

# How to Assign Privilege Levels with TACACS+ and RADIUS

Document ID: 13860

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Example

- Configurations – Router
- Configurations – Server

#### Related Information

## Introduction

This document explains how to change the privilege level for certain commands, and provides an example with parts of sample configurations for a router and TACACS+ and RADIUS servers.

## Prerequisites

### Requirements

Readers of this document should have knowledge of privilege levels on a router.

By default, there are three privilege levels on the router.

- privilege level 1 = non-privileged (prompt is `router>`), the default level for logging in
- privilege level 15 = privileged (prompt is `router#`), the level after going into enable mode
- privilege level 0 = seldom used, but includes 5 commands: **disable**, **enable**, **exit**, **help**, and **logout**

Levels 2–14 are not used in a default configuration, but commands that are normally at level 15 can be moved down to one of those levels and commands that are normally at level 1 can be moved up to one of those levels. Obviously, this security model involves some administration on the router.

To determine the privilege level as a logged-in user, type the **show privilege** command. To determine what commands are available at a particular privilege level for the version of Cisco IOS® software that you are using, type a **?** at the command line when logged in at that privilege level.

**Note:** Instead of assigning privilege levels, you can do command authorization if the authentication server supports TACACS+. The RADIUS protocol does not support command authorization.

### Components Used

The information in this document is based on Cisco IOS Software Releases 11.2 and later.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live

network, ensure that you understand the potential impact of any command before using it.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Example

In this example, **snmp-server** commands are moved down from privilege level 15 (the default) to privilege level 7. The **ping** command is moved up from privilege level 1 to privilege level 7. When user seven is authenticated, that user is assigned privilege level 7 by the server and a **show privilege** command displays "Current privilege level is 7." The user can ping and do snmp-server configuration in configuration mode. Other configuration commands are not available.

## Configurations – Router

### Router – 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

### Router – 11.3.3.T and Later (until 12.0.5.T)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

### Router – 12.0.5.T and Later

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
```

```
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

## Configurations – Server

### Cisco Secure NT TACACS+

Follow these steps to configure the server.

1. Fill in the username and password.
2. In Group Settings, make sure shell/exec is checked, and that 7 has been entered in the privilege level box.

### TACACS+ – Stanza in Freeware Server

```
Stanza in TACACS+ freeware:
user = seven {
login = cleartext seven
service = exec {
priv-lvl = 7
}
}
```

### Cisco Secure UNIX TACACS+

```
user = seven {
password = clear "seven"
service = shell {
set priv-lvl = 7
}
}
```

### Cisco Secure NT RADIUS

Follow these steps to configure the server.

1. Enter the username and password.
2. In the Group Settings for IETF, Service-type (attribute 6) = **Nas-Prompt**
3. In the CiscoRADIUS area, check **AV-Pair**, and in the rectangular box underneath, enter **shell:priv-lvl=7**.

### Cisco Secure UNIX RADIUS


```
user = seven{
radius=Cisco {
check_items= {
2="seven"
}
reply_attributes= {
6=7
9,1="shell:priv-lvl=7"
}
}
}
```

This is the user file for the username "seven."

**Note:** The server must support Cisco av-pairs.

- seven Password = **passwdxyz**
- Service-Type = **Shell-User**
- cisco-avpair =**shell:priv-lvl=7**

## Related Information

- **RADIUS in IOS Documentation**
- **RADIUS Support Page**
- **Requests for Comments (RFCs)** 
- **TACACS+ in IOS Documentation**
- **TACACS+ Support Page**
- **Documentation for Cisco Secure ACS for UNIX**
- **Cisco Secure UNIX Support Page**
- **Documentation for Cisco Secure ACS for Windows**
- **Cisco Secure ACS for Windows Support Page**
- **Technical Support – Cisco Systems**

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 26, 2008

Document ID: 13860

---