

Command Authorization on PIX/ASA 7.x

[1] Configuration on PIX/ASA 7.x :

!—Local user account for fallback purpose

```
username <username> password <password> privilege 15  
username enable_15 password <enable-password> privilege 15
```

```
aaa-server TACACS+ protocol tacacs+  
aaa-server TACACS+ host <ACS-ip-addr> <Shared-Key>
```

```
aaa authentication telnet console TACACS+ LOCAL  
aaa authentication ssh console TACACS+ LOCAL  
aaa authentication serial console TACACS+ LOCAL  
aaa authentication http console TACACS+ LOCAL
```

```
aaa authentication enable console TACACS+ LOCAL
```

```
aaa authorization command TACACS+ LOCAL
```

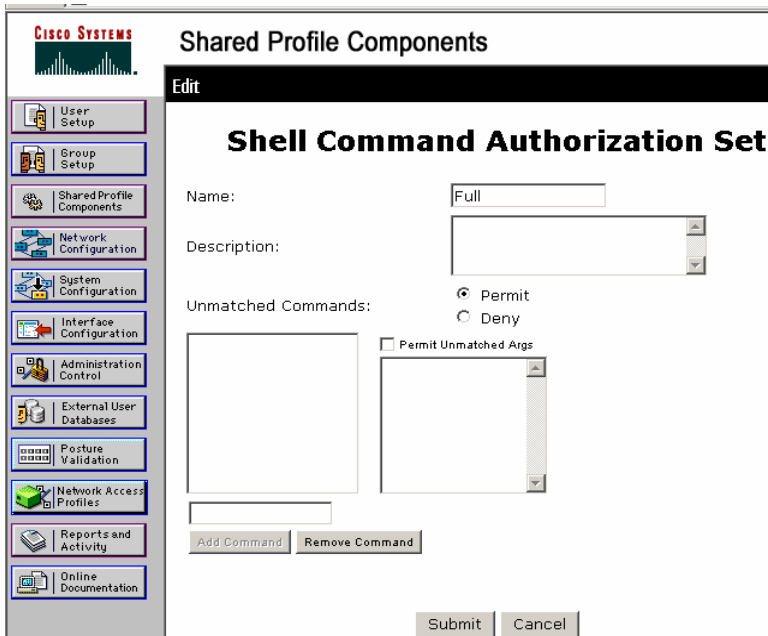
```
aaa accounting telnet console TACACS+  
aaa accounting ssh console TACACS+  
aaa accounting serial console TACACS+  
aaa accounting enable console TACACS+  
aaa accounting command TACACS+
```

[2] Configuration on ACS:

[a] Create Shell Command authorization Set :



[b] One for Full Access:



[c] One for Limited Access:

The screenshot shows the 'Edit' page for a Shell Command Authorization Set named 'Limited'. The interface includes a left-hand navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Shell Command Authorization Set' and contains the following fields and controls:

- Name:** Limited
- Description:** (Empty text area)
- Unmatched Commands:** Radio buttons for Permit and Deny.
- Permit Unmatched Args:** (unchecked)
- Command Lists:** A list on the left contains 'show', 'enable', and 'exit'. A list on the right contains 'permit running-config'.
- Buttons:** 'Add Command' and 'Remove Command' are located below the command lists. 'Submit' and 'Cancel' are at the bottom of the form.

For detail on how to specify command, please refer to link provided below

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysad/min/mgaccess.htm#wp1042042

The screenshot shows the 'Select' page for Shell Command Authorization Sets. The interface is similar to the 'Edit' page, with a left-hand navigation menu. The main content area is titled 'Shell Command Authorization Sets' and contains a table with the following data:

Shell Command Authorization Sets	
Name	Description
Full	
Limited	

[d] Create two users and two groups on ACS from User Setup:

--A group for Full Access:

The screenshot shows the Cisco ACS Group Setup interface. The left sidebar contains navigation icons for User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, and Reports and Activity. The main content area is titled "Group Setup" and has a "Jump To" dropdown menu set to "TACACS+". Below this is a checkbox for "On submit reset all usage counters for all users of this group". The "Enable Options" section is active, showing three radio button options: "No Enable Privilege", "Max Privilege for any AAA Client" (selected), and "Define max Privilege on a per network device group basis". The "Max Privilege for any AAA Client" option has a "Level 15" dropdown menu. Below these options is a table with columns "Device Group" and "Privilege". A "Remove Associate" button is positioned above the table. Below the table, there is a "Device Group" dropdown menu set to "mySwitches" and a "Privilege" dropdown menu set to "Level 0". An "Add Association" button is located at the bottom of this section.

The screenshot shows the Cisco ACS Group Setup interface, similar to the previous one. The "Jump To" dropdown is still set to "TACACS+". The "Shell (exec)" section is expanded, showing several checkboxes and input fields: "Access control list", "Auto command", "Callback line", "Callback rotary", "Idle time", "No callback verify" (with an "Enabled" checkbox), "No escape" (with an "Enabled" checkbox), "No hangup" (with an "Enabled" checkbox), "Privilege level" (set to "15"), and "Timeout". Below this is the "Shell Command Authorization Set" section, which has three radio button options: "None", "Assign a Shell Command Authorization Set for any network device" (selected), and "Assign a Shell Command Authorization Set on a per Network Device Group Basis". The "Assign a Shell Command Authorization Set for any network device" option has a "Full" dropdown menu. Below these options is a table with columns "Device Group" and "Command Set". At the bottom of the page are three buttons: "Submit", "Submit + Restart", and "Cancel".

--A group for Limited Access:

The screenshot shows the Cisco Systems Group Setup interface. The 'Jump To' dropdown is set to 'TACACS+'. The 'On submit reset all usage counters for all users of this group' checkbox is unchecked. The 'Enable Options' section is active, showing three radio button options: 'No Enable Privilege', 'Max Privilege for any AAA Client' (selected), and 'Define max Privilege on a per network device group basis'. The 'Max Privilege for any AAA Client' option has a 'Level 15' dropdown menu. Below this is a table for device group associations:

Device Group	Privilege

Buttons for 'Remove Associate', 'Add Association', and a 'Device Group' dropdown (set to 'mySwitches') with a 'Privilege' dropdown (set to 'Level 0') are visible.

This screenshot shows the same Cisco Systems Group Setup page within a Microsoft Internet Explorer browser window. The address bar shows 'http://192.168.26.10:2004/index2.htm'. The 'Jump To' dropdown is 'TACACS+'. The 'Shell (exec)' section is expanded, showing several options with checkboxes and input fields:

- Shell (exec)
- Access control list
- Auto command
- Callback line
- Callback rotary
- Idle time
- No callback verify
- No escape
- No hangup
- Privilege level
- Timeout

The 'Privilege level' is set to '15'. Below this is the 'Shell Command Authorization Set' section with three radio button options: 'None', 'Assign a Shell Command Authorization Set for any network device' (selected), and 'Assign a Shell Command Authorization Set on a per Network Device Group Basis'. The selected option has a 'Limited' dropdown menu. At the bottom, there are 'Submit', 'Submit + Restart', and 'Cancel' buttons.

--A User for account:

By default a user doesn't have Enable Privileges, and as user setting over takes group setting, so either we can specify the enable privilege per user, or check "Use Group Level Setting". Also, by default for a user, "Use separate password" is checked, and the field is empty. To log in to enable mode, we can choose password of our choice, as in example, the user account is a local user so we have selected same password for enable password.

CISCO SYSTEMS User Setup

TACACS+ Enable Control:

- Use Group Level Setting
- No Enable Privilege
- Max Privilege for any AAA Client
Level 0
- Define max Privilege on a per network device group basis

Device Group	Privilege
--------------	-----------

Remove Associate

Device Group: mySwitches
Privilege: Level 0

Add Association

TACACS+ Enable Password

- Use CiscoSecure PAP password
- Use external database password
Windows Database
- Use separate password
Password: _____
Confirm Password: _____

Submit Cancel

Please go through following link, before applying command authorization :

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm#wp1042042

Please be aware that ASA will not log for show command :

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm#wp1059882

-pbanga@cisco.com