Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Securely Managing BYOD

BRKEWN-2020

TOMORROW
starts here.

Agenda

Addressing the BYOD Phenomenon Securely

- What is BYOD?
- Cisco BYOD Solution Components
- Integrating the Wireless LAN Controller and ISE
  - Using strong security with WPA2 and EAP
  - Profiling devices through client attributes
- Defining a Security Policy within ISE
  - Configuring authentication and authorisation rules
- BYOD Device Provisioning
  - Pushing certificates and Wi-Fi profiles
- BYOD Monitoring and Reporting

Workplace Trends

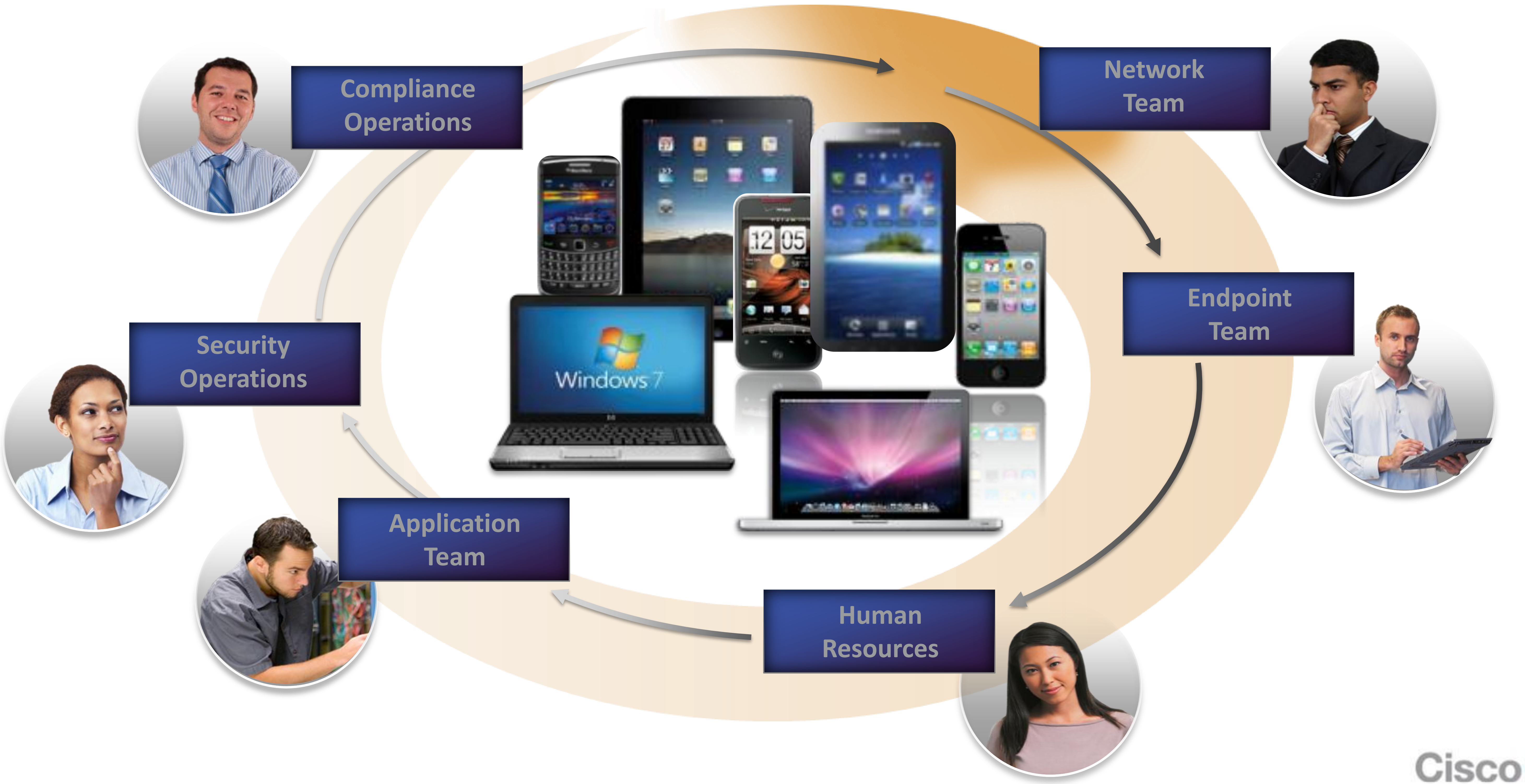
Old School

- Enterprise provided mobile devices
- Work is a **place you go to**
    - limited off campus access
- IT visibility and control into user devices and applications

New School

- Anywhere, anytime, any device usage
- Work is a **function**
    - Globally dispersed, mixed device ownership
- Change in IT control and management paradigm

BYOD: An Enterprise Wide Project



Compliance Operations

Network Team

Endpoint Team

Human Resources

Application Team

Security Operations

Cisco Unique BYOD Value Proposition

Enable Any Device, Any Access, Any Policy Through One Centrally Managed Network

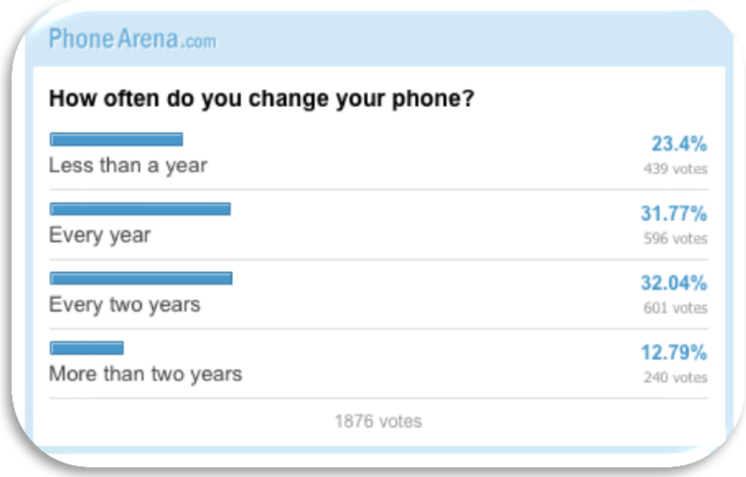
More Than Just Personal Devices — Device ownership is irrelevant: corporate, personal, guest, etc…

More Than Just Wireless Access — BYO devices need wired, wireless, remote and mobile access

More Than Just iPads — BYO devices can be any device: Windows PCs, Mac OS devices, any tablet, any smartphone, gaming consoles, printers… etc

Wireless BYOD

Drivers and Assumptions



PhoneArena.com

How often do you change your phone?

Less than a year	23.4%	439 votes
Every year	31.77%	596 votes
Every two years	32.04%	601 votes
More than two years	12.79%	240 votes

1876 votes

- Drivers
  - – Majority of new network devices have no wired port
  - – Users will change devices more frequently than in the past
  - – Mobile devices have become an extension of our personality
  - – Guest / Contractor access and accountability has become a mandatory business need

- Assumptions
  - – Guest and Contractors must be isolated and accounted for.
  - – Users will have 1 wired and 2+ wireless devices moving forward
  - – The wireless network must be secure and as predictable as the wired network
  - – There can be no unmanaged devices any more – only managed and semi-managed

Spectrum of BYOD Strategies

Different Deployment Requirements for Different Environments

Restrict

- BYOD is not allowed as per corporate policy.
- All non-corporate assets should be denied access.

Allow

- BYOD used to allow employee internet access on mobile devices.
- Secure access to email and other corporate services is possible.

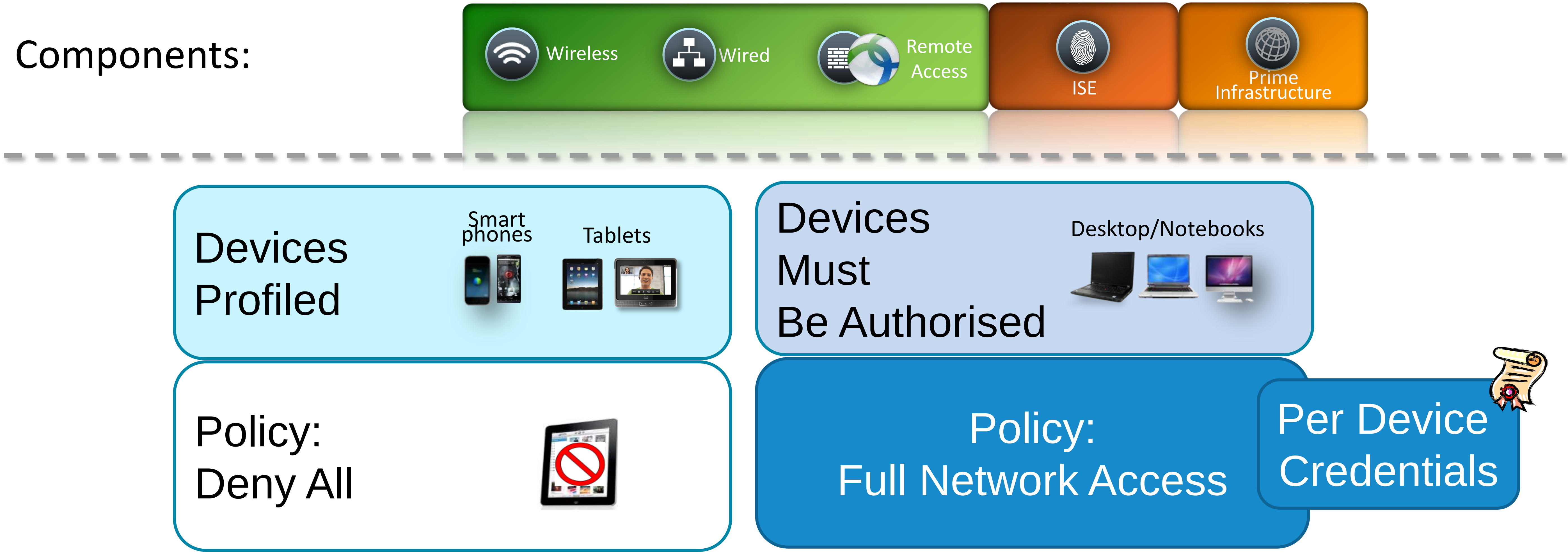
Embrace

- BYOD used to enhance business processes and improve productivity.
- Per device identification via certificates is used for high security.

Restrict

“Restrict” Deployment Strategy

Allowing only Corporate Assets on the Network Infrastructure



Components:

Wireless

Wired

Remote Access

ISE

Prime Infrastructure

Devices Profiled

Smart phones

Tablets

Devices Must Be Authorised

Desktop/Notebooks

Policy: Deny All

Policy: Full Network Access

Per Device Credentials

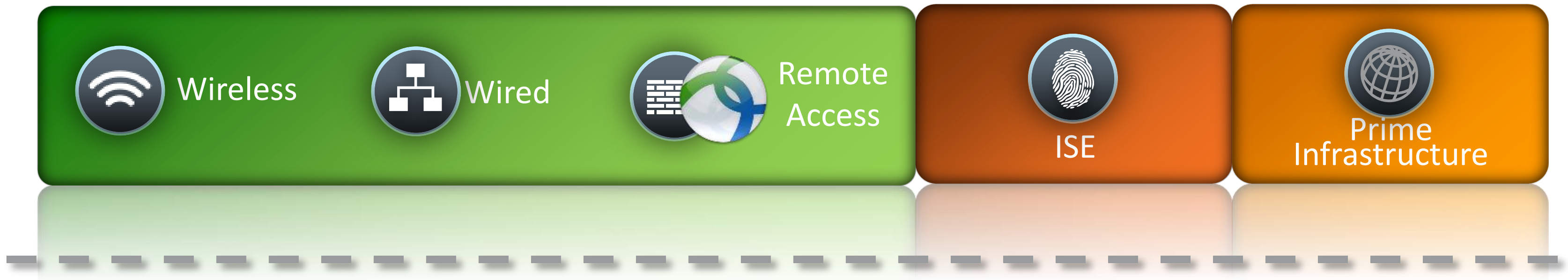
- “Restrict” policy only allows corporate assets onto the network
- BYOD is not supported (as per policy) and the network will enforce this.

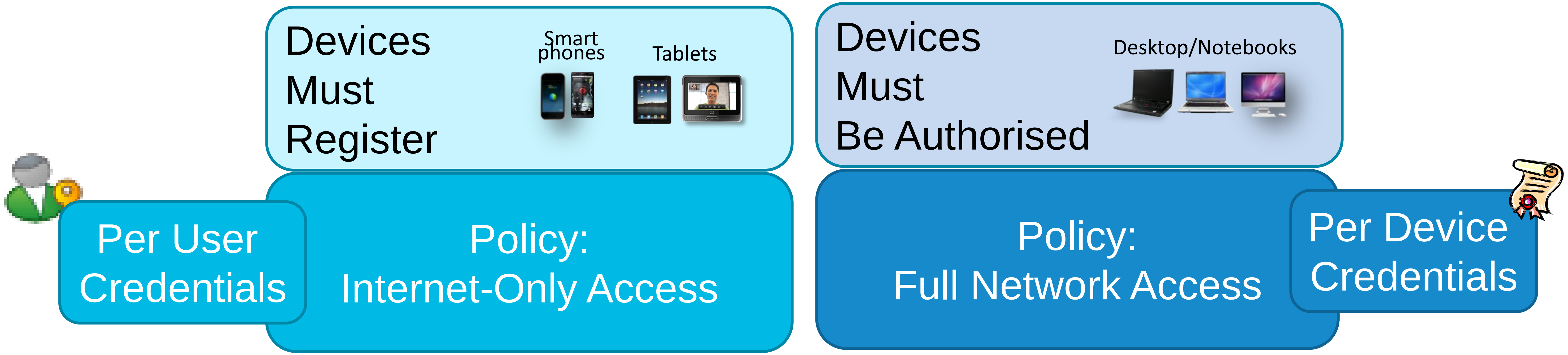
"Allow" Deployment Strategy

Allowing BYOD Devices for Internet Access Only

Allow

Components:



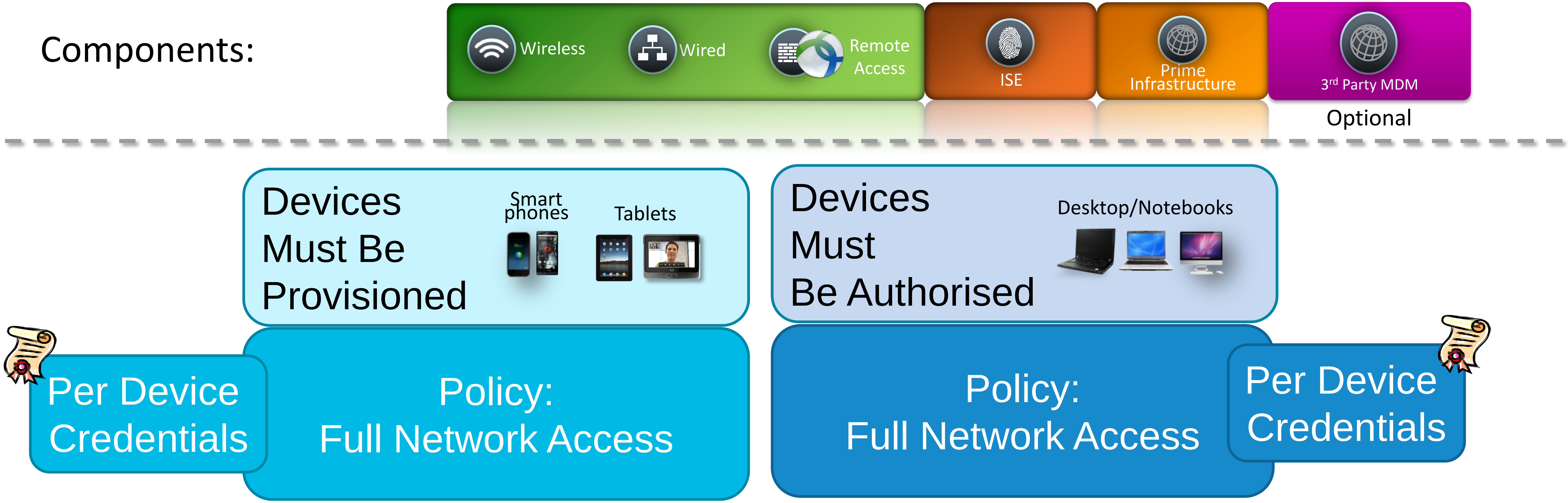


- Employee owned devices allowed to access Internet resources.
- Per user credential is used along with device registration to regulate the number of BYOD devices.

“Embrace” Deployment Strategy

Embrace

Using BYOD with Business Relevant Applications



Components:

Wireless

Wired

Remote Access

ISE

Prime Infrastructure

3rd Party MDM

Optional

Devices Must Be Provisioned

Smart phones

Tablets

Devices Must Be Authorised

Desktop/Notebooks

Per Device Credentials

Policy: Full Network Access

Policy: Full Network Access

Per Device Credentials

- Both corporate assets and BYOD devices are allowed onto the network using per-device credentials.
- BYOD devices used to enhance business processes.

BYOD Solution Components

Required Components and Versions

Cisco Wireless LAN and Identity Services Engine

- Cisco Wireless LAN Controller
  - Version 7.0.116 or greater (440X, WiSM1, 210X or later)

    Central Switching supported for device profiling and posture assessment.

    802.1x WLANs only supported for CoA.
  - Version 7.2.X or greater (5508, WiSM2, 250X or later)

    Central and FlexConnect switching supported for device profiling and posture assessment.

    802.1x and Open (L3 Web authentication) supported for CoA.
- Cisco Identity Services Engine
  - Version 1.1.1 or later
  - Advanced Package License for Profiling

Cisco's Unified Policy Management Components

User and Device Specific Attributes

Employee Workstation

- Employee VLAN
- Gold QoS

Employee BYOD

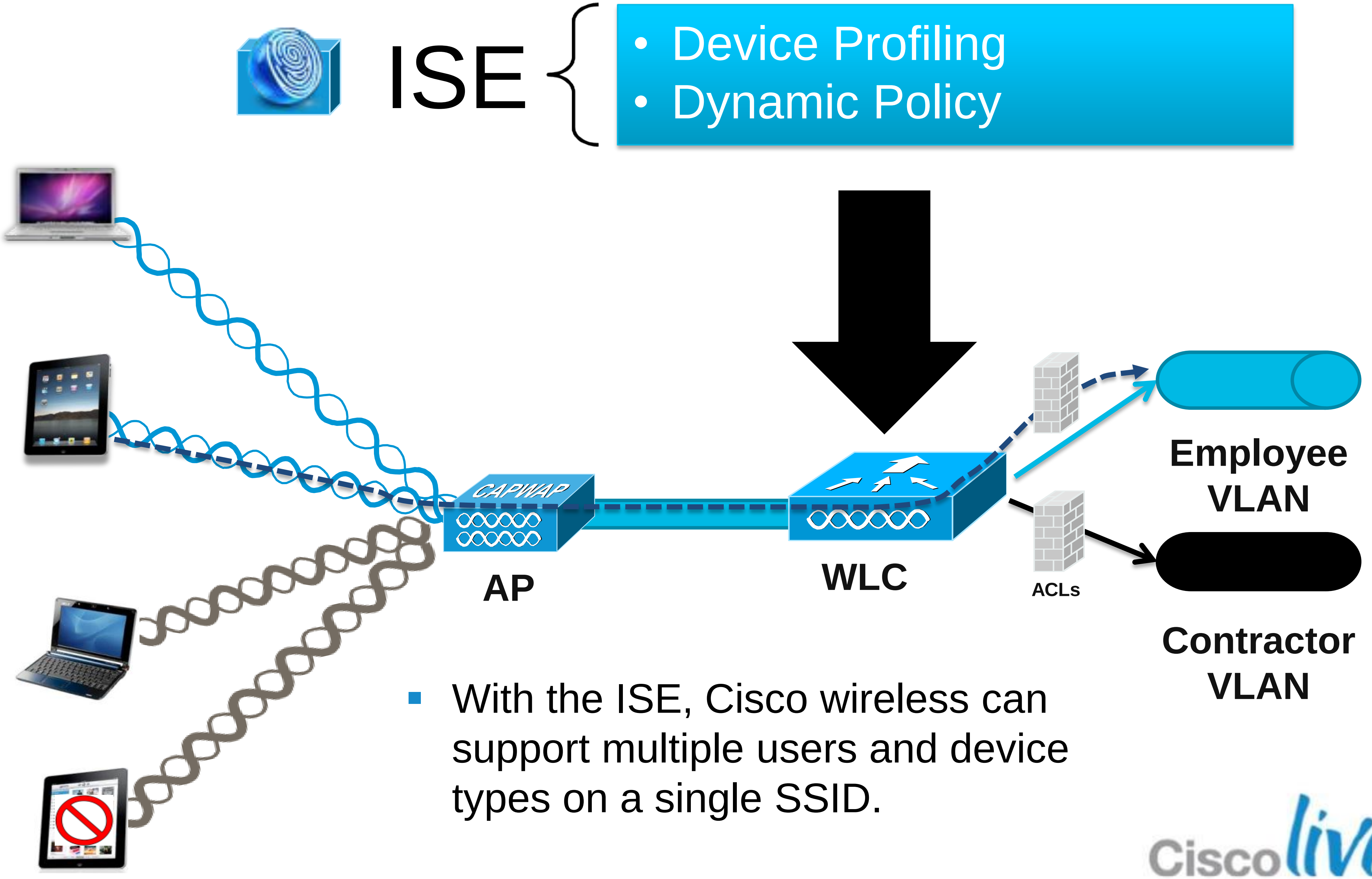
- Employee VLAN
- Gold QoS
- **Restrictive ACL**

Contractor Workstation

- Contractor VLAN
- No QoS
- **Restrictive ACL**

Contractor BYOD

- No Access



- With the ISE, Cisco wireless can support multiple users and device types on a single SSID.

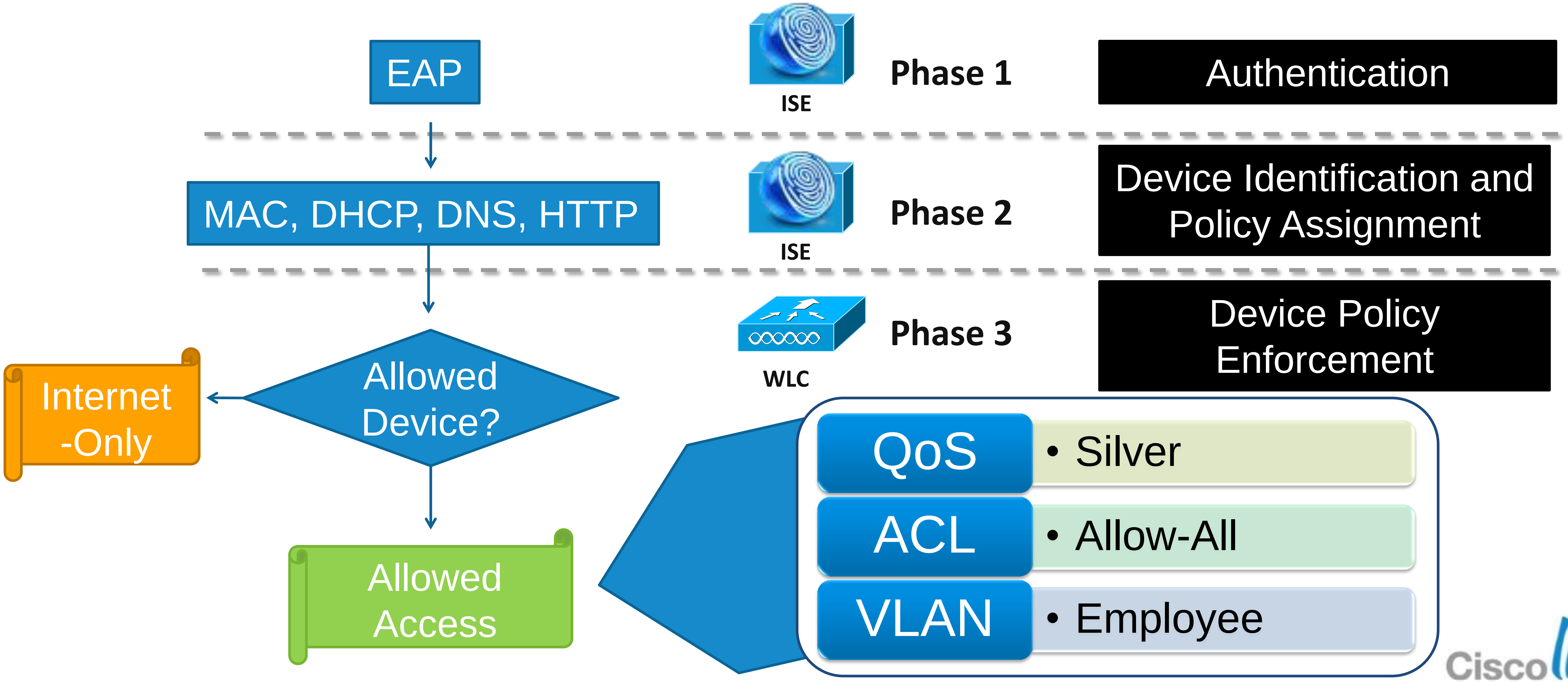
Cisco's Unified Policy Management

Example of BYOD / Mobility Policy Table

User	Device	Access Method	Location	Time	Policy
Guest	Personal Laptop Personal Device	Wireless	Conference Rooms	M – F 8 am – 6 pm	Captive Portal DMZ Guest Tunnel Guest VLAN
Contractor	Contractor Computer Personal Device	Wireless Wired	Anywhere Anywhere	Anytime M – S 8 am - 6 pm	Contractor VLAN Contractor ACL
Employee	Corporate Computer Personal Device	Wired Wireless VPN	Anywhere Anywhere Anywhere	Anytime Anytime Anytime	Employee VLAN Employee ACL

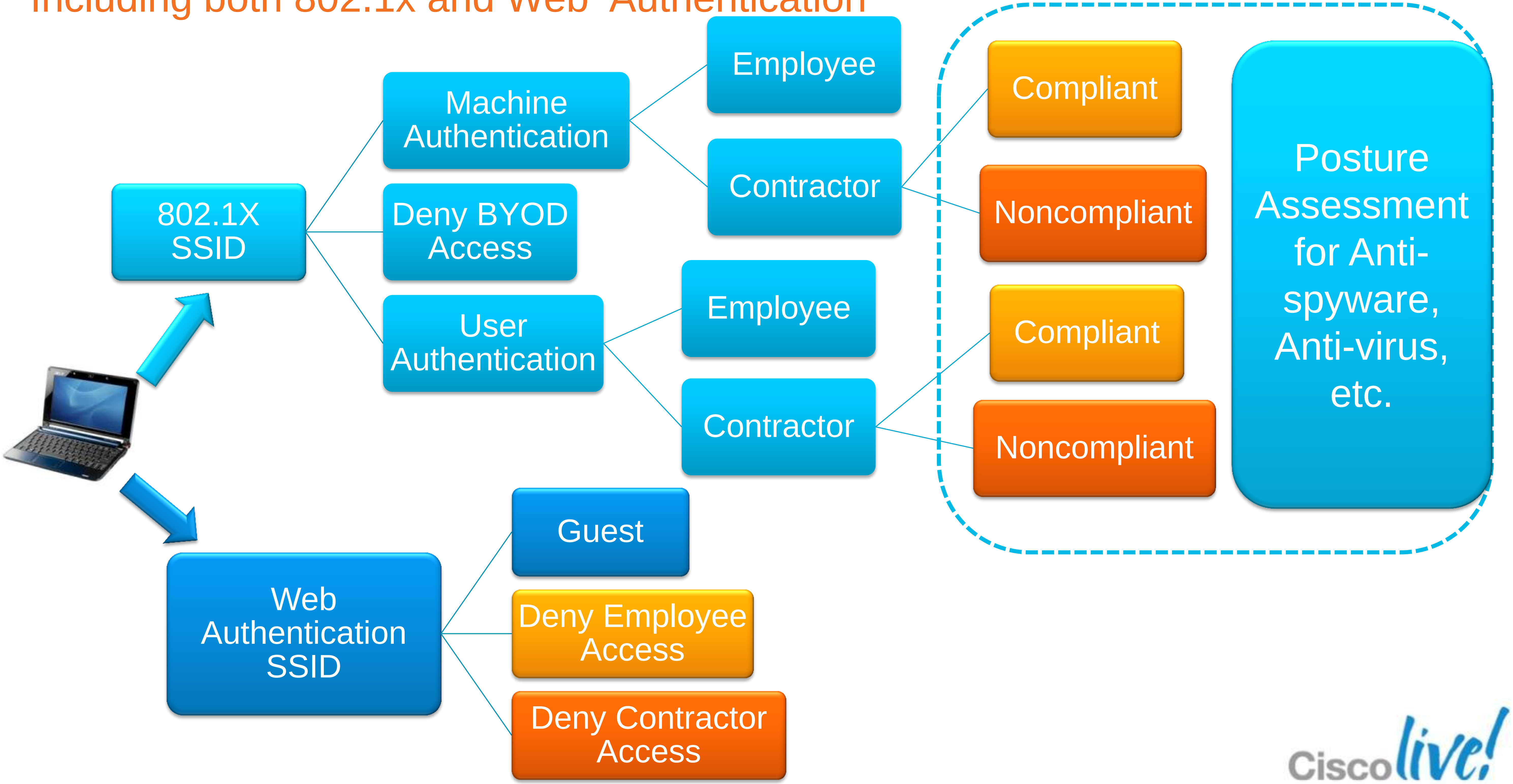
IF $Identity AND $Device AND $Access AND $Location AND $Time THEN $Permission

Cisco ISE Device Policy Steps



Example Policy + Posture Flow Chart

Including both 802.1x and Web Authentication



802.1X SSID

Machine Authentication

Employee

Contractor

Deny BYOD Access

User Authentication

Employee

Contractor

Compliant

Noncompliant

Compliant

Noncompliant

Posture Assessment for Anti-spyware, Anti-virus, etc.

Web Authentication SSID

Guest

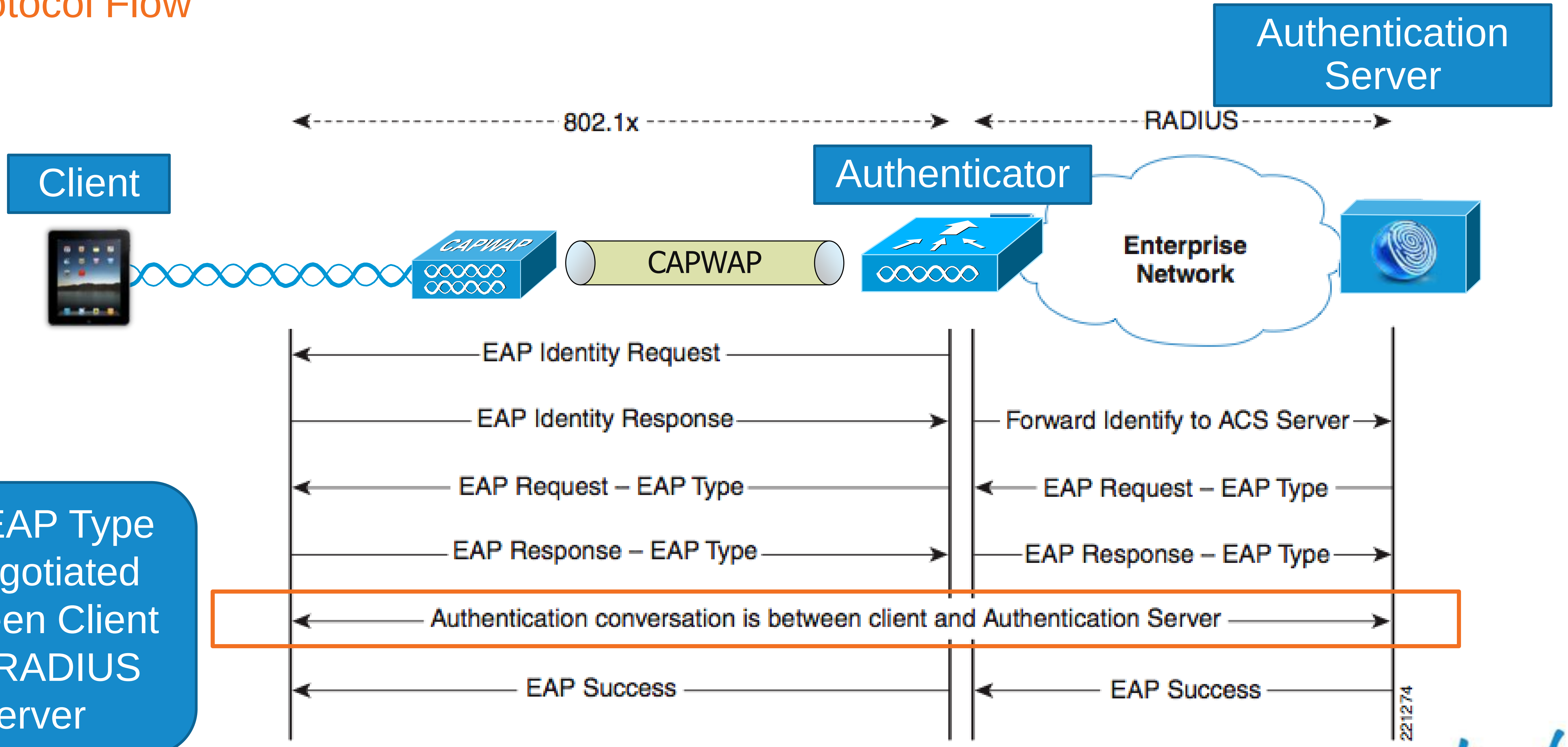
Deny Employee Access

Deny Contractor Access

Integrating the WLC and ISE for Secure Authentication and Profiling

Extensible Authentication Protocol (EAP)

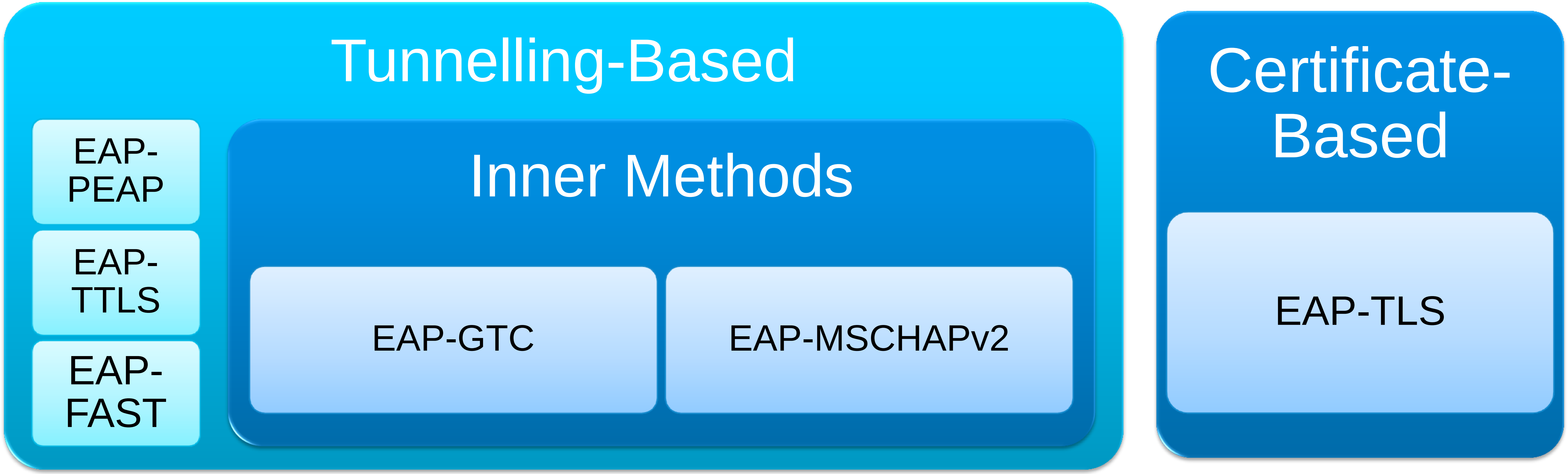
Protocol Flow



The EAP Type is negotiated between Client and RADIUS Server

EAP Authentication Types

Different Authentication Options Leveraging Different Credentials



Tunnelling-Based

EAP-PEAP

EAP-TTLS

EAP-FAST

Inner Methods

EAP-GTC

EAP-MSCHAPv2

Certificate-Based

EAP-TLS

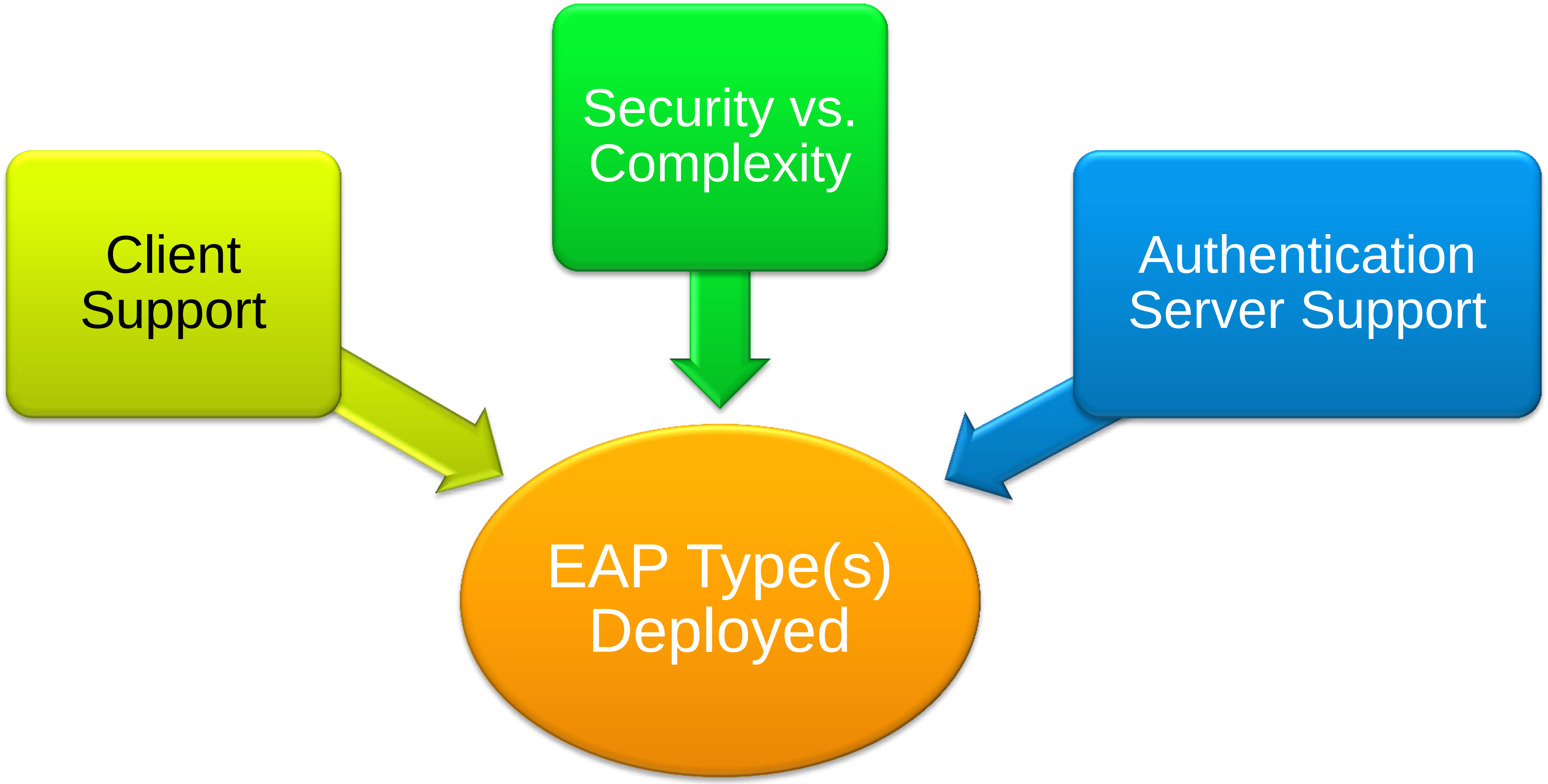
- Tunnel-based - Common deployments use a tunnelling protocol combined with an inner EAP type.
  - – Provides security for the inner EAP type which may be vulnerable by itself.
- Certificate-based – Authentication of both the server and client.

EAP Methods Comparison

	EAP-TLS	PEAP
Fast Secure Roaming (CCKM)	Yes	Yes
Local WLC Authentication	Yes	Yes
OTP (One Time Password) Support	**No**	Yes
Server Certificates	Yes	Yes
Client Certificates	Yes	**No**
Deployment Complexity*	High	Low

Factors in Choosing an EAP Method

The Most Common EAP Types are PEAP and EAP-TLS



- Most clients support EAP-TLS, PEAP (MS-CHAPv2).
  - Additional supplicants can add more EAP types (Cisco AnyConnect).
- Certain EAP types can be more difficult to deploy.
- Cisco ISE Supplicant Provisioning can aid deployment.

Cisco Wireless Controller User-Based Policy AAA Override Attributes

Network Access

- **“Airespace-Interface-Name”**
  - Sets the Interface to which the client is connected.

Network Restrictions

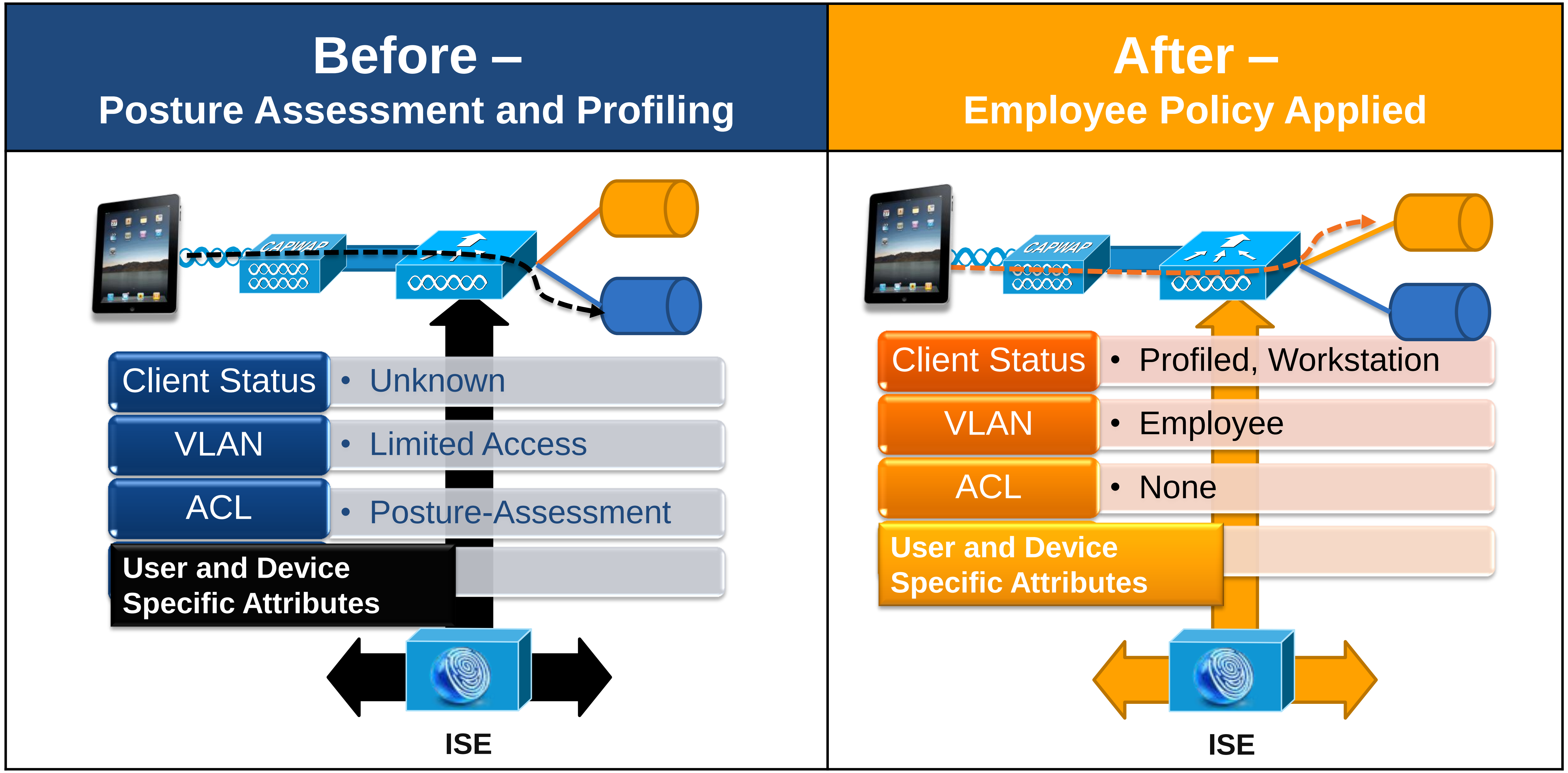
- **“Airespace-ACL-Name”**
  - Sets the Access Control List used to filter traffic to/from the client.

Quality of Service

- **“Airespace-QOS-Level”**
  - Sets the maximum QoS queue level available for use by the client (Bronze, Silver, Gold or Platinum).
- **“Airespace-802.1p-Tag” and/or “Airespace-DSCP-Tag”**
  - Sets the maximum QoS tagging level available for use by the client.

Change of Authorisation (CoA)

Changing Connection Policy Attributes Dynamically



Before – Posture Assessment and Profiling

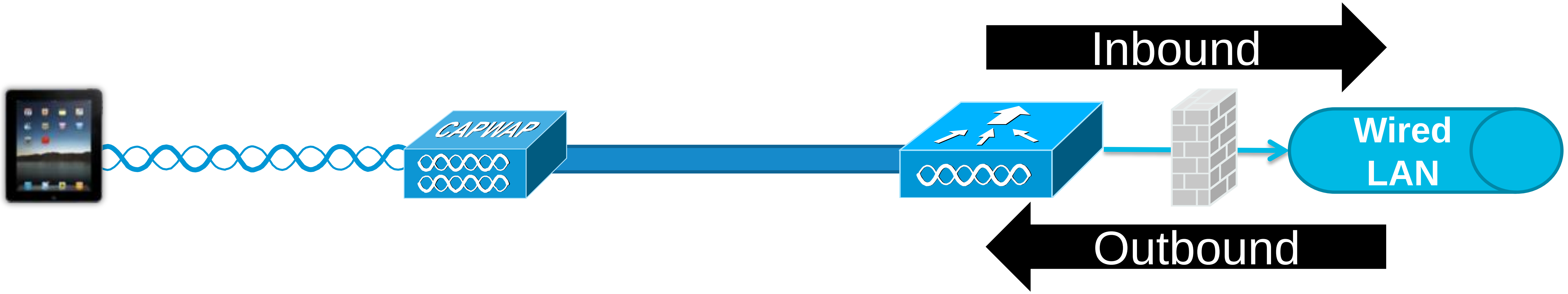
Client Status	• Unknown
VLAN	• Limited Access
ACL	• Posture-Assessment
User and Device Specific Attributes	

After – Employee Policy Applied

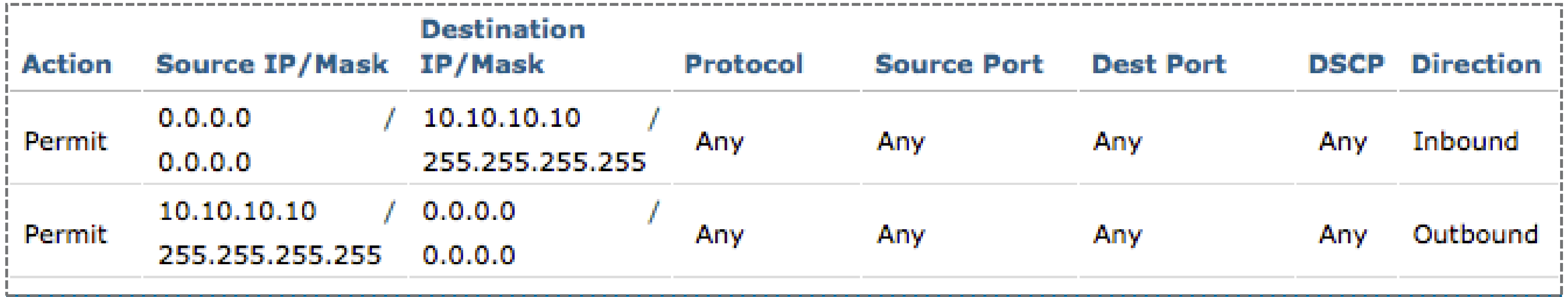
Client Status	• Profiled, Workstation
VLAN	• Employee
ACL	• None
User and Device Specific Attributes	

Cisco Wireless LAN Controller ACLs

Layer 3-4 filtering at line-rate.



- ACLs provide L3-L4 policy, applied per interface or per user.
- Cisco 2500, 5508 WiSM2 implement hardware, line-rate ACLs.
- Up to 64 rules can be configured per ACL.



Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
Permit	0.0.0.0 / 0.0.0.0	10.10.10.10 / 255.255.255.255	Any	Any	Any	Any	Inbound
Permit	10.10.10.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound

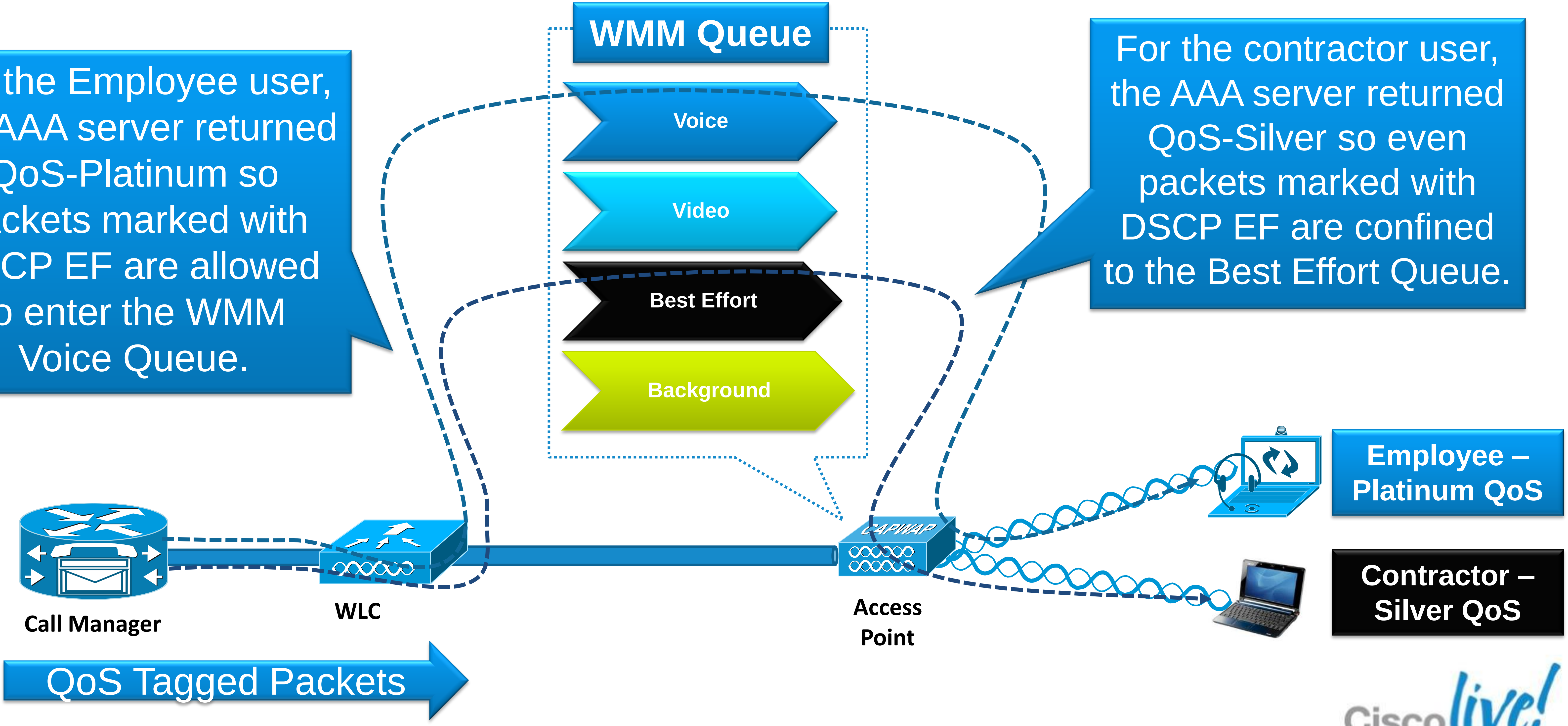
Implicit Deny All at the End

Cisco Wireless User-Based QoS Capabilities

Allowing Per-User and Per-Devices Limiting of the Maximum QoS Level

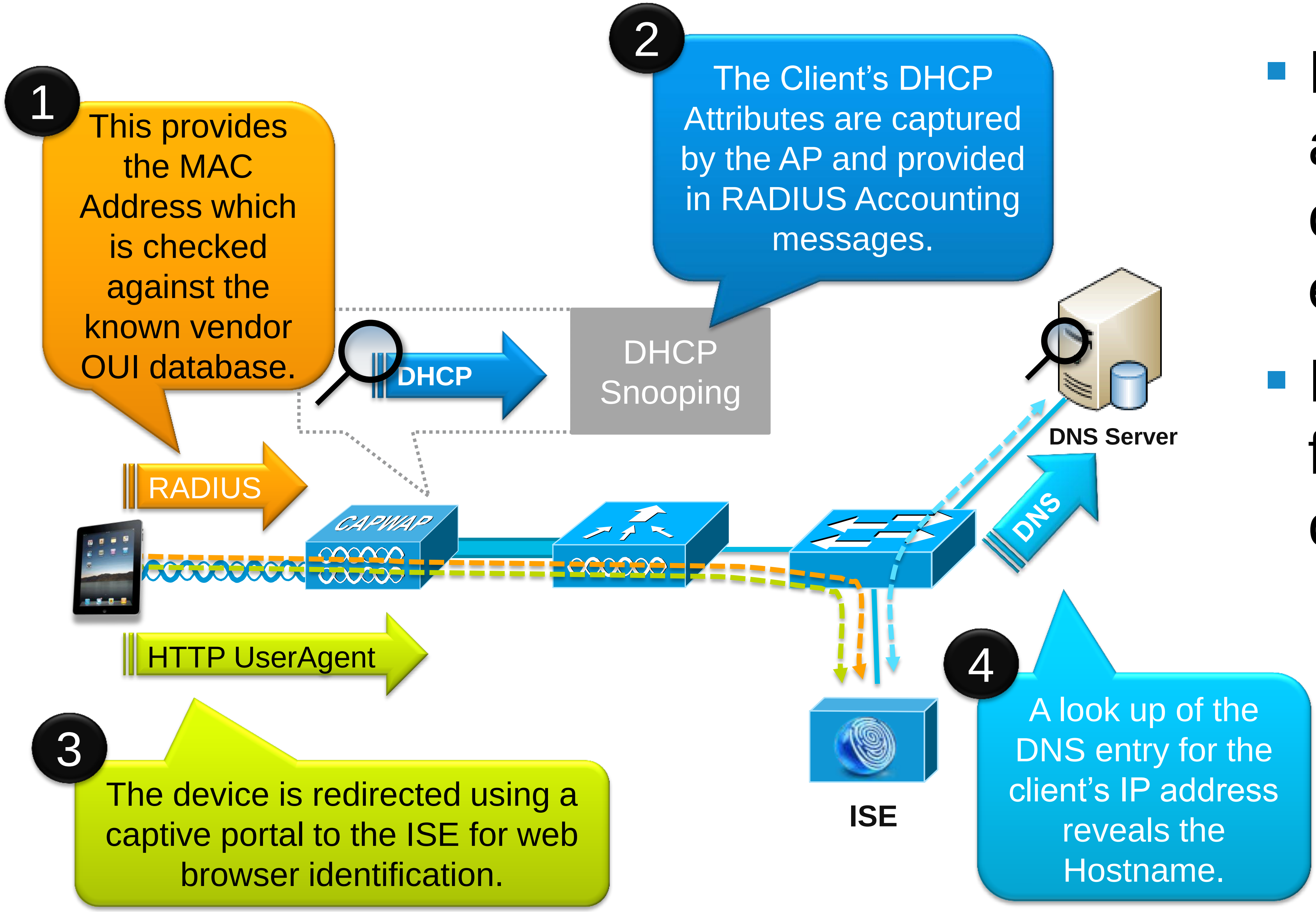
For the Employee user, the AAA server returned QoS-Platinum so packets marked with DSCP EF are allowed to enter the WMM Voice Queue.

For the contractor user, the AAA server returned QoS-Silver so even packets marked with DSCP EF are confined to the Best Effort Queue.



Client Attributes Used for ISE Profiling

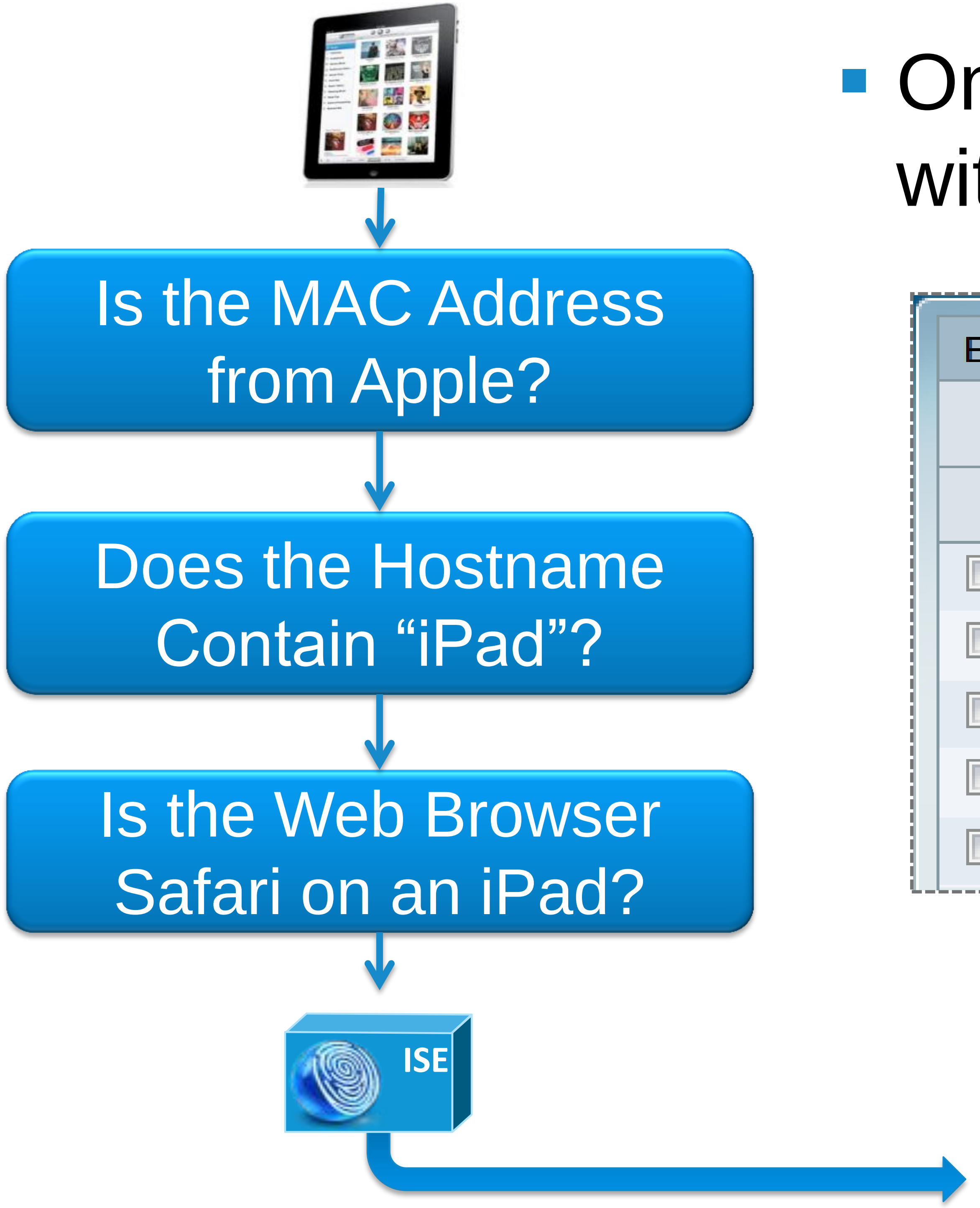
How RADIUS, HTTP, DNS and DHCP (and others) are used to identify clients.


1
This provides the MAC Address which is checked against the known vendor OUI database.
2
The Client's DHCP Attributes are captured by the AP and provided in RADIUS Accounting messages.
DHCP
DHCP Snooping
DNS Server
RADIUS
CAPWAP
DNS
HTTP UserAgent
ISE
3
The device is redirected using a captive portal to the ISE for web browser identification.
4
A look up of the DNS entry for the client's IP address reveals the Hostname.

- ISE uses multiple attributes to build a complete picture of the end client's device profile.
- Information is collected from sensors which capture different attributes
  - The ISE can initiate NMAP scan of the host IP to determine more details.

ISE Device Profiling

iPad Example

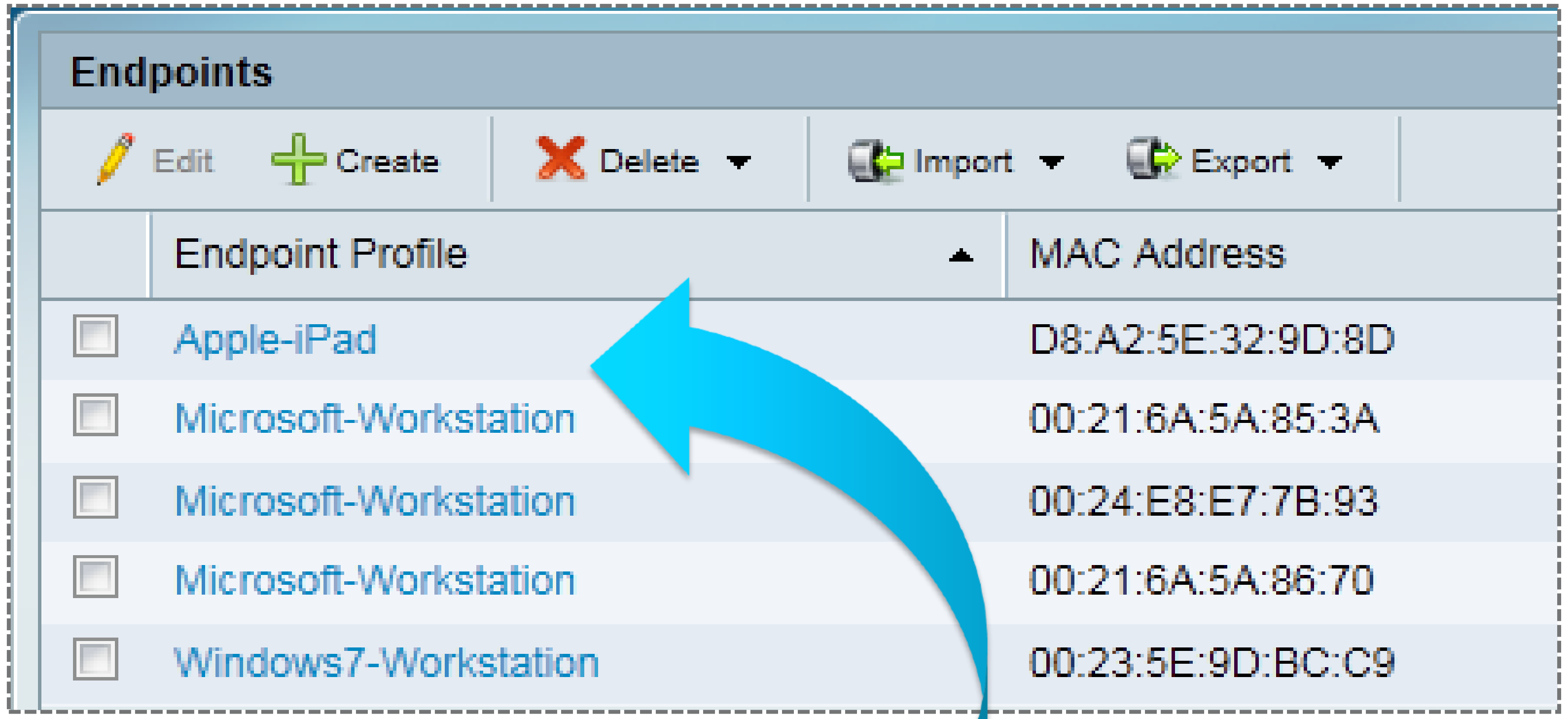


Is the MAC Address from Apple?

Does the Hostname Contain “iPad”?

Is the Web Browser Safari on an iPad?

- Once the device is profiled, it is stored within the ISE for future associations:



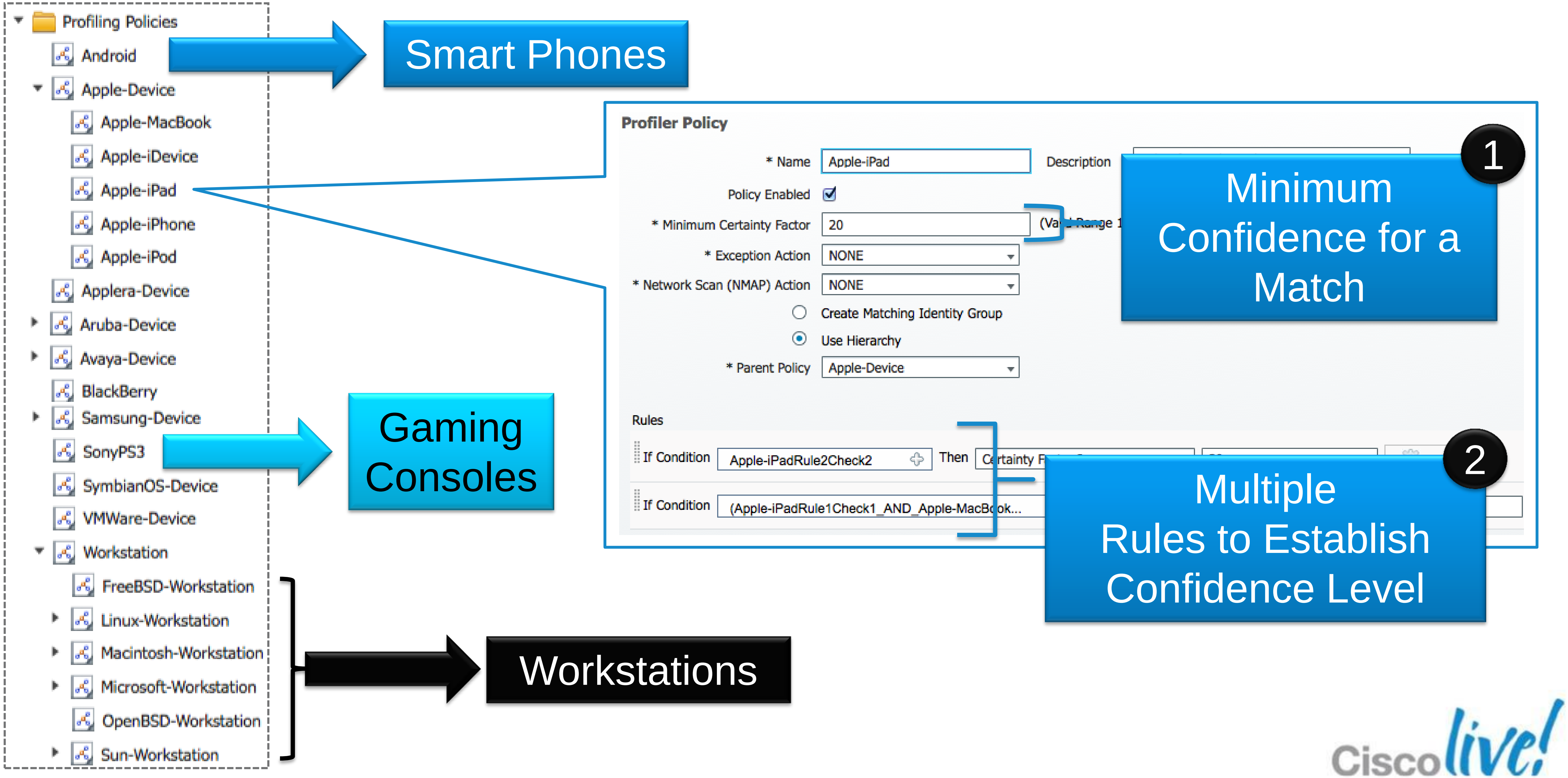
Endpoints

	Endpoint Profile	MAC Address
□	Apple-iPad	D8:A2:5E:32:9D:8D
□	Microsoft-Workstation	00:21:6A:5A:85:3A
□	Microsoft-Workstation	00:24:E8:E7:7B:93
□	Microsoft-Workstation	00:21:6A:5A:86:70
□	Windows7-Workstation	00:23:5E:9D:BC:C9

Apple iPad

ISE Device Profiling Capabilities

Over 200 Built-in Device Policies, Defined Hierarchically by Vendor



- Profiling Policies
  - Android
  - Apple-Device
    - Apple-MacBook
    - Apple-iDevice
    - Apple-iPad
    - Apple-iPhone
    - Apple-iPod
  - Applera-Device
  - Aruba-Device
  - Avaya-Device
  - BlackBerry
  - Samsung-Device
  - SonyPS3
  - SymbianOS-Device
  - VMWare-Device
  - Workstation
    - FreeBSD-Workstation
    - Linux-Workstation
    - Macintosh-Workstation
    - Microsoft-Workstation
    - OpenBSD-Workstation
    - Sun-Workstation

Smart Phones

Gaming Consoles

Workstations

Profiler Policy

* Name	Apple-iPad	Description
Policy Enabled	☑	
* Minimum Certainty Factor	20	(Va Range 1
* Exception Action	NONE	
* Network Scan (NMAP) Action	NONE	
	○ Create Matching Identity Group	
	● Use Hierarchy	
* Parent Policy	Apple-Device	

Rules

If Condition	Apple-iPadRule2Check2	Then	Certainty F
If Condition	(Apple-iPadRule1Check1_AND_Apple-MacBook...		

1 Minimum Confidence for a Match

2 Multiple Rules to Establish Confidence Level

Steps for Integrating Controller and ISE

1. Configure WLAN for 802.1x Authentication

- Configure RADIUS Server on Controller
- Setup WLAN for AAA Override, Profiling and RADIUS NAC

2. Configure ISE Profiling

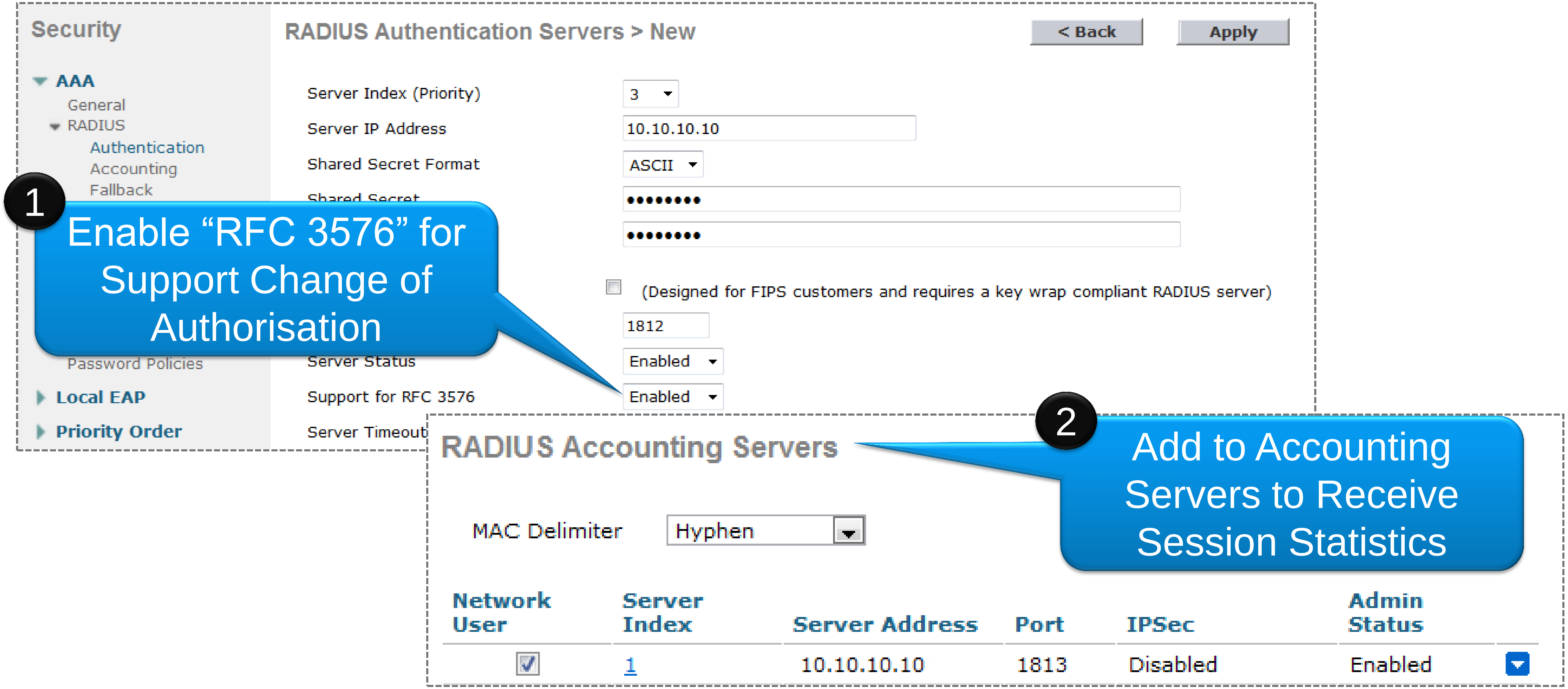
- Enable profiling sensors

3. Setup Access Restrictions

- Configure ACLs to filter and control network access.

Configure ISE as the AAA Server

Authentication and Accounting



RADIUS Authentication Servers > New

Server Index (Priority)	3
Server IP Address	10.10.10.10
Shared Secret Format	ASCII
Shared Secret	••••••••
	••••••••
	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	

1 Enable "RFC 3576" for Support Change of Authorisation

RADIUS Accounting Servers

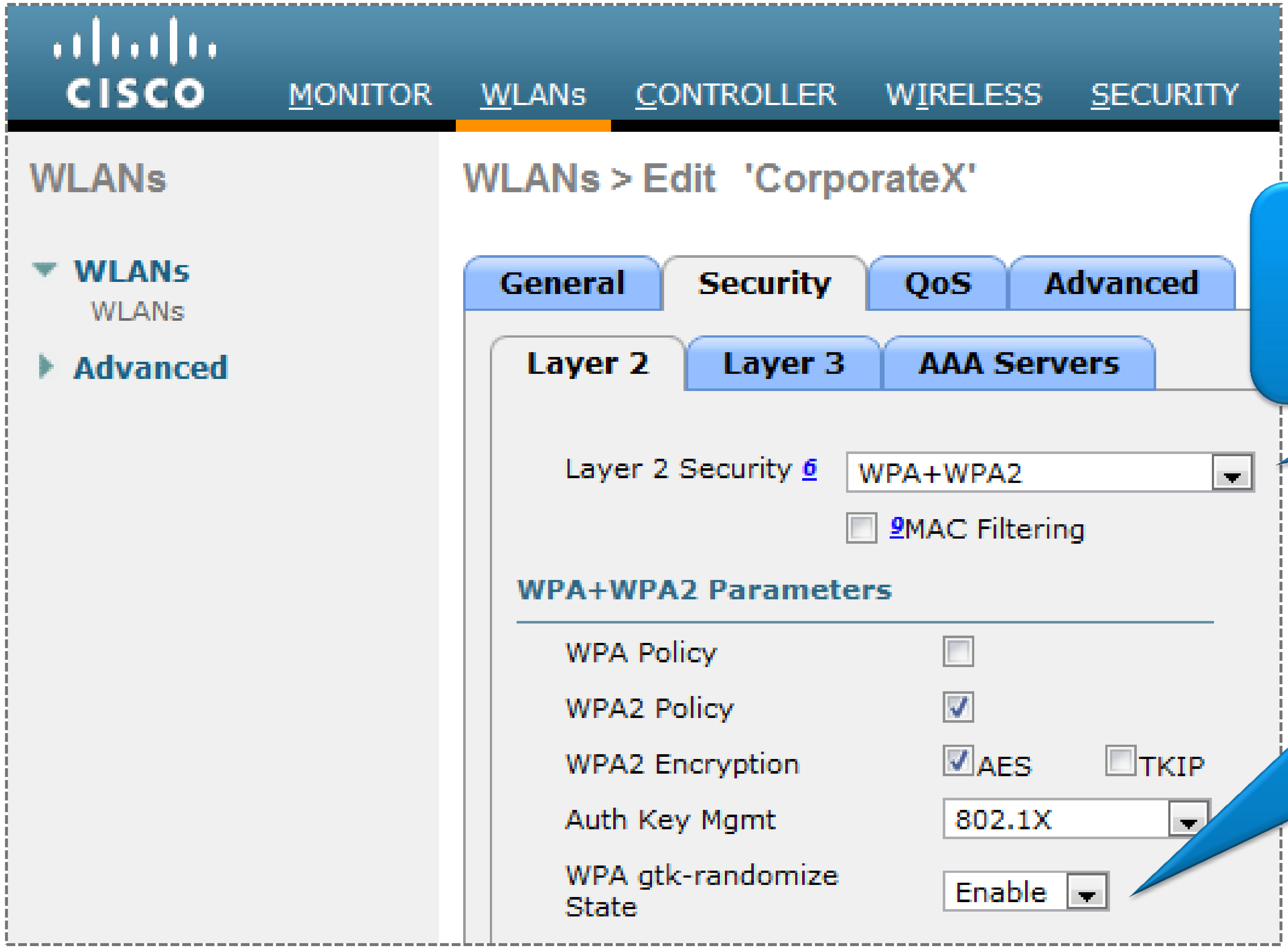
MAC Delimiter: Hyphen

Network User	Server Index	Server Address	Port	IPSec	Admin Status
☑	1	10.10.10.10	1813	Disabled	Enabled

2 Add to Accounting Servers to Receive Session Statistics

Configure WLAN for Secure Connectivity

Enabling Secure Authentication and Encryption with WPA2-Enterprise



WLANs > Edit 'CorporateX'

Layer 2 Security 6: WPA+WPA2

□ 9MAC Filtering

WPA+WPA2 Parameters

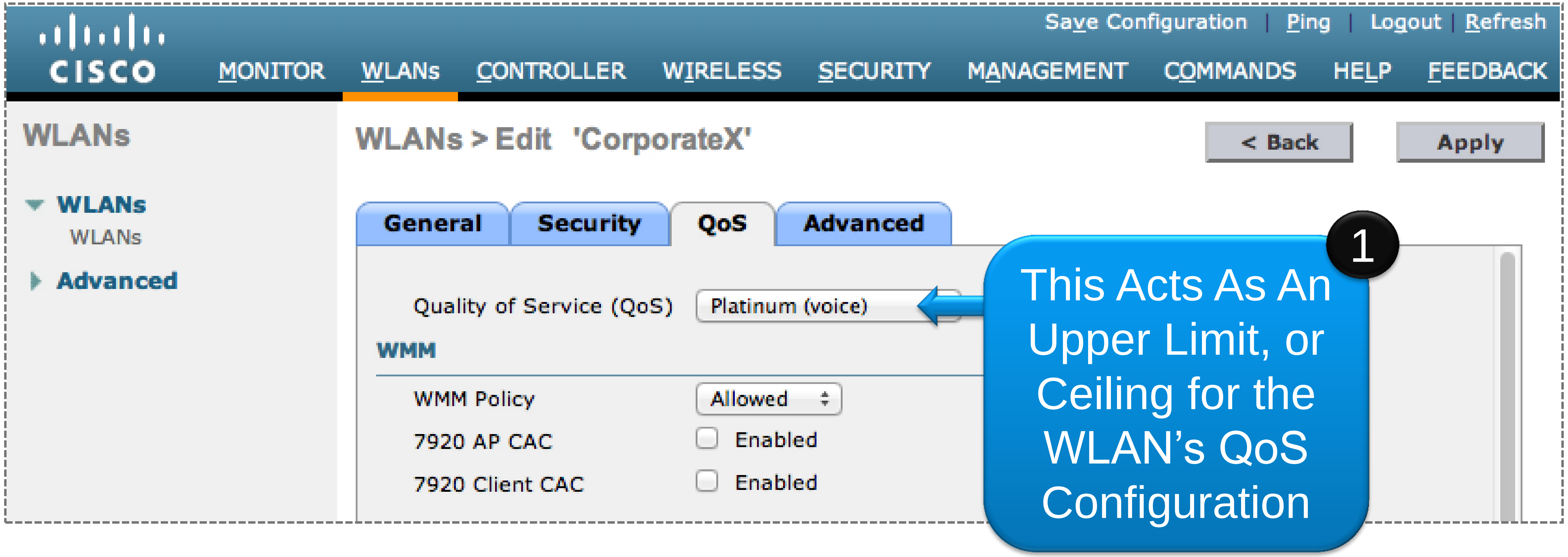
WPA Policy	□
WPA2 Policy	☑
WPA2 Encryption	☑ AES □ TKIP
Auth Key Mgmt	802.1X
WPA gtk-randomize State	Enable

1 WPA2 Security with AES Encryption

2 Use GTK-Randomisation to Prevent “Hole196” Attacks as each client receives a unique GTK.

Set WLAN QoS Level for Override

Using WMM, the QoS level is based on the marking of the packet.



WLANs > Edit 'CorporateX'

Quality of Service (QoS) Platinum (voice)

WMM

WMM Policy Allowed

7920 AP CAC □ Enabled

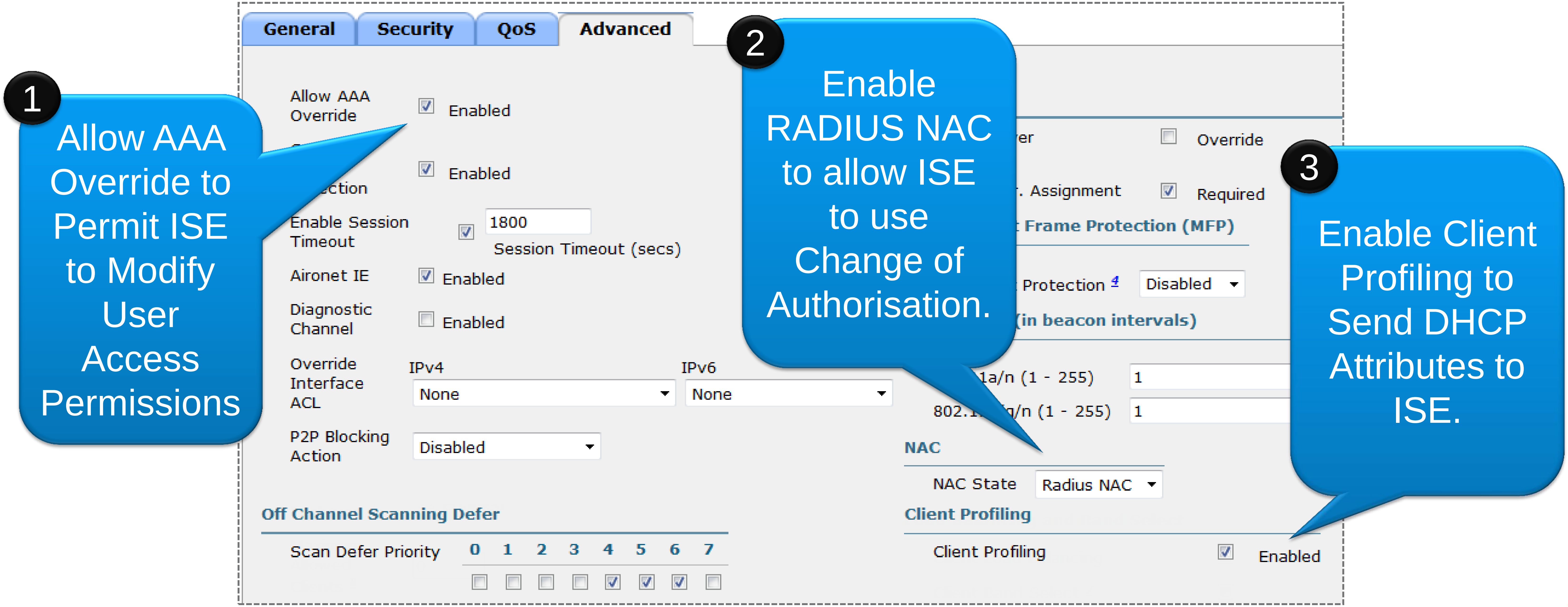
7920 Client CAC □ Enabled

This Acts As An Upper Limit, or Ceiling for the WLAN's QoS Configuration

- If WMM is set to Allowed, the QoS configuration serves as a limit for the entire SSID.
- Ensure all controller uplinks, media servers and Access Points have proper QoS trust commands in IOS.

Configure WLAN for ISE Integration

AAA Override, CoA and Profiling



General | Security | QoS | Advanced

Allow AAA Override ☑ Enabled

☑ Enabled

...ection

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

Override Interface ACL IPv4 None ▾ IPv6 None ▾

P2P Blocking Action Disabled ▾

Off Channel Scanning Defer

Scan Defer Priority	0	1	2	3	4	5	6	7
	□	□	□	□	☑	☑	☑	□

...er □ Override

. Assignment ☑ Required

Frame Protection (MFP)

Protection 4 Disabled ▾

(in beacon intervals)

1a/n (1 - 255) 1

802.1 g/n (1 - 255) 1

NAC

NAC State Radius NAC ▾

Client Profiling

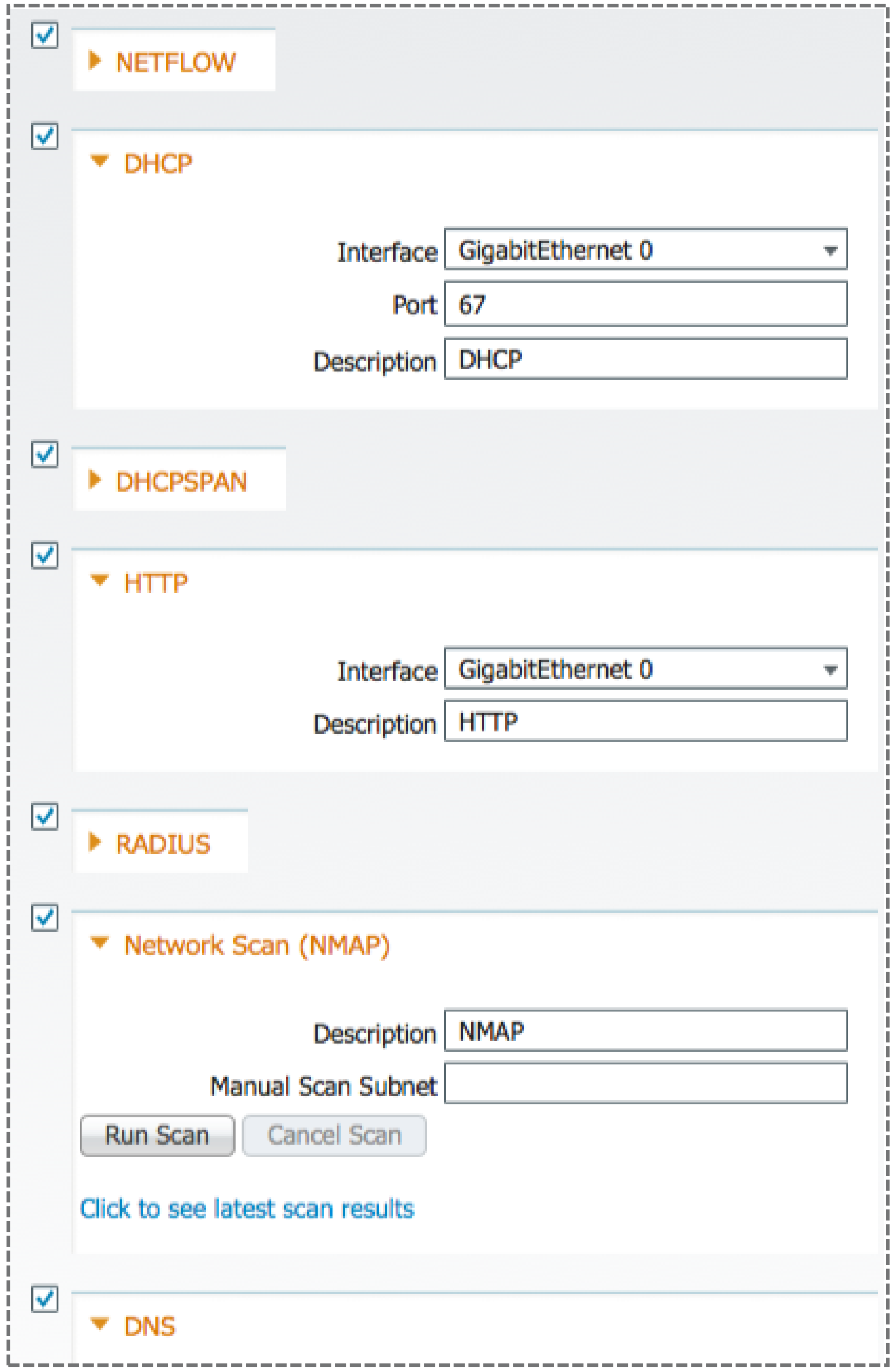
Client Profiling ☑ Enabled

1 Allow AAA Override to Permit ISE to Modify User Access Permissions

2 Enable RADIUS NAC to allow ISE to use Change of Authorisation.

3 Enable Client Profiling to Send DHCP Attributes to ISE.

Configuring ISE Profiling Sensors



☑ NETFLOW

☑ DHCP

Interface: GigabitEthernet 0

Port: 67

Description: DHCP

☑ DHCPSPAN

☑ HTTP

Interface: GigabitEthernet 0

Description: HTTP

☑ RADIUS

☑ Network Scan (NMAP)

Description: NMAP

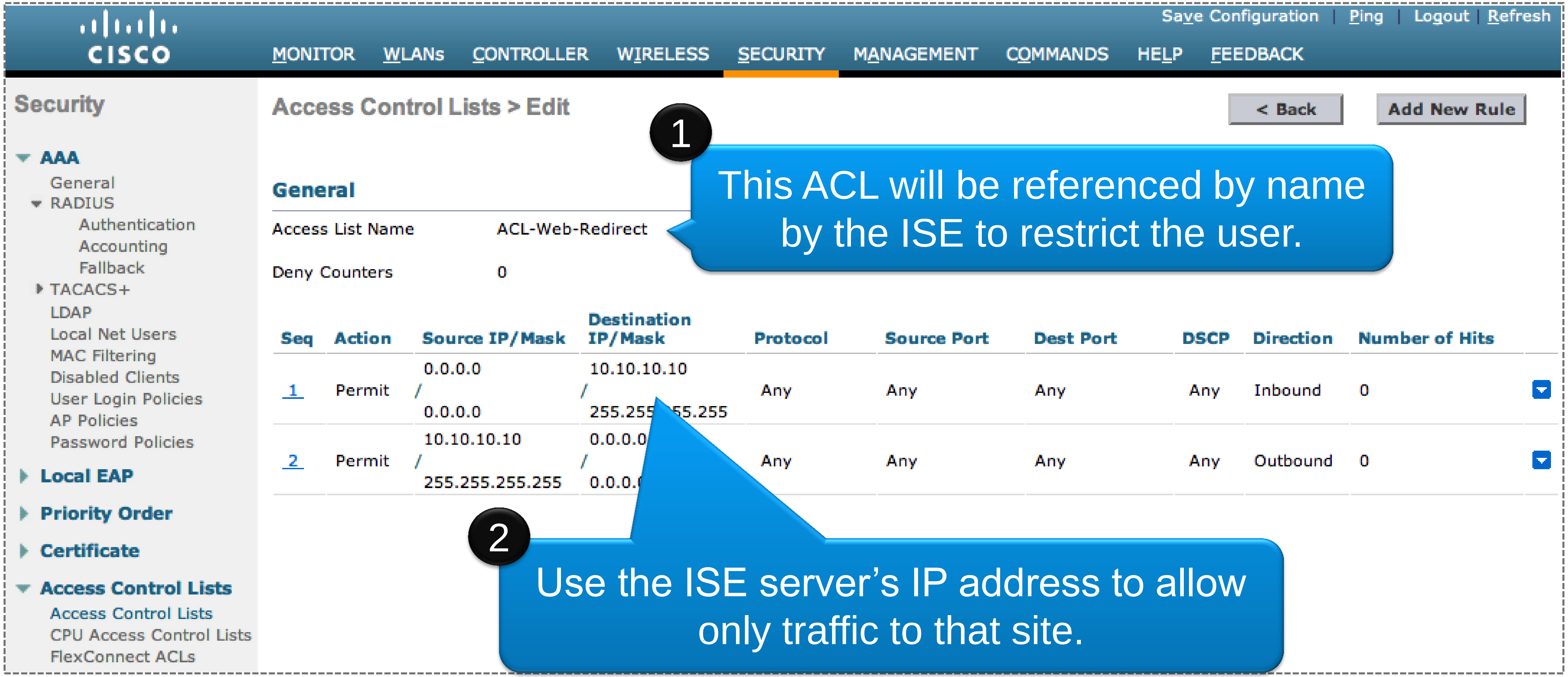
Manual Scan Subnet:

☑ DNS

- Profiling can be achieved through a span port.
- More efficient profiling is achieved through sensors which selectively forward attributes.
- For DHCP Profiling:
  - Use v7.2 MR1 code to capture and send attributes in RADIUS accounting; or
  - Use Cisco IOS "ip helper" addressed to ISE on switches adjacent to the WLC.
- For HTTP Profiling:
  - Use v7.4 code to capture and send attributes in RADIUS accounting; or
  - Use the Web-Authentication redirect to get the HTTP user agent.

Configuring the Web-Auth Redirect ACL

The ACL is used in HTTP profiling as well as posture and client provisioning.



Access Control Lists > Edit

General

Access List Name ACL-Web-Redirect

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.10 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
2	Permit	10.10.10.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0

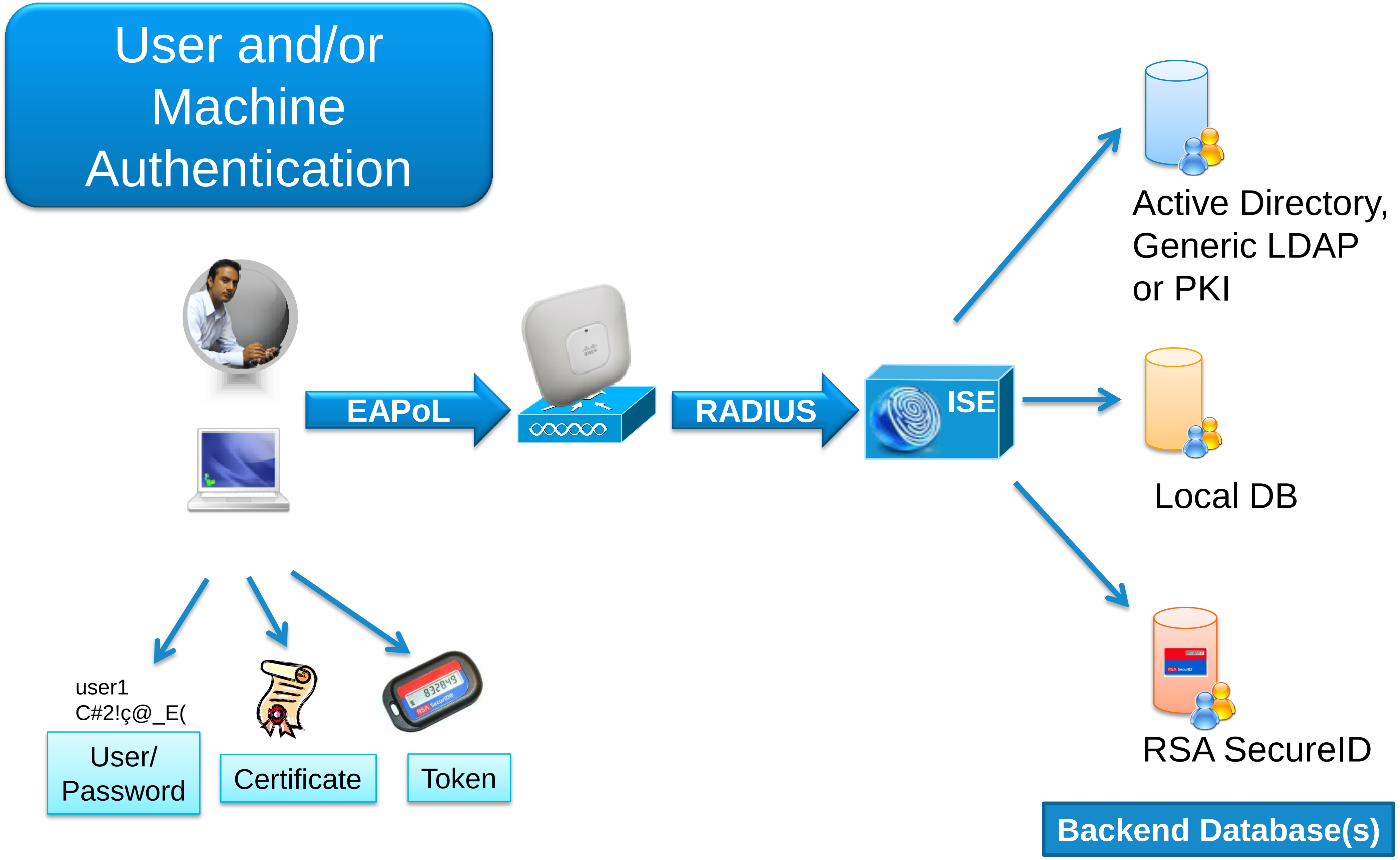
1 This ACL will be referenced by name by the ISE to restrict the user.

2 Use the ISE server's IP address to allow only traffic to that site.

Cisco live!

Defining a Security Policy Within ISE

ISE Authentication Sources



- Cisco ISE can reference backend identity stores including Active Directory, PKI, LDAP and RSA SecureID.
- The local database can also be used on the ISE itself for small deployments.

Steps for Configuring ISE Policies

Authentication and Authorisation

1. Authentication Rules

- Define what identity stores to reference.
  - – Example – Active Directory, LDAP, CA Server or Internal DB.

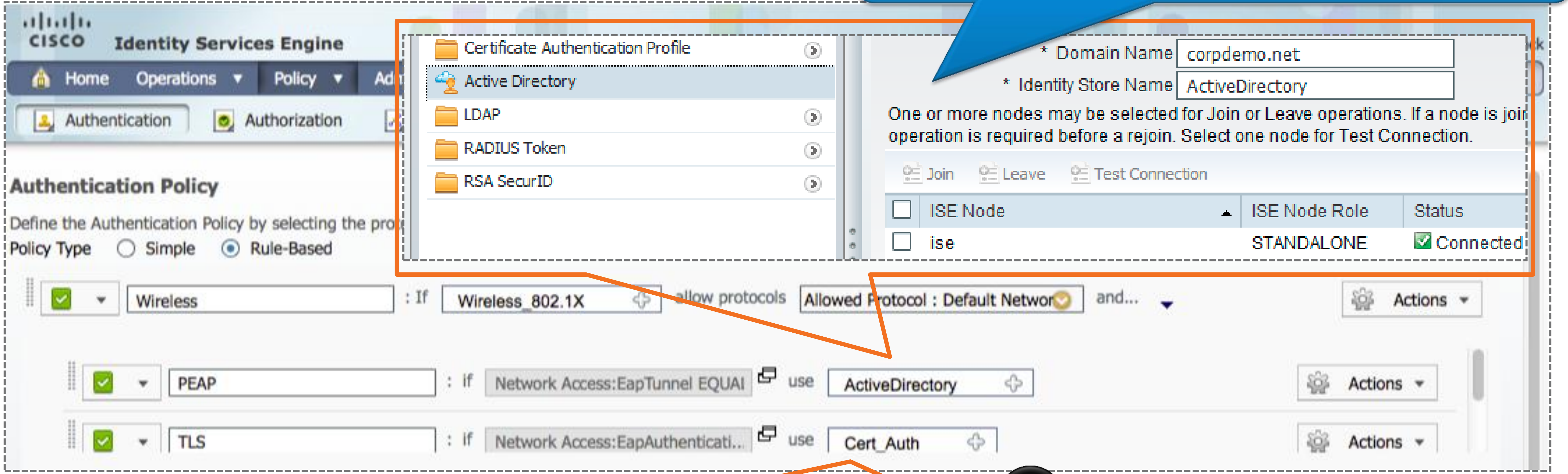
2. Authorisation Rules

- Define what users and devices get access to resources.
  - – Example – All Employees, with Windows Laptops have full access.

Authentication Rules

Example for PEAP and EAP-TLS

1 Reference Active Directory for PEAP Authentication



Authentication Policy

Define the Authentication Policy by selecting the pro

Policy Type ○ Simple ● Rule-Based

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

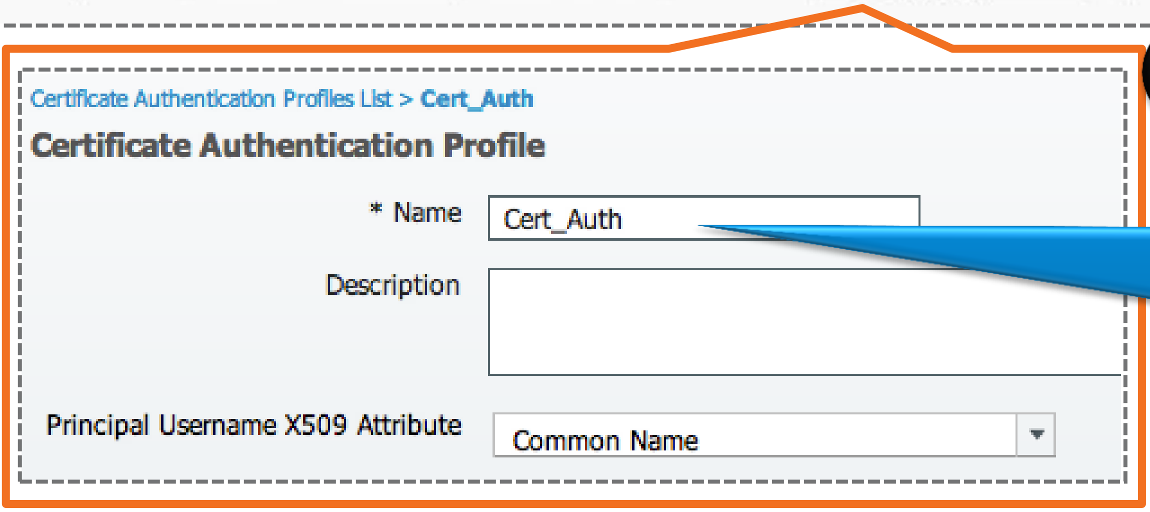
* Domain Name corpdemo.net

* Identity Store Name ActiveDirectory

One or more nodes may be selected for Join or Leave operations. If a node is joi operation is required before a rejoin. Select one node for Test Connection.

□	ISE Node	ISE Node Role	Status
□	ise	STANDALONE	☑ Connected

	Rule		Condition				
☑	Wireless	: If	Wireless_802.1X	allow protocols	Allowed Protocol : Default Networ	and...	Actions ▾
☑	PEAP	: if	Network Access:EapTunnel EQUAl	use	ActiveDirectory		Actions ▾
☑	TLS	: if	Network Access:EapAuthenticati...	use	Cert_Auth		Actions ▾



Certificate Authentication Profiles List > Cert_Auth

Certificate Authentication Profile

* Name Cert_Auth

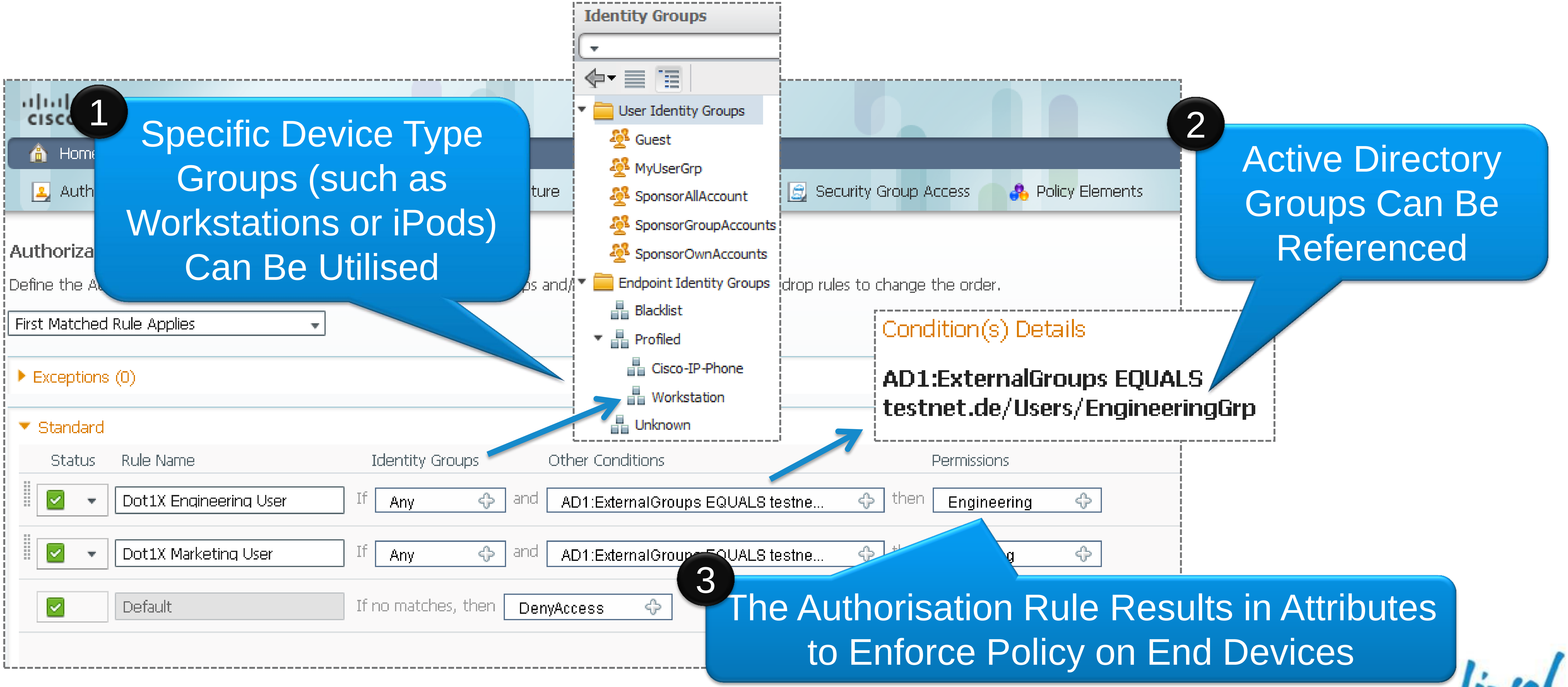
Description

Principal Username X509 Attribute Common Name ▾

2 Create Another Profile to Reference the Certificate Store

Authorisation Rules Configuration

Flexible Conditions Connecting Both User and Device



Identity Groups

- User Identity Groups
  - Guest
  - MyUserGrp
  - SponsorAllAccount
  - SponsorGroupAccounts
  - SponsorOwnAccounts
- Endpoint Identity Groups
  - Blacklist
  - Profiled
    - Cisco-IP-Phone
    - Workstation
  - Unknown

Authoriza

Define the A ps and/ drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Identity Groups		Other Conditions		Permissions
☑	Dot1X Engineering User	If	Any	and	AD1:ExternalGroups EQUALS testne...	then	Engineering
☑	Dot1X Marketing User	If	Any	and	AD1:ExternalGroup EQUALS testne...		g
☑	Default	If no matches, then	DenyAccess				

Condition(s) Details

AD1:ExternalGroups EQUALS testnet.de/Users/EngineeringGrp

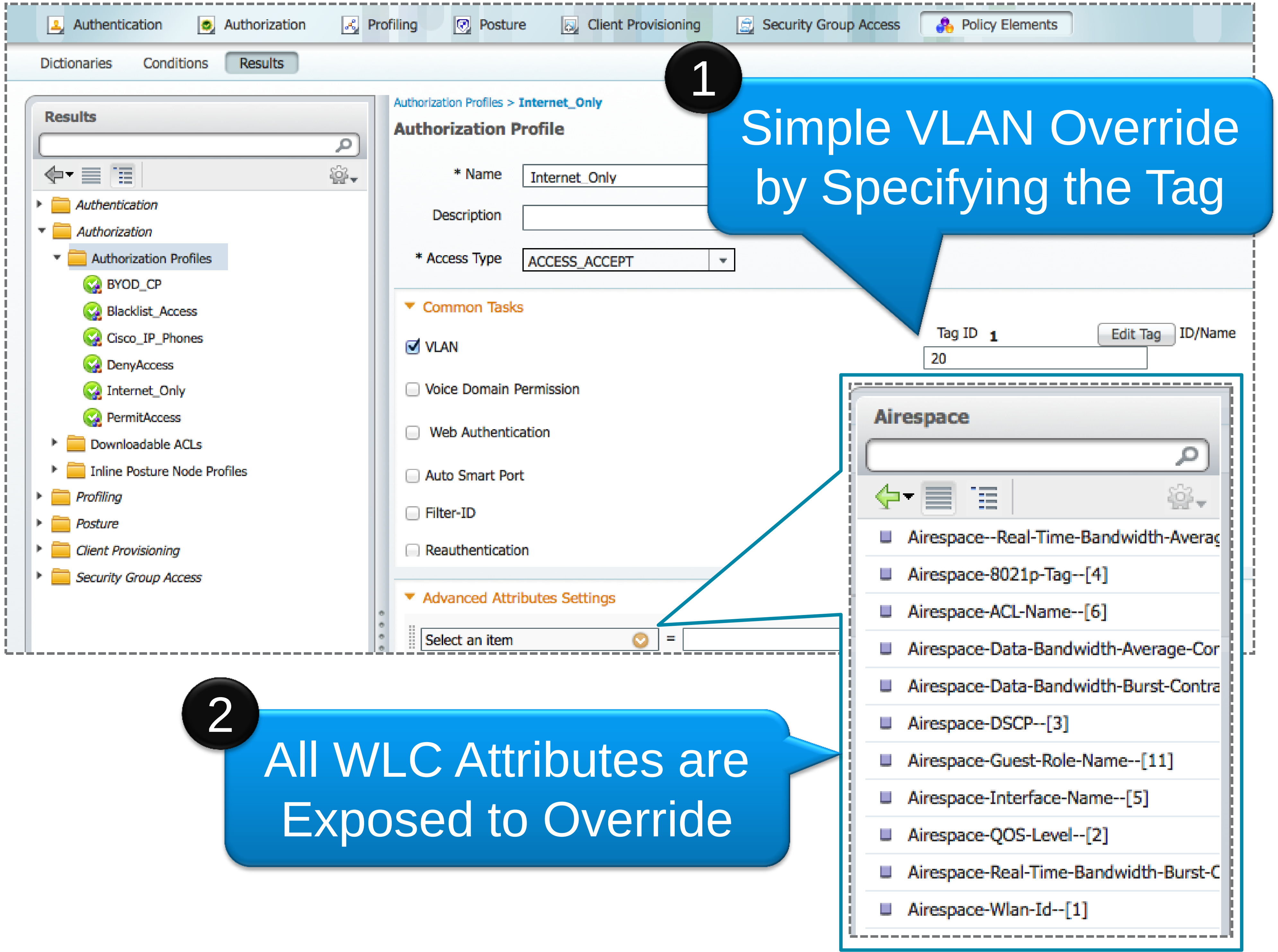
1 Specific Device Type Groups (such as Workstations or iPods) Can Be Utilised

2 Active Directory Groups Can Be Referenced

3 The Authorisation Rule Results in Attributes to Enforce Policy on End Devices

Authorisation Rule “Results”

The Actual Permissions Referenced by the Authorisation Rules



Authentication | Authorization | Profiling | Posture | Client Provisioning | Security Group Access | Policy Elements

Dictionaries | Conditions | Results

Results

- Authentication
- Authorization
  - Authorization Profiles
    - BYOD_CP
    - Blacklist_Access
    - Cisco_IP_Phones
    - DenyAccess
    - Internet_Only
    - PermitAccess
  - Downloadable ACLs
  - Inline Posture Node Profiles
- Profiling
- Posture
- Client Provisioning
- Security Group Access

Authorization Profiles > **Internet_Only**

Authorization Profile

* Name: Internet_Only

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☑ VLAN — Tag ID 1 — Edit Tag — ID/Name 20

☐ Voice Domain Permission

☐ Web Authentication

☐ Auto Smart Port

☐ Filter-ID

☐ Reauthentication

Advanced Attributes Settings

Select an item =

Airspace

- Airspace--Real-Time-Bandwidth-Averag
- Airspace-8021p-Tag--[4]
- Airspace-ACL-Name--[6]
- Airspace-Data-Bandwidth-Average-Cor
- Airspace-Data-Bandwidth-Burst-Contra
- Airspace-DSCP--[3]
- Airspace-Guest-Role-Name--[11]
- Airspace-Interface-Name--[5]
- Airspace-QOS-Level--[2]
- Airspace-Real-Time-Bandwidth-Burst-C
- Airspace-Wlan-Id--[1]

1 Simple VLAN Override by Specifying the Tag

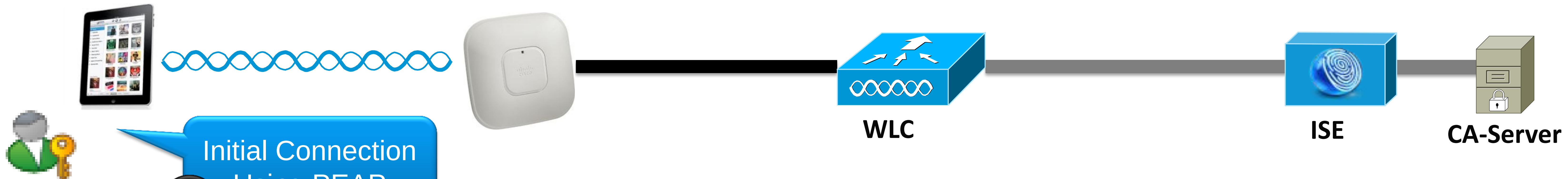
2 All WLC Attributes are Exposed to Override

- The profile contains all of the connection attributes
  - including VLAN, ACL and QoS.
- These attributes are sent to the controller for enforcement,
- Attributes can be changed at a later time using CoA (Change of Authorisation).

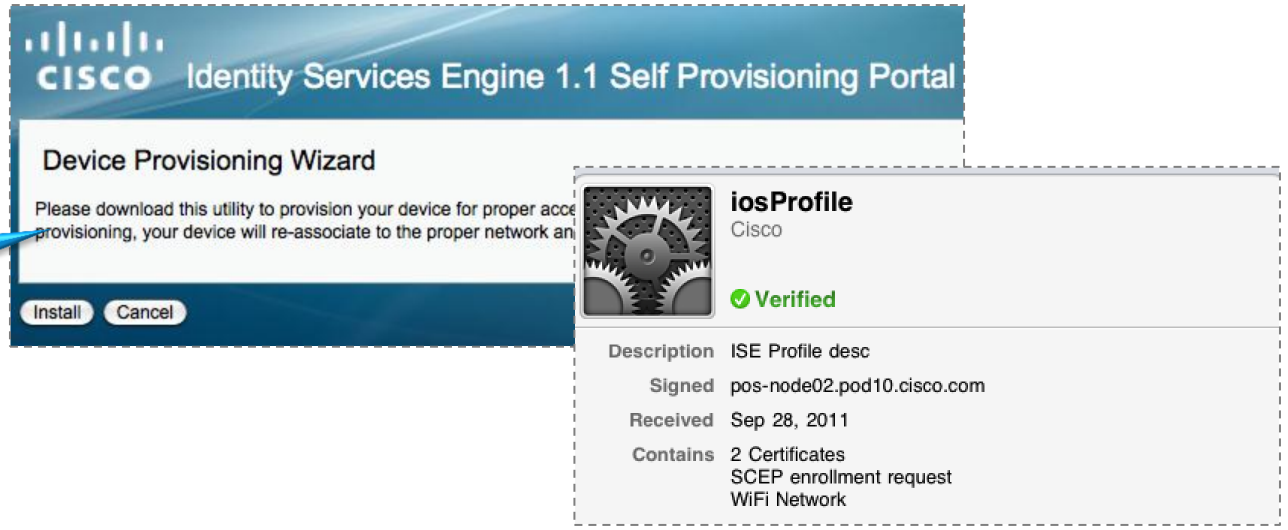
BYOD Device Provisioning

Apple iOS Device Provisioning

Use Native APIs



1 Initial Connection Using PEAP



Identity Services Engine 1.1 Self Provisioning Portal

Device Provisioning Wizard

Please download this utility to provision your device for proper acce provisioning, your device will re-associate to the proper network an

Install Cancel

iosProfile
Cisco

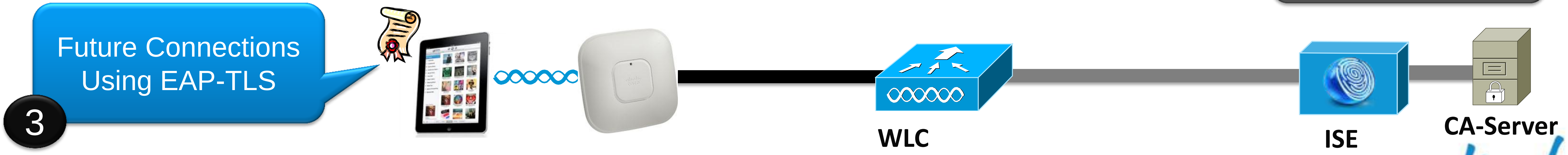
Verified

Description ISE Profile desc
Signed pos-node02.pod10.cisco.com
Received Sep 28, 2011
Contains 2 Certificates
SCEP enrollment request
WiFi Network

2 Device Provisioning Wizard

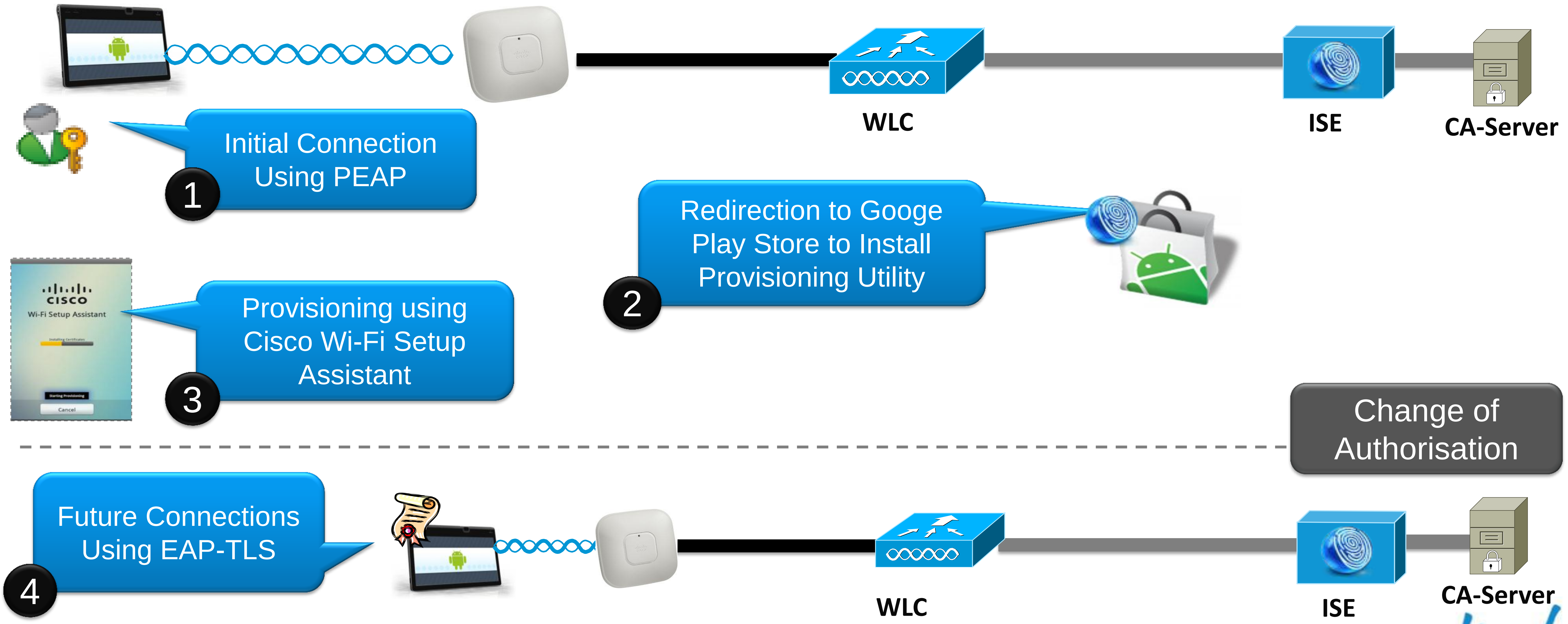
Change of Authorisation

3 Future Connections Using EAP-TLS



Android Device Provisioning

Wide variety of OS flavours = no consistent native API



1 Initial Connection Using PEAP

2 Redirection to Googe Play Store to Install Provisioning Utility

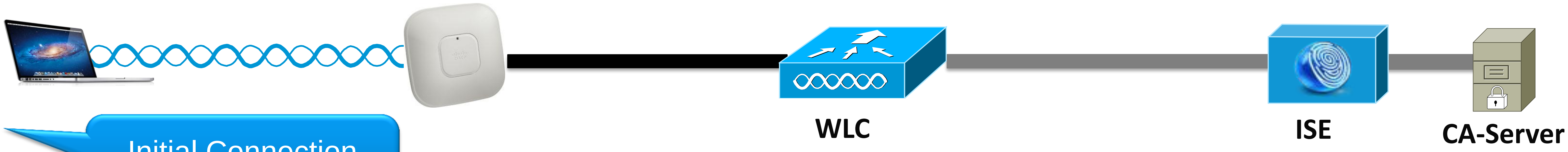
3 Provisioning using Cisco Wi-Fi Setup Assistant

Change of Authorisation

4 Future Connections Using EAP-TLS

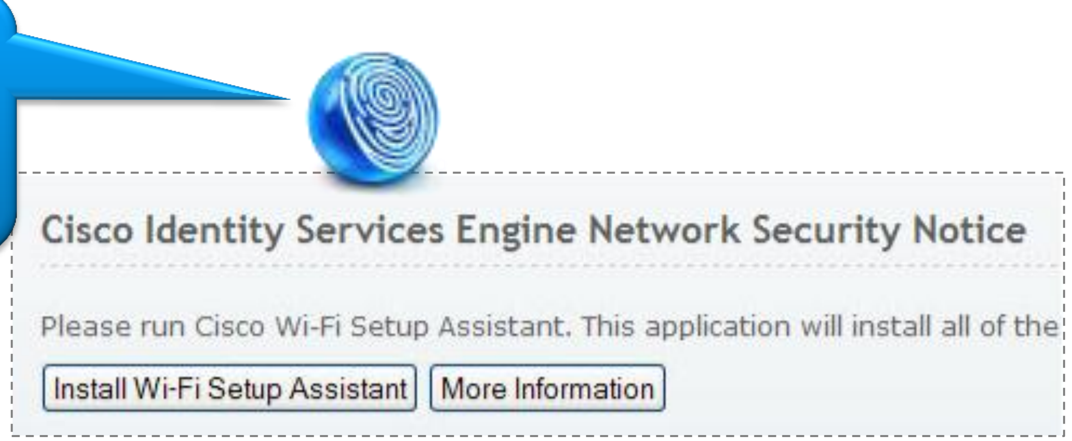
Windows/Mac OS X Device Provisioning

Configure Native OS Supplicant



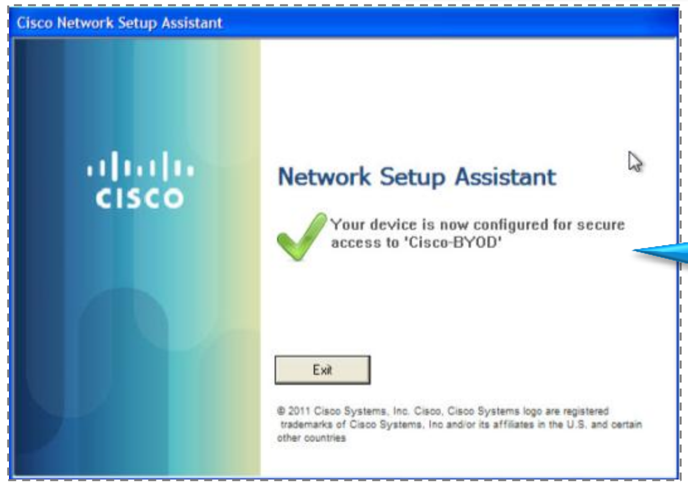
Initial Connection Using PEAP 1

Redirection to ISE to Install OS-Specific Provisioning Utility 2



Cisco Identity Services Engine Network Security Notice

Please run Cisco Wi-Fi Setup Assistant. This application will install all of the



Cisco Network Setup Assistant

Network Setup Assistant

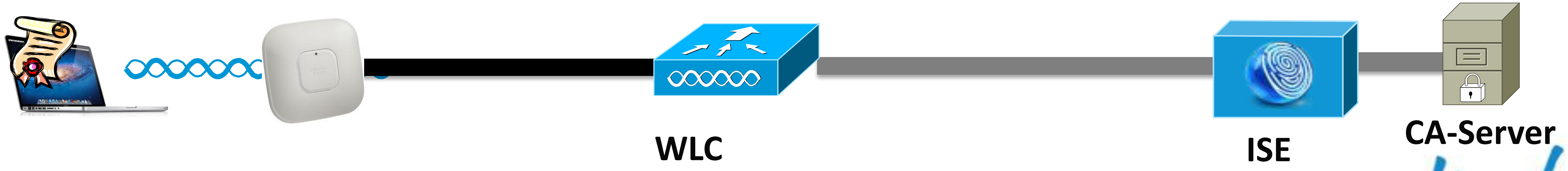
Your device is now configured for secure access to 'Cisco-BYOD'

© 2011 Cisco Systems, Inc. Cisco, Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries

Provisioning using Cisco Wi-Fi Setup Assistant 3

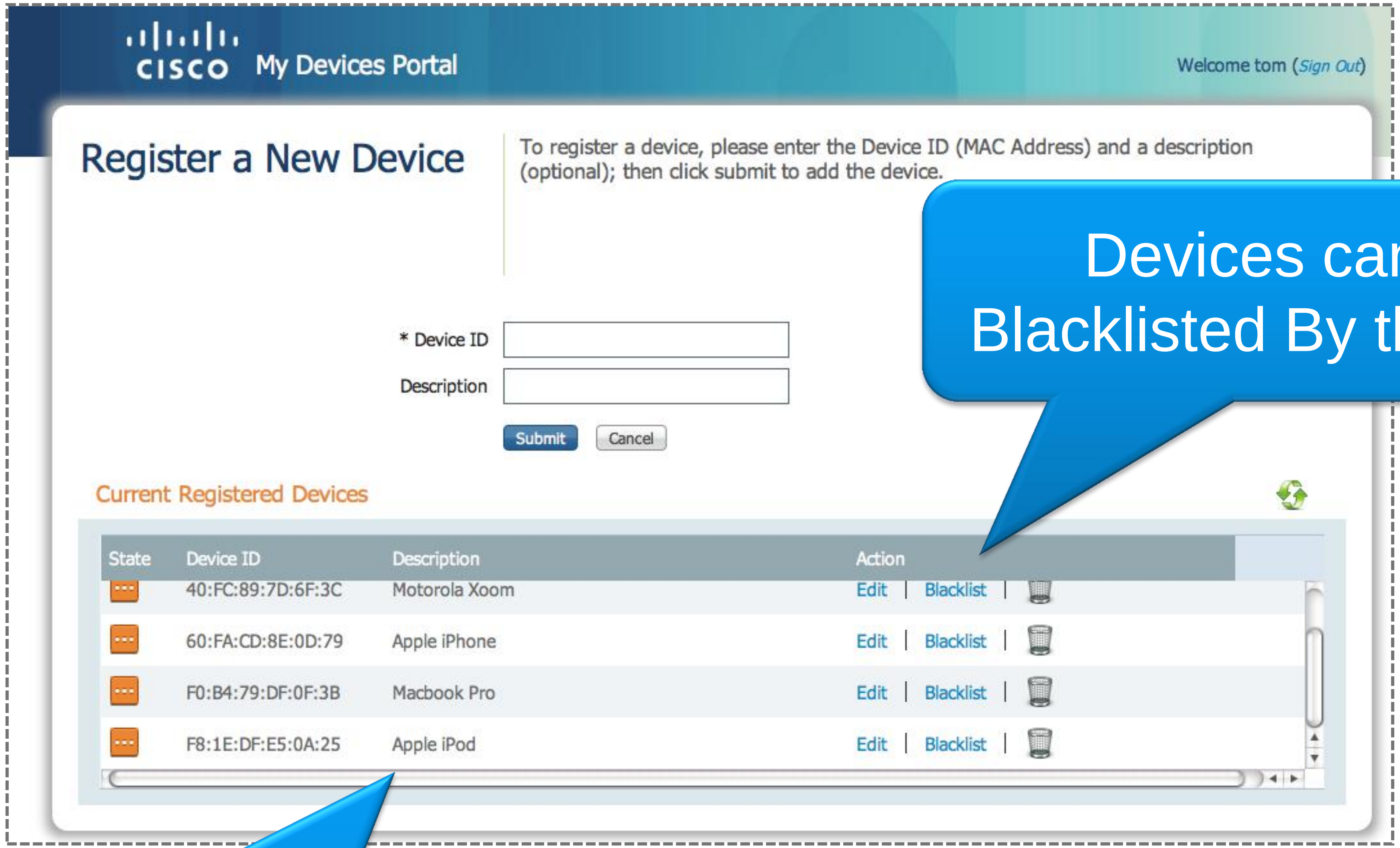
Change of Authorisation

Future Connections Using EAP-TLS 4



“My Devices” Portal

Self-Registration and Self-Blacklisting of BYOD Devices



Register a New Device

To register a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

* Device ID

Description

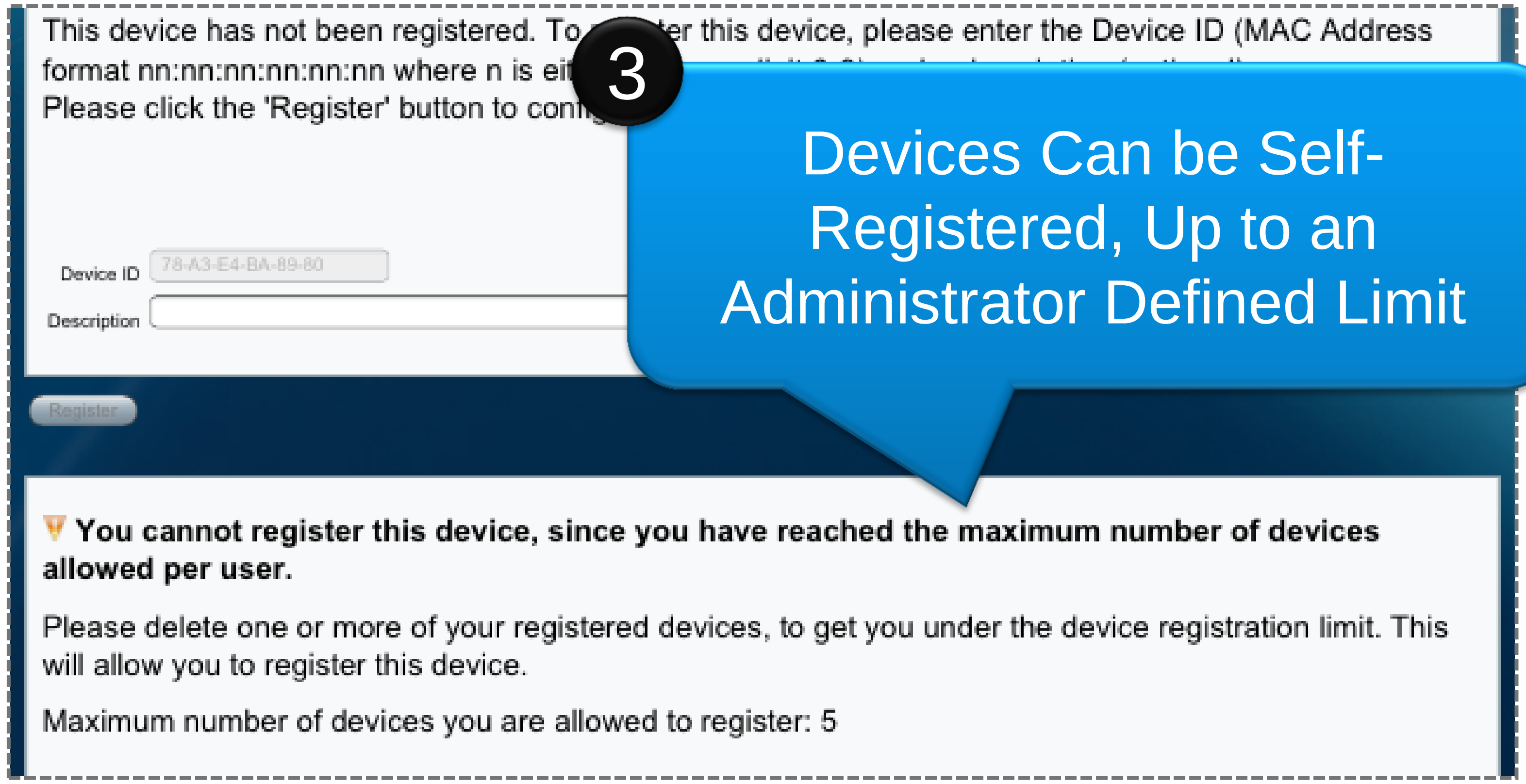
Submit Cancel

Current Registered Devices

State	Device ID	Description	Action
▭	40:FC:89:7D:6F:3C	Motorola Xoom	Edit | Blacklist | 🗑
▭	60:FA:CD:8E:0D:79	Apple iPhone	Edit | Blacklist | 🗑
▭	F0:B4:79:DF:0F:3B	Macbook Pro	Edit | Blacklist | 🗑
▭	F8:1E:DF:E5:0A:25	Apple iPod	Edit | Blacklist | 🗑

2 Devices can be Blacklisted By the User.

1 New Devices Can be Added with a Description



This device has not been registered. To [re]gister this device, please enter the Device ID (MAC Address format nn:nn:nn:nn:nn:nn where n is ei[ther]

Please click the 'Register' button to con[firm]

Device ID 78-A3-E4-BA-89-80

Description

Register

You cannot register this device, since you have reached the maximum number of devices allowed per user.

Please delete one or more of your registered devices, to get you under the device registration limit. This will allow you to register this device.

Maximum number of devices you are allowed to register: 5

3 Devices Can be Self-Registered, Up to an Administrator Defined Limit

Steps for Configuring Device Provisioning

1. Configure Integration with External CA Server

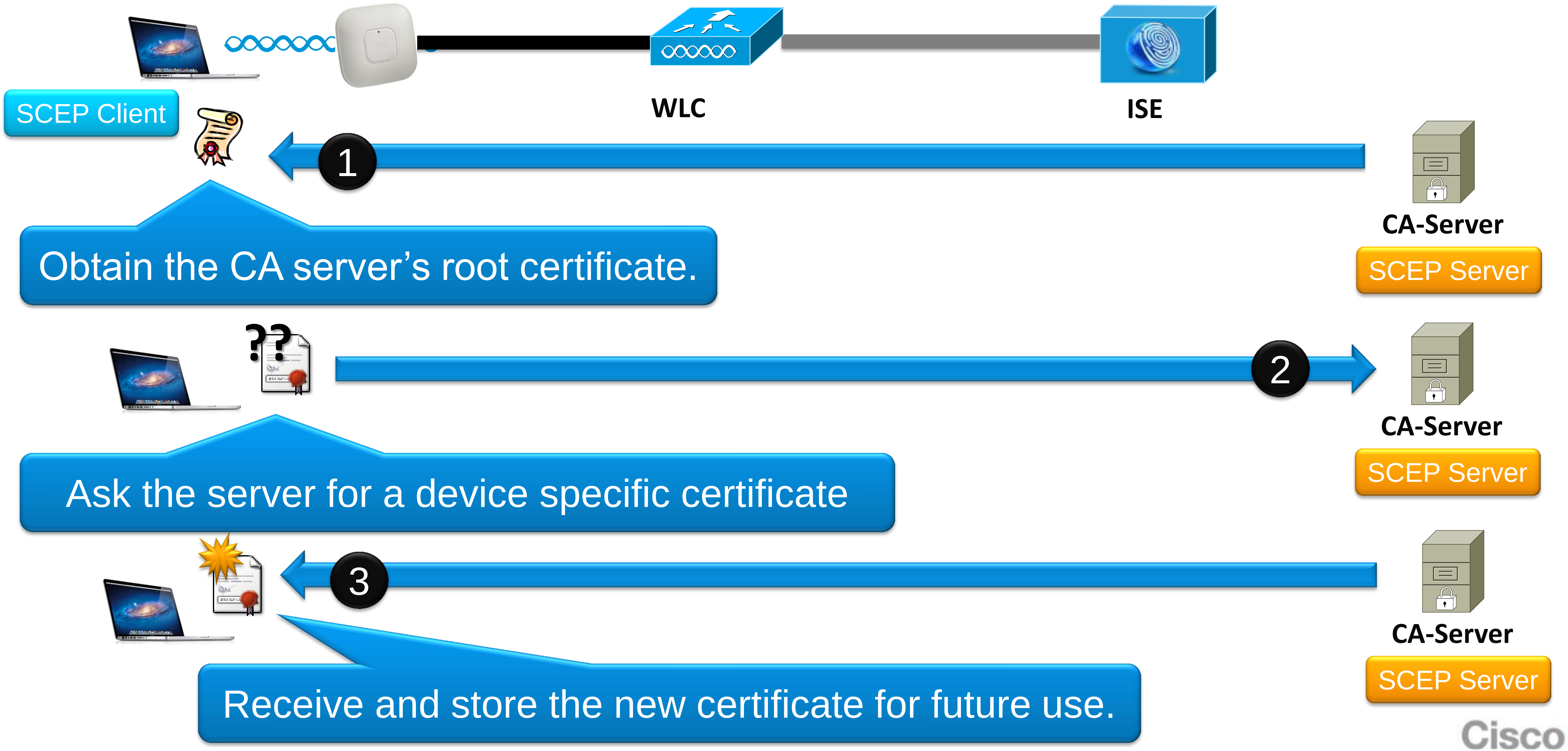
- Define SCEP URL and certificates

2. Define Supplicant Provisioning Profile

- Define what security and EAP type is deployed to end devices.

Certificate Provisioning Steps Using SCEP

Providing Certificates Using Simple and Secure Methods



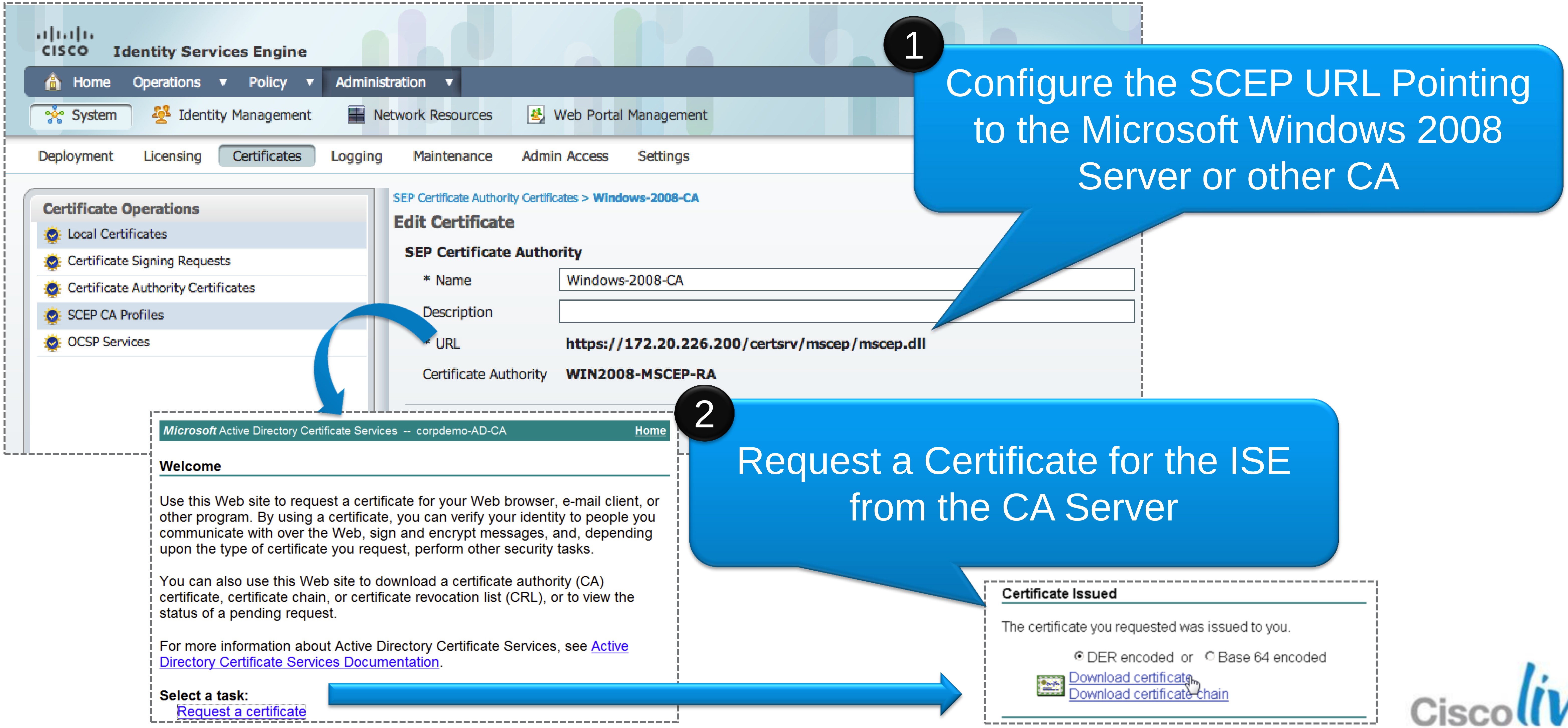
1. Obtain the CA server’s root certificate.

2. Ask the server for a device specific certificate

3. Receive and store the new certificate for future use.

Configuring SCEP Integration on the ISE

The ISE must point to the SCEP Server and have a valid certificate signed by the CA



Edit Certificate

SEP Certificate Authority

* Name: Windows-2008-CA

Description:

* URL: **https://172.20.226.200/certsrv/mscep/mscep.dll**

Certificate Authority: **WIN2008-MSCEP-RA**

1 Configure the SCEP URL Pointing to the Microsoft Windows 2008 Server or other CA

Microsoft Active Directory Certificate Services -- corpdemo-AD-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate

2 Request a Certificate for the ISE from the CA Server

Certificate Issued

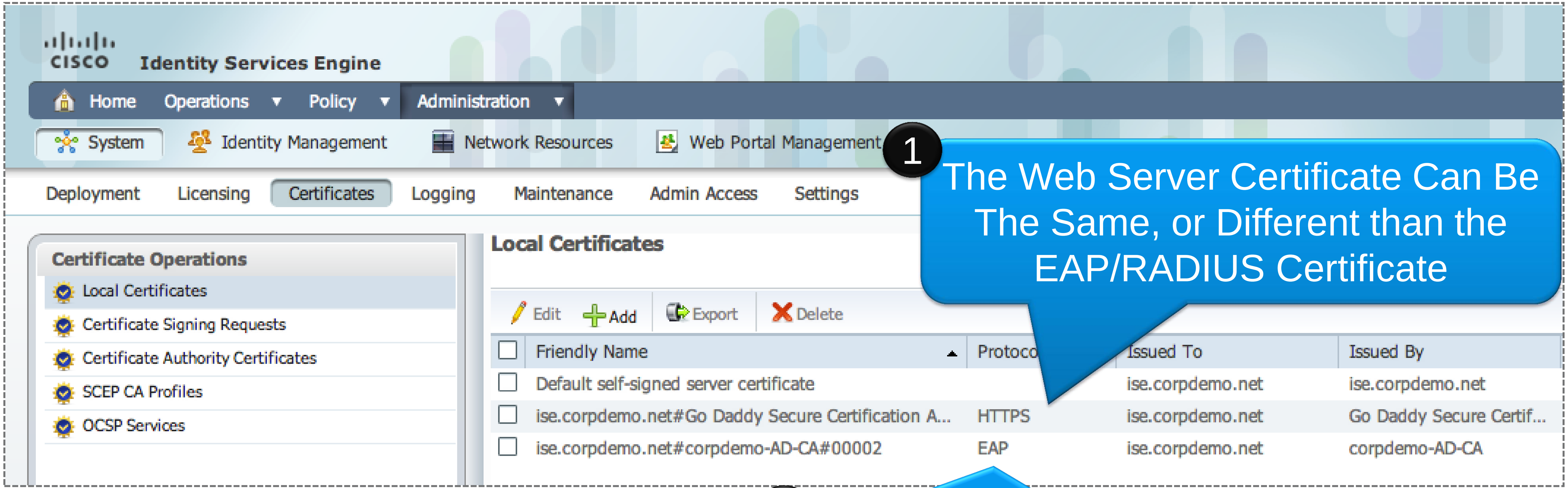
The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

Configuring Certificates on the ISE

Certificates are used for HTTPS and EAP Connections



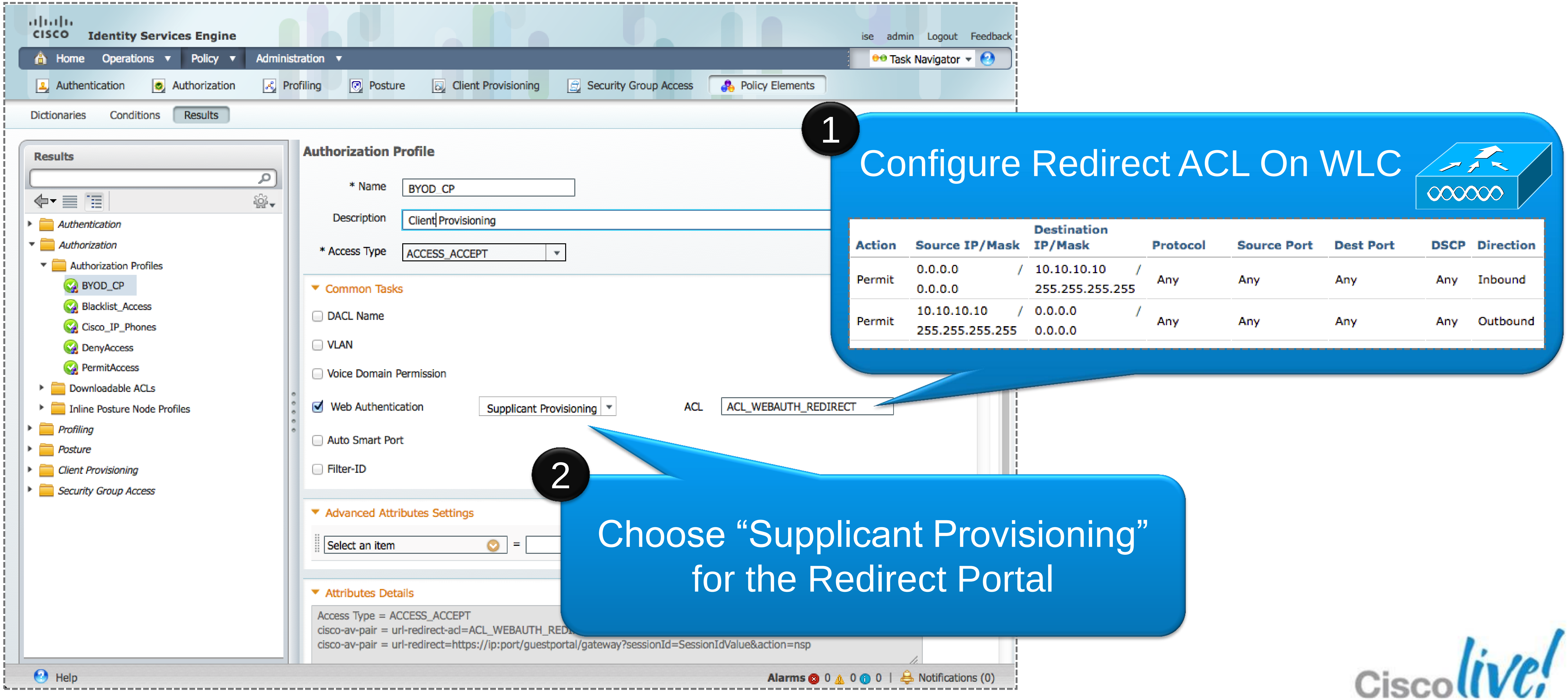
Local Certificates

□	Friendly Name	Protoco	Issued To	Issued By
□	Default self-signed server certificate		ise.corpdemo.net	ise.corpdemo.net
□	ise.corpdemo.net#Go Daddy Secure Certification A...	HTTPS	ise.corpdemo.net	Go Daddy Secure Certif...
□	ise.corpdemo.net#corpdemo-AD-CA#00002	EAP	ise.corpdemo.net	corpdemo-AD-CA

1 The Web Server Certificate Can Be The Same, or Different than the EAP/RADIUS Certificate

2 Use the Certificate from Your CA Server for EAP Authentication

Defining the Provisioning Authorisation Profile


Identity Services Engine
ise admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
BYOD_CP
Blacklist_Access
Cisco_IP_Phones
DenyAccess
PermitAccess
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Help
Alarms 0 0 0 Notifications (0)

Authorization Profile

* Name	BYOD_CP
Description	Client Provisioning
* Access Type	ACCESS_ACCEPT

Common Tasks

- □ DACL Name
- □ VLAN
- □ Voice Domain Permission
- ☑ Web Authentication: Supplicant Provisioning, ACL: ACL_WEBAUTH_REDIRECT
- □ Auto Smart Port
- □ Filter-ID

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL_WEBAUTH_RED
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp
```

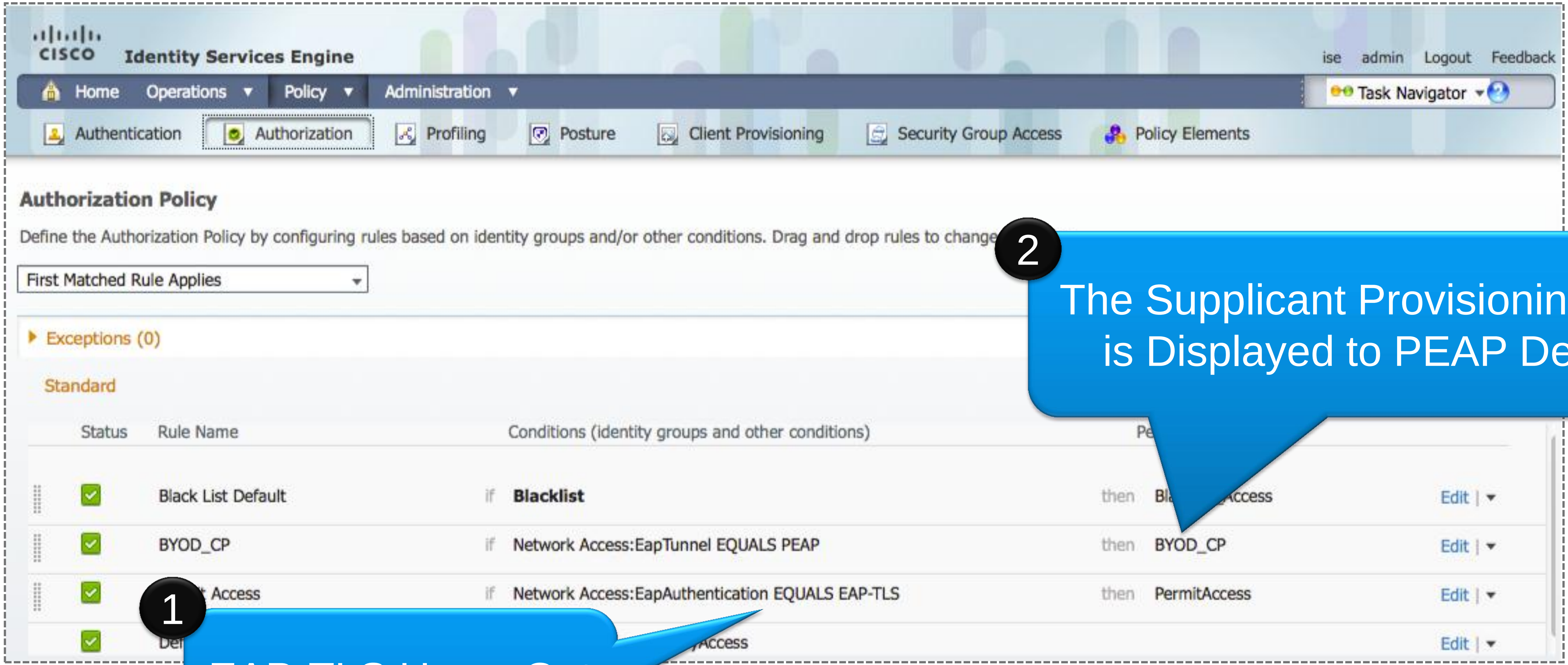
1 Configure Redirect ACL On WLC

Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
Permit	0.0.0.0 / 0.0.0.0	10.10.10.10 / 255.255.255.255	Any	Any	Any	Any	Inbound
Permit	10.10.10.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound

2 Choose “Supplicant Provisioning” for the Redirect Portal

Authorisation Rule for Provisioning

Example Rule to force PEAP devices to Register.



Identity Services Engine
ise admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change

First Matched Rule Applies ▾

▸ Exceptions (0)

Standard

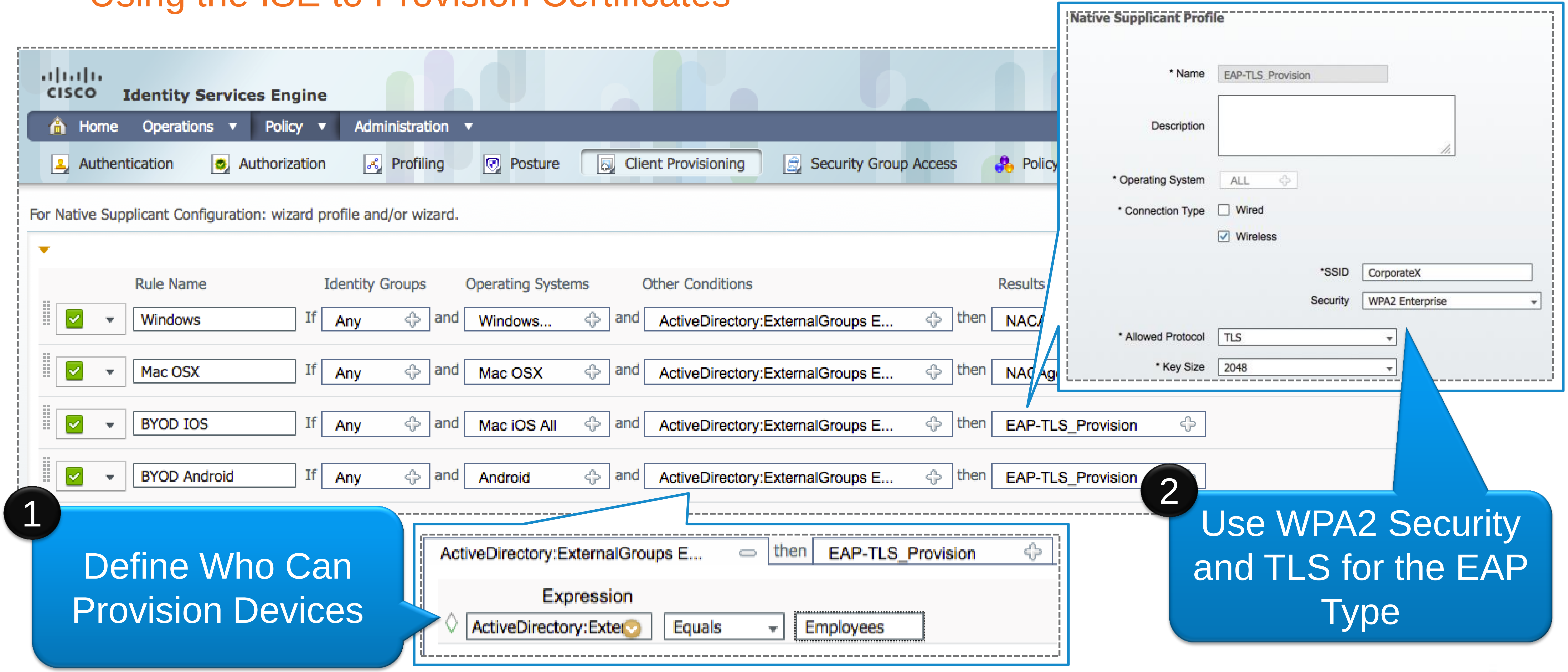
Status	Rule Name		Conditions (identity groups and other conditions)		Pe	
☑	Black List Default	if	**Blacklist**	then	Bl Access	Edit | ▾
☑	BYOD_CP	if	Network Access:EapTunnel EQUALS PEAP	then	BYOD_CP	Edit | ▾
☑	t Access	if	Network Access:EapAuthentication EQUALS EAP-TLS	then	PermitAccess	Edit | ▾
☑	De				Access	Edit | ▾

2 The Supplicant Provisioning Portal is Displayed to PEAP Devices

1 EAP-TLS Users Get Full Access

Supplicant Provisioning Config: EAP-TLS

Using the ISE to Provision Certificates



For Native Supplicant Configuration: wizard profile and/or wizard.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	Windows	If	Any	and	Windows...	and	ActiveDirectory:ExternalGroups E...	then	NAC/
☑	Mac OSX	If	Any	and	Mac OSX	and	ActiveDirectory:ExternalGroups E...	then	NAC Ag
☑	BYOD IOS	If	Any	and	Mac iOS All	and	ActiveDirectory:ExternalGroups E...	then	EAP-TLS_Provision
☑	BYOD Android	If	Any	and	Android	and	ActiveDirectory:ExternalGroups E...	then	EAP-TLS_Provision

Native Supplicant Profile

* Name	EAP-TLS_Provision
Description	
* Operating System	ALL
* Connection Type	□ Wired ☑ Wireless
*SSID	CorporateX
Security	WPA2 Enterprise
* Allowed Protocol	TLS
* Key Size	2048

ActiveDirectory:ExternalGroups E... then EAP-TLS_Provision

Expression

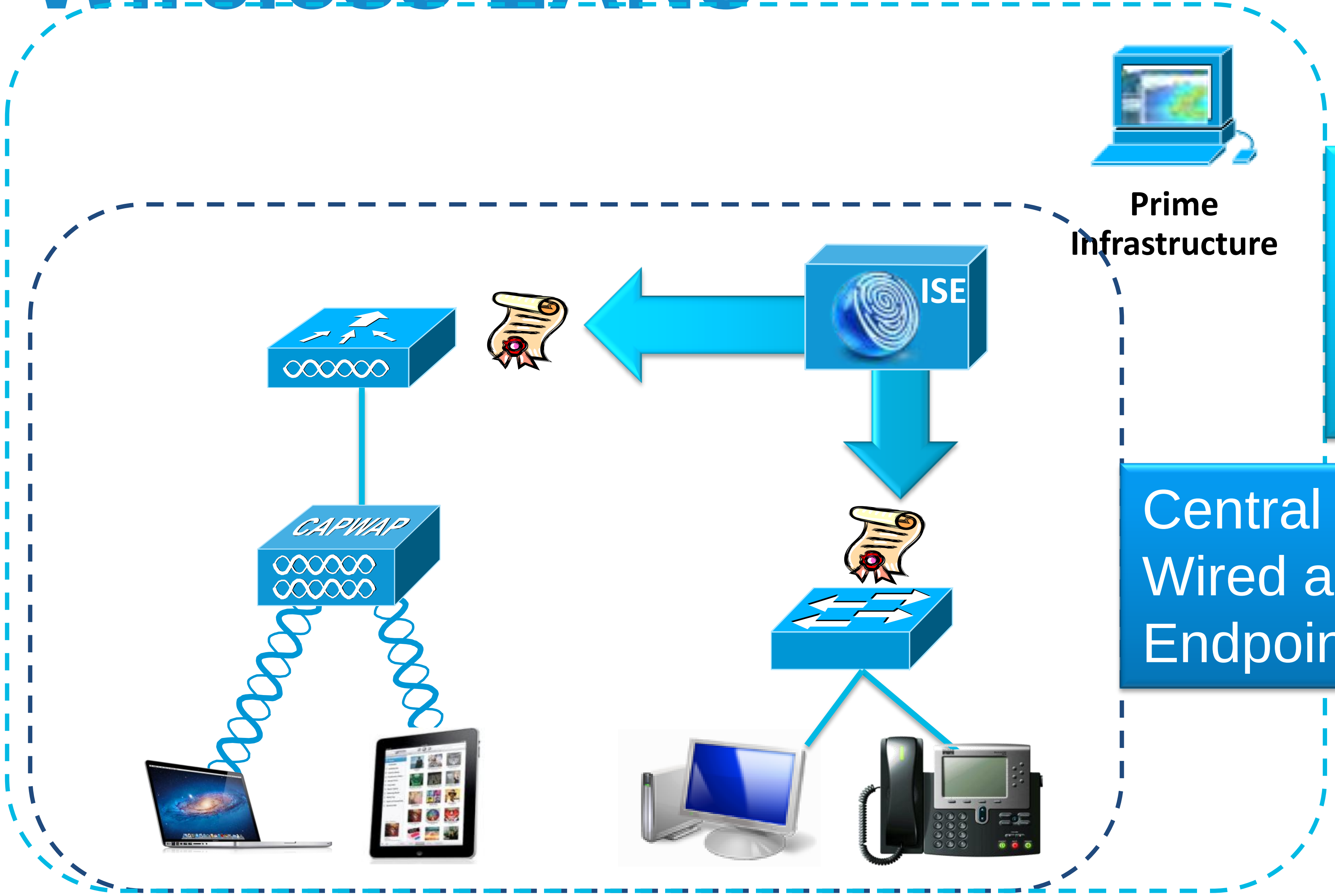
ActiveDirectory:Exter | Equals | Employees

1 Define Who Can Provision Devices

2 Use WPA2 Security and TLS for the EAP Type

BYOD Monitoring and Reporting

Cisco ISE Provides Policy for Wired and Wireless LANs



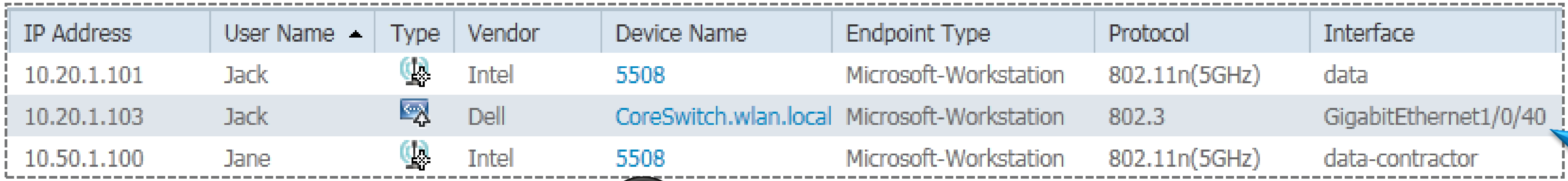
Centralised Monitoring of Wired and Wireless Networking, Users and Endpoints

Central Point of Policy for Wired and Wireless Users and Endpoints

- Unified wired and wireless policy (ISE) and management (PI).

Client Type and Policy Visibility

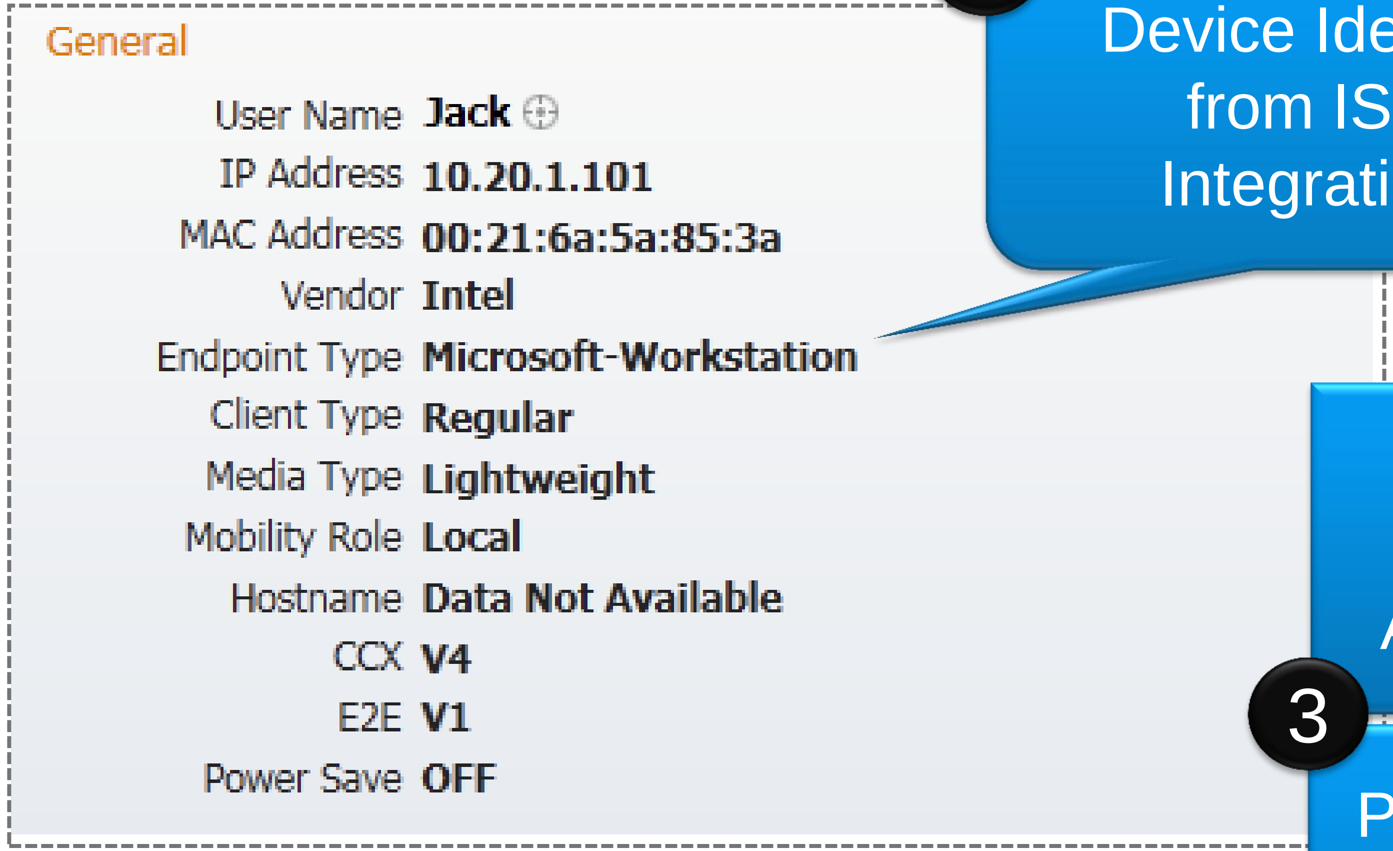
Endpoint Identity is Shared Between ISE and Prime Infrastructure



IP Address	User Name ▲	Type	Vendor	Device Name	Endpoint Type	Protocol	Interface
10.20.1.101	Jack		Intel	5508	Microsoft-Workstation	802.11n(5GHz)	data
10.20.1.103	Jack		Dell	CoreSwitch.wlan.local	Microsoft-Workstation	802.3	GigabitEthernet1/0/40
10.50.1.100	Jane		Intel	5508	Microsoft-Workstation	802.11n(5GHz)	data-contractor

1 Both Wired + Wireless Clients in a Single List

2 Device Identity from ISE Integration

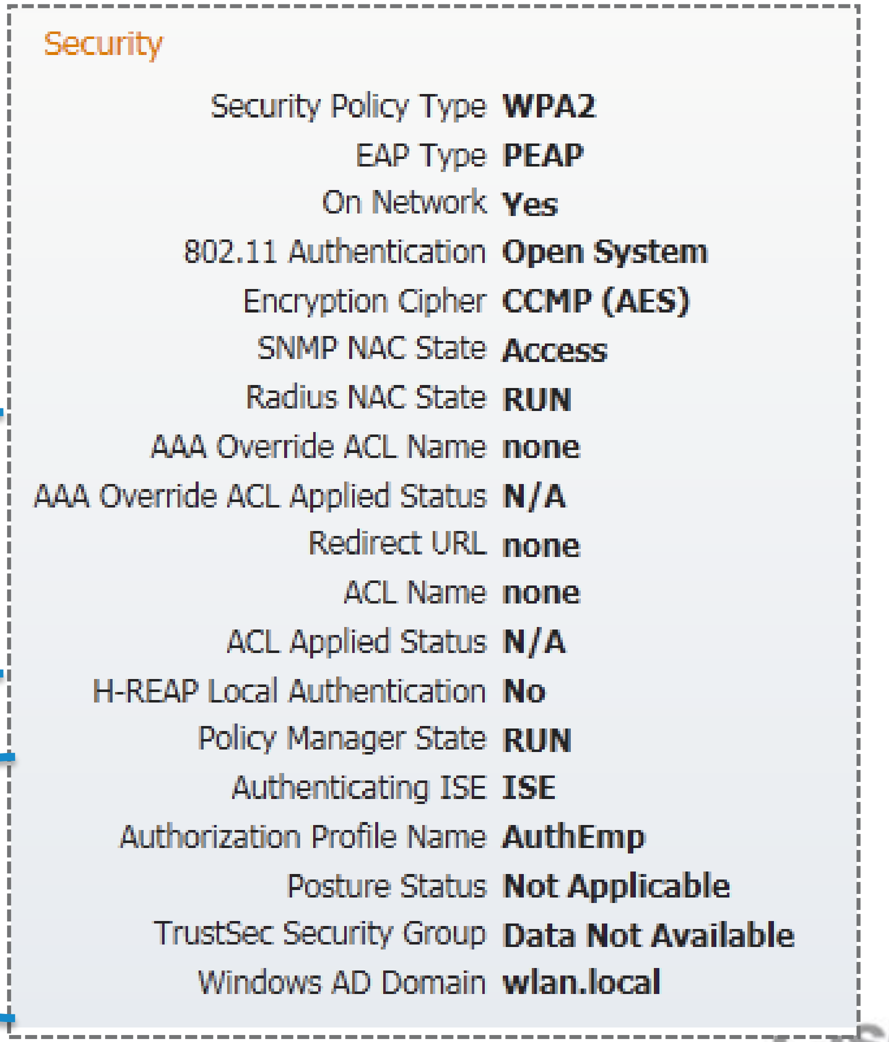


General

User Name	Jack
IP Address	10.20.1.101
MAC Address	00:21:6a:5a:85:3a
Vendor	Intel
Endpoint Type	Microsoft-Workstation
Client Type	Regular
Media Type	Lightweight
Mobility Role	Local
Hostname	Data Not Available
CCX	V4
E2E	V1
Power Save	OFF

AAA Override Parameters Applied to Client

3 Policy Information Including Windows AD Domain

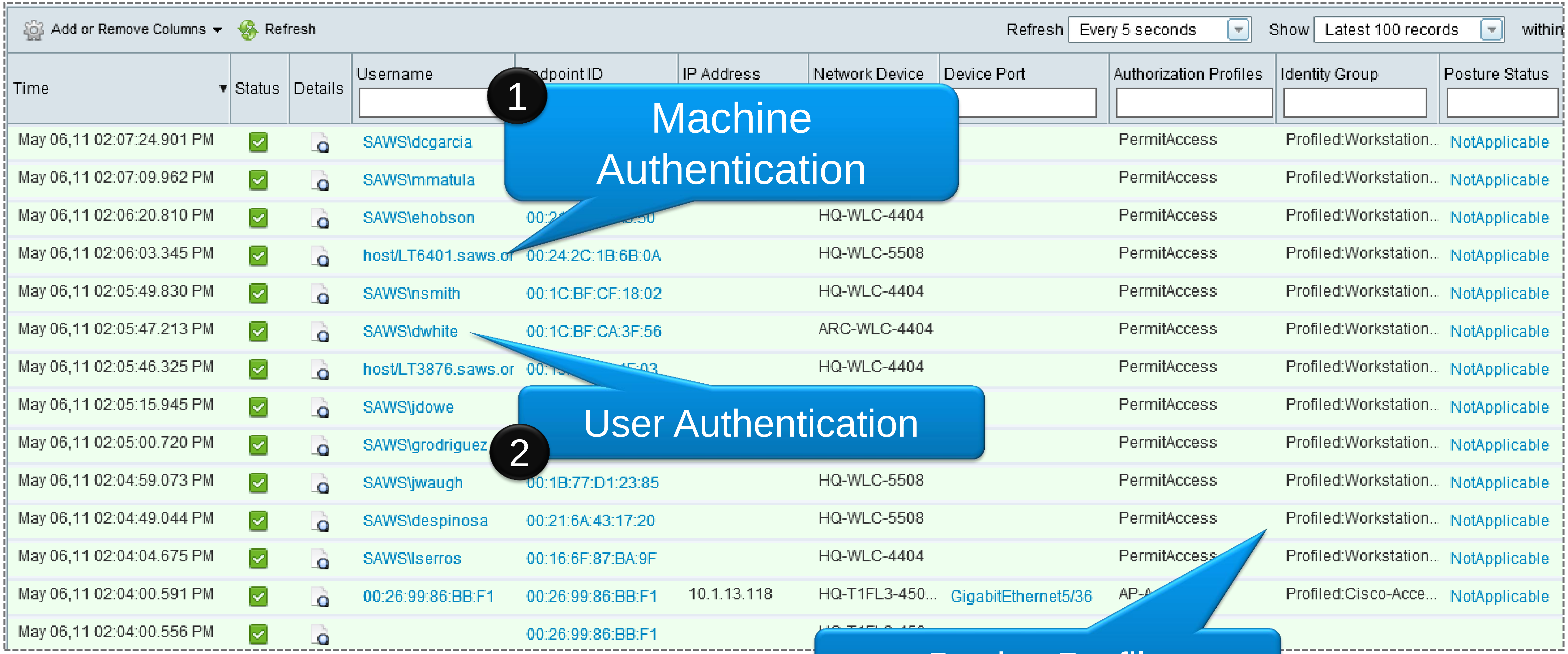


Security

Security Policy Type	WPA2
EAP Type	PEAP
On Network	Yes
802.11 Authentication	Open System
Encryption Cipher	CCMP (AES)
SNMP NAC State	Access
Radius NAC State	RUN
AAA Override ACL Name	none
AAA Override ACL Applied Status	N/A
Redirect URL	none
ACL Name	none
ACL Applied Status	N/A
H-REAP Local Authentication	No
Policy Manager State	RUN
Authenticating ISE	ISE
Authorization Profile Name	AuthEmp
Posture Status	Not Applicable
TrustSec Security Group	Data Not Available
Windows AD Domain	wlan.local

ISE Live Log

Providing instant troubleshooting of identity and policy.



Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status
May 06,11 02:07:24.901 PM	✓		SAWS\dcgarcia	[illegible]	[illegible]	[illegible]	[illegible]	PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:07:09.962 PM	✓		SAWS\mmatula	[illegible]	[illegible]	[illegible]	[illegible]	PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:06:20.810 PM	✓		SAWS\ehobson	00:2[illegible]B:50		HQ-WLC-4404		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:06:03.345 PM	✓		host/LT6401.saws.or	00:24:2C:1B:6B:0A		HQ-WLC-5508		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:05:49.830 PM	✓		SAWS\nsmith	00:1C:BF:CF:18:02		HQ-WLC-4404		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:05:47.213 PM	✓		SAWS\dwhite	00:1C:BF:CA:3F:56		ARC-WLC-4404		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:05:46.325 PM	✓		host/LT3876.saws.or	00:1[illegible]F:03		HQ-WLC-4404		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:05:15.945 PM	✓		SAWS\jdowe	[illegible]	[illegible]	[illegible]	[illegible]	PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:05:00.720 PM	✓		SAWS\grodriguez	[illegible]	[illegible]	[illegible]	[illegible]	PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:04:59.073 PM	✓		SAWS\jwaugh	00:1B:77:D1:23:85		HQ-WLC-5508		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:04:49.044 PM	✓		SAWS\despinosa	00:21:6A:43:17:20		HQ-WLC-5508		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:04:04.675 PM	✓		SAWS\lserros	00:16:6F:87:BA:9F		HQ-WLC-4404		PermitAccess	Profiled:Workstation..	NotApplicable
May 06,11 02:04:00.591 PM	✓		00:26:99:86:BB:F1	00:26:99:86:BB:F1	10.1.13.118	HQ-T1FL3-450...	GigabitEthernet5/36	AP-[illegible]	Profiled:Cisco-Acce...	NotApplicable
May 06,11 02:04:00.556 PM	✓			00:26:99:86:BB:F1		[illegible]				

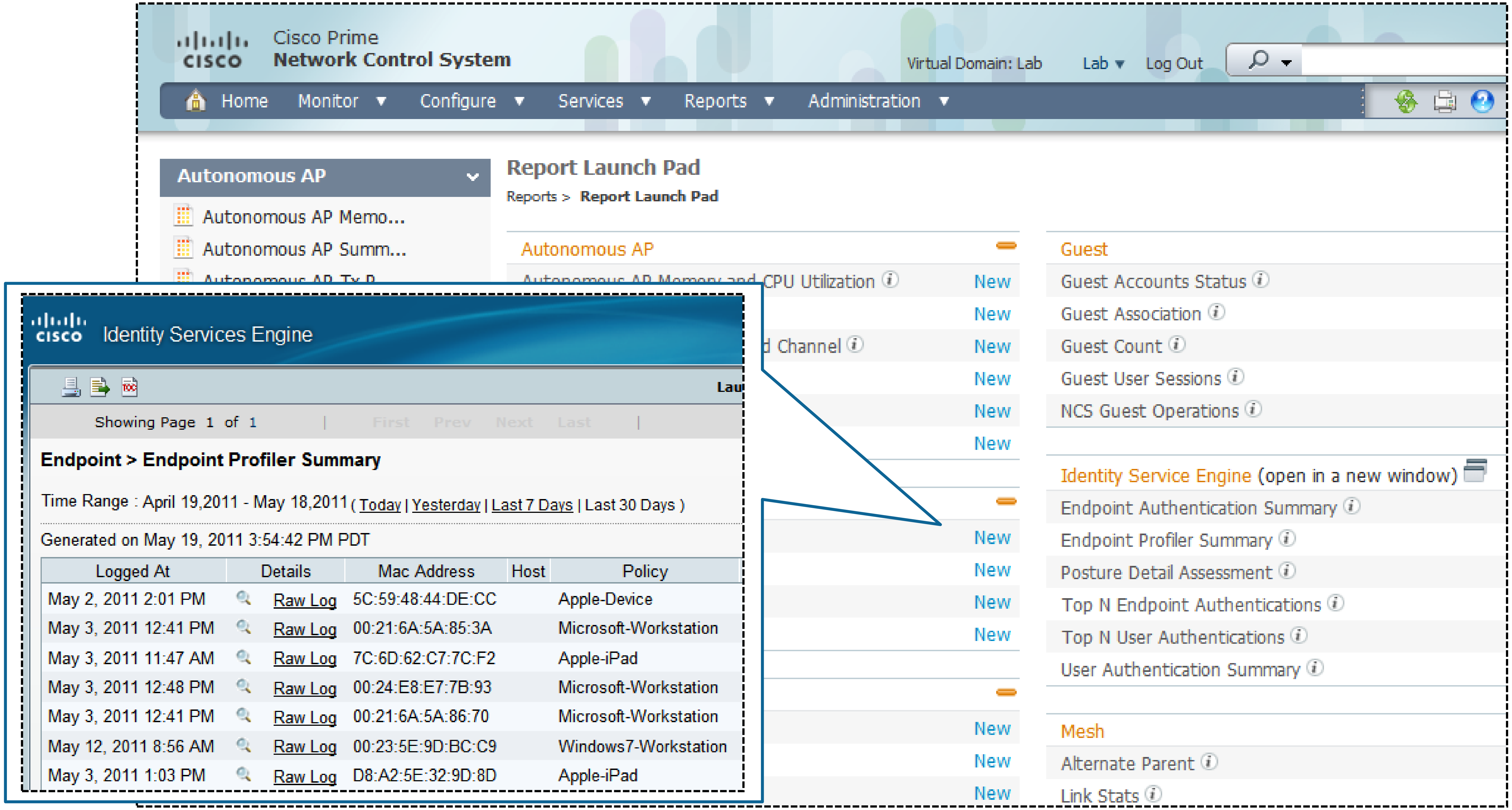
1 Machine Authentication

2 User Authentication

3 Device Profile

Prime Infrastructure Reporting

Cross-linking to ISE Reports on Profiling



Report Launch Pad

Reports > **Report Launch Pad**

Autonomous AP	
Autonomous AP Memory and CPU Utilization	New
	New
...d Channel	New
	New
	New
	New
	New
	New
	New
	New
	New
	New
	New

Guest

- Guest Accounts Status
- Guest Association
- Guest Count
- Guest User Sessions
- NCS Guest Operations

Identity Service Engine (open in a new window)

- Endpoint Authentication Summary
- Endpoint Profiler Summary
- Posture Detail Assessment
- Top N Endpoint Authentications
- Top N User Authentications
- User Authentication Summary

Mesh

- Alternate Parent
- Link Stats

Endpoint > Endpoint Profiler Summary

Time Range : April 19,2011 - May 18,2011 (Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on May 19, 2011 3:54:42 PM PDT

Logged At	Details	Mac Address	Host	Policy
May 2, 2011 2:01 PM	Raw Log	5C:59:48:44:DE:CC		Apple-Device
May 3, 2011 12:41 PM	Raw Log	00:21:6A:5A:85:3A		Microsoft-Workstation
May 3, 2011 11:47 AM	Raw Log	7C:6D:62:C7:7C:F2		Apple-iPad
May 3, 2011 12:48 PM	Raw Log	00:24:E8:E7:7B:93		Microsoft-Workstation
May 3, 2011 12:41 PM	Raw Log	00:21:6A:5A:86:70		Microsoft-Workstation
May 12, 2011 8:56 AM	Raw Log	00:23:5E:9D:BC:C9		Windows7-Workstation
May 3, 2011 1:03 PM	Raw Log	D8:A2:5E:32:9D:8D		Apple-iPad

Other Recommended Sessions for BYOD

Wireless Focus

- Design and Deployment of Enterprise WLANs
  - BRKEWN-2010, Wed 1:30pm
- Understanding RF Fundamentals and the Radio Design of Wireless Networks
  - BRKEWN-2017, Thur 2:00pm

Other Recommended Sessions for BYOD

Security Focus

- Demystifying Trustsec, Identity, NAC and ISE
  - BRKSEC-2022, Wed 1:30pm
- Advanced ISE and Secure Access Deployment
  - BRKSEC-3040, Fri 10:00am

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww