Configuring Local Policies

Information About Local Policies

Controller can do profiling of devices based on protocols such as HTTP, DHCP, and so on to identify the clients. You can configure the device-based policies and enforce per-user or per-device policy on the network. The controller also displays statistics that are based on per-user or per-device end points and policies that are applicable per device. The maximum number of policies that you can configure is 64.

The policies are defined based on the following attributes:

- User group or user role
- Device type such as Windows clients, smartphones, tablets, and so on
- Service Set Identifier (SSID)
- Location, based on the access point group that the end point is connected to
- Time of the day
- Extensible Authentication Protocol (EAP) type, to check what EAP method that the client is getting connected to

When these policy attributes match, you can define the following actions:

- Virtual local area network (VLAN)
- Access control list (ACL)
- Quality of Service (QoS) level

- Session timeout value
- Sleeping client timeout value
- Select either AVC profile or role, or both based on local policy attributes defined in the AAA server.

  The following are the different ways by which local policies are applied based on a combination of AVC profile and role defined in the AAA server:

  - Both AVC profile and role are derived from the AAA server, the following options are available:
    - If AAA override is enabled, then AVC profile is prioritized and is applied.
    - If AAA override is disabled, then role matching is applied.
  - Only role is derived from the AAA server and role matching takes place, the following options are available:
    - If profile is defined in the policy, then role policy is applied.
    - If profile is not defined in the policy, then AVC profile defined in WLAN is applied.
  - Only AVC profile is derived from the AAA server, the following options are available:
    - If AAA override is enabled, then AVC profile received from the AAA server is applied.
    - If AAA override is disabled, then AVC profile defined on the WLAN is applied.

Restrictions for Local Policy Classification

- If you enable AAA override and there are AAA attributes other than the role type from the AAA server, the configured policy action is not applied. The AAA override attributes have higher precedence.
- On a WLAN, when local profiling is enabled, RADIUS profiling is not allowed.
- Client profiling uses existing profiles on the controller.
- You cannot create custom profiles.
- Wired clients behind the workgroup bridge (WGB) are not profiled and the policy action is not taken.
- Only the first policy rule which matches with the policy profile is given precedence. Each policy profile has an associated policy rule, which is used to match the policies.
- You can configure up to 64 policies, out of which you can configure up to 16 policies per WLAN.
- Policy action is taken after Layer 2 authentication is complete, or after Layer 3 authentication is complete, or when the device sends HTTP traffic and gets the device profiled. Therefore, profiling and policy actions occur more than once per client.
- Only VLAN, ACL, Session Timeout, and QoS are supported as policy action attributes.
- Profiling is performed only on IPv4 clients.
- For all the controllers in a mobility group, it is mandatory that the local policy configurations have the same match criteria attributes and action attributes. Otherwise, the local policy configuration becomes invalid when roaming occurs across the controllers.

- When local policy is configured for device type policy match and configured on a WLAN with guest anchor enabled, the AVC profile name from local policy is not applied at anchor.

Table 1: Differences Between Cisco Identity Services Engine (ISE) and Controller Profiling Support

ISE	Controller
Supports profiling using RADIUS probes, DHCP probes, HTTP, and other protocols used to identify the client type.	Supports MAC OUI, DHCP, and HTTP-based profiling.
Supports multiple different attributes for the policy action and has an interface to pick and select each of the attributes.	Supports VLAN, ACL, Session Timeout, and QoS as policy action attributes.
Supports customization of profiling rules with user-defined attributes.	Supports only default profiling rules.

Configuring Local Policies (GUI)

Step 1 Choose **Security** > **Local Policies**.

Step 2 Click **New** to create a new policy.

Step 3 Enter the policy name and click **Apply**.

Step 4 On the **Policy List** page, click the policy name to be configured.

Step 5 On the **Policy > Edit** page, follow these steps:

a) In the **Match Criteria** area, enter a value for **Match Role String**. This is the user type or user group of the user, for example, student, teacher, and so on.

b) From the **Match EAP Type** drop-down list, choose the EAP authentication method used by the client.

c) From the **Device Type** drop-down list, choose the device type.

d) Click **Add** to add the device type to the policy device list.
The device type you choose is listed in the **Device List**.

e) In the **Action** area, specify the policies that are to be enforced. From the **IPv4 ACL** drop-down list, choose an IPv4 ACL for the policy.

f) Enter the **VLAN ID** that should be associated with the policy.

g) From the **QoS Policy** drop-down list, choose a QoS policy to be applied.

h) Enter a value for **Session Timeout**. This is the maximum amount of time, in seconds, after which a client is forced to reauthenticate.

i) Enter a value for **Sleeping Client Timeout**, which is the timeout for sleeping clients.
Sleeping clients are clients with guest access that have had successful web authentication that are allowed to sleep and wake up without having to go through another authentication process through the login page.

This sleeping client timeout configuration overrides the WLAN-specific sleeping client timeout configuration.

j) From the **AVC Profile** drop-down list, choose an AVC profile to be applied based on the role defined in AAA.

k) In the **Active Hours** area, from the **Day** drop-down list, choose the days on which the policy has to be active.

l) Enter the **Start Time** and **End Time** of the policy.
m) Click **Add**.
The day and start time and end time that you specify is listed.
n) Click **Apply**.

What to Do Next

Apply a local policy that you have created to a WLAN by following these steps:

1. Choose **WLANs**.
2. Click the corresponding WLAN ID.
   The **WLANs > Edit** page is displayed.
3. Click the **Policy-Mapping** tab.
4. Enter the **Priority Index** for a policy.
5. From the **Local Policy** drop-down list, choose the policy that has to be applied for the WLAN.
6. Click **Add**.
   The priority index and the policy that you choose is listed. You can apply up to 16 policies for a WLAN.

Configuring Local Policies (CLI)

- Create or delete a local policy by entering this command:
  config policy *policy-name* {**create** | **delete**}
- Configure a match type to a policy by entering these commands:
  - **config policy** *policy-name* **match device-type** {**add** | **delete**} *device-type*
  - **config policy** *policy-name* **match eap-type** {**add** | **delete**} {**eap-fast** | **eap-tls** | **leap** | **peap**}
  - **config policy** *policy-name* **match role** {*role-name* | *none*}
- Configure an action that has to be enforced as part of a policy by entering these commands:
  - ACL action to a policy—**config policy** *policy-name* **action acl** {**enable** | **disable**} *acl-name*
  - QoS average data rate—**config policy** *policy-name* **action average-data-rate** {**enable** | **disable**} *rate*
  - QoS average real-time data rate—**config policy** *policy-name* **action average-realtime-rate** {**enable** | **disable**} *rate*
  - QoS burst data rate—**config policy** *policy-name* **action burst-data-rate** {**enable** | **disable**} *rate*
  - QoS burst real-time data rate—**config policy** *policy-name* **action burst-realtime-rate** {**enable** | **disable**} *rate*

- QoS action—**config policy** *policy-name* **action qos** {**enable** | **disable**} {**bronze** | **gold** | **platinum** | **silver**}
- Session timeout action—**config policy** *policy-name* **action session-timeout** {**enable** | **disable**} *timeout-in-seconds*
- Sleeping client timeout action—**config policy** *policy-name* **action sleeping-client-timeout** {**enable** | **disable**} *timeout-in-hours*
- Enable AVC profile—**config policy** *policy-name* **action avc-profile-name enable** *avc-profile-name*
- Disable AVC profile—**config policy** *policy-name* **action avc-profile-name disable**
- VLAN action—**config policy** *policy-name* **action vlan** {**enable** | **disable**} *vlan-id*

Note Ensure that you configure the Average Data Rate before you configure the Burst Data Rate.

- Configure the active time for a policy by entering this command:
  config policy *policy-name* **active** {**add** | **delete**} **hours start-time end-time days** {*mon* | *tue* | *wed* | *thu* | *fri* | *sat* | *sun* | *daily* | *weekdays*}
- Apply a local policy to a WLAN by entering this command:
  config wlan policy {**add** | **delete**} *priority-index policy-name wlan-id*
- Enable or disable client profiling in local mode for a WLAN, based on HTTP, DHCP, or both by entering this command:
  config wlan profiling local {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*
- Apply a local policy to an AP group of a WLAN by entering this command:
  config wlan apgroup policy {**add** | **delete**} *priority-index policy-name ap-group-name wlan-id*
- View information about a policy by entering this command:
  show policy {**summary** | *policy-name*} **statistics**
- View local device classification profile summary by entering this command:
  show profiling policy summary
- View all the clients with a type of device by entering this command:
  show client wlan *wlan-id* **device-type** *device-type*
- View a client profiling status that includes profiling done by the RADIUS server and the controller by entering this command:
  show wlan *wlan-id*
- View the policy details for AP groups by entering this command:
  show wlan apgroups
- Configure the task of debugging of policies by entering this command:
  debug policy {**error** | **event**} {**enable** | **disable**}

Updating Organizationally Unique Identifier List

Updating Organizationally Unique Identifier List (GUI)

Step 1 Copy the latest OUI list available at http://standards.ieee.org/develop/regauth/oui/oui.txt to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.
The **Download file to Controller** page is displayed.

Step 3 From the **File Type** drop-down list, choose **OUI Update**.

Step 4 From the **Transfer Mode** drop-down list, choose the server type.
The server details are displayed on the same page.

Step 5 Click **Download**.

Step 6 After the download is complete, reboot the Cisco WLC by choosing **Commands** > **Reboot**.

Step 7 If prompted to save your changes, click **Save and Reboot**.

Step 8 Click **OK**.

Updating Organizationally Unique Identifier List (CLI)

Step 1 Copy the latest OUI list available at http://standards.ieee.org/develop/regauth/oui/oui.txt to the default directory on your server.

Step 2 Specify the server type by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the file type by entering this command:
transfer download datatype oui-update

Step 4 Begin the download of the file by entering this command:
transfer download start
Note Follow the on-screen instructions to complete the download process.

Step 5 Reboot the Cisco WLC by entering this command:
reset system

Step 6 See the updated OUI list by entering this command:
show profiling oui-string summary
Note HA support for OUI update: HA link must be up while downloading the OUI file to the Active controller, so that the OUI update gets applied to the Standby controller as well.

Updating Device Profile List

Updating Device Profile List (GUI)

Step 1 Copy the latest device profile list file to the default directory on your server.

Step 2 Choose **Commands** > **Download File**.
The **Download file to Controller** page is displayed.

Step 3 From the **File Type** drop-down list, choose **Device Profile**.

Step 4 From the **Transfer Mode** drop-down list, choose the server type.
The server details are displayed on the same page.

Step 5 Click **Download**.

Step 6 After the download is complete, reboot the Cisco WLC by choosing **Commands** > **Reboot**.

Step 7 If prompted to save your changes, click **Save and Reboot**.

Step 8 Click **OK**.

Updating Device Profile List (CLI)

Step 1 Copy the latest device profile list file to the default directory on your server.

Step 2 Specify the server type by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the file type by entering this command:
transfer download datatype device-profile

Step 4 Specify the file name by entering this command:
transfer download filename *device_profile-xml-file*

Step 5 Begin the download of the file by entering this command:
transfer download start
Note Follow the on-screen instructions to complete the download process.

Step 6 Reboot the Cisco WLC by entering this command:
reset system

Step 7 See the updated OUI list by entering this command:
show profiling policy summary