

Cisco IOS Router: Local, TACACS+ and RADIUS authentication of the HTTP connection Configuration Example

Document ID: 13852

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Background Theory

Configure

Configuring Local Authentication for HTTP Server Users

Configuring TACACS+ Authentication for HTTP Server Users

Configuring RADIUS Authentication for HTTP Server Users

Verify

Troubleshoot

Troubleshooting Commands

Related Information

Introduction

This document shows how to configure local, TACACS+, and RADIUS authentication of the HTTP connection. Some relevant debugging commands are also provided.

Before You Begin

Conventions

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

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco IOS® Software Releases 11.2 or later
- Hardware that supports these software revisions

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.

Background Theory

In Cisco IOS® Software Release 11.2, a feature to manage the router through HTTP was added. The "Cisco IOS Web Browser Commands" section of the Cisco IOS Configuration Fundamentals Command Reference includes the following information about this feature.

"The **ip http authentication** command enables you to specify a particular authentication method for HTTP server users. The HTTP server uses the enable password method to authenticate a user at privilege level 15. The **ip http authentication** command now lets you specify enable, local, TACACS, or authentication, authorization, and accounting (AAA) HTTP server user authentication."

Configure

In this section, you are presented with the information to configure the features described in this document.

This document uses the configurations shown below.

- Configuring Local Authentication for HTTP Server Users
- Configuring TACACS+ Authentication for HTTP Server Users
- Configuring RADIUS Authentication for HTTP Server Users

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Configuring Local Authentication for HTTP Server Users

- Router Configurations
- User Results

Router Configurations

Local Authentication with Cisco IOS Software Release 11.2

```
!--- This is the part of the configuration related to local authentication.
!
aaa new-model
aaa authentication login default local
aaa authorization exec local
username one privilege 15 password one
username three password three
username four privilege 7 password four
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to level 7
!
privilege exec level 7 clear line
```

Local Authentication with Cisco IOS Software Releases 11.3.3.T or later

```
!--- This is the part of the configuration
!--- related to local authentication.
```

```

!
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username one privilege 15 password one
username three password three
username four privilege 7 password four
ip http server
ip http authentication local
!
!--- Example of command moved from level 15 (enable) to level 7
!
privilege exec level 7 clear line

```

User Results

These results apply to the users in the previous router configurations.

• User One

- ◆ User will pass web authorization if URL is entered as http://#.#.#.#.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be in enable mode after login (**show privilege** will be 15).
- ◆ If command authorization is added to the router, user will still succeed in all commands.

• User Three

- ◆ User will fail web authorization due to not having a privilege level.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be in non-enable mode after login (**show privilege** will be 1).
- ◆ If command authorization is added to the router, user will still succeed in all commands.

• User Four

- ◆ User will pass web authorization if URL is entered as http://#.#.#.#/level/7/exec.
- ◆ Level 1 commands plus the level 7 **clear line** command will appear.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be at privilege level 7 after login (**show privilege** will be 7)
- ◆ If command authorization is added to the router, user will still succeed in all commands.

Configuring TACACS+ Authentication for HTTP Server Users

- Router Configurations
- User Results
- Freeware Daemon Server Configuration
- Cisco Secure ACS for UNIX Server Configuration
- Cisco Secure ACS for Windows Server Configuration

Router Configurations

Authentication with Cisco IOS Software Release 11.2

```

aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server

```

```
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
```

!--- Example of command moved from level 15 (enable) to level 7

```
privilege exec level 7 clear line
```

Authentication with Cisco IOS Software Releases 11.3.3.T to 12.0.5.T

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
```

!--- Example of command moved from level 15 (enable) to level 7

```
privilege exec level 7 clear line
```

Authentication with Cisco IOS Software Releases 12.0.5.T and Later

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
```

!--- Example of command moved from level 15 (enable) to level 7

```
privilege exec level 7 clear line
```

User Results

The following results apply to the users in the server configurations below.

• User One

- ◆ User will pass web authorization if URL is entered as http://#.#.#.#.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be in enable mode after login (**show privilege** will be 15).
- ◆ If command authorization is added to the router, user will still succeed in all commands.

• User Two

- ◆ User will pass web authorization if URL is entered as http://#.#.#.#.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be in enable mode after login (**show privilege** will be 15).
- ◆ If command authorization is added to the router, user will fail all commands as the server configuration does not authorize them.

• User Three

- ◆ User will fail web authorization due to not having a privilege level.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be in non-enable mode after login (**show privilege** will be 1).
- ◆ If command authorization is added to the router, user will still succeed in all commands.

• User Four

- ◆ User will pass web authorization if URL is entered as http://#.#.#./level/7/exec.
- ◆ Level 1 commands plus the level 7 **clear line** command will appear.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be at privilege level 7 after login (**show privilege** will be 7)
- ◆ If command authorization is added to the router, user will still succeed in all commands.

Freeware Daemon Server Configuration

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure ACS for UNIX Server Configuration

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "*****"
default service=permit
service=shell {
set priv-lvl=15
}
}

# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "*****"
service=shell {
set priv-lvl=15
}
}

# ./ViewProfile -p 9900 -u three
User Profile Information
```

```

user = three{
profile_id = 29
profile_cycle = 1
password = clear "*****"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "*****"
default service=permit
service=shell {
set priv-lvl=7
}
}

```

Cisco Secure ACS for Windows Server Configuration

User One in Group One

- Group Settings
 - ◆ Check **shell (exec)**.
 - ◆ Check **privilege level=15**.
 - ◆ Check **Default (Undefined) Services**.

Note: If this option does not appear, go to **Interface Configuration** and select **TACACS+** and then **Advanced Configuration Options**. Choose **Display enable default (undefined) service** configuration.

- User Settings
 - ◆ Password from whichever database; enter password and confirm in top area.

User Two in Group Two

- Group Settings
 - ◆ Check **shell (exec)**.
 - ◆ Check **privilege level=15**.
 - ◆ Do not check **Default (Undefined) Services**.

- User Settings
 - ◆ Password from whichever database; enter password and confirm in top area.

User Three in Group Three

- Group Settings
 - ◆ Check **shell (exec)**.
 - ◆ Leave **privilege level** blank.
 - ◆ Check **Default (Undefined) Services**.

Note: If this option does not appear, go to **Interface Configuration** and select **TACACS+** and then **Advanced Configuration Options**. Choose **Display enable default (undefined) service** configuration.

- User Settings

- ◆ Password from whichever database; enter password and confirm in top area.

User Four in Group Four

- Group Settings

- ◆ Check **shell (exec)**.
 - ◆ Check **privilege level=7**.
 - ◆ Check **Default (Undefined) Services**.

Note: If this option does not appear, go to **Interface Configuration** and select **TACACS+** and then **Advanced Configuration Options**. Choose **Display enable default (undefined) service** configuration.

- User Settings

- ◆ Password from whichever database; enter password and confirm in top area.

Configuring RADIUS Authentication for HTTP Server Users

- Router Configurations
- User Results
- RADIUS Configuration on Server That Supports Cisco AV-Pairs
- Cisco Secure ACS for UNIX Server Configuration
- Cisco Secure ACS for Windows Server Configuration

Router Configurations

Authentication with Cisco IOS Software Release 11.2

```

aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!

!--- Example of command moved from level 15 (enable) to level 7
!
privilege exec level 7 clear line
radius-server host 171.68.118.101
radius-server key cisco

```

Authentication with Cisco IOS Software Releases 11.3.3.T to 12.0.5.T

```

aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-port 1646
radius-server key cisco
privilege exec level 7 clear line

```

Authentication with Cisco IOS Software Releases 12.0.5.T and Later

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-port 1646
radius-server key cisco
privilege exec level 7 clear line
```

User Results

The following results apply to the users in the server configurations below.

• User One

- ◆ User will pass web authorization if URL is entered as `http://#.#.#.#`.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be in enable mode after login (**show privilege** will be 15).

• User Three

- ◆ User will fail web authorization due to not having a privilege level.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be in non-enable mode after login (**show privilege** will be 1).

• User Four

- ◆ User will pass web authorization if URL is entered as `http://#.#.#.#/level/7/exec`.
- ◆ Level 1 commands plus the level 7 **clear line** command will appear.
- ◆ After Telnet to the router, user can perform all commands after login authentication.
- ◆ User will be at privilege level 7 after login (**show privilege** will be 7)

RADIUS Configuration on Server That Supports Cisco AV-Pairs

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Cisco Secure ACS for UNIX Server Configuration

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
```

```

# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}

```

Cisco Secure ACS for Windows Server Configuration

- User = one, service type (attribute 6) = administrative
- User = three, service type (attribute 6) = login
- User = four, service type (attribute 6) = login, check the Cisco AV-pairs box and enter shell:priv-lvl=7

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The following commands are useful for debugging HTTP authentication. They are issued on the router.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **terminal monitor** – Displays **debug** command output and system error messages for the current terminal and session.
- **debug aaa authentication** – Displays information on AAA/TACACS+ authentication.
- **debug aaa authorization** – Displays information on AAA/TACACS+ authorization.
- **debug radius** – Displays detailed debugging information associated with RADIUS.
- **debug tacacs** – Displays information associated with TACACS.

- **debug ip http authentication** – Use this command to troubleshoot HTTP authentication problems. Displays the authentication method the router attempted and authentication–specific status messages.
-

Related Information

- [Cisco TACACS+ Access Software Support Page](#)
 - [RADIUS Support Page](#)
 - [RADIUS in IOS Documentation](#)
 - [Cisco Secure ACS for Windows Support Page](#)
 - [Documentation for Cisco Secure ACS for Windows](#)
 - [Cisco Secure ACS for UNIX Support Page](#)
 - [Documentation for Cisco Secure ACS for UNIX](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 14, 2009

Document ID: 13852
