Configuring Local Policies

Restrictions for Configuring Local Policies

- The policy map attributes supported on the device are QoS, VLAN, session timeout, and ACL.
- Apple iphone 6s will get classified as "workstation" after HTTP profiling.

Information About Configuring Local Policies

Local policies can profile devices based on HTTP and DHCP to identify the end devices on the network. Users can configure device-based policies and enforce the policies per user or per device policy on the network.

Local policies allow profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN. They also assign ACL and QoS or configure session timeouts. You can configure local policies as two separate components:

- Defining policy attributes as service templates specific to clients joining the network and applying policy match criteria.
- Applying match criteria to the policy.

The following policy match attributes are used for configuring local policies:

- Device—Defines the type of device. Windows-based computer, Smart phone, Apple devices such as iPad and iPhone.
- Username—Defines the username of the user.
- User role—Defines the user type or the user group the user belongs to, such as a student or employee.

- MAC—Defines the mac-address of the end point.
- MAC OUI—Defines the mac-address OUI.

Once the device has a match corresponding to these parameters per end point, the policy can be added. Policy enforcement allows basic device on-boarding of mobile devices based on the following session attributes:

- VLAN
- QoS
- ACL
- Session timeout

You can configure these policies and enforce end points with specified policies. The wireless clients are profiled based on MAC OUI and DHCP. The device uses these attributes and predefined classification profiles to identify devices.

Replacing Default Profile Text File

If a new device is not classified, contact the Cisco support team with the device MAC address. The Cisco support team will provide a new **dc_default_profile.txt** file with the MAC address included in the file. You need to replace the **dc_default_profile.txt** file with the earlier file. Follow these steps to change the **dc_default_profile.txt** file:

1. Stop device classifier by entering this command:

   device**(config)# no device classifier**

2. Copy the file by entering this command:

   device**# device classifier profile location** *filepath*

3. Start the device classifier by entering this command:

   device**(config)# device classifier**

Disabling session monitor on trunk ports

On uplink trunk ports, you should not create any session monitoring. By default, session monitoring is enabled. You should disable session monitoring.

1. Enter into global configuration mode by entering this command:

   device**# configure terminal**

2. Enter into interface configuration mode by entering this command:

   device**(config)# interface** *interface-id*

3. Disable session monitoring by entering this command:

   device**(config-if)# no access-session monitor**

How to Configure Local Policies

Configuring Local Policies (CLI)

To configure local policies, complete these procedures:

1. Create a service template.
2. Create an interface template.
3. Create a parameter map.
4. Create a policy map.
5. Apply a local policy on a WLAN.

Creating an Interface Template (CLI)

Procedure

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

Step 2	**template** *interface-template-name*
	Example:
	`Device(config)# template cisco-phone-template`
	`Device(config-template)#`
		Enters interface template configuration mode.

Step 3	**switchport mode access** **Example:** `Device(config-template)# switchport mode access`	Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1.
Step 4	**switchport voice vlan** *vlan_id* **Example:** `Device(config-template)# switchport voice vlan 20`	Specifies to forward all voice traffic through the specified VLAN. You can specify a value from 1 to 4094.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Parameter Map (CLI)

Parameter map is preferred to use than class map.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* **Example:** `Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	Specifies the parameter map type and name.
Step 3	*map-index* **map** { **device-type** | **mac-address** | **oui** | **user-role** | **username**} {**eq** | **not-eq** | **regex** *filter-name* } **Example:** `Device(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	Specifies parameter map attribute filter criteria.

Step 4	**interface-template** *interface-template-name*
	Example:
	`Device(config-parameter-map-filter-submode)# interface-template cisco-phone-template`
	`Device(config-parameter-map-filter-submode)#`
		Enters service template configuration mode.

Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Class Map (CLI)

Procedure

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

	Command or Action	Purpose
Step 2	**class-map type control subscriber** *class-map-name* { **match-all** | **match-any** | **match-first** } **Example:** `Device(config)# class-map type control subscriber CLASS_AC_1 match-all`	Specifies the class map type and name.
Step 3	**match** {**device-type** | **mac-address** | **oui** | **username** | **userrole**} *filter-type-name* **Example:** `Device(config-class-map)# match device-type Cisco-IP-Phone-7961`	Specifies class map attribute filter criteria.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Creating a Policy Map (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map type control subscriber** *policy-map-name* **Example:** `Device(config)# policy-map type control subscriber Aironet-Policy`	Specifies the policy map type.
Step 3	**event identity-update** {**match-all** | **match-first**} **Example:** `Device(config-policy-map)# event identity-update match-all`	Specifies match criteria to the policy map.
Step 4	*class_number* **class** {*class_map_name* | **always** } {**do-all** | **do-until-failure** | **do-until-success**}	Configures the local profiling policy class map number and specifies how to perform the action. The class map configuration mode includes the following command options:

	Command or Action	Purpose
	Example: `Device(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	• **always**—Executes without doing any matching but return success. • **do-all**—Executes all the actions. • **do-until-failure**—Execute all the actions until any match failure is encountered. This is the default value. • **do-until-success**—Execute all the actions until any match success happens.
Step 5	*action-index* **map attribute-to-service table** *parameter-map-name* **Example:** `Device(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	Specifies parameter map table to be used.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Applying a Local Policy for a Device on a WLAN (CLI)

Before you begin

If the service policy contains any device type-based rules in the parameter map, ensure that the device classifier is already enabled.

Note You should use the **device classification** command to classify the device for it to be displayed correctly on the show command output.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device(config)# wlan wlan1`	Enters WLAN configuration mode.
Step 3	**service-policy type control subscriber** *policymapname*	Applies local policy to WLAN.

	Command or Action	Purpose
	Example: `Device(config-wlan)# service-policy type control subscriber Aironet-Policy`	
Step 4	**profiling local http (optional)** **Example:** `Device(config-wlan)# profiling local http`	Enables only profiling of devices based on HTTP protocol (optional).
Step 5	**profiling radius http (optional)** **Example:** `Device(config-wlan)# profiling radius http`	Enables profiling of devices on ISE (optional).
Step 6	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Specifies not to shut down the WLAN.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Local Policies

The following commands can be used to monitor local policies configured on the device.

Table 1: Monitoring Local Policies Command

Command	Purpose
show access-session	Displays the summary of access session with authorization status, method and domain for each client or MAC address displayed.
show access-session cache	Displays the latest classification for the client.
show device classifier attached detail	Displays the latest classification for the client based on parameters such as Mac, DHCP, or HTTP.
show access-session mac *mac-address* **details**	Displays the policy mapped, service template used, and attributes for the client. **Note** If the **show access-session detail** command output is not displaying session timeout details, you should enable client profiling with session timeout in client access session and then run the **show access-session mac** *mac-address* **details** command to see the session timeout details.

show access-session mac *mac-address* **policy**	Displays the policy mapped, service template used, and attributes for the client. In addition, you can view the **Resultant Policy** that displays the following information: • The final attributes applied to the session when the session has locally configured attributes. • Attributes applied from the server.

Examples: Local Policies Configuration

Note At the end of each configuration command line, enter CTRL Z to execute the command and proceed to the next line.

This example shows how to create interface template:

```
Device# configure terminal
Device(config)#template cisco-phone-template
Device(config-template)#switchport mode access
Device(config-template)#switchport voice vlan 20
Device(config-template)# end
```

This example shows how to create parameter map:

```
Device# configure terminal
Device(config)#parameter-map type subscriber attribute-to-service param-wired
Device(config-parameter-map-filter)#10 map device-type regex Cisco-IP-Phone
Device(config-parameter-map-filter-submode)#10 interface-template cisco-phone-template
Device(config-parameter-map)# end
```

This example shows how to create policy map:

```
Device(config)# policy-map type control subscriber apple-tsim
Device(config-policy-map)# event identity-update match-all
Device(config-policy-map)# 1 class always do-until-failure
Device(config-policy-map)# 1 map attribute-to-service table apple-tsim-param
Device(config-policy-map)# end
```

This example shows how to apply policy to a device on a WLAN:

```
Device(config)# wlan wlan1
Device(config-wlan)# client vlan VLAN0054
Device(config-wlan)# profiling local http
Device(config-wlan)# service-policy type control subscriber apple-tsim
Device(config-wlan)# no shutdown
Device# end
```

Additional References for Configuring Local Policies

Related Documents

Related Topic	Document Title
Security commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 History for Performing Local Policies Configuration

Release	Feature Information
Cisco IOS XE 3E	This feature was introduced.