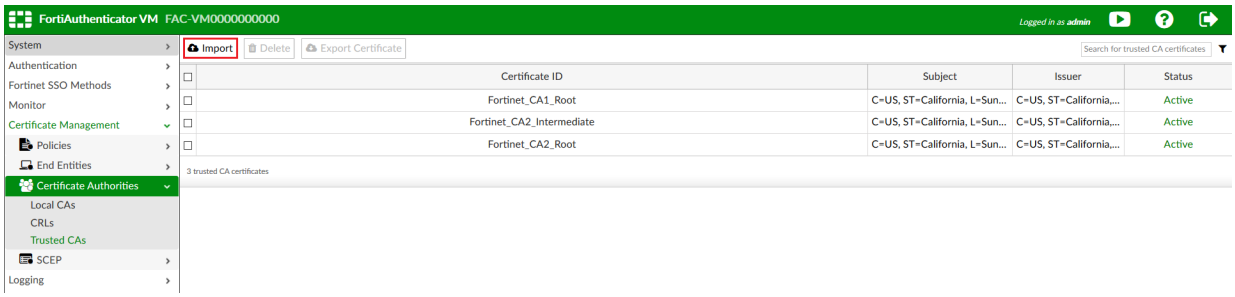
You can test whether your products are compatible with our roots by following the test links for each root.

Importing the certificate to FortiAuthenticator

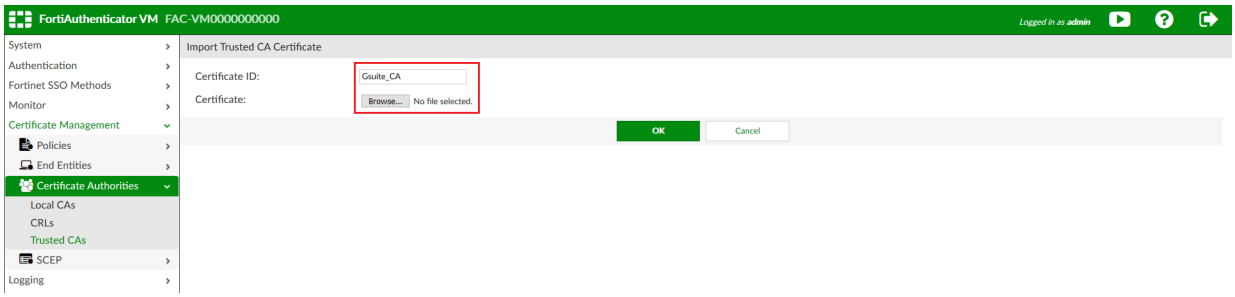
This series of steps can be performed on the primary FortiAuthenticator.

To import the trusted CA certificate:

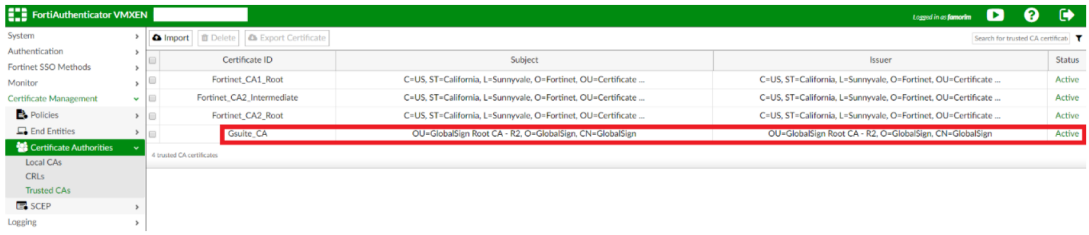
1. Go to **Certificate Management > Certificate Authorities > Trusted CAs > Import**.



2. Enter a Certificate ID, select the certificate, and click **OK**.



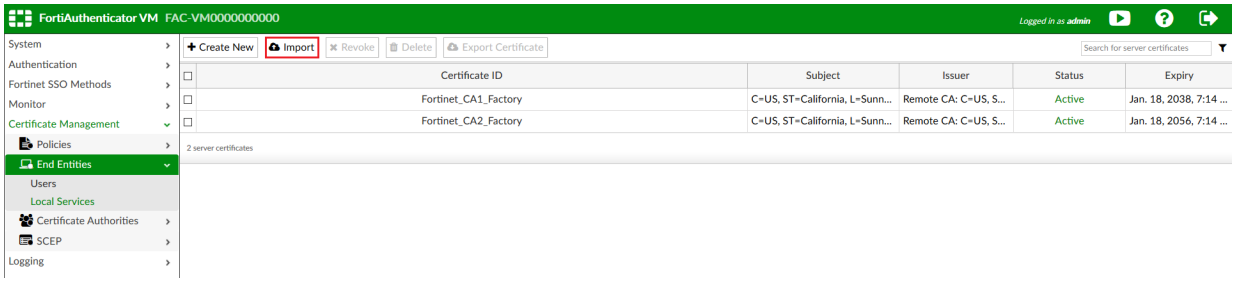
Results:



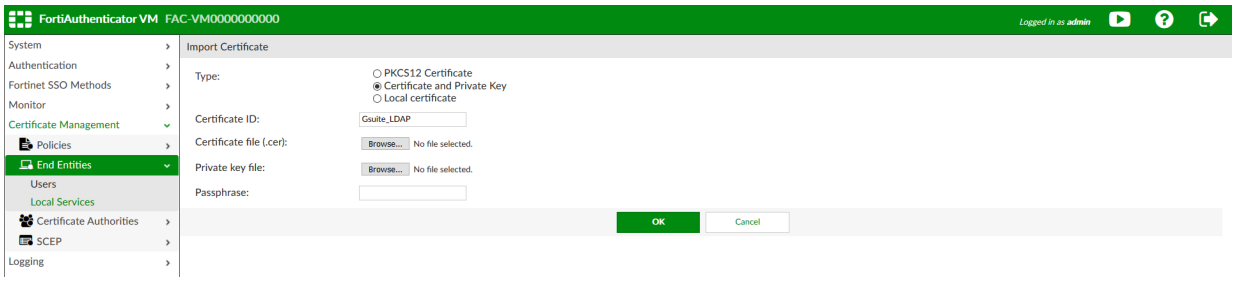
You can now import the LDAP certificate generated by G Suite.

To import the client authentication certificate:

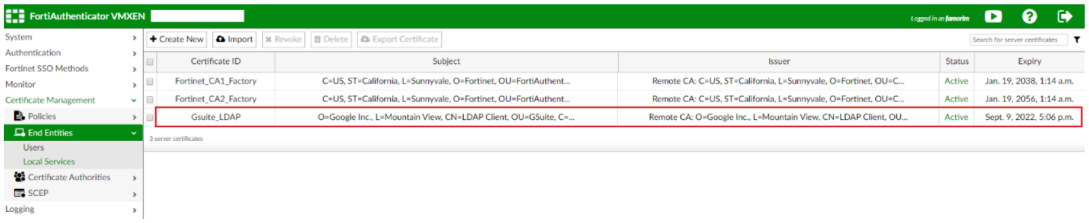
1. Go to **Certificate Management > End Entities > Local Services > Import**.



2. As the Type, select **Certificate and Private Key**.
3. Provide a Certificate ID, choose the file for the previously saved certificate and private key files, and select **OK**.

4. 

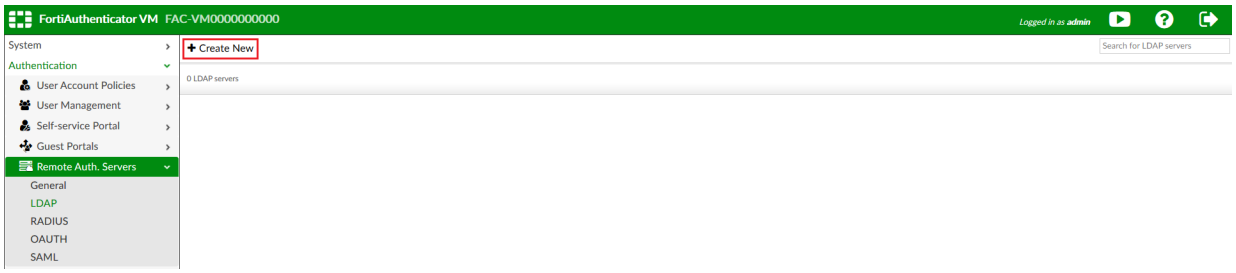
Results:



Configuring LDAP on the FortiAuthenticator

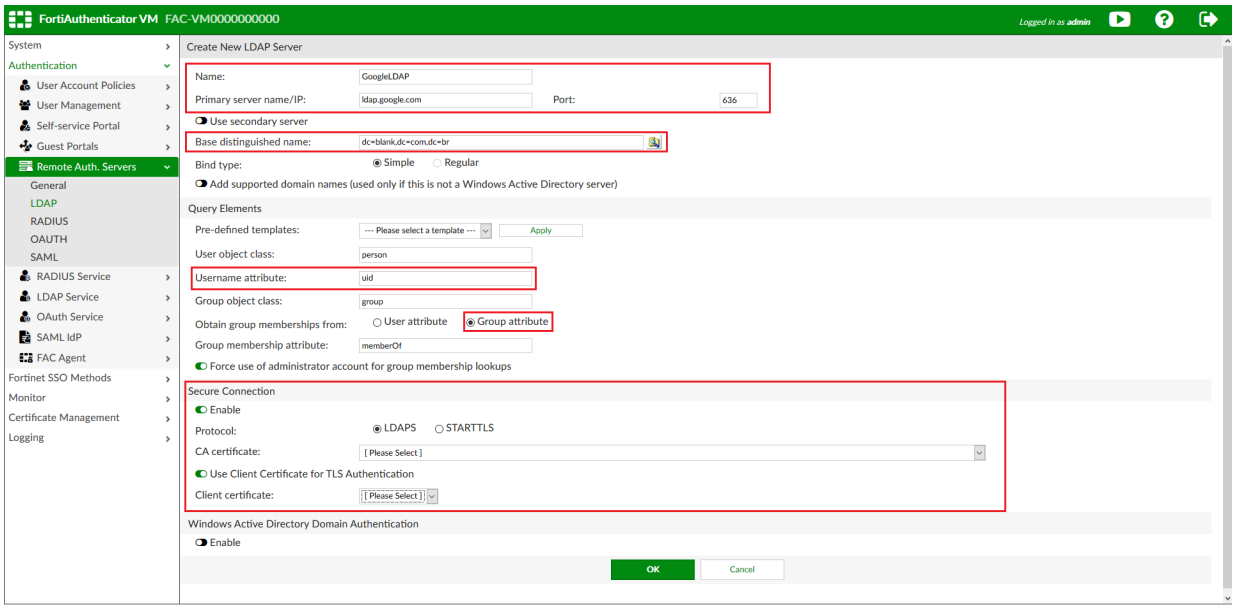
Now you can finish the LDAPS configuration using client authentication through certificate.

1. Go to **Authentication** > **Remote Auth. Servers** > **LDAP** > **Create New**.

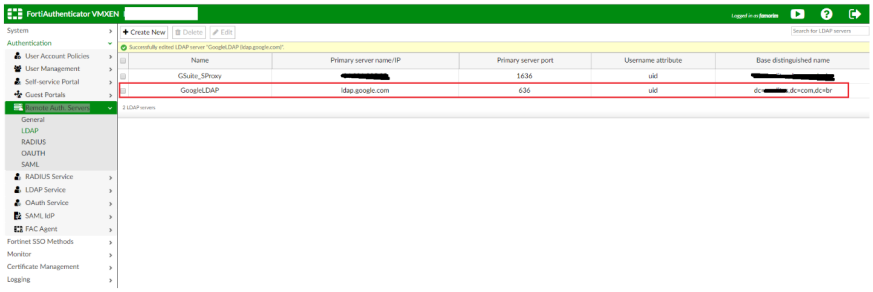


2. Enter a name.
3. For Primary server name/IP enter **ldap.google.com**, and set the port to **636.**
4. Enter the base distinguished name.
5. For the Username attribute, enter **uid**.
6. Select the option to obtain group memberships from **Group attribute**.
7. Enable **Secure Connection** and select either **LDAPS** or **STARTTLS** as the Protocol, and select the Google CA certificate.

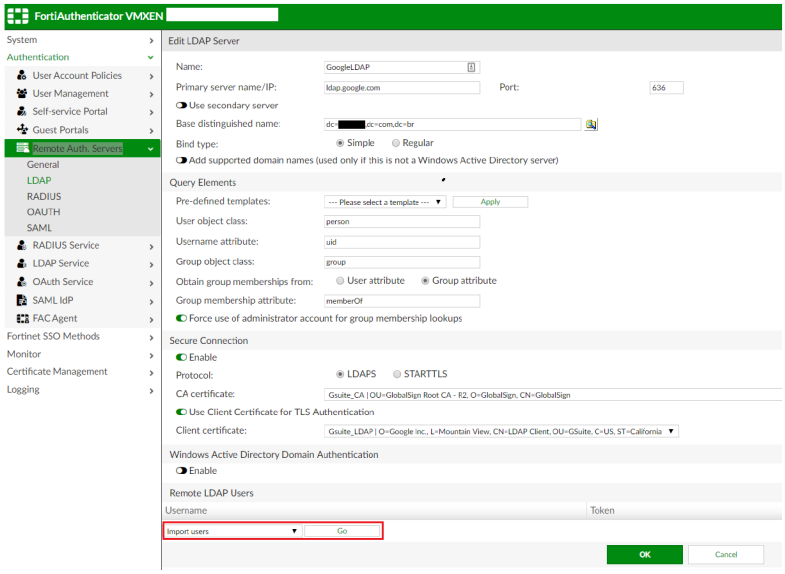
8. Enable **Use Client Certificate for TLS Authentication,** and select the LDAP certificate.



9. Select **OK**.



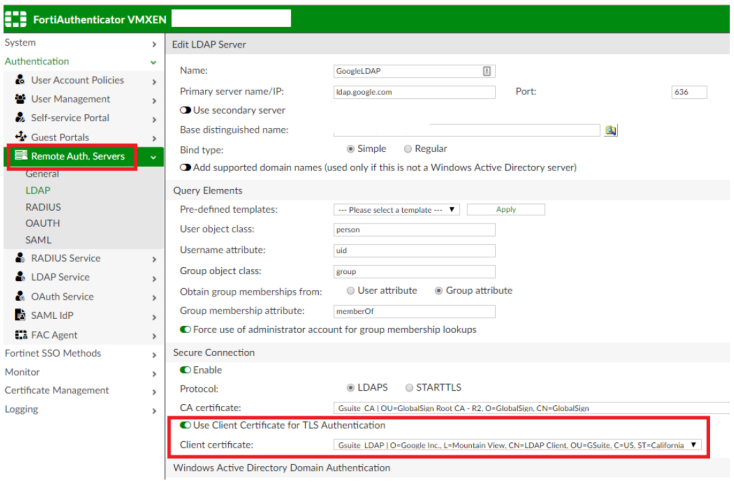
If required, you can now import users by clicking the **Go** button next to the **Import users** dropdown. This is not a required step, but can be done in cases where you want to include additional information to their accounts or assign FortiTokens.



Troubleshooting

Missing option to use client certificate for TLS authentication

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



Certificate error messages

The following is an example of an incorrect Trusted CA certificate entry. Please verify that you have followed the steps included in Generating the G Suite certificate on page 126.