# Command Authorization and Privilege Levels for Cisco Secure UNIX

## Contents



## Introduction

This document gives information on how to use authentication, authorization, and accounting (AAA) for centralized shell and command control.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

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

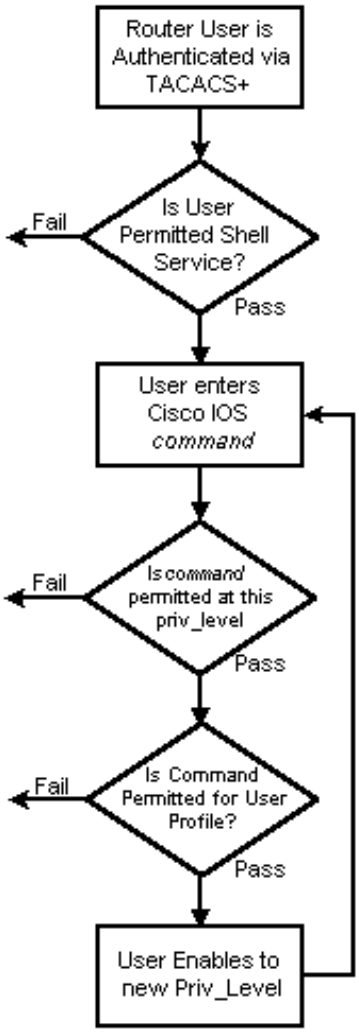
- Cisco IOS® Software Releases 12.0(5)T and later
- Cisco Secure for UNIX 2.3(6)

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.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

# Sample AAA Flow

| | Cisco IOS (AAA Client) | Cisco Secure (AAA Server) |
|---|---|---|
|  | `aaa authentication login default group tacacs+ local` | user=fred { password=des } |
| | `aaa authorization exec default group tacacs+ local` | service-shell { set priv-level=x } |
| | `privilege exec level x command` (See notes below.) | |
| | `aaa authorization commands # default \ group tacacs none`<br>`aaa authorization config-commands` | service=shell { default cmd=(permit/deny) prohibit cmd=x cmd=y{ }} |
| | `enable secretaaa authentication enable default \ group tacacs+ enable` | privilege = des "********" 15 |

# Privilege Levels

By default, there are three command levels on the router:

- privilege level 0 Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands
- privilege level 1 Includes all *user*-level commands at the `router>` prompt
- privilege level 15 Includes all *enable*-level commands at the `router>` prompt

You can move commands around between privilege levels with this command:

`privilege exec level priv-lvl command`

# Console Port Authentication

Console port authorization was not added as a feature until the implementation of Cisco bug ID CSCdi82030 ( registered customers only) . Console port authorization is off by default in order to lessen the likelihood of accidentally being locked out of the router. If a user has physical access to the router via the console, console port authorization is not extremely effective. However, for images in which Cisco bug ID CSCdi82030 is implemented, you can turn on console port authorization under line con 0 with the hidden command **aaa authorization console**.

# Cisco Secure User Profile

This output shows a sample user profile.

```
# ./ViewProfile -p 9900 -u fred
User Profile Information
user = fred{
profile_id = 189
profile_cycle = 1
password = clear "********"
privilege = clear "********" 15
service=shell {
cmd=show {
permit "users"
}
}

}
```

# Router Configuration

```
Partial router configuration:

aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ none
aaa authorization exec default group tacacs+ none
aaa authorization commands 1 default group tacacs+ none
tacacs-server host 172.18.124.113
tacacs-server key cisco
```

# Sample Output

Note that some output is wrapped onto two lines because of spatial considerations.

## AAA Session - User Capture

```
telnet 10.32.1.64
Trying 10.32.1.64...
Connected to 10.32.1.64.
Escape character is '^]'.


User Access Verification

Username: fred
Password:
```

```
vpn-2503>show users
    Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:00:51
*  2 vty 0     fred       idle                 00:00:00 rtp-cherry.cisco.com

  Interface      User        Mode                    Idle     Peer Address

vpn-2503>enable
Password:
vpn-2503#
```

## AAA Session - Cisco IOS Debug

```
vpn-2503#show debug
General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
vpn-2503#terminal monitor
vpn-2503#

!--- In this capture, AAA authentication first tries the TACACS+
!--- server (and goes to local authentication only if the server is down),
!--- as configured in aaa authentication login default group tacacs+ local.

*Mar 15 18:21:25: AAA: parse name=tty3 idb type=-1 tty=-1
*Mar 15 18:21:25: AAA: name=tty3 flags=0x11 type=5 shelf=0 slot=0 adapter=0
   port=3 channel=0
*Mar 15 18:21:25: AAA/MEMORY: create_user (0x524528) user='' ruser='' port='tty3'
   rem_addr='172.18.124.113' authen_type=ASCII service=LOGIN priv=1
*Mar 15 18:21:25: AAA/AUTHEN/START (4191717920): port='tty3' list=''
   action=LOGIN service=LOGIN
*Mar 15 18:21:25: AAA/AUTHEN/START (4191717920): using "default" list
*Mar 15 18:21:25: AAA/AUTHEN/START (4191717920): Method=tacacs+ (tacacs+)

!--- Test TACACS+ for user authentication.

*Mar 15 18:21:25: TAC+: send AUTHEN/START packet ver=192 id=4191717920
*Mar 15 18:21:25: TAC+: Using default tacacs server-group "tacacs+" list.
*Mar 15 18:21:25: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5
*Mar 15 18:21:25: TAC+: Opened TCP/IP handle 0x5475C8 to 172.18.124.113/49
*Mar 15 18:21:25: TAC+: 172.18.124.113 (4191717920) AUTHEN/START/LOGIN/ASCII queued
*Mar 15 18:21:25: TAC+: (4191717920) AUTHEN/START/LOGIN/ASCII processed
*Mar 15 18:21:25: TAC+: ver=192 id=4191717920 received AUTHEN status = GETUSER
*Mar 15 18:21:25: AAA/AUTHEN (4191717920): status = GETUSER
*Mar 15 18:21:27: AAA/AUTHEN/CONT (4191717920): continue_login (user='(undef)')
*Mar 15 18:21:27: AAA/AUTHEN (4191717920): status = GETUSER
*Mar 15 18:21:27: AAA/AUTHEN (4191717920): Method=tacacs+ (tacacs+)
*Mar 15 18:21:27: TAC+: send AUTHEN/CONT packet id=4191717920
*Mar 15 18:21:27: TAC+: 172.18.124.113 (4191717920) AUTHEN/CONT queued
*Mar 15 18:21:27: TAC+: (4191717920) AUTHEN/CONT processed
*Mar 15 18:21:27: TAC+: ver=192 id=4191717920 received AUTHEN status = GETPASS
*Mar 15 18:21:27: AAA/AUTHEN (4191717920): status = GETPASS
*Mar 15 18:21:29: AAA/AUTHEN/CONT (4191717920): continue_login (user='fred')
*Mar 15 18:21:29: AAA/AUTHEN (4191717920): status = GETPASS
*Mar 15 18:21:29: AAA/AUTHEN (4191717920): Method=tacacs+ (tacacs+)
*Mar 15 18:21:29: TAC+: send AUTHEN/CONT packet id=4191717920
*Mar 15 18:21:29: TAC+: 172.18.124.113 (4191717920) AUTHEN/CONT queued
```

```
*Mar 15 18:21:29: TAC+: (4191717920) AUTHEN/CONT processed
*Mar 15 18:21:29: TAC+: ver=192 id=4191717920 received AUTHEN status = PASS
*Mar 15 18:21:29: AAA/AUTHEN (4191717920): status = PASS

!--- TACACS+ passes user authentication. There is a check
!--- to see if shell access is permitted for this user, as configured in
!--- aaa authorization exec default group tacacs+ local.

*Mar 15 18:21:29: TAC+: Closing TCP/IP 0x5475C8 connection to 172.18.124.113/49
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): Port='tty3' list='' service=EXEC
*Mar 15 18:21:29: AAA/AUTHOR/EXEC: tty3 (3409614729) user='fred'
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): send AV service=shell
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): send AV cmd*
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): found list "default"
*Mar 15 18:21:29: tty3 AAA/AUTHOR/EXEC (3409614729): Method=tacacs+ (tacacs+)
*Mar 15 18:21:29: AAA/AUTHOR/TAC+: (3409614729): user=fred
*Mar 15 18:21:29: AAA/AUTHOR/TAC+: (3409614729): send AV service=shell
*Mar 15 18:21:29: AAA/AUTHOR/TAC+: (3409614729): send AV cmd*
*Mar 15 18:21:29: TAC+: using previously set server 172.18.124.113 from group tacacs+
*Mar 15 18:21:29: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5
*Mar 15 18:21:29: TAC+: Opened TCP/IP handle 0x547A10 to 172.18.124.113/49
*Mar 15 18:21:29: TAC+: Opened 172.18.124.113 index=1
*Mar 15 18:21:29: TAC+: 172.18.124.113 (3409614729) AUTHOR/START queued
*Mar 15 18:21:29: TAC+: (3409614729) AUTHOR/START processed
*Mar 15 18:21:29: TAC+: (3409614729): received author response status = PASS_ADD
*Mar 15 18:21:29: TAC+: Closing TCP/IP 0x547A10 connection to 172.18.124.113/49
*Mar 15 18:21:29: AAA/AUTHOR (3409614729): Post authorization status = PASS_ADD
*Mar 15 18:21:29: AAA/AUTHOR/EXEC: Authorization successful
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): Port='tty3' list='' service=CMD

!--- TACACS+ passes exec authorization and wants to perform the
!--- show users command, as configured in
!--- aaa authorization commands 1 default group tacacs+ none.

*Mar 15 18:21:32: AAA/AUTHOR/CMD: tty3 (4185871454) user='fred'
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV service=shell
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV cmd=show
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV cmd-arg=users
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): send AV cmd-arg=
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): found list "default"
*Mar 15 18:21:32: tty3 AAA/AUTHOR/CMD (4185871454): Method=tacacs+ (tacacs+)
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): user=fred
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV service=shell
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV cmd=show
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV cmd-arg=users
*Mar 15 18:21:32: AAA/AUTHOR/TAC+: (4185871454): send AV cmd-arg=
*Mar 15 18:21:32: TAC+: using previously set server 172.18.124.113 from group tacacs+
*Mar 15 18:21:32: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5
*Mar 15 18:21:32: TAC+: Opened TCP/IP handle 0x54F26C to 172.18.124.113/49
*Mar 15 18:21:32: TAC+: Opened 172.18.124.113 index=1
*Mar 15 18:21:32: TAC+: 172.18.124.113 (4185871454) AUTHOR/START queued
*Mar 15 18:21:33: TAC+: (4185871454) AUTHOR/START processed
*Mar 15 18:21:33: TAC+: (4185871454): received author response status = PASS_ADD
*Mar 15 18:21:33: TAC+: Closing TCP/IP 0x54F26C connection to 172.18.124.113/49
*Mar 15 18:21:33: AAA/AUTHOR (4185871454): Post authorization status = PASS_ADD

!--- TACACS+ passes command authorization and wants to
!--- get into enable mode, as configured in
```

```
!--- aaa authentication enable default group tacacs+ enable.

*Mar 15 18:21:34: AAA/MEMORY: dup_user (0x523E58) user='fred' ruser=''
   port='tty3' rem_addr='172.18.124.113' authen_type=ASCII service=ENABLE
   priv=15 source='AAA dup enable'
*Mar 15 18:21:34: AAA/AUTHEN/START (125091438): port='tty3' list=''
   action=LOGIN service=ENABLE
*Mar 15 18:21:34: AAA/AUTHEN/START (125091438): using "default" list
*Mar 15 18:21:34: AAA/AUTHEN/START (125091438): Method=tacacs+ (tacacs+)
*Mar 15 18:21:34: TAC+: send AUTHEN/START packet ver=192 id=125091438
*Mar 15 18:21:34: TAC+: Opening TCP/IP to 172.18.124.113/49 timeout=5
*Mar 15 18:21:34: TAC+: Opened TCP/IP handle 0x54D080 to 172.18.124.113/49
*Mar 15 18:21:34: TAC+: Opened 172.18.124.113 index=1
*Mar 15 18:21:34: TAC+: 172.18.124.113 (125091438) AUTHEN/START/LOGIN/ASCII queued
*Mar 15 18:21:34: TAC+: (125091438) AUTHEN/START/LOGIN/ASCII processed
*Mar 15 18:21:34: TAC+: ver=192 id=125091438 received AUTHEN status = GETPASS
*Mar 15 18:21:34: AAA/AUTHEN (125091438): status = GETPASS
*Mar 15 18:21:37: AAA/AUTHEN/CONT (125091438): continue_login (user='fred')
*Mar 15 18:21:37: AAA/AUTHEN (125091438): status = GETPASS
*Mar 15 18:21:37: AAA/AUTHEN (125091438): Method=tacacs+ (tacacs+)
*Mar 15 18:21:37: TAC+: send AUTHEN/CONT packet id=125091438
*Mar 15 18:21:37: TAC+: 172.18.124.113 (125091438) AUTHEN/CONT queued
*Mar 15 18:21:37: TAC+: (125091438) AUTHEN/CONT processed
*Mar 15 18:21:37: TAC+: ver=192 id=125091438 received AUTHEN status = PASS
*Mar 15 18:21:37: AAA/AUTHEN (125091438): status = PASS
*Mar 15 18:21:37: TAC+: Closing TCP/IP 0x54D080 connection to 172.18.124.113/49
*Mar 15 18:21:37: AAA/MEMORY: free_user (0x523E58) user='fred' ruser=''
   port='tty3' rem_addr='172.18.124.113' authen_type=ASCII service=ENABLE priv=15

!--- TACACS+ passes enable authentication.
```

## AAA Session - Cisco Secure UNIX Debug

```
!
--- In this capture, AAA authentication first tries the TACACS+
!--- server (and goes to local authentication only if the server is down),
!--- as configured in aaa authentication login default group tacacs+ local.

Sep  7 07:22:32 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
   START request (bace1fbf)
Sep  7 07:22:32 rtp-cherry CiscoSecure: DEBUG -
Sep  7 07:22:32 rtp-cherry User Access Verification

!--- Test TACACS+ for user authentication:

Sep  7 07:22:32 rtp-cherry CiscoSecure: DEBUG - Username:
Sep  7 07:22:33 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
   CONTINUE request (bace1fbf)
Sep  7 07:22:33 rtp-cherry CiscoSecure: DEBUG - Password:
Sep  7 07:22:35 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
   CONTINUE request (bace1fbf)
Sep  7 07:22:35 rtp-cherry CiscoSecure: DEBUG - Authentication -
   LOGIN successful; [NAS=10.32.1.64, Port=tty2, User=fred, Priv=1]

!--- TACACS+ passes user authentication. There is a check
!--- to see if shell access is permitted for this user, as configured in
!--- aaa authorization exec default group tacacs+ local.
```

```
   Sep  7 07:22:35 rtp-cherry CiscoSecure: DEBUG -
   Sep  7 07:22:36 rtp-cherry CiscoSecure: DEBUG - AUTHORIZATION request (9ad05c71)
   Sep  7 07:22:36 rtp-cherry CiscoSecure: DEBUG - Authorization - Request authorized;
      [NAS = 10.32.1.64, user = fred, port = tty2, input: service=shell cmd* output: ]

   !--- TACACS+ passes exec authorization and wants to perform the
   !--- show users command, as configured in
   !--- aaa authorization commands 1 default group tacacs+ none.

   Sep  7 07:22:38 rtp-cherry CiscoSecure: DEBUG - AUTHORIZATION request (563ba541)
   Sep  7 07:22:38 rtp-cherry CiscoSecure: DEBUG - Authorization - Request authorized;
      [NAS = 10.32.1.64, user = fred, port = tty2, input: service=shell cmd=show
      cmd-arg=users cmd-arg= output: ]

   !--- TACACS+ passes command authorization and wants to
   !--- get into enable mode, as configured in
   !--- aaa authentication enable default group tacacs+ enable.

   Sep  7 07:22:40 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
      START request (f7e86ad4)
   Sep  7 07:22:40 rtp-cherry CiscoSecure: DEBUG - Password:
   Sep  7 07:22:41 rtp-cherry CiscoSecure: DEBUG - AUTHENTICATION
      CONTINUE request (f7e86ad4)
   Sep  7 07:22:41 rtp-cherry CiscoSecure: DEBUG - Authentication - ENABLE successful;
      [NAS=10.32.1.64, Port=tty2, User=fred, Priv=15]

   !--- TACACS+ passes enable authentication.
```

# Advanced Cisco Secure Profile Examples

| | |
|---|---|
| `group LANadmins{`<br>` service=shell {`<br>` cmd=interface{`<br>`  permit "Ethernet *"`<br>`  deny "Serial *"`<br>` }`<br>` cmd=aaa{`<br>`  deny ".*"`<br>` }`<br>` cmd=tacacs-server{`<br>`  deny ".*"`<br>` }`<br>` default cmd=permit`<br>`}` | This profile allows any user that is a member of group "LANadmins" to log into a router and enter most commands. Users are not allowed to make changes to the serial interface configuration, or to make changes to the AAA config (so they cannot remove the command authorization or disable the TACACS server). |

| | |
|---|---|
| `group Boston_Admins{`<br>` service=shell {`<br>`  allow "10.28.17.1" ".*" ".*"`<br>`  allow bostonswitch ".*" ".*"`<br>`  allow "^bostonrtr[0-9]+" ".*" ".*"`<br>`  set priv-lvl=15`<br>`  default cmd=permit`<br>` }`<br>` service=shell {`<br>`  allow "^NYrouter[0-9]+" ".*" ".*"`<br>`  set priv-lvl=1`<br>`  default cmd=deny`<br>` }`<br>`}` | This profile gives its group members **enable** privileges on the bostonswitch, the *bostonrtr1* - *bostonrtr9* devices, and the 10.28.17.1 device. All commands are permitted for these devices.<br><br>Access to the *NYrouterX* devices is restricted to user exec level only, and all commands are denied if asked for authorization. |
| `group NY_wan_admins{`<br>` service=shell {`<br>`  allow "^NYrouter[0-9]+" ".*" ".*"`<br>`  set priv-lvl=15`<br>`  default cmd=permit`<br>` }`<br>` service=shell {`<br>`  allow "^NYcore$" ".*" ".*"`<br>`  default cmd=permit`<br>`  cmd=interface{`<br>`   permit "Serial 0/[0-9]+"`<br>`   permit "Serial 1/[0-9]+"`<br>`  }`<br>` }`<br>`}` | This group has full access to all NY routers, as well as full access to the NY core router on the Serial 0/x & Serial 1/x interfaces.<br><br>Note that users also have the ability to disable AAA on the core router. |
| `user bob{`<br>` password = des "********"`<br>` privilege = des "********" 15`<br>` member = NY_wan_admins`<br>`}` | This user is a member of the "NY_wan_admins" group and inherits those privileges. This user also has a login password as well as an enable password specified. |

| | |
|---|---|
| `group LAN_support {`<br>` service=shell {`<br>`  default cmd = deny`<br>`  cmd = set{`<br>`  deny "port enable 3/10"`<br>`  permit "port enable *"`<br>`  deny "port disable 3/10"`<br>`  permit "port disable *"`<br>`  permit "port name *"`<br>`  permit "port speed *"`<br>`  permit "port duplex *"`<br>`  permit "vlan [0-9]+ [0-9]+/[0-9]+"`<br>`  deny ".*"`<br>`  }`<br>`  cmd = show{`<br>`  permit ".*"`<br>`  }`<br>`  cmd = enable{`<br>`  permit ".*"`<br>`  }`<br>` }`<br>`}` | This profile is designed for a Catalyst switch. Users are allowed only certain **set** commands. They are not allowed to disable port 3/10 (a trunk port).<br><br>Users are allowed to specify the VLAN a port is assigned to, but all other **set vlan** commands are denied. |

# NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

| NetPro Discussion Forums - Featured Conversations for Security |
|---|
| Security: Intrusion Detection [Systems] |
| Security: AAA |
| Security: General |
| Security: Firewalling |

# Related Information

- **Cisco Secure ACS for UNIX Documentation**
- **Cisco Secure UNIX Product Support**
- **Technical Support & Documentation - Cisco Systems**