ISE
Profilování typů koncových zařízení

T-SECA2
Jiří Tesař – Cisco
Prosíme, ptejte se nás

- Twitter  www.twitter.com/CiscoCZ
- Talk2cisco  www.talk2cisco.cz/dotazy
- SMS  721 994 600
Program

- K čemu použít ISE Profiling?
- Implementace ISE profilování v živé síti
- Konfigurace profilování
- Monitorování a reportování
- Demo
ISE Profiling
Cisco ISE Device Profiling and Policy Steps

Phase 1: Device Authentication
- EAP
- MAC, DHCP, DNS, HTTP

Phase 2: Device Identification
- ISE

Phase 3: Device Policy
- Limited Access
  - Allowed Device?
  - Allowed Access
  - QoS: • Gold
  - ACL: • Allow-All
  - VLAN: • Employee
ISE Profiler: 3 Steps

Profiling: OUI, DHCP, Netflow, DNS, HTTP, CDP, LLDP

Id Group assignment

Apply Policies

Internet Only  Video Vlan assignment  Printing Vlan  Voice Vlan  SNMP only  Dynamic vlans
Dynamic Policy with Change of Authorization (CoA)

Before – Posture Assessment and Profiling

- **Client Status**: Unknown
- **VLAN**: Limited Access
- **ACL**: Posture-Assessment
- **QoS**: Silver

After – Employee Policy Applied

- **Client Status**: Profiled, Workstation
- **VLAN**: Employee
- **ACL**: None
- **QoS**: Gold

User and Device Specific Attributes

- CoA is based on an extension of RADIUS through RFC3576
Authorization – AAA Server (ISE)

Policy → Authorization

![Image of Identity Services Engine interface with policy rules and authorization profiles]

- **Policy Rule:**
  - **Rule Name:** Dot1X Engineering User
  - Condition: AD1:ExternalGroups EQUALS testname...
  - **Permissions:** Engineering

- **Authorization Profile:**
  - **Name:** Engineering
  - **Description:** Engineering User
  - **Access Type:** ACCESS_ACCEPT

- **Common Tasks:**
  - **DACL Name:** Engineering
  - **VLAN:** Tag ID: 1, ID/Name: Engineering
Authorization – AAA Server (ISE)

Policy → Authorization - Simple

**Identity Services Engine**

**Authorization Policy**
Define the Authorization Policy by configuring rules based on identity groups and/or context.

- **First Matched Rule Applies**
- **Exceptions (0)**

**Standard**

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Identity Groups</th>
<th>Other Conditions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dot1X Engineering User</td>
<td>Any</td>
<td>AD1:ExternalGroups EQUALS testnet.de/Users/EngineeringGrp</td>
<td>Engineering</td>
</tr>
<tr>
<td></td>
<td>Dot1X Marketing User</td>
<td>Any</td>
<td>AD1:ExternalGroups EQUALS testnet.de/Users/MarketingGrp</td>
<td>Marketing</td>
</tr>
<tr>
<td></td>
<td>Default</td>
<td></td>
<td>DenyAccess</td>
<td></td>
</tr>
</tbody>
</table>

**Condition(s) Details**

- AD1:ExternalGroups EQUALS testnet.de/Users/EngineeringGrp
- AD1:ExternalGroups EQUALS testnet.de/Users/MarketingGrp

- **Endpoint Identity Groups**
  - Guest
  - MyUserGrp
  - SponsorAllAccount
  - SponsorGroupAccounts
  - SponsorOwnAccounts
  - Blacklist
  - Profiled
  - Cisco-IP-Phone
  - Workstation
  - Unknown
## Authorization – AAA Server (ISE)

### Policy → Authorization - Advanced

### Authorization Policy At A Glance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Rule Name</th>
<th>Identity Groups</th>
<th>Other Conditions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Profiled Cisco IP Phones</td>
<td>Cisco-IP-Phone</td>
<td>demo.local/ExternalGroups EQUALS demo.local/Users/Domain</td>
<td>Cisco_IP_Phone</td>
</tr>
<tr>
<td>Enabled</td>
<td>Game_Console</td>
<td>Game_Console-Registered</td>
<td></td>
<td>Game_Console</td>
</tr>
<tr>
<td>Enabled</td>
<td>Domain_Computer</td>
<td>Any</td>
<td>Computers AND San_Jose</td>
<td>AD_Login</td>
</tr>
<tr>
<td>Enabled</td>
<td>Employee-Wired</td>
<td>Employee_Wired AND Posture_Compliant</td>
<td></td>
<td>Employee</td>
</tr>
<tr>
<td>Enabled</td>
<td>Employee-IPAD</td>
<td>Employee_Wireless</td>
<td></td>
<td>Employee_IPAD</td>
</tr>
<tr>
<td>Enabled</td>
<td>Contractor-IPAD</td>
<td>Contractor_Wireless</td>
<td></td>
<td>Contractor_IPAD</td>
</tr>
<tr>
<td>Enabled</td>
<td>Guest-Wired</td>
<td>Guest</td>
<td></td>
<td>Guest</td>
</tr>
<tr>
<td>Enabled</td>
<td>Guest-Wireless</td>
<td>Guest</td>
<td></td>
<td>Guest_Wireless</td>
</tr>
<tr>
<td>Disabled</td>
<td>Default-Posture</td>
<td>Any</td>
<td></td>
<td>CWA_Posture_Remediation</td>
</tr>
<tr>
<td>Enabled</td>
<td>Default</td>
<td>Any</td>
<td></td>
<td>Central_web_auth</td>
</tr>
</tbody>
</table>
How do we Build a BYOD Policy?

What are the Required Parts of the Policy?

- Corp Asset?
  - AD Member?
  - Static List?
  - MDM?
  - Certificate?

- AuthC Type
  - Machine Certs?
  - User Certs?
  - Uname/Pwd

- Profile
  - i-Device
  - Android
  - Windows
  - Other

- AuthZ Result
  - Full Access
  - i-Net only
  - VDI + i-Net
Do you know your MAC addresses?

- Number of "other devices" often exceeds number of computers
- Do you know every MAC address?
  - Process to add MAC addresses when purchasing devices
  - Process to remove MAC addresses when removing devices
- Some organization already may have processes in place and be in full control
- For others, Profiling, will help discover and categorize devices, effectively enabling a successful implementation of 802.1X
ISE – MAC Authentication Bypass

Configuration

How to build a MAC Databases?
- Find It (Existing DB)
  e.g. CUCM
- Build It (Not existing DB)
  e.g. Monitor Mode
- Buy It
  e.g. ISE Profiler
# ISE – MAC Authentication Bypass

## Monitor Authentications

![Image of ISE interface showing MAC authentication bypass](image)

### Live Authentications

<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Details</th>
<th>Username</th>
<th>Endpoint ID</th>
<th>IP Address</th>
<th>Network Device</th>
<th>Device Port</th>
<th>Authorization Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 25, 2011 04:51:00.714 PM</td>
<td>✔</td>
<td>00:0C:29:5C:49:6A</td>
<td>00:0C:29:5C:49:6A</td>
<td>00:0C:29:5C:49:6A</td>
<td>Cat3560X</td>
<td>GigabitEthernet0/3</td>
<td>PermitAccess</td>
<td></td>
</tr>
</tbody>
</table>

### Endpoint

- **MAC Address**: 00:0C:29:5C:49:6A
- **Policy Assignment**: Windows7-Workstation
- **Static Assignment**: ✔
- **Identity Group Assignment**: Workstation
- **Static Group Assignment**: ✔
ISE Profiler in a Real Network
Phase 1: Select Profiling Probes

ISE Probes

- ISE Profiler uses a lot of probes to identify devices. It is not easy to choose which ones to use:

- RADIUS
- HTTP
- DHCPSPAN
- DHCP
- SNMP
- Netflow
- DNS
- Network Scan (NMAP)
- SNMPQUERY
- SNMPTRAP
Profiling Probes

• There are a number of profiling probes in ISE

  DHCP Helper
  DHCP Span
  HTTP

  ▪ In-band
  ▪ Explicit configuration
  ▪ SPAN

  RADIUS
  DNS
  SNMPQuery
  SNMPTrap
  Netflow

  ▪ Out-of-band
  ▪ Triggered
Select ISE Probes for a Wired Network

Best Practice

- For **wired network** we recommend using a combination of RADIUS, DHCP, DNS and SNMP:

  - **RADIUS**: OUI (MAC @ prefix), IP
  - **DNS**: Hostname
  - **DHCP**: DHCP class identifier, Client Identifier, parameters, req list
  - **SNMP**: CDP/ LLDP/ Mac Move
  - **NMAP Scan**: OS and Common Ports
  - **HTTP**: User agent (OS type/version)
  - **NetFlow**: Traffic identification

HTTP, and NetFlow could also be used as additional methods when required.

(Use HTTP Probe with WebAuth Portal & I-net Edge or VACLs to limit traffic)
Profiling Flow for a Wired Network

SNMP Query, SNMP Trap, RADIUS, DHCP Helper

Device

Initial Attempt

Open Mode: Time when MAC address is moved to FWD state

MAC-Notification Trap is sent if configured

DCHP Discovery / Request

Authenticator

authentication order dot1x mab

Link-State trap if configured

MAC-Notification Trap

ISE

30 sec to start SNMP Query

Primary Key: 00:11:22:33:44:55:66

Attributes
Switch IP
Port ID
CDP Info
VLAN Data
Session Data
DHCP Options

Authorized


Access-Accept

SNMP Query

SNMP Response

Point of Profiling

EAPOL / ID-Req

(max-reauth-req +1) x tx-timer

802.1X times out

802.1X

MAB

Authorized
ISE Profiler Probes Implementation
Using Profiling Base on RADIUS, DNS, DHCP in a Wired Network

radius-server host @IP_ISE key xxxx
ip device tracking

EAP-OL
DHCP

Dot1x Selective Open Mode
Only DHCP is permitted

DHCP Server
interface Vlan20
ip helper-address @IP_DHCP server
ip helper-address @IP_ISE

RADIUS
Oui, IP

DNS
DNS probe
(reverse-lookup)

ISE

DHCP probe
DHCP class identifier, hostname
req attributes

DHCP Server

RADIUS
Description RADIUS

DNS
Timeout 2
Description DNS

DHCP
Interface GigabitEthernet 0
Port 67
Description DHCP
SNMP/CDP/LLDP, NetFlow

**Queries following mibs:**
- system
- cdpCacheEntry
- cLApEntry (If device is WLC)
- cldcClientEntry (If device is WLC)

**LinkUp/Mac Notification/RADIUS Acct Start event queries:**
- interface data (ifIndex, ifDesc, etc)
- Port and Vlan data
- Session Data (if interface type is Ethernet)
- CDP data (if device is Cisco)

**SNMP**

snmp-server community xxxxxx RW
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host @IP_ISE version 2c xxxxxx

**CDP/LLDP/Mac notification**

**ISE**

**Netflow v5 or v9**

ip flow-export destination @IP ISE
ip flow-export source FastEthernet 0/1
ip flow-export version 9
Devices will be added to the database only if the real MAC address is known.

Use alternate probe to discover MAC @ (eg RADIUS or SNMP probe)

Large network scan could be very time consuming and could add a heavy load to ISE service node
Network Scan (NMAP) In Profiler Policies

Using Network Scan Option in a Profiler Policy

SNMP Scan use « public » as default Ro community

Select NMAP Scan type And Take activate network scan
RADIUS and DNS Probe Requirements

- **DNS and NMAP Probes**
  
  requires **IP address** for reverse DNS lookup or NMAP Scan

  - RADIUS Probe Framed-IP-Address
  - SNMP Probe cdpCacheAddress
  - HTTP Probe Source IP
  - DHCP Probe Dhcp-requested-address

- **NMAP Probe**
  
  requires **MAC - IP binding**

  Device will be included in the database only if MAC is known.
  ARP cache in the profiler service maps IP addresses and MAC addresses.
  Requires **DHCP probe** or the **RADIUS probe**.
IOS Sensor

• Low touch deployment
• Centralize visibility without big ISE sensor investment
• Automatic discovery for most common devices (Printers, Cisco devices, phones)
• Topology independent
IOS Sensor

IOS Sensor Implementation

• It is possible also to use Cisco switches as collectors with:
  - ISE 1.1
  - 3K with 15.0(1)SE1
  - 4K with 15.1(1)SG
  - WLC 7.2 MR1 release - DHCP data only

• IOS Sensor collects data based on:
  - OUI
  - CDP
  - LLDP
  - DHCP

• Avoid SPAN (for HTTP try to use HTTP redirection to ISE portal)

• IP Helper when possible for DHCP
IOS Sensor Implementation

Device Detection Base on CDP, LLDP or DHCP

MAB or EAP-OL -> ISE

- Enable RADIUS probe
- RADIUS Accounting

Filter dhcp, cdp or lldp options/TLV

device-sensor accounting device-sensor notify all-changes

device-sensor filter-list dhcp list my_dhcp_list
tlv name host-name
option name class-identifier
option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list

device-sensor filter-list cdp list my_cdp_list
tlv name device-name
tlv name platform-type
device-sensor filter-spec cdp include list my_cdp_list

device-sensor filter-list lldp list my_lldp_list
tlv name system-name
tlv name system-description
device-sensor filter-spec lldp include list my_lldp_list
IOS Sensor in Action

```
# show device-sensor cache all
Device: 00:21:55:DG:01:33 on port GigabitEthernet1/0/1

Proto Type:Name    Len Value
    cdp   2:address-type    17  00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 64 0F
    cdp   16:power-type     6  00 10 00 06 2E E0
    cdp   11:duplex-type    5  00 08 00 05 01
    cdp   25:power-request-type 12  00 19 00 0C 01 33 00 03 00 00 2E E0
    cdp   6:platform-type   23  00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
                                                6E 65 20 37 39 34 35
    cdp   5:version-type    17  00 05 00 11 53 43 43 50 34 35 2E 39 20 30 2D 33
                                                53
    cdp   4:capabilities-type 8  00 04 00 08 00 00 04 90
    cdp   3:port-id-type    10  00 03 00 0A 50 6F 72 74 20 31
    cdp   1:device-name    19  00 01 00 13 53 45 50 30 30 32 31 33 35 44 3F 30 31
                                                33 33 33
    dhcp  50:requested-address 6  32 04 0A 64 0F 64
    dhcp  54:server-identifier 6  36 04 0A 64 07 64
    dhcp  55:parameter-request-list 9  37 07 01 42 06 03 0F 96 23
    dhcp  60:class-Identifier 40  3C 26 43 69 73 63 6F 20 53 79 73 74 65 6D 73 2C
                                                26 49 6E 63 2E 20 49 50 20 50 68 6F 6E 65 20 43
                                                50 2D 37 39 34 35 47 00
                                                17 DC 0F 53 45 50 30 30 32 31 35 35 44 36 30 31 33
                                                33
    dhcp  12:host-name     9  3D 07 01 00 21 55 06 01 33
    dhcp  61:client-identifier 9  3D 07 01 00 21 55 06 01 33

Cisco IP Phone 7945
SEP002155D60133
Cisco Systems, Inc. IP Phone CP-7945G
SEP002155D60133
Cisco Systems, Inc. IP Phone CP-7945G
1, 66, 6, 3, 15, 150, 35
10.100.15.100
10.100.7.100
2
2
00-21-55-D6-01-33
```

ISE Profiling result
Select ISE Probes for a Wireless Network

Best Practice for a Wireless Network

• For wireless network we recommend to use a combination of RADIUS, DHCP, DNS and HTTP:

- RADIUS
- DNS
- DHCP
- DHCPSPAN
- HTTP

- Oui (MAC @ prefix), IP
- Hostname
- DHCP class identifier, req attributes …
- User agent (OS type/version)

NMAP Scan
OS Identification

NMAP still available as complementary method
Wireless Profiling

- Set Calling-Station-ID to MAC Address for non-1X WLANs [more specifically, applies to any WLAN where NAC type != RADIUS]
  Security > AAA > RADIUS > Authentication

- Disable DHCP Proxy to allow forwarding of DHCP -> IP Helpers
  Controller > Advanced > DHCP
ISE Profiler Probes Implementation for Wireless
RADIUS, DNS, DHCP (IP Helper)

No open mode for Wireless ACL could be enforced for not yet profiled devices. Vlan / ACL could be change after profiling.

interface Vlan20
ip helper-address @IP DHCP server
ip helper-address @IP_ISE
HTTP Best Practice: Use of Controller for HTTP Redirect

802.1X or web auth

HTTP redirect to ISE

WLC 7.2

Access Control Lists > New

Access Control List Name
ACL Type

802.1X SSID must be on Management WLAN

- To allow the initial profiling of HTTP(S) traffic redirected to ISE Policy Service.
- Once profiled, client can be assigned to a different VLAN per Authorization Policy.

HTTP User agent

Access List Name | ACL-HTTP-REDIRECT
---|---
Deny Counters | 0

<table>
<thead>
<tr>
<th>Seq</th>
<th>Action</th>
<th>Source IP/Mask</th>
<th>Destination IP/Mask</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>DSCP</th>
<th>Direction</th>
<th>Number of Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Permit</td>
<td>10.200.7.10 / 255.255.255.255</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Permit</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>10.100.7.10 / 0.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Permit</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>255.255.255.255 / 0.0.0.0</td>
<td>UDP</td>
<td>Any</td>
<td>DNS</td>
<td>Any</td>
<td>Any</td>
<td>0</td>
</tr>
</tbody>
</table>
Wireless Profiling w/ URL Redirects

No SPAN

ISE port includes profiling for HTTP / DHCP probes

- If ISE is L2 adjacent to WLC, then 802.1X WLANs must be on Management interface, else MAC/IP binding required
- If ISE is L3 adjacent to WLC, then MAC/IP binding required.

Management WLAN (10.1.100.0/24)
Employee WLAN (10.1.100.0/24)
Guest WLAN (10.1.50.0/24)
ISE Profiler Probes Implementation for Wireless

HTTP / DHCP alternate solution: Use SPAN to capture traffic

- Some probes require to send a copy of the traffic to ISE
- Sends a copy of the traffic to another port on the switch by using SPAN / RSPAN feature.

```
monitor session 1 source vlan xx , yy
monitor session 1 destination interface Gi1/0/24
```

Source PORTS or VLANs

ISE Probe

HTTP

User agent

DHCPSPAN

Alternative to ip helper

```
DHCPSPAN

Interface Description
GigabitEthernet 0 DHCPSPAN

HTTP

Interface Description
GigabitEthernet 0 HTTP
```
Best Practice: Use « VACL Capture » to Capture only HTTP

Cat6K(config)#ip access-list extended HTTP_TRAFFIC
Cat6K(config-ext-nacl)#permit tcp any any eq www

Cat6K(config)#ip access-list extended ALL_TRAFFIC
Cat6K(config-ext-nacl)#permit ip any any

Cat6K(config)#vlan access-map HTTP_MAP 10
Cat6K(config-access-map)#match ip address HTTP_TRAFFIC
Cat6K(config-access-map)#action forward capture

Cat6K(config)#vlan access-map HTTP_MAP 20
Cat6K(config-access-map)#match ip address ALL_TRAFFIC
Cat6K(config-access-map)#action forward

Cat6K(config)#vlan filter HTTP_MAP vlan-list 10, 20

Cat6K(config)#int fa2/24
Cat6K(config-if)#switchport capture allowed vlan 10
Cat6K(config-if)#switchport capture

Capture HTTP
Forward all other traffic
Applied to vlan 10, 20
Capture port
Wireless Profiling w/ SPAN

- 802.1X WLANs can be on different interface than Management interface
  - ISE interface dedicated to SPAN can profile HTTP traffic directly on each SSID (even those not L2 adjacent) without requiring redirection of user traffic to ISE web service interface (Client Provisioning).

Management WLAN (10.1.100.0/24)
Employee WLAN (10.1.10.0/24)
Guest WLAN (10.1.50.0/24)
How to choose which probes to enable?

<table>
<thead>
<tr>
<th>Device type</th>
<th>OUI</th>
<th>DHCP</th>
<th>CDP</th>
<th>LLDP (1.1)</th>
<th>User agent</th>
<th>Radius</th>
<th>DNS</th>
<th>Netflow</th>
<th>Active scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>smartphone</td>
<td>Yes</td>
<td>yes</td>
<td></td>
<td></td>
<td>yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Tablets</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td>yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Worstation</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>hostname</td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>OS version</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Printer</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>hostname</td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Camera</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td>Yes (cisco)</td>
<td>Yes (lldp required)</td>
<td>Yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>IP Phone</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td>Yes (cisco)</td>
<td>Yes (lldp required)</td>
<td>Yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Network devices</td>
<td>yes</td>
<td></td>
<td></td>
<td>Yes (cisco)</td>
<td>Yes (lldp required)</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
</tbody>
</table>
Configuring Profiling
Using the Profiler Policies

Profiles Policies use a Combination of Conditions to Identify Devices

- DHCP:host-name CONTAINS iPad
- IP:User-Agent CONTAINS iPad

I’m certain this device is an iPad
### ISE Profiler Library

**100+ Already Existing Policies for Devices Identification**

<table>
<thead>
<tr>
<th>Android</th>
<th>Cisco-AP-Aironet-1250</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple-Device</td>
<td>Cisco-AP-Aironet-3500</td>
</tr>
<tr>
<td>Apple-MacBook</td>
<td>Cisco-Access-Point</td>
</tr>
<tr>
<td>Apple-iPad</td>
<td>Cisco-DMP</td>
</tr>
<tr>
<td>Apple-iPhone</td>
<td>Cisco-DMP-4305</td>
</tr>
<tr>
<td>Apple-iPod</td>
<td>Cisco-DMP-4310</td>
</tr>
<tr>
<td>Applera-Device</td>
<td>Cisco-DMP-4400</td>
</tr>
<tr>
<td>Aruba-AP</td>
<td>Cisco-Device</td>
</tr>
<tr>
<td>Aruba-Device</td>
<td>Cisco-IP-Conference-Station-7935</td>
</tr>
<tr>
<td>Avaya-Device</td>
<td>Cisco-IP-Conference-Station-7936</td>
</tr>
<tr>
<td>Avaya-IP-Phone</td>
<td>Cisco-IP-Conference-Station-7937</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>Cisco-IP-Phone</td>
</tr>
<tr>
<td>Cisco-AIR-AP</td>
<td>Cisco-IP-Phone-7902</td>
</tr>
<tr>
<td>Cisco-AIR-AP-1130</td>
<td>Cisco-IP-Phone-7905</td>
</tr>
<tr>
<td>Cisco-AIR-AP-1240</td>
<td>Cisco-IP-Phone-7906</td>
</tr>
<tr>
<td>Cisco-AIR-AP-1250</td>
<td>Cisco-IP-Phone-7910</td>
</tr>
<tr>
<td>Cisco-AIR-LAP</td>
<td>Cisco-IP-Phone-7911</td>
</tr>
<tr>
<td>Cisco-AIR-LAP-1130</td>
<td>Cisco-IP-Phone-7912</td>
</tr>
<tr>
<td>Cisco-AIR-LAP-1240</td>
<td>Cisco-IP-Phone-7940</td>
</tr>
<tr>
<td>Cisco-AIR-LAP-1250</td>
<td>Cisco-IP-Phone-7941</td>
</tr>
<tr>
<td>Cisco-AP-Aironet-1130</td>
<td>Cisco-IP-Phone-7942</td>
</tr>
<tr>
<td>Cisco-AP-Aironet-1240</td>
<td>Cisco-IP-Phone-7945</td>
</tr>
<tr>
<td>FreeBSD-Workstation</td>
<td>Cisco-IP-Phone-7945G</td>
</tr>
<tr>
<td>HP-Device</td>
<td>Cisco-IP-Phone-7960</td>
</tr>
<tr>
<td>HP-JetDirect-Printer</td>
<td>Cisco-IP-Phone-7961</td>
</tr>
<tr>
<td>HTC-Device</td>
<td>Cisco-IP-Phone-7962</td>
</tr>
<tr>
<td>IP-Phone</td>
<td>Cisco-IP-Phone-7965</td>
</tr>
<tr>
<td>ISE-Appliance</td>
<td>Cisco-IP-Phone-7970</td>
</tr>
<tr>
<td>Lexmark-Device</td>
<td>Cisco-IP-Phone-7971</td>
</tr>
<tr>
<td>Lexmark-Printer-E260dn</td>
<td>Cisco-IP-Phone-7975</td>
</tr>
<tr>
<td>Linksys-Device</td>
<td>Cisco-IP-Phone-7985</td>
</tr>
<tr>
<td>LinksysWAP54G-Device</td>
<td>Cisco-IP-Phone-8941</td>
</tr>
<tr>
<td>Linux-Workstation</td>
<td>Cisco-IP-Phone-8945</td>
</tr>
<tr>
<td>Macintosh-Workstation</td>
<td>Cisco-IP-Phone-8961</td>
</tr>
<tr>
<td>Microsoft-Device</td>
<td>Cisco-IP-Phone-9951</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>Cisco-IP-Phone-9971</td>
</tr>
<tr>
<td>MotorolaDroid-Device</td>
<td>Cisco-Router</td>
</tr>
<tr>
<td>MotorolaMobile-Device</td>
<td>Cisco-WLC</td>
</tr>
<tr>
<td>Netgear-Device</td>
<td>Cisco-WLC-2100-Series</td>
</tr>
<tr>
<td>NintendoWII</td>
<td>Cisco-WLC-4400-Series</td>
</tr>
<tr>
<td>Nortel-Device</td>
<td>Cisco-WLC-5500-Series</td>
</tr>
<tr>
<td>Nortel-IP-Phone-2000-Series</td>
<td>DLink-DAP-1522</td>
</tr>
<tr>
<td>OS_X-Workstation</td>
<td>DLink-Device</td>
</tr>
<tr>
<td>OS_X_Lion-Workstation</td>
<td>Enterasys-Device</td>
</tr>
<tr>
<td>OS_X_Big-Lion-Workstation</td>
<td>FreeBSD-Workstation</td>
</tr>
</tbody>
</table>

**For Your Reference**
Profiler Policies

Select this option to create a matching Identity group

Parent Policy

Conditions Details
Name Apple-DeviceRule1Check1
Description Apple-DeviceRule1Check1
Expression MAC:OUI CONTAINS Apple

Conditions Details
Name Apple-iPadRule2Check2
Description Apple-iPadRule2Check2
Expression DHCP:host-name CONTAINS iPad

Conditions Details
Name Apple-ipadRule1Check1
Description Apple-ipadRule1Check1
Expression IP:User-Agent CONTAINS iPad

Conditions Details
Name Apple-MacBookRuleCheck2
Description Apple-MacBookRuleCheck2
Expression IP:User-Agent CONTAINS Mac OS

Conditions Details
Name Apple-iPadRule1Check3
Description Apple-iPadRule1Check3
Expression IP:User-Agent CONTAINS AppleWebKit
Using Profiling in Authorization Policies

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Identity Groups</th>
<th>Other Conditions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS IP Phones</td>
<td>Cisco-IP-Phone</td>
<td></td>
<td>Cisco_IP_Phone</td>
</tr>
<tr>
<td>SS smartphones - tablets</td>
<td>Android OR Apple-iPad OR Apple-iPhone</td>
<td>Radius:Service-Type EQUALS Framed</td>
<td>internet_only</td>
</tr>
<tr>
<td>SS Camera</td>
<td>cisco-camera</td>
<td></td>
<td>PermitAccess</td>
</tr>
</tbody>
</table>

Identity groups directly used as a policy condition

Endpoint Identity Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Identity Group for Profile: Android</td>
</tr>
<tr>
<td>Apple-iPad</td>
<td>Identity Group for Profile: Apple-iPad</td>
</tr>
<tr>
<td>Apple-iPhone</td>
<td>Identity Group for Profile: Apple-iPhone</td>
</tr>
<tr>
<td>Blacklist</td>
<td>Blacklist Identity Group</td>
</tr>
<tr>
<td>Cisco-AP-Aironet-3500</td>
<td>Identity Group for Profile: Cisco-AP-Aironet-3500</td>
</tr>
<tr>
<td>Cisco-IP-Phone</td>
<td>Identity Group for Profile: Cisco-IP-Phone</td>
</tr>
<tr>
<td>Profiloid</td>
<td>Profiloid Identity Group</td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown Identity Group</td>
</tr>
<tr>
<td>Workstation</td>
<td>Identity Group for Profile: Workstation</td>
</tr>
<tr>
<td>cisco-camera</td>
<td>Identity Group for Profile: cisco-camera</td>
</tr>
</tbody>
</table>
Create a Custom Profiling Policy

Profiling Policy

- Name: test
- Description: this is a test for BR3030 Techtorial
- Policy Enabled: Yes
- 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

1. If Condition: MAC_OUI_EQUALS_02345__DHCP_dhcp_class_id... Then: Certainty Factor Increases 10
2. If Condition: LLDP_lldpSystemDescription_EQUALS_test... Then: Certainty Factor Increases 10

Add All Conditions Below to Library

- Condition Name: MAC_OUI
  Expression: EQUALS 012345

- Condition Name: DHCP_dhcp_class_id
  Expression: CONTAINS test

- Condition Name: IP_User-Agent
  Expression: CONTAINS test
Example of Conditions to Use in Custom Policies

- **NMAP**
  - EndPointSource
  - FQDN
  - Host
  - port
  - mask
  - PortAll
  - User-Agent

- **DHCP**
  - boot-file
  - client-fqdn
  - client-identifier
  - device-class
  - dhcp-class-identifier
  - dhcp-client-identifier
  - dhcp-message-type
  - dhcp-parameter-request-list
  - dhcp-rejected-address
  - dhcp-user-class-id
  - domain-name
  - host-name

- **LLDP**
  - lldpCacheCapabilities
  - lldpCapabilitiesMapSupported
  - lldpChassisId
  - lldpManAddress
  - lldpPortDescription
  - lldpPortId
  - lldpSystemCapabilitiesMapEnabled
  - lldpSystemDescription
  - lldpSystemName
  - lldpTimeToLive

- **CDP**
  - cdpCacheAddress
  - cdpCacheCapabilities
  - cdpCacheDeviceId
  - cdpCachePlatform
  - cdpCacheVersion

- **Netflow**
  - FIRST_SWITCHED
  - FLOW_SAMPLER_ID
  - flow_sequence
  - FLOWS
  - FragmentOffset
  - ICMP_TYPE
  - IN_BYTES
  - IN_PKTS
  - input
  - INPUT_SNMP
  - IP_PROTOCOL_VERSION
  - IPV4_DST_ADDR

- **SNMP**
  - hDeviceStatus
  - ifDescr
  - ifIndex
  - ifOperStatus
  - port
  - portIfIndex
  - sysContact
  - sysDescr
  - sysLocation
  - sysName
  - sysObjectID
  - sysUpTime
  - vlan

- **RADIUS**
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Tunnel-Connection
  - Acct-Tunnel-Packets-Lost
  - Callback-ID
  - Callback-Number
  - Called-Station-ID
  - Calling-Station-ID
  - CHAP-Challenge
  - CHAP-Password
  - Class
  - Connect-Info

- **IP**
  - 445-tcp
  - 445-udp
  - 500-udp
  - 520-udp
  - 53-tcp
  - 53-udp
  - 631-udp
  - 57-udp
  - 58-udp
  - 80-tcp
  - 8080-tcp
  - operating-system
### Profiler Conditions Library

Any Combination of Theses Conditions Could be use in your Policies

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AndroidRule1Check1</strong></td>
<td>User-Agent CONTAINS Android</td>
</tr>
<tr>
<td><strong>AndroidRule1Check2</strong></td>
<td>host-name CONTAINS android</td>
</tr>
<tr>
<td><strong>Apple-DeviceRule1Check1</strong></td>
<td>OUI CONTAINS Apple</td>
</tr>
<tr>
<td><strong>Apple-MacBookRuleCheck1</strong></td>
<td>User-Agent CONTAINS Macintosh</td>
</tr>
<tr>
<td><strong>Apple-MacBookRuleCheck2</strong></td>
<td>User-Agent CONTAINS Mac OS</td>
</tr>
<tr>
<td><strong>Apple-iPadRule1Check1</strong></td>
<td>User-Agent CONTAINS iPad</td>
</tr>
<tr>
<td><strong>Apple-iPadRule1Check3</strong></td>
<td>User-Agent CONTAINS AppleWebKit</td>
</tr>
<tr>
<td><strong>Apple-iPadRule2Check2</strong></td>
<td>host-name CONTAINS iPad</td>
</tr>
<tr>
<td><strong>Apple-iPhoneRule1Check1</strong></td>
<td>User-Agent CONTAINS iPhone; U; CPU iPho</td>
</tr>
<tr>
<td><strong>Apple-iPhoneRule2Check1</strong></td>
<td>host-name CONTAINS iPhone</td>
</tr>
<tr>
<td><strong>Apple-iPodRule1Check1</strong></td>
<td>User-Agent CONTAINS iPod; U; CPU iPho</td>
</tr>
<tr>
<td><strong>Apple-iPodRule3Check3</strong></td>
<td>User-Agent CONTAINS iPod; U;</td>
</tr>
<tr>
<td><strong>Applera-Check</strong></td>
<td>OUI EQUALS Applera Holding B.V. Singapore</td>
</tr>
<tr>
<td><strong>Aruba-APRule1Check1</strong></td>
<td>dhcp-class-identifier EQUALS ArubaAP</td>
</tr>
<tr>
<td><strong>Aruba-DeviceRuleCheck1</strong></td>
<td>OUI CONTAINS ARUBA NETWORKS</td>
</tr>
<tr>
<td><strong>Avaya-DeviceRuleCheck1</strong></td>
<td>OUI CONTAINS Avaya</td>
</tr>
<tr>
<td><strong>AvayaIPPhoneCheck</strong></td>
<td>dhcp-class-identifier EQUALS ccip.avaya.com</td>
</tr>
</tbody>
</table>
RADIUS CoA: Configuration
Allow ISE to Actively Enforce Policy Over Connected Endpoints

CoA is triggered dynamically when a scenario is matched:
- Endpoint is profiled for the 1st time.
- Endpoint is statically assigned with a new Policy
- Endpoint is deleted from ISE DB.

```
aaa server radius dynamic-author
client 10.100.7.20 server-key xxxxxxx
```
Profiling Exceptions
Profile Transitions

• Default Exception Actions – CoA sent on these events based on Administration → System → Settings → Profiling setting

<table>
<thead>
<tr>
<th>Profiler Action Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EndpointDelete</td>
<td>When endpoint is deleted or reassigned to the unknown profile.</td>
</tr>
<tr>
<td>FirstTimeProfile</td>
<td>When an endpoint profile changes from unknown to known for the first time.</td>
</tr>
<tr>
<td>StaticAssignment</td>
<td>When an endpoint has connected to the network and is now statically assigned.</td>
</tr>
</tbody>
</table>

• Top 3 predefined actions are not configurable
• Administrator may define additional Actions

• If insufficient attributes collections, device may be profiled in a more generic profile and CoA sent only for this profile. Ex:
  Apple-Device versus Apple-iPad
  HP-Device versus HP-JetDirect-Printer

• Exception action required to send CoA when device is eventually profiled into more specific policy.
## Using Profiling Inside Authorization Rules

Identity Group are used as a Condition for Authorization Rules

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Conditions (identity groups and other conditions)</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Profiled Cisco IP Phones</td>
<td>if Cisco-IP-Phone</td>
<td>then Cisco_IP_Phone</td>
</tr>
<tr>
<td>✔</td>
<td>Profiled Smartphones</td>
<td>if Apple-iPad OR Apple-iPhone OR Android OR BlackBerry</td>
<td>then internet_only</td>
</tr>
<tr>
<td>✔</td>
<td>Profiled Cameras</td>
<td>if real_camera</td>
<td>then video_vlan</td>
</tr>
</tbody>
</table>

**Conditions**
- Android, iPhone, iPad or BlackBerry Devices

**Result**
- Enforce ACL To permit only http on internet
Monitoring and Reporting
### Profiled Monitoring

**Real-Time Monitoring**

#### Profiled endpoint Dashboard

<table>
<thead>
<tr>
<th>Endpoint Profile</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco-Device</td>
<td>C8:4C:75:85:30:C0</td>
</tr>
<tr>
<td>Cisco-Device</td>
<td>00:1F:9D:CA:38:40</td>
</tr>
<tr>
<td>Cisco-Device</td>
<td>00:19:56:D9:29:68</td>
</tr>
<tr>
<td>Cisco-IP-Phone-7945</td>
<td>00:21:55:D6:00:8D</td>
</tr>
<tr>
<td>Cisco-IP-Phone-7945</td>
<td>00:21:55:D6:03:08</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>00:0C:29:D0:E2:82</td>
</tr>
<tr>
<td>Microsoft-Workstation</td>
<td>00:24:D7:3A:0E:18</td>
</tr>
<tr>
<td>Nortel-Device</td>
<td>5C:FF:35:01:F6:DE</td>
</tr>
<tr>
<td>Unknown</td>
<td>E0:F8:47:53:3D:7D</td>
</tr>
<tr>
<td>VMWare-Device</td>
<td>00:0C:29:52:3A:DB</td>
</tr>
<tr>
<td>Windows7-Workstation</td>
<td>F0:DE:F1:0D:59:58</td>
</tr>
<tr>
<td>Xerox-Device</td>
<td>00:00:00:00:E2:82</td>
</tr>
</tbody>
</table>
Endpoint Detail

Give you all Details About Authentication and Profiling

ENDPOINT

* MAC Address: 00:0C:29:E6:69:01
* Policy Assignment: Windows7-Workstation

* Identity Group Assignment: Workstation
Static Group Assignment: 

ATTRIBUTES LIST

- ADDomain: live.cisco.com
- AcsSessionID: ISE-02/112815005/44633
- AuthState: Authenticated
- AuthenticationIdentityStore: AD2008R2
- AuthenticationMethod: MSCHAPV2
- AuthorizationPolicyMatchedRule: S2 1x marketing

USER-AGENT: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)

dhcp-class-identifier: MSFT 5.0
dhcp-client-identifier: 01:00:0c:29:e6:69:01
dhcp-message-type: DHCPREQUEST
dhcp-parameter-request-list: 1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43, 252
dhcp-requested-address: 10.100.12.101
## Endpoint Profiler Summary

### Detailed Report for Profiler Activity

### Endpoint > Endpoint Profiler Summary

<table>
<thead>
<tr>
<th>Logged At</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Raw Log</td>
</tr>
</tbody>
</table>

### Endpoint Details

- **Endpoint Static Assignment**: Wistron InfoComm (Kunshan)Co
- **Endpoint Host Name**: 
- **Endpoint Subnet**: 
- **Endpoint NAD Address**: 10.100.7.1
- **Endpoint VLAN**: 14
- **Endpoint FQDN**: 
- **Endpoint Nameserver**: 
- **Endpoint Property**: 
- **CPMSessionId**: 0707070000001940E08049E
  - **VlanName**: guest
  - **Cookie**: guestid=0753B56535853576; pid=v3A313219B84952298418627
  - **NetDeviceGroup**: GigabitEthernet1/0/8
  - **NetworkLocation**: Location=All Locations;Cisco Live#TECHSEC-3030
  - **IfOperStatus**: 2
  - **Cisco-aaa-account-type**: Framed
  - **audit-session-id**: 0707070700001940E08049E
  - **Callname-Id**: F0:DE:F1:00:FE:20

### Profiler Summary

<table>
<thead>
<tr>
<th>Logged At</th>
<th>Dec 15, 2011 12:24 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>ISE-01</td>
</tr>
<tr>
<td>Event</td>
<td>Profiler is triggering Change Of Authorization Request</td>
</tr>
</tbody>
</table>

### Endpoint History

<table>
<thead>
<tr>
<th>Day</th>
<th>Endpoint policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 15, 2011 12:24 AM</td>
<td>Windows7-Workstation</td>
</tr>
<tr>
<td>Dec 8, 2011 3:14 PM</td>
<td>Windows7-Workstation</td>
</tr>
<tr>
<td>Dec 8, 2011 3:14 PM</td>
<td>Windows7-Workstation</td>
</tr>
<tr>
<td>Dec 8, 2011 3:13 PM</td>
<td>Microsoft-Workstation</td>
</tr>
<tr>
<td>Nov 17, 2011 4:15 PM</td>
<td>Microsoft-Workstation</td>
</tr>
</tbody>
</table>
# NCS Prime Reporting

## Client Summary By Vendors

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Average Number of Sessions</th>
<th>Maximum Number of Clients</th>
<th>Average Number of Clients</th>
<th>Total Session Time (Hours)</th>
<th>Total Traffic (MB)</th>
<th>% of Sessions</th>
<th>% of Clients</th>
<th>% of Session Time</th>
<th>% of Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>16</td>
<td>9</td>
<td>8</td>
<td>236.62</td>
<td>0.0</td>
<td>37.21</td>
<td>34.78</td>
<td>30.91</td>
<td>0.0</td>
</tr>
<tr>
<td>IBM</td>
<td>15</td>
<td>9</td>
<td>8</td>
<td>314.98</td>
<td>0.0</td>
<td>34.88</td>
<td>34.78</td>
<td>41.15</td>
<td>0.0</td>
</tr>
<tr>
<td>VMware</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>209.93</td>
<td>0.0</td>
<td>13.95</td>
<td>21.74</td>
<td>27.43</td>
<td>0.0</td>
</tr>
<tr>
<td>Apple</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>3.75</td>
<td>0.88</td>
<td>11.63</td>
<td>4.35</td>
<td>0.49</td>
<td>100.0</td>
</tr>
<tr>
<td>Intel</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0.17</td>
<td>0.0</td>
<td>2.33</td>
<td>4.35</td>
<td>0.02</td>
<td>0.0</td>
</tr>
</tbody>
</table>

![Clients by Vendor](image-url)
# NCS Prime Reporting

## Client Summary by Endpoint Type

<table>
<thead>
<tr>
<th>Endpoint Type</th>
<th>Average Number of Sessions</th>
<th>Maximum Number of Clients</th>
<th>Average Number of Clients</th>
<th>Total Session Time (Hours)</th>
<th>Total Traffic (MB)</th>
<th>% of Sessions</th>
<th>% of Clients</th>
<th>% of Session Time</th>
<th>% of Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>17</td>
<td>14</td>
<td>10</td>
<td>325.53</td>
<td>0.0</td>
<td>29.82</td>
<td>37.04</td>
<td>42.53</td>
<td>0.0</td>
</tr>
<tr>
<td>Cisco-Device</td>
<td>9</td>
<td>5</td>
<td>5</td>
<td>42.0</td>
<td>0.0</td>
<td>15.79</td>
<td>13.52</td>
<td>5.49</td>
<td>0.0</td>
</tr>
<tr>
<td>True</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>17.82</td>
<td>0.0</td>
<td>8.77</td>
<td>3.7</td>
<td>2.33</td>
<td>0.0</td>
</tr>
<tr>
<td>Real-Camera</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>20.0</td>
<td>0.0</td>
<td>0.77</td>
<td>3.7</td>
<td>2.61</td>
<td>0.0</td>
</tr>
<tr>
<td>VMWare-Device</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>155.88</td>
<td>0.0</td>
<td>8.77</td>
<td>14.81</td>
<td>20.36</td>
<td>0.0</td>
</tr>
<tr>
<td>Apple-iPad</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1.0</td>
<td>0.12</td>
<td>7.02</td>
<td>3.7</td>
<td>0.13</td>
<td>0.35</td>
</tr>
<tr>
<td>Apple-iPhone</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2.75</td>
<td>0.76</td>
<td>7.02</td>
<td>3.7</td>
<td>0.36</td>
<td>53.89</td>
</tr>
<tr>
<td>Cisco-WLC</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>38.17</td>
<td>0.0</td>
<td>5.26</td>
<td>3.7</td>
<td>4.99</td>
<td>0.0</td>
</tr>
<tr>
<td>Cisco-IP-Phone-7945</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>54.05</td>
<td>0.0</td>
<td>3.51</td>
<td>3.7</td>
<td>7.06</td>
<td>0.0</td>
</tr>
<tr>
<td>Microsoft Workstation</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>54.22</td>
<td>0.53</td>
<td>3.51</td>
<td>3.7</td>
<td>7.08</td>
<td>37.77</td>
</tr>
<tr>
<td>Cisco-Access-Point</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>54.05</td>
<td>0.0</td>
<td>1.75</td>
<td>3.7</td>
<td>7.06</td>
<td>0.0</td>
</tr>
</tbody>
</table>

*Clients by Endpoint Type*
ISE Demo of Profiling
Case Study
Different Security to Different Security Roles

<table>
<thead>
<tr>
<th>Identity (Authentication)</th>
<th>Device (Profiling)</th>
<th>Permission (Authorization)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>John</td>
<td>Apple-iPhone</td>
<td>iPhoneEmployee VLAN #135</td>
</tr>
<tr>
<td>Peter</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apple-iPad</td>
<td>iPadEmployee VLAN #136</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td></td>
<td>AndroidEmployee VLAN #137</td>
</tr>
<tr>
<td>Blackberry</td>
<td></td>
<td>BlackBerryEmployee VLAN #138</td>
</tr>
<tr>
<td>Contractor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractor1</td>
<td></td>
<td>Contractors VLAN #145</td>
</tr>
<tr>
<td>Contractor2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IF $Identity$ AND $Device$ THEN $Permission$**
Use Case

- Users, using the same SSID, can be associated to different wired VLAN interfaces after EAP authentication.
- Employees using iPhone with their AD user id in AD group “employee” are assigned to **VLAN 135**
- Employees using iPad with their AD user id in AD group “employee” are assigned to **VLAN 136**
- Contractors using any device with their AD user id in AD group “contractor” are assigned to **VLAN 145**
BYOD Remote - Demonstration


https://demos-us.cisco.com/QuestCAP/Custom/Internal/Login.aspx

Required

- Cisco Aironet 3500/3600/600 Series
- BYOD endpoint – Laptop/tablet/smartphone acting as personal device
- Monitoring laptop – Laptop accessing the demonstration environment and displaying management systems
ISE BYOD Demo Scenarios

2 roles available:
- Doctor
- IT admin

3 roles available:
- Professor
- Student
- Itadmin

2 roles available:
- Corporate
- IT admin

Healthcare Scenario

Demo Healthcare Portal

Demo Pod7 Healthcare Specific Credentials

Username: doctor7
Password: cisco123

Username: itadmin7
Password: cisco123

see IE page on your Hosted Workstation for a correct number

Education Scenario

Demo Education Portal

Demo Pod7 Education Specific Credentials

Username: professor7
Password: cisco123

Username: student7
Password: cisco123

Username: itadmin7
Password: cisco123

see IE page on your Hosted Workstation for a correct number

Corporate Office Scenario

Demo Corporate Portal

Demo Pod7 Corporate Specific Credentials

Username: corporate7
Password: cisco123

Username: itadmin7
Password: cisco123

see IE page on your Hosted Workstation for a correct number
ISE – Demo BYOD - Dashboard
ISE – Demo BYOD - Monitoring
## Trustsec Roadmap Platform/Feature Matrix

<table>
<thead>
<tr>
<th>Platform</th>
<th>Models</th>
<th>802.1x / Identity Features</th>
<th>Security Group Access</th>
<th>Device Sensors</th>
<th>MACSec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Classification</td>
<td>Transport</td>
<td>Enforcement</td>
<td>Switch to Switch</td>
</tr>
<tr>
<td>Cat 2K</td>
<td>2960, 2960-S</td>
<td>√</td>
<td></td>
<td>SXP</td>
<td>✓</td>
</tr>
<tr>
<td>Cat 3K</td>
<td>3560, 3650E, 3750, 3750E, 3560-X</td>
<td>√</td>
<td>√</td>
<td>SXP</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>3560 C</td>
<td></td>
<td>SXP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cat 4K</td>
<td>Sup6E, Sup 6L-E</td>
<td>√</td>
<td>√</td>
<td>SXP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sup7E, Sup 7L-E</td>
<td></td>
<td>SXP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cat 6K</td>
<td>Sup32 / Sup720</td>
<td>√</td>
<td>√</td>
<td>SXP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sup2T</td>
<td>√</td>
<td>√</td>
<td>SXP/SGT</td>
<td>SGACL</td>
</tr>
<tr>
<td>Nexus 7K</td>
<td></td>
<td>√</td>
<td>SXP/SGT</td>
<td>SGACL</td>
<td></td>
</tr>
<tr>
<td>Nexus 5K</td>
<td></td>
<td>√</td>
<td>SXP/SGT</td>
<td>SGACL</td>
<td></td>
</tr>
<tr>
<td>ASR 1K</td>
<td>Pr1 / Pr2, 1001, 1002, 1004, 1006, 1013, ESP10/20/40, SIP 10/40</td>
<td>√</td>
<td></td>
<td>SXP</td>
<td></td>
</tr>
<tr>
<td>ISR G2</td>
<td>88X 89X 19xx 29xx 39xx</td>
<td>√</td>
<td>√</td>
<td>SXP/SGT/SGT-IPSEC</td>
<td></td>
</tr>
<tr>
<td>ASA</td>
<td></td>
<td></td>
<td>SXP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless LAN Controller</td>
<td></td>
<td>√</td>
<td>√</td>
<td>SXP</td>
<td></td>
</tr>
<tr>
<td>AnyConnect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Red x indicates new in TrustSec v2.1*
Summary

- ISE Profiling: Support Device profiling for Wired and wireless networks
- Use a combination of advanced probes to identify devices
- Is Integrated in ISE policies
- Use Cisco Infrastructure for distributed features (IOS Sensor)
Where To Find Out More

Whitepapers

<table>
<thead>
<tr>
<th>Topic</th>
<th>Link</th>
</tr>
</thead>
</table>
Recommended Reading
Otázky a odpovědi

- Twitter  www.twitter.com/CiscoCZ
- Talk2Cisco  www.talk2cisco.cz/dotazy
- SMS  721 994 600

- Zveřejníme Vás na Ptali jste se… v sále LEO
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00
Prosíme, ohodnoťte tuto přednášku.