

Pulse Secure with GreenRADIUS 2FA - Integration Guide

February 15, 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

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 Pulse Secure:
 - a. Client IP – enter in the IP address of Pulse Secure. 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 Pulse Secure to GreenRADIUS. Once done, the details entered will appear below.

Summary Users/Groups Groups Directory Server Configuration **RADIUS Clients**

Add Client

The client administrator of RADIUS Service can configure its RADIUS Client IP address and shared secret for security of RADIUS messages. Please note, RADIUS Service uses UDP port 1812 for communication.

Client IP (e.g. 192.168.1.0/24)

Client Secret (shared encryption key) this can be maximum 32 characters and consists of alphabets, digits and special chracters except <space>, <forwardslash> and <single quote>

Confirm Client Secret

Select all. | Invert selection.

Client IP	Created	Status
<input type="checkbox"/> 192.168.10.123	2018-01-29 21:30:06	✓

Select all. | Invert selection.

◀◀ 1 of 1 ▶▶

2 Pulse Secure Configuration

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

1. Log into the Pulse Secure Administrator Sign-In Page.
2. Open the “Authentication” tab and select “Auth. Servers”.
3. Locate “RADIUS Server” and choose “New Server...”.

Pulse Secure Pulse Connect Secure

System **Authentication** Administrators Users Maintenance Wizards

Authentication Servers

New: RADIUS Server **New Server...** Delete...

10 records per page Search:

<input type="checkbox"/>	Authentication/Authorization Servers	Type	User Record Synchronization	Logical Auth Server Name
Administrators		Local Authentication		
<input type="checkbox"/>	System Local	Local Authentication		

← Previous 1 Next →

4. Configure the following fields:

Name: **GreenRADIUS**

RADIUS Server: **your_greenradius_ip**

Authentication Port: **1812**

Shared Secret: The same **Client Secret** configured under RADIUS Clients in GreenRADIUS

[Auth Servers](#) > [GreenRADIUS](#) > Settings

Settings

Settings Users

*Name: Label to reference this server.

NAS-Identifier: Name of the device as known to RADIUS server

▼ **Primary Server**

*RADIUS Server: Name or IP address

*Authentication Port:

*Shared Secret:

*Accounting Port: Port used for RADIUS accounting, if applicable

NAS IPv4/IPv6 Address: IPv4/IPv6 address

*Timeout: seconds

*Retries:

5. Click “Save Changes” at the bottom.

6. Navigate to Users > User Realms
7. Select your Authentication Realm (default "Users").
8. Change the authentication server to GreenRADIUS or add an Additional Authentication Server.

[User Realms](#) > [Users](#) > General

General

General	Authentication Policy	Role Mapping
---------	-----------------------	--------------

* Name:

Users

Description:

Default authentication realm for users

When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

GreenRADIUS

User Directory/Attribute:

Same as above

Accounting:

GreenRADIUS

Device Attributes:

None

9. Choose "Save Changes".

3 Pulse Secure Prompt for Token (Optional)

By default, users submit their token OTPs (one-time passcodes) by appending them to their passwords in the password field. If desired, a separate OTP field can be used to submit OTPs instead of appending them to passwords. To configure this, follow the steps below.

1. Enable “**Prompt For OTP (RADIUS only)**” in GreenRADIUS in the Global Configuration tab > General

[Module Index](#)

General Configuration



General Configuration

General Configuration

OTP Input Method

Append OTP To Username
 Append OTP To Password
 Prompt For OTP (RADIUS only)

Enable Password Authentication Through GreenRADIUS

Yes No

Temporary Token Length

Max Number of Tokens Per User

On Service Fail, Send Email Alert

Yes No
Selecting "Yes" will send an email alert if OTP validation server is unavailable.

Email Address(es)

Email Sent From

2. Choose “Save”.
3. In Pulse Secure, navigate to Authentication > **Auth. Servers**
4. Open GreenRADIUS server settings
5. Create a new custom RADIUS rule

▼ Custom RADIUS Rules

<input type="checkbox"/>	Name	Response Packet Type	Attribute criteria	Action
<input type="checkbox"/>	OTP prompt	Access Challenge	(Reply-Message matches the expression "Please provide OTP")	Show Next Token page

6. Configure the following fields:

Name: **OTP prompt**

Reply-Message(18) > matches the expression > **Please provide OTP** > choose Add
 Then take action > show **Next Token** page

Auth Servers > GreenRADIUS > Edit Custom Radius Rule

Edit Custom Radius Rule

Name:

▼ If received Radius Response Packet ...

Response Packet Type:

Attribute criteria:

Radius Attribute	Operand	Value	
<input type="text" value="Reply-Message (18)"/>	<input type="text" value="matches the expression"/>	<input type="text" value="Please provide OTP"/>	<input type="button" value="Add"/>


▼ Then take action ...

- show **New Pin** page
- show **Next Token** page
- show **Generic Login** page
- show **user login page** with error message
-
- show **Reply-Message** attribute from the Radius server to the user
- send **Access Request** with additional attributes

Radius Attribute	Value	
<input type="text" value="User-Name (1)"/>	<input type="text"/>	<input type="button" value="Add"/>

7. Click "Save Changes"

A dedicated token page will appear after the usual user login:



Welcome to Pulse Connect Secure

⚠ Token Resync Required

Please enter an additional token code to continue.

The server requires that you enter an additional token code to verify that your credentials are valid. To continue, wait for the token code to change and then enter the new code in the SecurID Token Code field.

SecurID Token Code: