RADIUS 2FA Interoperability Guide

FortiAuthenticator 6.5.0

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 13, 2023
FortiAuthenticator 6.5.0 RADIUS 2FA Interoperability Guide
23-650-779547-20230213

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-02-13	Initial release.

About this guide

The purpose of this guide is to aid in the configuration of two-factor authentication (2FA) using FortiAuthenticator for Fortinet solutions and other third party products.

Testing was performed with the following product versions:

- FortiAuthenticator 6.3.0
- FortiGate 7.0.0
- FortiManager 7.0.0
- FortiAnalyzer 7.0.0
- FortiWeb 6.4.0
- FortiMail 6.4.5

FortiAuthenticator setup

This section includes configuration information for the FortiAuthenticator. Any deviations from this configuration will be detailed in the relevant section. For more information on the setup and configuration of the FortiAuthenticator, see the Administration Guide.

This section includes the following information:

Initial setup

Upon initial deployment, the FortiAuthenticator is configured to the following default settings:

```
Port 1 IP: 192.168.1.99
Port 1 Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
```

These settings can be modified by configuring a PC to an address on the same subnet and accessing the GUI via https://192.168.1.99/. Alternatively, you can configure these settings using the CLI.

To configure basic settings using the CLI:

1. Connect the management computer to the FortiAuthenticator using the supplied console cable.
2. Log in to the FortiAuthenticator unit using the default credentials below:
   ```
   Username: admin
   Password: <blank>
   ```
   You will be prompted to change and confirm your new password.
3. Configure the network settings as required, for example:
   ```
   config system interface
      edit port1
         set ip <ip-address>/<netmask>
         set allowaccess https-gui https-api ssh
      next
   end
   config router static
      edit 0
         set device port1
         set dst 0.0.0.0/0
         set gateway <ip-gateway>
      next
   end
   ```
   Substitute your own desired FortiAuthenticator IP address and default gateway. This will give you access to the GUI through the specified IP address.

For more information on FortiAuthenticator initial setup, see the FortiAuthenticator Administration Guide in the Fortinet Document Library.

System settings

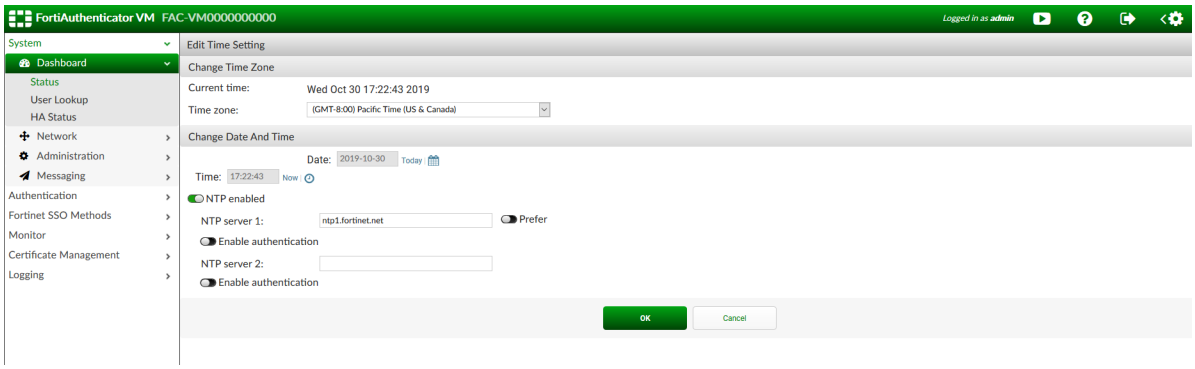
Once the initial setup of the FortiAuthenticator is complete, further configuration can be performed through the GUI.

DNS

To enable resolution of the FortiGuard network and other systems such as NTP servers, set your DNS to your local or ISP nameserver configuration via *Network* > *DNS*.

Time synchronization

FortiToken two-factor authentication uses a time-based algorithm to generate token PINs for use in the authentication process. It is essential that the time is accurate on the FortiAuthenticator system, therefore, NTP time synchronization is recommended. Change your settings to a local NTP server for accurate timing by going to *Dashboard* > *Status* and clicking the *Edit* button next to *System Time* in the *System Information* widget.



Creating a test user and token

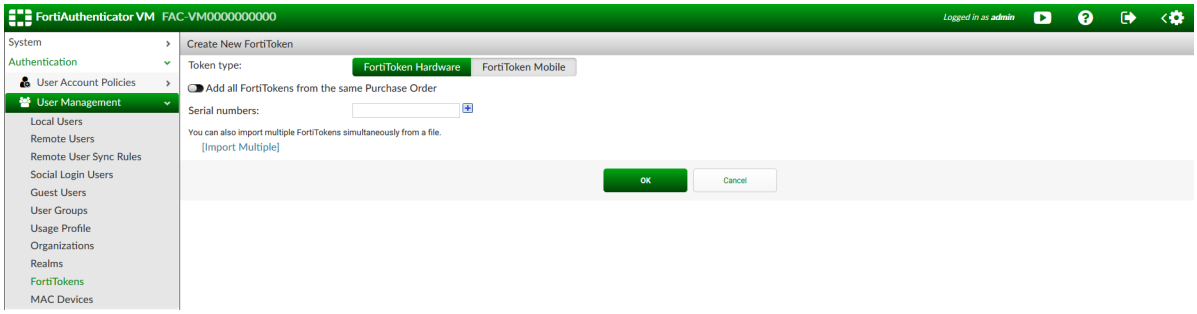
Registering FortiToken

In order to test two-factor authentication, a token is required. The configuration instructions included in this guide use FortiToken.

For security reasons, a token can only be automatically registered from the FortiGuard network a single time. If you need to register it a subsequent time, please contact Fortinet support.

To register a FortiToken:

1. Go to *Authentication* > *User Management* > *FortiTokens*, and select *Create New*.
2. Select the *Token type* and enter the FortiToken *Serial number* or *Activation code*. Click *OK*.
   Once registered, tokens will be displayed with an *Available* status.

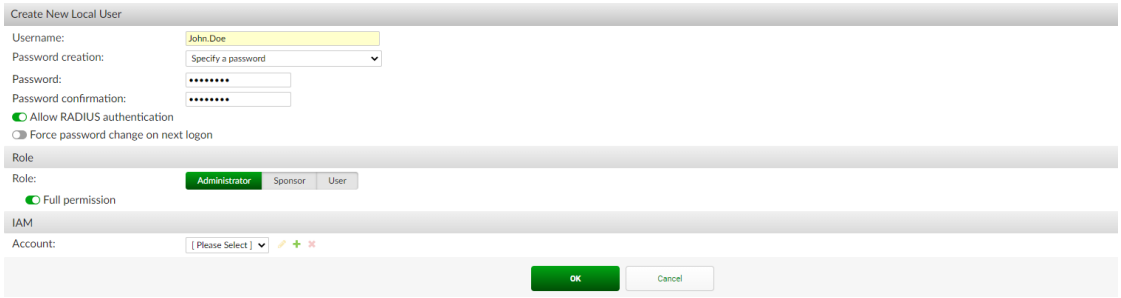


Creating a test user

Create a single test user with RADIUS authentication and FortiToken two-factor authentication enabled.

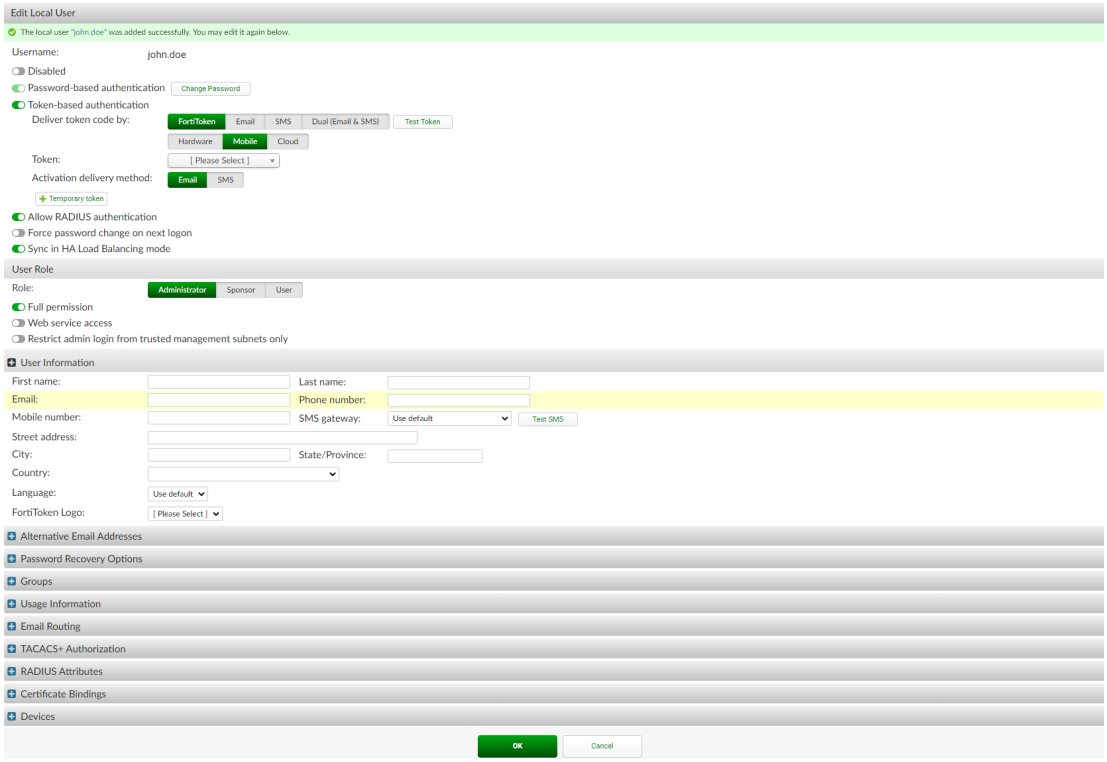
To create the user:

1. Go to *Authentication* > *User Management* > *Local Users*, and click *Create New*.
2. Enter a username and password for the local user.
   The configuration instructions included in this guide use the username *John.Doe*.
3. Enable *Allow RADIUS authentication*, and click *OK* to access additional settings.



4. Enable *Token-based authentication* and choose *Deliver the token code by FortiToken*.
   Select the FortiToken added earlier from the relevant dropdown menu.
5. Set the *Delivery method* to *Email*. This will automatically open the *User Information* section where you can enter the user email address in the field provided.

6. Click *OK* to save changes to the local user.



Configuring RADIUS settings

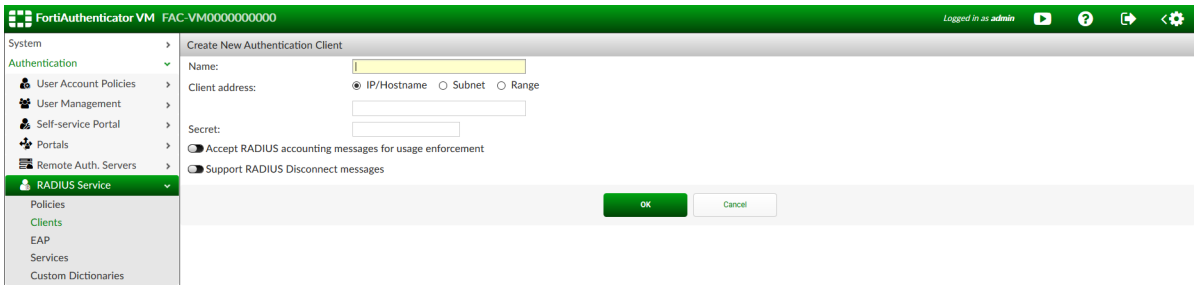
Before any device can connect to the FortiAuthenticator, it must be configured as a RADIUS client and assigned to a RADIUS policy. Until this is done, FortiAuthenticator will ignore authentication requests. You must repeat this process for each device that you wish to authenticate against the FortiAuthenticator.

Adding the RADIUS client

To configure the RADIUS client:

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

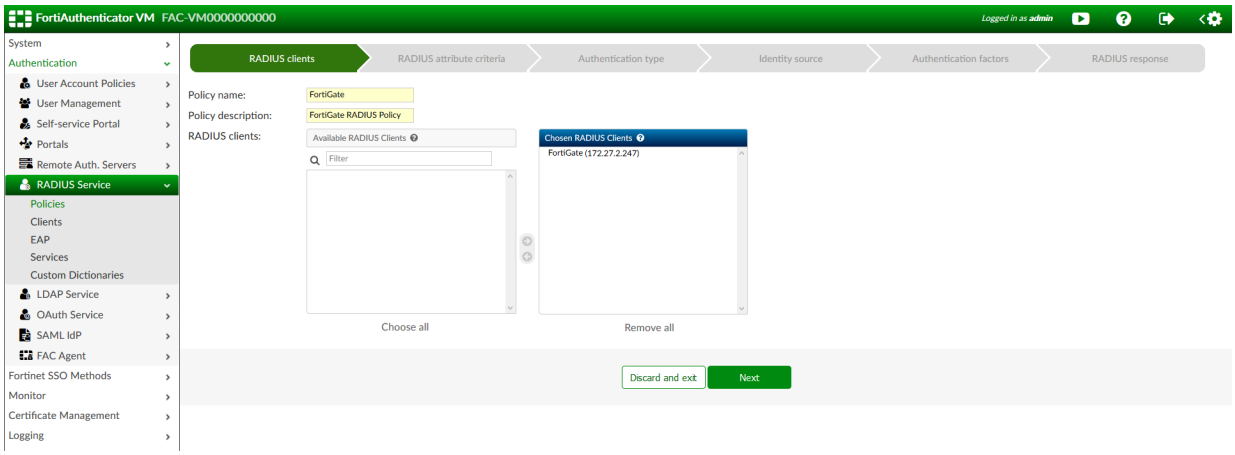
4. Click *OK* to save changes to the RADIUS client.



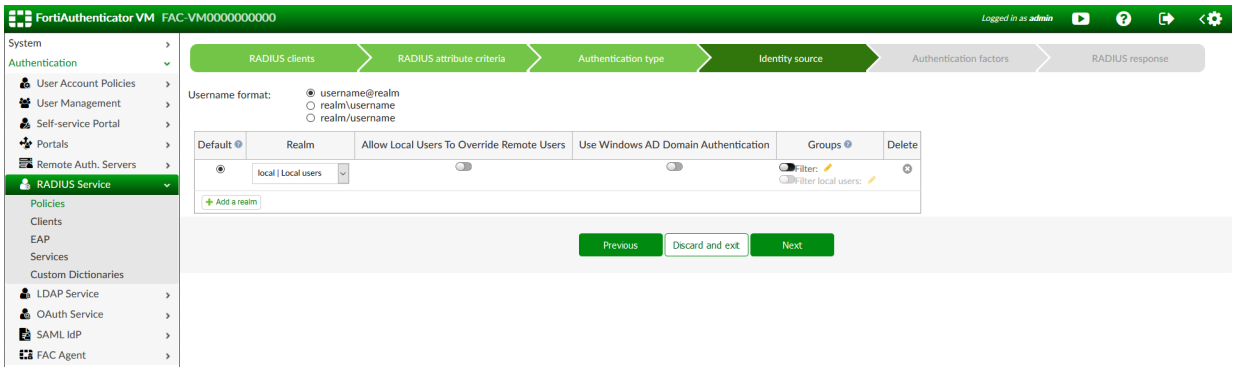
Creating the RADIUS policy

To create the RADIUS policy:

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



3. For *RADIUS attribute criteria,* no settings are required. Click *Next*.
4. For *Authentication type*, select *Password/OTP authentication*, and click *Next*.
5. For *Identity source*, choose a username format, and select the *local* realm. Click *Next*.



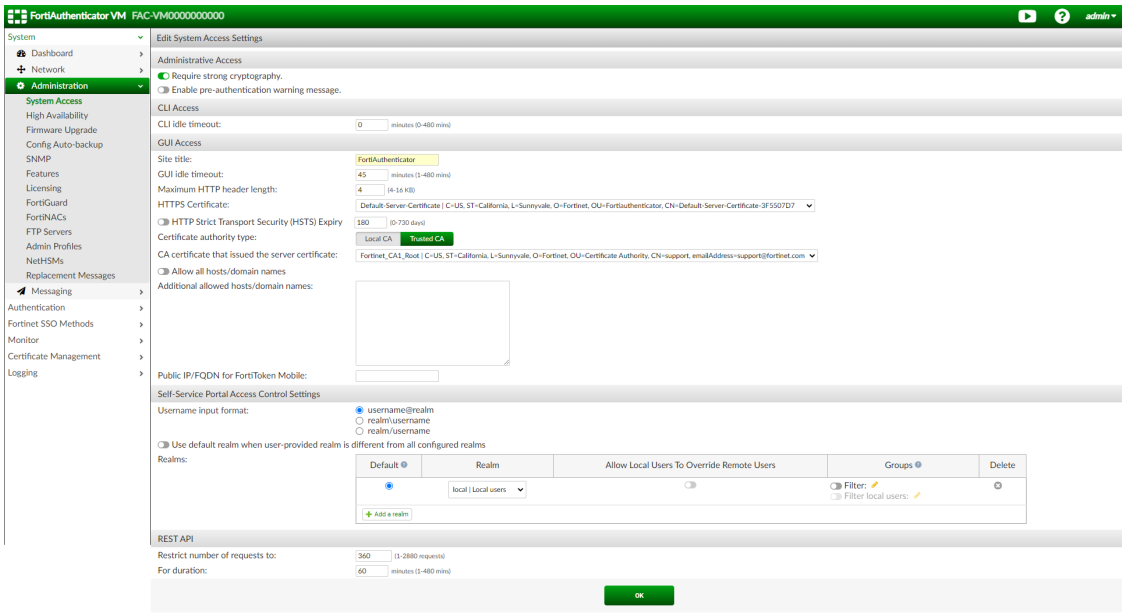
6. For *Authentication factors*, select *Every configured password and OTP factors*, and click *Next*.
   In this menu you can also enable the option to *Allow FortiToken Mobile push notifications*.
7. For *RADIUS response*, review the policy, and click *Save and exit*.

Optional: Enabling FortiToken Mobile push notifications

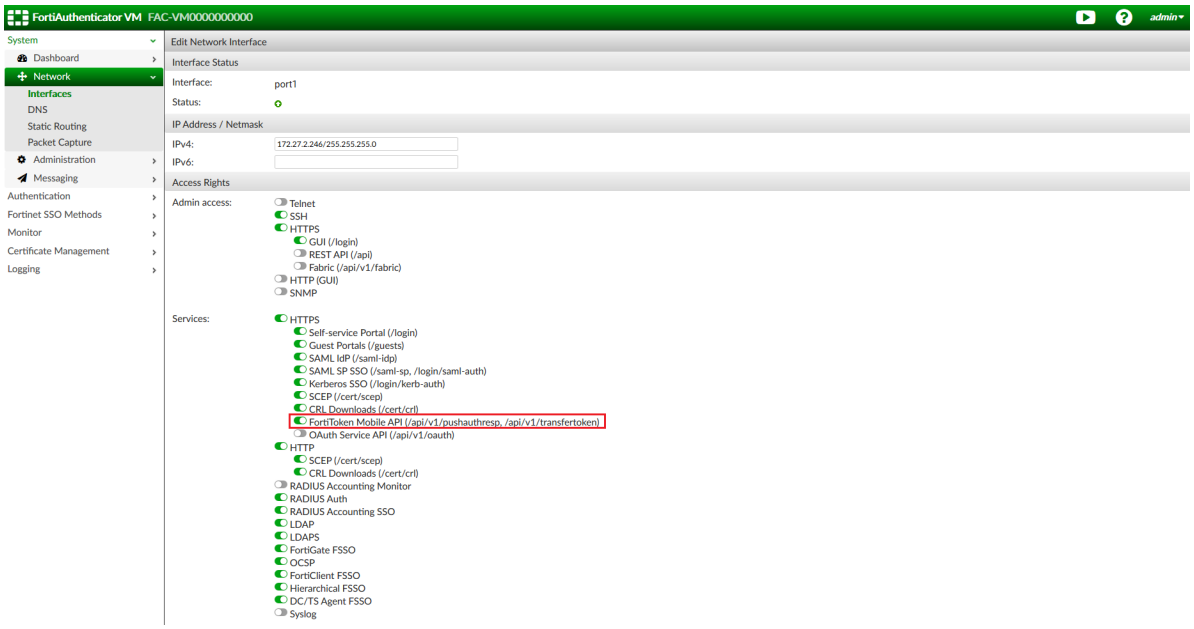
When push notifications are enabled, users can accept or deny authentication requests directly from a notification on their device.

To configure FTM push on FortiAuthenticator:

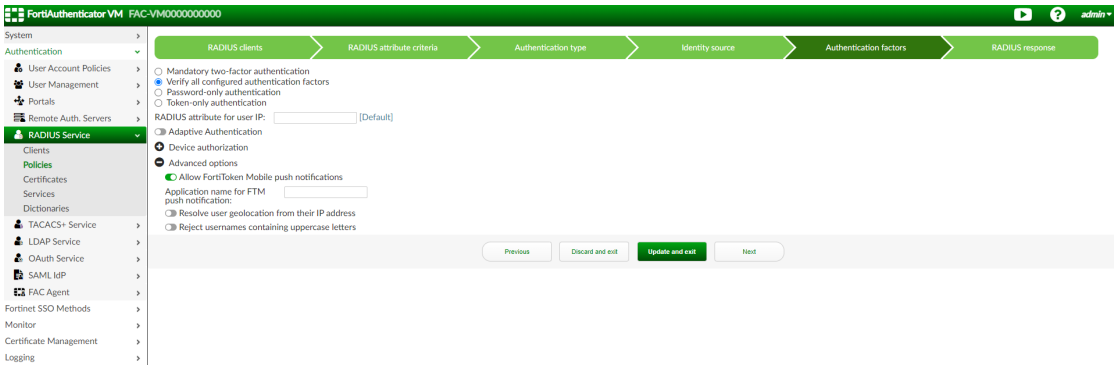
1. Before push notifications can be enabled, a *Public IP/FQDN for FortiToken Mobile* must be configured in *System > Administration > System Access*.
   If the FortiAuthenticator is behind a firewall, the public IP/FQDN will be an IP/port forwarding rule directed to one of the FortiAuthenticator interfaces.



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



2. Once configured, FTM push notifications can be enabled for clients through the RADIUS policy in the *Authentication factors* > *Advanced options* setting.



FortiGate

Before proceeding, ensure that you have configured the RADIUS client and policy on FortiAuthenticator. See System settings on page 8.

The FortiGate appliance is the Gateway to your network, therefore, securing remote access, whether to the appliance itself (administration) or the network behind it (VPN), is critical.

FortiOS supports native two factor authentication using FortiToken, however, to use two-factor authentication on multiple FortiGate devices, you should use a FortiAuthenticator to enable strong authentication.

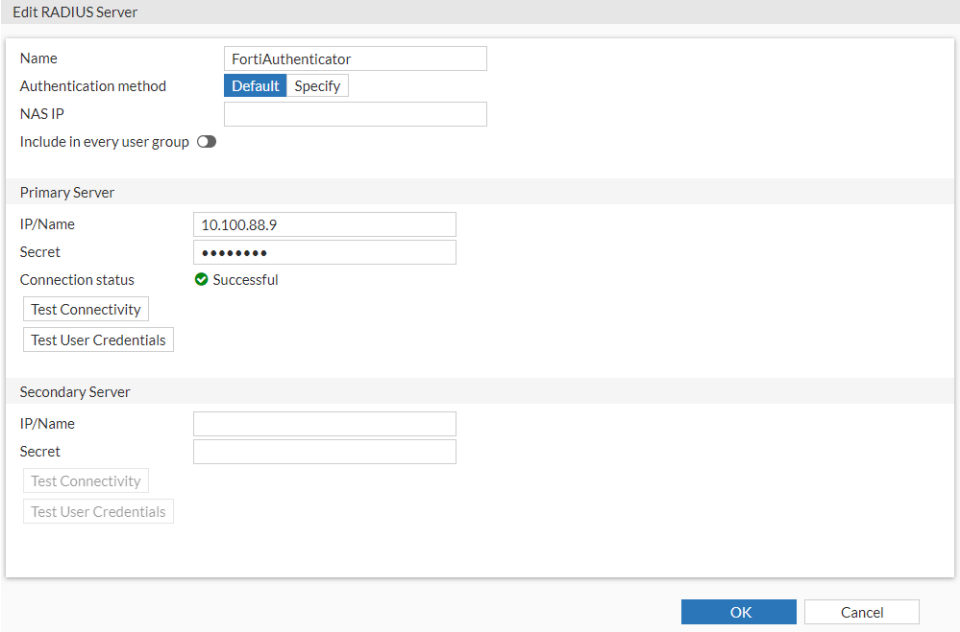
To configure two-factor authentication using FortiAuthenticator:

1. Configure FortiAuthenticator local users, RADIUS client, and RADIUS policy:
   - Creating a test user and token on page 8
   - Configuring RADIUS settings on page 10
2. Configure the RADIUS server on your FortiGate:
   - Configuring the RADIUS server on page 14
3. Set up authentication using one or more of the following configurations:
   - Configuring authentication for administrators on page 15
   - Configuring authentication for SSL-VPN users on page 19
4. Optional: Configure timeout settings on the FortiGate when using FortiToken Mobile push.
   - Configuring FortiToken Mobile push on FortiGate on page 20
5. Optional: Validate the configuration.
   - Verifying logs on page 21

Configuring the RADIUS server

To configure the FortiGate authentication settings:

1. Go to *User & Authentication* > *RADIUS Servers*, and click *Create New*.
2. Configure the details of the FortiAuthenticator.
3. Enter the shared *Secret* key, and click *OK*.



4. Click *Test Connectivity* to test the connection to the server, and ensure that *Connection status* is *Successful*.
5. Optionally, click *Test User Credentials* to test user credentials and validate the group name returned for this user.

To configure the RADIUS server from the CLI:

```
config user radius
   edit "FortiAuthenticator"
      set server "10.100.88.9"
      set secret mysecret
   next
end
```

Configuring authentication for administrators

To configure authentication for administrators with RADIUS 2FA from FortiAuthenticator, you will first need to create a user group and administrator profile on the FortiGate. The administrator profile should match a user account on the FortiAuthenticator.

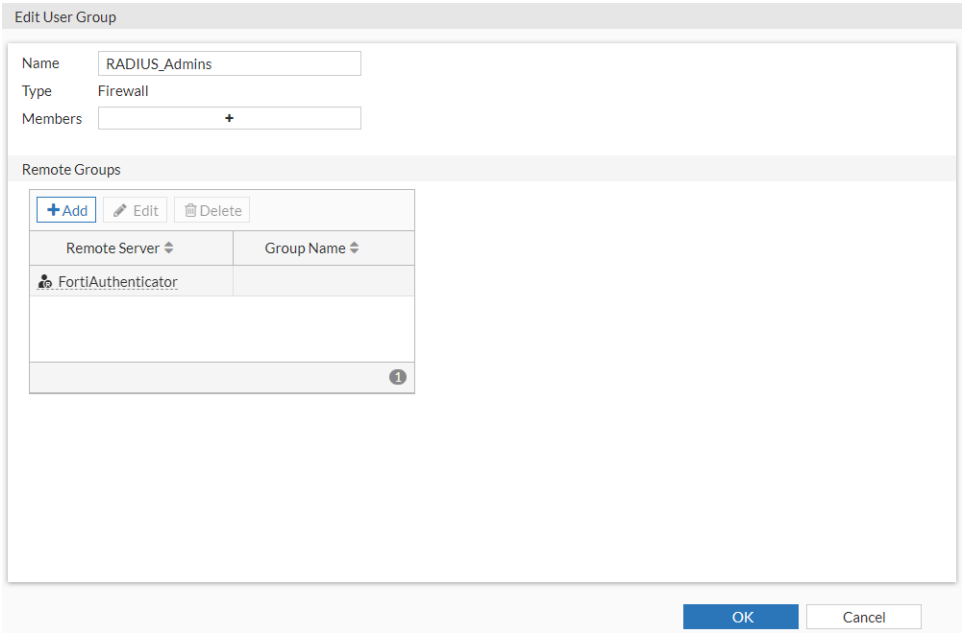
Creating user groups

To create a user group:

1. Go to *User & Authentication* > *User Groups*, and select *Create New*.
2. Enter a name for the user group, for example *RADIUS_Admins*.
3. Select *Firewall* as the type.
4. Under *Remote Groups*, click *Add*, and select the FortiAuthenticator RADIUS server from the dropdown list. Click

OK.

Do not add any local users to this policy in *Members* as this will cause RADIUS authentication to fail.



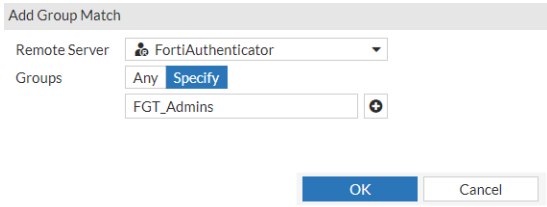
FortiAuthenticator also supports sending group membership as an AVP. For example, when users configured in the FortiAuthenticator group *FGT_Admins* authenticate, the AVP *Fortinet-Group-Name=FGT_Admins* will be sent in the *Authentication-Accept* packet. This can be used to authorize the user onto the FortiGate by allowing only members of that group.

To create a user group from the CLI:

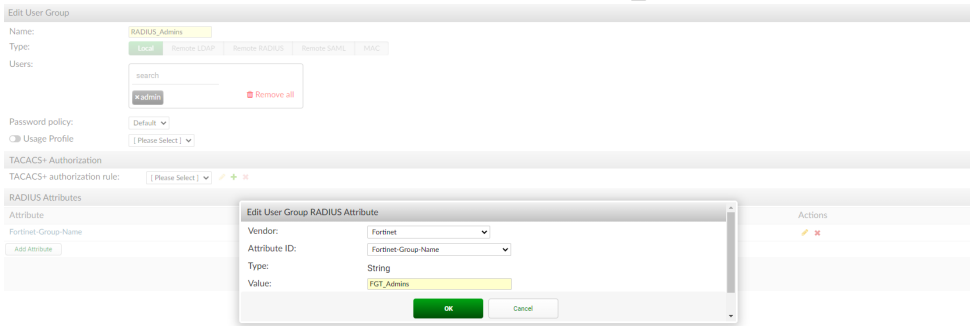
```
config user group
   edit "RADIUS_Admins"
      set member "FortiAuthenticator"
      config match
         edit 1
            set server-name "FortiAuthenticator"
            set group-name "RADIUS_Admins"
         next
      end
   next
end
```

To specify group membership:

1. In the FortiGate user group:
   a. Double-click on the FortiAuthenticator *Remote Group*.
   b. Select *Specify*, and enter a RADIUS attribute group name (example: `FGT_Admins`).



2. On FortiAuthenticator, go to *Authentication* > *User Management* > *User Groups*.
3. Create or edit a *Local* user group, and add the administrator(s).
4. Click *Add Attribute* to add a RADIUS AVP with the following details:
   a. Vendor: *Fortinet*
   b. Attribute ID: *Fortinet-Group-Name*
   c. Value: The RADIUS attribute group name (example: `FGT_Admins`).



RADIUS attributes can also be added directly to user profiles by going to *Authentication* > *User Management* > *Local Users*, selecting a user, and clicking *Add Attributes* in the *RADIUS Attributes* menu.

For administrator and sponsor user roles, the *RADIUS Attributes* field is available only when **Sync in HA Load Balancing mode** is enabled in *Authentication* > *User Management* > *Local Users*.

Creating administrators

To create a RADIUS administrator with 2FA:

1. In *System* > *Administrators*, click *Create New* and select *Administrator* from the dropdown.
2. In the *New Administrator* page, enter the following, then click *OK*.
   a. Username: Enter the administrator's username (example: `john.doe`).
   b. Type: *Match a user on a remote server group.*
   c. Backup Password: Enter a backup password which can be used in the event that the RADIUS authentication is unavailable.

d. Administration Profile: *super_admin.*

e. Remote User Group: Select the previously created RADIUS user group (example: *RADIUS_Admins*).

Do not select two-factor authentication at this point. The two factor authentication is performed external to the FortiGate.

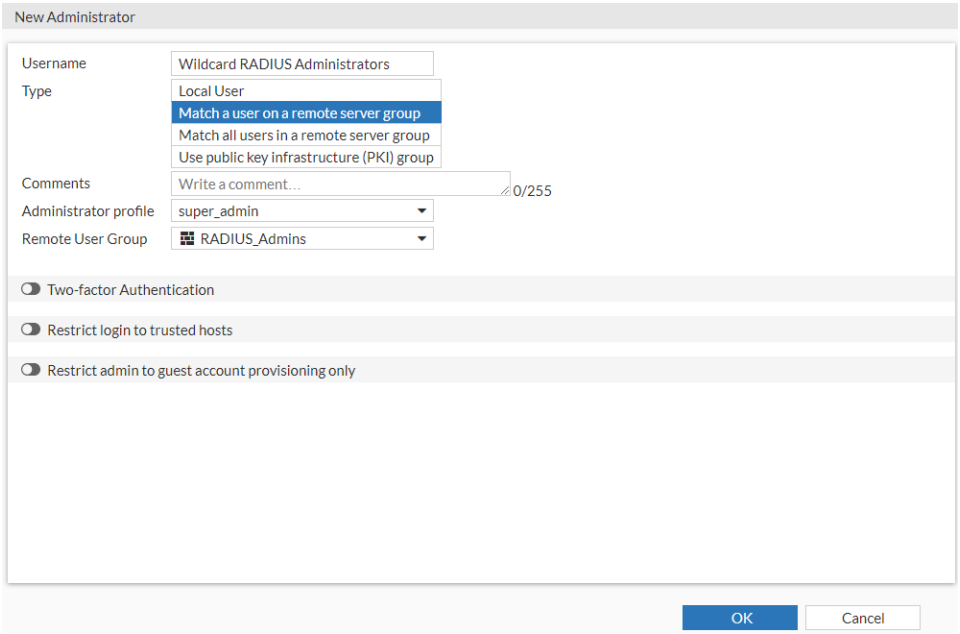
Creating a wildcard administrator account

Wildcard accounts can also be used in order to avoid specifying each user locally. When this option is enabled, any user included in the remote user group will be able to authenticate as an administrator on the FortiGate.

In order for wildcard authentication to function, the selected remote user group must correspond with a user group on the FortiAuthenticator. User groups can be created in the FortiAuthenticator GUI by going to *Authentication* > *User Management* > *User Groups*.

To create a wildcard administrator account:

1. In *System* > *Administrators*, click *Create New* and select *Administrator* from the dropdown.
2. Create a new administrator with a descriptive name.
   The name is for internal purposes only and is not used during authentication.
3. Select *Match all users in a remote server group* as the administrator Type.
4. Choose the Remote User Group previously created.
5. Select an Administrator Profile, and click OK.



Once you have created the user group and administrator, log into the FortiGate GUI with the newly created RADIUS administrator credentials.

After you have entered your username and password, you will be prompted to add the two-factor authentication PIN from FortiToken. Successful authentication will provide the user with access to the FortiGate, and will generate a login event on the FortiAuthenticator.

To create an administrator from the CLI:

```
config system admin
   edit "Wildcard RADIUS Administrators"
      set remote-auth enable
      set accprofile "super_admin"
      set wildcard enable
      set remote-group "RADIUS_Admins"
   next
end
```

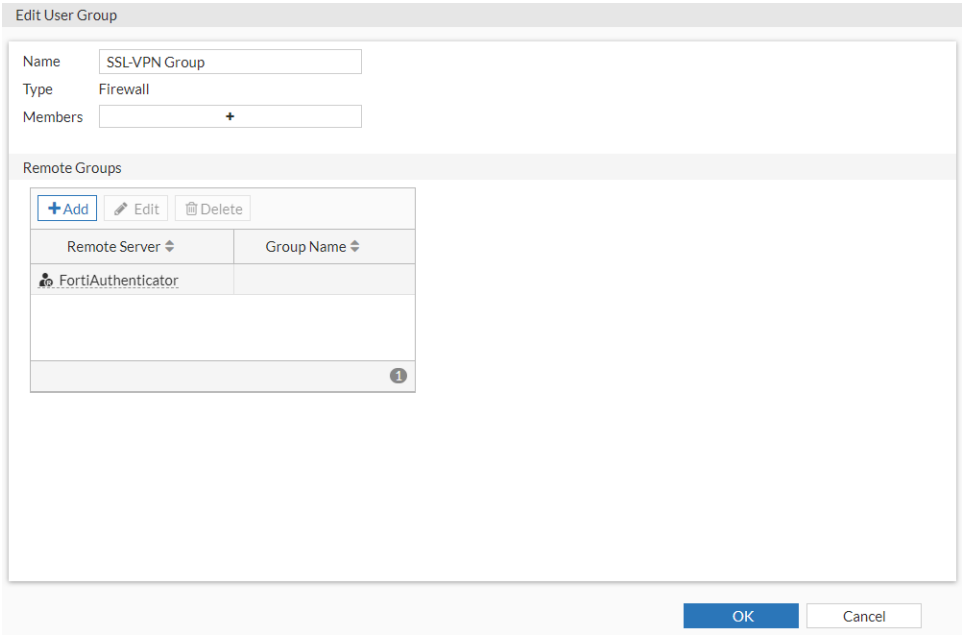
Configuring authentication for SSL-VPN users

The process described in this guide is for enabling secure authentication through FortiAuthenticator. It does not include full configuration instructions for enabling SSL-VPN. For more information on configuring SSL-VPN, please see the FortiGate Cookbook on the Fortinet Documentation Library.

In order to set up authentication for SSL-VPN users, you must first create a new user group.

To create a user group:

1. Go to *User & Authentication* > *User Groups*, and select *Create New*.
2. Enter a name for the user group, for example: *SSL-VPN Group*.
3. Select *Firewall* as the type.
4. Under *Remote Groups*, click *Add*, and select the FortiAuthenticator RADIUS server from the dropdown menu. Click *OK*.



You can now create a firewall policy which enables SSL-VPN access into your chosen network.

To configure the SSL-VPN settings:

1. Configure the SSL VPN web portal.
   a. Go to *VPN* > *SSL-VPN Portals* to edit the full-access portal.
   b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
2. Configure the SSL VPN settings.
   a. Go to *VPN* > *SSL-VPN Settings*.
   b. Select the *Listen on Interface(s)*.
   c. *Set Listen on Port* to `10443`.
   d. Set *Service Certificate* to the authentication certificate.
   e. Under *Authentication/Portal Mapping*, select the full-access portal for the SSL-VPN group, and choose a portal for *All Other Users/Groups*.
3. Configure the SSL VPN Firewall policy.
   a. Go to *Policy & Objects* > *Firewall Policy*, select IPv4 from the dropdown on the right, and select *Create New*.
   b. Fill in the firewall policy name.
   c. Set the *Incoming Interface* to the *SSL-VPN tunnel interface(ssl.root)*.
   d. Set the *Source* to *all* and *Source User* to the *SSL-VPN group*.
   e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network.
   f. Set the *Destination* to the internal protected subnet.
   g. Set the *Schedule* to *always*, *Service* to *ALL*, and *Action* to *ACCEPT*.
   h. Enable *NAT*.
   i. Configure any remaining firewall and security options as desired.
   j. Click *OK*.

Open a new browser and navigate to the SSL VPN web portal identified when you set up the SSL-VPN settings (example: `172.27.2.247:10443`). Enter a valid username and password, and select *Login*, and you will be prompted to enter a FortiToken PIN. Once entered, you will have access to the SSL VPN tunnel.

Configuring FortiToken Mobile push on FortiGate

By default, the RADIUS servers on FortiGate are configured with a short timeout (5 seconds), which is not long enough when using FTM push. The timeout must be long enough to allow for:

1. Sending the notification.
2. The end-user to pick up their mobile device and navigate to the FTM app.
3. The end-user to decide whether to approve or deny the request.

The FortiGate also has a short global authentication timeout (5 seconds). When larger than the RADIUS server timeout, it allows for one or more retries before the FortiGate gives up. This timeout must be at least as long as the RADIUS server timeout.

Both settings can only be configured using the CLI.

To configure the RADIUS server timeout:

```
config user radius
   edit <RADIUS server name>
```

```
     set timeout <value, e.g. 30>
end
```

To configure the global authentication timeout:

```
config system global
   set remoteauthtimeout <value, e.g. 60>
end
```

For FortiGate SSL-VPN configurations using 2FA, depending on the version of FOS, the push notification is either automatically triggered after first factor is validated, or when the end user submits the string `push` in the VPN client.

For instructions on enabling FortiToken Mobile push notifications on FortiAuthenticator, see: Optional: Enabling FortiToken Mobile push notifications on page 12.

Verifying logs

You can use the *Logging* menu tree in FortiAuthenticator to validate the two-factor authentication configuration that you have set up.

To verify the two-factor authentication configuration:

1. Log in as the remote admin.
2. Go to *Logging* > *Log Access* > *Logs*.
3. From the log list, select the authentication log whose details you need to view by clicking anywhere within the log's row.
   The *Log Details* pane will open on the right side of the window.
4. After viewing the log details, select the close icon in the top right corner of the pane to close the *Log Details* pane.

FortiManager

Before proceeding, ensure that you have configured the RADIUS client and policy on FortiAuthenticator. See System settings on page 8.

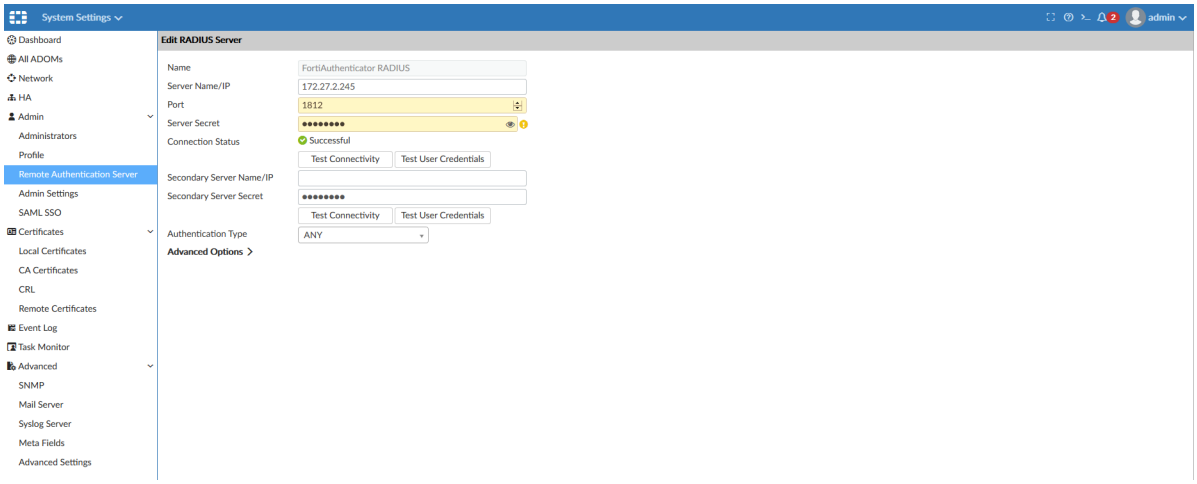
To configure two-factor authentication using FortiAuthenticator:

1. Configuring the RADIUS server on page 22
2. Creating an admin user on page 22

Configuring the RADIUS server

To configure the RADIUS server:

1. In FortiManager, go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Click *Create New*, and choose *RADIUS Server* from the dropdown menu.
3. Enter the details of the remote FortiAuthenticator, including the *Shared Secret*, and click *OK*.

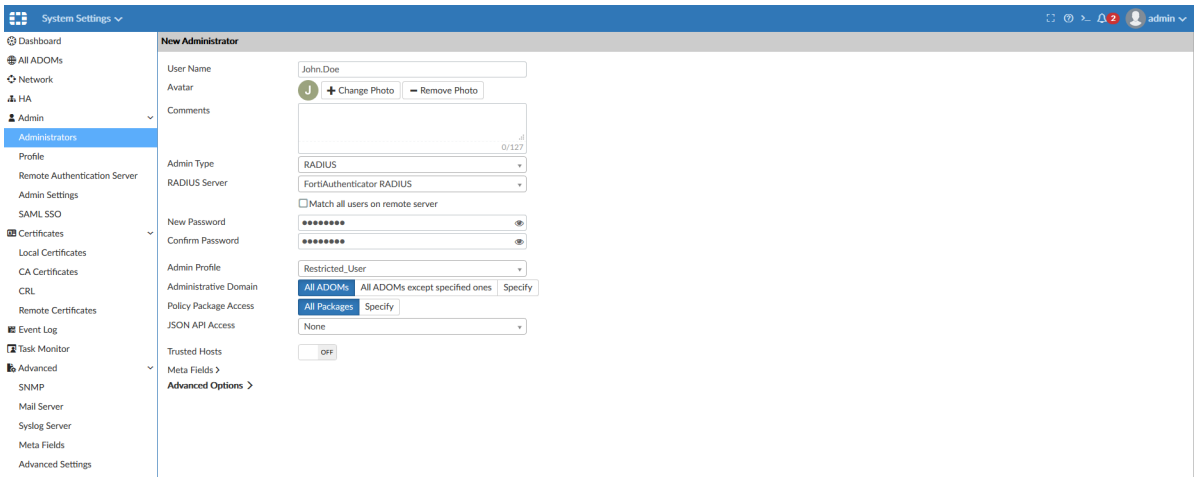


Creating an admin user

To create a RADIUS administrator with 2FA:

1. In FortiManager, go to *System Settings* > *Admin* > *Administrators*, and click *Create New*.
2. Enter a user name for the administrator.
3. Choose *RADIUS* as the *Admin Type*, and select the *RADIUS Server* created in the previous step.

4. Enter and confirm the administrator's password, and click *OK*.



Once completed, log into the FortiManager GUI with the newly created RADIUS administrator credentials.

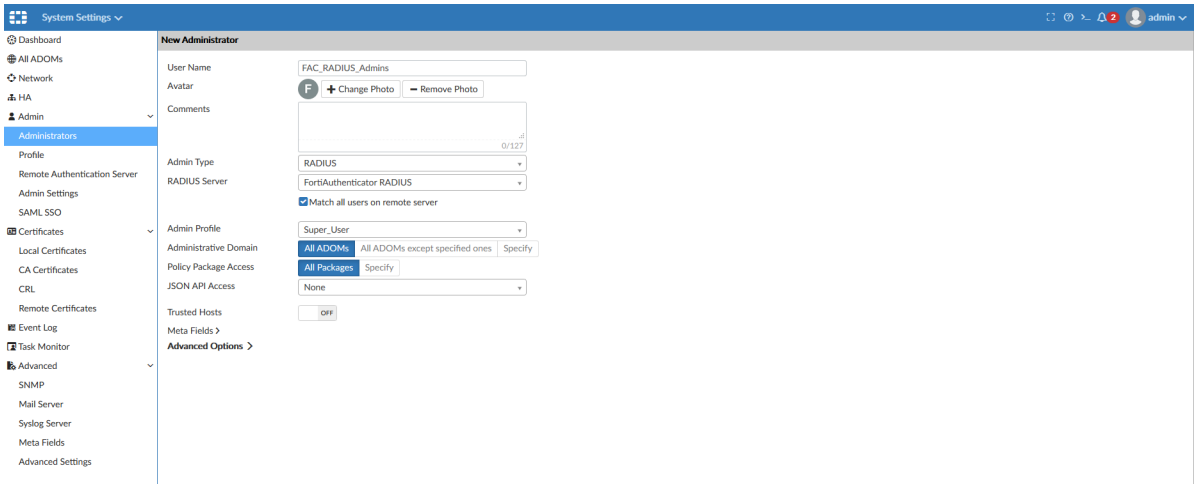
After you have entered your username and password, you will be prompted to add the two-factor authentication PIN from FortiToken. Successful authentication will provide the user with access to the FortiManager, and will generate a login event on the FortiAuthenticator.

Creating a wildcard administrator account

Wildcard accounts can also be used in order to avoid specifying each user locally. When this option is enabled, users included on the RADIUS server will be able to authenticate as an administrator on the FortiManager.

To create a wildcard administrator account:

1. Create a new administrator profile with a descriptive name.
   The name is for internal purposes only and is not used during authentication.
2. Select *Match all users in a remote server group* as the administrator *Admin Type*.
3. Choose the *RADIUS Server* previously created.
4. Select an *Admin Profile*, and click *OK*.



FortiAnalyzer

Before proceeding, ensure that you have configured the RADIUS client and policy on FortiAuthenticator. See System settings on page 8.

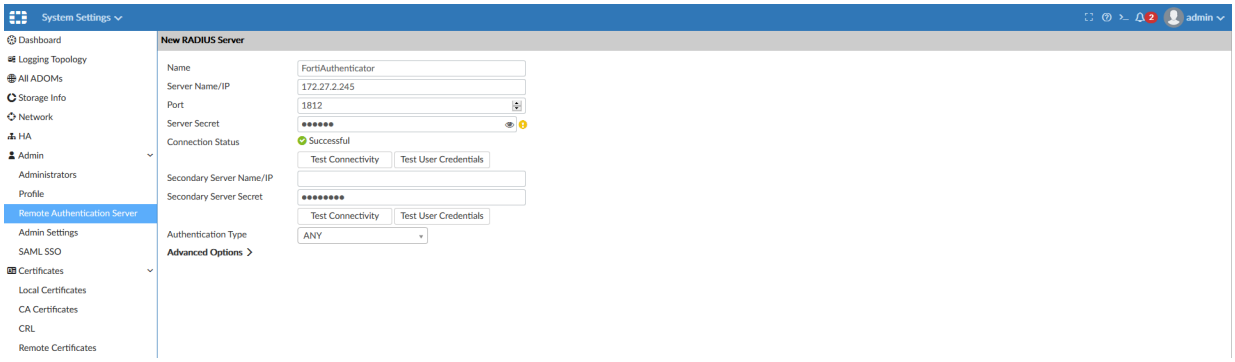
To configure two-factor authentication using FortiAuthenticator:

1. Configuring the RADIUS server on page 24
2. Creating an admin user on page 24

Configuring the RADIUS server

To configure the RADIUS server:

1. In FortiAnalyzer, go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Click *Create New*, and choose *RADIUS Server* from the dropdown menu.
3. Enter the details of the remote FortiAuthenticator, including the *Shared Secret*, and click *OK*.

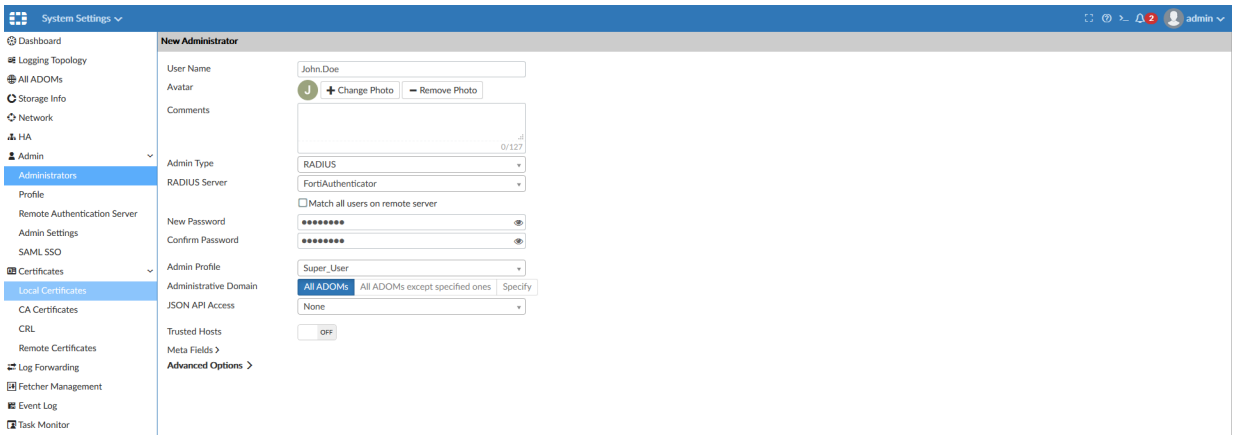


Creating an admin user

To create a RADIUS administrator with 2FA:

1. In FortiAnalyzer, go to *System Settings* > *Admin* > *Administrators*, and click *Create New*.
2. Enter a user name for the administrator.
3. Choose *RADIUS* as the *Admin Type*, and select the *RADIUS Server* created in the previous step.

4. Enter and confirm the administrator's password, and click *OK*.



Once completed, log into the FortiAnalyzer GUI with the newly created RADIUS administrator credentials.

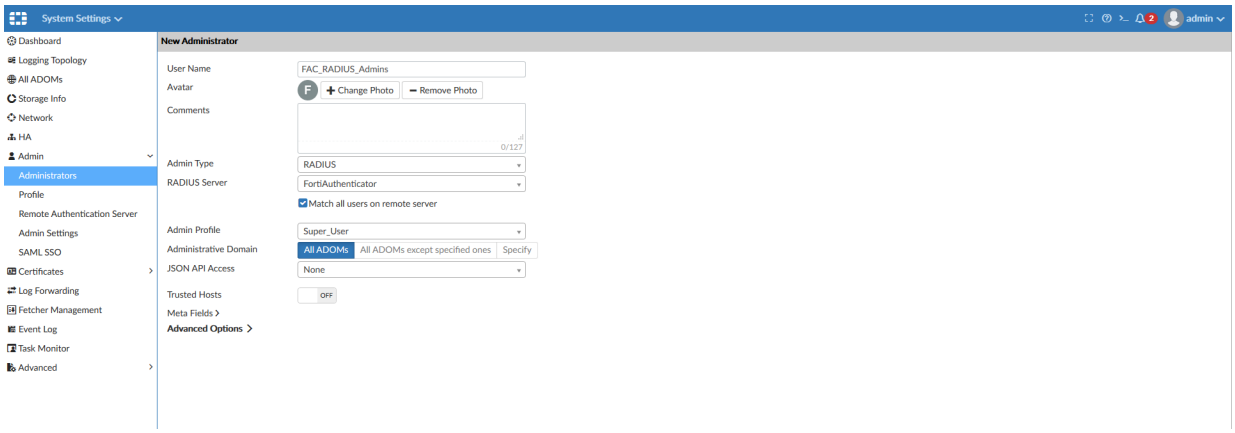
After you have entered your username and password, you will be prompted to add the two-factor authentication PIN from FortiToken. Successful authentication will provide the user with access to the FortiAnalyzer, and will generate a login event on the FortiAuthenticator.

Creating a wildcard administrator account

Wildcard accounts can also be used in order to avoid specifying each user locally. When this option is enabled, users included on the RADIUS server will be able to authenticate as an administrator on the FortiAnalyzer.

To create a wildcard administrator account:

1. Create a new administrator profile with a descriptive name.
   The name is for internal purposes only and is not used during authentication.
2. Select *Match all users in a remote server group* as the administrator *Admin Type*.
3. Choose the *RADIUS Server* previously created.
4. Select an *Admin Profile*, and click *OK*.



FortiWeb

Before proceeding, ensure that you have configured the RADIUS client and policy on FortiAuthenticator. See System settings on page 8.

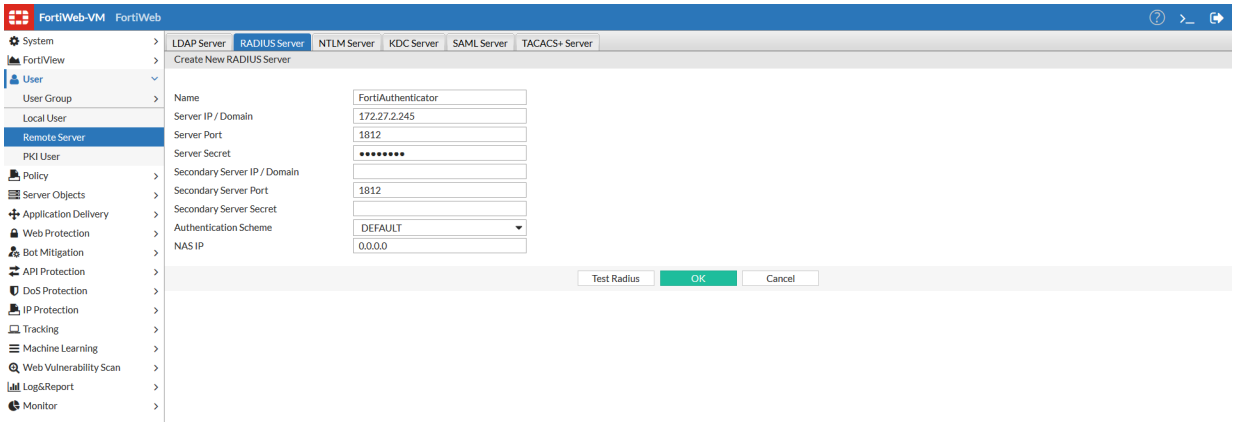
To configure two-factor authentication using FortiAuthenticator:

1. Configuring the RADIUS server on page 26
2. Creating an admin group on page 26
3. Creating an admin user on page 27

Configuring the RADIUS server

To configure the RADIUS server:

1. In FortiWeb, go to *User* > *Remote Server*, select the *RADIUS Server* tab, and click *Create New*.
2. Enter the details of the remote FortiAuthenticator, including the shared *Server Secret*.
3. Select *OK* to create the RADIUS server.

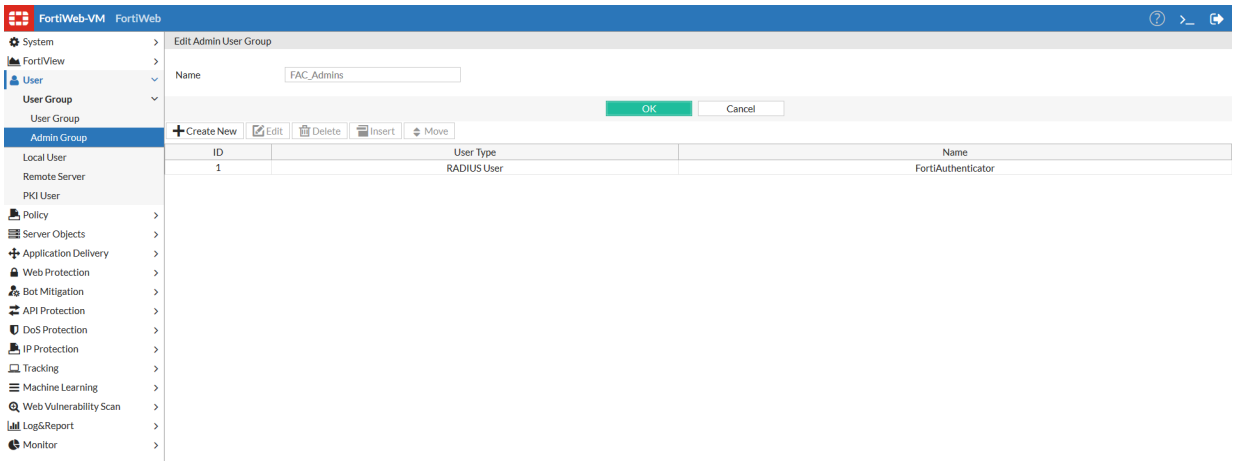


Creating an admin group

To create an admin group with RADIUS authentication:

1. In FortiWeb, go to *User* > *User Group* > *Admin Group*, select *Create New*.
2. Enter a name for the admin group, and click *OK*.
3. Click *Create New*, choose *RADIUS User* as the *User Type*, and select the FortiAuthenticator RADIUS server

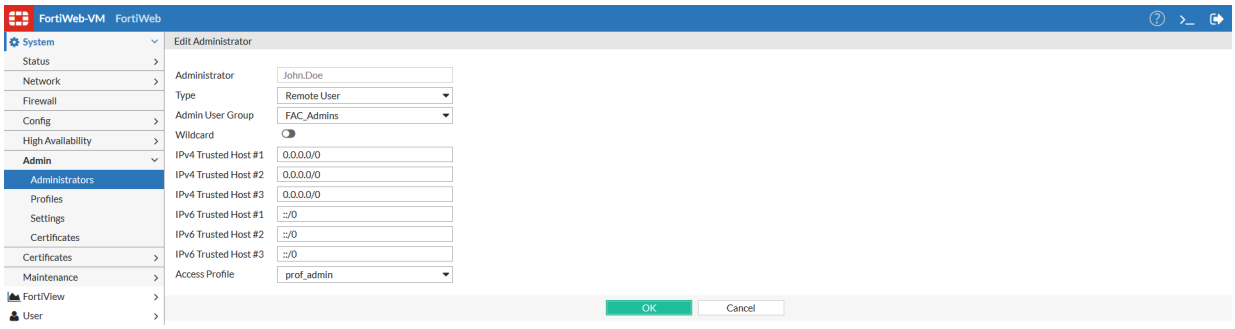
created in the previous step.



Creating an admin user

To create a RADIUS administrator with 2FA:

1. In FortiWeb, go to *System* > *Admin* > *Administrators*, and from the *Create New* dropdown select *Administrator*.
2. Enter a username and password for the administrator.
3. Select *Remote User* as the *Type*.
4. Choose the previously created *Admin User Group*.
5. Select the *Access Profile* for the administrator, and click *OK*.



Once completed, log into the FortiWeb GUI with the newly created RADIUS administrator credentials. Enter the token when prompted.

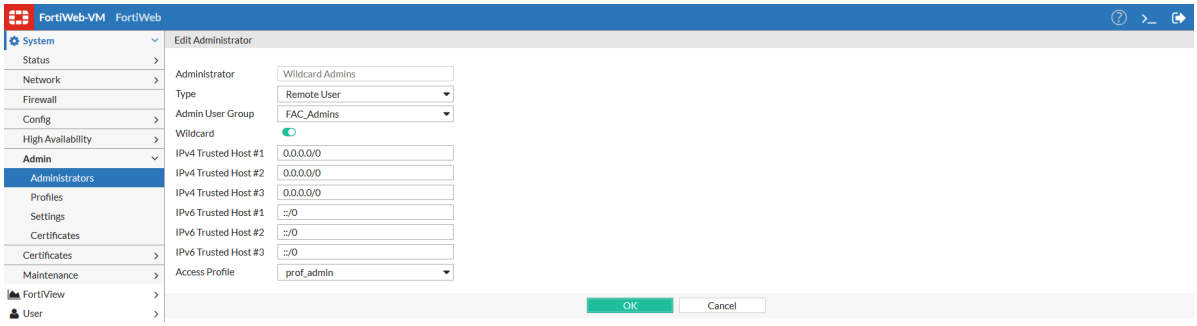
Successful authentication will provide the user with access to the FortiWeb, and will generate a login event on the FortiAuthenticator.

Creating a wildcard administrator account

Wildcard accounts can also be used in order to avoid specifying each user locally. When this option is enabled, any user included on the RADIUS server associated with the selected Admin User Group will be able to authenticate as an administrator on the FortiWeb.

To create a wildcard administrator account:

1. Create a new administrator profile with a descriptive name.
   The name is for internal purposes only and is not used during authentication.
2. Choose *Remote User* as the Type, and enable *Wildcard*.
3. Choose the RADIUS *Admin User Group* previously created.
4. Select an *Access Profile*, and click *OK*.



FortiMail

Before proceeding, ensure that you have configured the RADIUS client and policy on FortiAuthenticator. See System settings on page 8.

To configure two-factor authentication using FortiAuthenticator:

1. Configuring the RADIUS server on page 29
2. Creating an admin user on page 30

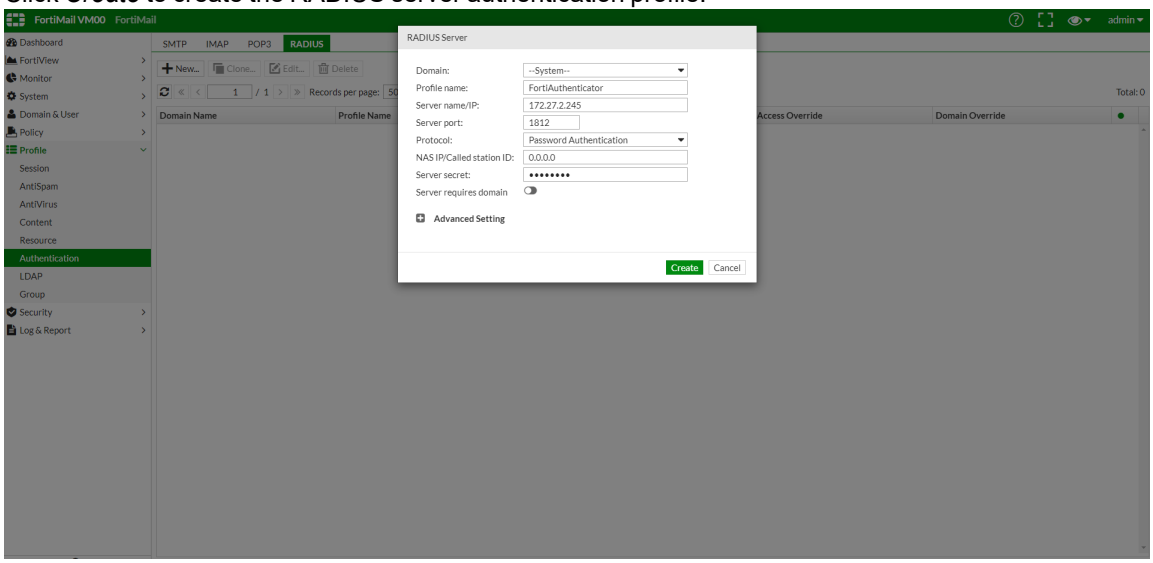
Configuring the RADIUS server

To configure the RADIUS server:

1. In FortiMail, go to *Profile* > *Authentication*, select the *RADIUS* tab, and click *New*.
2. Enter the details of the remote FortiAuthenticator:
   - In the *Profile name* field, enter a profile name.
   - In the *Server name/IP* field, enter the fully qualified name (FQDN) or IP address of a server that will be queried to authenticate email users if they authenticate to send email, or when they are accessing their personal quarantine.
   - In the *Server port* field, enter the port number on which the authentication server listens. For a RADIUS server, the port number is `1812`.
   - In the *Protocol* dropdown, select an authentication scheme. Here, *Password Authentication* is selected.
   - In the *Server secret* field, enter the secret required by the RADIUS server.

The secret is identical to the secret configured on the RADIUS server. Here, FortiAuthenticator.

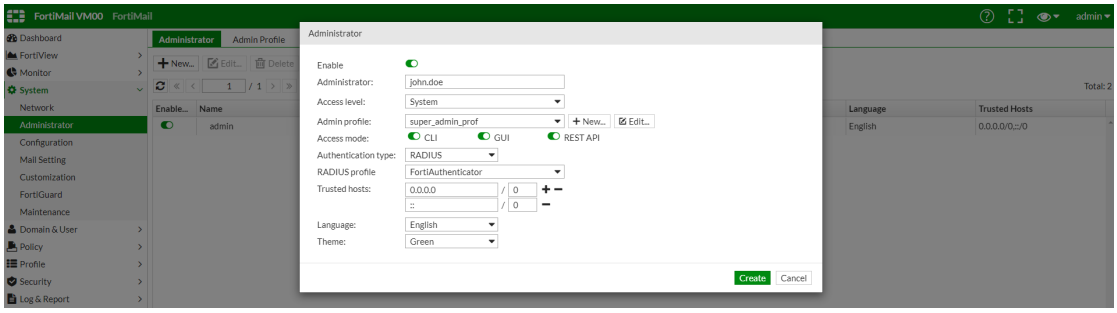
3. Click *Create* to create the RADIUS server authentication profile.



Creating an admin user

To create a RADIUS administrator with 2FA:

1. In FortiMail, go to *System* > *Administrator*, and click *New*.
2. Choose an *Admin profile*.
3. Select *RADIUS* as the *Authentication type*.
4. Select the *RADIUS profile* created in the previous step, and click *Create*.



Once completed, log into the FortiMail GUI with the newly created RADIUS administrator credentials.

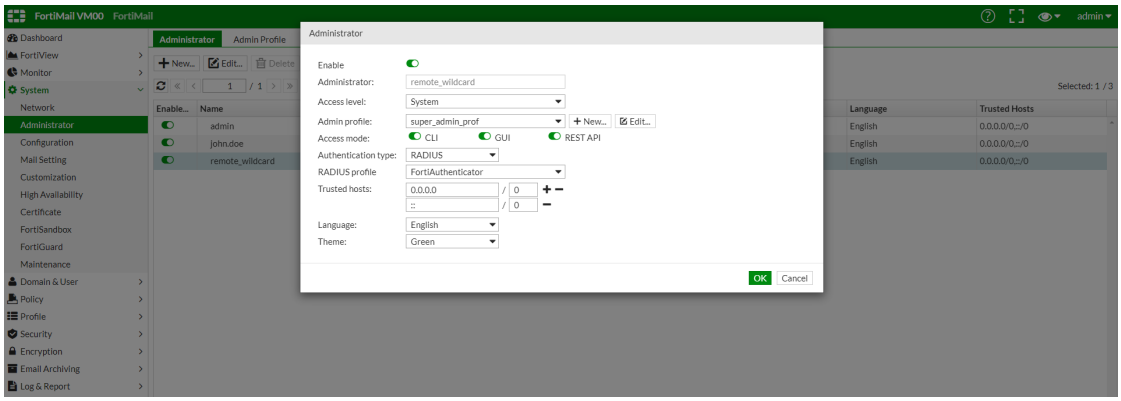
After you have entered your username and password, you will be prompted to add the two-factor authentication PIN from FortiToken. Successful authentication will provide the user with access to the FortiMail admin GUI, and will generate a login event on the FortiAuthenticator.

Creating a wildcard administrator account

Wildcard accounts can also be used in order to avoid specifying each user locally. When this option is enabled, any user included on the RADIUS server will be able to authenticate as an administrator on the FortiMail.

To create a wildcard administrator account:

1. Enable the *remote_wildcard* account.
   a. In FortiMail, enter *Advanced View* from the *Simple/Advanced View* dropdown on the top right.
   b. Go to *System* > *Administrator*, and enable the *remote_wildcard* account.
2. Configure the administrator profile.
   a. Edit the *remote_wildcard* account.
   b. Select an *Admin profile*.
   c. Select *RADIUS* as the *Authentication type*, and choose the *RADIUS profile*. Click *OK*.



Third-party RADIUS clients

After completing FortiAuthenticator setup on page 7, please consult the vendor's documentation for information about configuring your third-party device as a RADIUS client.

Most third-party RADIUS client configurations require the following information obtained from the FortiAuthenticator:

- The name for the RADIUS auth server.
- The IP/FQDN for the RADIUS auth server.
- The port for the RADIUS auth server – the default is port number is *1812*.
- The RADIUS secret. This is the same as what is configured on the RADIUS auth server on FortiAuthenticator.

Troubleshooting

Logging

If authentication fails, you can check the FortiAuthenticator log files for additional information.

To debug a bad password:

If the user insists that they have the correct credentials, try resetting the password.

If authentication continues to fail, verify that you have entered the correct shared Secret on both the client and FortiAuthenticator.

To debug a bad token code:

This issue may be due to a user error (entering the incorrect Token), or caused by a timing issue.

To troubleshoot this issue, verify the following:

- The user is not attempting to use a previously used PIN. You cannot log in twice with the same token PIN.
- The time and time zone on the FortiAuthenticator is correct, and preferably synchronized using NTP.
- The token is correctly synched with FortiAuthenticator.

To debug when nothing is logged:

If the logs do not include either a failure or a successful authentication logged, it is likely due to one of the following:

- The request is not reaching the FortiAuthenticator.
  - Verify that any intervening firewalls are permitting the required traffic through the network. RADIUS authentication traffic requires UDP Port 1812 to be open to the FortiAuthenticator and that pseudo-stateful responses are allowed to return.
- The request is reaching the FortiAuthenticator but is being ignored.
  - If traffic is seen reaching the FortiAuthenticator (e.g. by packet sniffing) but is being ignored, it is likely that the requesting client is not configured in the FortiAuthenticator.
  - Verify that the client is sending the traffic from the expected IP address and not from a secondary IP address or alternative interface. The FortiAuthenticator RADIUS server will not respond to requests from an unknown client for security reasons.

Extended logging

The logs found at *Logging* > *Log Access* > *Logs* provide a summary of events occurring on the system, particularly the information required for audit purposes (e.g. who logged in and where from). When a more detailed view is required in order to troubleshoot issues, detailed system application logs can be found by navigating to `https://<FAC IP>/debug`.

RADIUS authentication debugging mode can be accessed to debug RADIUS authentication issues.

From the Service dropdown menu, select *RADIUS Authentication,* and click *Enter debug mode* from the toolbar.

Enter the username and password and select *OK* to test the RADIUS authentication and view the authentication response and returned attributes.

Traffic sniffing

Wireshark can be used to monitor traffic being sent and received to the FortiAuthenticator by setting it to capture traffic on UDP port 1812.

RADIUS packet generation

Testing authentication directly without the use of a NAS device is useful to rule out issues with the client. This is most easily achieved using a tool such as NTRADPing on Windows or radclient on Linux.

Appendix A - Supported two-factor authentication methods

Product	Version in guide	Authentication type	Token-appended	Token-challenge	Wildcard authentication
FortiGate	7.0.0	Web management	Yes	Yes	Yes
		CLI based management	Yes	Yes	Yes
		SSL-VPN (Web)	Yes	Yes	Yes
		SSL-VPN (FortiClient)	Yes	Yes	Yes
		Identity based policy	Yes	Yes	Yes
FortiManager	7.0.0	Web based management	Yes	Yes	Yes
		CLI based management	Yes	Yes	Yes
FortiAnalyzer	7.0.0	Web based management	Yes	Yes	Yes
		CLI based management	Yes	Yes	Yes
FortiWeb	6.4.0	Web management	Yes		Yes
		CLI based management	Yes		Yes
FortiMail	6.4.5	Web based management	Yes	Yes	Yes
		CLI based management	Yes	Yes	Yes
Cisco Switch	IOS 12.1 (13)	Web based management	Yes		
		CLI based management	Yes		
Citrix Access Gateway	5.0	Web based management	Yes	Yes	Yes
		CLI based management	Yes	Yes	Yes
Linux OpenSSH	5.8p1	SSH Login	Yes	Yes	Yes
Apache	2.2.17	Web Authentication	Yes	Yes	Yes

Appendix B - Synchronizing FortiTokens

Under normal circumstances, it is not necessary to synchronize FortiToken unless the time on the host FortiAuthenticator system has been allowed to deviate from the correct time. It is essential that the time is accurate in order to prevent synchronization issues from occurring, therefore configuration of an NTP server is recommended.

The natural drift time of the FortiToken is accounted for automatically by the FortiAuthenticator. Every time a user logs in, the FortiAuthenticator calculates the drift, and if it is within +/- 1 (where 1 is a token cycle of 60 seconds), the drift is adjusted accordingly. Should the drift deviate by greater than 1 (i.e. the clock is more than 60 seconds out) since the last login, a manual synchronization is required.

If manual synchronization is required for multiple tokens, this could be a sign that the FortiAuthenticator time is inaccurate. Verify the current time and the NTP settings.

Administrator synchronization

It is possible for the administrator to synchronize a token for use on the FortiAuthenticator. This can be useful when new tokens have been issued which have been held in storage for an extended period of time or are being reissued to a new user.

To perform a drift adjustment on a FortiToken:

1. In a browser, go to:
   `https://<FortiAuthenticator-IP-Address>/admin/fortitoken/fortitokendrift/`
2. Select the FortiToken to adjust, then select *Adjust Drift*.
   The Adjust Token Drift window opens.
3. Enter the required Time adjustment in minutes.
   Make sure to include a minus sign (-) for a negative value, but don't use a plus sign (+) for a positive value.
4. Select *OK* to adjust the token drift.

Key points to note during the synchronization process are:

- Ensure that the FortiAuthenticator time is accurate before proceeding.
- Ensure that the serial of the token you are synchronizing matches that on the reverse of the token.
- Ensure that the token has not been used in the proceeding 60 seconds. All tokens are one-time passwords and cannot therefore be used to authenticate (successful or otherwise) and synchronize.
- Once successfully synchronized, wait a further 60 seconds before attempting to log in. A token used to synchronize cannot be re-used to authenticate.

User synchronization

Should it be required, FortiAuthenticator provides a mechanism allowing the user to perform their own manual synchronization. The user should be allowed to access the FortiAuthenticator GUI (*https://<FAC IP>/login/*).

Upon logging into the FortiAuthenticator, the user will be prompted to enter their token PIN. If the token PIN is out of sync, they will be prompted to enter two consecutive PINs. If the user does not receive the prompt, the token is already correctly synchronized.

www.fortinet.com