Authentication and Authorization Between Multiple RADIUS Servers

- Information About Authentication and Authorization Between Multiple RADIUS Servers, on page 1
- Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers, on page 2
- Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers, on page 7
- Verifying Split Authentication and Authorization Configuration, on page 9
- Configuration Examples, on page 10

Information About Authentication and Authorization Between Multiple RADIUS Servers

Cisco Embedded Wireless Controller on Catalyst Access Points uses the approach of request and response transaction with a single RADIUS server that combines both authentication and authorization. You can split the authentication and authorization on the controller between multiple RADIUS servers.

A RADIUS sever can assume the role of either an authentication server, authorization server, or both. In cases where there are disparate RADIUS servers for authentication and authorization, the Session Aware Networking (SANet) component on the embedded wireless controller now allows authentication on one server and authorization on another when a client joins the embedded wireless controller.

Authentication can be done using the Cisco ISE, Cisco DNAC, Free RADIUS, or any third-party RADIUS Server. After successful authentication from an authentication server, the embedded wireless controller relays attributes received from the authentication server to another RADIUS sever designated as authorization server.

The authorization server then performs the following:

- Processes received attributes with the other policies or rules defined on the server.
- Derives attributes as part of the authorization response and returns it to the embedded wireless controller.

Note In a split authentication and authorization configuration, both servers must be available and must successfully authenticate and authorize with an ACCESS-ACCEPT for a session to be accepted by the embedded wireless controller.

Note A maximum of 100 entries is supported in the Authentication/Authorization list created through Cisco DNA Center provisioning. The entries beyond 100 do not work even though they can be created.

Configuring 802.1X Security for WLAN with Split Authentication and Authorization Servers

Configuring Explicit Authentication and Authorization Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**.

Step 2 On the **Authentication Authorization and Accounting** page, click the **Servers/Groups** tab.

Step 3 Click the type of AAA server you want to configure from the following options:

- RADIUS
- TACACS+
- LDAP

In this procedure, the RADIUS server configuration is described.

Step 4 With the **RADIUS** option selected, click **Add**.

Step 5 Enter a name for the RADIUS server and the IPv4 or IPV6 address of the server.

Step 6 Enter the authentication and encryption key to be used between the device and the key string RADIUS daemon running on the RADIUS server. You can choose to use either a PAC key or a non-PAC key.

Step 7 Enter the server timeout value; valid range is 1 to 1000 seconds.

Step 8 Enter a retry count; valid range is 0 to 100.

Step 9 Leave the **Support for CoA** field in **Enabled** state.

Step 10 Click **Save & Apply to Device**.

Step 11 On the **Authentication Authorization and Accounting** page, with **RADIUS** option selected, click the **Server Groups** tab.

Step 12 Click **Add**.

Step 13 In the **Create AAA RADIUS Server Group** window that is displayed, enter a name for the RADIUS server group.

Step 14 From the **MAC-Delimiter** drop-down list, choose the delimiter to be used in the MAC addresses that are sent to the RADIUS servers.

Step 15 From the **MAC Filtering** drop-down list, choose a value based on which to filter MAC addresses.

Step 16 To configure dead time for the server group and direct AAA traffic to alternative groups of servers that have different operational characteristics, in the **Dead-Time** field, enter the amount of time, in minutes, after which a server is assumed to be dead.

Step 17 Choose the servers that you want to include in the server group from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 18 Click **Save & Apply to Device**.

Configuring Explicit Authentication Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups**.

Step 2 Choose **RADIUS** > **Servers** tab.

Step 3 Click **Add** to add a new server or click an existing server.

Step 4 Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port.** Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**

Step 5 Click **Apply to Device**.

Step 6 Choose **RADIUS** > **Server Groups** and click **Add** to add a new server group or click an existing server group.

Step 7 Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 8 Click **Apply to Device**.

Configuring Explicit Authentication Server List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:**	Specifies the RADIUS server name.

	Command or Action	Purpose
	`Device(config)# radius server free-radius-authc-server`	
Step 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* **Example:** `Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813`	Specifies the RADIUS server parameters.
Step 5	[**pac**] **key** *key* **Example:** `Device(config-radius-server)# key cisco`	Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authc-server-group`	Creates a radius server-group identification. *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters. If the IP address of the RADIUS server is not added to the routes defined for the controller, the default route is used. We recommend that you define a specific route to source the traffic from the defined SVI in the AAA server group.
Step 8	**server name** *server-name* **Example:** `Device(config)# server name free-radius-authc-server`	Configures the server name.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. For more information, see **Configuring AAA for External Authentication**.

Configuring Explicit Authorization Server List (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA** > **Servers/Groups**.

Step 2 Choose **RADIUS** > **Servers** tab.

Step 3 Click **Add** to add a new server or click an existing server.

Step 4 Enter the **Name**, the **Server Address**, **Key**, **Confirm Key**, **Auth Port** and **Acct Port.** Check the **PAC Key** checkbox and enter the **PAC key** and **Confirm PAC Key**

Step 5 Click **Apply to Device**.

Step 6 Choose **RADIUS** > **Server Groups** and click **Add** to add a new server group or click an existing server group.

Step 7 Enter the **Name** of the server group and choose the servers that you want to include in the server group, from the **Available Servers** list and move them to the **Assigned Servers** list.

Step 8 Click **Apply to Device**.

Configuring Explicit Authorization Server List (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server cisco-dnac-authz-server`	Specifies the RADIUS server name.
Step 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* **Example:** `Device(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813`	Specifies the RADIUS server parameters.
Step 5	[**pac**] **key** *key* **Example:** `Device(config-radius-server)# pac key cisco`	Specify the authorization and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.

	Command or Action	Purpose
Step 7	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authz-server-group`	Creates a radius server-group identification.
Step 8	**server name** *server-name* **Example:** `Device(config)# server name cisco-dnac-authz-server`	
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Authentication and Authorization List for 802.1X Security (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 In the **Security** > **AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.

Step 5 Click **Apply to Device**.

Configuring Authentication and Authorization List for 802.1X Security

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name wlan-id SSID-name* **Example:**	Enters WLAN configuration sub-mode. • *wlan-name*: Is the name of the configured WLAN.

	Command or Action	Purpose
	`Device(config)# wlan wlan-foo 222 foo-ssid`	• *wlan-id*: Is the wireless LAN identifier. Range is from 1 to 512. • *SSID-name*: Is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *wlan-name* command.
Step 4	**security dot1x authentication-list** *authenticate-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list authc-server-group`	Enables authentication list for dot1x security.
Step 5	**security dot1x authorization-list** *authorize-list-name* **Example:** `Device(config-wlan)# security dot1x authorization-list authz-server-group`	Specifies authorization list for dot1x security. For more information on the **Cisco Digital Network Architecture Center (DNAC)**, see the **DNAC documentation**.
Step 6	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Web Authentication for WLAN with Split Authentication and Authorization Servers

Configuring Authentication and Authorization List for Web Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 In the **Security** > **Layer2** tab, uncheck the **WPAPolicy**, **AES** and **802.1x** check boxes.

Step 5 Check the **MAC Filtering** check box to enable the feature. With MAC Filtering enabled, choose the Authorization list from the **Authorization List** drop-down list.

Step 6 In the **Security** > **AAA** tab, choose the Authentication list from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Configuring Authentication and Authorization List for Web Authentication

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-bar 1 bar-ssid`	Enters WLAN configuration sub-mode. • *wlan-name*: Is the name of the configured WLAN. • *wlan-id*: Is the wireless LAN identifier. • *SSID-name*: Is the SSID name which can contain 32 alphanumeric characters. **Note** If you have already configured this command, enter **wlan** *wlan-name* command.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**security web-auth** {**authentication-list** *authenticate-list-name* | **authorization-list** *authorize-list-name*}	Enables authentication or authorization list for dot1x security.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security web-auth authentication-list authc-server-group`	**Note** You get to view the following error, if you do not disable WPA security, AKM for dot1x, and WPA2 security: *% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.*
Step 8	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Split Authentication and Authorization Configuration

To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan-foo 2 foo-ssid
security dot1x authentication-list authc-server-group
security dot1x authorization-list authz-server-group

wlan wlan-bar 3 bar-ssid
security web-auth authentication-list authc-server-group
security web-auth authorization-list authz-server-group
```

To view the AAA authentication and server details, use the following command:

```
Device# show run aaa
!
aaa authentication dot1x default group radius
username cisco privilege 15 password 0 cisco
!
!
radius server free-radius-authc-server
 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
 key cisco
!
radius server cisco-dnac-authz-server
 address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
 pac key cisco
!
!
aaa new-model
aaa session-id common
!
```

To view the authentication and authorization list for 802.1X security, use the following command:

```
Device# show wlan name wlan-foo | sec 802.1x
802.1x authentication list name               : authc-server-group
802.1x authorization list name                : authz-server-group
            802.1x                            : Enabled
```

To view the authentication and authorization list for web authentication, use the following command:

```
Device# show wlan name wlan-bar | sec Webauth
    Webauth On-mac-filter Failure             : Disabled
    Webauth Authentication List Name          : authc-server-group
    Webauth Authorization List Name           : authz-server-group
    Webauth Parameter Map                     : Disabled
```

Configuration Examples

Configuring Cisco Embedded Wireless Controller on Catalyst Access Points for Authentication with a Third-Party RADIUS Server: Example

This example shows how to configure Cisco Embedded Wireless Controller on Catalyst Access Points for authentication with a third-party RADIUS server:

```
Device(config)# radius server free-radius-authc-server
Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
Device(config-radius-server)# key cisco
Device(config-radius-server)# exit
Device(config)# aaa group server radius authc-server-group
Device(config)# server name free-radius-authc-server
Device(config)# end
```

Configuring Cisco Embedded Wireless Controller on Catalyst Access Points for Authorization with Cisco ISE or DNAC: Example

This example shows how to configure Cisco Embedded Wireless Controller on Catalyst Access Points for authorization with Cisco ISE or DNAC:

```
Device(config)# radius server cisco-dnac-authz-server
Device (config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
Device (config-radius-server)# pac key cisco
Device (config-radius-server)# exit
Device(config)# aaa group server radius authz-server-group
Device(config)# server name cisco-dnac-authz-server
Device(config)# end
```