Local Extensible Authentication Protocol

Information About Local EAP

Local Extensible Authentication Protocol (EAP) feature refers to the controller that acts as authenticator and authentication server. Local EAP allows 802.1x authentication on WPA Enterprise wireless clients without the use of any RADIUS server. The Local EAP refers to the EAP authentication server activity and not necessarily tied to the user credentials validation (for example) that can be delegated to an external LDAP database.

Feature Scenarios

Local EAP is designed to allow administrators to use Enterprise-grade 802.1x authentication for a limited number of users in situations and branches where an external dedicated RADIUS server may not be available. It can also work as an emergency backup in case the RADIUS server is not available.

Use Cases

You can implement Local EAP either with users local to the controller or use an external LDAP database to store the user credentials.

Restrictions for Local EAP

- It is not possible to configure AAA attributes, such as per-user ACL or per-user session timeout using local EAP.
- Local EAP only allows user database either locally on the controller or on an external LDAP database.
- Local EAP supports TLS 1.2 as of 17.1 and later software release.
- Local EAP uses the trustpoint of your choice on the controller. You will either need to install a publicly trusted certificate on the controller or import it on the clients for the EAP session to be trusted by the client.
- Local EAP supports *EAP-FAST*, *EAP-TLS*, and *PEAP* as EAP authentication methods.

Note *PEAP-mschapv2* does not work when using certain external LDAP databases that only support clear text passwords.

Configuring Local EAP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**eap profile** *name* **Example:** `Device(config)# eap profile mylocapeap`	Creates an EAP profile.
Step 3	**method peap** **Example:** `Device(config-eap-profile)# method peap`	Configures the PEAP method on the profile.
Step 4	**pki-trustpoint** *name* **Example:** `Device(config-eap-profile)# pki-trustpoint admincert`	Configures the PKI trustpoint on the profile.

Configuring Local EAP profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Local EAP**.

Step 2 Click **Add**.

Step 3 In the **Create Local EAP Profiles** page, enter a profile name.

Note
It is not advised to use LEAP EAP method due to its weak security. You can use any of the following EAP methods to configure a trustpoint:

- EAP-FAST
- EAP-TLS
- PEAP

Clients do not trust the default controller certificate, so you need to deactivate the server certificate validation on the client side or install a certificate trustpoint on the controller.

Step 4 Click **Apply to Device**.

Configuring AAA Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **AAA**, and navigate to the **AAA Method List** > **Authentication** tabs.

Step 2 Click **Add**.

Step 3 Choose **dot1x** as the **Type** and **local** as the **Group Type**.

Step 4 Click **Apply to Device**.

Configuring AAA Authorization Method (GUI)

Procedure

Step 1 Navigate to **Authorization** sub-tab.

Step 2 Create a new method for **credential-download** type and point it to local.

Note
Perform the same for **network** authorization type.

Configuring AAA Authorization Method (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 3	**aaa authentication dot1x default local** **Example:** `Device(config)# aaa authentication dot1x default local`	Configures the default local RADIUS server.
Step 4	**aaa authorization credential-download default local** **Example:** `Device(config)# aaa authorization credential-download default local`	Configures default database to download credentials from local server.
Step 5	**aaa local authentication default authorization default** **Example:** `Device(config)# aaa local authentication default authorization default`	Configures the local authentication method list.
Step 6	**aaa authorization network default local** **Example:** `Device(config)# aaa authorization network default local`	Configures authorization for network services.

Configuring Local Advanced Methods (GUI)

Procedure

Step 1 In the **Configuration** > **Security** > **AAA** window, perform the following:

a. Navigate to **AAA Advanced** tab.

b. From the **Local Authentication** drop-down list, choose a default local authentication.

c. From the **Local Authorization** drop-down list, choose a default local authorization.

Step 2 Click **Apply**.

Configuring WLAN (GUI)

Procedure

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

Step 2 In the **WLANs** window, click the name of the **WLAN** or click **Add** to create a new one.

Step 3 In the **Add/Edit WLAN** window that is displayed, click the **General** tab to configure the following parameters.

- In the **Profile Name** field, enter or edit the name of the profile.
- In the **SSID** field, enter or edit the SSID name.

  The SSID name can be alphanumeric, and up to 32 characters in length.
- In the **WLAN ID** field, enter or edit the ID number. The valid range is between 1 and 512.
- From the **Radio Policy** drop-down list, choose the **802.11** radio band.
- Using the **Broadcast SSID** toggle button, change the status to either **Enabled** or **Disabled**.
- Using the **Status** toggle button, change the status to either **Enabled** or **Disabled**.

Step 4 In the **AAA** tab, you can configure the following:

a. Choose an authentication list from the drop-down.

b. Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN. Also, choose the required **EAP Profile Name** from the drop-down list.

Step 5 Click **Save & Apply to Device**.

Configuring WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan localpeapssid 1 localpeapssid`	Enters the WLAN configuration sub-mode. *wlan-name*—Is the name of the configured WLAN. *wlan-id*—Is the wireless LAN identifier. The range is 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 3	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	**local-auth** *profile name* **Example:** `Device(config-wlan)# local-auth mylocaleap`	Sets EAP Profile on an WLAN. *profile name*—Is the EAP profile on an WLAN.

Creating a User Account (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**user-name** *user-name* **Example:** `Device(config)# user-name 1xuser`	Creates a user account.
Step 3	**creation-time** *time* **Example:** `Device(config)# creation-time 1572730075`	Creation time of the user account.
Step 4	**description** *user-name* **Example:** `Device(config)# description 1xuser`	Adds a user-defined description to the new user account.
Step 5	**password 0** *password* **Example:** `Device(config)# password 0 Cisco123`	Creates a password for the user account.
Step 6	**type network-user description** *user-name* **Example:** `Device(config)# type network-user description 1xuser`	Specifies the type of user account.

Attaching a Policy Profile to a WLAN Interface (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.
Step 2 On the **Manage Tags** page, click **Policy** tab.
Step 3 Click **Add** to view the **Add Policy Tag** window.
Step 4 Enter a name and description for the policy tag.
Step 5 Click **Add** to map the WLAN and policy.
Step 6 Choose the WLAN profile to map with the appropriate policy profile, and click the tick icon.
Step 7 Click **Save & Apply to Device**.

Deploy Policy Tag to Access Points (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **All Access Points** page, click the access point you want to configure.

Make sure that the tags assigned are the ones you configured.

Step 3 Click **Apply**.