Policy Classification Engine

The Policy Classification Engine feature helps configure device-based policies and client (network endpoint) profiling and enforces a per user or per device policy on a network. The policy classification engine enables bring-your-own-device (BYOD) deployments integrate user or wireless device policies into the wireless controller. This module explains how to configure policies and apply them to a wireless LAN (WLAN).

- Finding Feature Information, page 1
- Restrictions for Policy Classification Engine, page 1
- Information About Policy Classification Engine, page 2
- How to Configure Policy Classification Engine, page 2
- Configuration Examples for Policy Classification Engine, page 7
- Additional References for Policy Classification Engine, page 8
- Feature Information for Policy Classification Engine, page 9

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Policy Classification Engine

Interface templates are not valid on wireless sessions.

Information About Policy Classification Engine

Policy Classification Engine Overview

The Policy Classification Engine feature helps configure device-based policies and client (network endpoint) profiling and enforces a per user or per device policy on a network.

You can configure sets of different policies that can be used for lookup and sequential matching. A policy is matched based on the configured policy statement. Use policies to profile devices based on the Dynamic Host Control Protocol (DHCP) or HTTP to identify end devices in a network. You can enforce specific policies at network endpoints.

The device (switch; for example, Cisco Catalyst 3850 Wireless LAN Controller) uses these attributes and predefined classification profiles to identify devices.

Policies are configured based on the following parameters:

- Device—Types of end devices. Examples are Windows machines, smart phones, Apple device like iPads, iPhones, and so on.
- Regular expressions
- User role—The user type or user group to which an user belongs. Examples are students, employees, and so on.
- Username—Login credentials entered by users.
- Time-of-day—The time-of-day when endpoints are allowed into a network.
- OUI—The MAC address that identifies the Organizational Unique Identifier (OUI).
- MAC address—The MAC address of the endpoint.

Once the device (switch) has a match corresponding to the policy parameters per end point, a policy is added. Policy enforcement is based on the following session attributes:

- VLAN—User-defined VLAN
- Access control list (ACL)
- Session timeout value—User-defined timeout for client sessions
- Quality of service (QoS)

You can configure policies and based on the session attributes, enforce these policies on end points.

How to Configure Policy Classification Engine

Configuring Policies in Identity-Based Networking Services

To configure policies, perform the following tasks:

1 Configure a service template.

For more information, see the Configuring Identity Services Templates module.

2 Configure an interface template.

For more information, see the Interface Templates module.

3 Create a parameter map.

4 Create a policy map.

5 Apply the policy on a wireless LAN (WLAN).

Configuring a Subscriber Parameter Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type subscriber attribute-to-service** *parameter-map-name*
4. *priority-number* **map device-type eq** *device-type* **oui eq** *MAC-address*
5. *action-number* **interface-template** *interface-template-name*
6. **end**
7. **show parameter-map type subscriber attribute-to-service** *parameter-map-name*

DETAILED STEPS

	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	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Device(config)# parameter-map type subscriber attribute-to-service param-map`	Configures a subscriber parameter map and enters parameter-map filter configuration mode.

	Command or Action	Purpose
Step 4	*priority-number* **map device-type eq** *device-type* **oui eq** *MAC-address* **Example:** `Device(config-parameter-map-filter)# 1 map device-type eq “Cisco-IP-Phone-9971” oui “eq 08.cc.68”`	Maps the priority and the Organizationally Unique Identifier (OUI) of the configured device, and enters parameter-map filter submode configuration mode.
Step 5	*action-number* **interface-template** *interface-template-name* **Example:** `Device(config-parameter-map-filter-submode)# 2 interface-template IP-PHONE-INTERFACE-TEMPLATE`	Maps the action number to an interface template.

Step 6	**end**
	Example:
	`Device(config-parameter-map-filter-submode)# end`
		Exits parameter-map filter submode configuration mode and returns to privileged EXEC mode.

Step 7	**show parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Device# parameter-map type subscriber attribute-to-service parameter-map-name`	Displays information about the specified parameter map.

Example

The following is sample output from the **show parameter-map type subscriber attribute-to-service** command:

```
Device# show parameter-map type subscriber attribute-to-service param-map

Parameter-map name: param-map
 Map: 1 map device-type eq "Cisco-IP-Phone-9971" oui eq "08.cc.68"
  Action(s):
   2 interface-template IP-PHONE-INTERFACE-TEMPLATE
```

Configuring a Subscriber Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control subscriber** *policy-map-name*
4. **event identity-update** {**match-all** | **match-first**}
5. *priority-number* **class always** {**do-all** | **do-until-failure** | **do-until-success**}
6. *action-number* **map attribute-to-service table** *parameter-map-name*
7. **end**
8. **show policy-map type control subscriber** *policy-map-name*

DETAILED STEPS

	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	**policy-map type control subscriber** *policy-map-name* **Example:** `Device(config)# policy-map type control subscriber pmap`	Defines a control policy for subscriber sessions and enters control policy-map event configuration mode.

Step 4	**event identity-update** {**match-all** | **match-first**}
	Example:
	`Device(config-event-control-policymap)# event identity-update match-all`
		Specifies the event type that triggers actions in a control policy if conditions are met, and enters control policy-map class configuration mode.

Step 5	*priority-number* **class always** {**do-all** | **do-until-failure** | **do-until-success**}
	Example:
	`Device(config-class-control-policymap)# 1 class always do-until-failure`
		Associates a control class with one or more actions in a control policy and enters control policy-map action configuration mode.

Step 6	*action-number* **map attribute-to-service table** *parameter-map-name*	Maps identity-update attribute to an autoconf template.

	Command or Action	Purpose
	Example: `Device(config-action-control-policymap)# 2 map attribute-service table param-map`	

Step 7	**end**
	Example:
	`Device(config-action-control-policymap)# end`
		Exits control policy-map action configuration mode and returns to privileged EXEC mode.

Step 8	**show policy-map type control subscriber** *policy-map-name* **Example:** `Device# show policy-map type control subscriber pmap`	Displays information and statistics about the control policies.

Example

The following is sample output from the **show policy-map type control subscriber** command:

```
Device# show policy-map type control subscriber pmap

show policy-map type control subscriber pmap
policy-map
  event identity-update match-all
    1 class always do-until-failure
      1 map attribute-to-service table param-map
```

Applying a Subscriber Policy to a WLAN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wlan** *wlan-name wlan-ID SSID*
4. **service-policy type control subscriber** *policy-map-name*
5. **profiling local http**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wlan** *wlan-name wlan-ID SSID* **Example:** `Device(config)# wlan wlan1 9 policywlan`	Configures a wireless LAN (WLAN) network and enters WLAN configuration mode.
Step 4	**service-policy type control subscriber** *policy-map-name* **Example:** `Device(config-wlan)# service-policy type control subscriber pmap`	Defines a service policy for subscriber sessions.
Step 5	**profiling local http** **Example:** `Device(config-wlan)# profiling local http`	Configures client profiling on a WLAN based on HTTP attributes.

Step 6	**end**
	Example:
	`Device(config-wlan)# end`
		Exits WLAN configuration mode and returns to privileged EXEC mode.

Configuration Examples for Policy Classification Engine

Example: Configuring a Subscriber Parameter Map

```
Device# configure terminal
Device(config)# parameter-map type subscriber attribute-to-service param-map
Device(config-parameter-map-filter)# 1 map device-type eq “Cisco-IP-Phone-9971” oui “eq
08.cc.68”
Device(config-parameter-map-filter-submode)# 2 interface-template IP-PHONE-INTERFACE-TEMPLATE
Device(config-parameter-map-filter-submode)# end
```

Example: Configuring a Subscriber Policy Map

```
Device# configure terminal
Device(config)# policy-map type control subscriber pmap
Device(config-event-control-policymap)# event identity-update match-all
Device(config-class-control-policymap)# 1 class always do-until-failure
Device(config-action-control-policymap)# 2 map attribute-service table param-map
Device(config-action-control-policymap)# end
```

Example: Applying a Subscriber Policy to a WLAN

```
Device# configure terminal
Device(config)# wlan wlan1 9 policywlan
Device(config-wlan)# service-policy type control subscriber pmap
Device(config-wlan)# profiling local http
Device(config-wlan)# end
```

Additional References for Policy Classification Engine

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Identity commands	Cisco IOS Identity-Based Networking Services Command Reference
Service templates	"Configuring Identity Service Templates" module of the `Identity-Based Networking Services Configuration Guide`
Interface templates	"Interface Templates" module of the `Identity-Based Networking Services Configuration Guide`

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Policy Classification Engine

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Policy Classification Engine

Feature Name	Releases	Feature Information
Policy Classification Engine	Cisco IOS XE Release 3.6E Cisco IOS 15.2(1)SY	The Policy Classification Engine feature helps configure device-based policies and client (network endpoint) profiling and enforces a per user or per device policy on a network. The policy classification engine enables bring-your-own-device (BYOD) deployments integrate user or wireless device policies into the wireless controller. In Cisco IOS XE 3.6E, this feature is supported on the following platforms: • Cisco 5700 Series Wireless LAN Controllers • Cisco Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches In Cisco IOS 15.2(SY), this feature was supported on Cisco Catalyst 6500 Series Switches.