Configuration Example: TACACS Administrator Access to Converged Access Wireless LAN Controllers

This document provides a configuration example for Terminal Access Controller Access Control System Plus (TACACS+) in a Cisco Catalyst 3850 Series, and Cisco Catalyst 3650 Series Switches for CLI and GUI. This document also provides basic tips to troubleshoot the configuration.

TACACS+ is a client and server protocol that provides centralized security for users who attempt to gain management access to a router or network access server. TACACS+ provides the following Authentication, Authorization, and Accounting (AAA) services:

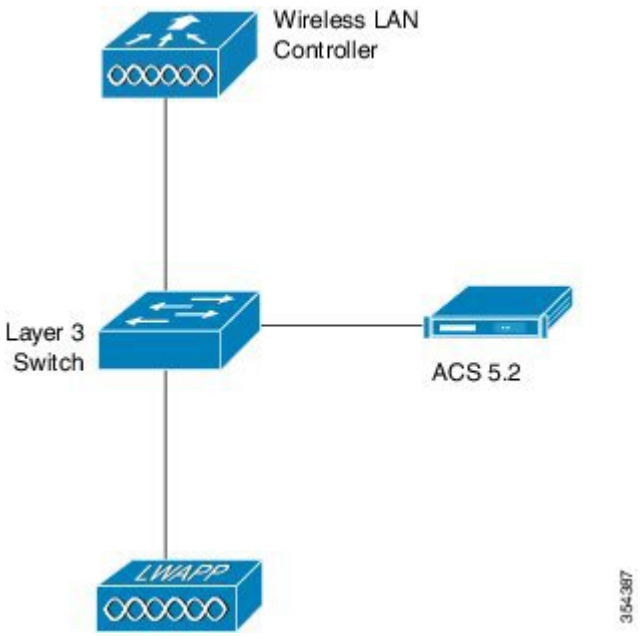
- Authentication of users who attempt to log in to the network equipment.
- Authorization to determine what level of access users should have.
- Accounting to keep track of all changes the users make.

- Network Diagram for TACACS Administrator Access, page 2
- Configuring TACACS Administrator Access to the Converged Access WLCs, page 2
- Configuring TACACS Administrator Access to Converged Access WLCs, page 3
- Verifying TACACS Administrator Access to the Converged Access WLC, page 8
- Troubleshooting TACACS Administrator Access to the Converged Access WLC, page 8

Network Diagram for TACACS Administrator Access

The following figure displays the network diagram for TACACS Administrator Access:

Figure 1: Network Diagram for TACACS Administrator Access



Configuring TACACS Administrator Access to the Converged Access WLCs

Configuring TACACS Administrator Access to the Converged Access WLCs includes the following two steps:

- Configuring on the WLC
- Configuring on the RADIUS and TACACS server

Step 1 To define the TACACS server on the WLC, use the following commands. Ensure you configure the same shared secret on the TACACS.

```
tacacs-server host 198.51.100.71 key Cisco123
tacacs server ACS
address ipv4 198.51.100.50
 key Cisco123
 timeout 10
```

Step 2 To configure the server groups and map the server configured in the step 1, use the following commands.

```
aaa group server tacacs+ ACS
 server name ACS
!
```

Step 3 To configure the Authentication and the Authorization policies for administrator access, use the following commands. Provide the administrator access to TACACS group followed by local (which is the fallback).

```
 aaa authentication login Admin_Access group ACS local
aaa authorization exec Admin_Access group ACS local
```

Step 4 To apply the policy to the line vty, use the following commands:

```
line vty 0 4
 authorization exec Admin_Access
 login authentication Admin_Access
line vty 5 15
 exec-timeout 0 0
 authorization exec Admin_Access
 login authentication Admin_Access
```

Step 5 To apply the policy to HTTP, use the following commands:

```
ip http server
ip http authentication aaa login-authentication Admin_Access
ip http authentication aaa exec-authorization Admin_Access
```

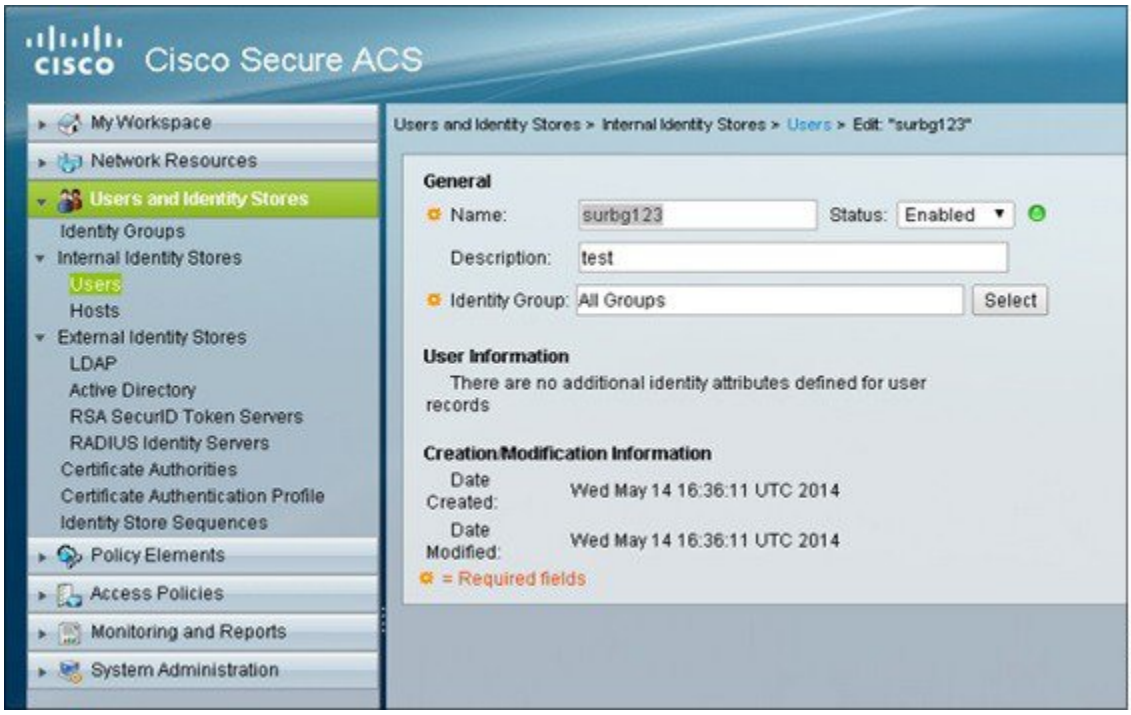
Configuring TACACS Administrator Access to Converged Access WLCs

Step 1 To add WLC as the AAA client for TACACS on the ACS, navigate to **Network Resources** > **Network Devices**, and AAA Clients. Ensure the Shared Secret configured here matches the one configured on the WLC.

Figure 2: Add WLC as the AAA Client

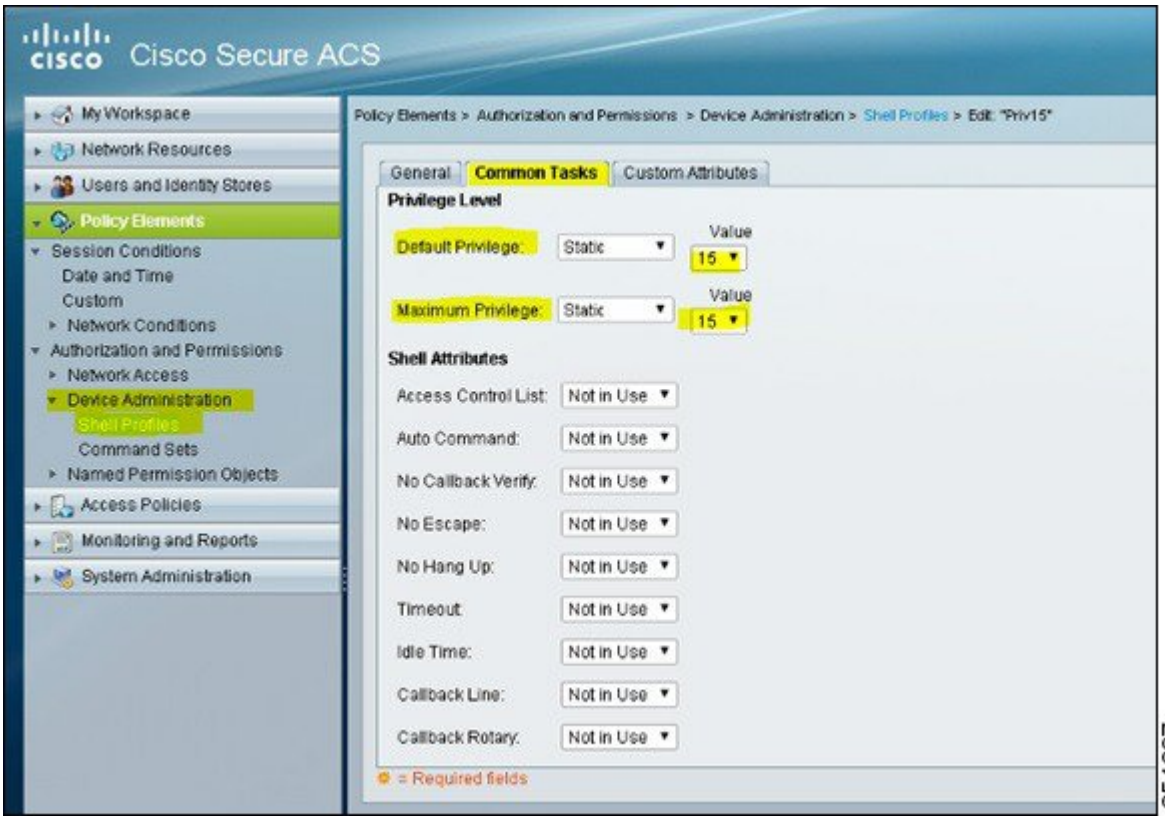
Step 2 To define the user for administrator access, navigate to **Users and Identity Stores** > **Internal Identity Stores** > **Users** .

Figure 3: Define Administrator Access



Step 3 To set the privilege levels to 15, navigate to **Policy Elements** > **Authorization and Permissions** > **Device Administration** > **Shell Profiles**.

Figure 4: Set Priviledge Level

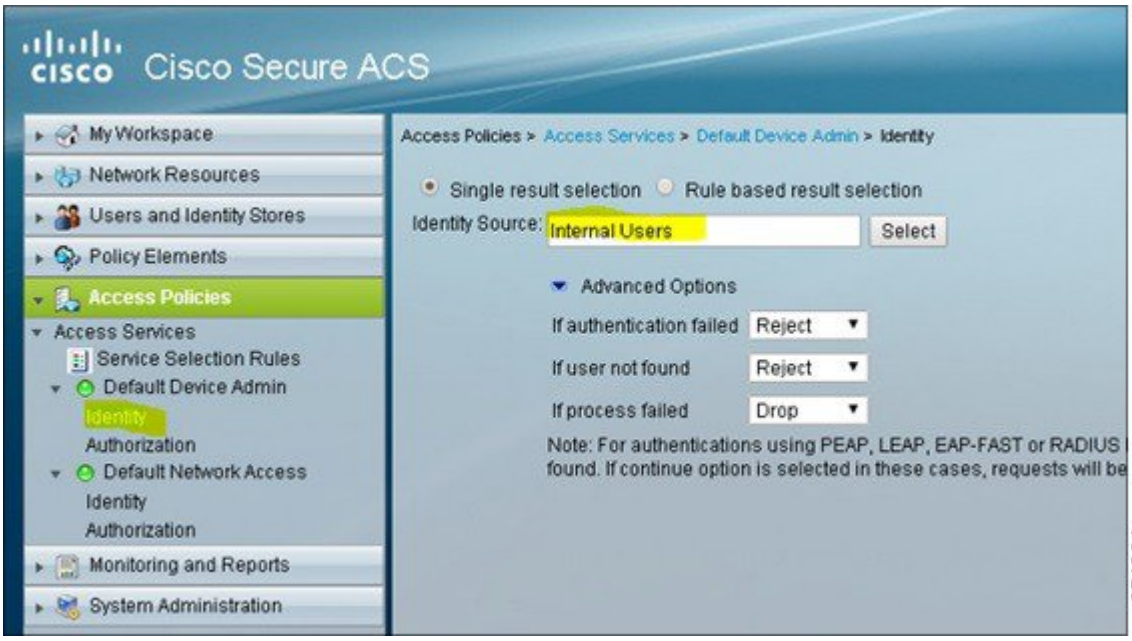


Step 4 To allow the required protocols, navigate to **Access Policies** > **Access Services** > **Default Device Admin**.

Figure 5: Enable Protocols

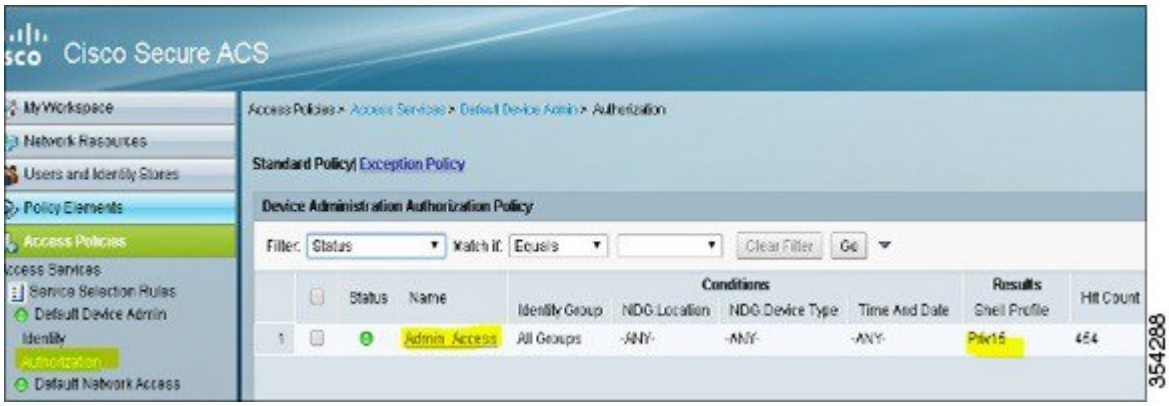
Step 5 To create an identity for the device administrator which allows internal users with authentication options, navigate to **Access Policies** > **Access Services** > **Default Device Admin** > **Identity** .

Figure 6: Create Identity for Device Administrator



Step 6 To allow the Priv15 authorization profile created in Step 3, navigate to **Access Policies** > **Access Services** > **Default Device Admin** > **Authorization**. The client authenticated successfully (internal users) is put on the Priv15 profile.

Figure 7: Enable Priv15 Authorization Profile



Verifying TACACS Administrator Access to the Converged Access WLC

Confirm that your configuration works properly by perform the following steps:

Step 1 Open a browser and enter the switch IP address. The Authentication Required prompt displays.

Step 2 Enter the group user credentials to log in to the device.

Step 3 To check the Telnet or SSH access, Telnet or SSH to the switch IP address and enter the credentials. The ACS Log in details is displayed.

Troubleshooting TACACS Administrator Access to the Converged Access WLC

The following section provides information to troubleshoot your configuration.

Note Refer to Important Information on before using debug commands

To troubleshoot your configuration, use the **debug tacacs** command.

debug tacacs

```
*May 14 23:11:06.396: TPLUS: Queuing AAA Authentication request 4775 for processing
*May 14 23:11:06.396: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:06.396: TPLUS: processing authentication continue request id 4775
*May 14 23:11:06.396: TPLUS: Authentication continue packet generated for 4775
*May 14 23:11:06.396: TPLUS(000012A7)/0/WRITE/962571D4: Started 10 sec timeout
*May 14 23:11:06.396: TPLUS(000012A7)/0/WRITE: wrote entire 25 bytes request
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
 16 bytes data)
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: read entire 28 bytes response
*May 14 23:11:06.398: TPLUS(000012A7)/0/962571D4: Processing the reply packet
*May 14 23:11:06.398: TPLUS: Received authen response status GET_PASSWORD (8)
*May 14 23:11:08.680: TPLUS: Queuing AAA Authentication request 4775 for processing
*May 14 23:11:08.680: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:08.680: TPLUS: processing authentication continue request id 4775
*May 14 23:11:08.680: TPLUS: Authentication continue packet generated for 4775
*May 14 23:11:08.680: TPLUS(000012A7)/0/WRITE/962571D4: Started 10 sec timeout
*May 14 23:11:08.680: TPLUS(000012A7)/0/WRITE: wrote entire 25 bytes request
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
 6 bytes data)
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: read entire 18 bytes response
*May 14 23:11:08.687: TPLUS(000012A7)/0/962571D4: Processing the reply packet
*May 14 23:11:08.687: TPLUS: Received authen response status PASS (2)
*May 14 23:11:08.687: TPLUS: Queuing AAA Authorization request 4775 for processing
*May 14 23:11:08.687: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:08.687: TPLUS: processing authorization request id 4775
```

```
*May 14 23:11:08.687: TPLUS: Protocol set to None .....Skipping
*May 14 23:11:08.687: TPLUS: Sending AV service=shell
*May 14 23:11:08.687: TPLUS: Sending AV cmd*
*May 14 23:11:08.687: TPLUS: Authorization request created for 4775(surbg123)
*May 14 23:11:08.687: TPLUS: using previously set server 10.106.102.50 from
 group SURBG_ACS
*May 14 23:11:08.688: TPLUS(000012A7)/0/NB_WAIT/93C63F04: Started 10 sec timeout
*May 14 23:11:08.690: TPLUS(000012A7)/0/NB_WAIT: socket event 2
*May 14 23:11:08.690: TPLUS(000012A7)/0/NB_WAIT: wrote entire 61 bytes request
*May 14 23:11:08.690: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.690: TPLUS(000012A7)/0/READ: Would block while reading
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
 18 bytes data)
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: read entire 30 bytes response
*May 14 23:11:08.696: TPLUS(000012A7)/0/93C63F04: Processing the reply packet
*May 14 23:11:08.696: TPLUS: Processed AV priv-lvl=15
*May 14 23:11:08.696: TPLUS: received authorization response for 4775: PASS
```

-