

WatchGuard with GreenRADIUS 2FA - Integration Guide

June 18, 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.

Module Config

GreenRADIUS - Virtual Appliance

GreenRocket Security

Domain Global Configuration Diagnostics Troubleshoot Reports Updates Import Secrets List Tokens License Alerts About

Select all. | Invert selection.

Domain Name	Status	Default Domain
<input type="checkbox"/> demo.lab	✓	✓ Yes
<input type="checkbox"/> greenradius.demo	✓	✗ No

Select all. | Invert selection.

1 of 1

Enable Selected Disable Selected Delete Selected Set As Default Reset Default Edit Selected

Add Domain

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 WatchGuard:
 - a. Client IP – enter in the IP address of the WatchGuard. 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.

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

The screenshot shows the 'RADIUS Clients' configuration page. At the top, there are tabs for 'Summary', 'Users/Groups', 'Groups', 'Directory Server', 'Configuration', and 'RADIUS Clients'. Below the tabs is the 'Add Client' section with a text box explaining that the administrator can configure the RADIUS Client IP address and shared secret. The form includes fields for 'Client IP (e.g. 192.168.1.0/24)', 'Client Secret (shared encryption key)', and 'Confirm Client Secret'. An 'Add' button is located below the 'Confirm Client Secret' field.

Below the form is a table with the following columns: 'Client IP', 'Created', and 'Status'. The table contains one entry: '192.168.10.110' with a creation date of '2018-01-14 20:37:44' and a status of '✓'. Below the table are navigation controls and buttons for 'Enable Selected', 'Disable Selected', and 'Delete Selected'.

1.3 Enable Filter-Id group attribute

- After adding WatchGuard as a RADIUS client, navigate to the Configuration tab.
- Select **Yes** for “Return User’s Group Membership In RADIUS Response”.
- Choose **Filter-Id** for “RADIUS Group Attribute”.
- Click on **Update**.

The screenshot shows the 'Domain Configuration' page. At the top, there are tabs for 'Summary', 'Users/Groups', 'Groups', 'Directory Server', 'Configuration', and 'RADIUS Clients'. Below the tabs is the 'Domain Configuration' section with a sub-section for 'General Configuration'. The 'General Configuration' section includes several options with radio buttons for 'Yes' and 'No':

- Enable Gradual Deployment: Yes No
- Return User’s Group Membership In RADIUS Response: Yes No
- RADIUS Group Return Attribute: **Filter-Id** (selected from a dropdown menu)
- Response Format: <Group name>
- Group Return Information: Group DN Only Group Name
- Return All Groups: Yes No
- Enable YubiApp Registration: Yes No
- Set This Domain As Default: Yes No

Below the 'General Configuration' section are sections for 'YubiKey (Yubico OTP Mode) Configuration' and 'YubiKey (OATH-HOTP Mode) Configuration', each with two options for 'Yes' and 'No'. At the bottom of the form is a 'Token Label Prefix for Google Authenticator' field and an 'Update' button.

1.4 Return your VPN users group

1. After enabling the Filter-Id group attribute, navigate to the Groups tab.
2. Look for your directory VPN group object and set it to the highest priority = 1
e.g. "vpnusers" is the AD group in which members are allowed to connect via VPN.
3. Click on **Update**.

Summary	Users/Groups	Groups	Directory Server	Configuration	RADIUS Clients
Domain Configuration					
Domain Controllers	<input type="text" value="0"/>				
GRSOU	<input type="text" value="0"/>				
Administrators	<input type="text" value="0"/>				
Guests	<input type="text" value="0"/>				
vpnusers	<input type="text" value="1"/>				
Group1	<input type="text" value="0"/>				
Group2	<input type="text" value="0"/>				
Schema Admins	<input type="text" value="0"/>				
Enterprise Admins	<input type="text" value="0"/>				
Domain Admins	<input type="text" value="0"/>				
Group Policy Creator Owners	<input type="text" value="0"/>				
Denied RODC Password Replication Group	<input type="text" value="0"/>				
Update					

1.5 Using YubiKeys with WatchGuard

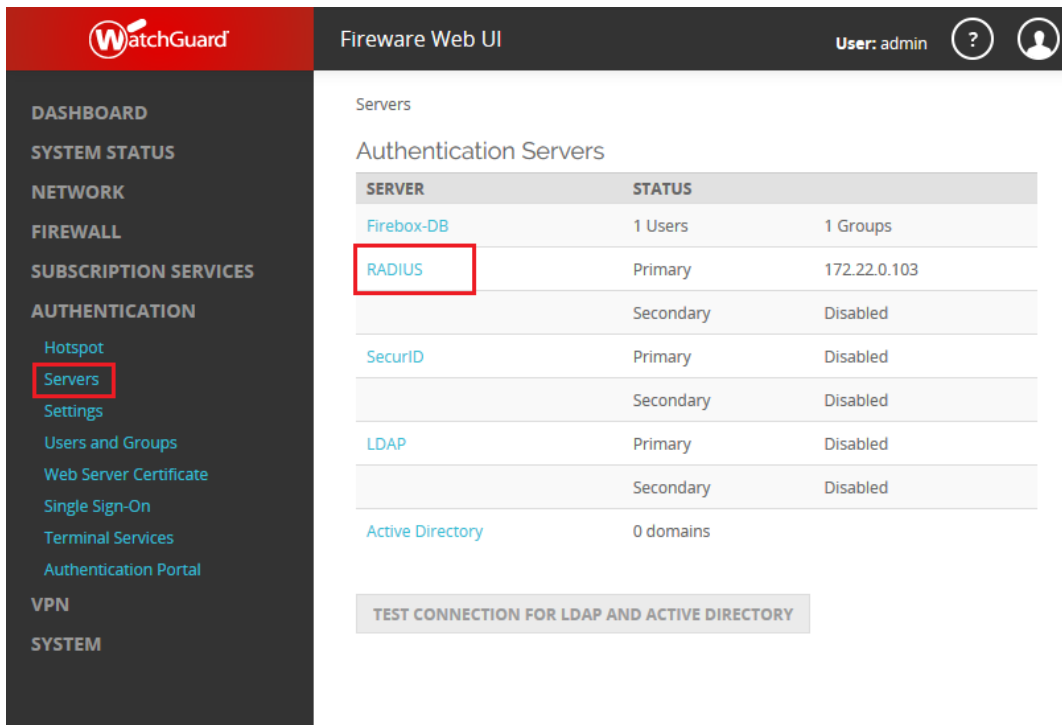
WatchGuard has a password field character limit of 48. Thus, using the default YubiKey OTP, which has a character length of 44, is not feasible. Instead, we recommend that YubiKeys be programmed in OATH HOTP mode so OTPs are 18 characters (12-character token identifier plus 6-digit OATH HOTP OTP). This will allow your users to use a LDAP password of up to 30 characters and append the programmed YubiKey's 18-character OTP without any issues with the WatchGuard password field limitation.

Please refer to our [YubiKey OATH HOTP programming guide](#).

2 WatchGuard Configuration

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

1. Log in to the WatchGuard Firewall Web UI.
2. Navigate to AUTHENTICATION > **Servers**.
3. Click on **RADIUS**.



The screenshot shows the WatchGuard Fireware Web UI. The left sidebar contains a navigation menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION (with sub-items: Hotspot, Servers, Settings, Users and Groups, Web Server Certificate, Single Sign-On, Terminal Services, Authentication Portal), VPN, and SYSTEM. The 'Servers' item is highlighted with a red box. The main content area is titled 'Servers' and 'Authentication Servers'. It contains a table with the following data:

SERVER	STATUS	
Firebox-DB	1 Users	1 Groups
RADIUS	Primary	172.22.0.103
	Secondary	Disabled
SecurID	Primary	Disabled
	Secondary	Disabled
LDAP	Primary	Disabled
	Secondary	Disabled
Active Directory	0 domains	

Below the table is a button labeled 'TEST CONNECTION FOR LDAP AND ACTIVE DIRECTORY'.

4. Select **Enable RADIUS Server**.
5. Configure the following fields:
 - IP Address: **your_greenradius_ip**
 - Port: **1812**
 - Passphrase: the **Client Secret** provided under RADIUS Clients in GreenRADIUS
 - Confirm: the **Client Secret** once again
 - Timeout: **30** seconds
 - Retries: 3
 - Group Attribute: 11
 - Dead Time: 10 Minutes
6. Click on **SAVE**.

WatchGuard Fireware Web UI User: admin

Servers / RADIUS

Before you configure your Firebox device to use a RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication requests.

Primary Server Settings

Enable RADIUS Server

IP Address: 172.22.0.103

Port: 1812

Passphrase: [Masked]

Confirm: [Masked]

Timeout: 30 seconds

Retries: 3

Group Attribute: 11

Dead Time: 10 Minutes

7. Navigate to VPN > Mobile VPN with SSL > **Authentication**.

WatchGuard Fireware Web UI User: admin

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication Advanced

Authentication Server Settings

Auto reconnect after a connection is lost

Force users to authenticate after a connection is lost

Allow the Mobile VPN with SSL client to remember password

Define users and groups to authenticate with Mobile VPN with SSL. The users and groups you define are automatically included in the "SSLVPN-Users" group.

	NAME	TYPE	AUTHENTICATION SERVER
<input type="checkbox"/>	vpnusers	Group	RADIUS

ADD REMOVE

8. Add your "vpnusers" group name.
9. Select **RADIUS** as Authentication Server.
10. Click OK.

Add User or Group ✕

Type Group
 User

Name

Authentication Server ▼

11. The Firebox/XTM RADIUS integration is now done.

3 Authentication Test

At this point, you can try a single-factor (password only) login attempt and then verify that the authentication successfully went through GreenRADIUS.

1. Make sure the test user you are using is single-factor in GreenRADIUS.
 - a. Click on the domain the user is in, then click on the Users/Groups tab.
 - b. Find the user you will test with. (You can use the search function if you have many pages of users.)
 - c. In the Single Factor Flag column, if the user has a red "X", click the checkbox next to the user, then click on "Enable Single Factor". The user should have a green checkmark in the Single Factor Flag for this password-only test.
2. Log in to the WatchGuard VPN client with the user's username and password.
3. In GreenRADIUS, you can check that the authentication went through by going to GreenRADIUS Virtual Appliance → Reports tab → Authentication Requests
 - a. Click on Run Report
 - b. The authentication attempt should then be listed there.