HOW TO ENABLE GREENRADIUS TWO-FACTOR AUTHENTICATION FOR SSH USERS IN CENTOS

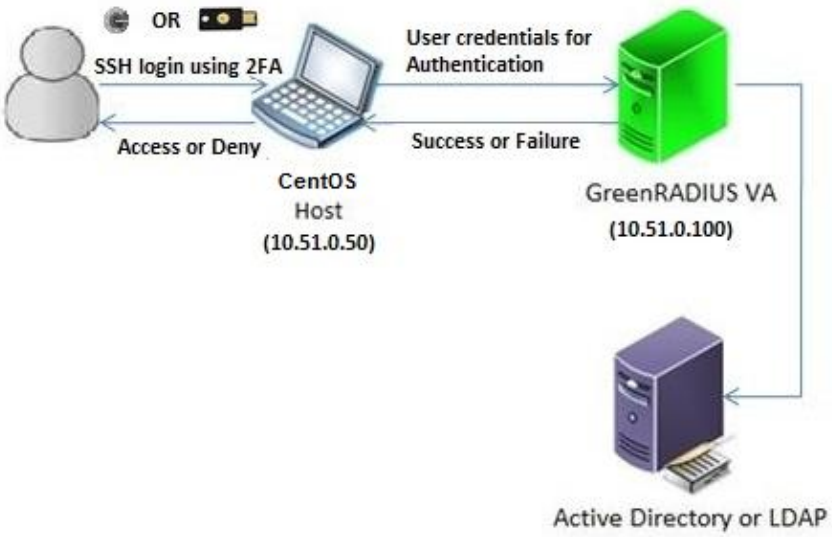
INTRODUCTION

This document explains how to enable Two-Factor-Authentication (2FA) for SSH users in CentOS host using GreenRADIUS Virtual Appliance.

PREREQUISITES

- This document assumes that GreenRADIUS Virtual Appliance is already set up with users imported in a domain from Active Directory/LDAP and also tokens are assigned to users
- CentOS host 32 or 64 bit

DEPLOYMENT DIAGRAM



STEPS TO BE PERFORMED ON CENTOS HOST

1. Login to CentOS host using any SSH client programs like PuTTY
2. Change current directory to "/tmp" directory using the following command:

```
cd /tmp/
```

3. Download the "pam_radius_auth.so" file using the following command:

```
sudo wget -O "pam_radius_auth.so"
"https://files.greenrocketsecurity.com/pamradiuscentos"
```

Output:

```
……

Saving to: ‘pam_radius_auth.so’

100%[===================================================
=================================================>]
40,750       140KB/s   in 0.3s

2016-06-17 14:00:37 (140 KB/s) - ‘pam_radius_auth.so’
saved [40750/40750]
```

4. For 32 bit CentOS host, copy the ‘pam_radius_auth.so’ file to ‘/lib/security/’ using the following command:

```
sudo cp pam_radius_auth.so /lib/security/
```

5. For 64 bit CentOS host, copy the ‘pam_radius_auth.so’ file to ‘/lib64/security/’ using the following command:

```
sudo cp pam_radius_auth.so /lib64/security/
```

6. Edit file ‘/etc/pam.d/sshd’ and add the following line at the top of this file:

```
auth required pam_radius_auth.so
```

7. Comment the line “auth include password-auth” as follows and save the file:

```
#auth        include      password-auth
```

8. Create a directory "raddb" in "/etc/" folder using the following command:

```
sudo mkdir /etc/raddb/
```

9. Change current directory to "raddb" directory and create a file named "server" using the following commands:

```
cd /etc/raddb/

sudo touch server
```

10. Edit the file "/etc/raddb/server" and add the following details into this file (each separated by a space):

```
<<GreenRADIUS Virtual Appliance IP>><<Shared
Secret>><<Timeout(seconds)>>

E.g. If your GreenRADIUS Virtual Appliance IP address is
"10.51.0.100" and shared secret is "test", you can use
following configuration:

      10.51.0.100 test 3
```

11. Add a new user without password to the server using the following command:

```
useradd -d /home/<<user name>> -m <<user name>>

E.g. If you want to add user say "john", you can use
following command to add user:

      useradd -d /home/john -m john
```

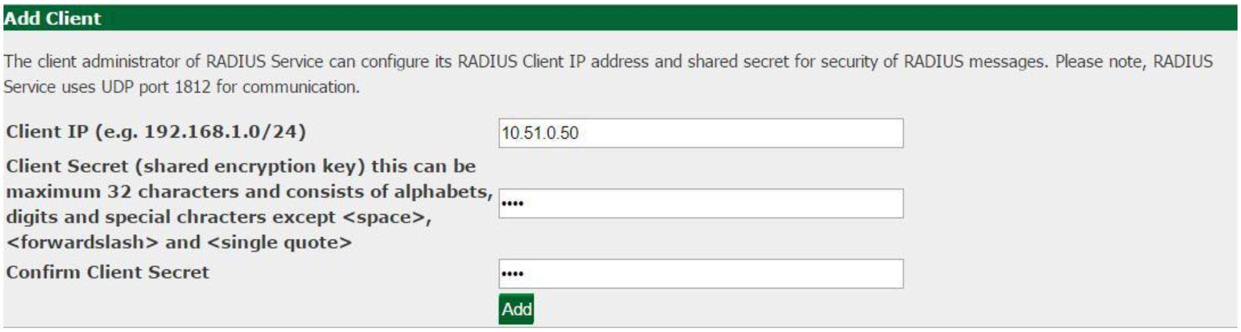
Note: The username added must also be present in any one of the domains created in GreenRADIUS Virtual Appliance.

12. Restart SSH service using the following command:

```
sudo service sshd restart
```

STEPS TO BE PERFORMED ON GREENRADIUS VIRTUAL APPLIANCE

1. Login to GreenRADIUS admin console using any web browser
2. Go to the ‘Domain’ tab and select the domain in which the user (in our case "John") is present.
3. Go to "Configuration" tab
4. Fill in the details of the CentOS host in the "Add Client" section:
   - E.g. If your CentOS host's IP address is "10.51.0.50" and shared secret will be same as shared secret mentioned in step 10 of previous section (i.e. "test" in our case), hence add RADIUS client as shown in the image below and click ‘Add’:



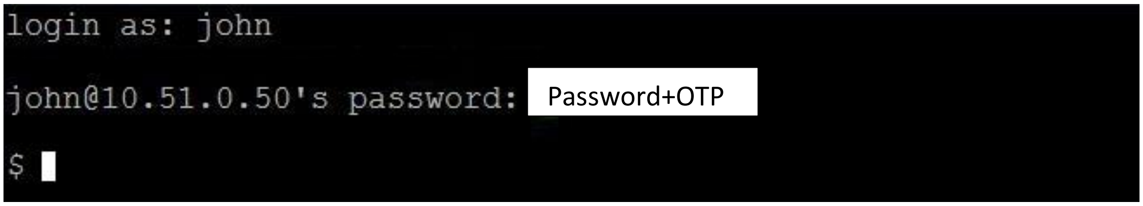
Add Client

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)	10.51.0.50
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	••••

TEST SSH LOGIN ON CENTOS HOST USING TWO-FACTOR AUTHENTICATION:

1. Login to CentOS host using any SSH client programs like PuTTY
2. Type username and hit enter
3. You will be prompted for password. At the prompt for password, enter the user's password configured in Active Directory/LDAP and immediately followed by an OTP from a token assigned to the user (in our case "John").
    - E.g. If username is "John", test login as shown in the image below:



```
login as: john
john@10.51.0.50's password: Password+OTP
$ █
```

DEBUGGING:

For debugging, use following command on CentOS host:

```
tail -f /var/log/secure
```

SSH LOGIN WITH PROMPT FOR OTP

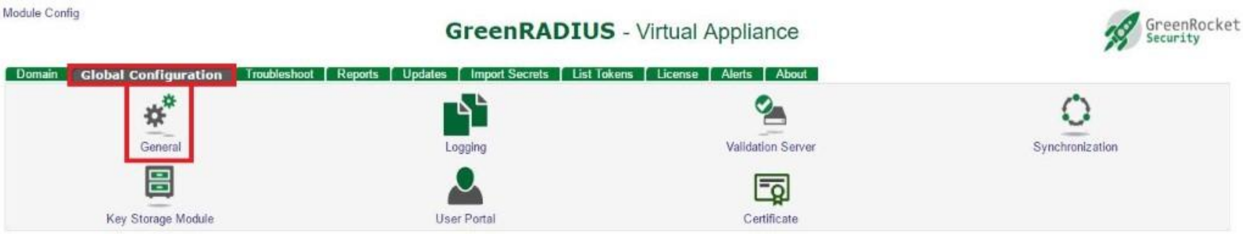
If you want to enable SSH login to prompt for OTP, follow the below steps.

ADDITIONAL STEPS TO BE PERFORMED ON CENTOS HOST

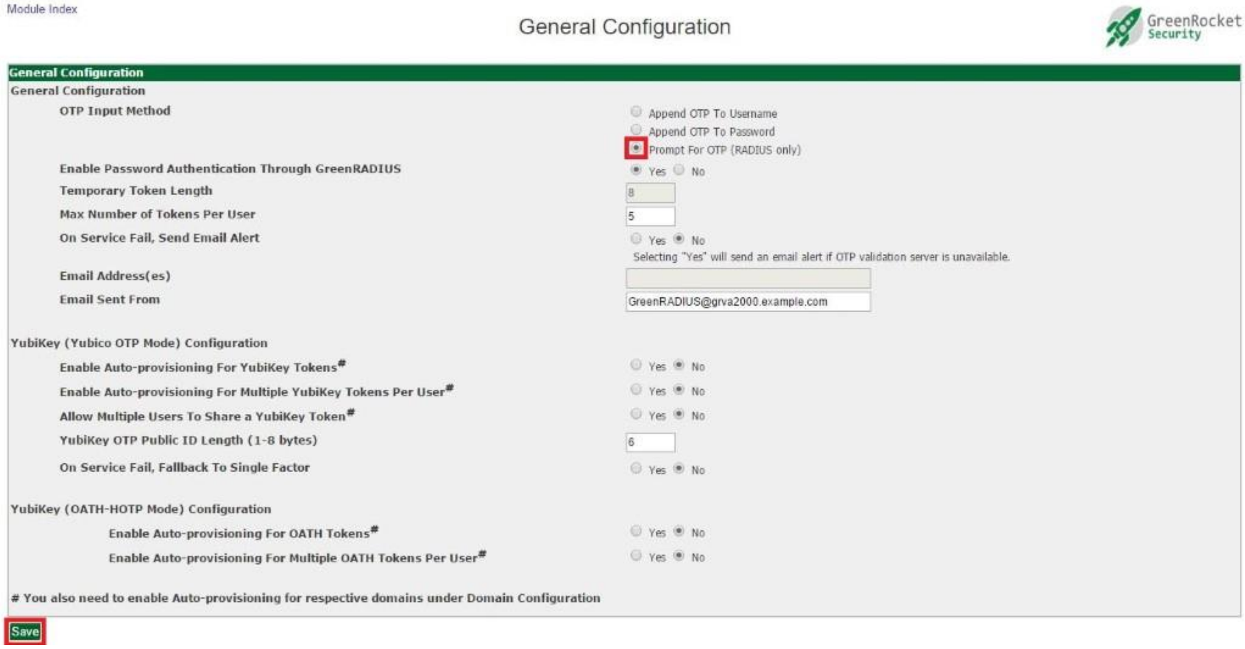
1. First follow the steps performed in the above section "Steps to be performed on CentOS host"
2. Edit the file "/etc/ssh/sshd_config".
3. Find the line "ChallengeResponseAuthentication no" and change
   it to "ChallengeResponseAuthentication yes".
4. Restart SSH service using the following command:
   sudo service sshd restart

STEPS TO BE PERFORMED ON GREENRADIUS

1. Log in to the GreenRADIUS web admin console
2. Go to the "Global Configuration" tab and click on "General"



3. Under "General Configuration" section select "OTP Input Method" as "Prompt For OTP (RADIUS only)" and click "Save".



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	8
Max Number of Tokens Per User	5
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	GreenRADIUS@grva2000.example.com

YubiKey (Yubico OTP Mode) Configuration

Enable Auto-provisioning For YubiKey Tokens#	○ Yes ● No
Enable Auto-provisioning For Multiple YubiKey Tokens Per User#	○ Yes ● No
Allow Multiple Users To Share a YubiKey Token#	○ Yes ● No
YubiKey OTP Public ID Length (1-8 bytes)	6
On Service Fail, Fallback To Single Factor	○ Yes ● No

YubiKey (OATH-HOTP Mode) Configuration

Enable Auto-provisioning For OATH Tokens#	○ Yes ● No
Enable Auto-provisioning For Multiple OATH Tokens Per User#	○ Yes ● No

You also need to enable Auto-provisioning for respective domains under Domain Configuration

Save