FortiGate with GreenRADIUS 2FA - Integration Guide

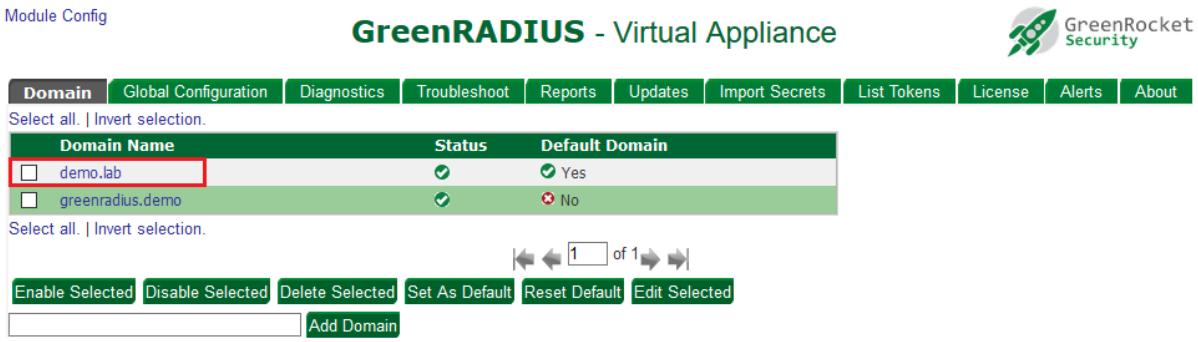
March 7, 2018

1 GreenRADIUS Setup

Before starting, ensure GreenRADIUS is configured correctly to communicate with the local Active Directory or LDAP domain, as well as with the validation service (either local validation or the YubiCloud). Full instructions on setting up GreenRADIUS can be found in our Document Library -- http://www.greenrocketsecurity.com/resources/library/.

1.1 General Configuration

1. Open the GreenRADIUS web admin interface and navigate to the Domain tab.
2. Create a new domain for importing users from Active Directory. Use the same domain name as that of the name of the domain in Active Directory. See the image below.



1.2 Domain Configuration

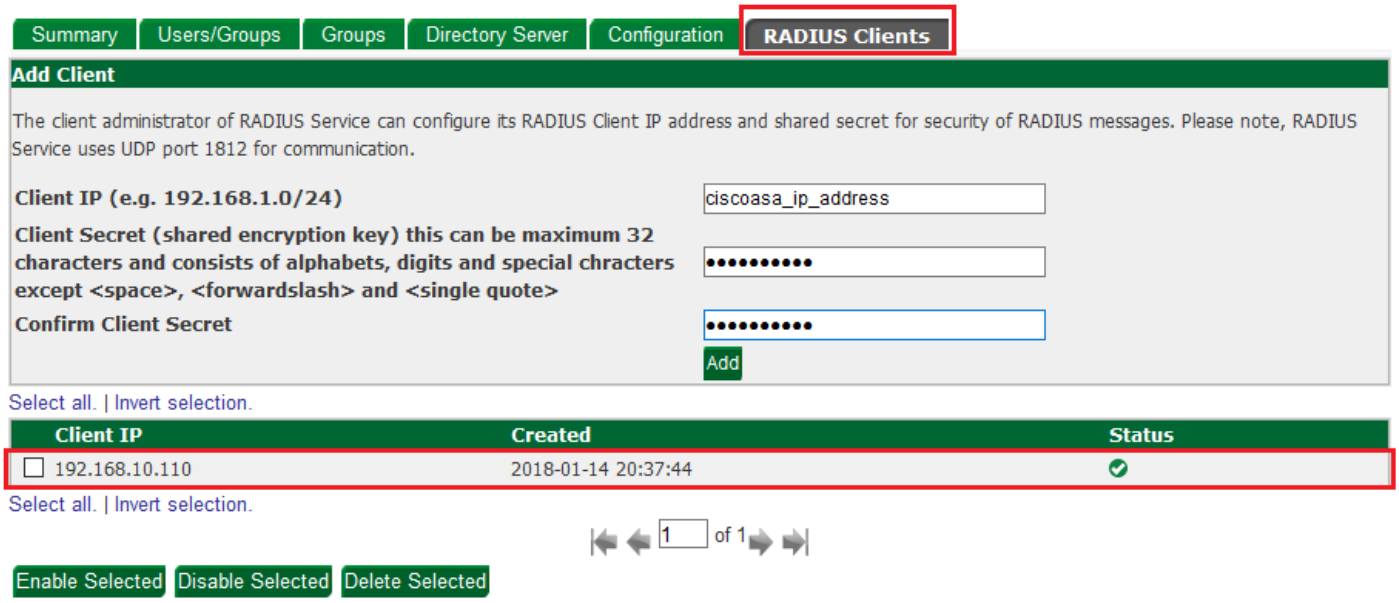
1. After creating the domain, import users from Active Directory. Assign a token to one or more users. These tokens will be used for two-factor authentication.

2. Click on the “RADIUS Clients” tab, and enter the following details about your FortiGate:

   a. Client IP – enter in the IP address of the FortiGate. If you enter an IP address that ends with 0/24, (such as 192.168.1.0/24), GreenRADIUS will accept a request from clients across the entire subnet on the selected port.

   b. Client Secret / Confirm Client Secret – This is a symmetric shared secret between GreenRADIUS and the RADIUS client. Please follow best practice with secure password policies when creating this shared secret. GreenRADIUS can hold a secret of up to 50 characters.

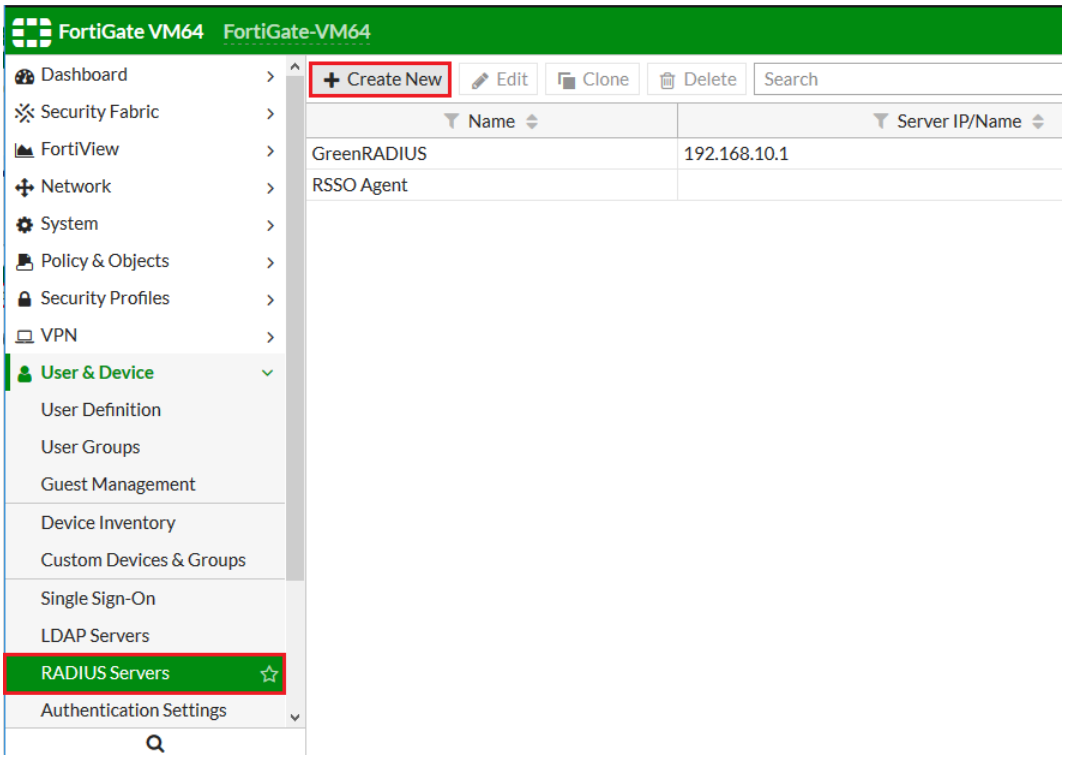
3. Click the “Add” button below the fields to add the FortiGate to GreenRADIUS. Once done, the details entered will appear below.



2 FortiGate Configuration

Before starting, ensure that network, interfaces, and client profiles are configured correctly.

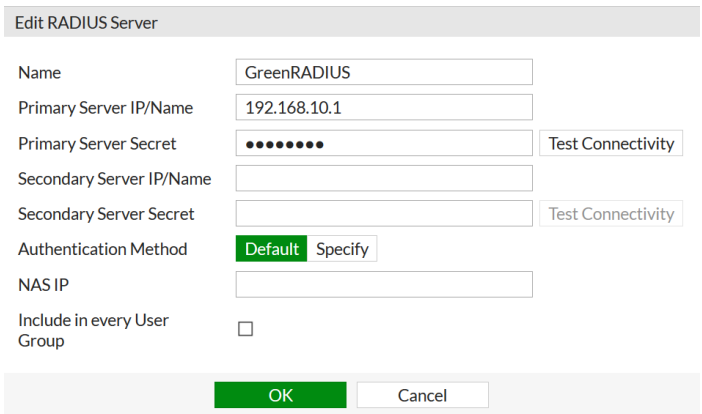
1. Login to FortiGate.
2. Open the “User & Device” menu.
3. Select RADIUS Servers and choose +Create New.



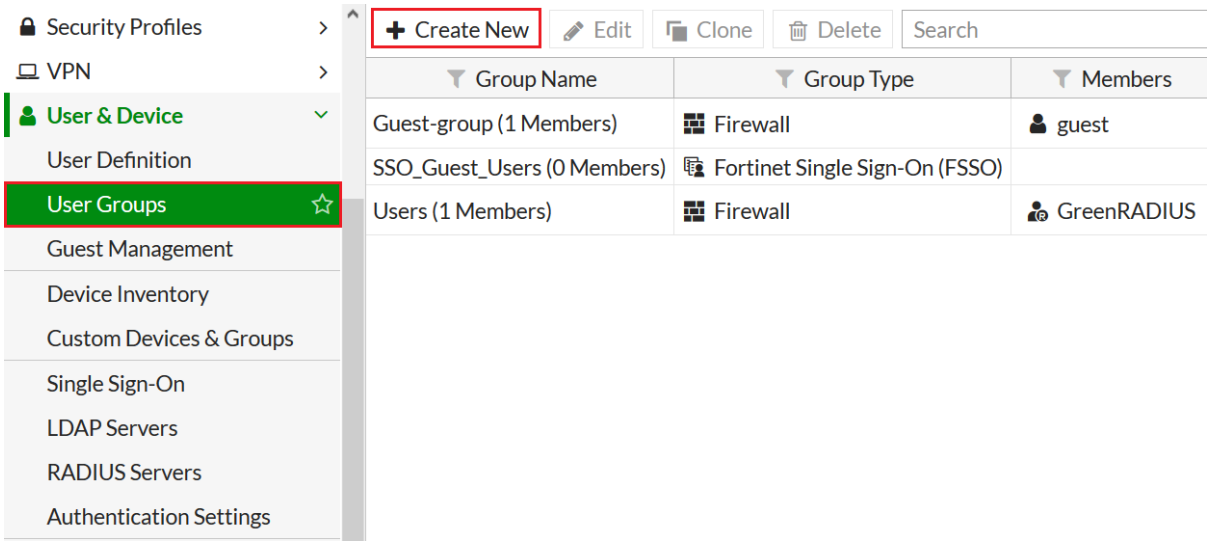
4. Configure the following fields:

   Name: **GreenRADIUS**
   Primary Server IP/Name: **<your_greenradius_ip>**
   Primary Server Secret: same **Client Secret** provided in the RADIUS Clients tab in GreenRADIUS

5. Use Test Connectivity to verify the above settings.
6. Click OK.



7. From the User & Device menu, open User Groups and choose +Create New.

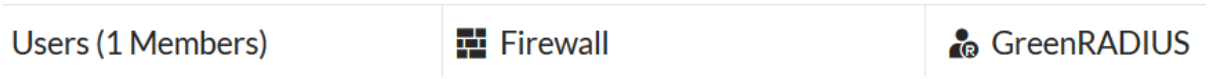


8. Configure the following fields:

   Name: any (e.g. Users)
   Type: **Firewall**
   Members: <leave this field empty>
   Remote Groups > choose +Add
   Remote Server: choose **GreenRADIUS**
   Groups: <leave this field empty>

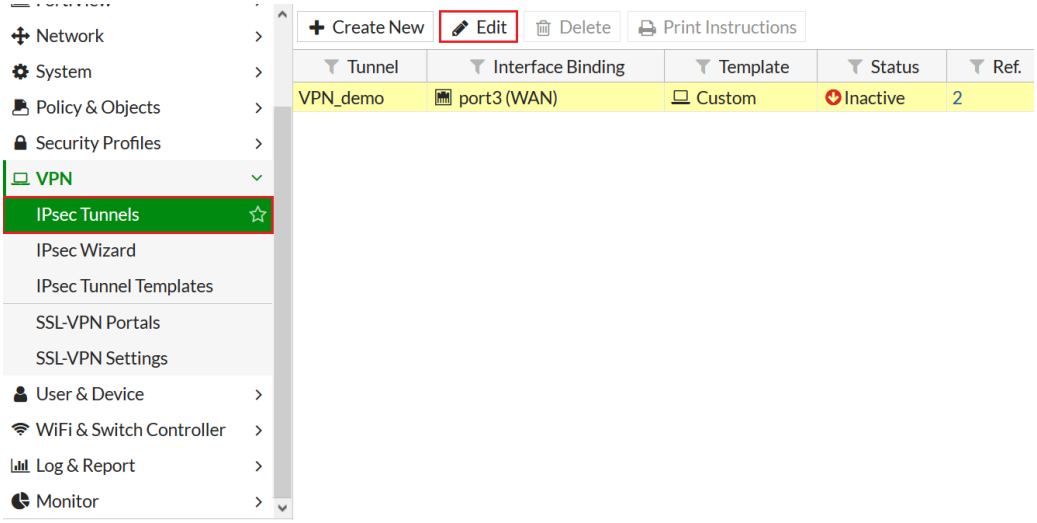
9. Click OK.

10. The new Users (1 Members) group with Members = GreenRADIUS should now be listed as below:



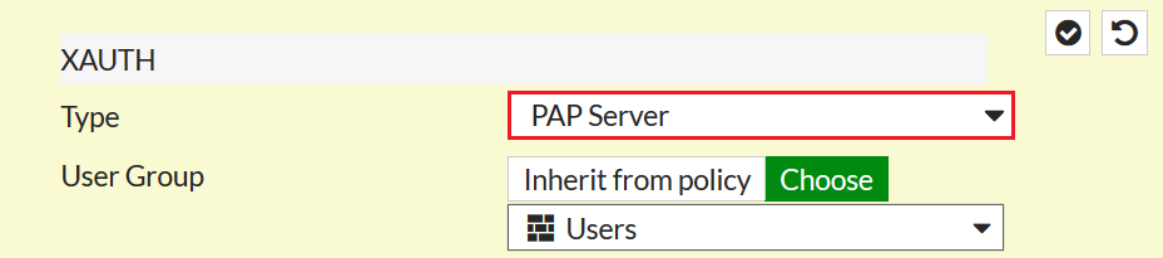
11. Open the VPN menu.

12. Select IPsec Tunnels, choose your current VPN and click Edit.



13. Navigate to XAUTH, choose Edit and apply the following settings:

    Type: **PAP Server**
    User Group: Choose > Users (Remote GreenRADIUS member group)



14. The GreenRADIUS quick integration is now completed. Ensure that XAuth has been enabled on your FortiClient. It should be set to “Prompt on login” or “Save login”. (Do not set to “Disable”.)

15. Try logging in on the VPN client. Enter the username and password. In the password field, append your Yubikey OTP or Google Authenticator OTP (to the end of the password). Then click Connect.