

RADIUS Server Authentication of Management Users on the Controller Configuration Example

Document ID: 71989

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations
- WLC Configuration
- ACS Configuration
- Manage the WLC Locally as well as Through the RADIUS Server

Verify

Troubleshoot

Related Information

Introduction

This document explains how to configure a Wireless LAN Controller (WLC) and an Access Control Server (ACS) so that the AAA server can authenticate management users on the controller. The document also explains how different management users can receive different privileges using Vendor-specific Attributes (VSAs) returned from the Cisco Secure ACS RADIUS server.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure basic parameters on WLCs
- Knowledge of how to configure a RADIUS server like the Cisco Secure ACS

Components Used

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

- Cisco 2006 Wireless LAN Controller that runs version 4.0.179.11
- A Cisco Secure ACS that runs software version 3.2 and is used as a RADIUS server in this configuration.

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 Cisco Technical Tips Conventions for more information on document conventions.

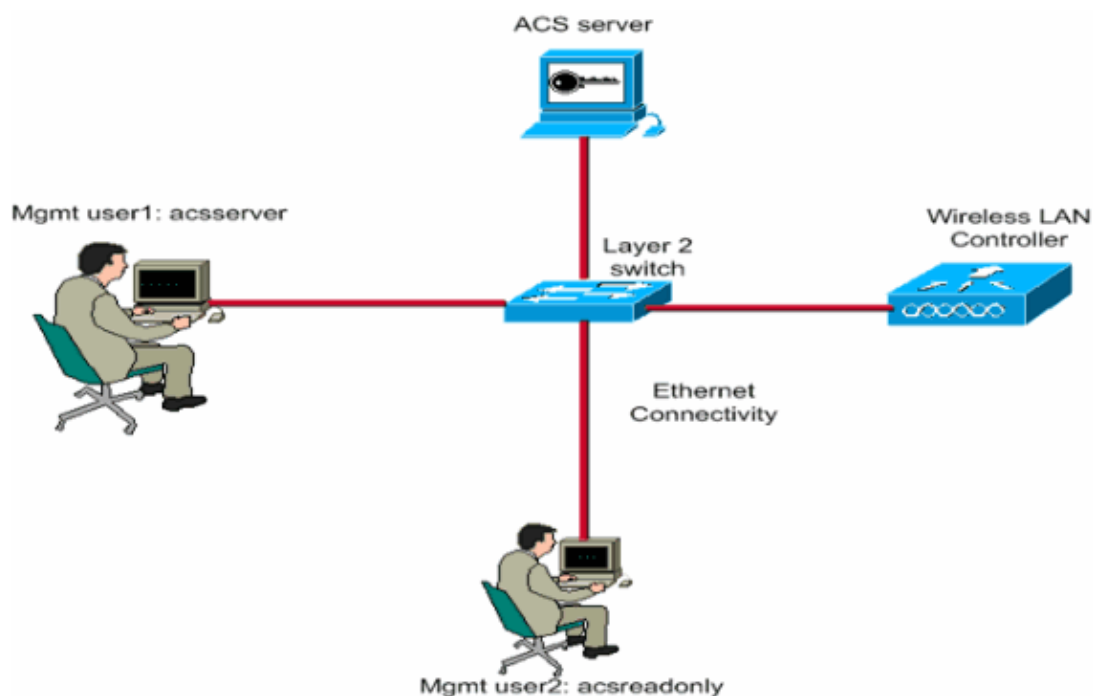
Configure

In this section, you are presented with the information on how to configure the WLC and the ACS for the purpose described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



This configuration example uses these parameters:

- IP address of the ACS;72.16.1.1/255.255.0.0
- Management interface IP address of the controller;72.16.1.30/255.255.0.0
- Shared secret key that is used on the access point (AP) and the RADIUS server cisco
- These are the credentials of the two users that this example configures on the ACS:

- ◆ Username – acsreadwrite

- Password – acsreadwrite

- ◆ Username – acsreadonly

- Password – acsreadonly

This configuration is in such a way that:

- Any user who logs into the WLC with the username and password as **acsreadwrite** is given full administrative access to the WLC.
- Any user who logs into the WLC with the username and password as **acsreadonly** is given read-only access to the WLC.

Configurations

This document uses these configurations:

- WLC Configuration
- ACS Configuration

WLC Configuration

In order to perform RADIUS authentication, for controller login and management, ensure that the **Admin-auth-via-RADIUS** flag is enabled on the controller.

This can be verified from the output of the **show radius summary** command. This output provides an example:

```
(Cisco Controller) >show radius summary
Vendor Id Backward Compatibility.....Disabled
Credentials Caching.....Disabled
Call Station Id Type.....IP Address
Administrative Authentication via RADIUS.....Disabled
Aggressive Failover.....Enabled
Keywrap.....Disabled
```

The highlighted information in the **show radius summary** output shows that administrative authentication via RADIUS is currently disabled. In order to enable it, issue the **config radius admin-authentication enable** command from the WLC CLI.

The **config radius admin-authentication enable** command enables administrative authentication via RADIUS. You can now configure the RADIUS server to manage WLC users.

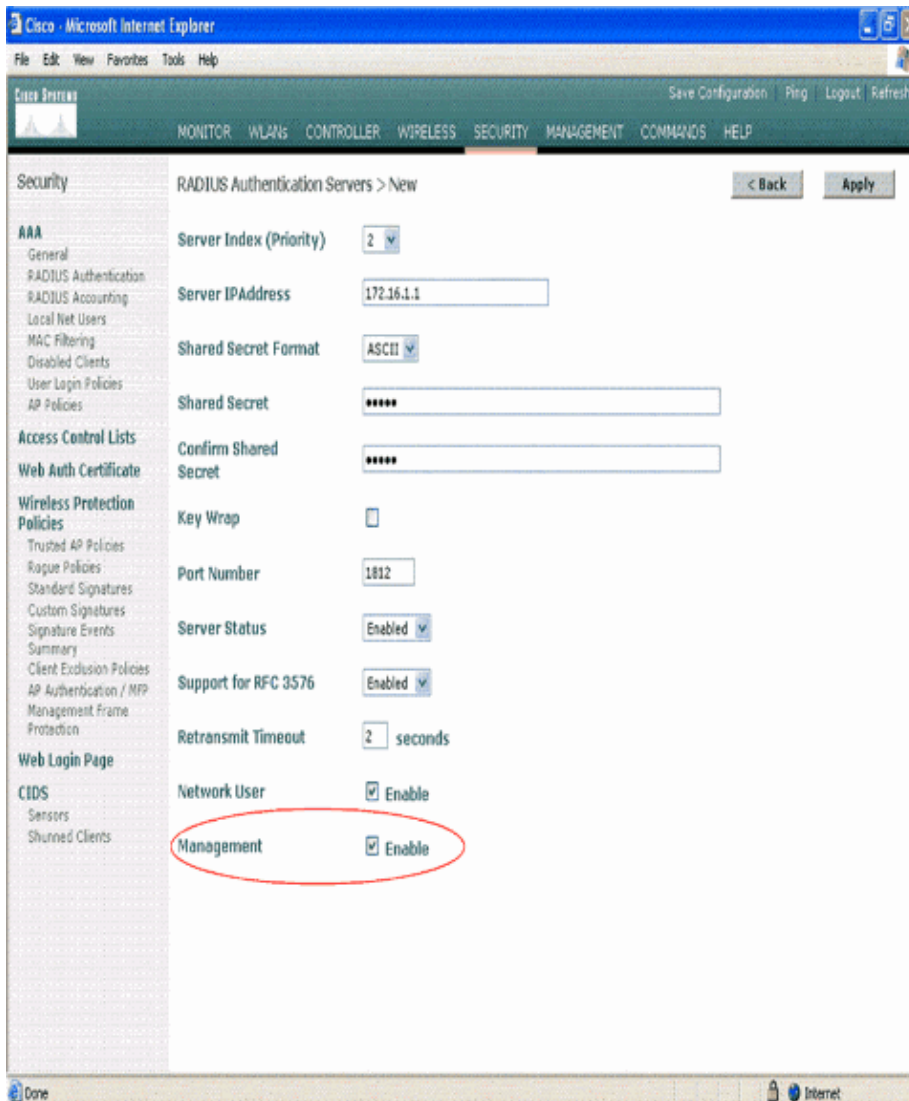
Once it is verified, complete the steps in the Configure the Controller to Accept Management through the ACS section at the controller side.

Configure the Controller to Accept Management through the ACS

Complete these steps in order to configure the WLC with details about ACS.

1. From the WLC GUI, go to the Security tab and configure the IP address and shared secret of the ACS server. Then click **Apply**.

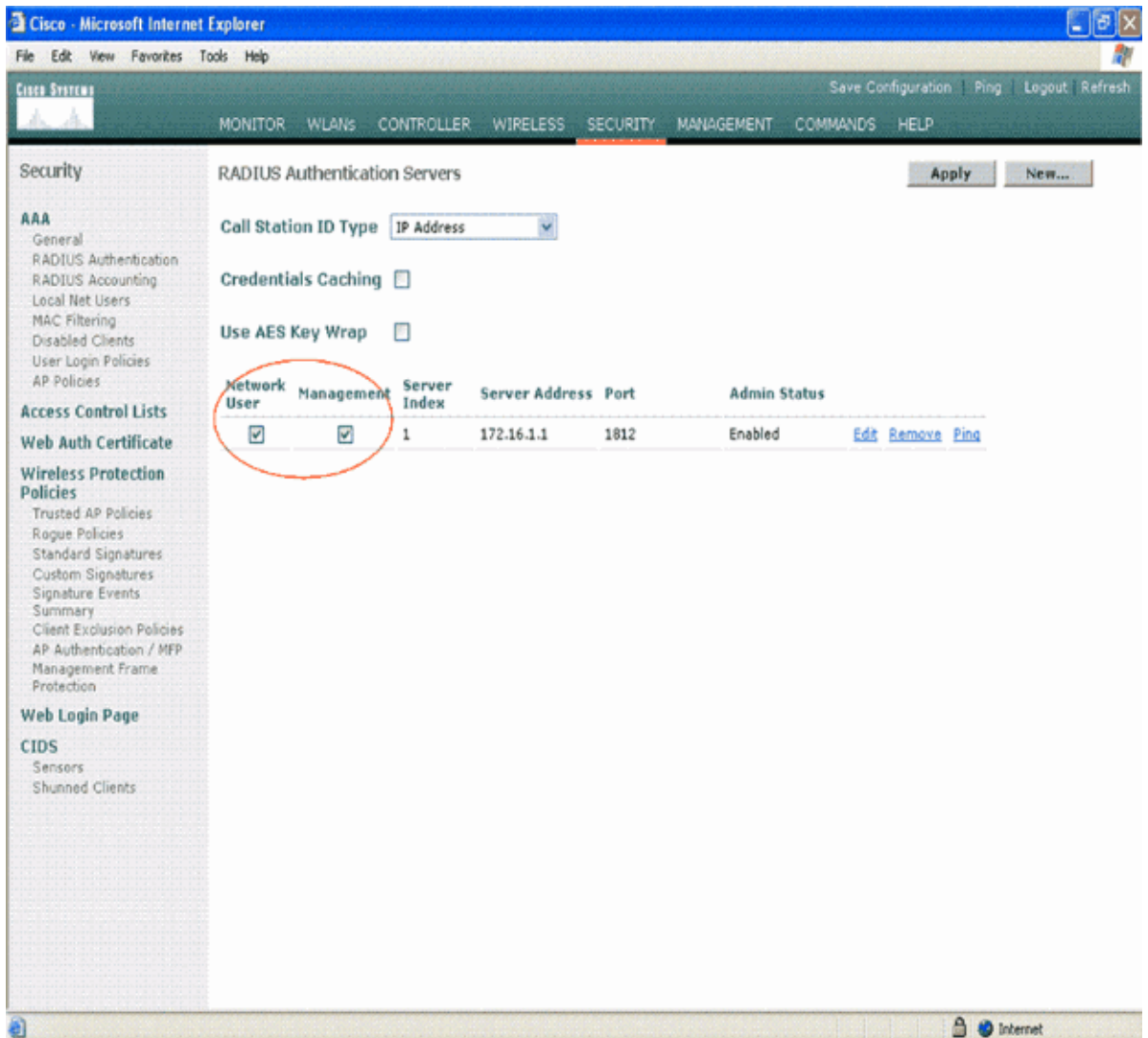
This shared secret needs to be the same on the ACS in order for the WLC to communicate with the ACS. This figure shows an example.



2. Check **Management** in order to allow the ACS to manage the WLC users as shown in the figure in step 1 of this procedure.

Note: The controller first looks for the username and password in the controller's locally defined management users before it tries to authenticate the management user via the RADIUS server.

3. Verify whether the WLC is configured to be managed by ACS. In order to do this, go to the WLC GUI and click **Security**. The resultant GUI window appears similar to this example.



You can see that the **Management** check box is enabled for RADIUS server 172.16.1.1. This illustrates that ACS is allowed to authenticate the management users on the WLC.

ACS Configuration

Complete the steps in these sections in order to configure the ACS:

1. Add the WLC as an AAA client to the RADIUS server.
2. Configure users and their appropriate RADIUS IETF attributes.
3. Configure a user with read–write access.
4. Configure a user with read–only access.

Add the WLC as an AAA Client to the RADIUS Server

This document uses the ACS as the RADIUS server. You can use any RADIUS server for this configuration.

Complete these steps in order to add the WLC as an AAA client in the ACS.

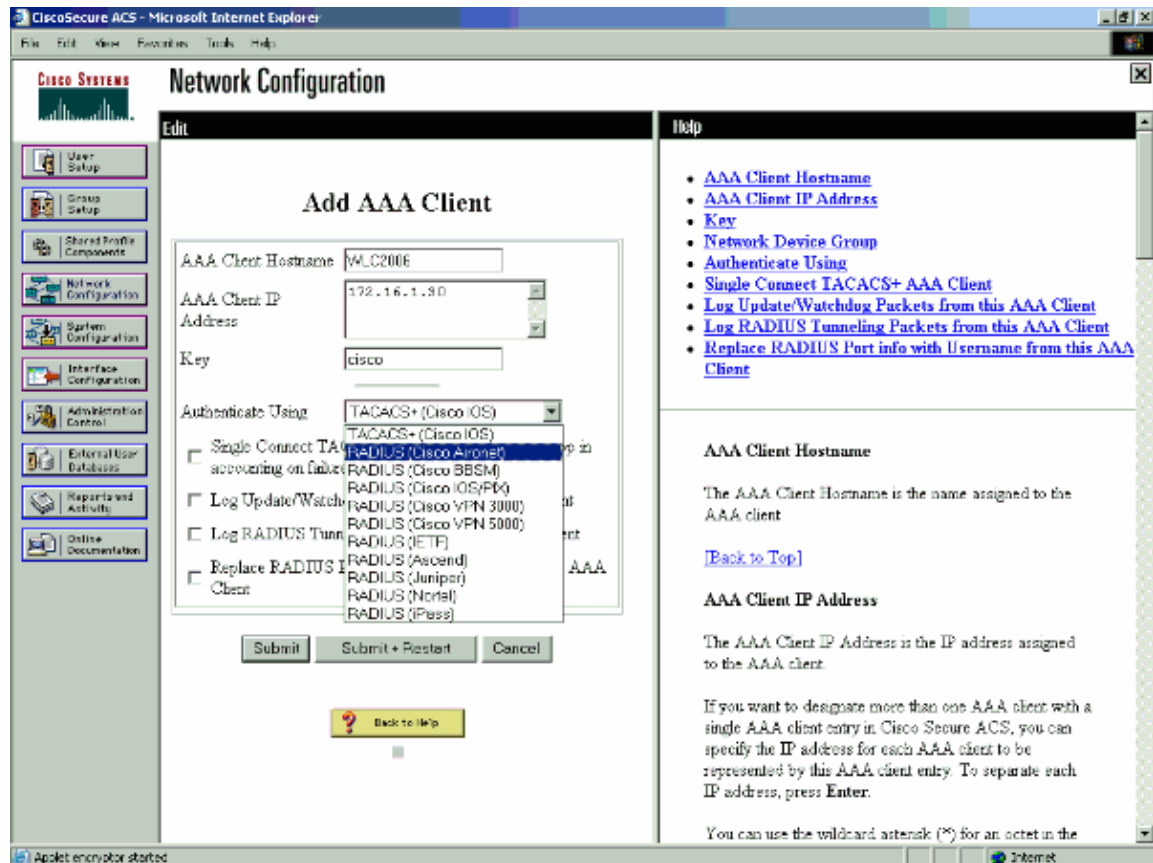
1. From the ACS GUI, go to the Network Configuration tab.
2. Under AAA Clients, click **Add Entry**.
3. In the Add AAA Client window, enter the WLC host name, the IP address of the WLC, and a shared secret key.

In this example, these are the settings:

- ◆ AAA Client Hostname is WLC2006
- ◆ 172.16.1.30/16 is the AAA Client IP Address, which, in this case is the WLC.
- ◆ The shared secret key is "cisco".

This shared secret key must be the same as the shared secret key that you configure on the WLC.

4. From the Authenticate Using drop-down menu, choose **RADIUS (Cisco Aironet)**.
5. Click **Submit + Restart** in order to save the configuration.



Configure Users and Their Appropriate RADIUS IETF Attributes

In order to authenticate a user via a RADIUS server, for controller login and management, you must add the user to the RADIUS database with the IETF RADIUS attributes Service-Type attribute set to the appropriate value according to the user's privileges.

- In order to set read-write privileges for the user, set the Service-Type Attribute to **Administrative**.
- In order to set read-only privileges for the user, set the Service-Type Attribute to **NAS-Prompt**.

Configure a User with Read-Write Access

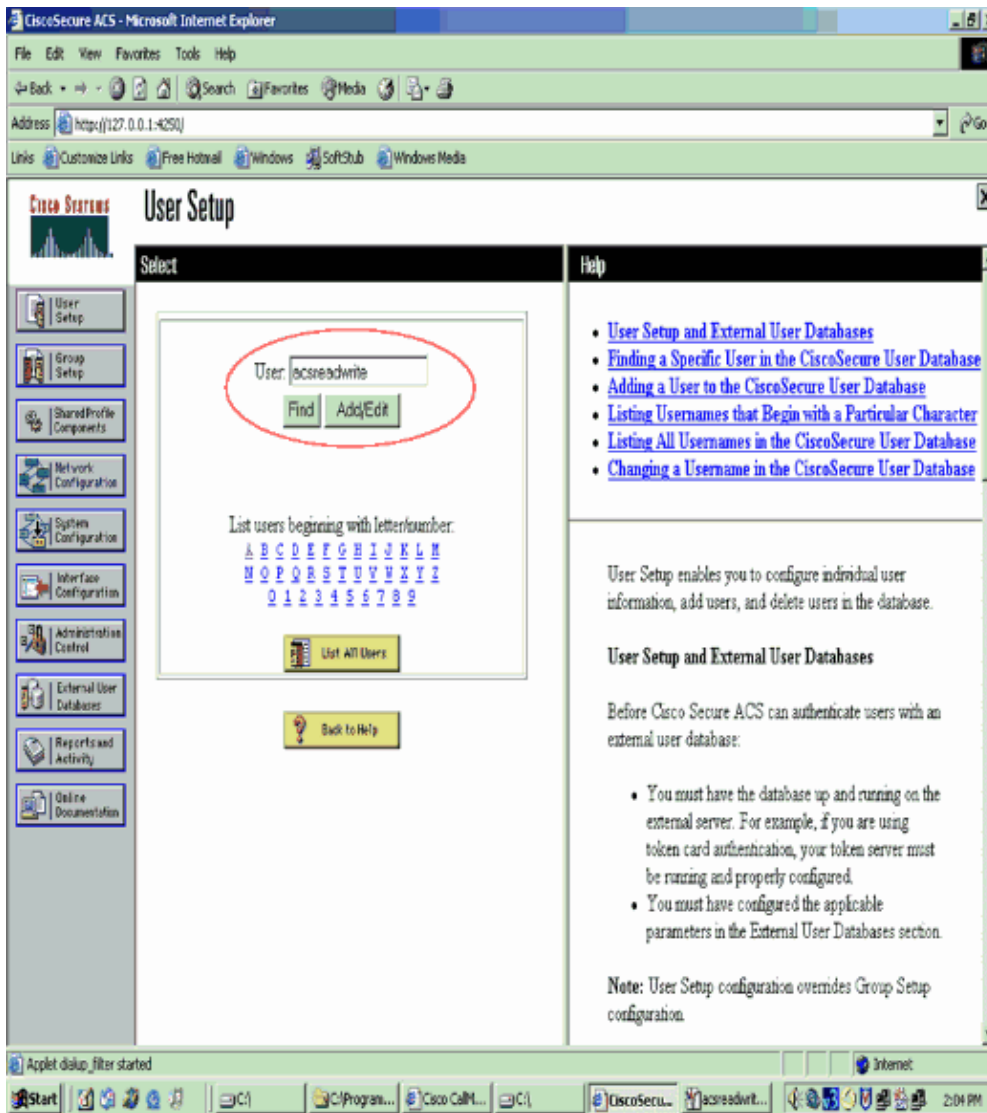
The first example shows the configuration of a user with full access to the WLC. Therefore, when this particular user tries to login to the controller, the RADIUS server authenticates and provides this user with full administrative access.

In this example, the username and password is **acsreadwrite**.

Complete these steps at the ACS.

1. From the ACS GUI, go to the User Setup tab.

2. Type the username to be added to the ACS as this example window shows.



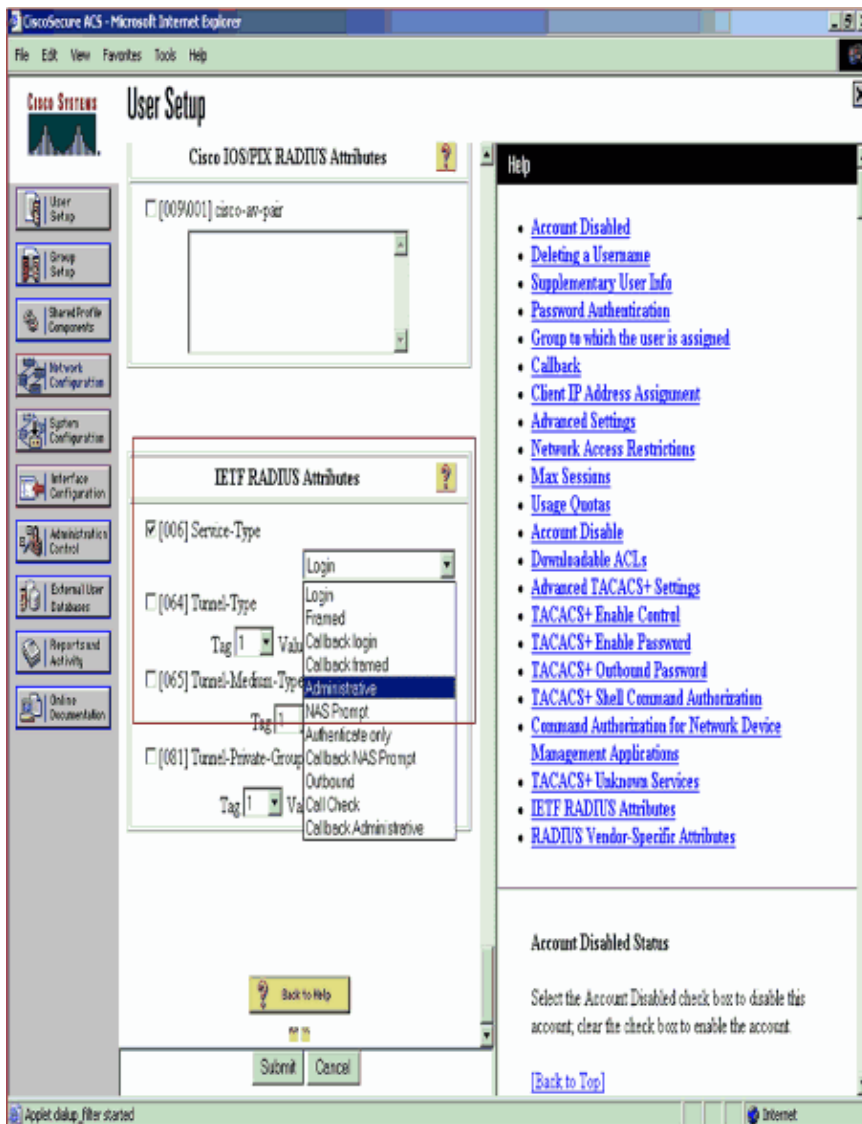
3. Click **Add/Edit** in order to go to the User Edit page.

4. In the User Edit page, provide the Real Name, Description and Password details of this user.

5. Scroll down to the IETF RADIUS Attributes setting and check **Service–Type Attribute**.

6. Since, in this example, user acsreadwrite needs to be given full access, choose **Administrative** for the Service–Type pull–down menu and click **Submit**.

This ensures that this particular user has read–write access to the WLC.

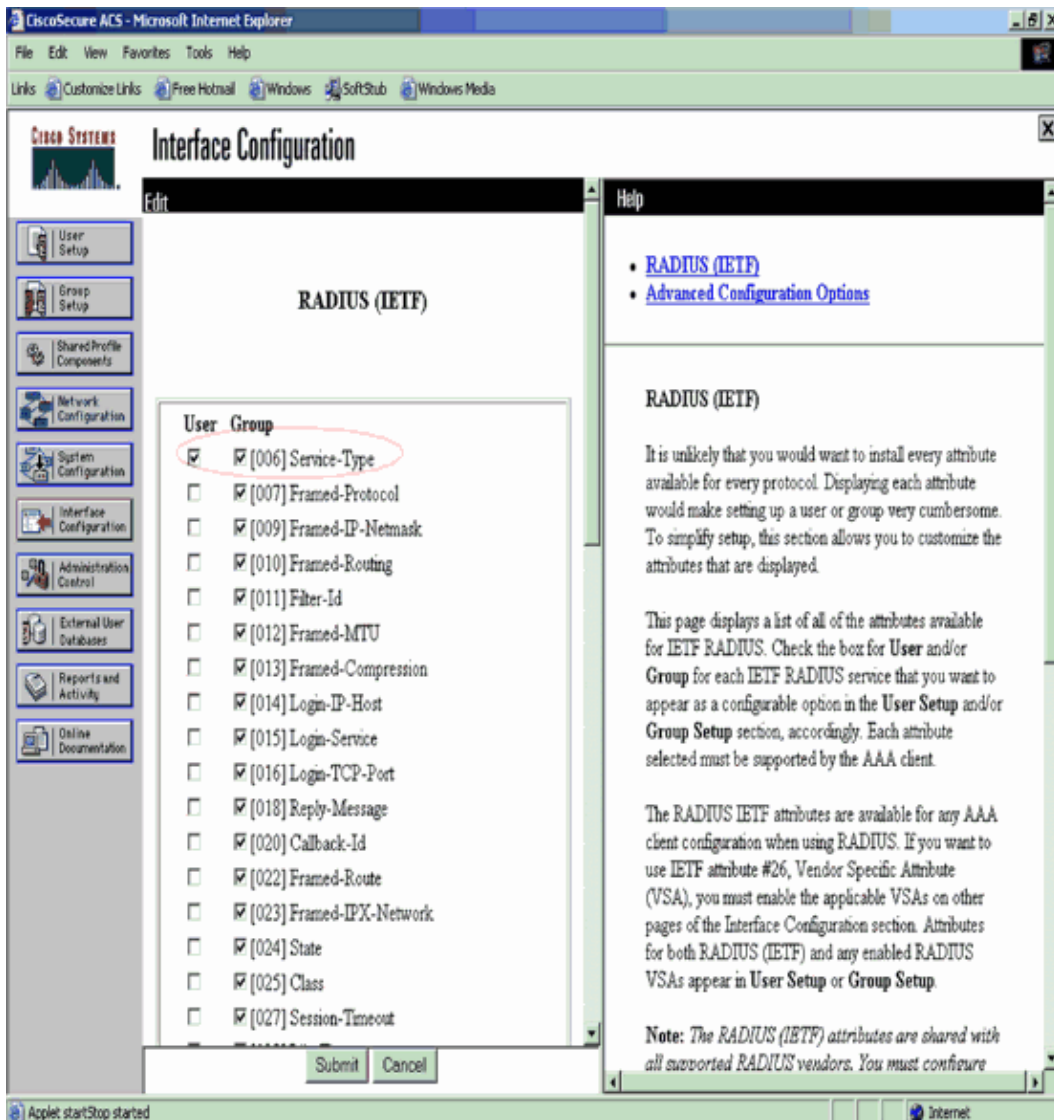


Sometimes, this Service–Type attribute is not visible under the user settings. In such cases, complete these steps in order to make it visible.

1. From the ACS GUI, choose **Interface Configuration > RADIUS (IETF)** in order to enable IETF attributes in the User Configuration window.

This takes you to the RADIUS (IETF) Settings page.

2. From the RADIUS (IETF) Settings page, you can enable the IETF attribute that needs to be visible under user or group settings. For this configuration, check **Service–Type** for the User column and click **Submit**. This window shows an example.



Note: This example specifies authentication on a per-user basis. You can also perform authentication based on the group to which a particular user belongs. In such cases, enable the **Group** check box so that this attribute is visible under Group settings. For this example, it is not necessary to check the Group check box.

Note: Also, if the authentication is on a group basis, you need to assign users to a particular group and configure the group setting IETF attributes to provide access privileges to users of that group. Refer to Group Management for detailed information on how to configure and manage groups.

Configure a User with Read-Only Access

This example shows the configuration of a user with read-only access to the WLC. Therefore, when this particular user tries to login to the controller, the RADIUS server authenticates and provides this user with read-only access.

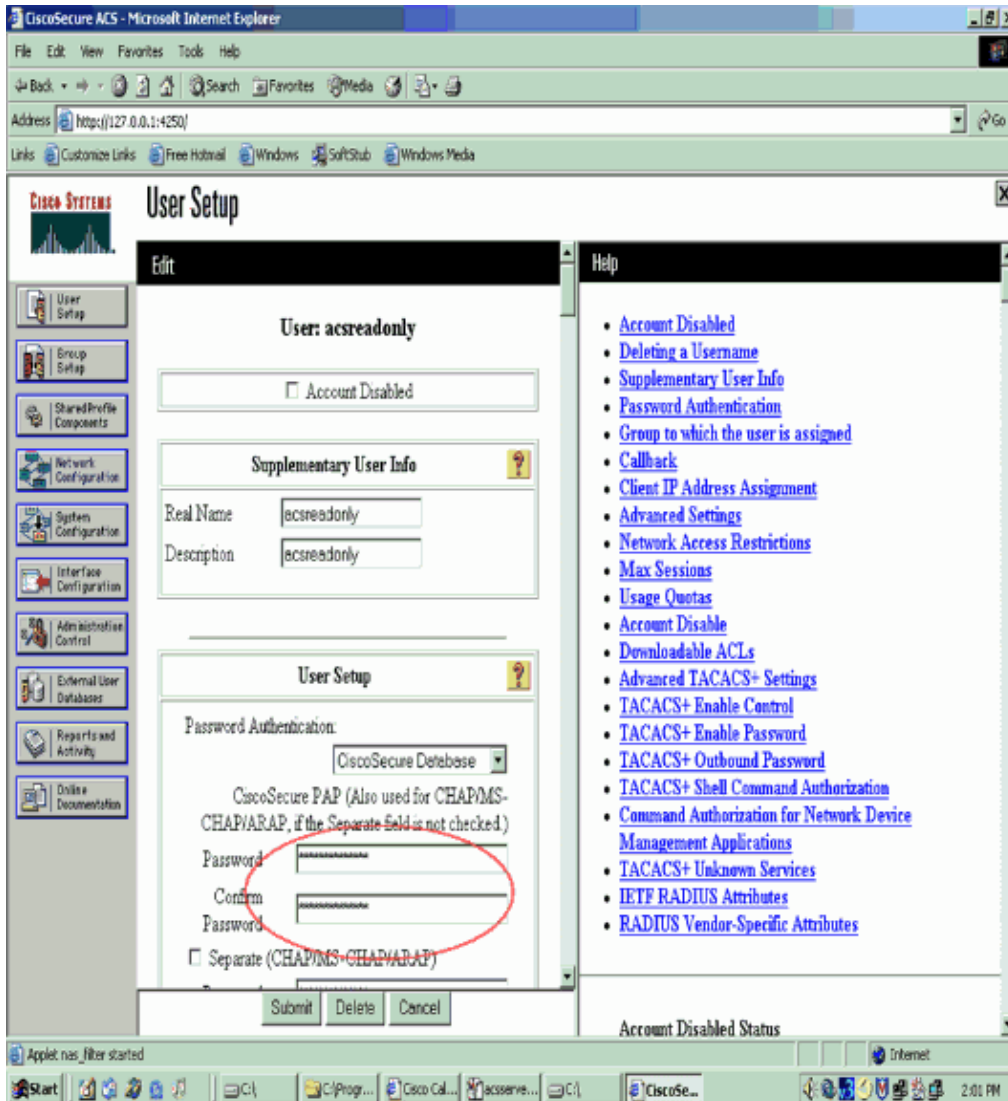
In this example, the username and password is **acsreadonly**.

Complete these steps on the ACS:

1. From the ACS GUI, go to the **User Setup** tab.
2. Type the username you want to add to the ACS and click **Add/Edit** in order to go to the User Edit

page.

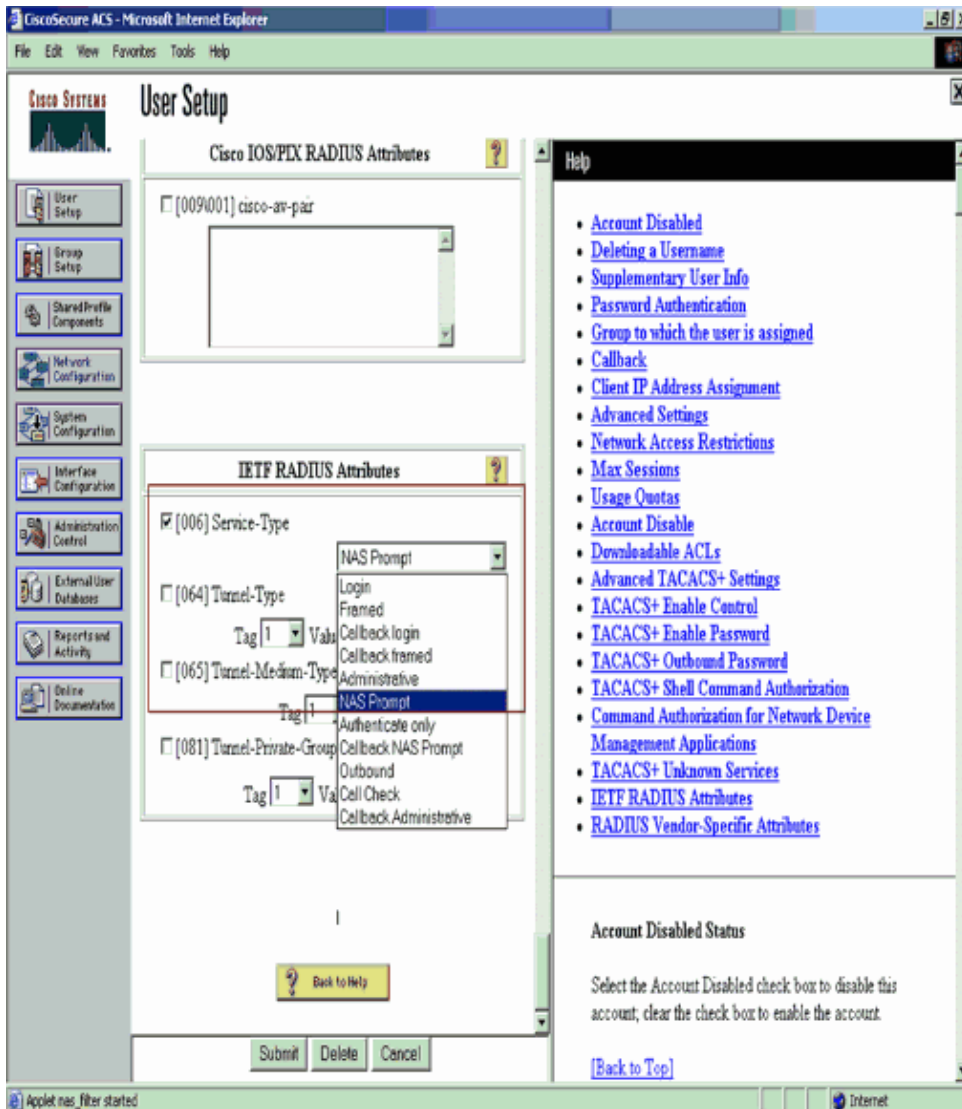
3. Provide the Real Name, Description and Password of this user. This window shows an example.



4. Scroll down to the IETF RADIUS Attributes setting and check **Service-Type Attribute**.

5. Since, in this example, user acsreadonly needs to have read-only access, choose **NAS Prompt** from the Service-Type pull-down menu and click **Submit**.

This ensures that this particular user has read-only access to the WLC.



Manage the WLC Locally as well as Through the RADIUS Server

You can also configure the management users locally on the WLC. This can be done from the controller GUI, under **Management > Local Management Users**.

Assume that the WLC is configured with management users both locally as well as in the RADIUS server with the **Management** check box enabled. In such a scenario, when a user tries to login to the WLC, the WLC behaves in this manner:

1. The WLC first looks at the local management users defined to validate the user. If the user exists in its local list, then it allows authentication for this user. If this user does not appear locally, then it looks to the RADIUS server.
2. If the same user exists both locally as well as in the RADIUS server but with different access privileges, then the WLC authenticates the user with the privileges specified locally. In other words, local configuration on the WLC always takes precedence when compared to the RADIUS server.

Note: Refer to Authentication of Wireless LAN Controller's Lobby Administrator via RADIUS Server to know how to authenticate a lobby administrator of the WLC via a RADIUS server.

Verify

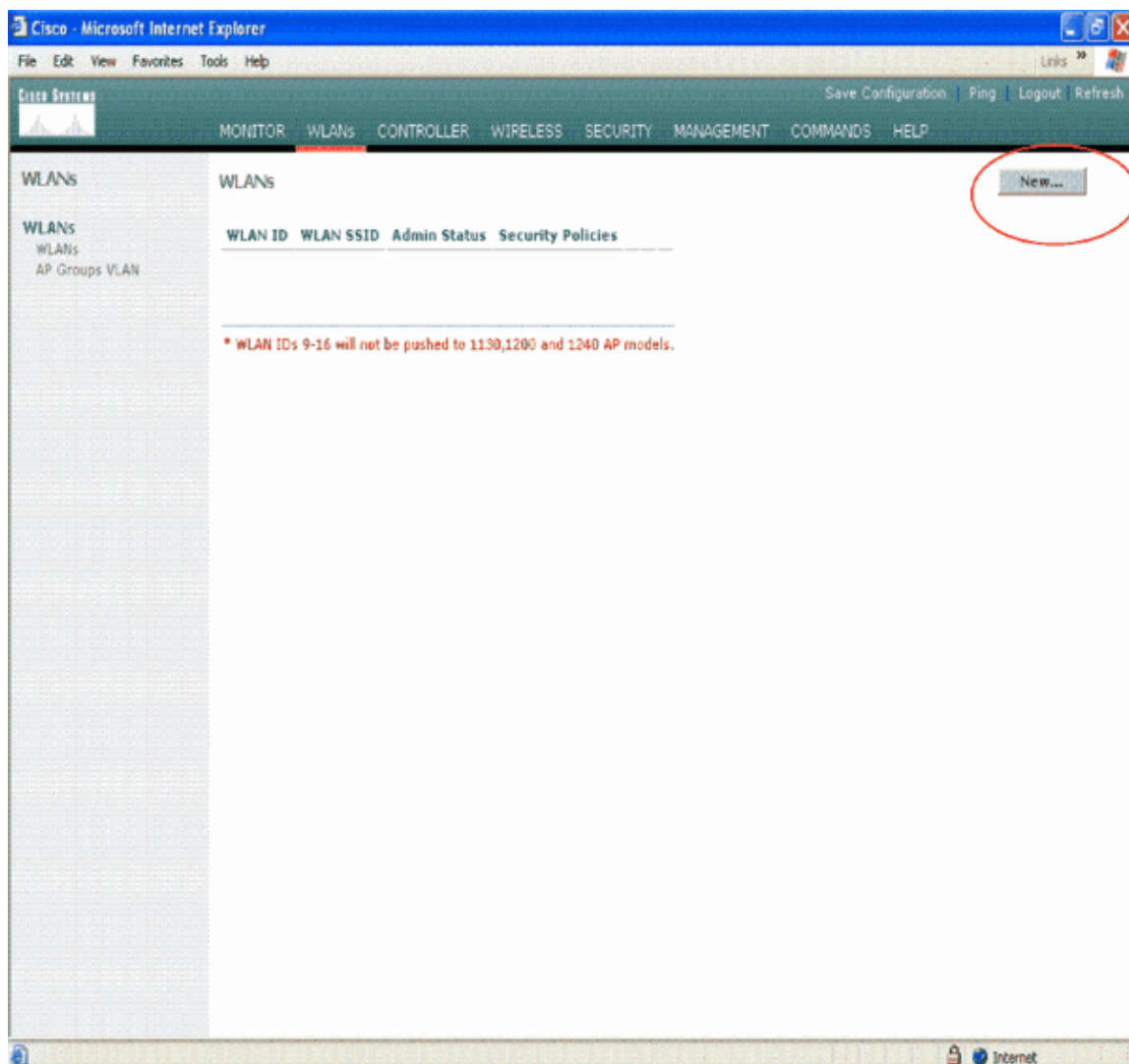
Use this section to confirm that your configuration works properly.

In order to verify whether your configuration works properly, access the WLC through the CLI or GUI (HTTP/HTTPS) mode. When the login prompt appears, type the username and password as configured on the ACS.

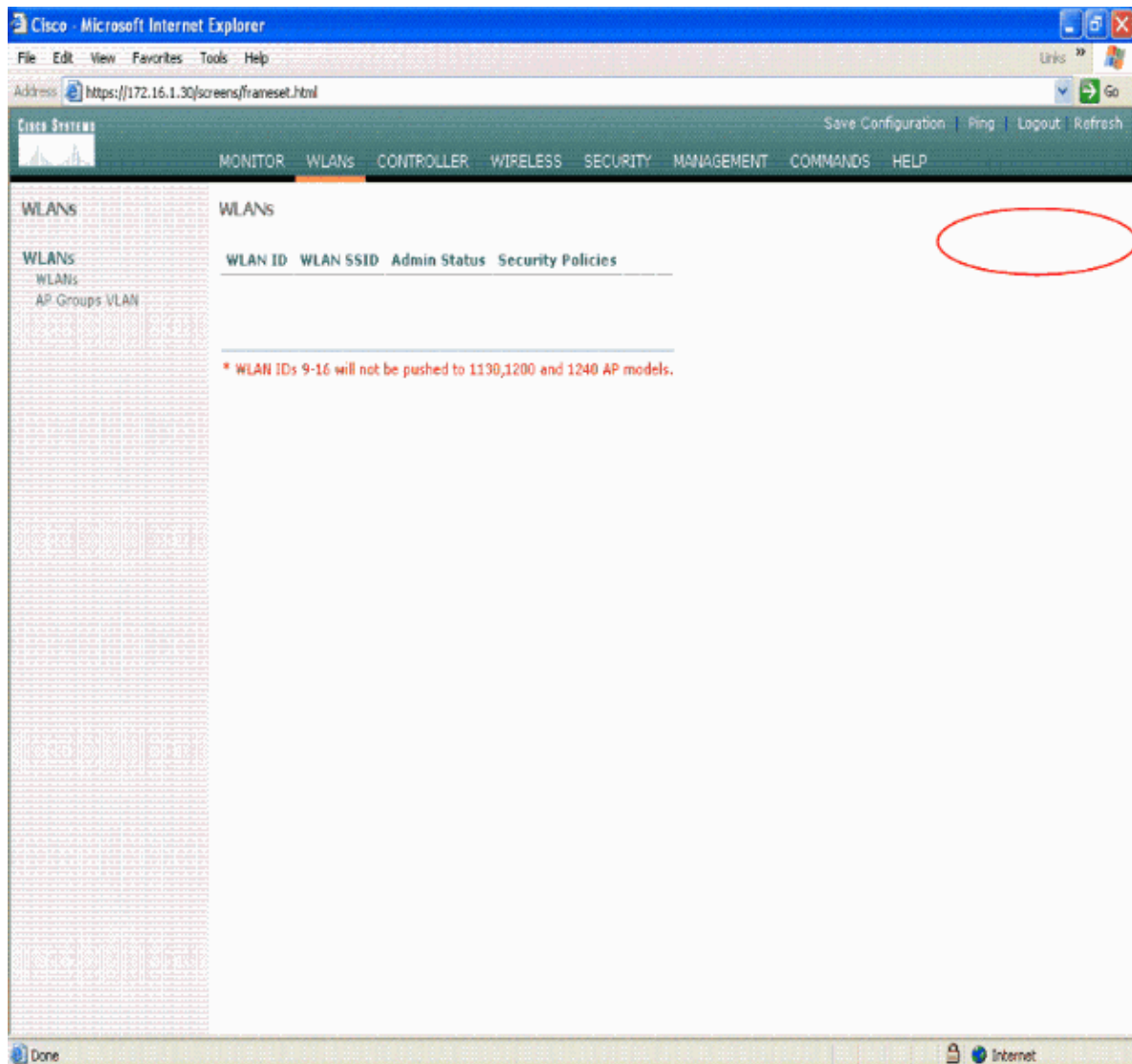
If you have the configurations correct, you are authenticated successfully into the WLC.

You can also ensure whether the authenticated user is provided with access restrictions as specified by the ACS. In order to do so, access the WLC GUI through HTTP/HTTPS (ensure that WLC is configured to allow HTTP/HTTPS).

A user with read–write access set in the ACS has several configurable privileges in the WLC. For example, a read–write user has the privilege to create a new WLAN under the WLANs page of the WLC. This window shows an example. The New button provides the read–write user an option to create a new WLAN. This option and all other configurable options are not available for a read–only user.



Here is an example that refers to the same WLANs page in the controller but for a read–only user. Notice that there is not the option to create a new WLAN.



These access restrictions can also be verified through the CLI of the WLC. This output shows an example.

```
(Cisco Controller) >?

debug          Manages system debug options.
help           Help
linktest       Perform a link test to a specified MAC address.
logout         Exit this session. Any unsaved changes are lost.
show           Display switch options and settings.
```

As this example output shows, a ? at the controller CLI displays a list of commands available for the current user. Also notice that the **config** command is not available in this example output. This illustrates that a read-only user does not have the privilege to do any configurations on the WLC. Whereas, a read-write user does have the privileges to do configurations on the controller (both GUI and CLI mode).

Note: Even after you authenticate a WLC user through the RADIUS server, as you browse from page to page, the HTTP[S] server still fully authenticates the client each time. The only reason you are not prompted for authentication on each page is that your browser caches and replays your credentials.

Troubleshoot

There are certain circumstances when a controller authenticates management users via the ACS, the

authentication finishes successfully (access-accept), and you do not see any authorization error on the controller. *But, the user is prompted again for authentication.*

In such cases, you cannot interpret what is wrong and why the user cannot log into the WLC by just using the **debug aaa events enable** command. Instead, the controller displays another prompt for authentication.

One possible reason for this is that the ACS is not configured to transmit the Service-Type attribute for that particular user or group even though the username and password are correctly configured on the ACS.

The output of the **debug aaa events enable** command does not indicate that a user does not have the required attributes (for this example, the Service-Type attribute) even though an **access-accept** is sent back from the AAA server. This example **debug aaa events enable** command output shows an example.

```
(Cisco Controller) >debug aaa events enable

Unable to find requested user entry for acsserver

Mon Nov 13 20:14:33 2006: AuthenticationRequest: 0xa449a8c

Mon Nov 13 20:14:33 2006: Callback.....0x8250c40

Mon Nov 13 20:14:33 2006: protocolType.....0x00020001

Mon Nov 13 20:14:33 2006: proxyState.....1A:00:00:00:00:00-00:00

Mon Nov 13 20:14:33 2006: Packet contains 5 AVPs (not shown)

Mon Nov 13 20:14:33 2006: 1a:00:00:00:00:00 Successful transmission of
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00

Mon Nov 13 20:14:33 2006: ****Enter processIncomingMessages: response code=2

Mon Nov 13 20:14:33 2006: ****Enter processRadiusResponse: response code=2

Mon Nov 13 20:14:33 2006: 1a:00:00:00:00:00 Access-Accept
received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0

Mon Nov 13 20:14:33 2006: AuthorizationResponse: 0x9802520

Mon Nov 13 20:14:33 2006: structureSize.....28

Mon Nov 13 20:14:33 2006: resultCode.....0

Mon Nov 13 20:14:33 2006: protocolUsed.....0x00000001

Mon Nov 13 20:14:33 2006: proxyState.....1A:00:00:00:00:00-00:00

Mon Nov 13 20:14:33 2006: Packet contains 0 AVPs:
```

In this first example **debug aaa events enable** command output, you see that Access-Accept is successfully received from the RADIUS server but the Service-Type attribute is not passed onto the WLC. This is because the particular user is not configured with this attribute on the ACS.

Cisco bug ID CSCsg48232 (registered customers only) is associated with this particular issue. Also refer to Cisco bug ID CSCsg48228 (registered customers only) for more information.

The workaround is to configure the user with the Service-Type attribute value set to either **Administrative** or **NAS-Prompt** according to the user privileges. This needs to be done on the ACS.

This second example shows the **debug aaa events enable** command output again. But this time the Service-Type attribute is set to **Administrative** on the ACS.

```
(Cisco Controller)>debug aaa events enable

Unable to find requested user entry for acsserver

Mon Nov 13 20:17:02 2006: AuthenticationRequest: 0xa449f1c

Mon Nov 13 20:17:02 2006: Callback.....0x8250c40

Mon Nov 13 20:17:02 2006: protocolType.....0x00020001

Mon Nov 13 20:17:02 2006: proxyState.....1D:00:00:00:00:00-00:00

Mon Nov 13 20:17:02 2006: Packet contains 5 AVPs (not shown)

Mon Nov 13 20:17:02 2006: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Nov 13 20:17:02 2006: ****Enter processIncomingMessages: response code=2

Mon Nov 13 20:17:02 2006: ****Enter processRadiusResponse: response code=2

Mon Nov 13 20:17:02 2006: 1d:00:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0

Mon Nov 13 20:17:02 2006: AuthorizationResponse: 0x9802520

Mon Nov 13 20:17:02 2006: structureSize.....100

Mon Nov 13 20:17:02 2006: resultCode.....0

Mon Nov 13 20:17:02 2006: protocolUsed.....0x00000001

Mon Nov 13 20:17:02 2006: proxyState.....1D:00:00:00:00:00-00:00

Mon Nov 13 20:17:02 2006: Packet contains 2 AVPs:

Mon Nov 13 20:17:02 2006: AVP[01] Service-Type.....0x00000006 (6) (4 bytes)

Mon Nov 13 20:17:02 2006: AVP[02] Class.....
CISCOACS:000d1b9f/ac100128/acserver (36 bytes)
```

You can see in this example output that the Service-Type attribute is passed onto the WLC.

Related Information

- [Configuring Wireless LAN Controller – Configuration Guide](#)
 - [VLANs on Wireless LAN Controllers Configuration Example](#)
 - [Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller Configuration Example](#)
 - [Wireless LAN Controller and Lightweight Access Point Basic Configuration Example](#)
 - [AP Group VLANs with Wireless LAN Controllers Configuration Example](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

