

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

INTRODUCTION

This document explains how to enable Two-Factor-Authentication (2FA) for SSH users in Ubuntu 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
- Ubuntu host 32 or 64 bit

DEPLOYMENT DIAGRAM



STEPS TO BE PERFORMED ON UBUNTU HOST

1. Login to Ubuntu 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://greenrocketsecurity-  
my.sharepoint.com/personal/support_greenrocketsecurity_c  
om/_layouts/15/guestaccess.aspx?guestaccesstoken=NcABlMN  
S06QtkeUaX2zYepONwsP3vnQmamKVgSXwjtE%3d&docid=02bce7f7d1  
dbd4dbe87cb947e2832d781"
```

```
.....  
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 Ubuntu 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 Ubuntu host, copy the 'pam_radius_auth.so' file to '/lib/x86_64-linux-gnu/security/' using the following command:

```
sudo cp pam_radius_auth.so /lib/x86_64-linux-  
gnu/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 "@include common-auth" as follows and save the file:

```
#@include common-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 /etc/init.d/ssh 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 Ubuntu host in the "Add Client" section:
 - E.g. If your Ubuntu 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)	<input type="text" value="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>	<input type="text" value="...."/>
Confirm Client Secret	<input type="text" value="...."/>
	<input type="button" value="Add"/>

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

1. Login to Ubuntu 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:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-24-generic x86_64)

* Documentation:  https://help.ubuntu.com/

$
```

CONFIGURE SSH LOGIN TO ASK FOR OTP

This section assumes that you have performed all the steps mentioned in the previous section “Steps to be performed on Ubuntu host” and “Steps to be performed on GreenRADIUS Virtual Appliance”. To configure SSH login to ask for OTP, we need to perform some additional configurations on Ubuntu host as well as GreenRADIUS Virtual Appliance.

STEPS TO BE PERFORMED ON UBUNTU HOST

1. Edit the file “/etc/ssh/sshd_config” and change “ChallengeResponseAuthentication no” as shown below:

```
ChallengeResponseAuthentication yes
```

2. Restart SSH service using the following command:

```
sudo /etc/init.d/ssh restart
```

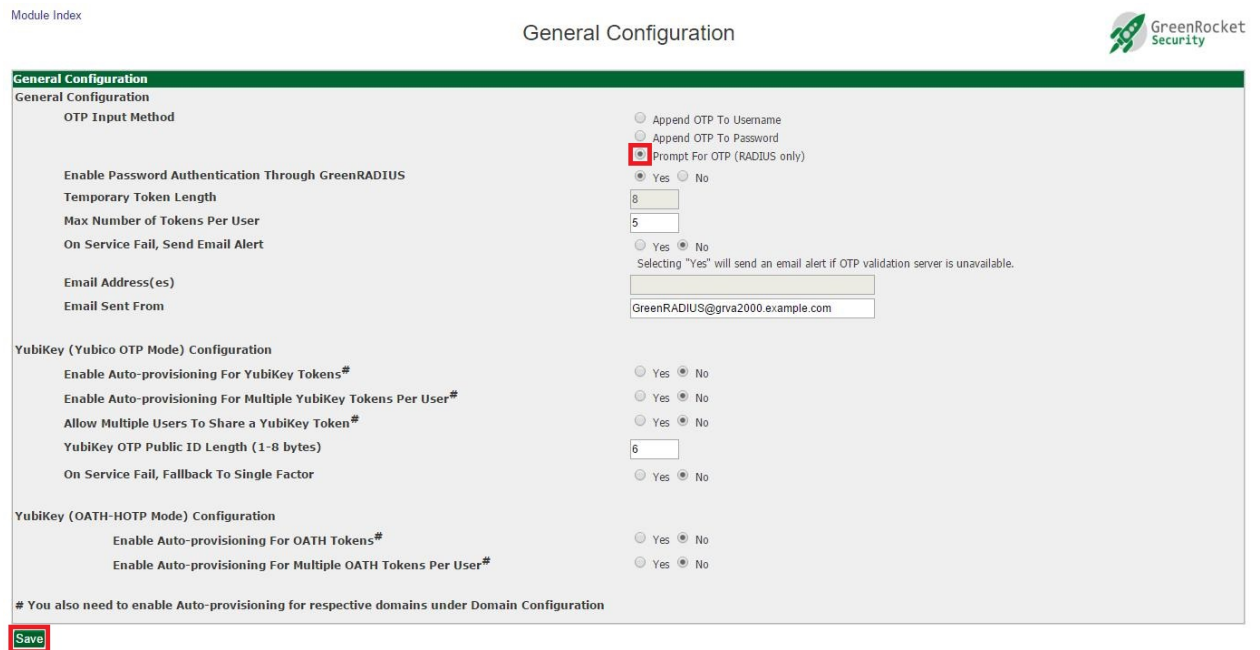
STEPS TO BE PERFORMED ON GREENRADIUS VIRTUAL APPLIANCE

1. Login to GreenRADIUS admin console using any web browser.

- Go to “Global Configuration” tab and click on “General” icon.



- Under “General Configuration” section, select “OTP Input Method” as “Prompt For OTP (RADIUS only)” and click on “Save”.



Module Index

General Configuration

GreenRocket Security

General Configuration

General Configuration

OTP Input Method

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

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

Yes No
 Yes No
 Yes No

YubiKey OTP Public ID Length (1-8 bytes): 6

On Service Fail, Fallback To Single Factor

Yes No
 Yes No

YubiKey (OATH-HOTP Mode) Configuration

Yes No
 Yes No

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

Save

TEST SSH LOGIN ON UBUNTU HOST USING TWO-FACTOR AUTHENTICATION TO ASK FOR OTP

- Login to Ubuntu host using any SSH client programs like PuTTY.
- Type username and hit enter.
- You will be prompted for password, enter the user’s password configured in Active Directory/LDAP and hit enter

4. You will be asked for OTP, enter an OTP from any one of the tokens assigned to the user.
 - E.g. If username is "John", test login as shown in the image below:

```
login as: John
Using keyboard-interactive authentication.
Password: Password
Using keyboard-interactive authentication.
Please provide OTP: OTP

Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

* Documentation:  https://help.ubuntu.com/

$ █
```

DEBUGGING:

For debugging, use following command on Ubuntu host

```
tail -f /var/log/auth.log
```