

# FreeRADIUS Used for Administrative Access on Cisco IOS Configuration Example



Document ID: 116291

Contributed by Minakshi Kumar, Cisco TAC Engineer.  
Jul 11, 2013

## Contents

### Introduction

### Prerequisites

- Requirements

- Components Used

### Configure

- Configure a Switch for Authentication and Authorization

- FreeRADIUS Configuration

### Verify

### Troubleshoot

### Related Information

## Introduction

This document describes how to configure RADIUS Authentication on Cisco IOS<sup>®</sup> switches with a third party RADIUS server (FreeRADIUS). This example covers the placement of a user directly into privilege 15 mode upon authentication.

## Prerequisites

### Requirements

Ensure that you have your Cisco switch defined as a client in FreeRADIUS with the IP address and the same shared secret key defined on FreeRADIUS and the switch.

### Components Used

The information in this document is based on these software and hardware versions:

- FreeRADIUS
- Cisco IOS Version 12.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configure

## Configure a Switch for Authentication and Authorization

1. In order to create a local user on the switch with full privileges for fallback access, enter:

```
Switch(config)#username admin privilege 15 password 0 cisco123!
```

2. In order to enable AAA, enter:

```
switch(config)# aaa new-model
```

3. In order to provide the IP address of the RADIUS server as well as the key, enter:

```
switch# configure terminal
switch(config)#radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
switch(config)#radius-server key hello123
```

*Note:* The key must match the shared secret configured on the RADIUS server for the switch.

4. In order to test RADIUS server availability, enter the *test aaa* command:

```
switch# test aaa server Radius 172.16.71.146 user1 Ur2Gd2BH
```

The test authentication fails with a Rejection from the server because it is not yet configured, but it will confirm that the server itself is reachable.

5. In order to configure login authentications to fall back to local users if RADIUS is unreachable, enter:

```
switch(config)#aaa authentication login default group radius local
```

6. In order to configure authorization for a privilege level of 15, as long as a user is authenticated, enter:

```
switch(config)#aaa authorization exec default group radius if-authenticated
```

## FreeRADIUS Configuration

### *Define the Client on the FreeRADIUS Server*

1. In order to navigate to the configuration directory, enter:

```
# cd /etc/freeradius
```

2. In order to edit the *clients.conf* file, enter:

```
# sudo nano clients.conf
```

3. In order to add each device (router/switch) identified by hostname and include the correct shared secret, enter:

```
client 192.168.1.1 {
secret = secretkey
nastype = cisco
shortname = switch
}
```

4. In order to edit the users file, enter:

```
# sudo nano users
```

5. Add each user allowed to access the device. This example demonstrates how to set a Cisco IOS privilege level of 15 for the user "cisco."

```
cisco Cleartext-Password := "password"
    Service-Type = NAS-Prompt-User,
```

```
Cisco-AVPair = "shell:priv-lvl=15"
```

6. In order to restart FreeRADIUS, enter:

```
# sudo /etc/init.d/freeradius restart
```

7. In order to change the DEFAULT user group in the user's file in order to give all users who are members of cisco-rw a privilege level of 15, enter:

```
DEFAULT Group == cisco-rw, Auth-Type = System  
Service-Type = NAS-Prompt-User,  
cisco-avpair := "shell:priv-lvl=15"
```

8. You can add other users at different privilege levels as needed in the FreeRADIUS users file. For example, this user (life) is given a level of 3 (system maintenance):

```
sudo nano/etc/freeradius/users  
  
life Cleartext-Password := "testing"  
Service-Type = NAS-Prompt-User,  
Cisco-AVPair = "shell:priv-lvl=3"
```

```
Restart the FreeRADIUS service:  
sudo /etc/init.d/freeradius restart
```

**Note:** The configuration in this document is based on FreeRADIUS run on Ubuntu 12.04 LTE and 13.04.

## Verify

In order to verify the configuration on the switch, use these commands:

```
switch# show run / in radius           (Show the radius configuration)  
switch# show run / in aaa             (Show the running AAA configuration)  
switch# show startup-config Radius    (Show the startup AAA configuration in  
start-up configuration)
```

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Related Information

- *FreeRADIUS*
- *Technical Support & Documentation – Cisco Systems*