

TACACS and Radius Authentication for Management Login to WLC

Nasir Majeed

Management Login to WLC

- 3 Methods to add users to login to the WLC for management
- Local User on the WLC
- TACACS Account on ACS
- RADIUS Account on ACS

Management Login to WLC using TACACS Account on ACS 4.2

- Configuration of WLC

The screenshot shows a Microsoft Internet Explorer browser window displaying the Cisco WLC configuration page. The address bar shows the URL: `https://192.168.75.44/screens/frameset.html`. The page title is "5508-3 - Microsoft Internet Explorer". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". The address bar contains "Back", "Go", and "Links" buttons. The Cisco logo is visible in the top left corner of the page. The navigation menu includes "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", "HELP", and "FEEDBACK". The "SECURITY" tab is selected. The left sidebar shows the "Security" configuration tree, with "TACACS+" under "AAA" highlighted. The main content area is titled "TACACS+ Authentication Servers > Edit" and contains the following configuration fields:

Server Index	1
Server Address	192.168.150.24
Shared Secret Format	ASCII
Shared Secret	...
Confirm Shared Secret	...
Port Number	49
Server Status	Disabled
Server Timeout	5 seconds

Buttons for "< Back" and "Apply" are located at the top right of the configuration area. The Windows taskbar at the bottom shows the "Internet" icon.

Configure WLC to use TACACS for Login to the GUI of WLC.

- We will need to change the Local Management Authentication on the WLC GUI → Security, as shown below:

The screenshot shows the Cisco WLC GUI interface. The browser address bar displays `https://192.168.75.44/screens/frameset.html`. The navigation menu includes **MONITOR**, **WLANS**, **CONTROLLER**, **WIRELESS**, **SECURITY** (highlighted), **MANAGEMENT**, **COMMANDS**, **HELP**, and **FEEDBACK**. The left sidebar shows the **Security** menu with **Priority Order** highlighted in a red box. The main content area is titled **Priority Order > Management User** and contains an **Authentication** section. Under **Not Used**, there is a dropdown menu with **RADIUS** selected. Under **Order Used for Authentication**, there are two dropdown menus: the first has **TACACS+** selected and is highlighted with a red box, and the second has **LOCAL** selected. **Up** and **Down** buttons are positioned to the right of the dropdowns. A note below the dropdowns states: *If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.*

Management Login to WLC using TACACS Account on ACS 4.2

- Add WLC as AAA client on ACS.

The screenshot shows the CiscoSecure ACS 4.2 web interface in Microsoft Internet Explorer. The browser address bar shows the URL `http://192.168.150.152:20613/index2.htm`. The page title is "Network Configuration".

The main content area is divided into two sections: "Network Device Groups" and "Proxy Distribution Table".

Network Device Groups

Network Device Group	AAA Clients	AAA Servers
(Not Assigned)	2	1

Buttons: Add Entry, Search

Proxy Distribution Table

Character String	AAA Servers	Strip	Account
(Default)	WIRELESS-AD	No	Local

Buttons: Add Entry, Sort Entries

Back to Help

Help

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Editing a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [Searching for Network Devices](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)
- [Editing a Proxy Distribution Table Entry](#)
- [Deleting a Proxy Distribution Table Entry](#)

Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

Network Device Groups

Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default, assigned to the Not Assigned NDG.

To view the AAA Client and AAA Servers

Management Login to WLC using TACACS Account on ACS 4.2

- Click on Add Entry to add the WLC.

The screenshot shows the CiscoSecure ACS 4.2 management interface in Microsoft Internet Explorer. The browser address bar shows the URL <http://192.168.150.152:20613/index2.htm>. The page title is "Network Configuration".

The main content area is titled "Select" and contains two tables under the heading "(Not Assigned) AAA Clients" and "(Not Assigned) AAA Servers".

AAA Clients Table:

AAA Client Hostname	AAA Client IP Address	Authenticate Using
5508-3	192.168.75.44	TACACS+ (Cisco IOS)
wlc	192.168.75.44	RADIUS (IETF)

The "Add Entry" button in this table is highlighted with a red box. Below the table, the text "Step 3" is displayed.

AAA Servers Table:

AAA Server Name	AAA Server IP Address	AAA Server Type
WIRELESS-AD	127.0.0.1	CiscoSecure ACS

Below the servers table are buttons for "Add Entry", "Search", and "Back to Help".

The left sidebar contains navigation links: 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 right sidebar is titled "Help" and contains a list of links: Network Device Groups, Adding a Network Device Group, Editing a Network Device Group, Deleting a Network Device Group, Searching for Network Devices, AAA Clients, Adding a AAA Client, Editing a AAA Client, Deleting a AAA Client, AAA Servers, Adding a AAA Server, Editing a AAA Server, Deleting a AAA Server, Proxy Distribution Table, Adding a Proxy Distribution Table Entry, Sorting Proxy Distribution Table Entries, Editing a Proxy Distribution Table Entry, and Deleting a Proxy Distribution Table Entry.

Below the help links is a "Note" section: "Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table."

Below the note is the "Network Device Groups" section: "Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default, assigned to the Not Assigned NDG."

Below the NDG section is the text: "To view the AAA Client and AAA Servers tables for a particular NDG, click the name of the NDG."

At the bottom of the page, there is a "[Back to Top]" link and a "Cancel" button.

Configure ACS 4.2 Server to Allow TACACS Protocol to login

- Configure the ACS to allow Cisco WLC attribute

192.168.150.152:16481/index2.htm

Interface Configuration

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration** (Step 1)
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

User Data Configuration (Step 2)

- TACACS+ (Cisco IOS)**
- RADIUS (IETF)
- RADIUS (Cisco IOS/PIX 6.0)
- RADIUS (Cisco Aironet)
- RADIUS (Cisco Airespace)
- Advanced Options

[Back to Help](#)

- User Data Configuration
- TACACS+ (Cisco IOS)
- RADIUS (Microsoft)
- RADIUS (Nortel)
- RADIUS (Juniper)
- RADIUS (Ascend)
- RADIUS (IETF)
- RADIUS (Cisco VPN 5000)
- RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
- RADIUS (Cisco BSSM)
- RADIUS (Cisco Aironet)
- RADIUS (Cisco IOS/PIX 6.0)
- RADIUS (3COMUSR)
- Advanced Options

You can configure the ACS web interface pages in the Interface Configuration section.

Note: RADIUS and TACACS+ security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000) only appears once you have configured a AAA client in **Network Configuration** that specifies RADIUS (Cisco VPN 3000) in the **Authenticate Using** list.

User Data Configuration

Click to add or edit up to five user defined fields that will display in the **User Setup** window.

[\[Back to Top\]](#)

TACACS+ (Cisco IOS)

Click to configure TACACS+ options.

[\[Back to Top\]](#)

RADIUS (Microsoft)

Click to configure Microsoft RADIUS options.

[\[Back to Top\]](#)

RADIUS (Nortel)

Click to configure Nortel RADIUS options.

[\[Back to Top\]](#)

RADIUS (Juniper)

Click to configure Juniper RADIUS options.

[\[Back to Top\]](#)

RADIUS (Ascend)

Click to configure Ascend RADIUS options.

Configure ACS 4.2 Server to Allow TACACS Protocol to login

192.168.150.152:16481/index2.htm

CISCO

Interface Configuration

TACACS+ (Cisco)

TACACS+ Services

User Group		Service	Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP	
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX	
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink	
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk	
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN	
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP	
<input type="checkbox"/>	<input type="checkbox"/>	ARAP	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)	
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)	
<input type="checkbox"/>	<input type="checkbox"/>	SLIP	

Step 3

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

Step 4

Advanced Configuration Options

- Advanced TACACS+ Features
- Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings
- Display a window for each service selected in which you can enter customized TACACS+ attributes
- Display enable default (Undefined) service

- [TACACS+ \(Cisco\)](#)
- [Advanced Configuration Options](#)

TACACS+ (Cisco)

Select the check box for either **User** and/or **Group** for each TACACS+ service that you want to appear as a configurable option in the **User Setup** and/or **Group Setup** window, accordingly. For correct operation, each protocol/service must be supported by the NAS. When you have finished selecting options, click **Submit**.

It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, this section enables you to customize the services and protocols that are displayed.

This list has two sections:

- TACACS+ Services.** This section includes the most commonly used services and protocols for TACACS+.
- New Services.** Enter the new services or protocols to add. Select those that should be displayed for configuration under User Setup and/or Group Setup.

Note: If you have configured ACS to interact with management applications for other Cisco products, such as a Management Center for PIX firewalls, ACS may display new TACACS+ services dictated by management applications. To ensure the proper function of ACS, the management applications with which it interacts, and the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

For more information about each attribute, see the [Online Documentation](#).

[\[Back to Top\]](#)

Advanced Configuration Options

The Advanced Configuration Options section lets you add more detailed information for even more tailored configurations. Select the applicable check box to enable the option to be displayed in the applicable setup window.

- Advanced TACACS+ Features.** This option displays or hides the Advanced TACACS+ Options section in the User Setup and Group Setup windows. These options include Privilege Level Authentication and Outbound Password Configuration for SENDPASS ar SENDAUTH clients, such as routers.
- Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings.** If this option is selected, a grid appears in the User Setup window that lets you override the TACACS+ scheduling attributes in the Group Setup window.
- Display a window for each service selected in which you can enter customized TACACS+ attributes.** If this option is selected, an area appears in the User Setup ar Group Setup windows that enables you to enter custom TACACS+ attributes.
- Display enable Default (Undefined) Service Configuration.** If this check box is selected, an area appears in the User Setup and Group Setup> windows that enables you to permit unknown TACACS+ services, such as CDP.

Note: This option should be used by advanced system administrators only.

[\[Back to Top\]](#)

Add Role to the User Group which the ACS user name is tied

- Define group role on ACS.

The screenshot shows the CiscoSecure ACS Group Setup page in Microsoft Internet Explorer. The browser address bar shows the URL `http://192.168.150.152:20613/index2.htm`. The page title is "Group Setup".

The main content area is divided into two sections: "Select" and "Help".

Select Section:

- A dropdown menu labeled "Group" is set to "0: Default Group (1 user)".
- Below the dropdown are three buttons: "Users in Group", "Edit Settings", and "Rename Group".
- A red box highlights the "Edit Settings" button, with a red arrow pointing to it from the text "Step 2".
- Another red box highlights the "Group" dropdown, with a red arrow pointing to it from the text "Step 1".
- A "Back to Help" button is located below the main content area.

Help Section:

- Default Group:** If group mapping has not been configured, usernames that are not configured in the ACS Internal Database are assigned to the Default Group by ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of ACS and kept your database information, users will map as configured in the previous version. [\[Back to Top\]](#)
- Group:** To select a group to configure, use the list to display the configurable groups. Click the group in the list, and then click **Users in Group**, **Edit Settings**, or **Rename Group**. [\[Back to Top\]](#)
- Users in Group:** Click **Users in Group** to see a list of all users assigned to the selected group. [\[Back to Top\]](#)
- Edit Settings:** Click **Edit Settings** to edit the selected group's authorization privileges and parameters. [\[Back to Top\]](#)
- Rename Group:** Click **Rename Group** to assign a new name to the selected group. [\[Back to Top\]](#)

Define Role of the Group on the ACS

- We will need to define the role on the Group of the user.

The screenshot displays the CiscoSecure ACS Group Setup page. The browser window title is "CiscoSecure ACS - Microsoft Internet Explorer" and the address bar shows "http://192.168.150.152:20613/index2.htm".

Group Setup Step 1

Jump To: TACACS+

Unmatched Cisco IOS commands

- Permit
- Deny

Command: []

Arguments: []

Unlisted arguments

- Permit
- Deny

ciscowlc common Step 2

Custom attributes

role1=ALL

IETF RADIUS Attributes

- [006] Service-Type: Authenticate only
- [007] Framed-Protocol: Ascend MPP
- [009] Framed-IP-Netmask: 0.0.0.0

Submit Submit + Restart Cancel Step 3

Help

- [Group Disabled](#)
- [Voice-over-IP \(VoIP\) Support](#)
- [Default Time-of-Day Access Settings](#)
- [Callback](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Enable Options](#)
- [Token Card Settings](#)
- [Password Aging Rules](#)
- [IP Assignment](#)
- [Downloadable ACLs](#)
- [TACACS+ Settings](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:

- A AAA client that uses the specified protocol has been configured in the Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA client that uses RADIUS.
- The specific services, protocols, and attributes have been selected for display for the appropriate protocol in the Interface Configuration section.
- A Token Card Server has been configured in the External User Databases section.

Group Setup is used to enable and configure the particular authorizations assigned to an entire group of users. The group a user is assigned to is configured in the User Setup section. User Setup overrides Group Setup.

[\[Back to Top\]](#)

Group Disabled

When the check box under **Group Disabled** is selected, users assigned to this group, either by manually setting the group in each user profile or by group mapping, are disabled. Authentication or posture validation requests for users belonging to a disabled group are rejected.

Note: Selecting the Group Disabled option does not change the configuration of

Define Role of the Group on the ACS

- Multiple Roles defined for Group

The screenshot displays the CiscoSecure ACS Group Setup interface. The browser window title is "CiscoSecure ACS - Microsoft Internet Explorer". The address bar shows "http://192.168.150.152:20613/index2.htm". The main content area is titled "Group Setup" and includes a "Jump To" dropdown menu set to "TACACS+".

Under "Unmatched Cisco IOS commands", the "Deny" radio button is selected. Below this, there are fields for "Command:" and "Arguments:". Under "Unlisted arguments", the "Deny" radio button is also selected.

The "Attributes" section is checked, and "Custom attributes" are defined as follows:

```
role1=Monitor
role2=WLAN
role3=Wireless
```

The "IETF RADIUS Attributes" section includes the following options:

- [006] Service-Type: Authenticate only
- [007] Framed-Protocol: Ascend MPP
- [009] Framed-IP-Netmask: 0.0.0.0

Buttons at the bottom include "Submit", "Submit + Restart", and "Cancel".

The "Help" sidebar on the right contains a list of links and a detailed explanation of the "Group Disabled" option:

- [Group Disabled](#)
- [Voice-over-IP \(VoIP\) Support](#)
- [Default Time-of-Day Access Settings](#)
- [Callback](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Enable Options](#)
- [Token Card Settings](#)
- [Password Aging Rules](#)
- [IP Assignment](#)
- [Downloadable ACLs](#)
- [TACACS+ Settings](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:

- A AAA client that uses the specified protocol has been configured in the Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA client that uses RADIUS.
- The specific services, protocols, and attributes have been selected for display for the appropriate protocol in the Interface Configuration section.
- A Token Card Server has been configured in the External User Databases section.

Group Setup is used to enable and configure the particular authorizations assigned to an entire group of users. The group a user is assigned to is configured in the User Setup section. User Setup overrides Group Setup.

[\[Back to Top\]](#)

Group Disabled

When the check box under **Group Disabled** is selected, users assigned to this group, either by manually setting the group in each user profile or by group mapping, are disabled. Authentication or posture validation requests for users belonging to a disabled group are rejected.

Note: Selecting the Group Disabled option does not change the configuration of

Debugs on the WLC for TACACS login

- The debug on the WLC for TACACS login is debug aaa tacacs enable.
- The output below shows successful authentication of TACACS user.

(Cisco Controller) >*spamApTask5: Dec 14 12:07:50.989:

spamApTask6: Dec 14 12:07:55.439:

spamApTask4: Dec 14 12:08:01.645:

tplusTransportThread: Dec 14 12:08:02.234: Forwarding request to 192.168.150.152 port=49

tplusTransportThread: Dec 14 12:08:02.236: tplus auth response: type=1 seq_no=2 session_id=e9a68809 length=16 encrypted=0

tplusTransportThread: Dec 14 12:08:02.236: **TPLUS_AUTHEN_STATUS_GETPASS**

tplusTransportThread: Dec 14 12:08:02.236: **auth_cont get_pass reply: pkt_length=28**

tplusTransportThread: Dec 14 12:08:02.236: processTplusAuthResponse: Continue auth transaction

tplusTransportThread: Dec 14 12:08:02.237: tplus auth response: type=1 seq_no=4 session_id=e9a68809 length=6 encrypted=0

tplusTransportThread: Dec 14 12:08:02.237: tplus_make_author_request() from tplus_authen_passed returns rc=0

tplusTransportThread: Dec 14 12:08:02.237: Forwarding request to 192.168.150.152 port=49

tplusTransportThread: Dec 14 12:08:02.245: author response body: status=1 arg_cnt=2 msg_len=0 data_len=0

tplusTransportThread: Dec 14 12:08:02.245: **arg[0] = [14][role1=COMMANDS]**

tplusTransportThread: Dec 14 12:08:02.245: **arg[1] = [16][role2=MANAGEMENT]**

tplusTransportThread: Dec 14 12:08:02.245:

User has the following mgmtRole 180

Debugs on the WLC for TACACS Login

- Unsuccessful TACACS login when the user roles are not defined correctly.

```
(Cisco Controller) >*tplusTransportThread: Dec 14 12:23:12.470: Forwarding request to
  192.168.150.152 port=49
tplusTransportThread: Dec 14 12:23:12.477: tplus auth response: type=1 seq_no=2
  session_id=da5851d2 length=16 encrypted=0
tplusTransportThread: Dec 14 12:23:12.477: TPLUS_AUTHEN_STATUS_GETPASS
tplusTransportThread: Dec 14 12:23:12.477: auth_cont get_pass reply: pkt_length=28
tplusTransportThread: Dec 14 12:23:12.477: processTplusAuthResponse: Continue auth
  transaction
tplusTransportThread: Dec 14 12:23:12.478: tplus auth response: type=1 seq_no=4
  session_id=da5851d2 length=6 encrypted=0
tplusTransportThread: Dec 14 12:23:12.479: tplus_make_author_request() from
  tplus_authen_passed returns rc=0
tplusTransportThread: Dec 14 12:23:12.479: Forwarding request to 192.168.150.152 port=49
tplusTransportThread: Dec 14 12:23:12.481: author response body: status=1 arg_cnt=1
  msg_len=0 data_len=0

tplusTransportThread: Dec 14 12:23:12.481: arg[0] = [14][role1=commands]
tplusTransportThread: Dec 14 12:23:12.481:User has the following mgmtRole 0
```

Debugs on WLC for TACACS Login

- When the user fails authentication, incorrect username and password.

tplusTransportThread: Dec 14 12:32:25.462: Forwarding request to 92.168.150.152 port=49

tplusTransportThread: Dec 14 12:32:25.465: tplus auth response: type=1 seq_no=2
session_id=f7f0855f length=16 encrypted=0

tplusTransportThread: Dec 14 12:32:25.465: TPLUS_AUTHEN_STATUS_GETPASS

tplusTransportThread: Dec 14 12:32:25.465: auth_cont get_pass reply: pkt_length=25

tplusTransportThread: Dec 14 12:32:25.465: processTplusAuthResponse: Continue auth transaction

tplusTransportThread: Dec 14 12:32:25.468: tplus auth response: type=1 seq_no=4
session_id=f7f0855f length=6 encrypted=0

Failed Attempt Log on the ACS 4.2

CiscoSecure ACS - Microsoft Internet Explorer

Address: http://192.168.150.152:28916/index2.htm

Reports and Activity

Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts** *Step 2*
- Logged-in Users *Step 2*
- Disabled Accounts
- ACS Backup And Restore
- RDBMS Synchronization
- Database Replication
- Administration Audit
- User Password Changes
- ACS Service Monitoring
- Entitlement Reports

Failed Attempts active.csv Refresh Download

Regular Expression: Start Date & Time: End Date & Time: Rows per page: 50

Apply Filter Clear Filter

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	Network Access Profile Name	Authen-Failure-Code	Author-Failure-Code	Authen-Data	NAS-Port	NAS-Addr
12/14/2011	10:09:59	Authen failed	admin	Default Group	192.168.1.176	(Default)	ACS password invalid	192.168
12/14/2011	10:09:41	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	10:02:36	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	10:02:06	Authen failed	admin	Default Group	192.168.1.176	(Default)	ACS password invalid	192.168
12/14/2011	10:01:57	Authen failed	admin	Default Group	192.168.1.176	(Default)	ACS password invalid	192.168
12/14/2011	10:00:21	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	10:00:03	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	09:59:55	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168

Back to Help

Management Login to WLC using TACACS Account on ACS 5.x

- Add the WLC as Network Device on ACS 5.x.

The screenshot shows the Cisco Secure ACS 5.x management console. The browser window title is 'Cisco WCS - Login - 192.168.5.100' and the URL is 'https://192.168.150.24/acsadmin/'. The page title is 'Cisco Secure ACS' and the user is logged in as 'ACAdmin'.

The left sidebar shows the navigation menu with 'Network Resources' expanded. A red arrow labeled 'Step 1' points to 'Network Devices and AAA Clients'.

The main content area shows 'Network Resources > Network Devices and AAA Clients'. The 'Network Devices' table is displayed with the following data:

Name	IP / Mask	NDG:Location	NDG:Device Type	Description
5508-3	192.168.75.44/32	All Locations	All Device Types	WW-Wireless LAB WLC 192.168.75.44

A red arrow labeled 'Step 2' points to the 'Create' button at the bottom of the page.

Management Login to WLC using TACACS Account on ACS 5.x

- Add the shared secret on the Radius for WLC.

The screenshot shows the Cisco Secure ACS 5.x configuration interface for a Wireless LAN Controller (WLC). The page is titled "Network Resources > Network Devices and AAA Clients > Create". The configuration fields are as follows:

- Name:** WLC_name (Step 3)
- Description:** Wireless LAN Controller Management Interface (Step 4)
- Network Device Groups:** Location: All Locations, Device Type: All Device Types
- IP Address:** Single IP Address selected, IP: (Step 5)
- Authentication Options:** TACACS+ (Step 6) and RADIUS (Step 7) are selected.

Red arrows and boxes highlight the following steps:

- Step 3:** Name field
- Step 4:** Description field
- Step 5:** IP Address field
- Step 6:** TACACS+ dropdown menu
- Step 7:** RADIUS dropdown menu

Legend: * = Required fields

Buttons: Submit, Cancel

Management Login to WLC using TACACS Account on ACS 5.x

- Create a Local Username on the ACS 5.x to use for WLC login.

The screenshot shows the Cisco Secure ACS 5.x web interface. The left navigation pane has 'Users' highlighted under 'Internal Identity Stores' with a red box and 'Step 1' label. The main content area shows a table of 'Internal Users' with the following data:

Status	User Name	Identity Group	Description
<input type="checkbox"/>	admin	All Groups:Admin	administrator
<input type="checkbox"/>	Joe	All Groups	

At the bottom of the page, the 'Create' button is highlighted with a red box and labeled 'Step 2'.

Management Login to WLC using TACACS Account on ACS 5.x

- Add the user name and password on the ACS.

The screenshot displays the Cisco Secure ACS 5.x web interface for creating a new user. The interface is in a browser window with the URL <https://192.168.150.24/acsadmin/>. The left sidebar shows the navigation menu with 'Users and Identity Stores' selected. The main content area is titled 'Users and Identity Stores > Internal Identity Stores > Users > Create'. The form is divided into three sections:

- General:** Contains fields for Name (nmaheed), Description (Wireless Administrator), Identity Group (All Groups.Admin), and Status (Enabled).
- Password Information:** Contains fields for Password and Confirm Password, both masked with asterisks. There are checkboxes for 'Enable Password Information' and 'Change password on next login'.
- User Information:** A section indicating that there are no additional identity attributes defined for user records.

Red arrows labeled 'Step 3' through 'Step 7' indicate the sequence of actions: Step 3 points to the Name field, Step 4 to the Identity Group dropdown, Step 5 to the Password field, Step 6 to the Confirm Password field, and Step 7 to the Submit button. A legend at the bottom left indicates that a red square icon represents a required field.

Management Login to WLC using TACACS Account on ACS 5.x

- Defining shell properties on ACS server for user created on ACS5.x

The screenshot shows the Cisco Secure ACS 5.x web interface. The browser address bar displays `https://192.168.150.24/acsadmin/`. The left-hand navigation pane is expanded to 'Policy Elements', with 'Shell Profiles' selected under 'Device Administration'. The main content area shows a table of shell profiles. The 'Permit Access' profile is highlighted in green, and its checkbox is checked. Red arrows and text labels indicate the following steps:

- Step 1:** Points to the 'Policy Elements' menu item in the left navigation pane.
- Step 2:** Points to the 'Shell Profiles' menu item in the left navigation pane.
- Step 3:** Points to the checked checkbox for the 'Permit Access' profile.
- Step 4:** Points to the 'Create' button at the bottom of the page.

Name	Description
<input type="checkbox"/> blahblah	
<input checked="" type="checkbox"/> Permit Access	
<input type="checkbox"/> TACACS for WLC	TACACS for WLC
<input type="checkbox"/> TACACS_WLC	TACACS configuration for WLC
<input type="checkbox"/> WLC	wlc tacacs

Buttons at the bottom: Create, Duplicate, Edit, Delete. Page 1 of 1.

Management Login to WLC using TACACS Account on ACS 5.x

Configure the Name of the Profile and description.

The screenshot displays the Cisco Secure ACS 5.x administration interface in a Firefox browser window. The address bar shows the URL `https://192.168.150.24/acsadmin/`. The page title is "Cisco Secure ACS" and the user is logged in as "ACSAadmin" for the "sall-ACS2 (Primary)" instance. The breadcrumb navigation path is "Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Duplicate: 'Permit Access'".

The "General" tab is selected, showing the configuration for a shell profile. The "Name" field is set to "TACACS for WLC" and the "Description" field is set to "TACACS Attributes for WLC". Red arrows point to these fields, with "Step 5" pointing to the Name field and "Step 6" pointing to the Description field. A legend indicates that orange dots next to the field labels denote "Required fields".

The left sidebar contains a navigation menu with the following items: My Workspace, Network Resources, Users and Identity Stores, Policy Elements (highlighted), Session Conditions (Date and Time, Custom), Network Conditions, Authorization and Permissions (Network Access, Device Administration, Shell Profiles, Command Sets, Named Permission Objects), Access Policies, Monitoring and Reports, and System Administration.

At the bottom of the configuration form, there are "Submit" and "Cancel" buttons.

Management Login to WLC using TACACS Account on ACS 5.x

- Define the Role to be Assigned to be assigned.

The screenshot shows the Cisco Secure ACS 5.x web interface. The breadcrumb trail indicates the current location: Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Duplicate: "Permit Access". The interface is divided into a left-hand navigation menu and a main configuration area. The main area has three tabs: General, Common Tasks, and Custom Attributes. The Custom Attributes tab is selected, displaying two tables for attributes. Below the tables are input fields for Attribute, Requirement, and Value. Red arrows and labels indicate the following steps:

- Step 8:** Points to the Attribute input field containing "role1".
- Step 9:** Points to the Requirement dropdown menu set to "Mandatory".
- Step 10:** Points to the Value input field containing "ALL".
- Step 11:** Points to the "Add" button, which is highlighted with a red box.
- Step 12:** Points to the "Submit" button at the bottom of the configuration area.

At the bottom left, there is a legend: = Required fields.

Management Login to WLC using TACACS Account on ACS 5.x

- Define Access Policies on the ACS server for Device configuration in order to pass the Role.

The screenshot displays the Cisco Secure ACS 5.x web interface. The browser address bar shows the URL `https://192.168.150.24/acsadmin/`. The page title is "Cisco Secure ACS". The navigation menu on the left includes "My Workspace", "Network Resources", "Users and Identity Stores", "Policy Elements", "Access Policies", "Access Services", "Service Selection Rules", "Default Device Admin", "Identity", "Authorization", "Default Network Access", "deleteme", "Monitoring and Reports", and "System Administration".

The main content area is titled "Access Policies > Access Services > Service Selection Rules". It shows a table of "Service Selection Policy" rules. The table has columns for "Status", "Name", "Protocol", "Conditions", "Results", and "Hit Count".

Status	Name	Protocol	Conditions	Results	Hit Count
<input type="checkbox"/>	Rule-1	match Radius		Default Network Access	1436
<input checked="" type="checkbox"/>	Rule-2	match Tacacs		Default Device Admin	283
<input type="checkbox"/>	Default	If no rules defined or no enabled rule matches.		DenyAccess	0

Red arrows indicate the following steps:

- Step 1:** Points to the "Access Policies" menu item in the left navigation pane.
- Step 2:** Points to the "Service Selection Rules" menu item in the left navigation pane.
- Step 3:** Points to the "Save Changes" button at the bottom of the page.

At the bottom of the interface, there are buttons for "Create...", "Duplicate...", "Edit", "Delete", "Move to...", "Customize", and "Hit Count".

Management Login to WLC using TACACS Account on ACS 5.x

- Create a new Authorization Policy to add the Shell Policy we created earlier along with the User group which we want to allow using the TACACS profile.

The screenshot displays the Cisco Secure ACS 5.x web interface in a Firefox browser. The browser address bar shows the URL `https://192.168.150.24/acsadmin/`. The interface includes a navigation sidebar on the left with the following menu items: My Workspace, Network Resources, Users and Identity Stores, Policy Elements, Access Policies (highlighted with a red arrow and labeled "Step 1"), Access Services, Service Selection Rules, Default Device Admin, Identity, Authorization (highlighted with a red arrow and labeled "Step 2"), Default Network Access, delete me, Monitoring and Reports, and System Administration. The main content area shows the breadcrumb path: `Access Policies > Access Services > Default Device Admin > Authorization`. Below this, there are tabs for "Standard Policy" and "Exception Policy". The "Device Administration Authorization Policy" section includes a filter bar with "Status" set to "Enabled" and a "Go" button. A table with columns for Status, Name, Identity Group, NDG:Location, NDG:Device Type, Time And Date, Results, and Hit Count is shown, with the text "No data to display" below it. At the bottom, a table row shows a policy named "Default" with the condition "if no rules defined or no enabled rule matches.", the result "TACACS for WLC", and a hit count of "0". A red arrow labeled "Step 3" points to the "Create..." button. Other buttons include "Duplicate...", "Edit", "Delete", "Move to...", "Customize", "Hit Count", "Save Changes", and "Discard Changes".

Management Login to WLC using TACACS Account on ACS 5.x

- Define the Group which the user is part of along with the Shell profile we want to allow for the user name to be applied.

Cisco Secure ACS - Mozilla Firefox

192.168.150.24 https://192.168.150.24/acsadmin/PolicyInputAction.do

General
Name: Rule-1 Status: Enabled **Step 4**

Conditions
 Identity Group: in | All Groups:Admin **Select** **Step 5**
 NDG:Location: -ANY-
 NDG:Device Type: -ANY-
 Time And Date: -ANY-

Results
Shell Profile: WLC **Select** **Step 6**

OK Cancel Help

Management Login to WLC using TACACS Account on ACS 5.x

- The shell profile is seen after in the new Policy created.

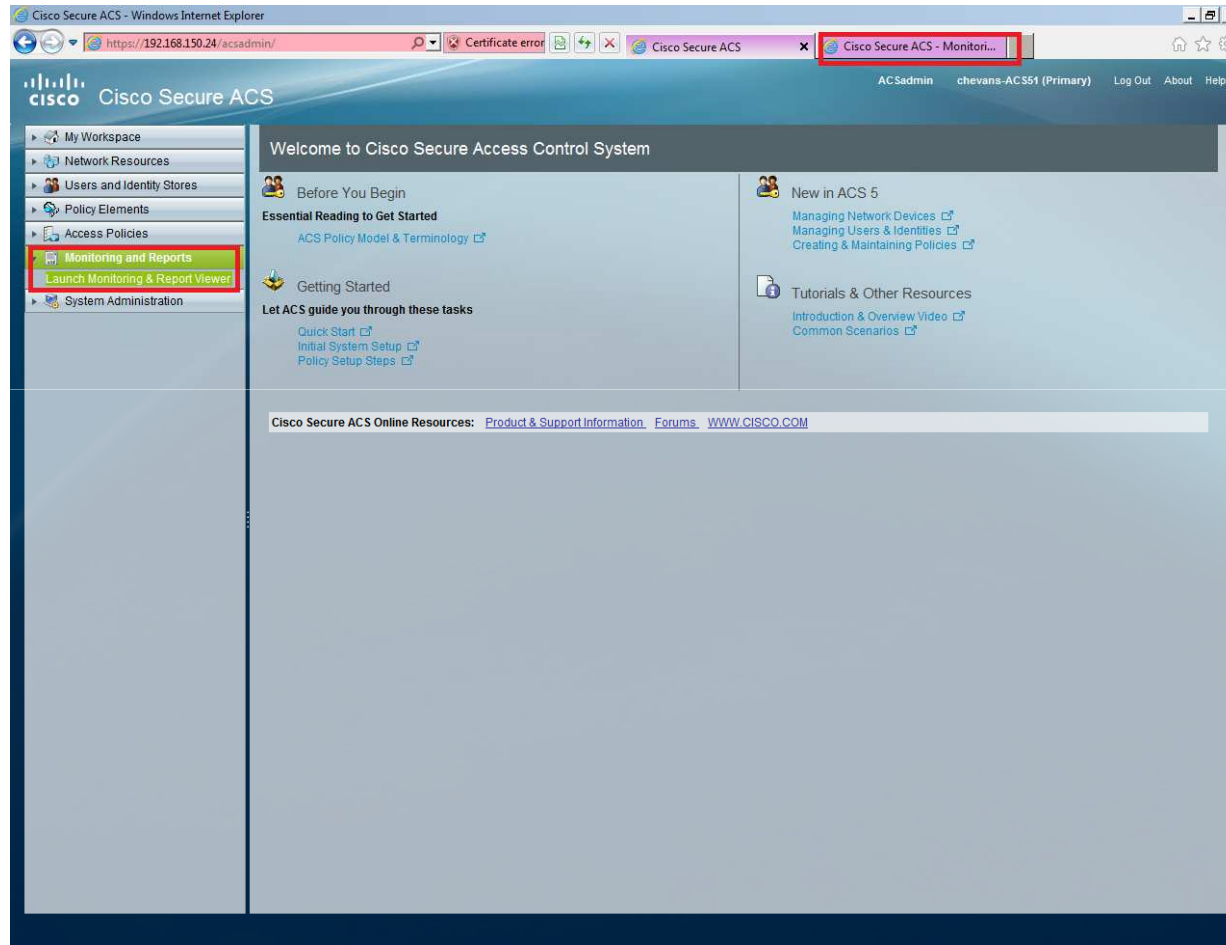
The screenshot shows the Cisco Secure ACS 5.x web interface in Microsoft Internet Explorer. The browser address bar shows `https://192.168.150.24/acsadmin/`. The page title is "Cisco Secure ACS". The navigation menu on the left includes "My Workspace", "Network Resources", "Users and Identity Stores", "Policy Elements", "Access Policies", "Access Services", "Monitoring and Reports", and "System Administration". The "Access Policies" section is expanded, showing "Service Selection Rules", "Default Device Admin", "Authorization", "Default Network Access", and "Identity".

The main content area displays the "Device Administration Authorization Policy" configuration. The "Filter" section shows "Status" set to "All" and "Match if" set to "Equals". The "Conditions" table is as follows:

	Status	Name	Identity Group	NDG:Location	NDG:Device Type	Time And Date	Results	Hit Count
1	<input type="checkbox"/>	Rule-1	In All Groups:Admin	In All Locations	In All Device Types	-ANY-	Shell Profile WLC	22

At the bottom of the table, there is a "Default" rule with the description "If no rules defined or no enabled rule matches." and a "Permit Access" result with a hit count of 0. The interface includes buttons for "Create...", "Duplicate...", "Edit", "Delete", "Move to...", "Save Changes", "Discard Changes", "Customize", and "Hit Count".

Failed Attempt Log on the ACS 5.x



Failed Attempt Log on ACS 5.x

The screenshot shows the Cisco Secure ACS View monitoring interface. The browser address bar indicates the URL <https://192.168.150.24/acsview/>. The dashboard is titled "Cisco Secure ACS View" and includes a navigation menu on the left with options like "Monitoring and Reports", "Alarms", "Reports", and "Monitoring Configuration".

The main content area is divided into several sections:

- Dashboard:** Includes tabs for "General", "Troubleshooting", "Authentication Trends", and "ACS Health".
- Top 5 Alarms:** A table showing the most recent alarms. The "Minimum Severity: Info" section contains the following data:

Severity	Name	Date	Cause
Critical	ACS - System Errors	Sat Jan 07 19:56:00	Alarm caused by ACS - System Errors threshold
Critical	ACS - System Errors	Wed Nov 16 01:08:00	Alarm caused by ACS - System Errors threshold
Critical	ACS - System Errors	Tue Jul 05 21:18:00	Alarm caused by ACS - System Errors threshold
Critical	ACS - System Errors	Tue Jul 05 21:10:00	Alarm caused by ACS - System Errors threshold
Info	System Alarm [Database Purging]	Tue May 31 04:00:22	Database Purge finished
- My Favorite Reports:** A table listing frequently accessed reports. The "Authentications - TACACS - Today" report is highlighted with a red box. The table contains the following data:

Favorite Name	Report Name	Report Type
ACS - Configuration Audit - Today	ACS Instance>ACS_Configuration_Audit	System Report
ACS - System Errors - Today	ACS Instance>ACS_System_Diagnostics	System Report
Authentications - RADIUS - Today	AAA Protocol>RADIUS_Authentication	System Report
Authentications - RADIUS - Yesterday	AAA Protocol>RADIUS_Authentication	System Report
Authentications - TACACS - Today	AAA Protocol>TACACS_Authentication	System Report
Authentications - TACACS - Yesterday	AAA Protocol>TACACS_Authentication	System Report

At the bottom of the page, a JavaScript snippet is visible: `javascript:openReport('/avreports/executereport.do?rptFailureReason=&rptAuthenticationStatus=...`

Management Login to WLC using TACACS Account on ACS 5.x

- The debug on the WLC show the same output regardless of the ACS server version being used.

```
debug aaa tacacs enable
```

```
portThread: Dec 14 14:29:16.090: Forwarding request to 192.168.150.24 port=49
```

```
tplusTransportThread: Dec 14 14:29:16.092: tplus auth response: type=1 seq_no=2 session_id=48f1bb06  
length=16 encrypted=0
```

```
tplusTransportThread: Dec 14 14:29:16.092: TPLUS_AUTHEN_STATUS_GETPASS
```

```
tplusTransportThread: Dec 14 14:29:16.092: auth_cont get_pass reply: pkt_length=28
```

```
tplusTransportThread: Dec 14 14:29:16.092: processTplusAuthResponse: Continue auth transaction
```

```
tplusTransportThread: Dec 14 14:29:16.095: tplus auth response: type=1 seq_no=4 session_id=48f1bb06  
length=6 encrypted=0
```

```
tplusTransportThread: Dec 14 14:29:16.095: tplus_make_author_request() from tplus_authen_passed  
returns rc=0
```

```
tplusTransportThread: Dec 14 14:29:16.095: Forwarding request to 192.168.150.24 port=49
```

```
tplusTransportThread: Dec 14 14:29:16.098: author response body: status=1 arg_cnt=1 msg_len=0  
data_len=0
```

```
tplusTransportThread: Dec 14 14:29:16.098: arg[0] = [9][role1=ALL]
```

Management Login to WLC using ACS server

- We can also use Radius server for management user login to WLC GUI.
- Using the Radius is not much granular control as using TACACS, where we can define the user roles on the ACS server.

Management Login to WLC using ACS 4.2 server

- We can use the IETF Radius attribute Service-Type to authenticate users to login WLC GUI.
- The main type of attributes are Administrative, NAS Prompt, and Callback Administrative.
- Administrative is for logging into the WLC with full access to WLC.
- NAS prompt will give read only access to the user.
- Callback Administrator will give Lobby Ambassador Privilege to user.

Management Login to WLC using ACS

- We will need to change the Local Management Authentication on the WLC GUI → Security, as shown below:

The screenshot shows the Cisco WLC GUI interface. The browser address bar displays the URL `https://192.168.75.44/screens/frameset.html`. The navigation menu includes **MONITOR**, **WLANS**, **CONTROLLER**, **WIRELESS**, **SECURITY** (highlighted), **MANAGEMENT**, **COMMANDS**, **HELP**, and **FEEDBACK**. The **SECURITY** section is expanded, showing a tree view with **AAA**, **RADIUS**, **Local EAP**, **Priority Order** (highlighted with a red box), **Certificate**, **Access Control Lists**, **Wireless Protection Policies**, **Web Auth**, and **Advanced**. The **Priority Order** sub-section is expanded to show **Management User**. The main content area is titled **Priority Order > Management User** and includes an **Apply** button. Under the **Authentication** heading, there are two sections: **Not Used** and **Order Used for Authentication**. The **Not Used** section contains a dropdown menu with **TACACS+** selected. The **Order Used for Authentication** section contains a dropdown menu with **RADIUS LOCAL** selected (highlighted with a red box), and **Up** and **Down** buttons. A note below the dropdowns states: *If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.*

Adding WLC as NAS device on ACS 4.2

- The WLC will be added to ACS 4.2 with Authenticate using Radius Cisco Airspace as shown below:

Network Configuration

AAA Client Setup for WLC

AAA Client IP Address: 192.168.75.44

Shared Secret: cisco123

Network Device Group: (Not Assigned)

RADIUS Key Wrap

Key Encryption Key: 00000000000000000000000000000000

Message Authenticator Code Key: 00000000000000000000000000000000

Key Input Format: ASCII Hexadecimal

Authenticate Using: RADIUS (Cisco Airspace)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Buttons: Submit, Submit + Apply, Delete, Delete + Apply, Cancel, Back to Help

AAA Client IP Address

Type the IP address information for this AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.

[\[Back to Top\]](#)

Shared Secret

Type the shared secret that the TACACS+ or RADIUS AAA client and ACS use to encrypt the data. The shared secret must be configured in the AAA client and ACS identically, including case sensitivity.

[\[Back to Top\]](#)

Network Device Groups

From the list, click the name of the Network Device Group (NDG) to which this AAA client belongs.

Note: To enable NDGs, click **Interface Configuration: Advanced Options: Network Device Groups**.

[\[Back to Top\]](#)

RADIUS Key Wrap

Enter the shared secret keys for RADIUS

Management Login to WLC using ACS 4.2 server

- Select the User Group in which the user name is added on ACS.

192.168.150.152:16481/index2.htm

Google

Group Setup

- 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
- Online Documentation

Group : 1: Group 1 (1 user)

Users in Group Edit Settings Rename Group

Back to Help

- [Default Group](#)
- [Group](#)
- [Users in Group](#)
- [Edit Settings](#)
- [Rename Group](#)

Default Group

If group mapping has not been configured, usernames that are not configured in the ACS Internal Database are assigned to the Default Group by ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of ACS and kept your database information, users will map as configured in the previous version.

[\[Back to Top\]](#)

Group

To select a group to configure, use the list to display the configurable groups. Click the group in the list, and then click **Users in Group**, **Edit Settings**, or **Rename Group**.

[\[Back to Top\]](#)

Users in Group

Click **Users in Group** to see a list of all users assigned to the selected group.

[\[Back to Top\]](#)

Edit Settings

Click **Edit Settings** to edit the selected group's authorization privileges and parameters.

[\[Back to Top\]](#)

Rename Group

Click **Rename Group** to assign a new name to the selected group.

[\[Back to Top\]](#)

Management Login to WLC using ACS 4.2 server

- Select IETF Radius attributes from the drop down, first attribute 006 is Service-Type which we can configure to give Read only, Read-Write and Lobby Ambassador value.

The screenshot shows the Cisco Group Setup configuration page for IETF RADIUS Attributes. The browser address bar shows the URL 192.168.150.152:16481/index2.htm. The page title is "Group Setup" and the sub-header is "Jump To: RADIUS (IETF)".

The main configuration area is titled "IETF RADIUS Attributes" and contains a list of attributes with checkboxes and various input fields. The following attributes are visible:

- [006] Service-Type: Administrative (Step 5)
- [007] Framed-Protocol: Ascend MPP
- [009] Framed-IP-Netmask: 0.0.0.0
- [010] Framed-Routing: None
- [011] Filter-Id
- [012] Framed-MTU (64..65535): 64
- [013] Framed-Compression: None
- [014] Login-IP-Host: 0.0.0.0 (NAS Specifies)
- [015] Login-Service: Telnet
- [016] Login-TCP-Port (0..65535): 0
- [018] Reply-Message

On the right side, there is a list of links for additional configuration options, including "Group Disabled", "Voice-over-IP (VoIP) Support", "Default Time-of-Day Access Settings", "Callback", "Network Access Restrictions", "Max Sessions", "Usage Quotas", "Enable Options", "Token Card Settings", "Password Aging Rules", "IP Assignment", "Downloadable ACLs", "TACACS+ Settings", "TACACS+ Shell Command Authorization", "Command Authorization for Network Device Management Applications", "TACACS+ Unknown Services", "IETF RADIUS Attributes", and "RADIUS Vendor-Specific Attributes".

Below the links, there is a section titled "Group Disabled" with a paragraph explaining its function and a "Note" about its effect on user accounts. There is also a "Voice-over-IP (VoIP) Support" section with a paragraph explaining its function.

Checking ACS 4.2 Logs for failed attempts

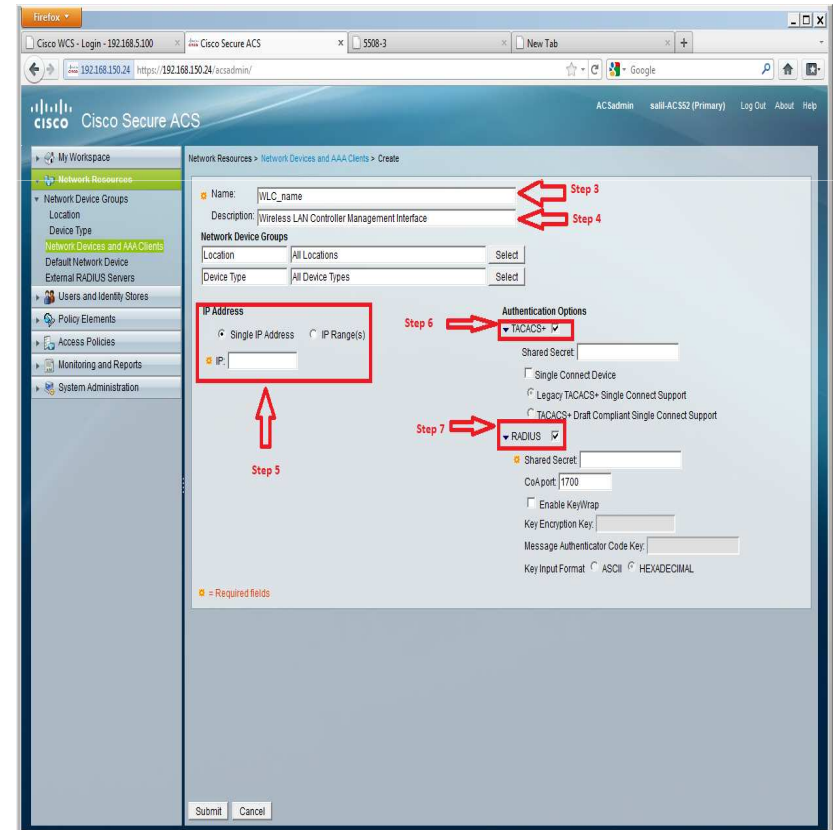
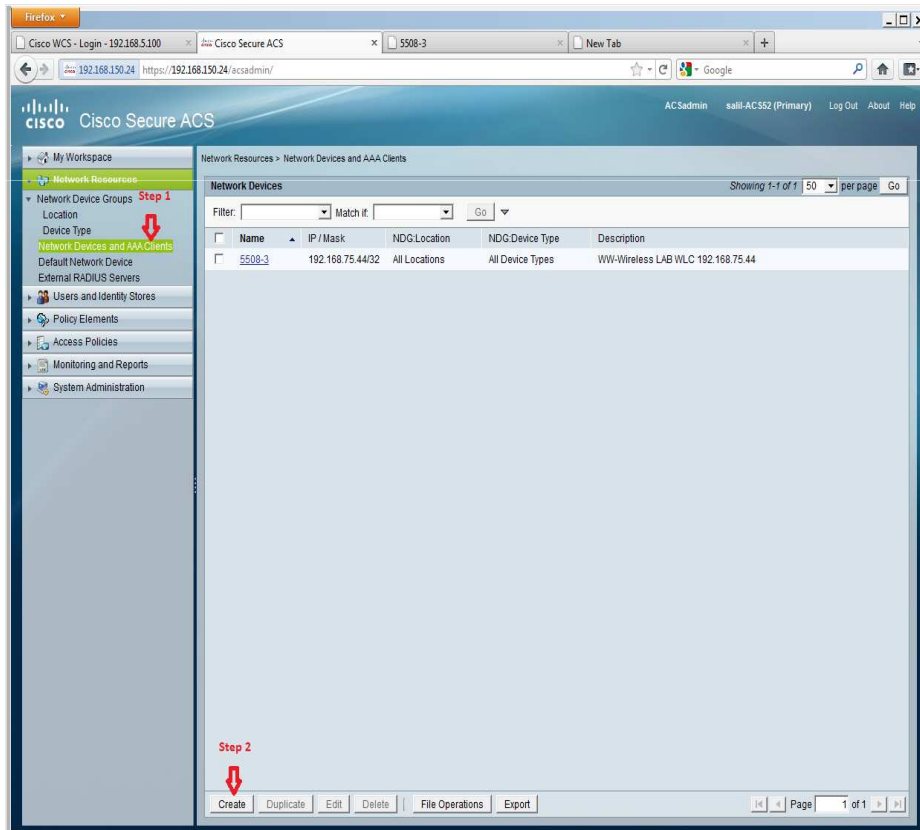
The screenshot shows the CiscoSecure ACS 4.2 web interface in Microsoft Internet Explorer. The browser address bar shows `http://192.168.150.152:28916/index2.htm`. The page title is "CiscoSecure ACS - Microsoft Internet Explorer". The main content area is titled "Reports and Activity" and contains a "Select" dropdown menu. Below this, there is a "Reports" section with a list of report types, including "Failed Attempts" which is highlighted with a red box and labeled "Step 2".

The "Failed Attempts active.csv" report is displayed in a table format. The table has the following columns: Date, Time, Message-Type, User-Name, Group-Name, Caller-ID, Network Access Profile Name, Authen-Failure-Code, Author-Failure-Code, Author-Data, NAS-Port, and NAS-Addr. The table contains 10 rows of data, all showing "Authen failed" messages from various users (admin, cisco) on 12/14/2011.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	Network Access Profile Name	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port	NAS-Addr
12/14/2011	10:09:59	Authen failed	admin	Default Group	192.168.1.176	(Default)	ACS password invalid	192.168
12/14/2011	10:09:41	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	10:02:36	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	10:02:06	Authen failed	admin	Default Group	192.168.1.176	(Default)	ACS password invalid	192.168
12/14/2011	10:01:57	Authen failed	admin	Default Group	192.168.1.176	(Default)	ACS password invalid	192.168
12/14/2011	10:00:21	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	10:00:03	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168
12/14/2011	09:59:55	Authen failed	cisco	Default Group	192.168.1.176	(Default)	External DB user invalid or bad password	192.168

Adding WLC as NAS device on ACS 5.x

- The WLC will be added to ACS 4.2 with Authenticate using Radius Cisco Airspace as shown below:



Management Login to WLC using ACS 5.x server

- The same concept applies here where can have to configure the ACS 5.x server to push the Radius attributes after successful user authentication.

The screenshot displays the Cisco Secure ACS 5.x web interface in a Windows Internet Explorer browser. The browser's address bar shows the URL `https://192.168.150.24/acsadmin/`. The interface includes a navigation menu on the left and a main content area for configuring Authorization Profiles.

Navigation Menu (Left):

- My Workspace
- Network Resources
- Users and Identity Stores
- Policy Elements** (Step 1)
- Session Conditions
 - Date and Time
 - Custom
- Network Conditions
- Authorization and Permissions**
 - Network Access**
 - Authorization Profiles** (Step 2)
 - Device Administration
 - Named Permission Objects
 - Access Policies
- Monitoring and Reports
- System Administration

Main Content Area (Right):

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles

Showing 1-2 of 2 | 50 per page | Go

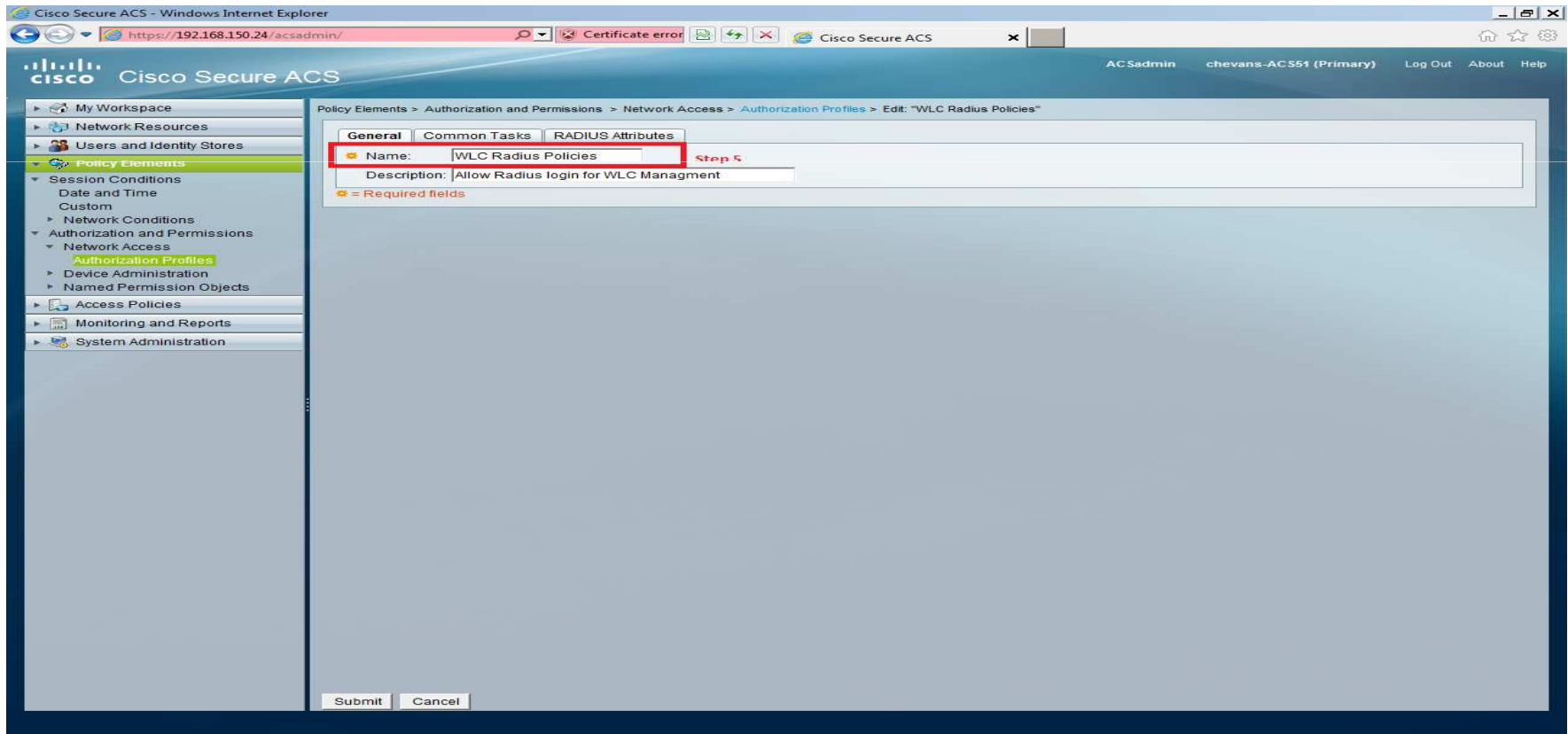
<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	Permit Access	
<input type="checkbox"/>	WLC Radius Policies	Allow Radius login for WLC Managment

Buttons (Bottom): Create, **Duplicate** (Step 4), Edit, Delete

Page 1 of 1

Management Login to WLC using ACS 5.x server

- When we duplicate the policies the screen will look as below which is where I can give the policy name and also define different Radius Attributes.



Management Login to WLC using ACS 5.x server

- On the Radius attributes tab, we can define different attributes.

The screenshot shows the Cisco Secure ACS 5.x web interface. The browser address bar indicates the URL <https://192.168.150.24/acsadmin/>. The page title is "Cisco Secure ACS" and the user is logged in as "ACSAdmin" on the "chevans-ACS51 (Primary)" server. The navigation menu on the left includes "My Workspace", "Network Resources", "Users and Identity Stores", "Policy Elements", "Session Conditions", "Authorization and Permissions", "Access Policies", "Monitoring and Reports", and "System Administration". The "Policy Elements" section is expanded to show "Authorization Profiles". The main content area is titled "Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: 'WLC Radius Policies'". The "RADIUS Attributes" tab is selected, and the "Common Tasks Attributes" table is empty. The "Manually Entered" table contains one entry: "Service-Type" with Type "Enumeration" and Value "Administrative". Below the tables are buttons for "Add A", "Edit V", "Replace A", and "Delete". The "Dictionary Type" is set to "RADIUS-IETF". The "RADIUS Attribute" is "Service-Type", the "Attribute Type" is "Enumeration", and the "Attribute Value" is "Administrative". Red boxes and labels highlight the "RADIUS Attributes" tab (Step 6), the "Dictionary Type" dropdown (Step 7), the "RADIUS Attribute" dropdown (Step 8), and the "Attribute Value" dropdown (Step 9). A legend at the bottom left indicates that an asterisk (*) denotes required fields. "Submit" and "Cancel" buttons are at the bottom.

Attribute	Type	Value
Service-Type	Enumeration	Administrative

Dictionary Type: RADIUS-IETF (Step 7)

RADIUS Attribute: Service-Type (Step 8)

Attribute Type: Enumeration

Attribute Value: Administrative (Step 9)

* = Required fields

Management Login to WLC using ACS 5.x server

- Step 8, select the Radius attribute Service Type.

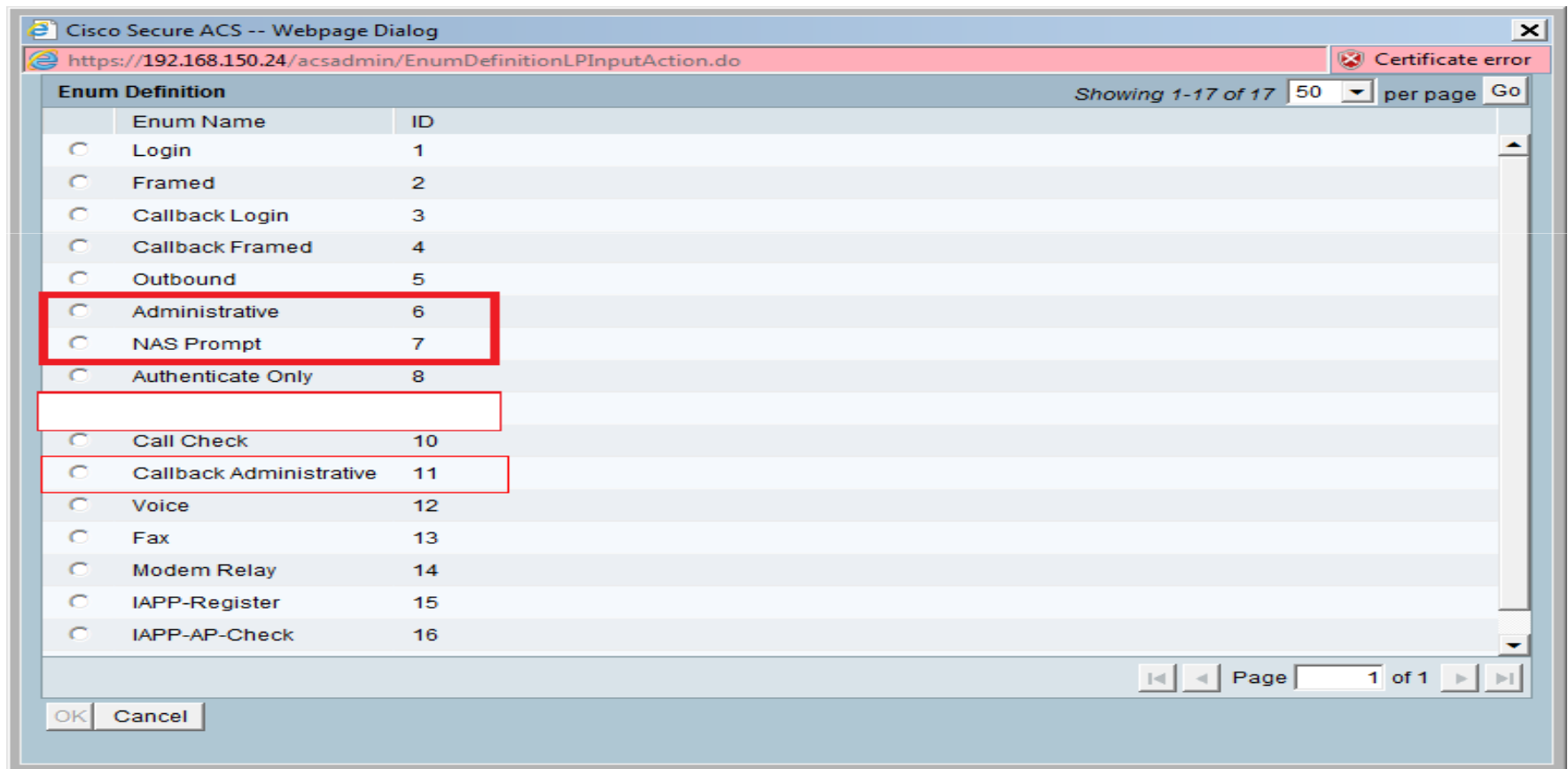
The screenshot shows a web browser window titled "Cisco Secure ACS -- Webpage Dialog" with the URL <https://192.168.150.24/acsadmin/DictionaryRadiusLPInputAction.do?contextData.externalFilter=available=true=boolean||dire>. The page displays a "RADIUS Dictionary" table with the following columns: Attribute, ID, Type, Direction, and Multiple Allowed. The "Service-Type" row is highlighted with a red border.

Attribute	ID	Type	Direction	Multiple Allowed
<input type="radio"/> Port-Limit	62	Unsigned Integer 32	BOTH	false
<input type="radio"/> Reply-Message	18	String	OUTBOUND	true
<input type="radio"/> Service-Type	6	Enumeration	BOTH	false
<input type="radio"/> Session-Timeout	27	Unsigned Integer 32	OUTBOUND	false
<input type="radio"/> State	24	String	BOTH	false
<input type="radio"/> Termination-Action	29	Enumeration	OUTBOUND	false
<input type="radio"/> Tunnel-Assignment-ID	82	Tagged String	OUTBOUND	true
<input type="radio"/> Tunnel-Client-Auth-ID	90	Tagged String	BOTH	true
<input type="radio"/> Tunnel-Client-Endpoint	66	Tagged String	BOTH	true
<input type="radio"/> Tunnel-Medium-Type	65	Tagged Enum	BOTH	true
<input type="radio"/> Tunnel-Password	69	Tagged String	OUTBOUND	true
<input type="radio"/> Tunnel-Preference	83	Tagged Integer 32	BOTH	true
<input type="radio"/> Tunnel-Private-Group-ID	81	Tagged String	BOTH	true
<input type="radio"/> Tunnel-Server-Auth-ID	91	Tagged String	BOTH	true

At the bottom of the dialog, there are "OK", "Cancel", and "Help" buttons. The page navigation shows "Page 1 of 1".

Management Login to WLC using ACS 5.x server

- Step 9, select the value such as Administrative or other attribute as defined in slide 29 to give Read only access, Read-Write Access or Lobby Admin Access.



Management Login to WLC using ACS 5.x server

- After defining the Radius Attributes, we have to apply these attributes into Device Access policy on the ACS 5.x.

The screenshot shows the Cisco Secure ACS 5.x web interface. The browser address bar displays `https://192.168.150.24/acsadmin/`. The page title is "Cisco Secure ACS". The navigation tree on the left includes "Access Policies" (Step 1), "Access Services", "Default Device Admin", "Default Network Access" (Step 2), "Identity", "Authorization" (Step 3), "deleteme", "Monitoring and F", and "System Administration".

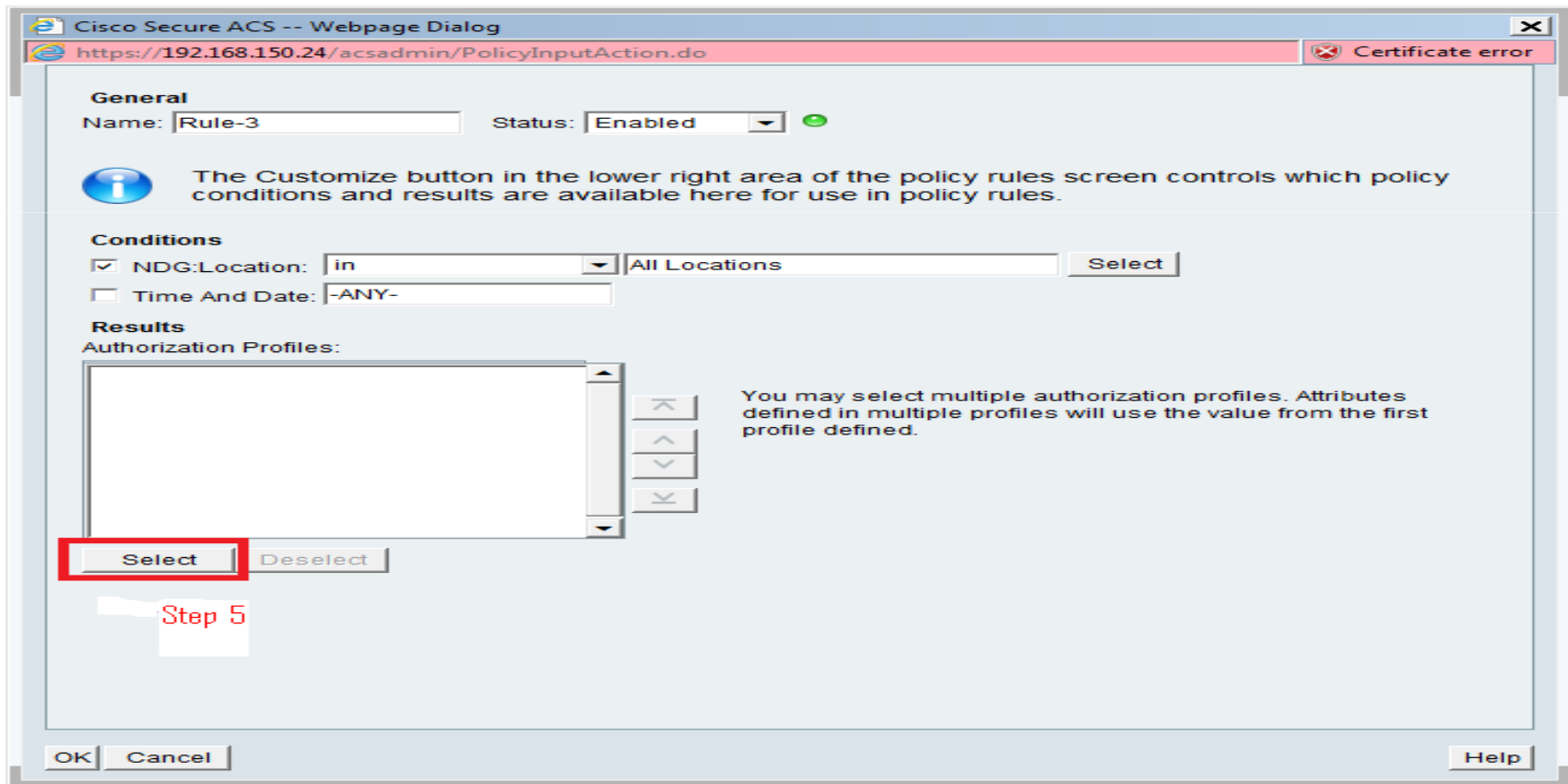
The main content area shows the configuration for a "Network Access Authorization Policy". The breadcrumb trail is "Access Policies > Access Services > Default Network Access > Authorization". The policy name is "Rule-1". The table below shows the policy details:

	Status	Name	NDG:Location	Conditions	Time And Date	Results	Authorization Profiles	Hit Count
1	<input checked="" type="checkbox"/>	Rule-1	in All Locations	-ANY-		WLC Radius Policies		67

At the bottom of the table, there is a "Default" row with a "Create..." button (Step 4), "Duplicate...", "Edit", "Delete", and "Move to..." buttons. The "Default" row shows "If no rules defined or no enabled rule matches." and "Permit Access" with a hit count of 0. The "Create..." button is highlighted with a red box.

Management Login to WLC using ACS 5.x server

- Select the WLC Access Policy which we defined under Policy Elements with the Radius Attributes for the user group to login.



Management Login to WLC using ACS 5.x server

- We select the Policy Element which we created to be applied in this Rule.

The screenshot displays the Cisco Secure ACS Administration Console interface. The browser address bar shows the URL `https://192.168.150.24/acsadmin/NetworkAccessLPInputAction.do`. The page title is "Authorization Profiles". A "Certificate error" warning is visible in the top right corner. The main content area shows a table of authorization profiles with the following entries:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DenyAccess	
<input type="checkbox"/>	Permit Access	
<input checked="" type="checkbox"/>	WLC Radius Policies	Allow Radius login for WLC Management

A red box highlights the "WLC Radius Policies" row, and a white callout box labeled "Step 6" points to it. At the bottom of the interface, there are buttons for "Create", "Duplicate", "Edit", "Delete", "OK", "Cancel", and "Help". The "OK" button is highlighted with a red box, and a white callout box labeled "Step 7" points to it. The bottom right corner shows "Page 1 of 1".

Checking failed logs on ACS 5.x

The screenshot shows the Cisco Secure ACS View web interface. The browser tab is labeled "Cisco Secure ACS V 5.2". The interface displays the "Monitoring and Reports" section, specifically the "Alarms" view. The "Top 5 Alarms" table is visible, showing several "ACS - System Errors" and one "System Alarm [Database Purging]". The "My Favorite Reports" table is also visible, listing various reports, with "Authentications - RADIUS - Today" highlighted.

Severity	Name	Date	Cause
Critical	ACS - System Errors	Sat Jan 07 19:56:00	Alarm caused by ACS - System Errors threshold
Critical	ACS - System Errors	Wed Nov 16 01:08:00	Alarm caused by ACS - System Errors threshold
Critical	ACS - System Errors	Tue Jul 05 21:18:00	Alarm caused by ACS - System Errors threshold
Critical	ACS - System Errors	Tue Jul 05 21:10:00	Alarm caused by ACS - System Errors threshold
Information	System Alarm [Database Purging]	Tue May 31 04:00:22	Database Purge finished

Favorite Name	Report Name	Report Type
ACS - Configuration Audit - Today	ACS Instance>ACS_Configuration_Audit	System Report
ACS - System Errors - Today	ACS Instance>ACS_System_Diagnostics	System Report
Authentications - RADIUS - Today	AAA Protocol>RADIUS_Authentication	System Report
Authentications - RADIUS - Yesterday	AAA Protocol>RADIUS_Authentication	System Report
Authentications - TACACS - Today	AAA Protocol>TACACS_Authentication	System Report
Authentications - TACACS - Yesterday	AAA Protocol>TACACS_Authentication	System Report

Debug From the WLC when using Radius for Authentication of user

- The output of debugs on the WLC whether using ACS 4.2 or 5.x is the same as below.

debug aaa all enable

```
*aaaQueueReader: Jan 09 10:50:49.194: Callback.....0x108f11e0
*aaaQueueReader: Jan 09 10:50:49.194: protocolType.....0x00020021
*aaaQueueReader: Jan 09 10:50:49.194: proxyState.....00:00:00:0E:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.194: Packet contains 5 AVPs (not shown)
*aaaQueueReader: Jan 09 10:50:49.195: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Jan 09 10:50:49.195: 00:00:00:0e:00:00 Successful transmission of Authentication Packet (id 148) to 192.168.150.24:1812, proxy state 00:00:00:0e:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.195: 00000000: 01 94 00 41 00 00 00 00 00 00 00 00 00 00 00 00 ...A.....
*aaaQueueReader: Jan 09 10:50:49.195: 00000010: 00 00 00 00 01 07 63 69 73 63 6f 02 12 cc 28 41 .....cisco...(A
*aaaQueueReader: Jan 09 10:50:49.195: 00000020: ab 74 b9 56 0b 11 bc 9a 5d 59 ed ca 23 06 06 00 .t.V....]Y..#...
*aaaQueueReader: Jan 09 10:50:49.195: 00000030: 00 00 07 04 06 c0 a8 4b 2c 20 08 35 35 30 38 2d .....K,..5508-
*aaaQueueReader: Jan 09 10:50:49.195: 00000040: 33 3
*radiusTransportThread: Jan 09 10:50:49.198: 00000000: 02 94 00 43 a8 0f 69 59 2f e8 4b 67 e5 ef 10 d0 ...C..iY/..Kg....
*radiusTransportThread: Jan 09 10:50:49.198: 00000010: 57 90 8b 68 01 07 63 69 73 63 6f 06 06 00 00 00 W..h..cisco.....
*radiusTransportThread: Jan 09 10:50:49.198: 00000020: 06 19 22 43 41 43 53 3a 63 68 65 76 61 6e 73 2d .."CACs:chevans-
*radiusTransportThread: Jan 09 10:50:49.198: 00000030: 41 43 53 35 31 2f 31 31 35 32 33 32 30 34 39 2f ACS51/115232049/
*radiusTransportThread: Jan 09 10:50:49.198: 00000040: 31 30 33 103
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: 00:00:00:0e:00:00 Access-Accept received from RADIUS server 192.168.150.24 for mobile 00:00:00:0e:00:00 received = 0
*radiusTransportThread: Jan 09 10:50:49.198: AuthorizationResponse: 0x14afbb40
*radiusTransportThread: Jan 09 10:50:49.198: structureSize.....121
*radiusTransportThread: Jan 09 10:50:49.198: resultCode.....0
*radiusTransportThread: Jan 09 10:50:49.198: protocolUsed.....0x00000001
*radiusTransportThread: Jan 09 10:50:49.198: proxyState.....00:00:00:0E:00:00-00:00
*radiusTransportThread: Jan 09 10:50:49.198: Packet contains 3 AVPs:
*radiusTransportThread: Jan 09 10:50:49.198: AVP[01] User-Name.....cisco (5 bytes)
*RADIUSTRANSPORTTHREAD: JAN 09 10:50:49.198: AVP[02] SERVICE-TYPE.....0X00000006 (6) (4 BYTES)
*radiusTransportThread: Jan 09 10:50:49.198: AVP[03] Class.....CACs:chevans-ACS51/115232049/103 (32 bytes)
*emWeb: Jan 09 10:50:49.198: Authentication succeeded for cisco
```


Debug From the WLC when using Radius for Authentication of user

- Failed user login:
aaaQueueReader: Jan 09 10:42:00.622: 00:00:00:05:00:00 Successful transmission of Authentication Packet (id 139) to 192.168.150.24:1812, proxy state 00:00:00:05:00:00-00:00
- *radiusTransportThread: Jan 09 10:42:00.626: ****Enter processIncomingMessages: response code=3
- *radiusTransportThread: Jan 09 10:42:00.626: ****Enter processRadiusResponse: response code=3
- *radiusTransportThread: Jan 09 10:42:00.626: 00:00:00:05:00:00 Access-Reject received from RADIUS server 192.168.150.24 for mobile 00:00:00:05:00:00 receiveId = 0

- *radiusTransportThread: Jan 09 10:42:00.627: 00:00:00:05:00:00 Returning AAA Error 'Authentication Failed' (-4) for mobile 00:00:00:05:00:00
- *emWeb: Jan 09 10:42:00.628: Authentication failed for admin
- aaaQueueReader: Jan 09 10:42:14.905: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
- *aaaQueueReader: Jan 09 10:42:14.905: 00:00:00:06:00:00 Successful transmission of Authentication Packet (id 140) to 192.168.150.24:1812, proxy state 00:00:00:06:00:00-00:00
- *radiusTransportThread: Jan 09 10:42:14.909: ****Enter processIncomingMessages: response code=3
- *radiusTransportThread: Jan 09 10:42:14.909: ****Enter processRadiusResponse: response code=3
- *radiusTransportThread: Jan 09 10:42:14.909: **00:00:00:06:00:00 Access-Reject received from RADIUS server 192.168.150.24 for mobile 00:00:00:06:00:00 receiveId = 0**
- *radiusTransportThread: Jan 09 10:42:14.910: 00:00:00:06:00:00 Returning AAA Error 'Authentication Failed' (-4) for mobile 00:00:00:06:00:00
- *emWeb: Jan 09 10:42:14.910: Authentication failed for admin

Debug From the WLC when using Radius for Authentication of user

- User passes authentication from Radius but the Attribute is not correct:

```
*aaaQueueReader: Jan 09 10:50:49.194: Callback.....0x108f11e0
*aaaQueueReader: Jan 09 10:50:49.194: protocolType.....0x00020021
*aaaQueueReader: Jan 09 10:50:49.194: proxyState.....00:00:00:0E:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.194: Packet contains 5 AVPs (not shown)
*aaaQueueReader: Jan 09 10:50:49.195: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Jan 09 10:50:49.195: 00:00:00:0e:00:00 Successful transmission of Authentication Packet (id 148) to 192.168.150.24:1812, proxy state
00:00:00:0e:00:00-00:00
*aaaQueueReader: Jan 09 10:50:49.195: 00000000: 01 94 00 41 00 00 00 00 00 00 00 00 00 00 00 00 ...A.....
*aaaQueueReader: Jan 09 10:50:49.195: 00000010: 00 00 00 00 01 07 63 69 73 63 6f 02 12 cc 28 41 .....cisco...(A
*aaaQueueReader: Jan 09 10:50:49.195: 00000020: ab 74 b9 56 0b 11 bc 9a 5d 59 ed ca 23 06 06 00 .t.V....]Y..#...
*aaaQueueReader: Jan 09 10:50:49.195: 00000030: 00 00 07 04 06 c0 a8 4b 2c 20 08 35 35 30 38 2d .....K,..5508-
*aaaQueueReader: Jan 09 10:50:49.195: 00000040: 33
3
*radiusTransportThread: Jan 09 10:50:49.198: 00000000: 02 94 00 43 a8 0f 69 59 2f e8 4b 67 e5 ef 10 d0 ...C..iY/.Kg....
*radiusTransportThread: Jan 09 10:50:49.198: 00000010: 57 90 8b 68 01 07 63 69 73 63 6f 06 06 00 00 00 W..h..cisco.....
*radiusTransportThread: Jan 09 10:50:49.198: 00000020: 06 19 22 43 41 43 53 3a 63 68 65 76 61 6e 73 2d .."CACS:chevans-
*radiusTransportThread: Jan 09 10:50:49.198: 00000030: 41 43 53 35 31 2f 31 31 35 32 33 32 30 34 39 2f ACS51/115232049/
*radiusTransportThread: Jan 09 10:50:49.198: 00000040: 31 30 33
103
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Jan 09 10:50:49.198: 00:00:00:0e:00:00 Access-Accept received from RADIUS server 192.168.150.24 for mobile
00:00:00:0e:00:00 receiveId = 0
*radiusTransportThread: Jan 09 10:50:49.198: AuthorizationResponse: 0x14afbb40
*radiusTransportThread: Jan 09 10:50:49.198: structureSize.....121
*radiusTransportThread: Jan 09 10:50:49.198: resultCode.....0
*radiusTransportThread: Jan 09 10:50:49.198: protocolUsed.....0x00000001
*radiusTransportThread: Jan 09 10:50:49.198: proxyState.....00:00:00:0E:00:00-00:00
*radiusTransportThread: Jan 09 10:50:49.198: Packet contains 3 AVPs:
*radiusTransportThread: Jan 09 10:50:49.198: AVP[01] User-Name.....cisco (5 bytes)
*radiusTransportThread: Jan 09 10:50:49.198: AVP[03] Class.....CACS:chevans-ACS51/115232049/103 (32 bytes)
*emWeb: Jan 09 10:50:49.198: Authentication succeeded for cisco
```

Common Troubleshooting issues

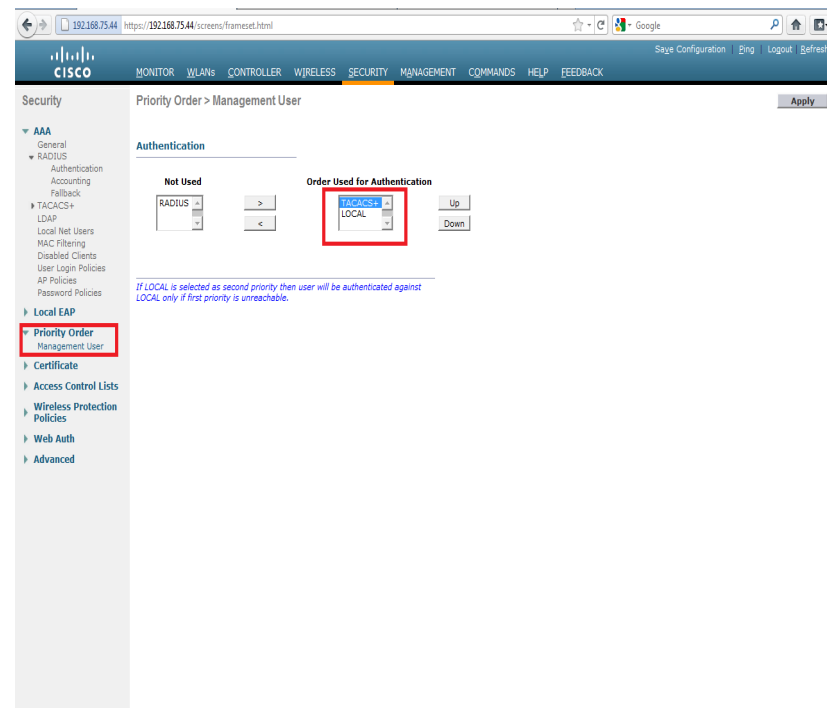
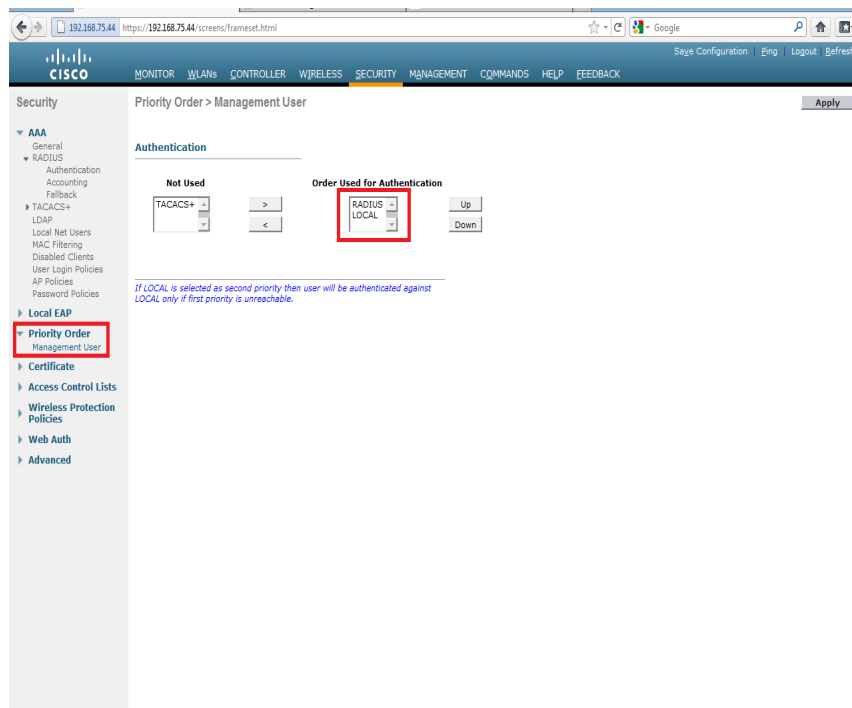
- Usually we see the issue with TACACS login when the role is not defined correctly on the ACS server. The role has to be from the first bar on the WLC as shown below.

The screenshot shows the Cisco WLC Monitor interface. The navigation bar at the top includes tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. The MONITOR tab is selected. The main content area is divided into several sections:

- Controller Summary:** Management IP Address: 192.168.75.44, Service Port IP Address: 0.0.0.0, Software Version: 7.0.220.0, Field Recovery Image Version: 6.0.182.0, License Level: base, System Name: 5508-3, Up Time: 2 days, 21 hours, 5 minutes, System Time: Mon Jan 9 10:23:57 2012, Internal Temperature: +39 C, 802.11a Network State: Enabled, 802.11b/g Network State: Enabled, Local Mobility Group: goa, CPU(s) Usage: 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/1%, 0%/0%, 0%/0%, 0%/0%, Individual CPU Usage: 0%/0%, Memory Usage: 43%.
- Rogue Summary:** Active Rogue APs: 0, Active Rogue Clients: 0, Adhoc Rogues: 0, Rogues on Wired Network: 0.
- Top WLANs:** Profile Name vs # of Clients table.
- Most Recent Traps:** Link Up: Slot: 0 Port: 2 Admin Status: Enable Oper Status: Link Up, Link Up: Slot: 0 Port: 2 Admin Status: Enable Oper Status: Link Up, Link Up: Slot: 0 Port: 2 Admin Status: Enable Oper Status: Link Up, Link Up: Slot: 0 Port: 2 Admin Status: Enable Oper Status: Link Up, Data path to mobility member 192.168.159.10 is up.
- Access Point Summary:** Table with columns Total, Up, Down, and Detail. All values are 0.
- Client Summary:** Section header.

Troubleshooting

- Always try to have a backup entry such as WCS or Console session into the WLC before changing the priority on the WLC from Local to TACACS or Radius.



Troubleshooting

- Show tacacs auth statistics, show tacacs acct statistics and show tacacs athr statistics are helpful commands to see any passed and failed attempts.

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:
Server Index..... 1
Server Address..... 192.168.150.24
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
Server Index..... 2
Server Address..... 192.168.150.152
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

- A new bug on 7.0.220.0 where the AAA queue is full due to which the authentication to the WLC GUI via TACACS is not possible.
- Bug id is : CSCtx03556, we see the TPLUS Transmission Queue is full– Dropping Accounting Packet when running aaa debug on the WLC.

Some Useful Links for Radius and TACACS Login

http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a0080871921.shtml

http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a0080782507.shtml

http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_tech_note09186a0080851f7c.shtml

http://www.cisco.com/en/US/docs/wireless/wcs/7.0/configuration/guide/7_0admin.html#wpmkr1064294