Converged Access: Securing Networks with AAA and Cisco ISE

The Cisco Catalyst 3650 Series Switches and the Cisco Catalyst 3850 Series Switches are capable of providing both wireless connectivity and wired services to end users. Since, wireless networks are equally prone to unauthorized access and attacks, they require the same level of security as wired networks.

This chapter provides a step-by-step instructions for configuring authentication, authorization, and accounting (AAA) and Cisco Identity Service Engine (ISE), to enable the Converged Access on Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches.

- Overview of Securing Networks with AAA and Cisco ISE, page 1
- Configuring AAA, page 2
- Verifying Dot1x Protocol and RADIUS Server, page 3
- Adding a Cisco Catalyst 3850 Switch to Cisco ISE, page 3
- Configuring Authentication and Authorization Policies, page 4

Overview of Securing Networks with AAA and Cisco ISE

For wireless clients, AAA enables the Cisco Catalyst 3850 Series Switches to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting). AAA helps secure the wireless network in the corresponding enterprise against unauthorized access.

The authentication component of AAA is responsible for providing a method to identify (authenticate) wireless users. With AAA, you can define one or more authentication methods the device should use when authenticating a user. For example, you can specify two authentication methods, an external security server and a local user database on the device.

When authentication for a user is completed successfully, AAA's authorization is used to restrict the actions a user can perform and the services a user can access. For example, if network access to a temporary worker in an enterprise network needs to be limited, you can enforce this restriction using AAA's authorization component.

AAA's accounting component is responsible for keeping a record of authentication and authorization actions of wireless users, and related metrics such as tracking users who log in to the network after business hours.

Note

- You can either use authentication by itself or along with authorization and accounting. Authorization requires a user to be authenticated first. If you use multiple security contexts, AAA settings are unique for each context, and are not shared between contexts.
- You can control the access, authorize resources and commands, and perform accounting differently among contexts.
- You can configure local authentication and authorization on the switch.
- For more information, refer to the chapter "Configuring Local Authentication and Authorization" in the Security Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches).

Configuring AAA

Before You Begin

The following are the prerequisites for configuring AAA on Cisco Catalyst 3850 Series Switches:

- Configure Cisco Catalyst 3850 Series Switches or Cisco Catalyst 3650 Series Switches with IP Base or IP Services license.
- Configure Cisco ISE with the following features:
  - IP reachability to the switch.
  - Client Username and Password Database or link to the Active Directory.

Step 1 To enable AAA, use the **aaa new-model** command in global configuration mode:

```
Device(config)# aaa new-model
```

Step 2 To define the AAA server group with a group name, use the **aaa group server radius** command. All the members should be of the group, RADIUS. Use the **server name** command to define the server name and enter server group radius configuration mode:

```
Device(config)#  aaa group server radius name
 Device(config)#  server name server-name
```

Step 3 To enable dot1x and 802.1X globally, use the **dot1x system-auth-control** command in global configuration mode:

```
Device(config)# dot1x system-auth-control
```

Step 4 To create an authentication list for 802.1X, use the **aaa authentication dot1x default group** command. This authentication contacts a RADIUS server in the RADIUS group specified using *group-name*.

```
Device(config)#  aaa authentication dot1x default group group-name
```

To configure network authorization through RADIUS, use the **aaa authorization network default group** command.

```
Device(config)#  aaa authorization network default group group-name
```

To configure a default accounting method list, where a RADIUS server provides accounting services, use the **aaa accounting identity default start-stop group** command.

```
Device(config)#  aaa accounting identity default start-stop groupgroup-name
```

Step 5 To define the RADIUS server name along with the IP address, port numbers, and the shared key, use the following commands:

```
Device(config)#  radius server  radius-server-name
Device(config-dia-peer)#  address ipv4  IP_Address  auth-port  authentication-port  acct-port  accounting_port
Device(config-keychain)#  key  radius-shared-key
```

Step 6 To configure the SNMP community string for Cisco ISE, use the **snmp-server community** command:

```
Device(config)#  snmp-server community  snmp-community-string  RO
```

Step 7 To configure a RADIUS source interface to connect to the RADIUS server, use the **ip radius source-interface** command:

```
Device(config)#  ip radius source-interface  interface
```

Verifying Dot1x Protocol and RADIUS Server

Use the following command to check if the dot1x protocol is enabled on the switch:

```
Device# show dot1x

sysauthcontrol              Enabled
dot1x Protocol Version            3
```

Use the following command to check the RADIUS server:

```
Device# show radius server-group all

server group group_Name
Server(Radius_Server_IP:Auth_Port,Acct_Port) Transactions:
```

Adding a Cisco Catalyst 3850 Switch to Cisco ISE

Step 1 Choose **Administration > Network Resources > Add**.

Step 2 Enter the **Name**, **Description** (optional), and **IP Address** of the switch.

Step 3 Check the **Authentication Settings** check box .

Step 4 Enter the shared secret key using the **radius_shared_key** field.

Step 5 Enter the SNMP settings and select the SNMP version.

Step 6 Enter the SNMP RO community in the **snmp_commnity_string** field.

Configuring Authentication and Authorization Policies

Cisco ISE comes with prepopulated authentication and authorization policies:

- Choose **Policy > Authentication** to check if the Wired_802.1X and Wireless_802.1X authentication policies exist.
- Choose **Policy > Authorization** and check if the Wired_802.1X and Wireless_802.1X authorization policies exist.
- Choose **Policy > Conditions > Compound Conditions**, if required, to edit these policies.

To create an authorization policy for an employee on Corporate WLAN using dot1x, perform the following steps:

Step 1 Choose **Policy > Authorization**.

Step 2 Click **Drop First Down Arrow** next to the Edit button and select **Insert New Rule Above**.

Step 3 Enter the name of the rule.

Step 4 Choose the following conditions from the **Condition** field:

- Condition 1: Add Identity groups for the incoming wireless user.
- Condition 2: Select **Wireless dot1x**.

Step 5 Provide the Permit Access using the **Permissions** field.

Step 6 Click **Save**.

Note For information about AAA concepts including converged access details, refer to:

RADIUS Configuration Guide - Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

For information about Cisco ISE, see the:

Wireless LAN802 and wireless–1x Authentication Deployment Guide.