

Profiling

New OUI's for Devices

- In the future, there is slated to be a “feed service” for profiling dictionaries.
 - This will alleviate the issues of not having the new OUI's for the latest i-device, etc...
- While we wait for the much anticipated ISE feature, new profile dictionaries are shipped with interim releases, etc...
 - We can manually update our own libraries.

Profiling

New OUI's for Devices

The screenshot displays the Cisco Profiling configuration page. The navigation bar includes Home, Operations, Policy, and Administration. The main menu has Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The 'Conditions' tab is active, showing a list of categories: Authentication, Authorization, Profiling, Posture, Guest, and Common. The 'New Profiler Condition' form is filled with the following details:

- Name:** Apple-OUI-Rule1
- Description:** New Apple OUI - Added 3-6-12
- Type:** Mac
- Attribute Name:** MACAddress
- Operator:** CONTAINS
- Attribute Value:** 18:20:32

Buttons for 'Submit' and 'Cancel' are visible at the bottom of the form.

Profiling

New OUI's for Devices

The screenshot shows the Cisco Profiling configuration interface. The top navigation bar includes Home, Operations, Policy, and Administration. Below it are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The left sidebar shows a tree view of Profiling Policies, with 'Apple-Device' selected. The main content area is titled 'Profiler Policy List > Apple-Device' and 'Profiler Policy'. It contains the following configuration fields:

- Name:** Apple-Device
- Description:** Generic policy for all Apple devices
- Policy Enabled:**
- Minimum Certainty Factor:** 10 (Valid Range 1 to 65535)
- Exception Action:** NONE
- Network Scan (NMAP) Action:** NONE
- Options:** Create Matching Identity Group, Use Hierarchy
- Parent Policy:** ***NONE***

Under the 'Rules' section, there is one rule: 'If Condition Apple-DeviceRule1Check1 Then Certainty Factor Increases 10'. A gear icon next to the rule allows for actions: 'Insert new rule above', 'Insert new rule below', and 'Delete'. The 'Insert new rule below' option is highlighted with an orange box. 'Save' and 'Reset' buttons are located at the bottom left of the rule configuration area.

Profiling

New OUI's for Devices

The screenshot displays a network management interface with a top navigation bar containing 'Home', 'Operations', 'Policy', and 'Administration'. Below this is a secondary bar with icons for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. A 'Task Navigator' is visible in the top right corner.

The main content area is titled 'Profiler Policy List > Apple-Device' and 'Profiler Policy'. The configuration for the 'Apple-Device' policy is shown, including:

- Name:** Apple-D
- Policy Enabled:**
- Minimum Certainty Factor:** 10
- Exception Action:** NONE
- Network Scan (NMAP) Action:** NONE
- Create M...** (radio button)
- Use Hier...** (radio button, selected)
- Parent Policy:** ***NON

A 'Dictionaries' dropdown menu is open, listing various rules. The rule 'Apple-OUI-Rule1' is highlighted with an orange box. Other visible rules include 'AndroidRule1Check1', 'AndroidRule1Check2', 'Apple-DeviceRule1Check1', 'Apple-MacBookRuleCheck1', 'Apple-MacBookRuleCheck2', 'Apple-iPadRule1Check1', 'Apple-iPadRule1Check3', 'Apple-iPadRule2Check2', 'Apple-iPhoneRule1Check1', 'Apple-iPhoneRule2Check1', 'Apple-iPodRule1Check1', and 'Apple-iPodRule2Check2'.

Below the dictionaries, there are 'Rules' sections with 'If Condition' fields. One field contains 'Apple-DeviceRule1Check1' and another contains 'Select_Attribute_'. There are also input fields for values like '10' and '0'.

At the bottom left, there are 'Save' and 'Res' buttons. A 'Condition Name' field contains 'Select Condition'.

Profiling

New OUI's for Devices

The screenshot shows a network management console with a navigation bar at the top containing: Home, Operations, Policy, Administration, Task Navigator, Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The main interface is titled "Profiler Policy List > Apple-Device".

Profiler Policy

- * Name: Apple-Device
- Description: Generic policy for all Apple devices
- Policy Enabled:
- * Minimum Certainty Factor: 10 (Valid Range 1 to 65535)
- * Exception Action: NONE
- * Network Scan (NMAP) Action: NONE
- Create Matching Identity Group
- Use Hierarchy
- Parent Policy: ***NONE***

Rules

- If Condition: Apple-DeviceRule1Check1 + Then: Certainty Factor Increases 10
- If Condition: Apple-OUI-Rule1 + Then: Certainty Factor Increases 10

Buttons: Save, Reset

Profiling

- Profiling Policies
 - Android
 - Apple-Device
 - Apple-MacBook
 - Apple-iPad
 - Apple-iPhone
 - Apple-iPod
 - Appiera-Device
 - Aruba-Device
 - Avaya-Device
 - BlackBerry
 - Brother-Device
 - Canon-Device
 - Cisco-Device
 - DLink-Device
 - Enterasys-Device
 - HP-Device
 - HTC-Device