PART 3

Configuring the Infrastructure

CHAPTER 8

Summary of Configuring the Infrastructure

Revised: August 7, 2013

This part of the CVD section discusses the different infrastructure components that are critical to the deployment of the BYOD design and the configuration steps used for this design guide.

There are numerous ways to enable a BYOD solution based on the unique business requirements of a specific organization. While some organizations may take a more open approach and rely on basic authentication, other organizations will prefer more secure ways to identify, authenticate, and authorize devices. A robust network infrastructure with the capabilities to manage and enforce these policies is critical to a successful BYOD deployment

The following components and the configuration steps are discussed to support different BYOD use cases:

- Wireless Controllers (Unified and Converged Access)
- Access Layer Switches
- Identity Service Engine
- Certification Authority (CA) server
- Integration with Mobile Device Managers

This part of the CVD includes the following chapters:

- BYOD Wireless Infrastructure Design—This section presents different network designs used to support BYOD, including Campus and Branch designs. This section presents both Unified Wireless and Converged Access designs with single or dual SSID configurations.
- Identity Services Engine for BYOD—The Cisco Identity Services Engine plays a critical role in enabling the BYOD model and allows for enforcement of centrally-configured policies across wired and wireless networks. The section focuses on digital certificates, authentication and authorization policies, device profiling, and different ways to on-board devices with either single or dual SSID configurations.
- BYOD Wired Infrastructure Design—This section highlights how to on-board wired devices and how to enforce BYOD policies and network access for wired devices. This section has details for both campus and branch deployments.
- Security Group Access for BYOD—This section presents two different deployment scenarios that rely on Security Group Tags to enforce BYOD policies. These scenarios are not mutually exclusive and may be used together to implement different business use cases.

- Mobile Device Manager Integration for BYOD—This section focuses on how to configure ISE to integrate with third party MDM products through an XML-based API. BYOD Advanced Use Case—Mobile Device Manager Integration expands this configuration to receive device posture information from the MDM.

CHAPTER 9

BYOD Wireless Infrastructure Design

Revised: August 7, 2013

The Cisco Wireless LAN Controller (WLC) is used to automate wireless configuration and management functions and to provide visibility and control of the wireless networks. The WLC is able to interact with the Identity Service Engine to enforce authentication and authorization policies across endpoints.

While designing WLAN networks, the following should be considered:

- The role of the WLAN
- The authentication mechanism for the WLAN
- The number of WLANs present in a network

This design guide logically separates the WLAN into distinct logical functions: device provisioning and secure network access. These two functions can be provided by two different WLANs or combined into a single WLAN. This design guide covers both single and dual SSID deployment models for both the branch and the campus locations. Note that in this design guide wireless guest access is implemented on a different WLAN.

Some considerations when selecting a single versus dual SSID configuration:

- Some organizations prefer having a dedicated SSID for on-boarding devices.
- Others see dual SSID as an extra management burden.
- A second SSID adds channel overhead.
- Enabling too many SSIDs may degrade wireless performance.

The organization's unique requirements and preferences will dictate which model to deploy. The configurations of both the ISE and WLC may be easily modified to support either single or dual SSID deployments.

Campus—Unified Wireless LAN Design

As mentioned in Centralized (Local Mode) Wireless Design in Chapter 5, "Campus and Branch Network Design for BYOD," the two wireless LAN designs for the campus which are discussed within this design guide are Centralized (Local Mode) and Converged Access designs. Clients connecting from the campus wireless infrastructure are served by a dedicated cluster of CT5508 Unified Controllers configured in local mode (central switching) or served by a combination of Catalyst 3850 series switches which provide the Mobility Agent (MA) function, while CT5760 wireless controllers provide the Mobility

Controller function. This section discusses the Unified Wireless LAN Design, while discussion on Converged Access follows. The wireless controllers are configured with the proper SSIDs to provide device on-boarding and secure access. This functionality may be provided via single or dual SSIDs.

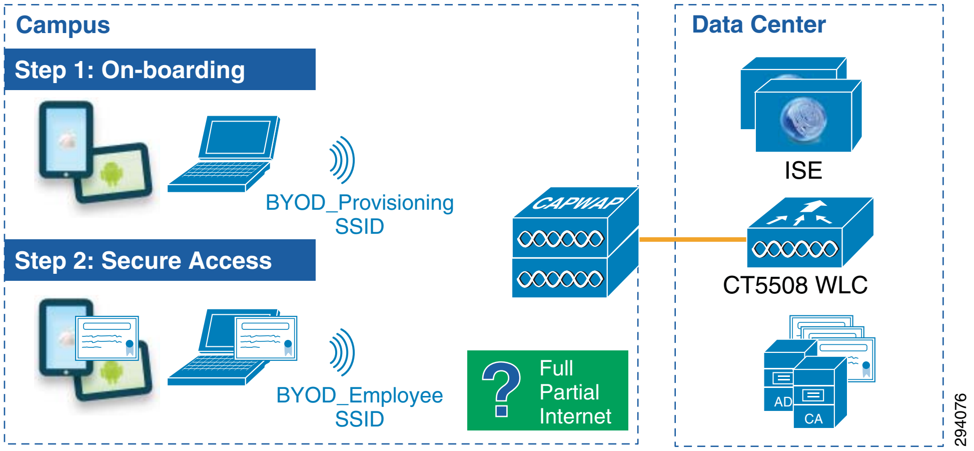
Note The CT5760 wireless controller can also be configured to function as a centralized (Local Mode) wireless controller. As discussed in Campus Migration Path of Chapter 5, "Campus and Branch Network Design for BYOD," this may be a necessary step in migrating from an existing wireless overlay design to a converged access design.

Centralized Campus—Dual SSID Design

In this design there are two SSIDs: one provides enrollment/provisioning and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides network access over a secure EAP-TLS connection.

Figure 9-1 shows the dual SSID design for the campus APs.

Figure 9-1 Campus-Dual SSIDs



In a dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID. In this design guide, the provisioning SSID is configured to be open and its only purpose is to provide on-boarding services.
- After the device is provisioned, it is assumed that the user will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list that provides only access to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of the ACL_Provisioning_Redirect ACL are shown below.
- This design guide makes use of the following SSIDs: BYOD_Provisioning and BYOD_Employee.

The properties of these two SSIDs are highlighted in Table 9-1.

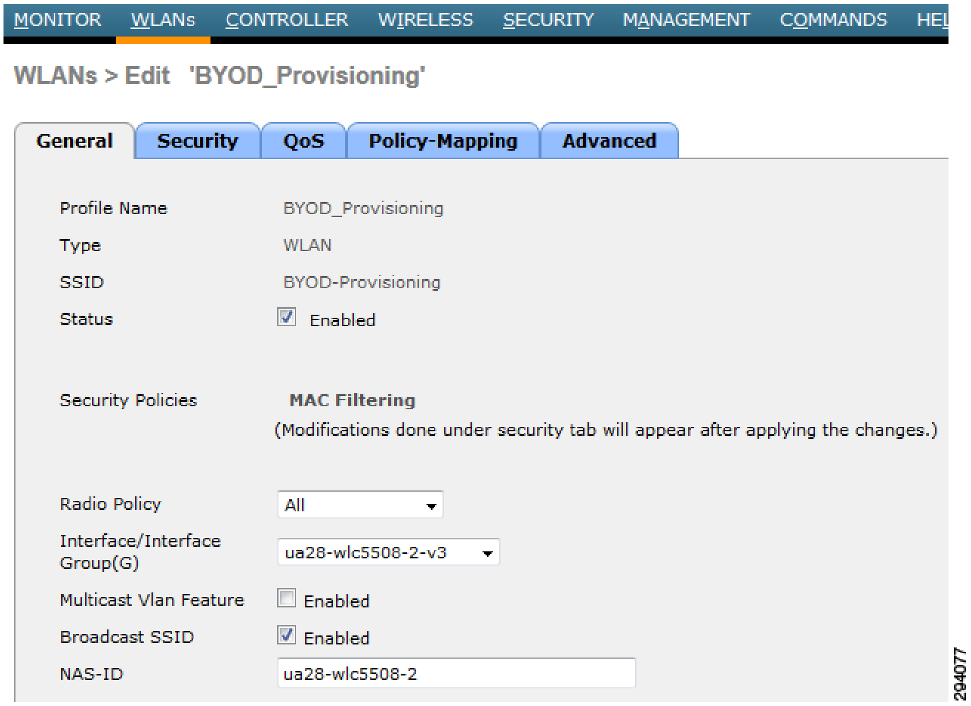
Table 9-1 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used only for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None (for Open SSID)	WPA+WPA2
MAC Filtering	Enabled (for Open SSID)	Disabled
WPA+WPA2 Parameters	None	WPA2 Policy, AES, 802.1X
Layer 3 Security	None	None
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State-RADIUS NAC	NAC State-RADIUS NAC
Quality of Service	Best Effort	Platinum
AVC	None	Enabled

To create a WLAN, click **WLANs > Create New > Go** and provide the SSID and profile details. Starting with Figure 9-2 the general configuration steps of the BYOD_Provisioning SSID are highlighted. The steps to configure the BYOD_Employee WLAN are similar, following the settings in Table 9-1.

Note When implementing BYOD solutions using more than one Wireless LAN Controller, WLAN IDs must be kept consistent. WLAN ID is used by ISE in determining which WLAN (SSID) clients are using to connect to the network. Ensuring each WLAN has the same WLAN ID on each WLC is essential for proper operation and security.

Figure 9-2 Creating the BYOD_Provisioning SSID



WLANs > Edit 'BYOD_Provisioning'

Profile Name BYOD_Provisioning

Type WLAN

SSID BYOD-Provisioning

Status ☑ Enabled

Security Policies **MAC Filtering**
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface/Interface Group(G) ua28-wlc5508-2-v3

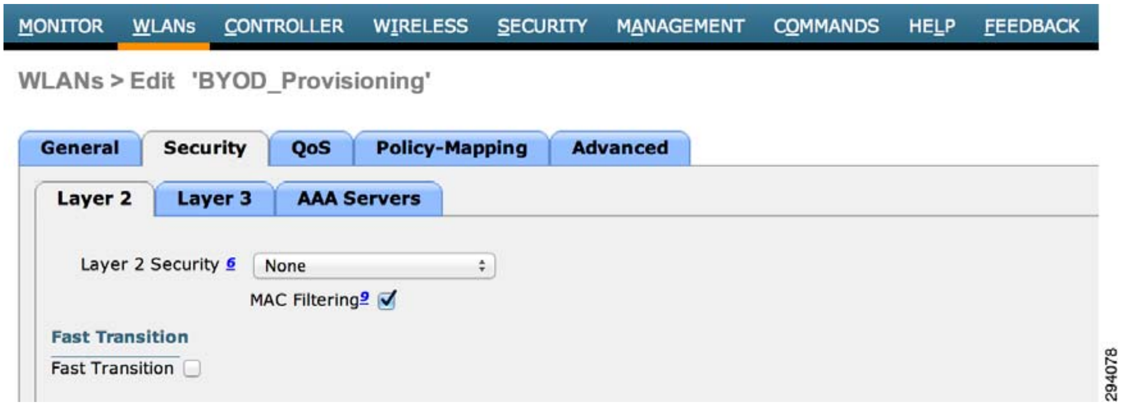
Multicast Vlan Feature □ Enabled

Broadcast SSID ☑ Enabled

NAS-ID ua28-wlc5508-2

The Layer 2 security settings are configured as **None** since BYOD_PROVISIONING is an open SSID. If the provisioning SSID has to be password-protected, then the Layer 2 security settings must be configured as WPA+WPA2 Enterprise.

Figure 9-3 Layer 2 Security Settings



WLANs > Edit 'BYOD_Provisioning'

Layer 2 Security 6 None

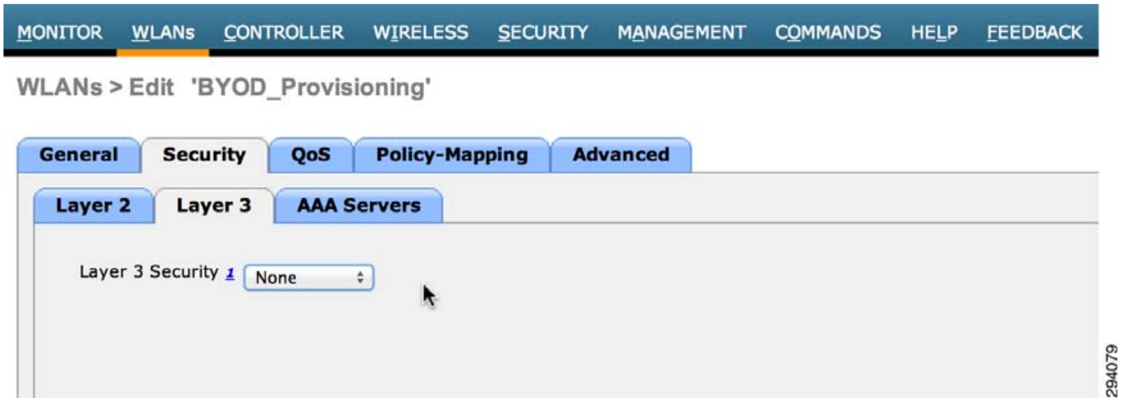
MAC Filtering9 ☑

Fast Transition

Fast Transition □

The Layer 3 Security is configured as **None**, as shown in Figure 9-4.

Figure 9-4 Layer 3 Security Settings

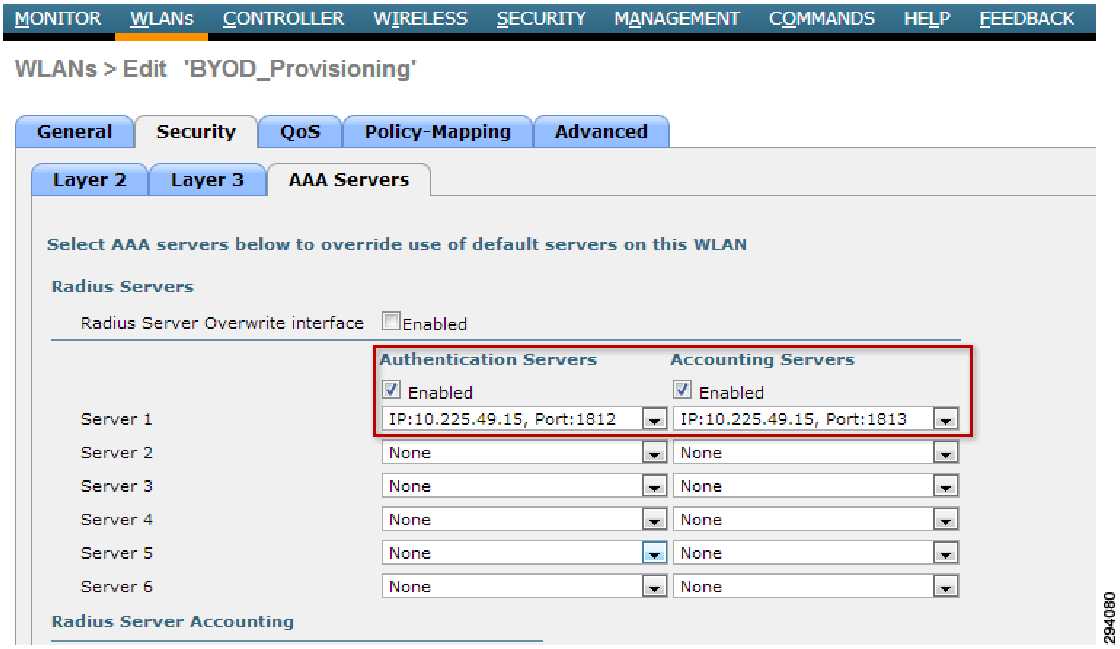


WLANs > Edit 'BYOD_Provisioning'

Layer 3 Security 1 None

The main configuration in the security settings is to specify the RADIUS server configuration details. Figure 9-5 shows how the ISE's IP address is configured for Authentication and Authorization.

Figure 9-5 AAA Security Settings



WLANs > Edit 'BYOD_Provisioning'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

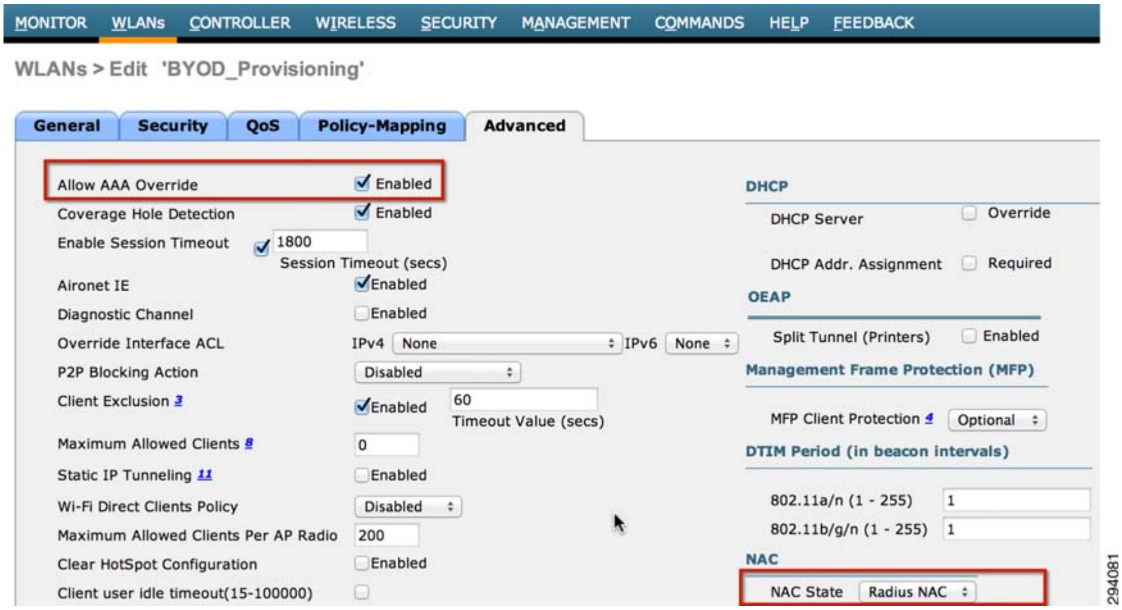
Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.225.49.15, Port:1812	IP:10.225.49.15, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Radius Server Accounting

Figure 9-6 shows the advanced settings, including AAA Override and NAC State.

Figure 9-6 Advanced Settings



WLANs > Edit 'BYOD_Provisioning'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
P2P Blocking Action Disabled
Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □ Enabled
Client user idle timeout(15-100000) □

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel (Printers) □ Enabled

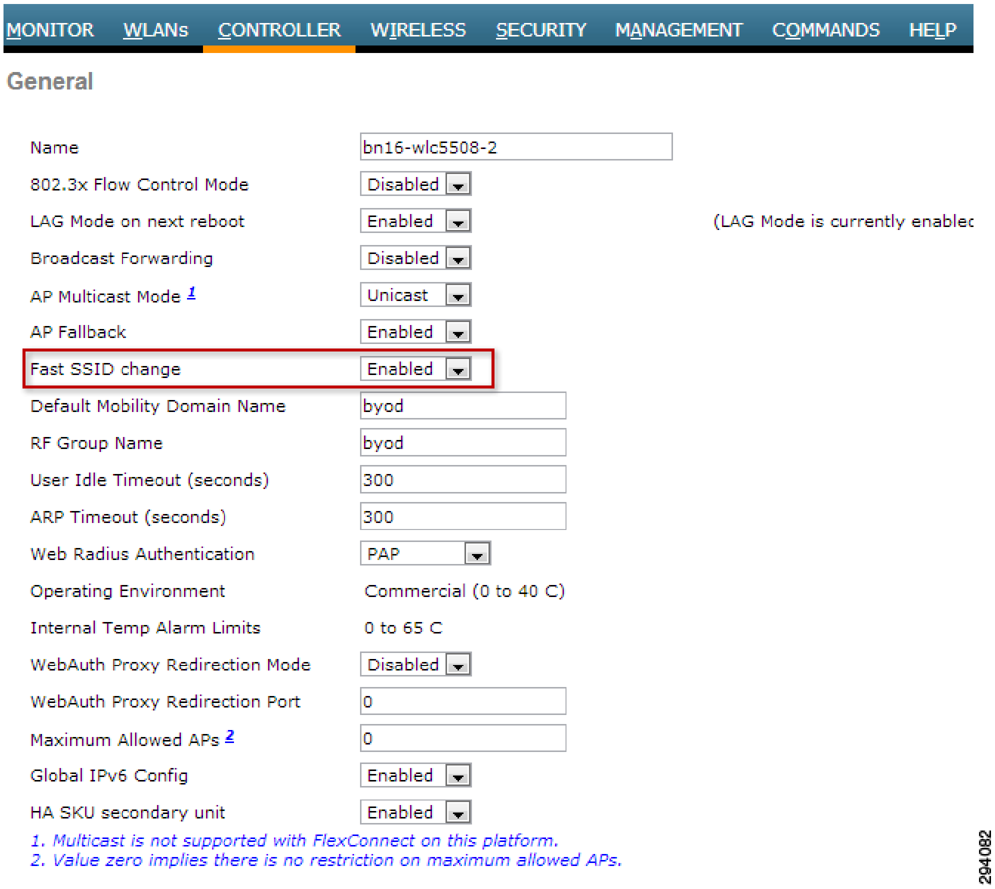
Management Frame Protection (MFP)
MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State Radius NAC

The Fast SSID Change feature is useful when a device needs to switch from one SSID to another. This applies to the dual SSID BYOD design. After the user completes registration with BYOD_Provisioning, the user is switched to BYOD_Employee SSID. By enabling the FAST SSID Change feature, the user switches immediately to the new SSID without experiencing delays. To enable Fast SSID Change, click **Controller > General > Fast SSID change**, as shown in Figure 9-7.

Figure 9-7 Fast SSID Change



General

Name	bn16-wlc5508-2
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled (LAG Mode is currently enablec
Broadcast Forwarding	Disabled
AP Multicast Mode [1]	Unicast
AP Fallback	Enabled
Fast SSID change	Enabled
Default Mobility Domain Name	byod
RF Group Name	byod
User Idle Timeout (seconds)	300
ARP Timeout (seconds)	300
Web Radius Authentication	PAP
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C
WebAuth Proxy Redirection Mode	Disabled
WebAuth Proxy Redirection Port	0
Maximum Allowed APs [2]	0
Global IPv6 Config	Enabled
HA SKU secondary unit	Enabled

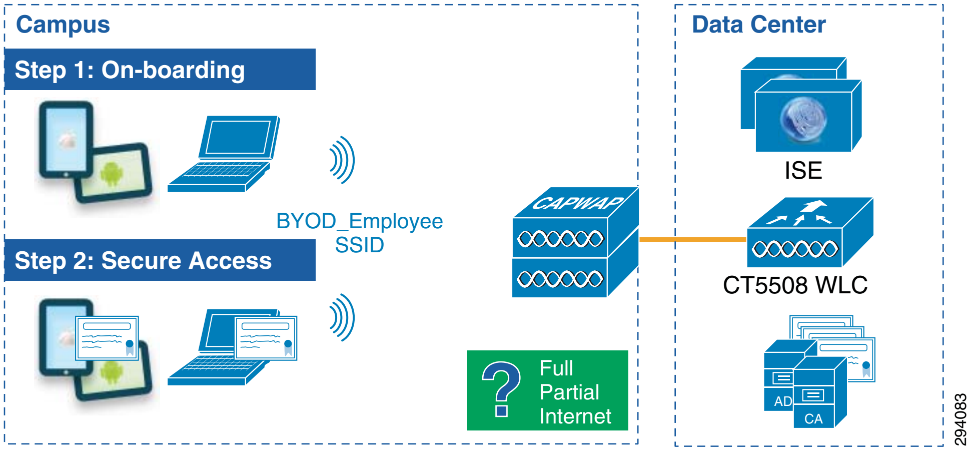
1. Multicast is not supported with FlexConnect on this platform.
2. Value zero implies there is no restriction on maximum allowed APs.

Note Authorization Policies and Profiles in Chapter 10, "Identity Services Engine for BYOD" shows the ACLs and authorization profiles used for dual and single SSID provisioning.

Centralized Campus—Single SSID Design

In a single SSID design the same WLAN (BYOD_Employee) is used for on-boarding and secure network access. Figure 9-8 shows how this design may be implemented using the 5508 Wireless LAN Controller. In this case, the controllers are dedicated to manage the APs in the campus.

Figure 9-8 Campus—Single SSID



Note [Authorization Policies and Profiles] in Chapter 10, "Identity Services Engine for BYOD" shows the ACLs and authorization profiles used for dual and single SSID provisioning.

Centralized Campus—Policy Enforcement using TrustSec

As discussed in ACL Complexity and Considerations in Chapter 5, "Campus and Branch Network Design for BYOD," past versions of the CVD utilized Named ACLs pre-configured on the wireless controllers to enforce role-based policies for access to network and Data Center resources. This CVD introduces a complimentary technology known as TrustSec and, more specifically, Security Group Access (SGA) to enforce role-based policies through the use of Security Group Tags (SGT) to control access to data center resources. This CVD discusses an approach to slowly migrate to the use of SGT as opposed to, or even in addition to, the use of ACLs through Network Device definitions created in ISE.

Branch—Unified Wireless LAN Design

FlexConnect Wireless LAN Design

In this design guide, endpoints connecting from branch locations are managed by a cluster of Flex 7500 Wireless LAN Controllers or Virtual Wireless LAN Controllers (vWLCs). The vWLC is software which can run on industry standard virtualization infrastructure and is more suitable for small- and medium-sized businesses.

The configuration parameters described in this section apply to both the vWLC and Flex 7500 controllers.

The following link provides more information on how to set up vWLCs using VMware: http://www.cisco.com/en/US/customer/products/ps12723/products_tech_note09186a0080bd2d04.shtml.

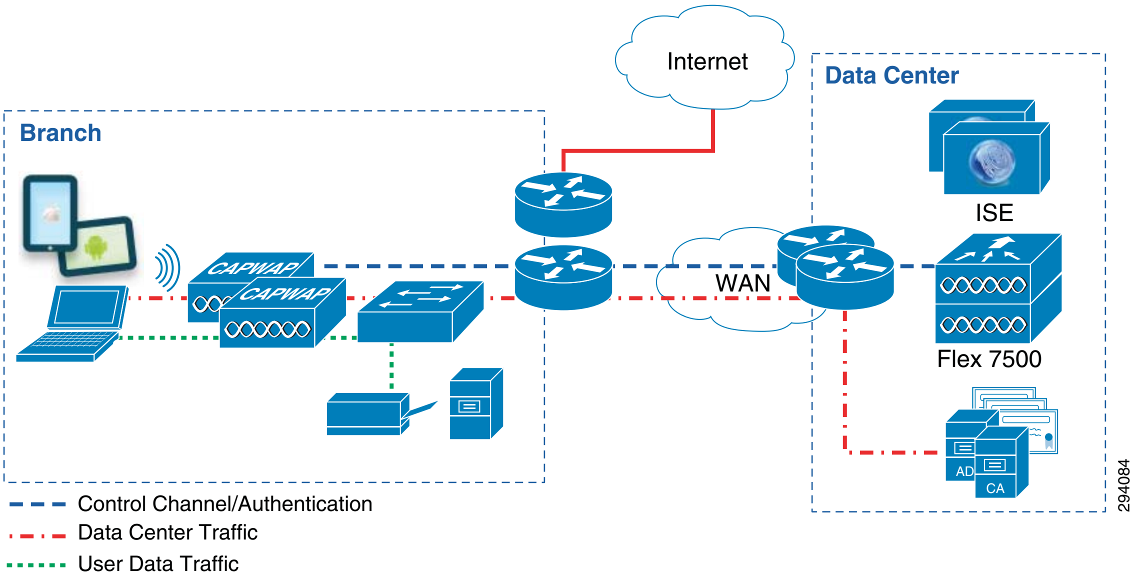
FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Distributing client data traffic using the FlexConnect architecture offers some advantages:

- A controller is not required at each branch location.
- Mobility resiliency within branch during WAN link failures.
- Central management and troubleshooting.

The FlexConnect architecture in Figure 9-9 shows different traffic flows originating at the branch.

Figure 9-9 FlexConnect Architecture



When an endpoint associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration.

With respect to data packet flows, the WLAN can be in any one of the following modes:

- Central switching—Central switched WLANs tunnel both the wireless user traffic and all control traffic to the centralized WLC, where the user traffic is mapped to a dynamic interface or VLAN.
- Local switching—In this mode the FlexConnect access point switches data packets locally by dropping all traffic locally at the wired interface. Wireless user traffic is mapped to discrete VLANs via 802.1Q trunking.

The Flex 7500 Wireless Branch Controller Deployment Guide offers more details: http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml.

The key strategy for providing differentiated access to users is done by assigning users to different VLANs dynamically. The AAA Override feature for FlexConnect assigns individual clients to specific VLANs, based on the returned RADIUS attributes from the ISE.

The access point must be preconfigured with all of the possible VLANs that can be returned by the ISE server. The VLAN assignment returned by the ISE as part of authorization is applied. If the VLAN that was returned from the ISE is not present on the AP, the client falls back to the default VLAN configured for the WLAN.

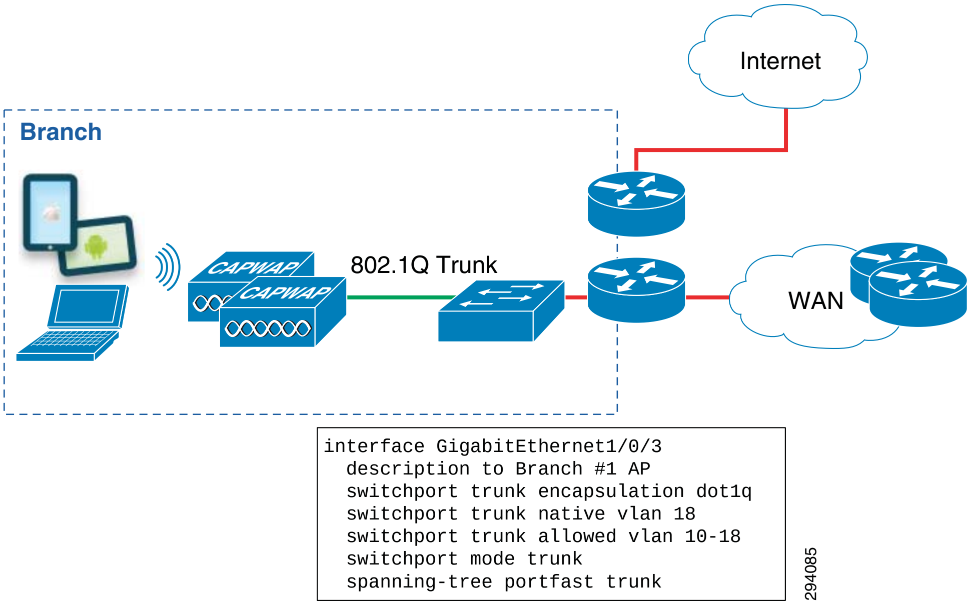
In this design three VLANs have been configured for wireless connectivity on the BYOD_Employee SSID. Table 9-2 illustrates those VLANs and their purpose.

Table 9-2 VLANs and Purpose

VLAN Number	VLAN Name	Description
10	Wireless_Full	Users assigned to this VLAN get full access to campus and branch servers.
11	Wireless_Partial	In addition to Internet access, users assigned to this VLAN access to additional campus and branch resources.
12	Wireless_Internet	Users assigned to this VLAN get only Internet access.
18	AP_Mgmt_Flex	This is the native VLAN that the user will initially be placed into, until the authorization policy determines the appropriate VLAN.

Since more than one VLAN is configured for local switching, FlexConnect APs at the branch must be connected to an 802.1Q trunk link. Both the AP and the upstream switchport need to be configured for 802.1Q trunking. Figure 9-10 shows an example configuration of the access layer switch that connects to the FlexConnect AP.

Figure 9-10 Trunk Configuration



```
interface GigabitEthernet1/0/3
  description to Branch #1 AP
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 18
  switchport trunk allowed vlan 10-18
  switchport mode trunk
  spanning-tree portfast trunk
```

Branch Wireless IP Address Design

Once the device has been dynamically assigned to a VLAN, the endpoint must obtain an IP address from a DHCP server. In the following example the branch router's Layer 3 subinterfaces are configured with the **ip-helper address** command, pointing to a DHCP server:

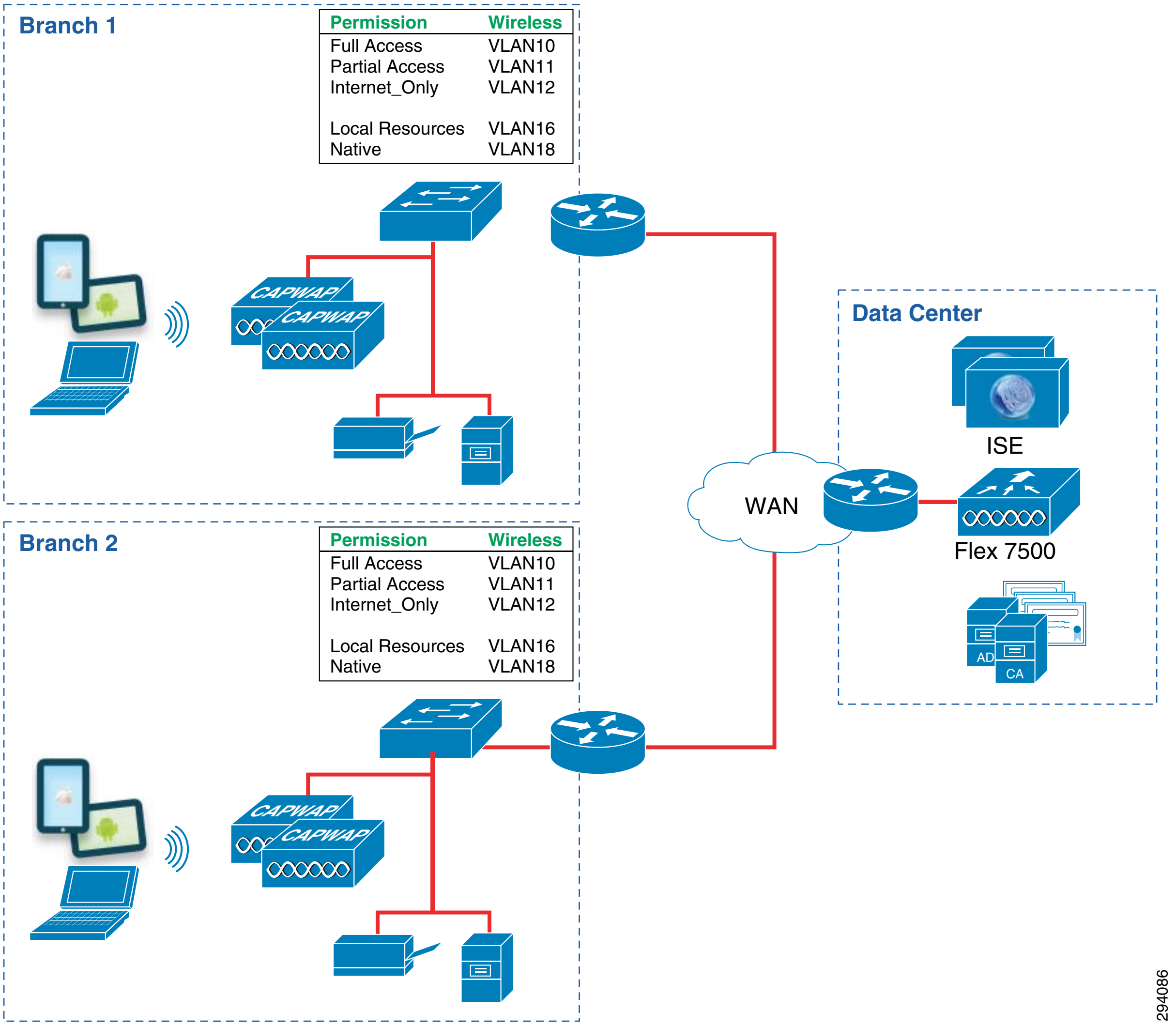
```
interface GigabitEthernet0/1
 description Trunk to branch bn22-3750x-1
 no ip address
 media-type sfp
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.200.10.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 10 ip 10.200.10.1
 standby 10 priority 110
 standby 10 preempt
!
interface GigabitEthernet0/1.11
 encapsulation dot1Q 11
 ip address 10.200.11.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 11 ip 10.200.11.1
 standby 11 priority 110
 standby 11 preempt
!
interface GigabitEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.200.12.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 12 ip 10.200.12.1
 standby 12 priority 110
 standby 12 preempt
```

The diagram in Figure 9-11 shows two branch locations utilizing resources from the data center and illustrates the following key points:

- At the branch, endpoints are placed in different VLANs based on the level of access to which they are entitled.
- The wireless infrastructure from the branches is managed by a single cluster of Flex 7500 controllers.
- Endpoints that get assigned to VLAN 10 are granted full access to network resources, VLAN 11 for partial access and VLAN 12 for Internet access.

Based on the matching authorization profile, a user is assigned to a specific VLAN where predefined permissions have been defined.

Figure 9-11 VLANs Used at the Branches



Permission	Wireless
Full Access	VLAN10
Partial Access	VLAN11
Internet_Only	VLAN12
Local Resources	VLAN16
Native	VLAN18

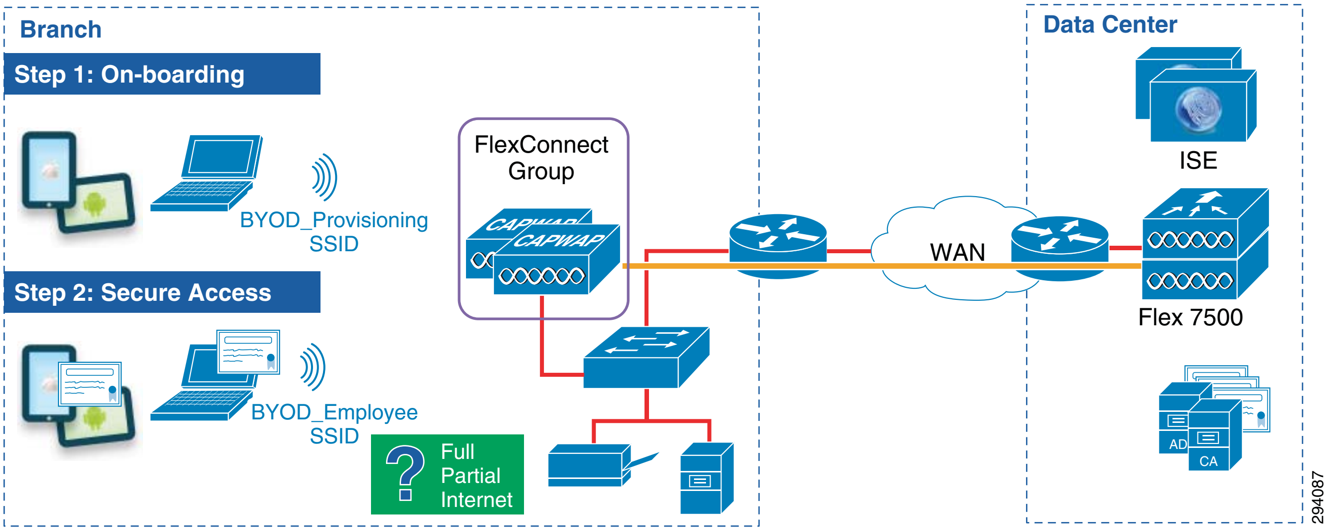
Permission	Wireless
Full Access	VLAN10
Partial Access	VLAN11
Internet_Only	VLAN12
Local Resources	VLAN16
Native	VLAN18

FlexConnect Branch—Dual SSID Design

In the Dual SSID design two SSIDs are configured: one SSID provides enrollment/provisioning while the other provides secure EAP-TLS access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides secure network access.

Figure 9-12 shows the dual SSID design for the branch APs.

Figure 9-12 Branch-Dual SSIDs



In a dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password-protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID.
- After the device is provisioned, the user connects via EAP-TLS to the BYOD_Employee SSID for network access. To prevent the user from remaining connected to the provisioning SSID, an access list that provides access only to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of this SSID are discussed in the Client Provisioning section.

Table 9-3 shows the WLAN parameters for the SSIDs used in this design guide.

Table 9-3 WLAN Parameters

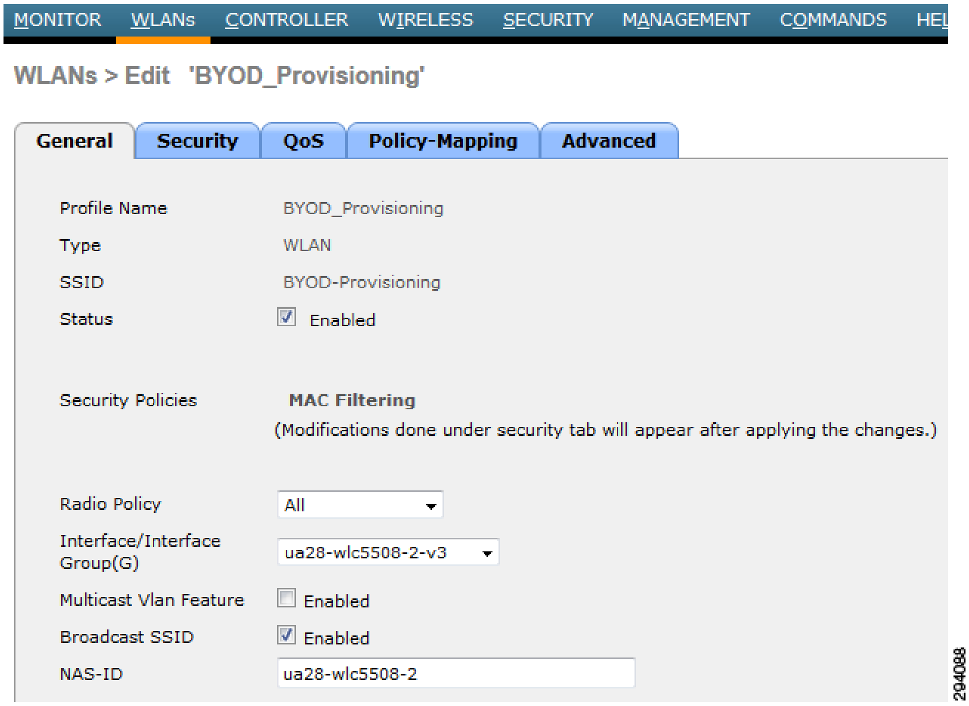
Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None (for Open SSID)	WPA+WPA2
MAC Filtering	Enabled (for Open SSID)	Disabled
WPA+WPA2 Parameters	None (for Open SSID)	WPA2 Policy, AES, 802.1X
Layer 3 Security	None	None
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State-RADIUS NAC	NAC State-RADIUS NAC
Advanced-FlexConnect Local Switching	Disabled for Central Switching Provisioning Enabled for Local Switching Provisioning	Enabled

Table 9-3 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Quality of Service	Best Effort	Platinum
AVC	Does Not Apply	Does Not Apply

To create a WLAN, click **WLANs > Create New > Go** and provide the SSID and profile details. Figure 9-13 shows the general configuration details of the BYOD_Provisioning SSID.

Figure 9-13 Creating the Branch BYOD_Provisioning SSID



WLANs > Edit 'BYOD_Provisioning'

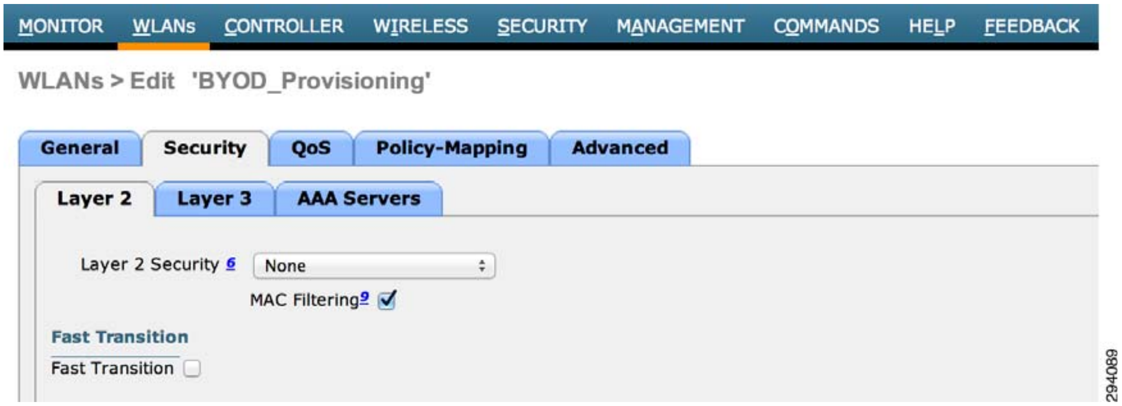
Profile Name BYOD_Provisioning
Type WLAN
SSID BYOD-Provisioning
Status ☑ Enabled

Security Policies **MAC Filtering**
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface/Interface Group(G) ua28-wlc5508-2-v3
Multicast Vlan Feature □ Enabled
Broadcast SSID ☑ Enabled
NAS-ID ua28-wlc5508-2

Since BYOD_Provisioning is an open SSID, the Layer 2 security settings in are configured as **None**. If the provisioning SSID had to be password-protected, the Layer 2 security settings would be configured as WPA+WPA2 Enterprise.

Figure 9-14 Layer 2 Security Settings



WLANs > Edit 'BYOD_Provisioning'

Layer 2 Security 6 None

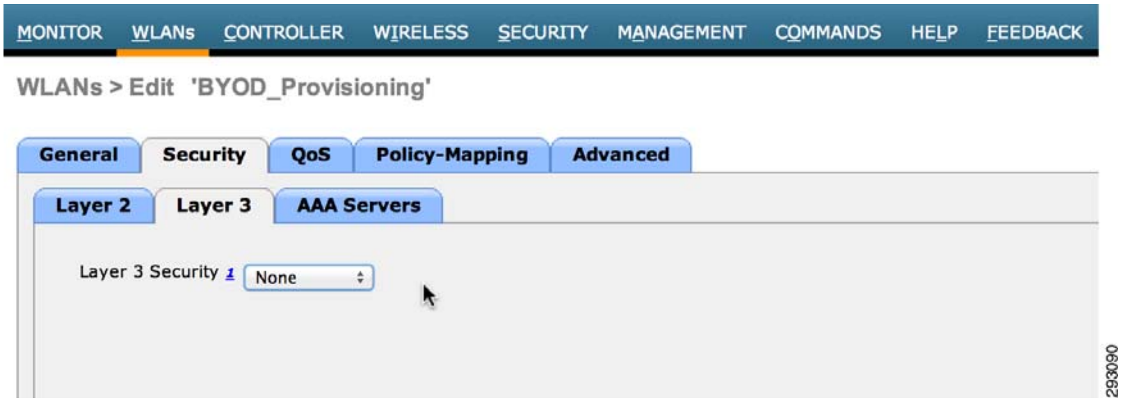
MAC Filtering9 ☑

Fast Transition

Fast Transition □

The Layer 3 Security is configured as **None**, as shown in Figure 9-15.

Figure 9-15 Layer 3 Security Settings

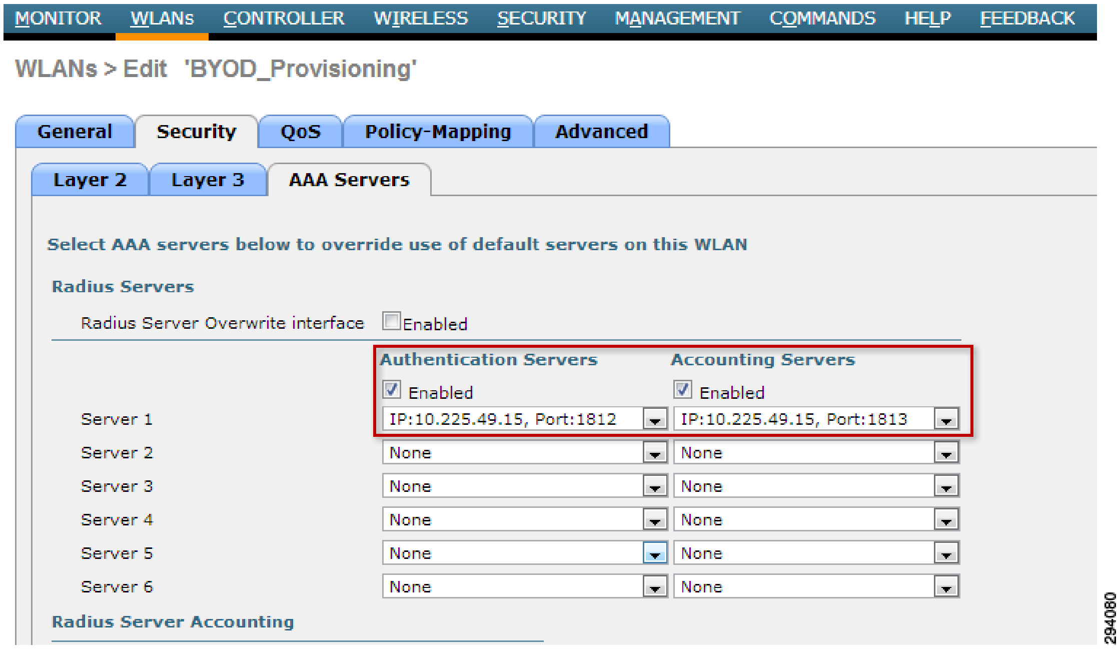


WLANs > Edit 'BYOD_Provisioning'

Layer 3 Security 1 None

Under **Security > AAA servers**, configure the RADIUS server details. Figure 9-16 shows the ISE's IP address configured for Authentication and Authorization.

Figure 9-16 AAA Security Settings



WLANs > Edit 'BYOD_Provisioning'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.225.49.15, Port:1812	IP:10.225.49.15, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Radius Server Accounting

Within the dual SSID deployment there are two possible ways to direct provisioning traffic:

- From the campus or data center—The endpoint receives an IP address from a DHCP scope at the data center and the provisioning traffic is directed through the CAPWAP tunnel between the branch and the Flex 7500 controller.
- At the branch—The endpoint receives an IP address from a DHCP scope at the branch and the provisioning traffic uses the switching and WAN infrastructure for connectivity to data center resources.

Dual SSID—Central Switching Provisioning

Figure 9-17 shows how with central switching provisioning, the endpoint communicates with ISE and data center resources using the CAPWAP tunnel and all traffic is tunneled back to the controller in the data center.

Figure 9-17 Central Switching Provisioning

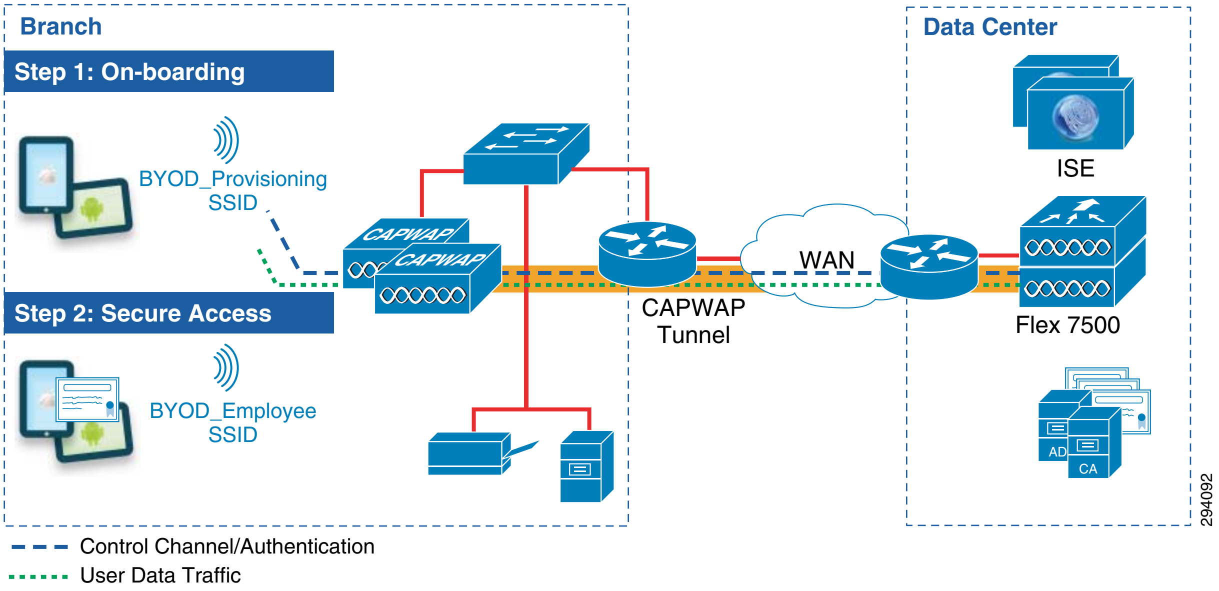
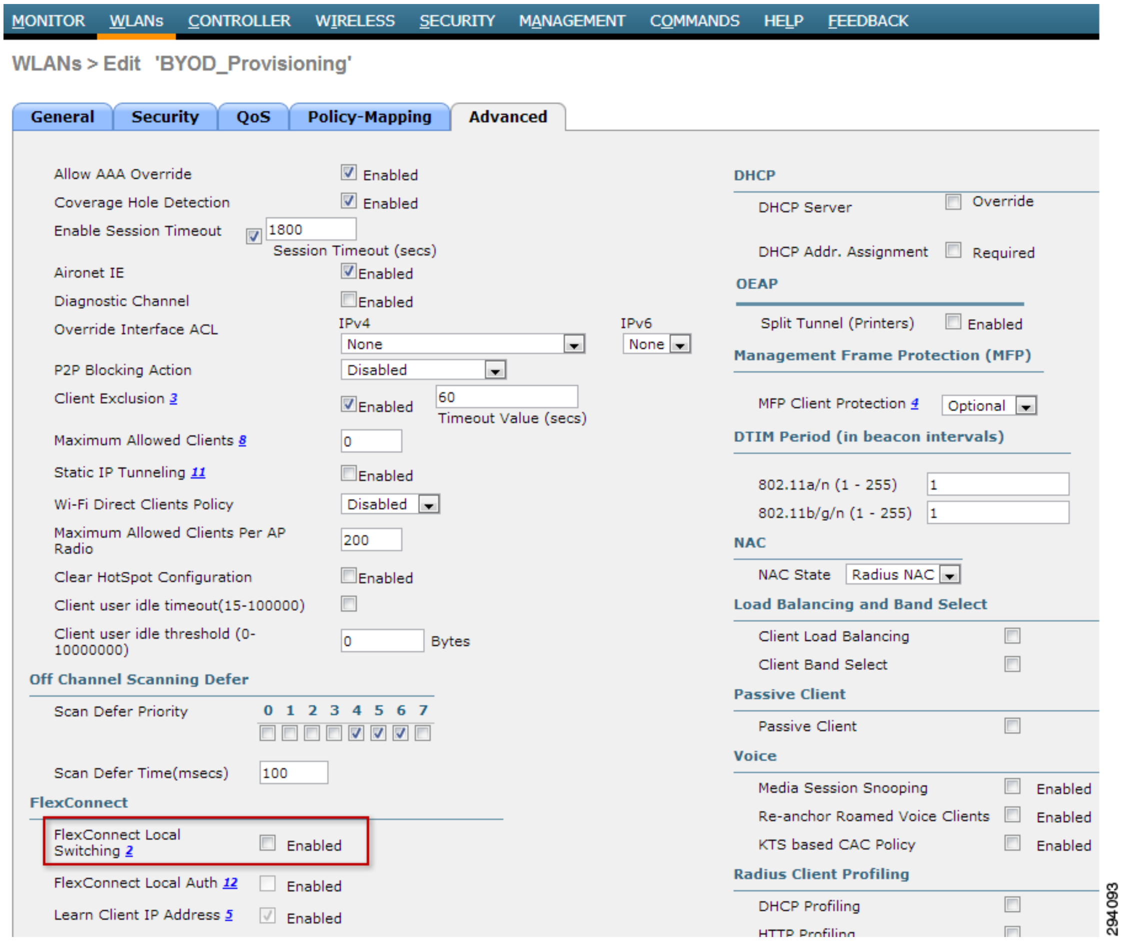


Figure 9-18 shows the advanced settings for BYOD_Provisioning, including the AAA Override and NAC State. The FlexConnect Local Switching setting is disabled for central switching provisioning.

Figure 9-18 Advanced Settings for Central Switching Provisioning



WLANs > Edit 'BYOD_Provisioning'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑Enabled

Diagnostic Channel □Enabled

Override Interface ACL IPv4 None IPv6 None

P2P Blocking Action Disabled

Client Exclusion 3 ☑Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 8 0

Static IP Tunneling 11 □Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 200

Clear HotSpot Configuration □Enabled

Client user idle timeout(15-100000) □

Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

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

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching 2 □ Enabled

FlexConnect Local Auth 12 □ Enabled

Learn Client IP Address 5 ☑ Enabled

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel (Printers) □ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State Radius NAC

Load Balancing and Band Select

Client Load Balancing □

Client Band Select □

Passive Client

Passive Client □

Voice

Media Session Snooping □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

KTS based CAC Policy □ Enabled

Radius Client Profiling

DHCP Profiling □

HTTP Profiling □

Note Authorization Policies and Profiles in Chapter 10, "Identity Services Engine for BYOD" shows the ACLs and authorization profiles used for dual and single SSID provisioning.

Dual SSID—Local Switching Provisioning

Figure 9-19 shows provisioning with local switching mode. The user data traffic is sent to the switch interface and the endpoint relies on the normal router/WAN infrastructure to reach the ISE and other network resources.

Figure 9-19 Local Switching Provisioning

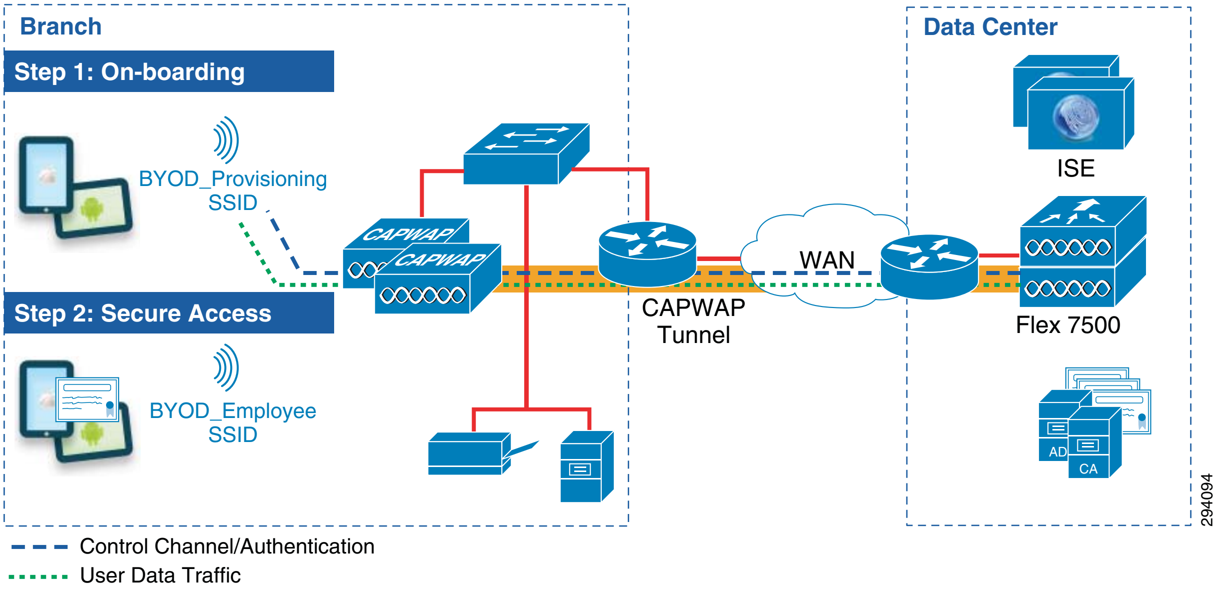
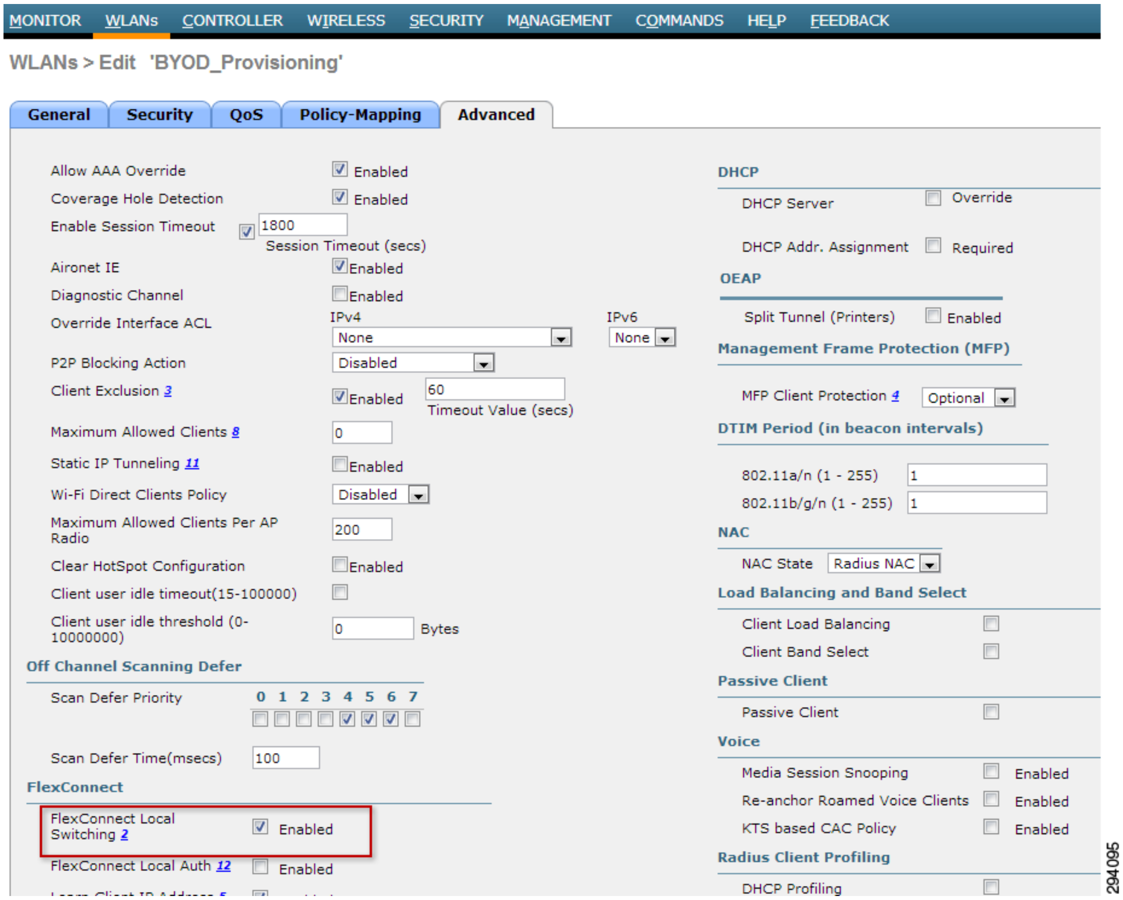


Figure 9-20 shows the advanced settings for BYOD_Provisioning, including the AAA Override and NAC State. The FlexConnect Local Switching is enabled for local switching provisioning.

Figure 9-20 Advanced Settings for Local Switching Provisioning


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
General Security QoS Policy-Mapping Advanced
294095

WLANs > Edit 'BYOD_Provisioning'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
P2P Blocking Action Disabled
Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □ Enabled
Client user idle timeout(15-100000) □
Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 ☑ 7 □
Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching 2 ☑ Enabled
FlexConnect Local Auth 12 □ Enabled

DHCP

DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP

Split Tunnel (Printers) □ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

NAC State Radius NAC

Load Balancing and Band Select

Client Load Balancing □
Client Band Select □

Passive Client

Passive Client □

Voice

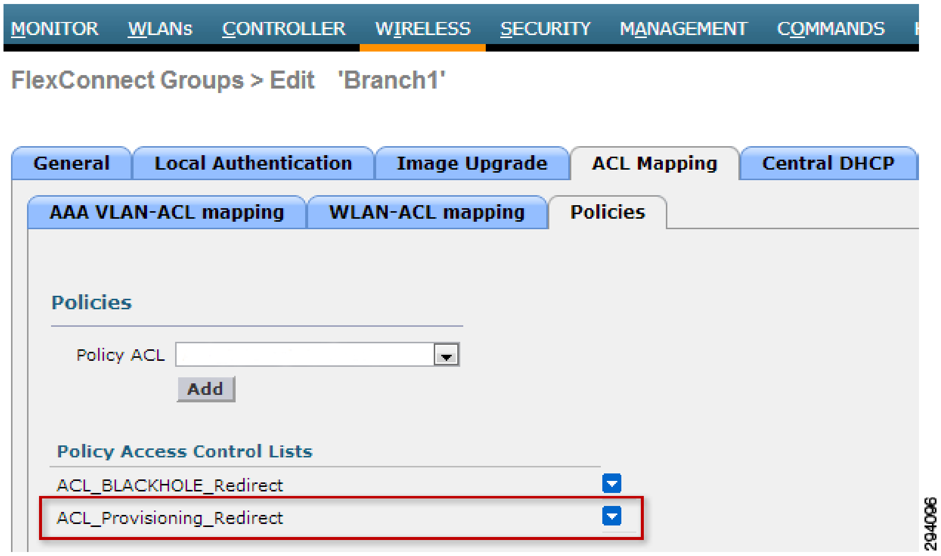
Media Session Snooping □ Enabled
Re-anchor Roamed Voice Clients □ Enabled
KTS based CAC Policy □ Enabled

Radius Client Profiling

DHCP Profiling □

To enforce the redirection to the self-registration portal, a FlexConnect ACL is defined under the Policies tab for the specific FlexConnect group, as shown in Figure 9-21.

Figure 9-21 Policies for FlexConnect Group



FlexConnect Groups > Edit 'Branch1'

Policies

Policy ACL

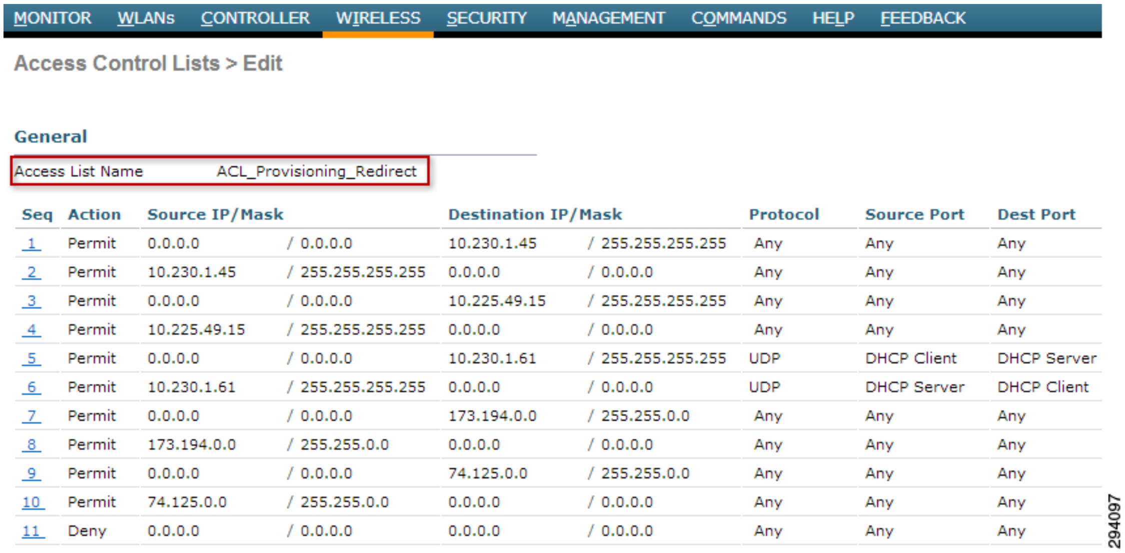
Policy Access Control Lists

ACL_BLACKHOLE_Redirect

ACL_Provisioning_Redirect

The ACL_Provisioning_Redirect FlexConnect ACL shown in Figure 9-22 allows access to ISE, DNS, the Google Play Store, and denies all other traffic. Android devices require access to the Google Play Store to download the SPW package.

Figure 9-22 ACL_Provisioning_Redirect FlexConnect ACL



Access Control Lists > Edit

General

Access List Name ACL_Provisioning_Redirect

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	173.194.0.0	/ 255.255.0.0	Any	Any	Any
8	Permit	173.194.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	74.125.0.0	/ 255.255.0.0	Any	Any	Any
10	Permit	74.125.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

The ACL_Provisioning_Redirect ACL specifies the following access:

- Allow IP access to and from the DNS server (10.230.1.45).
- Allow IP access to and from the ISE Server (10.225.49.15).
- Allow IP access to and from the DHCP server (10.230.1.61).
- Access to Google Play.

Note The purpose of the ACL shown above is to provide an example that network administrators can use to deploy in the network. The Google and Apple app stores may change their addresses, so it is advisable to validate those addresses before deploying the ACL.

Note ACL_Provisioning_Redirect must redirect all traffic sent to enroll.cisco.com. The Cisco Configuration Assistant for Android devices requires this redirect to discover the IP address of the ISE server.

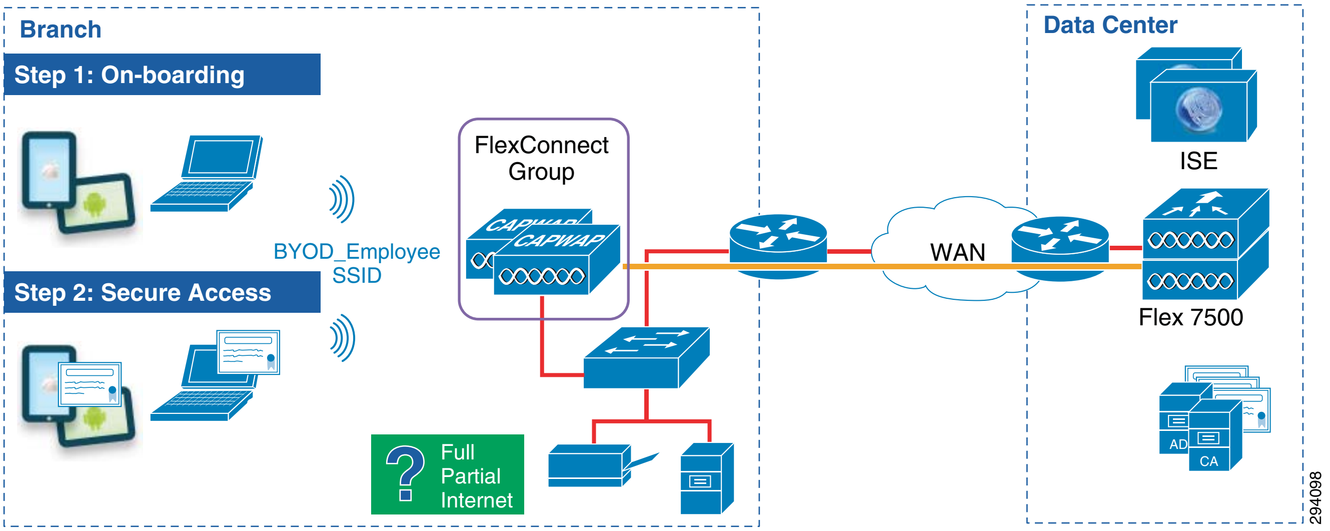
FlexConnect Branch—Single SSID Design

In a single SSID design, the same WLAN is used for certificate enrollment, provisioning (on-boarding process), and secure network access. There are some considerations that should be taken into consideration while deploying a Single SSID solution:

1. Since the authentication method is PEAP, the user is expected to enter the AD credentials before the registration process can begin. In the PEAP protocol, the server presents its identity certificate to the end user. In this design, ISE presents its identity certificate to the endpoint. Some endpoints may reject the certificate if the root certificate is not present in their list of trusted providers. During the registration process, the root CA certificate is installed on the endpoint, but this can't be done if the initial dialog itself fails. Hence, this presents a chicken-and-egg problem. To prevent this from happening the ISE identity certificate must be signed by a third-party trusted provider such as VeriSign.
2. If the above cannot be done, then it is better to deploy dual SSID design.

Figure 9-23 shows how this design uses the BYOD_Employee SSID and is implemented using the Flex 7500 Controller cluster, which is dedicated to manage the APs in the branch locations.

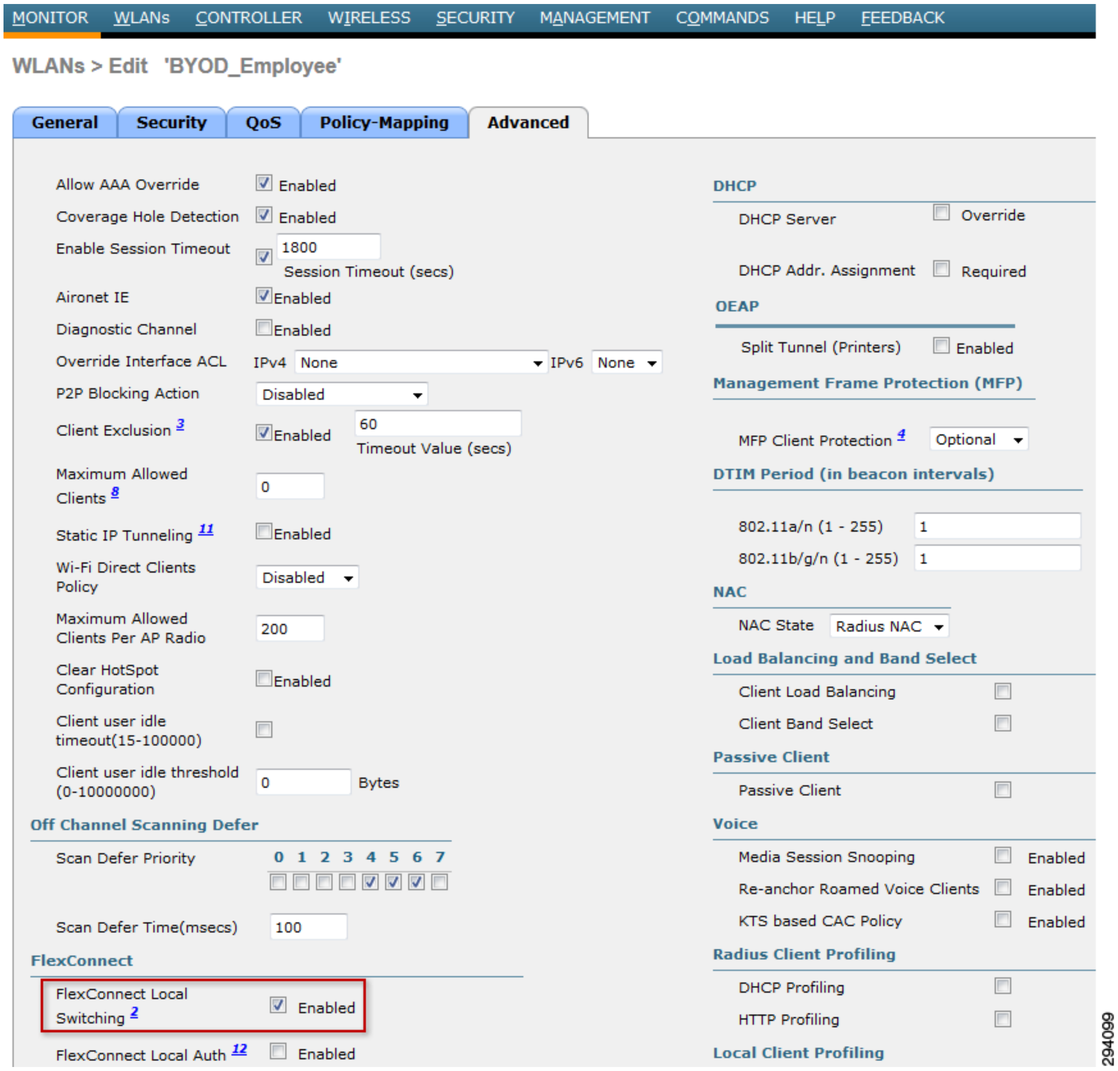
Figure 9-23 Branch-Single SSID



In this scenario the APs associate with the Flex 7500 controller and the FlexConnect capabilities allow the on-boarding and secure access capabilities to be handled by the single BYOD_Employee SSID.

The steps to configure the BYOD_Employee WLAN are similar, following the parameters outlined in Table 9-3. It is important to note that FlexConnect Local Switching is enabled on the BYOD_Employee WLAN, as highlighted in Figure 9-24.

Figure 9-24 FlexConnect Local Switching



WLANs > Edit 'BYOD_Employee'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
Override Interface ACL IPv4 None IPv6 None
P2P Blocking Action Disabled
Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients [8] 0
Static IP Tunneling [11] □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Clear HotSpot Configuration □ Enabled
Client user idle timeout(15-100000) □
Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 ☑ 7 □
Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching [2] ☑ Enabled
FlexConnect Local Auth [12] □ Enabled

DHCP

DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP

Split Tunnel (Printers) □ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

NAC State Radius NAC

Load Balancing and Band Select

Client Load Balancing □
Client Band Select □

Passive Client

Passive Client □

Voice

Media Session Snooping □ Enabled
Re-anchor Roamed Voice Clients □ Enabled
KTS based CAC Policy □ Enabled

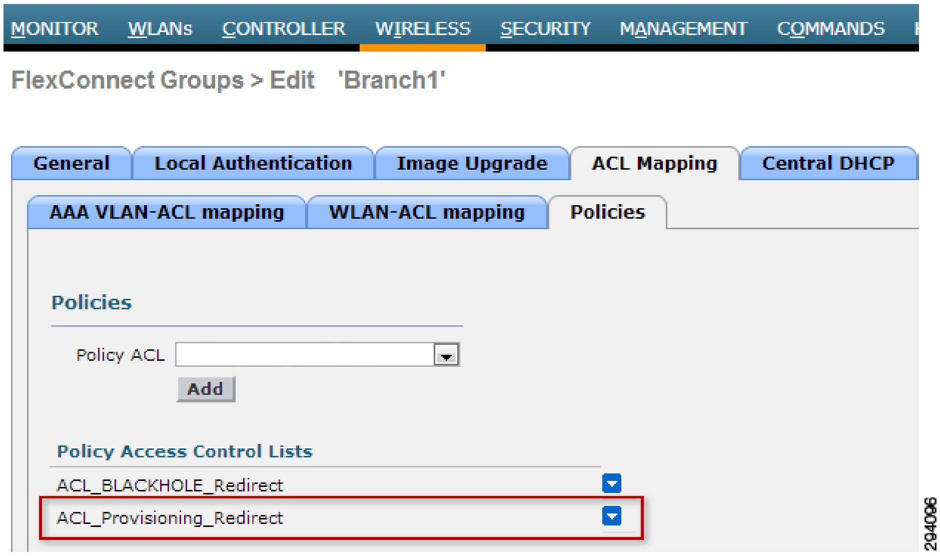
Radius Client Profiling

DHCP Profiling □
HTTP Profiling □

Local Client Profiling

To enforce the redirection to the self-registration portal, a FlexConnect ACL is defined under the Policies tab, as shown in Figure 9-25.

Figure 9-25 Policies for FlexConnect Group



FlexConnect Groups > Edit 'Branch1'

Policies

Policy ACL

Policy Access Control Lists

ACL_BLACKHOLE_Redirect

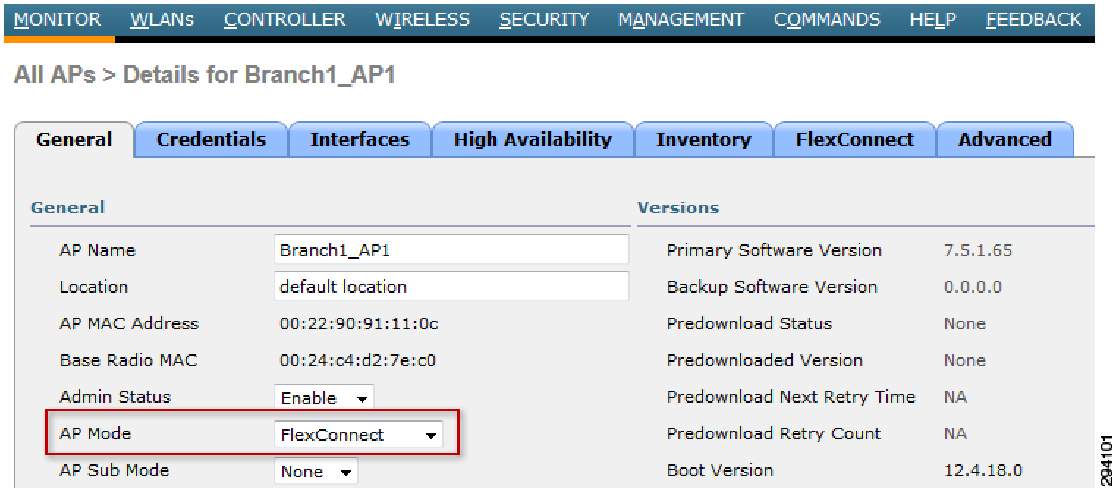
ACL_Provisioning_Redirect

The ACL_Provisioning_Redirect ACL is shown in Figure 9-22 above.

FlexConnect Access Point Configuration

Configure the access point in FlexConnect mode by changing the AP Mode to FlexConnect. Click **Wireless > Access Points** and select the proper branch AP. Figure 9-26 shows the setting for an access point in Branch1.

Figure 9-26 FlexConnect AP Mode

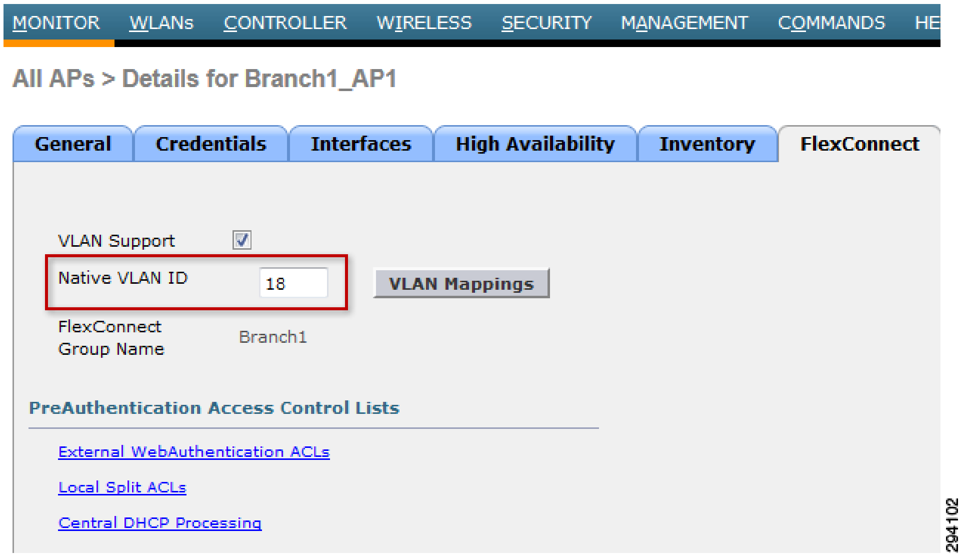


All APs > Details for Branch1_AP1

General		Versions	
AP Name	Branch1_AP1	Primary Software Version	7.5.1.65
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	00:22:90:91:11:0c	Predownload Status	None
Base Radio MAC	00:24:c4:d2:7e:c0	Predownloaded Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	FlexConnect	Predownload Retry Count	NA
AP Sub Mode	None	Boot Version	12.4.18.0

Click the **FlexConnect** tab and specify the Native VLAN for the branch, as shown in Figure 9-27. The access point relies on the native VLAN for IP connectivity.

Figure 9-27 Native VLAN ID



All APs > Details for Branch1_AP1

VLAN Support ☑

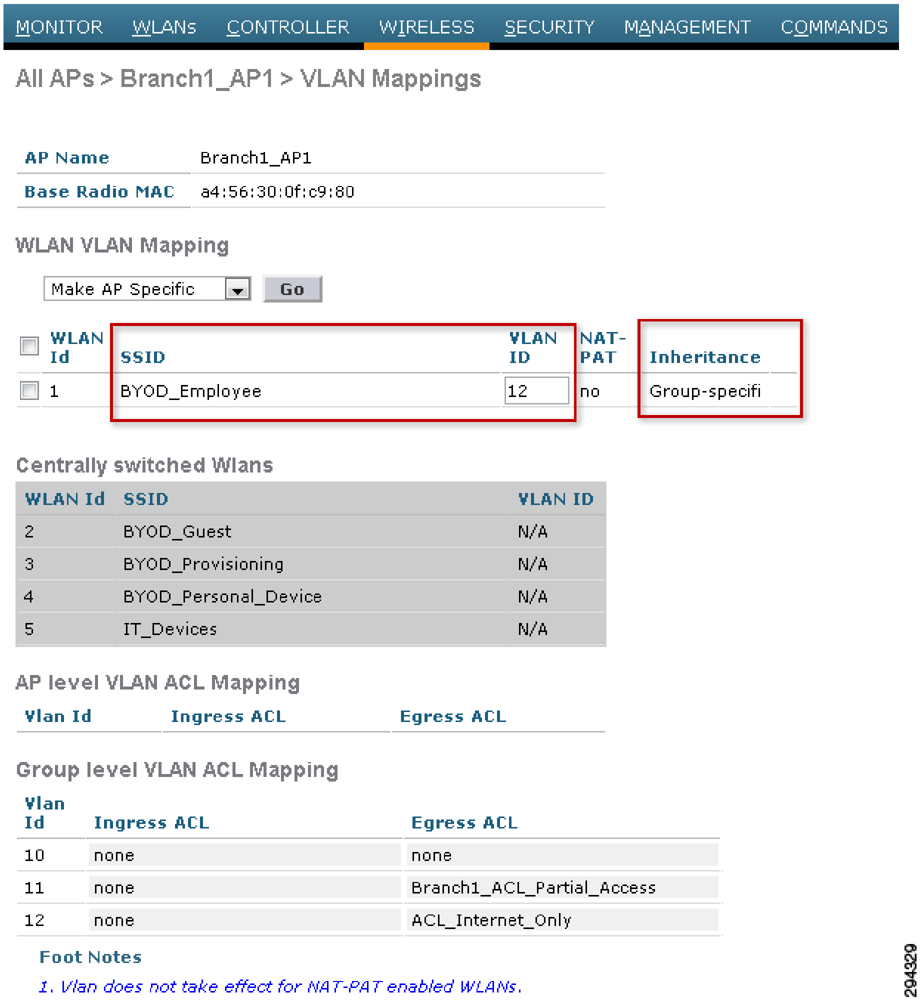
Native VLAN ID 18

FlexConnect Group Name Branch1

Define the VLAN ID to be used for local switching. In Figure 9-28, clients obtain an IP address from VLAN 12 (Internet access) when doing local switching. When using the AAA Overrides for FlexConnect feature, the client is moved to a different VLAN dynamically, based on the matched authorization profile and will obtain an IP address from the defined VLAN.

This setting can be configured at the AP level or the AP can inherit the settings from the FlexConnect Group. FlexConnect Groups are explained in the next section.

Figure 9-28 BYOD_Employee VLAN ID



All APs > Branch1_AP1 > VLAN Mappings

AP Name	Branch1_AP1
Base Radio MAC	a4:56:30:0f:c9:80

WLAN VLAN Mapping

□ WLAN Id	SSID	VLAN ID	NAT-PAT	Inheritance
□ 1	BYOD_Employee	12	no	Group-specifi

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
2	BYOD_Guest	N/A
3	BYOD_Provisioning	N/A
4	BYOD_Personal_Device	N/A
5	IT_Devices	N/A

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL

Group level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
10	none	none
11	none	Branch1_ACL_Partial_Access
12	none	ACL_Internet_Only

Foot Notes

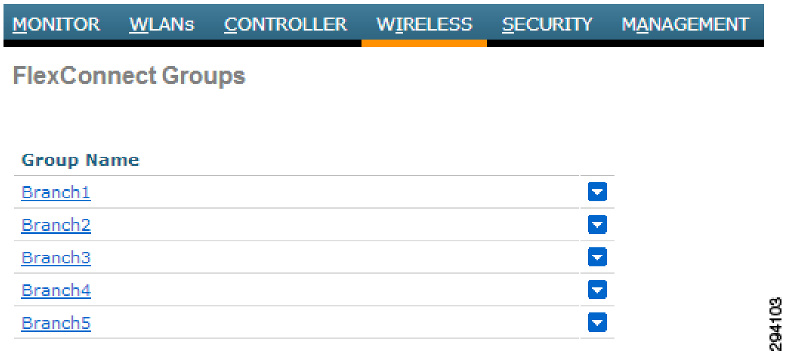
1. Vlan does not take effect for NAT-PAT enabled WLANs.

FlexConnect Groups

FlexConnect groups provide a convenient way to group access points that share the same configuration settings. This is particularly helpful when grouping several FlexConnect access points in remote or branch locations. Instead of configuring each access point separately, FlexConnect groups allow the configuration parameters to be applied to all access points at once. For example, a FlexConnect ACL can be applied to a particular VLAN across all access points within a branch simply by adding the access points to the same FlexConnect group.

For the purpose of this guide, a unique FlexConnect group was defined for each branch, as shown in Figure 9-29.

Figure 9-29 FlexConnect Groups

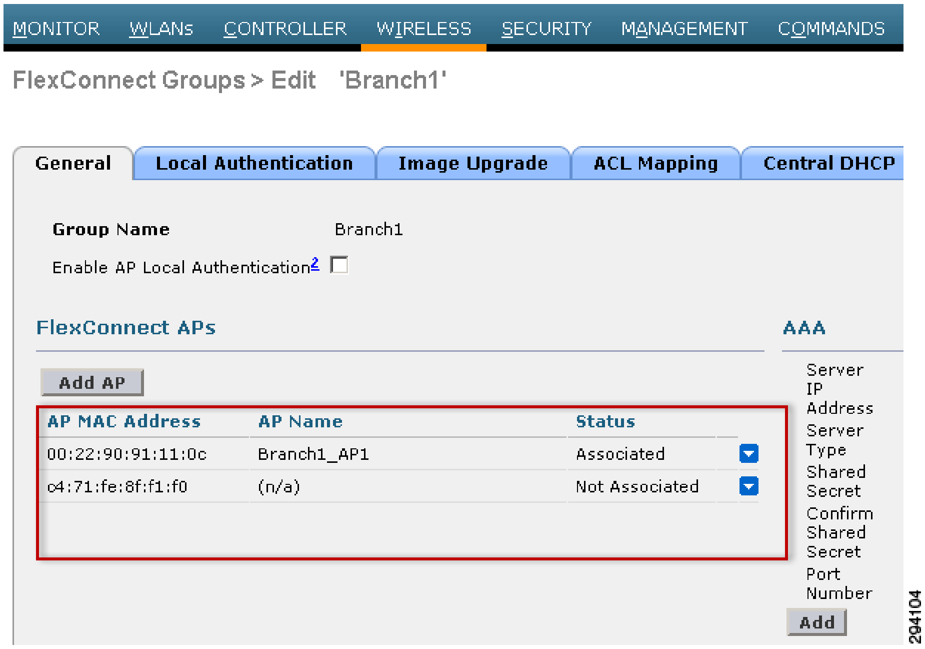


FlexConnect Groups

Group Name
Branch1
Branch2
Branch3
Branch4
Branch5

Figure 9-30 shows the access points that have been added to the Branch1 FlexConnect group.

Figure 9-30 Branch1 FlexConnect Group



FlexConnect Groups > Edit 'Branch1'

Group Name Branch1

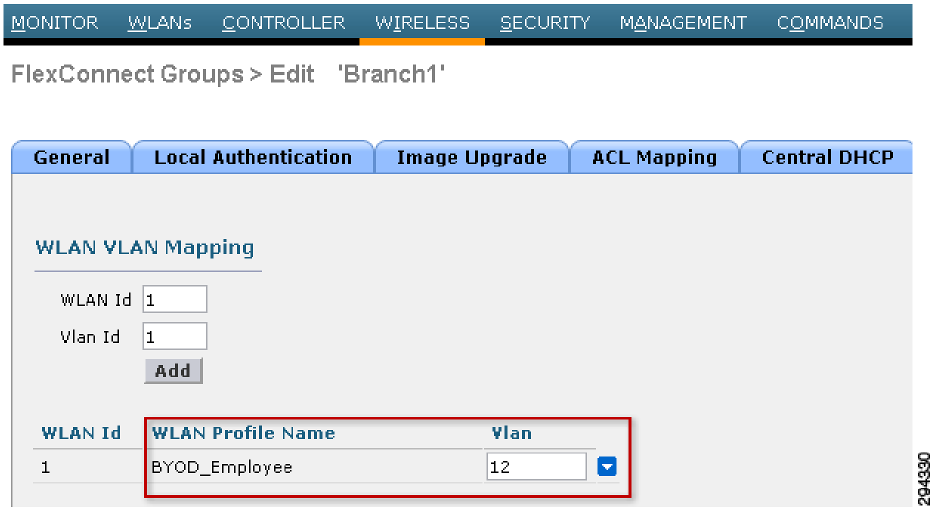
Enable AP Local Authentication[2] □

FlexConnect APs

AP MAC Address	AP Name	Status
00:22:90:91:11:0c	Branch1_AP1	Associated
c4:71:fe:8f:f1:f0	(n/a)	Not Associated

The VLAN ID used for local switching can be defined at the AP level,as shown in Figure 9-28, or at the FlexConnect Group level, as shown in Figure 9-31. In this example, clients will obtain an IP address from VLAN 12 (Internet access) when doing local switching. When using the AAA Overrides for FlexConnect feature, the client is moved to a different VLAN dynamically based on the matched authorization profile and will obtain an IP address from the defined VLAN.

Figure 9-31 Local Switching VLAN—FlexConnect Group Level



FlexConnect Groups > Edit 'Branch1'

WLAN VLAN Mapping

WLAN Id 1

Vlan Id 1

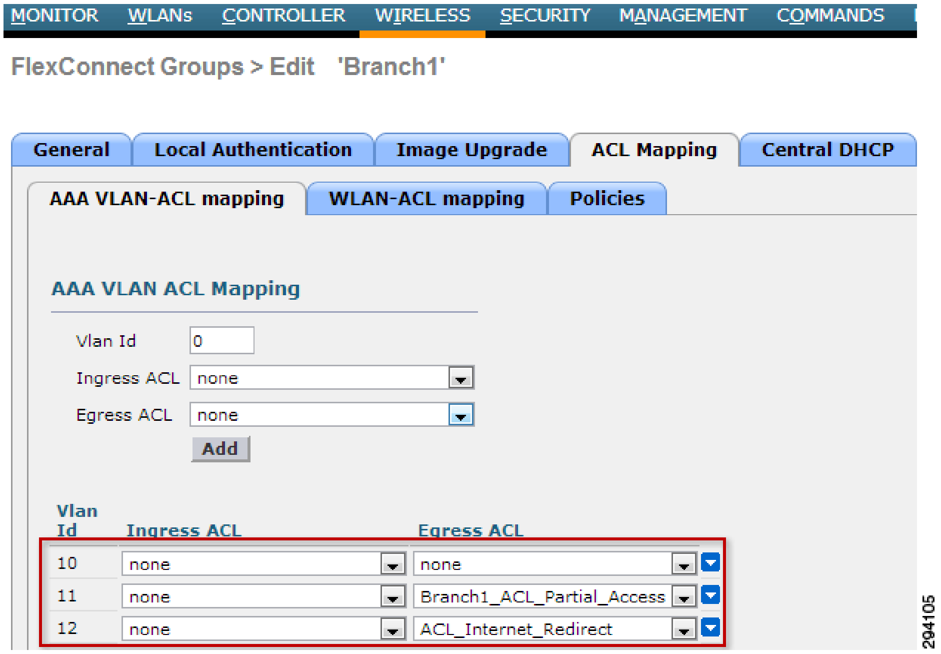
WLAN Id	WLAN Profile Name	Vlan
1	BYOD_Employee	12

Before ISE can enforce an authorization policy, FlexConnect ACLs must be defined and assigned to each VLAN. By clicking the AAA VLAN-ACL mapping tab, the FlexConnect ACL may be enforced for each VLAN ID. This assumes that every branch location shares the same VLAN ID numbers:

- VLAN 10 for full access
- VLAN 11 for partial access
- VLAN 12 for Internet only access

Figure 9-32 shows how the different FlexConnect ACLs have been mapped to each VLAN.

Figure 9-32 VLAN-ACL Mapping



FlexConnect Groups > Edit 'Branch1'

AAA VLAN ACL Mapping

Vlan Id 0

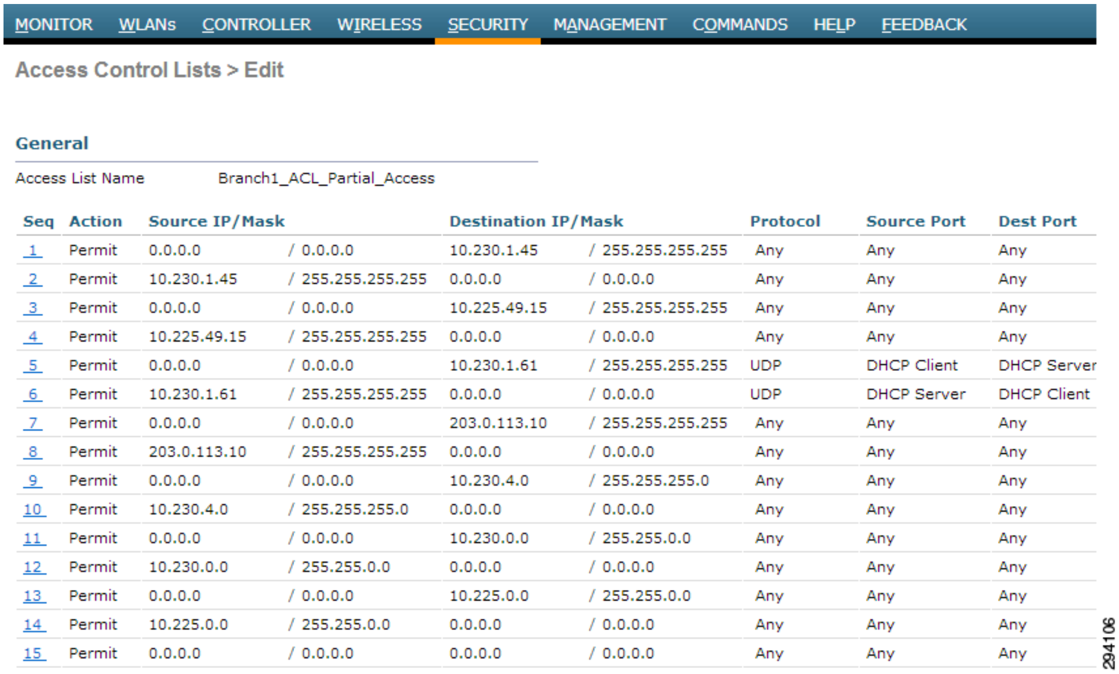
Ingress ACL none

Egress ACL none

Vlan Id	Ingress ACL	Egress ACL
10	none	none
11	none	Branch1_ACL_Partial_Access
12	none	ACL_Internet_Redirect

The FlexConnect ACLs shown in Figure 9-33 and Figure 9-34 are explained in more detail in Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices."

Figure 9-33 Branch1_ACL_Partial_Access FlexConnect ACL



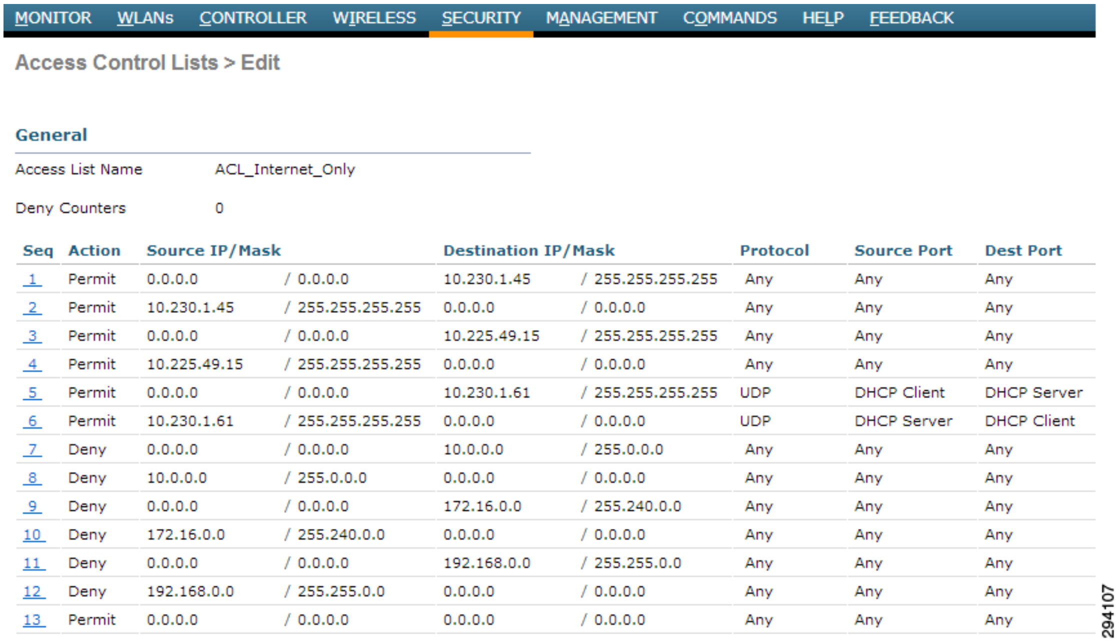
Access Control Lists > Edit

General

Access List Name Branch1_ACL_Partial_Access

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any
8	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	10.230.4.0	/ 255.255.255.0	Any	Any	Any
10	Permit	10.230.4.0	/ 255.255.255.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Permit	0.0.0.0	/ 0.0.0.0	10.230.0.0	/ 255.255.0.0	Any	Any	Any
12	Permit	10.230.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	10.225.0.0	/ 255.255.0.0	Any	Any	Any
14	Permit	10.225.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
15	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

Figure 9-34 ACL_Internet_Only



Access Control Lists > Edit

General

Access List Name ACL_Internet_Only

Deny Counters 0

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any
8	Deny	10.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any
10	Deny	172.16.0.0	/ 255.240.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any
12	Deny	192.168.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
13	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

FlexConnect VLAN Override

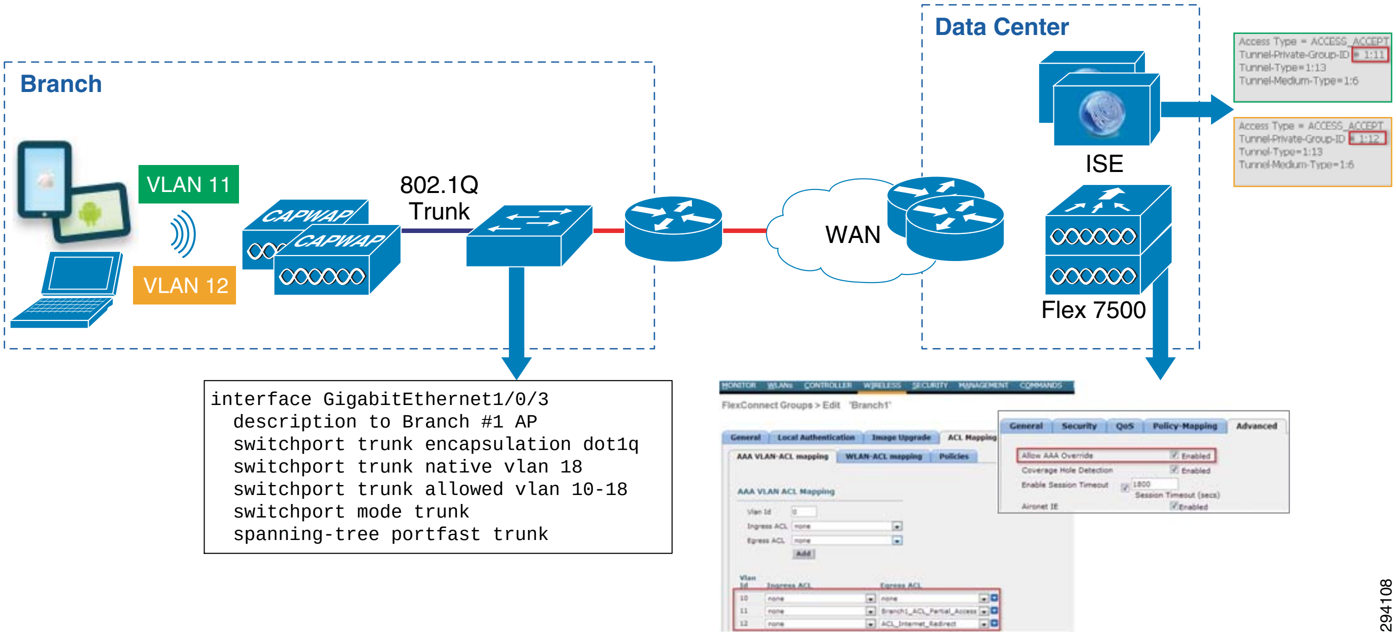
In the current FlexConnect architecture, there is a strict mapping of WLAN to VLAN, so the client getting associated on a particular WLAN on a FlexConnect AP has to abide by the VLAN which is mapped to it. This method has limitations because it requires clients to associate with different SSIDs in order to inherit different VLAN-based policies.

Starting on WLC release 7.2, AAA Override (Dynamic VLAN assignment) of VLANs on individual WLANs configured for local switching is supported. To assign endpoints dynamically to a VLAN, the VLAN IDs are pre-created and the corresponding WLAN-VLAN Mapping on a FlexConnect group is configured, as shown in Figure 9-32.

Figure 9-35 shows the different configuration settings required to dynamically assign endpoints to a branch VLAN, which include:

- The WLAN at the branch configured for local switching mode.
- 802.1Q trunk between the Catalyst switch and the access point.
- A native VLAN and allowed VLANs for the trunk.
- The ISE authorization profile defines what VLAN is assigned to the endpoint.
- The WLAN is configured at the controller to allow AAA Override.
- The VLANs are pre-defined and the VLAN-ACL mapping is defined for the FlexConnect group.

Figure 9-35 FlexConnect VLAN Override


Data Center
Branch
ISE
VLAN 11
VLAN 12
CAPWAP
CAPWAP
802.1Q
Trunk
WAN
Flex 7500
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS
FlexConnect Groups > Edit 'Branch1'
General Local Authentication Image Upgrade ACL Mapping
AAA VLAN-ACL mapping WLAN-ACL mapping Policies
General Security QoS Policy-Mapping Advanced
Add
294108

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:11
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
```

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:12
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
```

```
interface GigabitEthernet1/0/3
  description to Branch #1 AP
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 18
  switchport trunk allowed vlan 10-18
  switchport mode trunk
  spanning-tree portfast trunk
```

AAA VLAN ACL Mapping

Vlan Id: 0
Ingress ACL: none
Egress ACL: none

Vlan Id	Ingress ACL	Egress ACL
10	none	none
11	none	Branch1_ACL_Partial_Access
12	none	ACL_Internet_Redirect

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled

Campus—Converged Access Design

The converged large campus design looks at the hybrid large campus design model, as discussed in Campus Migration Path of Chapter 5, "Campus and Branch Network Design for BYOD." A hybrid large campus design consists of multiple Catalyst 3850s switches or switch stacks deployed at the access layer of the network, operating in Mobility Agent (MA) Mode. A centralized Cisco CT5760 controller within the campus contains the Mobility Controller (MC) function. A Unified Controller CT5508 exists within the campus controller and forms a mobility group with CT5760s. APs may be connected to the CT5760 or CT5508 controllers via Catalyst 3850 or CT3750 switches. In addition a CT5760 or CT5508 may be used as guest access anchor at the Internet edge of the campus. In this design guide the CT5508 is configured as a guest controller.

This design guide will make the following assumptions for the large campus converged access design:

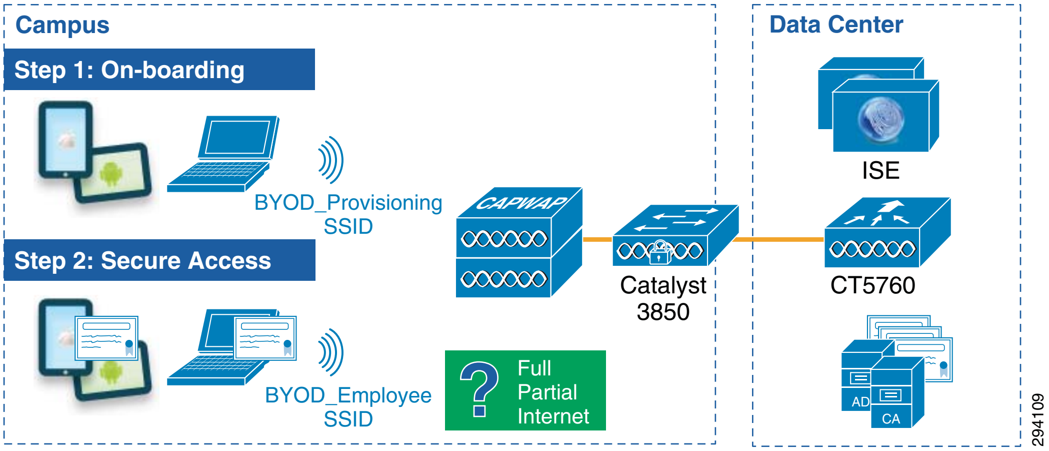
- On-boarded wired and wireless devices will share the same VLAN, and hence the same IP subnet addressing space. It is recognized that customers may implement separate subnets for wired and wireless devices due to issues such as additional security compliance requirements for wireless devices. This is not addressed within this version of the design guidance.
- Catalyst 3850 Series switches are deployed as Layer 2 access switches within the campus. Layer 3 connectivity will be provided by the Catalyst 6500 building distribution switches. Also, in keeping with campus best practices, VLANs will be limited to a single wiring closet. In other words, VLANs will not extend between access-layer switches. Future design guidance may address Catalyst 3850 Series switches deployed as Layer 3 switches or address spanning VLANs across access-layer switches.

Campus Converged Access—Dual SSID Design

In this design there are again two SSIDs: one provides enrollment/provisioning and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides network access over a secure EAP-TLS connection.

Figure 9-36 shows the dual SSID design for the campus APs.

Figure 9-36 Campus—Dual SSID



In the converged access dual SSID design, there are some additional considerations:

- The provisioning SSID can be either open or password protected. When the provisioning SSID is open, any user can connect to the SSID, whereas if it is password protected, then only users that have credentials, such as AD group membership, are allowed to connect to the SSID. In this design guide, the provisioning SSID is configured to be open and its only purpose is to provide on-boarding services.

- After the device is provisioned, it is assumed that the user will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list that provides only access to ISE, DHCP, and DNS must be enforced on the provisioning SSID. The details of the ACL_Provisioning_Redirect ACL are shown below.
- This design guide makes use of the following SSIDs: BYOD_Provisioning and BYOD_Employee.

The properties of these two SSIDs are highlighted in Table 9-4.

Table 9-4 WLAN Parameters

Attribute	BYOD_Provisioning	BYOD_Employee
Description	Used only for device provisioning	For employees that have completed the on-boarding process
Layer 2 Security	None (for Open SSID)	WPA+WPA2
MAC Filtering	Enabled (for Open SSID)	Disabled
WPA+WPA2 Parameters	None	WPA2 Policy, AES, 802.1X
Layer 3 Security	None	None
AAA Server	Select ISE	Select ISE
Advanced	AAA Override Enabled	AAA Override Enabled
Advanced	NAC State- NAC	NAC State- NAC

To configure WLAN BYOD_Provisioning SSID on a CT5760 and Catalyst 3850 follow the steps below. The security on the BYOD_Provisioning SSID is NONE as this is a provisioning SSID through which devices are provisioned on the network. The FAST-SSID feature provides a way for a client to directly switch from BYOD_Provisioning to BYOD_Employee SSID after it has been properly provisioned by ISE.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
captive-portal-bypass
!
mac access-list extended MAC_ALLOW
 permit any any
!
!
interface Vlan2
 description ### BYOD-Employee Vlan ###
 ip address 10.231.2.7 255.255.255.0
 load-interval 30
!
interface Vlan3
 description ### BYOD-Provisioning Vlan ###
 ip address 10.231.3.7 255.255.255.0
 load-interval 30
!
ip http server
ip http authentication local
ip http secure-server
!
wireless management interface Vlan47
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security web-auth parameter-map global
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD-Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
```

The example configuration shown above must be configured on both the Catalyst 3850 which functions as the Mobility Agent (MA), and the CT5760 which functions as the Mobility Controller (MC) in the campus design. Note that the IP addressing for the VLAN interfaces will be different for the MA and MC, however, since they are deployed in different parts of the network infrastructure. Mobility is handled as a separate topic within this chapter, following the WLAN configuration discussion. Additional configuration lines must be added to the MA and MC, respectively for mobility. These are discussed shortly.

The BYOD_Provisioning SSID has no Layer 2 security, as this is an SSID through which devices are provisioned on the network. Instead the wireless client uses MAC-filtering (basically a wireless version of MAB) to authenticate to the network. A URL re-direction and Centralized Web Authentication (CWA) policy is pushed down to the client from ISE, upon connecting to the network. Hence, the configuration for MAC-filtering, NAC, and AAA override are required on the BYOD_Provisioning SSID.

The security on the BYOD_Employee SSID is WPA2 with AES encryption. Note that this is the default setting for a WLAN on the Converged Access platforms (CT5760 or Catalyst 3850) and therefore does not appear within the configuration. The configuration for NAC and AAA override are required on this SSID in order to support a dynamic ACL assignment to the wireless client. In the case of this design guide, the dynamic ACL is a named ACL configured locally on the Catalyst 3850 switch.

Note The administrative level command **show wlan name <*name_of_wlan*>** can be used to show the details regarding the configuration of any WLAN on either the Catalyst 3850 Series switch or the CT5760 wireless controller. This includes any default settings which do not appear within the configuration.

Even though a CWA policy is pushed to the wireless client from ISE during on-boarding via the BYOD_Provisioning SSID, the HTTP and HTTPS server functionality must be globally enabled on the Catalyst 3850 Series switch. This is in order to support the URL re-direction of web sessions from wireless clients to the ISE provisioning portal. The RADIUS server group configuration points back to ISE as the RADIUS server for authentication and authorization of wireless (and wired) clients. The captive portal bypass functionality must be globally enabled on the Catalyst 3850 Series switch in order to allow Apple devices to on-board successfully. The fast-ssid-change global configuration provides a way for client to switch from BYOD_Provisioning to BYOD_Employee SSID after it has been properly provisioned by ISE.

The wireless mobility configuration commands for the CT5760 which functions as the MC will be different from the Catalyst 3850 which functions as the MA. An example of the global mobility configuration lines for the CT5760 wireless controller is shown below.

```
!
interface Vlan47
 description MGMT VLAN
 ip address 10.225.47.2 255.255.255.0
 load-interval 30
!
wireless mobility controller peer-group 100
wireless mobility controller peer-group 100 member ip 10.203.61.5 public-ip 10.203.61.5
wireless mobility controller peer-group 200
wireless mobility controller peer-group 200 member ip 10.207.61.5 public-ip 10.207.61.5
wireless mobility controller peer-group 200 member ip 10.207.71.5 public-ip 10.207.71.5
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36/Points to CT5508
wireless mobility group name byod
wireless management interface Vlan47
wireless rf-network byod
!
```

As can be seen, the CT5760 is configured as the mobility controller (MC) for two switch peer-groups (SPGs)—100 and 200—in the example above. Switch peer-group 100 contains a single Catalyst 3850 switch functioning as a MA. Switch peer-group 200 contains two Catalyst 3850 switches functioning as MAs. An example of the global mobility configuration lines for the Catalyst 3850 is shown below.

```
interface Vlan47
 description MGMT VLAN
 ip address 10.225.61.5 255.255.255.0
 load-interval 30
!

wireless mobility controller ip 10.225.47.2 public-ip 10.225.47.2 / IP Address of 5760 MC
```

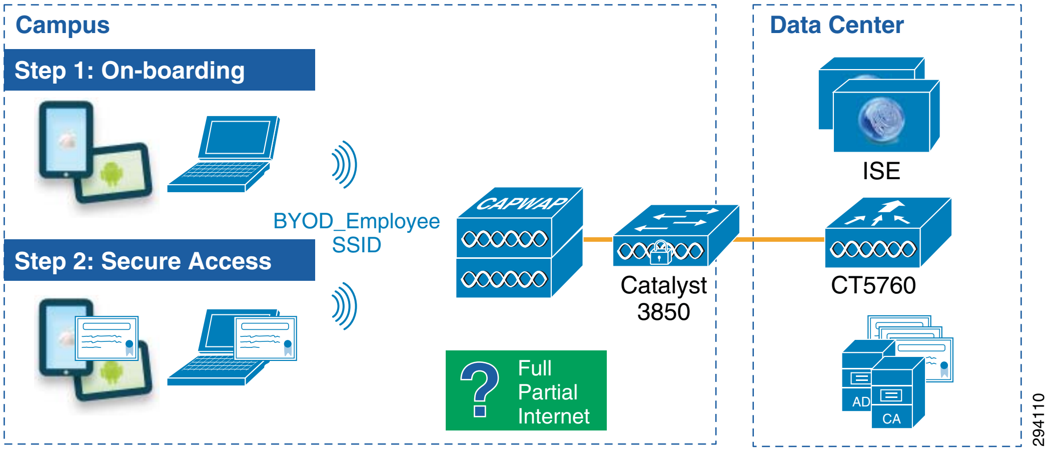
The IP address corresponding to the wireless management interface of the Catalyst 3850 series switch shown in the configuration above appears as a member of SPG 200. SPGs are designed to scale mobility within a Converged Access design. Roaming between Catalyst 3850 Series switch mobility agents (MAs) within a single SPG is handled directly by the switches without the involvement of the CT5760 mobility controller (MC). This is done via a full mesh of CAPWAP tunnels between the Catalyst 3850 Series switch mobility agents (MAs) within a single SPG. Roaming between Catalyst 3850 Series switch mobility agents (MAs) across two SPGs is handled by the CT5760 mobility controller (MC). This is done via CAPWAP tunnels between each Catalyst 3850 Series switch mobility agent (MA) and the CT5760 mobility controller (MC).

As discussed previously, a hybrid campus design may consist of CT5508 wireless controllers operating in Local Mode, alongside the Converged Access infrastructure. This may be necessary during the migration from a centralized wireless overlay model to a Converged Access deployment model. In order to support mobility between the CT5508 wireless controller and the CT5760 wireless controller, the IP address of the CT5508 wireless controller has been added as a wireless mobility group member to the configuration of the CT5760 shown above.

Campus Converged Access—Single SSID Design

In a single SSID design the same WLAN (BYOD_Employee) is used for on-boarding and secure network access. Figure 9-37 shows how this design may be implemented using the CT5760 as an MC and Catalyst 3850 as MA.

Figure 9-37 Campus-Single SSID



The configuration for a single SSID converged campus design is almost the same as a dual SSID design but without the use of the BYOD_Provisioning SSID. A snippet of configuration on the CT5760 and the Catalyst 3850 is shown below. Mobility is handled as separate topic following the WLAN configuration discussion.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
captive-portal-bypass
!
mac access-list extended MAC_ALLOW
 permit any any
!
```

```
!
interface Vlan2
 description ### BYOD-Employee Vlan ###
 ip address 10.231.2.7 255.255.255.0
 load-interval 30
!
interface Vlan3
 description ### BYOD-Provisioning Vlan ###
 ip address 10.231.3.7 255.255.255.0
 load-interval 30
!
ip http server
ip http authentication local
ip http secure-server
!
wireless management interface Vlan47
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security web-auth parameter-map global
 session-timeout 1800
 no shutdown
```

The mobility configuration for both the MC and MA will remain the same as discussed above for the dual SSID Converged Access design.

Campus Converged Access—Mobility

For the large campus design it is important to understand mobility and roaming considerations.

This design highlights multiple Catalyst 3850 Series switches or switch stacks deployed at the access layer of a large sized campus. Switch stacks form Switch Peer Groups (SPGs) in which all switches contain the Mobility Agent (MA) function. Roaming within a SPG is handled through a full mesh of mobility tunnels between MAs within the SPG. Multiple SPGs exist within the large sized campus. APs must be directly connected to MA and not via an intermediate switch (example: a Catalyst 3750 switch).

A Cisco CT5760 wireless controller deployed within a centralized service module within the campus contains the Mobility Controller (MC) function. Multiple SPGs connecting to a single MC form a Mobility Sub-Domain. Multiple Mobility Sub-Domains exist within the large sized campus. Roaming between SPGs within a Mobility Sub-Domain is done through the Cisco CT5760 and/or CT5508 wireless controller. APs connected to a Catalyst 3850 switch register with the CT5760 MC. APs can also be connected to CT5760 via Catalyst 3750 switches.

Multiple Cisco CT5760 and/or CT5508 wireless controllers form a Mobility Group. Hence, a Mobility Group also consists of multiple Mobility Sub-Domains. Roaming between Mobility Sub-domains is done through the Cisco CT5760 and/or CT5508 wireless controllers within the Mobility Group. A single Mobility Group and hence a single Mobility Domain extends across and are entirely contained within the large campus within this design.

For hybrid models consisting of both a CUWN local-mode and converged access products, either a Cisco CT5760 or a CT5508 also serves as a wireless controllers for access points connected to Catalyst 3750-X Series switches using traditional local mode (centralized switching) wireless connectivity.

Keeping above the considerations in mind, few things should be kept in mind.

By default Catalyst 3850 operates as a Mobility Agent and there is no need of any configuration. A Catalyst 3850 may also operate as a Mobility Controller. This mode is covered as part of Branch Design.

See Appendix C, "Software Versions" for details about the Catalyst 3850 software licensing.

CT5760 wireless controller operates only as a Mobility Controller. Mobility tunnels should be setup between CT5760s and Catalyst 3850s for APs connected on Catalyst 3850s to be registered with the MC (CT5760). A snippet of configuration for MC is as below:

```
wireless mobility controller peer-group 100
wireless mobility controller peer-group 100 member ip 10.203.61.5 public-ip 10.203.61.5
wireless mobility controller peer-group 200
wireless mobility controller peer-group 200 member ip 10.207.61.5 public-ip 10.207.61.5
wireless mobility controller peer-group 200 member ip 10.207.71.5 public-ip 10.207.71.5
```

On each Catalyst 3850 acting as an MA, the configuration below is needed to establish a mobility tunnel with the CT5760 MC or a 5508 MC.

```
wireless mobility controller ip 10.225.47.2 public-ip 10.225.47.2 / IP Address of MC
```

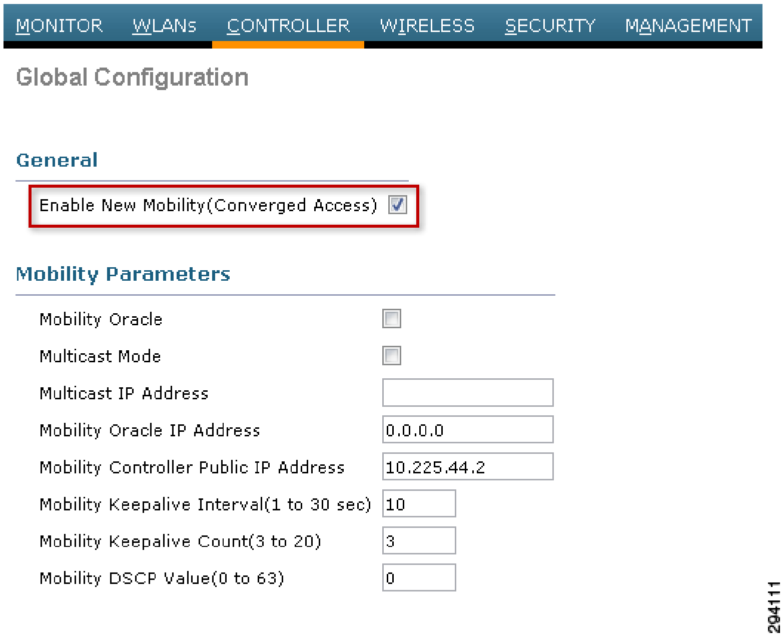
The CT5508 and CT5760 can also form a mobility group. The CT5508 should be upgraded to either 7.3.112 or a version above 7.5 of the WLC to support mobility between converged access and unified access products. The configuration on the CT5508 to enable mobility between the CT5760 and the CT5508 is shown below. The design guide provides guidance for version 7.5 for CT5508.

```
wireless mobility controller/ Enables the MC function, by default turned on CT5760
wireless mobility group name byod/ Create mobility group byod
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36/ IP of member CT5508
```

Note Only WLC versions 7.3.112 or 7.5 and above support mobility between converged access products and unified access products. Ensure that you have code version running compatible code. This design guide uses 7.5 release.

To enable mobility between converged access and unified access products, first the New Mobility should be enabled on the WLC as shown in Figure 9-38.

Figure 9-38 *Enable New Mobility*



Global Configuration

General

Enable New Mobility(Converged Access) ☑

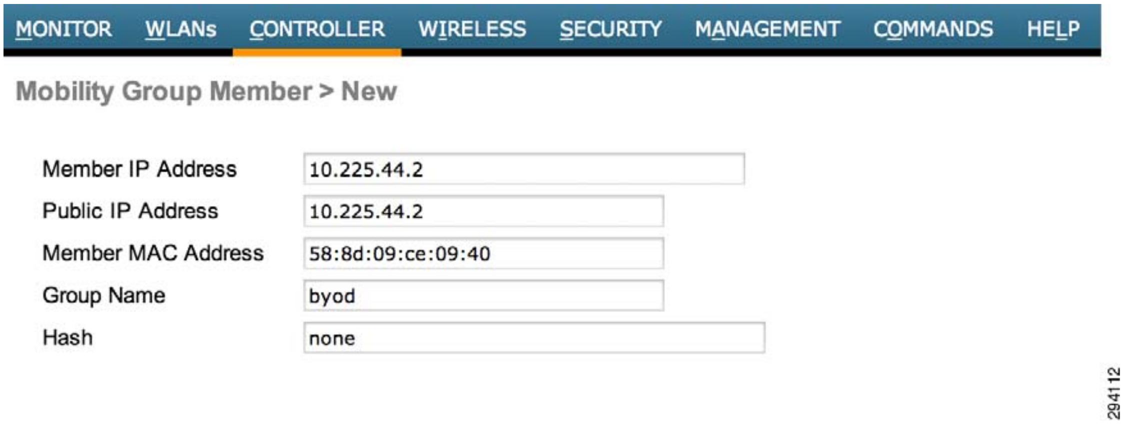
Mobility Parameters

Mobility Oracle	□
Multicast Mode	□
Multicast IP Address	
Mobility Oracle IP Address	0.0.0.0
Mobility Controller Public IP Address	10.225.44.2
Mobility Keepalive Interval(1 to 30 sec)	10
Mobility Keepalive Count(3 to 20)	3
Mobility DSCP Value(0 to 63)	0

After enabling New Mobility and restarting the Wireless LAN Controller, additional options for configuring switch peer groups as well as mobility groups are enabled. For CT5760 and CT5508 to form a group and talk to each other, additional configuration as below is required.

Click **Mobility Management > Mobility Groups** and click **New**, as shown in Figure 9-39.

Figure 9-39 *Create New Mobility Group*



Mobility Group Member > New

Member IP Address	10.225.44.2
Public IP Address	10.225.44.2
Member MAC Address	58:8d:09:ce:09:40
Group Name	byod
Hash	none

The Member IP address above should be the CT5760 IP address that enables mobility messaging and CAPWAP tunnels to be set up between CT5760 and CT5508.

Other design considerations while deploying a large campus WLAN infrastructure include the following:

- 802.1X, WLAN, and VLAN configurations should be replicated on all Catalyst 3850s and CT5760s.
- Mobility group name should be the same between CT5760s and CT5508s.

Branch—Converged Access Design

With a converged access design, a centralized FlexConnect wireless controller can be replaced by a Catalyst 3850 switch that operates both as a Mobility Agent (MA) and Mobility Controller (MC). Guest wireless access still utilizes the same model wherein the guest traffic is auto-anchored to a dedicated guest anchor controller located within the Internet Edge of the campus. The guest controller can be a CT5508 controller with a 7.5 version of code, or a CT5760 converged wireless LAN controller.

The integrated controller branch BYOD design guide makes the following assumptions:

- On-boarded wired and wireless devices will share the same VLAN and hence the same IP subnet addressing space. It is possible to use different VLAN and addressing space for wireless and wired clients, however it is not addressed in this design guide.
- The Catalyst 3850 switches are deployed as a Layer 2 switches within the branch location. Layer 3 connectivity within the branch will be provided by ISR routers which also serve as the WAN connectivity point for the branch. (Future design guides may address Catalyst 3850 deployed as Layer 3 switch within the branch location).

Branch Converged Access—Dual SSID Design

In the dual-SSID design, a dedicated open SSID (BYOD_Provisioning) with MAC-filtering (i.e., MAC Authentication Bypass) will be configured for on-boarding devices. The SSID will be statically mapped to a separate Provisioning VLAN on the Catalyst 3850 switch. Figure 9-40 shows the branch converged access for a dual SSID design.

Figure 9-40 Branch Converged Access—Dual SSID

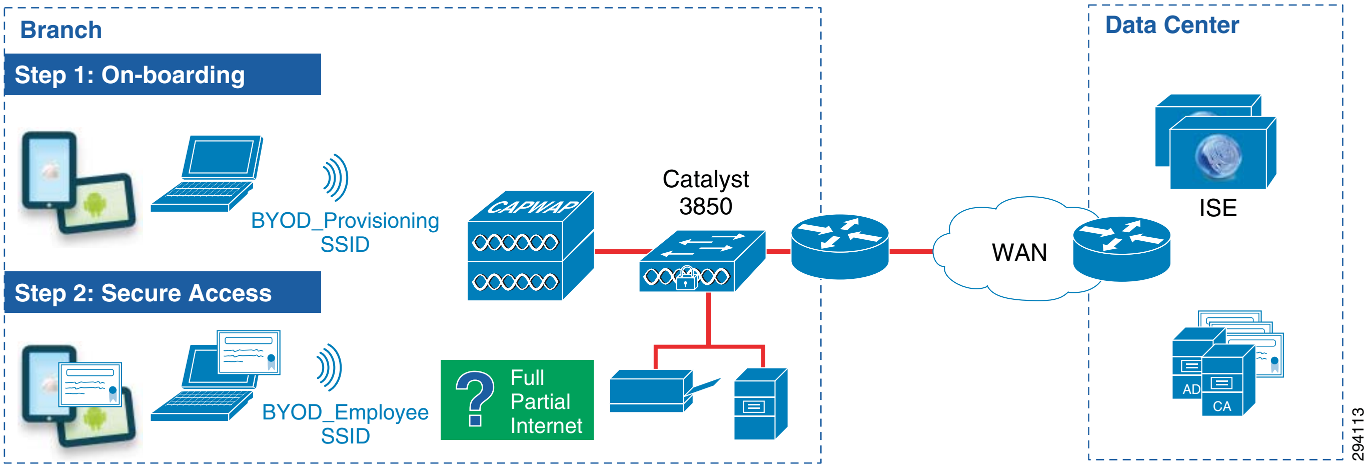


Table 9-5 summarizes the VLANs within the branch when utilizing the dual-SSID BYOD on-boarding design.

Table 9-5 VLANs in Branch with Dual-SSID BYOD On-boarding Design

Description	VLAN	VLAN Name
Wired and wireless corporate access. IT managed devices. Employee managed devices with full, partial, or Internet access.	12	BYOD_Employee
Provisioning VLAN for Dual-SSID wireless on-boarding.	13	BYOD_Provisioning
Separate VLAN for branch servers.	16	Server
Dedicated VLAN for management of network infrastructure.	18	Management
Isolated VLAN for pass through of wireless auto-anchor tunnels. Not trunked to Layer 3 router.	777	BYOD_Guest

The following configuration snippet provides an example of the possible configuration additions to the Catalyst 3850 in order to support on-boarding of wireless devices in a dual-SSID BYOD implementation using MAC-filtering.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
 auth-type any
!
aaa session-id common
!
ip device tracking
!

qos wireless-default-untrust
vtp domain bn
!
mac access-list extended MAC_ALLOW
 permit any any
!
wireless mobility controller
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group name byod
wireless management interface Vlan18
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless broadcast
wireless multicast
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD_Employee
 nac
 security dot1x authentication-list default
 session-timeout 1800
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD_Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
!
```

The following configuration snippet provides a partial example of the possible configuration additions to the branch router configuration in order to support on-boarding of wireless devices in a dual-SSID BYOD implementation using MAC-filtering—when the Catalyst 3850 Series switch is functioning as a Layer 2 switch.

```
!
interface GigabitEthernet0/0
 description CONNECTION TO CATALYST 3850 SWITCH
 no ip address
 load-interval 30
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.13/ Provisioning VLAN
 description CATALYST 3850 PROVISIONING VLAN
 encapsulation dot1Q 13
 ip address 10.200.13.2 255.255.255.0
 ip helper-address 10.230.1.61/ Relay DHCP to the DHCP server
 ip helper-address 10.225.42.15/ Relay DHCP to ISE for profiling
 standby 13 ip 10.200.13.1
 standby 13 priority 110
 standby 13 preempt
!
```

Branch Converged Access—Single SSID Design

In the single SSID design, the corporate SSID (BYOD_Employee) supports authentication via PEAP for non on-boarded devices. Once on-boarding is complete, the corporate SSID supports authentication via EAP-TLS for on-boarded devices. The corporate SSID is statically mapped to a separate Corporate VLAN on the Catalyst 3850 switch. Figure 9-41 shows the branch converged access for a single SSID Design.

Figure 9-41 Branch Converged Access—Single SSID

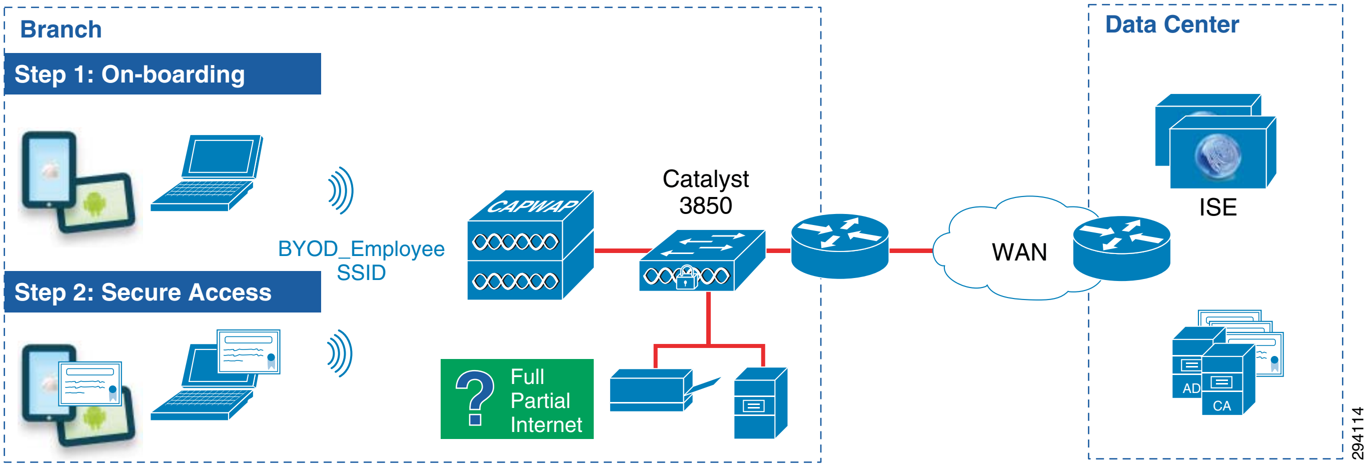


Table 9-6 summarizes the VLANs within the branch when utilizing the single-SSID BYOD on-boarding design.

Table 9-6 VLANs in Branch when Utilizing Single-SSID BYOD On-boarding Design

Description	VLAN	VLAN Name
Wired and wireless corporate access. IT managed devices. Employee managed devices with full, partial, or Internet access.	12	BYOD_Employee
Separate VLAN for branch servers.	16	Server
Dedicated VLAN for management of network infrastructure.	18	Management
Isolated VLAN for past through of wireless auto-anchor tunnels. Not trunked to Layer 3 router.	777	BYOD_Guest

The following configuration shows relevant parts of configuration for the Catalyst 3850 when utilizing a single SSID on-boarding model.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
 auth-type any
!
aaa session-id common
!
ip device tracking
!
!
qos wireless-default-untrust
!
mac access-list extended MAC_ALLOW
 permit any any
!
```

```
wireless mobility controller
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group name byod
wireless management interface Vlan18
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless broadcast
wireless multicast
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD_Employee
 nac
 security dot1x authentication-list default
 session-timeout 1800
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 session-timeout 1800
 no shutdown
!
?
```

CHAPTER 10

Identity Services Engine for BYOD

Revised: September 27, 2013

The Cisco Identity Services Engine (ISE) allows for enforcement of centrally configured policies across wired and wireless networks to help organizations provide secure unified access. The Cisco ISE plays a critical role in enabling the BYOD model, where employees are allowed to connect their personal devices securely to the network. By integrating with third-party Mobile Device Managers (MDM), additional device posture may be used to enforce permissions into the network.

Cisco ISE provides a highly scalable architecture that supports both standalone and distributed deployments. The configuration guidelines shown in this document reflect a distributed architecture with multiple nodes.

For small BYOD deployments, one or two ISE nodes may be configured in standalone mode. Depending on how the AAA connections are configured across the access layer switches and Wireless LAN Controllers, either an active/backup or load balancing of AAA workflows can be enabled across the redundant standalone ISE nodes.

For larger BYOD deployments, the ISE functionality can be distributed across multiple nodes. Distributed deployments support the following different ISE personas:

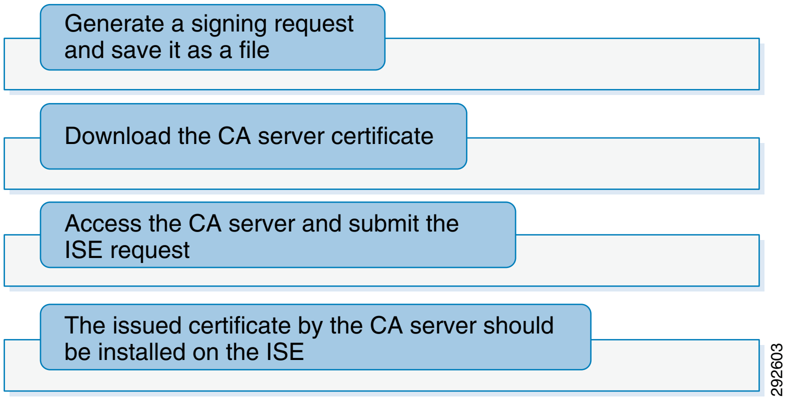
- Administration—The administration node handles all system level configuration. There can be one primary and one secondary administration node in a distributed deployment.
- Monitoring—The monitoring node handles log collection and provides monitoring and troubleshooting tools. There can be one primary and one secondary monitoring node in a distributed deployment.
- Policy Service—The policy service node provides authentication, authorization, guest access, client provisioning, and profiling services. There can be multiple policy services nodes in a distributed deployment.

To support a medium-sized BYOD deployment, both administration and monitoring personas can be deployed on a single node while dedicated policy services nodes can handle AAA functions. For a large BYOD deployment, the monitoring persona can be implemented on a dedicated node providing centralized logging functions.

Identity Certificate for ISE

ISE needs an identity certificate that is signed by a CA server so that it can be trusted by endpoints, gateways, and servers. Figure 10-1 illustrates the steps at a high level.

Figure 10-1 High-Level Steps for Deploying Identity Certificates on ISE


Generate a signing request and save it as a file
Download the CA server certificate
Access the CA server and submit the ISE request
The issued certificate by the CA server should be installed on the ISE
292603

For more details on installing a digital certificate on the Cisco ISE, refer to the TrustSec How-To Guide: http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

Network Device Definition within ISE

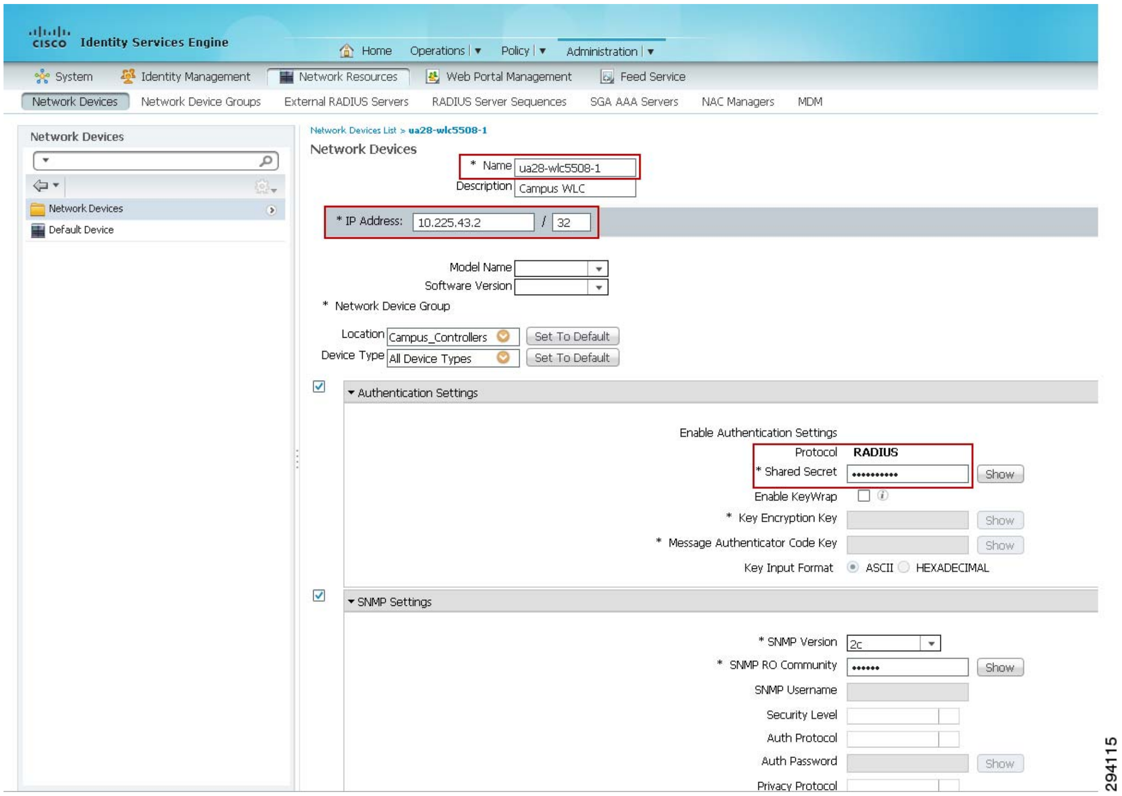
A network device is an authentication, authorization, and accounting (AAA) client through which AAA service requests are attempted, for example, switches, routers, and so on. The network device definition enables the Cisco Identity Services Engine (Cisco ISE) to interact with the network devices that are configured. A network device that is not defined cannot receive AAA services from Cisco ISE.

As users/devices connect to network infrastructure such as wireless controllers and switches enabled for 802.1X authentication, the network device serves as an 802.1X Authenticator to the client's Supplicant. In order for the network device to determine if access is to be granted and what services the device is authorized for, the network device must be able to communicate with the ISE serving as the Authentication Server. To enable this communication, the ISE must be configured with information about that network device as well as credentials to be used to authenticate it.

To configure ISE with this information, refer to Figure 10-2 and the following:

1. At ISE go to **Administration > Network Resources > Network Devices** and click **Add**.
2. Enter the hostname of the device.
3. Enter the IP Address of the network device. This must be the address used to source all RADIUS communications from the device.
4. Change the Network Device Location or Device Type if a custom location/type has been previously defined.
5. Configure the RADIUS Shared Secret. This must match that configured on the network device for the ISE server.
6. Click the down arrow next to SNMP Settings and complete as appropriate.

Figure 10-2 Network Device Configuration in ISE



Network Devices List > ua28-wlc5508-1

Network Devices

* Name ua28-wlc5508-1

Description Campus WLC

* IP Address: 10.225.43.2 / 32

Model Name

Software Version

* Network Device Group

Location Campus_Controllers Set To Default

Device Type All Device Types Set To Default

☑ Authentication Settings

Enable Authentication Settings

Protocol RADIUS

* Shared Secret •••••••••• Show

Enable KeyWrap □

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ● ASCII ○ HEXADECIMAL

☑ SNMP Settings

* SNMP Version 2c

* SNMP RO Community •••••• Show

SNMP Username

Security Level

Auth Protocol

Auth Password Show

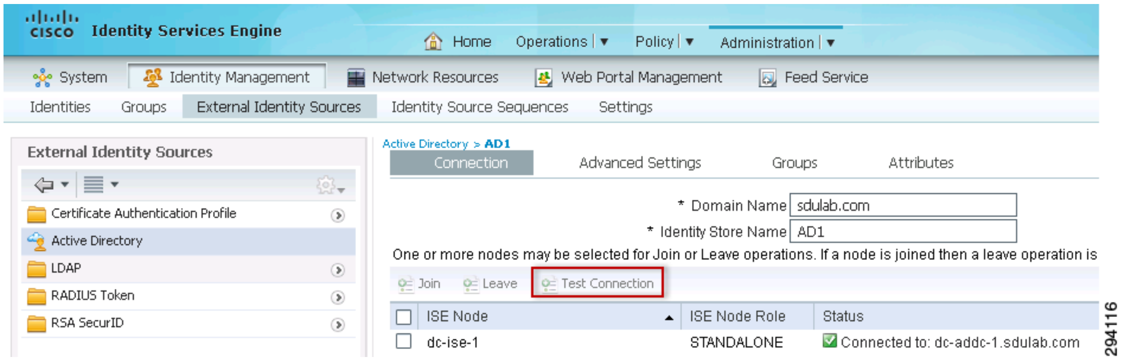
Privacy Protocol

ISE Integration with Active Directory

While the ISE can maintain an internal list of users for authentication purposes, most organizations rely on an external directory as the main identity source. By integrating with Microsoft's Active Directory, objects such as users and groups become critical in the authorization process and can be accessed from a single source.

To integrate with Active Directory, on the ISE click **Administration > External Identity Sources > Active Directory** and specify the domain name, as shown in Figure 10-3. To verify that the ISE node can connect to the Active Directory domain, click **Test Connection** and authenticate with an AD username and password, as shown in Figure 10-3. Click **Join** to join the ISE node to Active Directory.

Figure 10-3 Active Directory Integration



* Domain Name sdulab.com

* Identity Store Name AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is

ISE Node	ISE Node Role	Status
dc-ise-1	STANDALONE	Connected to: dc-addc-1.sdulab.com

Note The Cisco Identity Services Engine User Guide has detailed configuration steps: http://www.cisco.com/en/US/customer/docs/security/ise/1.2/user_guide/ise_user_guide.html.

Guest and Self-Registration Portals

The Cisco ISE server has the capability to host multiple portals. The BYOD system design relies on the Guest Portal to provide wireless guest access and, for provisioning purposes, the redirection of employees to the Self-Registration portal to on-board their devices. Chapter 21, "BYOD Guest Wireless Access" discusses the use of the Guest Portal for guest wireless access. The default ISE portals have standard Cisco branding that may be customized to identify unique portals for different purposes and with individual policies.

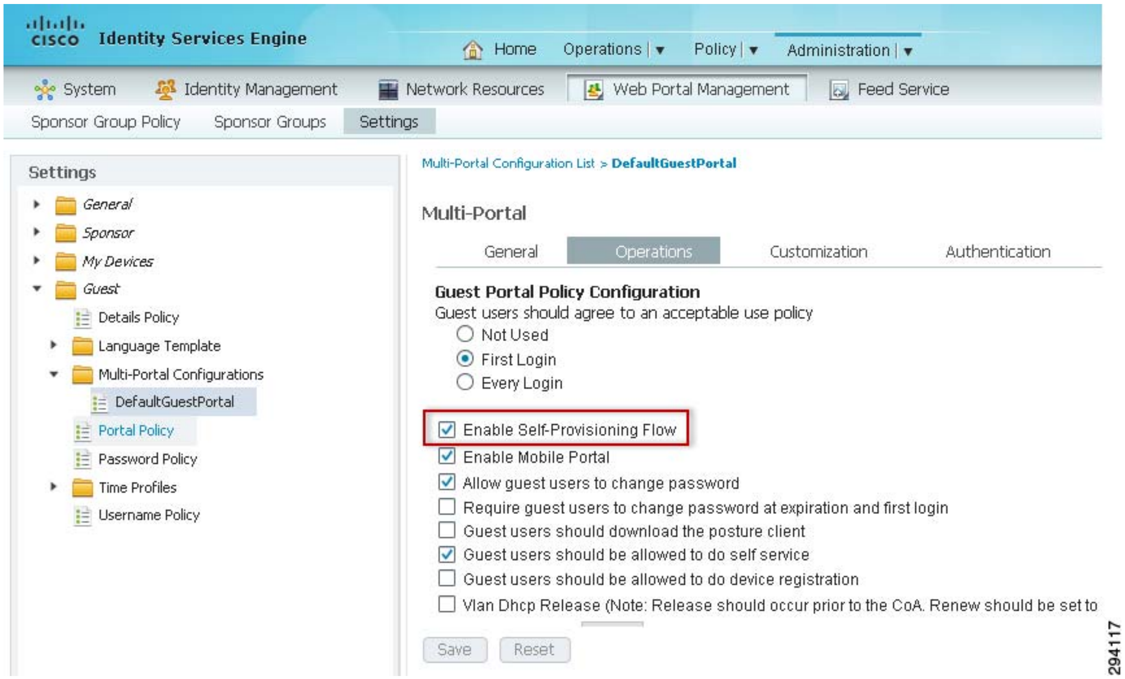
ISE enables self-provisioning, which allows employees to register their personal devices. The ISE provisions the device with its native supplicant during device registration.

The BYOD system leads the employee through the following provisioning steps the first time they bring their personal device to work and register:

1. The employee connects the device to the open SSID (BYOD_Provisioning SSID for dual SSIDs).
2. The device is redirected to the Guest Registration portal.
3. The employee enters credentials and ISE authenticates against Active Directory.
4. If the device is not yet registered on the network, the session is redirected to the self-registration portal.
5. The employee is asked to enter a unique device description and complete the device registration.

To enable Self-Provisioning, configure these portals as follows: click **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations**, as shown in Figure 10-4.

Figure 10-4 Portal Settings—Operations



Guest Portal Policy Configuration

Guest users should agree to an acceptable use policy

○ Not Used
● First Login
○ Every Login

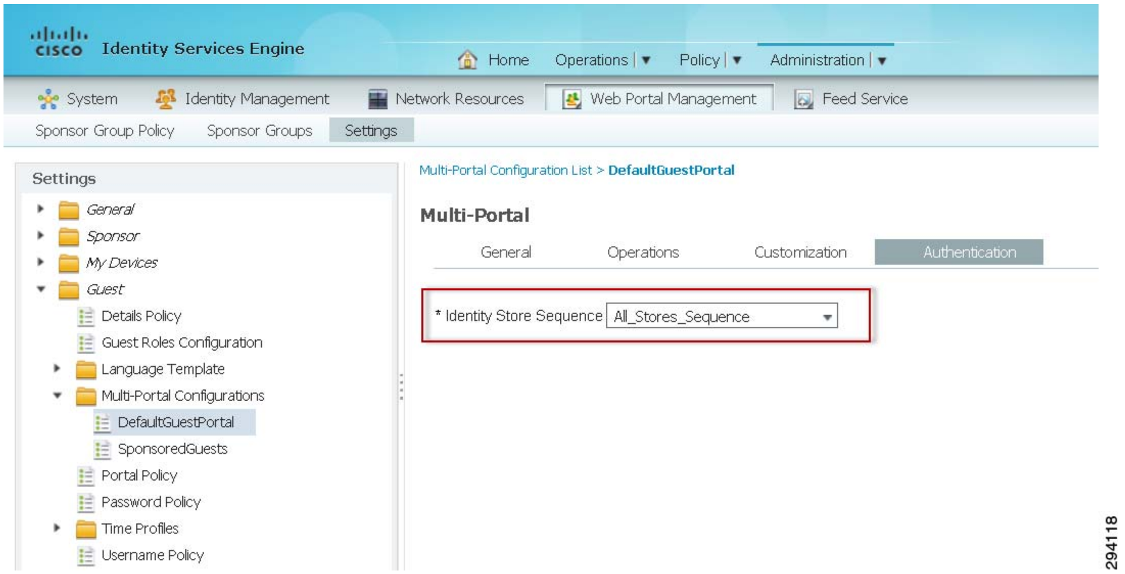
☑ Enable Self-Provisioning Flow
☑ Enable Mobile Portal
☑ Allow guest users to change password
□ Require guest users to change password at expiration and first login
□ Guest users should download the posture client
☑ Guest users should be allowed to do self service
□ Guest users should be allowed to do device registration
□ Vlan Dhcp Release (Note: Release should occur prior to the CoA. Renew should be set to

The DefaultGuestPortal refers to the portal used for self-registration—otherwise known as the Self-Registration portal in this document.

To specify how the portal authenticates users, select the Authentication tab within the particular portal, as shown in Figure 10-5, and select the appropriate option:

- Guest—The portal authenticates guest user accounts stored in the local database.
- Central WebAuth—The user is authenticated against the databases specified in the Identity Store Sequence.
- Both—The user is authenticated against a local guest database first. If the user is not found, authentication is attempted using additional databases defined in the Identity Store Sequence.

Figure 10-5 Authentication Portal Settings

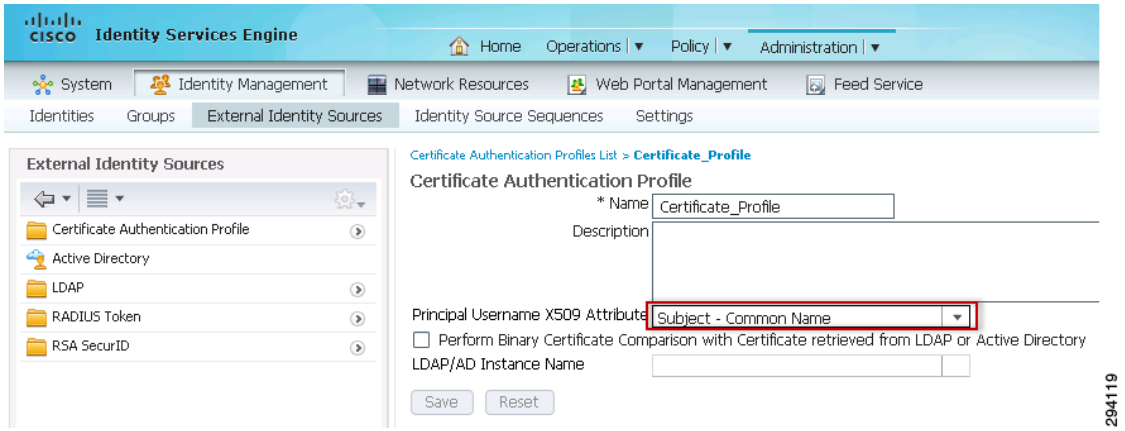


* Identity Store Sequence All_Stores_Sequence

ISE Using Certificates as an Identity Store

To configure ISE to use certificates as an identity store, choose **Administration > External Identity Sources > Certificate Authentication Profile > Add** and define the Certificate Authentication Profile, as shown in Figure 10-6.

Figure 10-6 Certificate Authentication Profile


cisco Identity Services Engine
Home
Operations
Policy
Administration
System
Identity Management
Network Resources
Web Portal Management
Feed Service
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Certificate Authentication Profiles List > Certificate_Profile
Certificate Authentication Profile
Save
Reset
294119

* Name Certificate_Profile

Description

Principal Username X509 Attribute Subject - Common Name

□ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

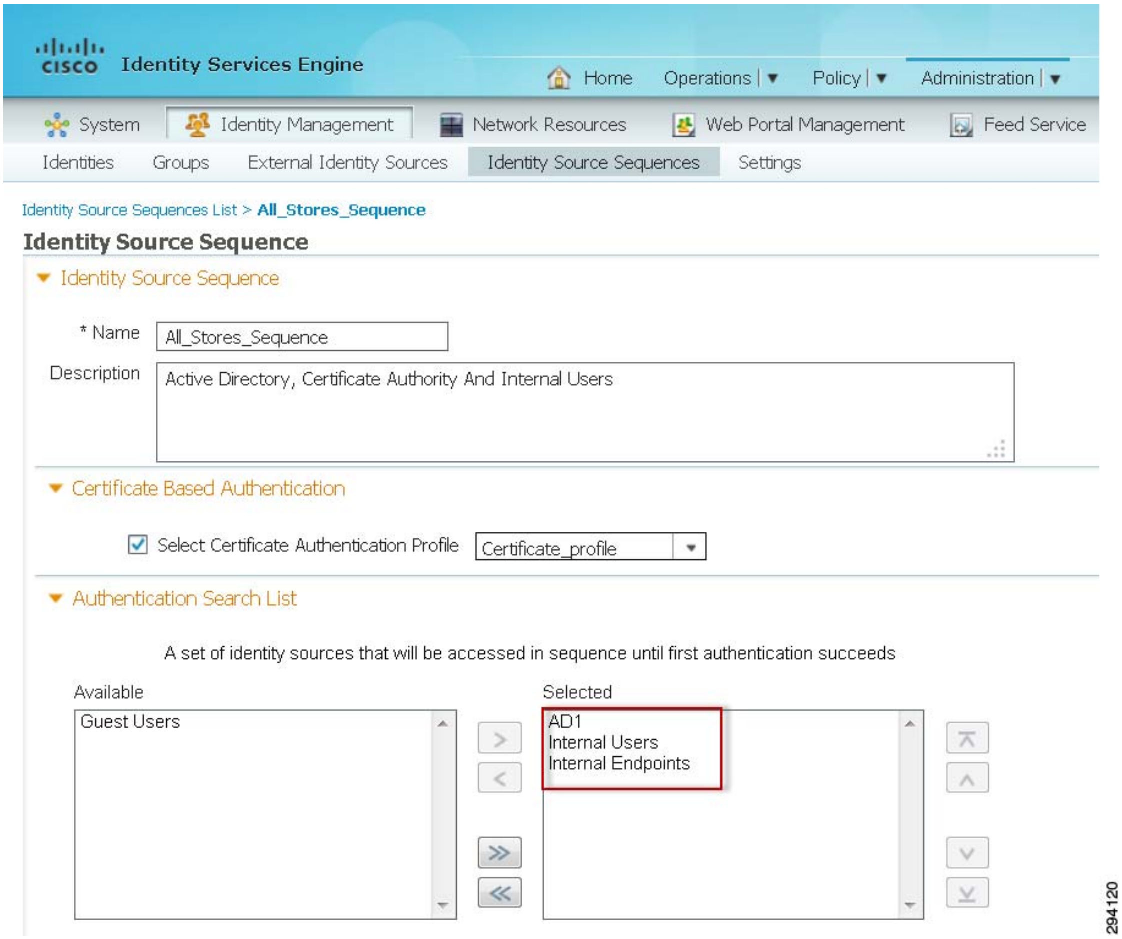
LDAP/AD Instance Name

Identity Source Sequences

Identity Source Sequences define the order in which ISE will look for user credentials in the different databases. These databases include Internal Users, Active Directory, LDAP, RSA, etc.

To add a new Identity Source Sequence, click **Administration > Identity Source Sequences > Add**. The configuration shown in Figure 10-7 creates a new Identity Source Sequence named All_Stores_Sequence. It relies on Active Directory (AD1), a certificate profile named "Certificate_profile" and Internal Users.

Figure 10-7 Identity Source Sequence



* Name: All_Stores_Sequence

Description: Active Directory, Certificate Authority And Internal Users

☑ Select Certificate Authentication Profile: Certificate_profile

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: Guest Users

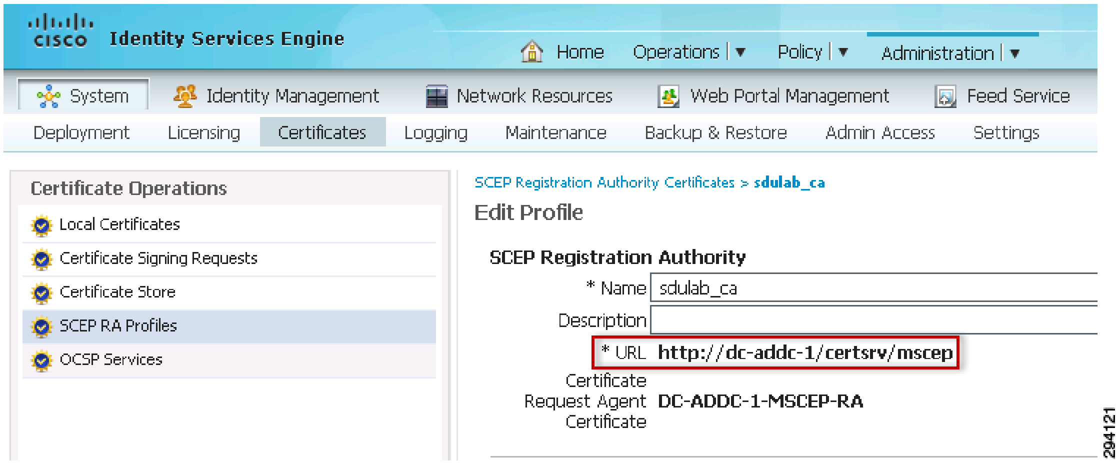
Selected: AD1, Internal Users, Internal Endpoints

SCEP Profile Configuration on ISE

Within this design, ISE is acting as a Simple Certificate Enrollment Protocol (SCEP) proxy server, thereby allowing mobile clients to obtain their digital certificates from the CA server. This important feature of ISE allows all endpoints, such as iOS, Android, Windows, and MAC, to obtain digital certificates through the ISE. This feature combined with the initial registration process greatly simplifies the provisioning of digital certificates on endpoints.

To configure SCEP profile on the ISE, click **Administration > Certificates > SCEP RA Profiles > Add**. Define the SCEP profile, as shown in Figure 10-8.

Figure 10-8 SCEP Profile Configuration



SCEP Registration Authority

* Name: sdulab_ca

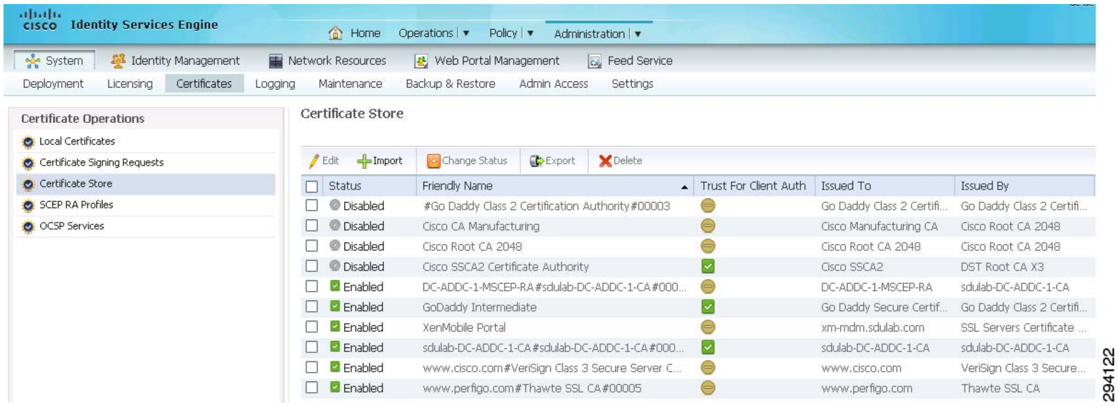
Description:

* URL: http://dc-addc-1/certsrv/mscep

Certificate Request Agent Certificate: DC-ADDC-1-MSCEP-RA

After the configuration is successful, ISE downloads the RA certificate and the root CA certificate of the CA server, as shown in Figure 10-9.

Figure 10-9 Certificate Store



□	Status	Friendly Name	Trust For Client Auth	Issued To	Issued By
□	Disabled	#Go Daddy Class 2 Certification Authority#00003	⊖	Go Daddy Class 2 Certifi...	Go Daddy Class 2 Certifi...
□	Disabled	Cisco CA Manufacturing	⊖	Cisco Manufacturing CA	Cisco Root CA 2048
□	Disabled	Cisco Root CA 2048	⊖	Cisco Root CA 2048	Cisco Root CA 2048
□	Disabled	Cisco SSCA2 Certificate Authority	☑	Cisco SSCA2	DST Root CA X3
□	Enabled	DC-ADDC-1-MSCEP-RA#sdulab-DC-ADDC-1-CA#000...	⊖	DC-ADDC-1-MSCEP-RA	sdulab-DC-ADDC-1-CA
□	Enabled	GoDaddy Intermediate	☑	Go Daddy Secure Certif...	Go Daddy Class 2 Certifi...
□	Enabled	XenMobile Portal	⊖	xm-mdm.sdulab.com	SSL Servers Certificate ...
□	Enabled	sdulab-DC-ADDC-1-CA#sdulab-DC-ADDC-1-CA#000...	☑	sdulab-DC-ADDC-1-CA	sdulab-DC-ADDC-1-CA
□	Enabled	www.cisco.com#VeriSign Class 3 Secure Server C...	⊖	www.cisco.com	VeriSign Class 3 Secure...
□	Enabled	www.perfigo.com#Thawte SSL CA#00005	⊖	www.perfigo.com	Thawte SSL CA

Authentication Policies

Authentication policies are used to define the protocols used by the ISE to communicate with the endpoints and the identity sources to be used for authentication. ISE evaluates the conditions and based on whether the result is true or false, it applies the configured result. An authentication policy includes:

- An allowed protocol service, such as PEAP, EAP-TLS, etc.
- An identity source used for authentication

Similar to the way access lists are processed, authentication rules are processed from the top down. When the first condition is met, processing stops and the assigned identity rule is used.

The rules are evaluated using "If, then, else" logic:

```
IF Wired_802.1X   Then
     Allow default protocols
Elseif   next condition
     Take action
```

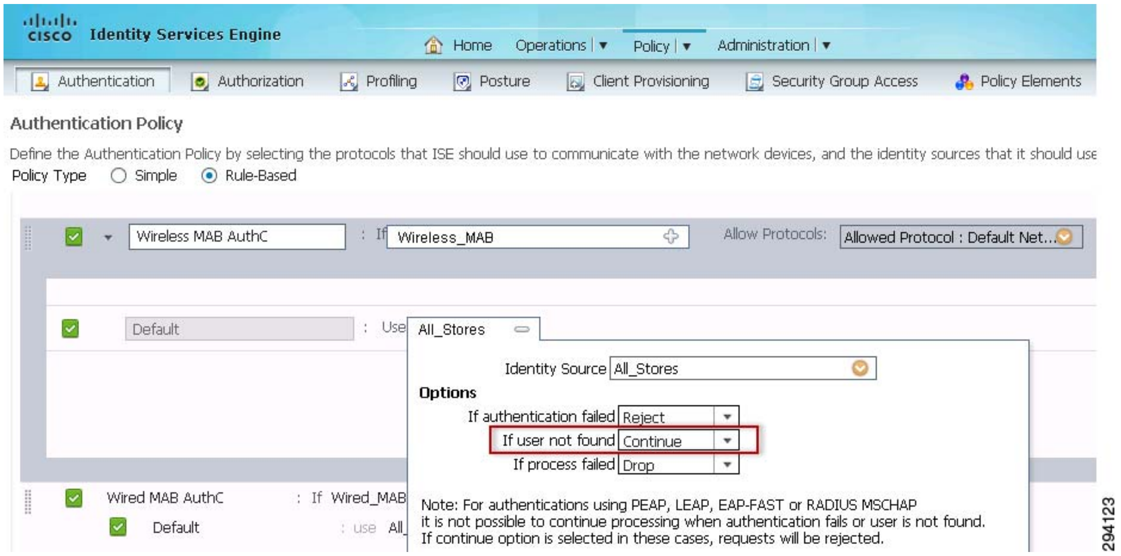
```
Else
     Use Default Rule
```

In BYOD designs discussed throughout this document, ISE authenticates several protocols such as MAB and dot1x against all the Identity Stores. The Identity Stores could be AD, Certificate_Profile, RSA, Internal Users, and Internal Endpoints. The network access medium could be wired, wireless, or remote connection. The network device uses any of the mediums mentioned before, using different protocols to connect to ISE.

MAC Authentication Bypass (MAB) protocol is used to authenticate devices not configured with dot1x. When a brand new device accesses the network it communicates via the MAB protocol and uses its own MAC address as its identity. In a normal scenario, ISE would validate if the MAC address is present in any of its identity stores; if not, it would reject the connection. However in this BYOD design the MAB protocol is used by new devices for on-boarding purposes and it may not be feasible to know the MAC address of the device in advance.

To circumvent this problem, ISE continues the authentication process and redirects the device to the next stage, even if the device's MAC address is not present in any of its identity stores. Figure 10-10 highlights this configuration.

Figure 10-10 Authentication Rule for MAB



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use

Policy Type ○ Simple ● Rule-Based

☑ Wireless MAB AuthC : If Wireless_MAB Allow Protocols: Allowed Protocol : Default Net...

☑ Default : Use All_Stores

Identity Source All_Stores

Options

If authentication failed Reject

If user not found Continue

If process failed Drop

☑ Wired MAB AuthC : If Wired_MAB

☑ Default : use All_

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP
it is not possible to continue processing when authentication fails or user is not found.
If continue option is selected in these cases, requests will be rejected.

In a normal deployment scenario, the endpoints would primarily use the dot1x protocol to communicate with ISE. ISE authenticates these endpoints against an Active Directory or authenticates them via digital certificates. Figure 10-11 depicts the different protocols and how these protocols use different identity stores for authentication.

Figure 10-11 Authentication Policy

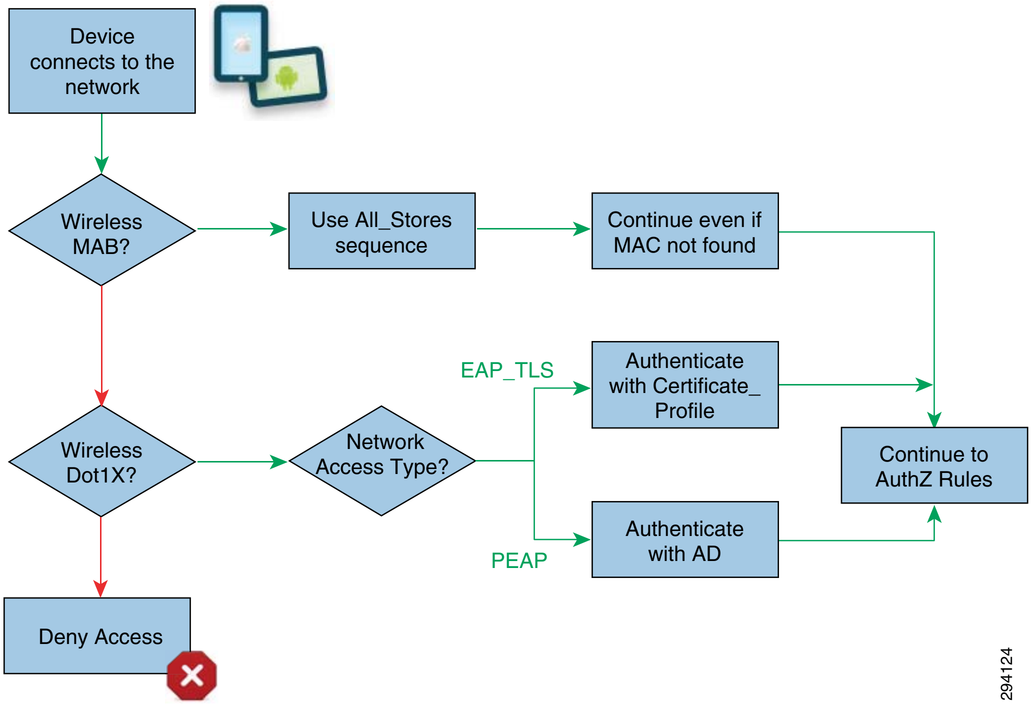


Table 10-1 explains how these rules are implemented in this design guide.

Table 10-1 Authentication Rules

Rule Name	Network Access Medium	Allowed Protocols	Conditions		Identity Store
Wireless MAB AuthC	Wireless MAB	All	Default		All_Stores
Wired MAB AuthC	Wired MAB	All	Default		All_Stores
Wireless Dot1X AuthC	Wireless_8021X	All	Wireless Certificate	EAP_TLS	Certificate_Profile
			Wireless Password	PEAP	All_Stores
Wired Dot1X AuthC	Wired_802.1X	All	Wired Certificate	EAP_TLS	Certificate_Profile
			Wired Password	PEAP	All_Stores
Default					Deny Access

Authentication Policy for Wireless

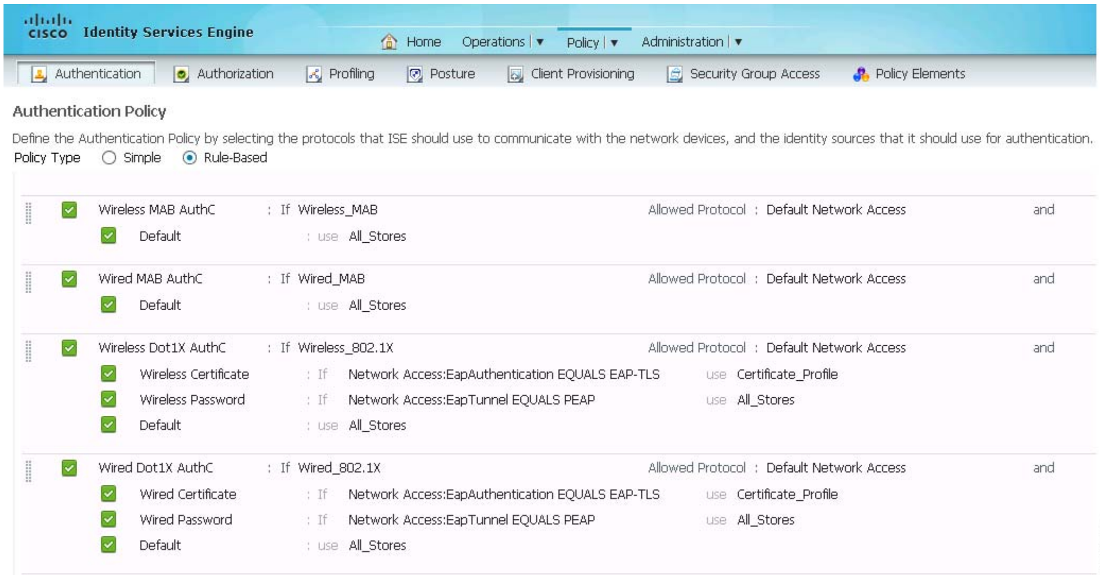
The endpoint devices could use either MAB or dot1x protocol when connecting to the wireless network. The authentication policy for wireless networks using MAB is explained in the previous section. This section explains the authentication policy for wireless medium using dot1X protocol, as shown in Table 10-1.

Wireless Dot1X AuthC is the rule name for wireless_dot1x protocol. This rule matches wireless_dot1x protocol and has two inner rules:

- Wireless Certificate—Matches when the authentication protocol is EAP_TLS and it verifies the digital certificate using the identity store Certificate_Profile.
- Wireless Password—Matches on the PEAP authentication protocol and uses the All_Stores identity store, which includes Active Directory.

Figure 10-12 shows how these rules were configured on the ISE for this design guide.

Figure 10-12 Authentication Rules



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑	Wireless MAB AuthC	: If Wireless_MAB	Allowed Protocol : Default Network Access		and
☑	Default	: use All_Stores			
☑	Wired MAB AuthC	: If Wired_MAB	Allowed Protocol : Default Network Access		and
☑	Default	: use All_Stores			
☑	Wireless Dot1X AuthC	: If Wireless_802.1X	Allowed Protocol : Default Network Access		and
☑	Wireless Certificate	: If Network Access:EapAuthentication EQUALS EAP-TLS		use Certificate_Profile	
☑	Wireless Password	: If Network Access:EapTunnel EQUALS PEAP		use All_Stores	
☑	Default	: use All_Stores			
☑	Wired Dot1X AuthC	: If Wired_802.1X	Allowed Protocol : Default Network Access		and
☑	Wired Certificate	: If Network Access:EapAuthentication EQUALS EAP-TLS		use Certificate_Profile	
☑	Wired Password	: If Network Access:EapTunnel EQUALS PEAP		use All_Stores	
☑	Default	: use All_Stores			

Client Provisioning

The Cisco ISE looks at various elements when classifying the end user's device type, including operating system version, browser type, etc. Once the ISE classifies the client machine, it uses client provisioning resource policies to ensure that the client is configured with an appropriate agent version, up-to-date compliance modules and correct agent customization packages and profiles, if necessary. The ISE Profiling service is discussed in Enabling the DHCP and RADIUS Probes. It is important to understand the difference between Client Provisioning Policy and Client Provisioning Resources. Client Provisioning Resources are basically the resources that are pushed to the end device and assist the end device in completing the on-boarding process. Client Provisioning Resources are of two types:

- Native profiles that can be configured on ISE; for example, iOS profile.
- Software Provisioning Wizards that must be downloaded from Cisco site.

Client Provisioning Policy on the other hand links an endpoint device to an appropriate Client Provisioning Resource. Therefore the Client Provisioning Resources must be added to the ISE before configuring the Client Provisioning Policy. This section discusses Client Provisioning Resources and Client Provisioning Policies for iOS, Android, Windows and Mac OS X devices.

The following are considerations for client provisioning on the endpoints:

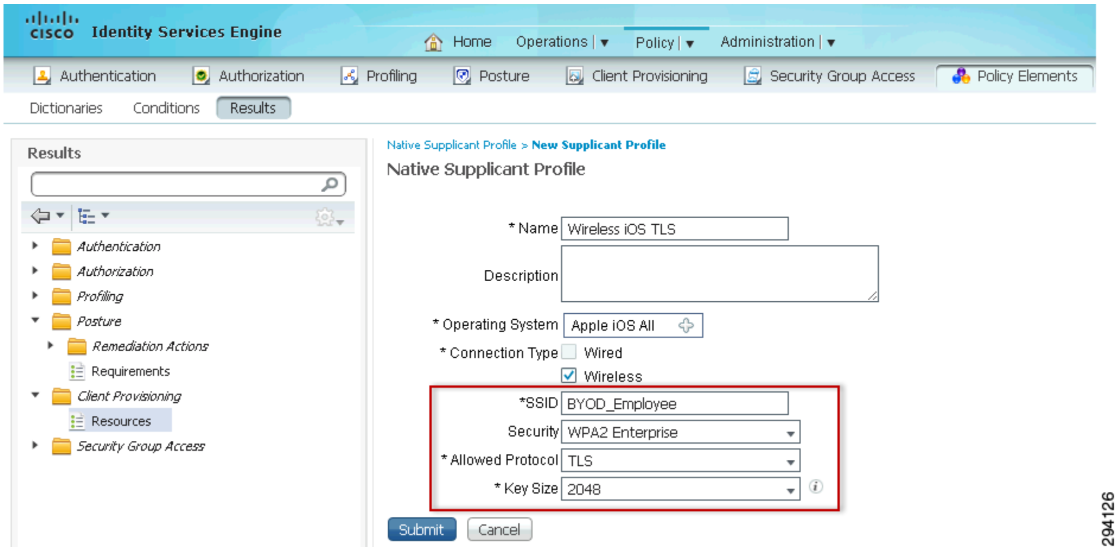
- Based on the endpoint, push an appropriate Software Provisioning Wizard (SPW) to the device. This Wizard configures the dot1x settings on the endpoint and configures the endpoint to obtain a digital certificate.

- In certain endpoints such as iOS devices, there is no need for SPW package because for iOS devices the native operating system is used to configure the dot1x settings.
- For Android devices, the SPW package needs to be downloaded from Google Play Store.

Client Provisioning Resources—Apple iOS and Android

To configure a client provisioning resource for mobile devices, click **Policy > Policy Elements > Results > Client Provisioning > Resources > Add Native Supplicant Profile**. Figure 10-13 shows the configuration details for the Wireless iOS TLS profile used by Apple iOS devices. This profile is used to configure the parameters required to access to the BYOD_Employee SSID after on-boarding.

Figure 10-13 Wireless iOS TLS Profile



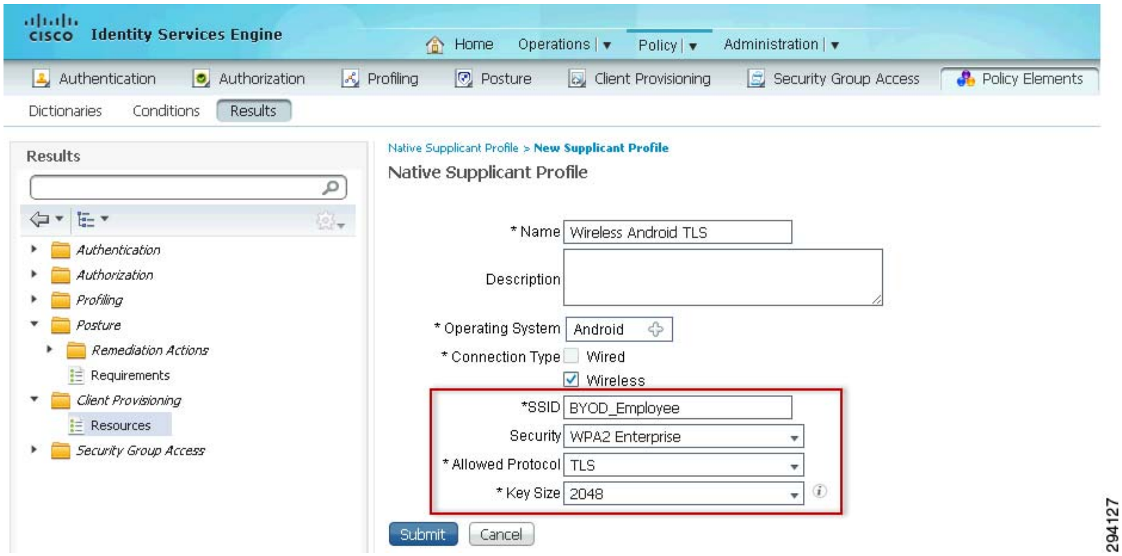
Native Supplicant Profile > **New Supplicant Profile**

Native Supplicant Profile

* Name	Wireless iOS TLS
Description	
* Operating System	Apple iOS All
* Connection Type	☐ Wired ☑ Wireless
*SSID	BYOD_Employee
Security	WPA2 Enterprise
* Allowed Protocol	TLS
* Key Size	2048

Figure 10-14 shows the configuration details for the Wireless Android TLS profile used by Android devices.

Figure 10-14 Wireless Android TLS



Native Supplicant Profile

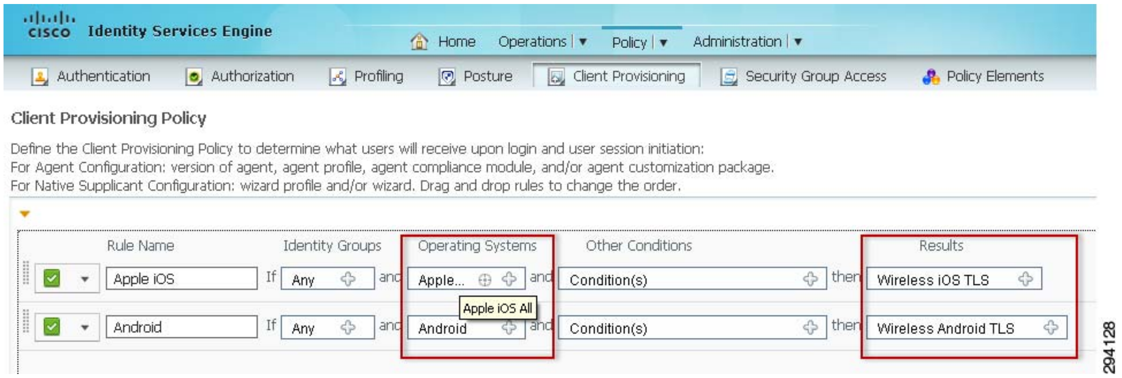
- * Name: Wireless Android TLS
- Description:
- * Operating System: Android
- * Connection Type: ☐ Wired ☑ Wireless
- *SSID: BYOD_Employee
- Security: WPA2 Enterprise
- * Allowed Protocol: TLS
- * Key Size: 2048

Client Provisioning Policy—Apple iOS and Android Devices

Client provisioning policies determine which users receive which version of resources. After defining the Native Supplicant Profile, the next step is to use the appropriate profile when devices connect to the network by clicking **Policy > Client Provisioning**.

The configuration in Figure 10-15 determines the operating system running on the device and defines which resources to distribute. In this case the previously defined profiles are distributed based on the appropriate operating system.

Figure 10-15 Client Provisioning Policies



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	Apple iOS	If	Any	and	Apple...	and	Condition(s)	then	Wireless iOS TLS
☑	Android	If	Any	and	Android	and	Condition(s)	then	Wireless Android TLS

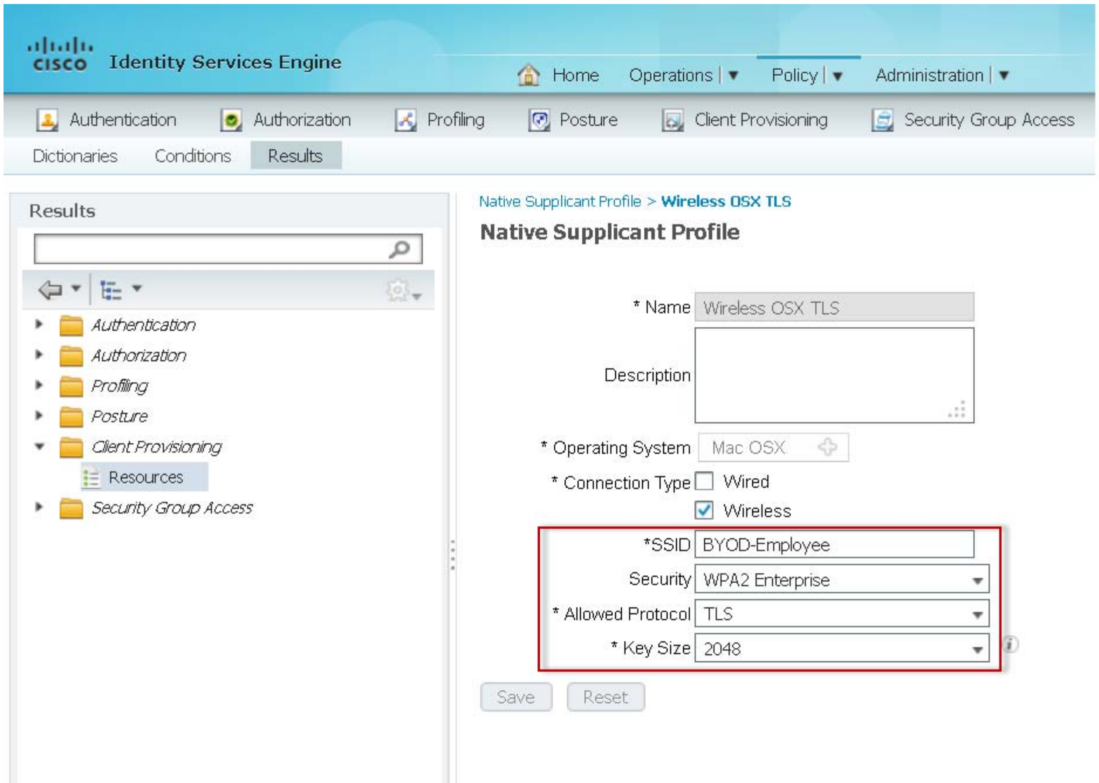
It is important to note that for Android devices the user is also required to download the software from Google's Play Store, since it cannot be distributed by ISE.

Client Provisioning Resources—Mac OS

For MAC OS workstations, the following is required:

- A Native Supplicant profile that determines what kind of configuration should be provisioned on the device, for example the Wireless SSID name. Figure 10-16 shows the native supplicant profile for Mac OSX devices.

Figure 10-16 Native Supplicant Profile for Mac OSX Devices



Native Supplicant Profile

* Name: Wireless OSX TLS

Description:

* Operating System: Mac OSX

* Connection Type: ☐ Wired ☑ Wireless

*SSID: BYOD-Employee

Security: WPA2 Enterprise

* Allowed Protocol: TLS

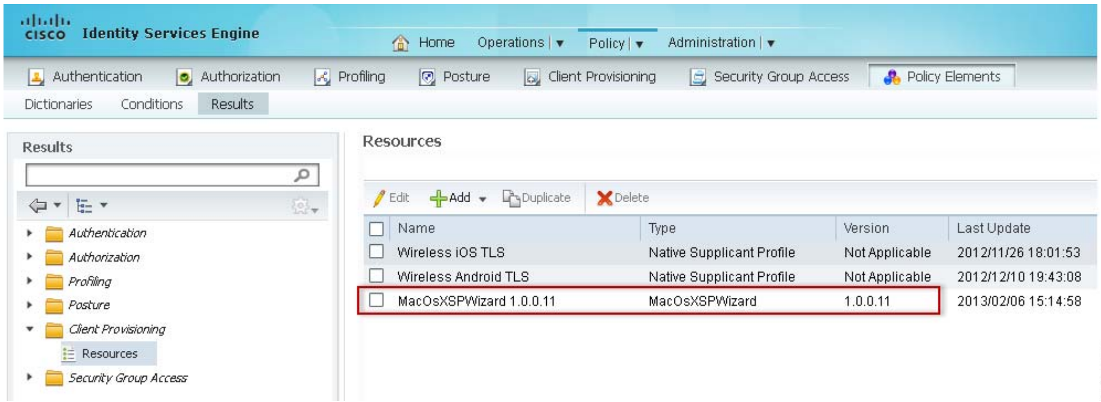
* Key Size: 2048

Save Reset

- A Wizard Profile—The Supplicant Provisioning Wizard profile is a software agent that may be downloaded from Cisco.

To define the client provisioning resources, click **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > Agent Resources** from the Cisco site and select the **MacOsXSPWizard**. Figure 10-17 shows the MacOsXSPWizard profile.

Figure 10-17 Mac OsXSPWizard Profile



Resources

	Name	Type	Version	Last Update
☐	Wireless iOS TLS	Native Supplicant Profile	Not Applicable	2012/11/26 18:01:53
☐	Wireless Android TLS	Native Supplicant Profile	Not Applicable	2012/12/10 19:43:08
☐	MacOsXSPWizard 1.0.0.11	MacOsXSPWizard	1.0.0.11	2013/02/06 15:14:58

Client Provisioning Policy for Mac OS Devices—Wireless

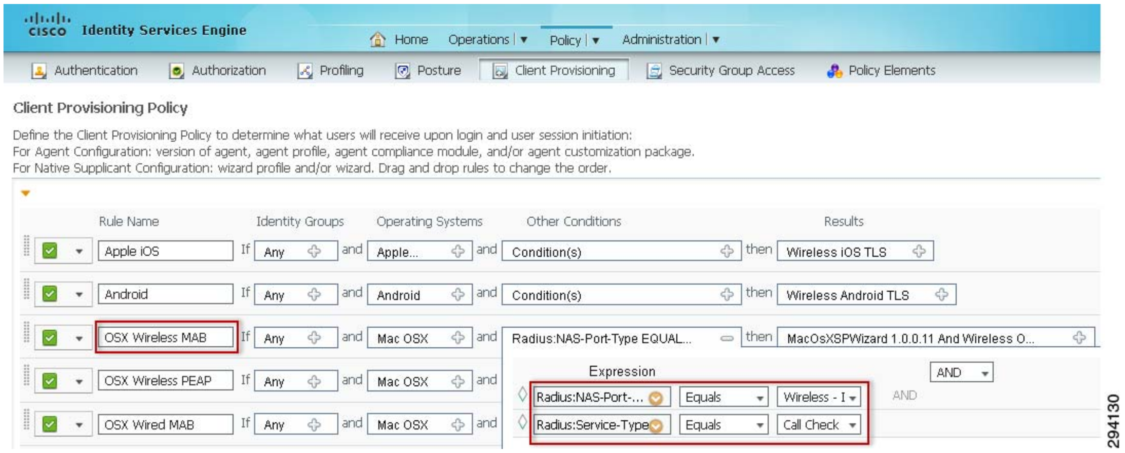
The previous section discussed the resources needed for provisioning Mac OS devices. Once the resources have been configured, the next step is to define under what conditions these resources will be used. The Mac OS X devices can use either MAB or PEAP protocol during the provisioning process. Therefore different conditions have to be configured to match either one of them.

The MAB protocol is matched by the following two conditions:

- RADIUS:NAS-Port-Type EQUALS Wireless—IEEE 802.11
- RADIUS:Service-Type EQUALS Call Check

Figure 10-18 shows the Client Provisioning Policy to match on the MAB protocol.

Figure 10-18 Client Provisioning Policy for MAB



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	Apple iOS	If	Any	and	Apple...	and	Condition(s)	then	Wireless iOS TLS
☑	Android	If	Any	and	Android	and	Condition(s)	then	Wireless Android TLS
☑	OSX Wireless MAB	If	Any	and	Mac OSX	and	Radius:NAS-Port-Type EQUAL...	then	MacOsXSPWizard 1.0.0.11 And Wireless O...
☑	OSX Wireless PEAP	If	Any	and	Mac OSX	and			
☑	OSX Wired MAB	If	Any	and	Mac OSX	and			

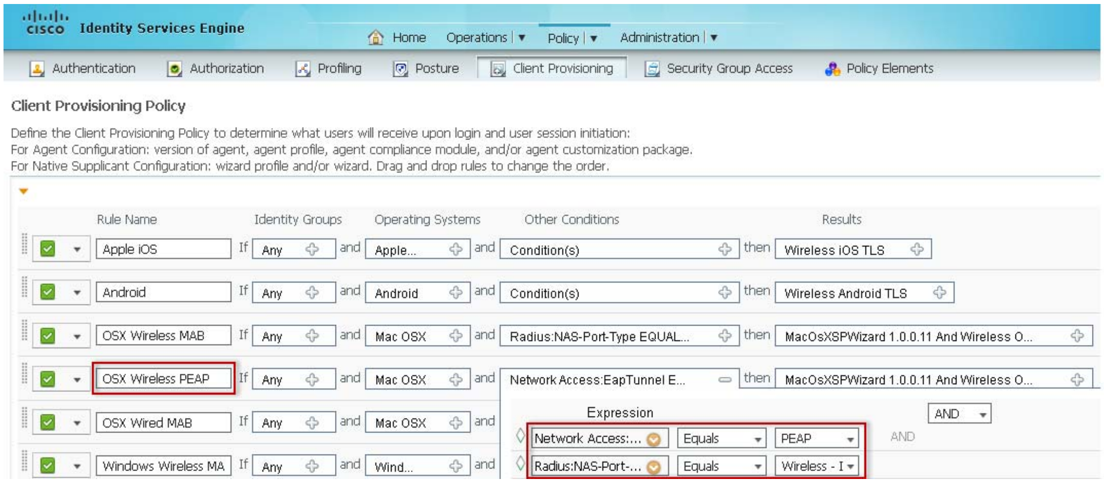
Expression			AND
Radius:NAS-Port-...	Equals	Wireless - I	AND
Radius:Service-Type	Equals	Call Check	

To match a Mac device using the PEAP protocol, the following conditions are needed:

- RADIUS:NAS-Port-Type EQUALS Wireless—IEEE 802.11
- Network Access:EapTunnel EQUALS PEAP

Figure 10-19 shows the condition to match on MAC devices using the PEAP protocol.

Figure 10-19 Client Provisioning Policy for PEAP



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
Apple iOS	If	Any	and	Apple...	and	Condition(s)	then	Wireless iOS TLS
Android	If	Any	and	Android	and	Condition(s)	then	Wireless Android TLS
OSX Wireless MAB	If	Any	and	Mac OSX	and	Radius:NAS-Port-Type EQUAL...	then	MacOsXSPWizard 1.0.0.11 And Wireless O...
OSX Wireless PEAP	If	Any	and	Mac OSX	and	Network Access:EapTunnel E...	then	MacOsXSPWizard 1.0.0.11 And Wireless O...
OSX Wired MAB	If	Any	and	Mac OSX	and			
Windows Wireless MA	If	Any	and	Wind...	and			

Expression — AND

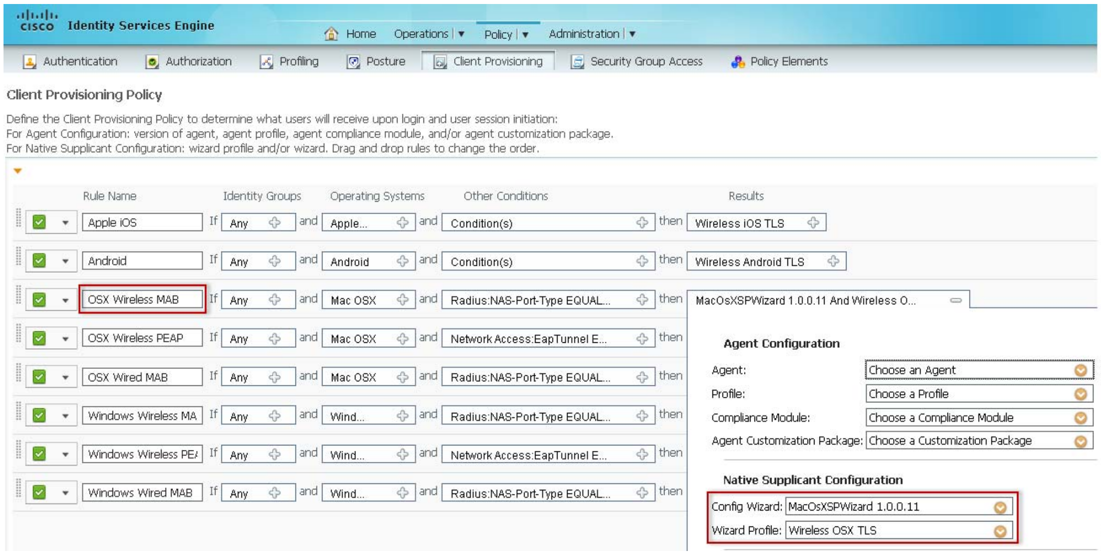
Network Access:...	Equals	PEAP	AND
Radius:NAS-Port-...	Equals	Wireless - I	

To complete a Client Provisioning policy for MAC_OSX_Wireless devices, the following must be defined:

- The Operating System must be selected as Mac OSX.
- The Conditions should be used to match either MAB or PEAP protocol.
- The result section must contain the Native Supplicant profile and the SPW for Mac OS X devices.

The complete policy is shown in Figure 10-20.

Figure 10-20 Client Provisioning Policy for Mac OS X



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
Apple iOS	If	Any	and	Apple...	and	Condition(s)	then	Wireless iOS TLS
Android	If	Any	and	Android	and	Condition(s)	then	Wireless Android TLS
OSX Wireless MAB	If	Any	and	Mac OSX	and	Radius:NAS-Port-Type EQUAL...	then	MacOsXSPWizard 1.0.0.11 And Wireless O...
OSX Wireless PEAP	If	Any	and	Mac OSX	and	Network Access:EapTunnel E...	then	
OSX Wired MAB	If	Any	and	Mac OSX	and	Radius:NAS-Port-Type EQUAL...	then	
Windows Wireless MA	If	Any	and	Wind...	and	Radius:NAS-Port-Type EQUAL...	then	
Windows Wireless PE/	If	Any	and	Wind...	and	Network Access:EapTunnel E...	then	
Windows Wired MAB	If	Any	and	Wind...	and	Radius:NAS-Port-Type EQUAL...	then	

Agent Configuration

Agent: Choose an Agent
Profile: Choose a Profile
Compliance Module: Choose a Compliance Module
Agent Customization Package: Choose a Customization Package

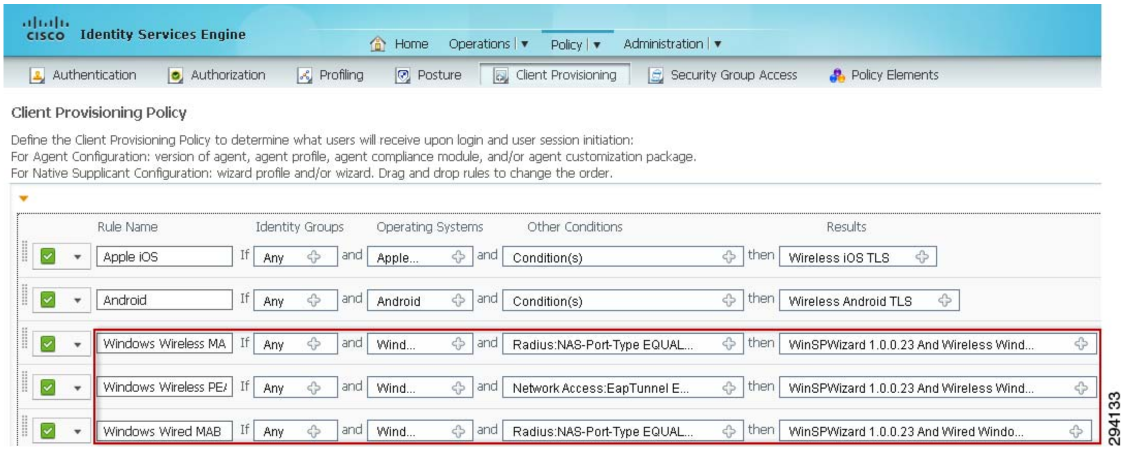
Native Supplicant Configuration

Config Wizard: MacOsXSPWizard 1.0.0.11
Wizard Profile: Wireless OSX TLS

Client Provisioning Policy for Windows Devices—Wireless/Wired

The configuration steps for defining the provisioning policy for Windows devices is very similar to Mac OS X or iOS devices, so the same configuration steps are not repeated here. The only difference to point out is that for Windows devices a different SPW package is needed. Figure 10-21 depicts the Client Provisioning Policy for Windows (wireless or wired) devices using either MAB or PEAP.

Figure 10-21 Client Provisioning Policy for Windows



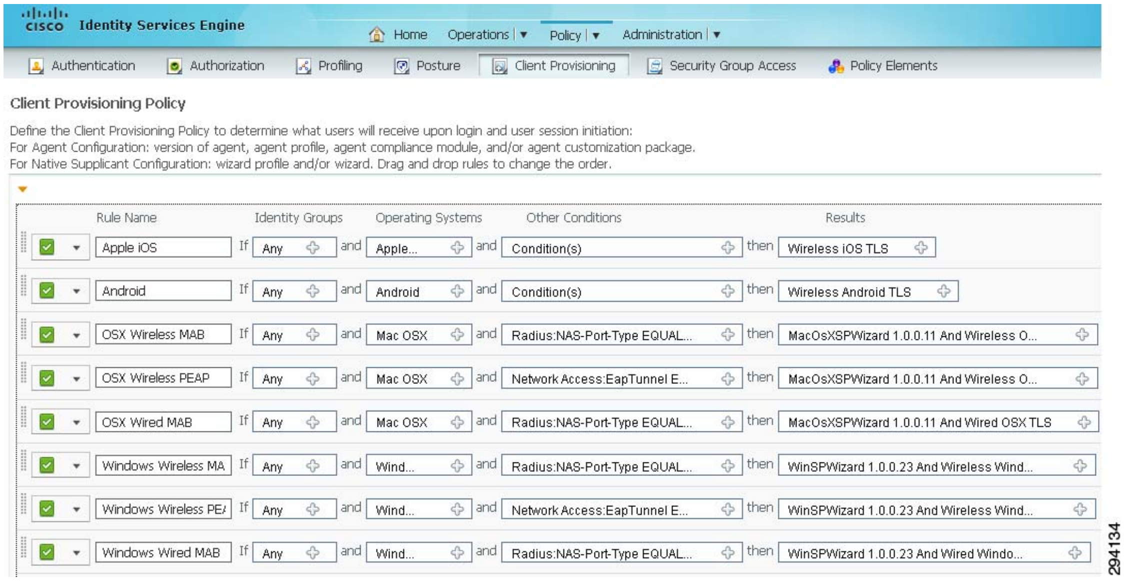
Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
Apple iOS	If	Any	and	Apple...	and	Condition(s)	then	Wireless iOS TLS
Android	If	Any	and	Android	and	Condition(s)	then	Wireless Android TLS
Windows Wireless MA	If	Any	and	Wind...	and	Radius:NAS-Port-Type EQUAL...	then	WinSPWizard 1.0.0.23 And Wireless Wind...
Windows Wireless PE/	If	Any	and	Wind...	and	Network Access:EapTunnel E...	then	WinSPWizard 1.0.0.23 And Wireless Wind...
Windows Wired MAB	If	Any	and	Wind...	and	Radius:NAS-Port-Type EQUAL...	then	WinSPWizard 1.0.0.23 And Wired Windo...

Figure 10-22 shows the complete client provisioning policy used during testing.

Figure 10-22 Complete Client Provisioning Policy



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
Apple iOS	If	Any	and	Apple...	and	Condition(s)	then	Wireless iOS TLS
Android	If	Any	and	Android	and	Condition(s)	then	Wireless Android TLS
OSX Wireless MAB	If	Any	and	Mac OSX	and	Radius:NAS-Port-Type EQUAL...	then	MacOsXSPWizard 1.0.0.11 And Wireless O...
OSX Wireless PEAP	If	Any	and	Mac OSX	and	Network Access:EapTunnel E...	then	MacOsXSPWizard 1.0.0.11 And Wireless O...
OSX Wired MAB	If	Any	and	Mac OSX	and	Radius:NAS-Port-Type EQUAL...	then	MacOsXSPWizard 1.0.0.11 And Wired OSX TLS
Windows Wireless MA	If	Any	and	Wind...	and	Radius:NAS-Port-Type EQUAL...	then	WinSPWizard 1.0.0.23 And Wireless Wind...
Windows Wireless PE/	If	Any	and	Wind...	and	Network Access:EapTunnel E...	then	WinSPWizard 1.0.0.23 And Wireless Wind...
Windows Wired MAB	If	Any	and	Wind...	and	Radius:NAS-Port-Type EQUAL...	then	WinSPWizard 1.0.0.23 And Wired Windo...

Profiling

Profiling is a key service responsible for identifying, locating, and determining the capabilities of endpoints that attach to the network to deny or enforce specific authorization rules. Two of the main profiling capabilities include:

- Collector—Used to collect network packets from network devices and forward attribute values to the analyzer.
- Analyzer—Used to determine the device type by using configured policies that match attributes.

There are two main methods to collect endpoint information:

- The ISE acting as the collector and analyzer.
- Starting in version 7.3, the WLC can act as the collector and send the required attributes to the ISE, which acts as the analyzer.

Client profiling from a controller running 7.3 or later is supported on access points that are in Local mode and FlexConnect mode. Table 10-2 shows the main differences between the WLC and ISE profiling.

Table 10-2 ISE versus WLC Profiling Support

ISE	WLC
Profiling using a large number of probes, including RADIUS, DHCP, DHCP SPAN, HTTP, DNS, etc.	DHCP and HTTP based profiling only
ISE supports as policy action multiple different attributes	WLC supports VLAN, ACL, session timeout, QoS
Profiling rules may be customized with user-defined attributes	Only default profiling rules may be used

Note This design guide uses the profiling capabilities of the ISE and did not test the controller client profiling capabilities.

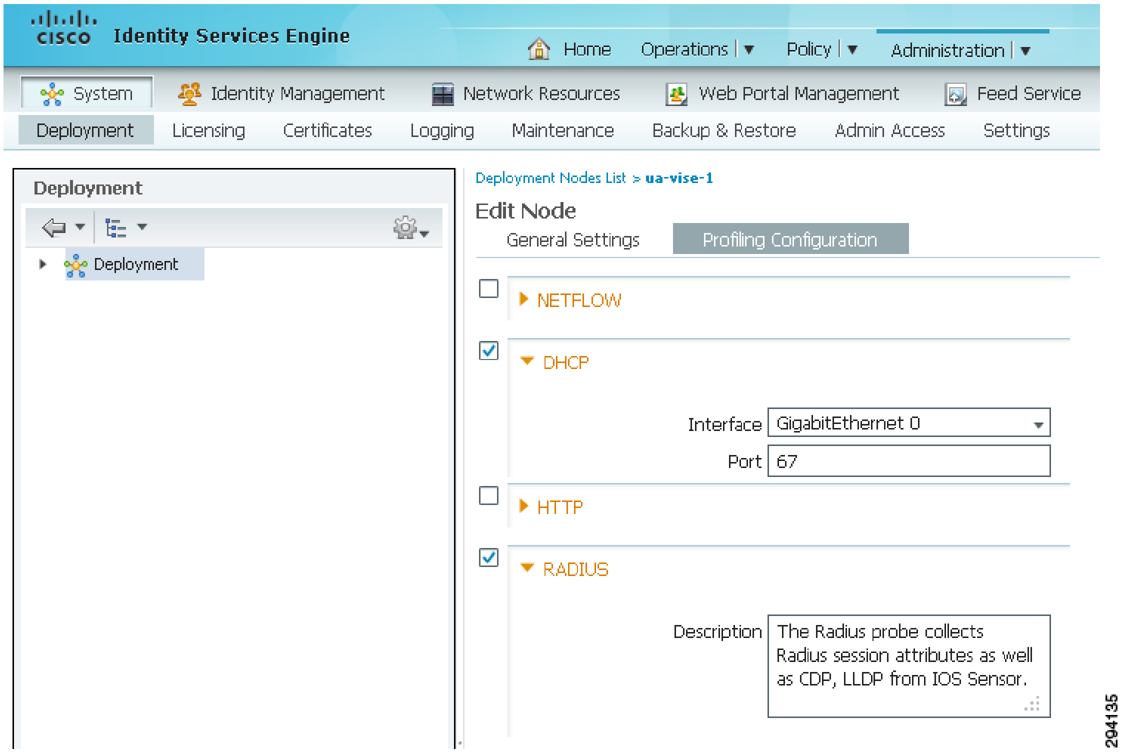
The ISE supports a number of sensors to capture endpoint attributes and classify them according to their profiles. The sensors rely on a number of probes that capture network packets by querying network access devices. Once the endpoints are profiled, different authentication and authorization policies may be enforced. Some examples of using different policies based on the device's profile include:

- Allow employee-owned iPads to access the network, but only for HTTP traffic.
- If the iOS device connecting to the network is a company-owned device, grant full access to the network.
- If an employee-owned iPad has been provisioned with a digital certificate, grant full access to the network.
- Force some devices to register with their Mobile Device Manager.
- Deny access to all iPads or Android devices.

Enabling the DHCP and RADIUS Probes

To enable profiling on the ISE, click **Administration > System > Deployment**. Click the ISE hostname and click **Profiling Configuration**. Enable the appropriated probes to listen to packets forwarded from the LAN switch or Wireless LAN Controller, as shown in Figure 10-23.

Figure 10-23 Profiling Probes



□ NETFLOW

☑ DHCP

Interface GigabitEthernet 0
Port 67

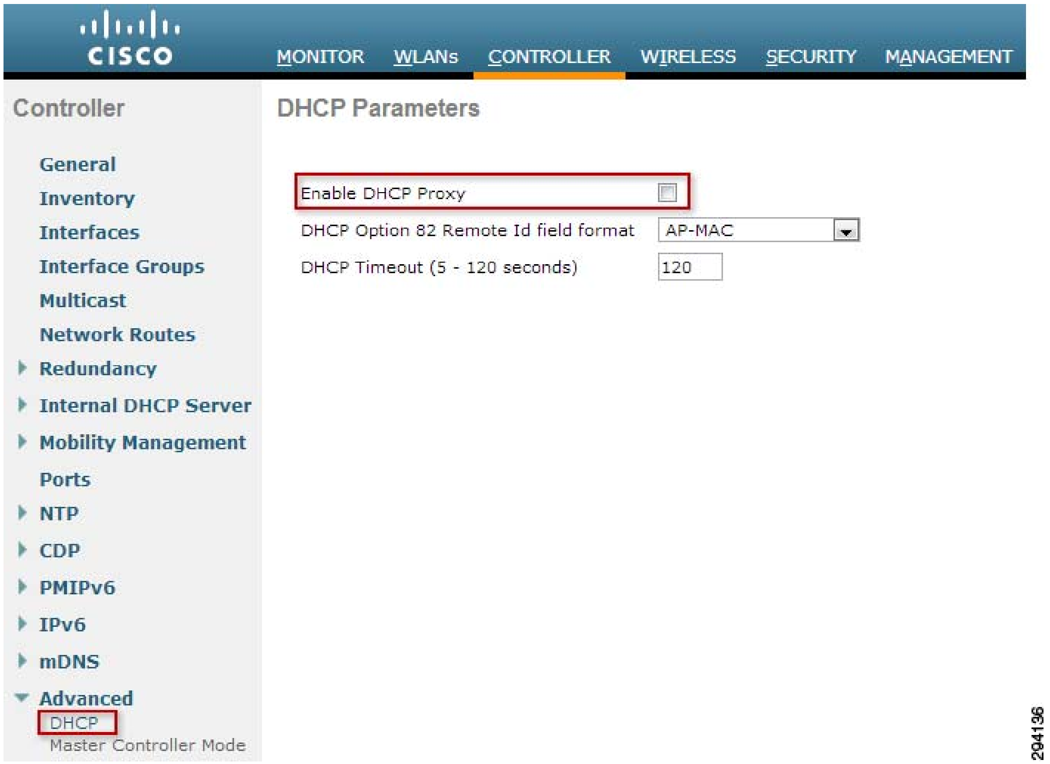
□ HTTP

☑ RADIUS

Description The Radius probe collects Radius session attributes as well as CDP, LLDP from IOS Sensor.

The Wireless LAN Controller should be configured in DHCP bridging mode to forward DHCP packets from the wireless endpoints to the ISE. Click **Controller > Advanced > DHCP** and clear the Enable DHCP Proxy check box, as shown in Figure 10-24.

Figure 10-24 Disable DHCP Proxy



DHCP Parameters

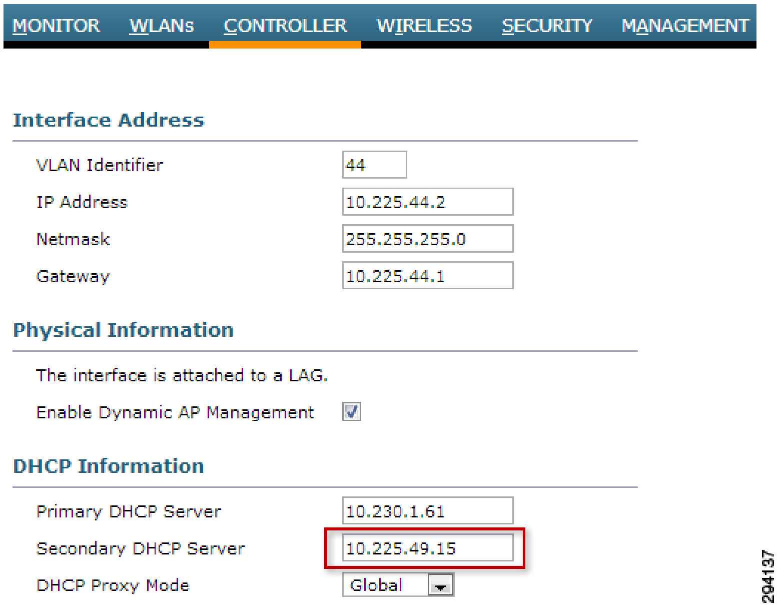
Enable DHCP Proxy □

DHCP Option 82 Remote Id field format AP-MAC

DHCP Timeout (5 - 120 seconds) 120

Specify the ISE’s IP address as the secondary DHCP server in the WLC by clicking **Controller > Interfaces > Secondary DHCP**, as shown in Figure 10-25.

Figure 10-25 Secondary DHCP Server



Interface Address

VLAN Identifier	44
IP Address	10.225.44.2
Netmask	255.255.255.0
Gateway	10.225.44.1

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management ☑

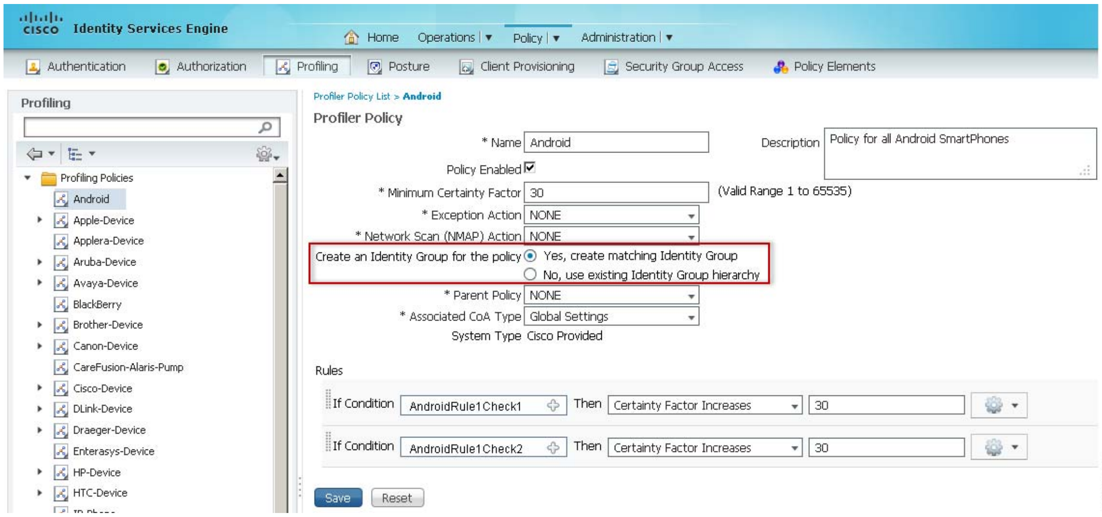
DHCP Information

Primary DHCP Server	10.230.1.61
Secondary DHCP Server	10.225.49.15
DHCP Proxy Mode	Global

Profiling Android Devices

To create an identity group based on the Android policy, click **Policy > Profiling > Profiling Policies > Android** and enable the Create Matching Identity Group, as shown in Figure 10-26.

Figure 10-26 Android Profiling Policy



Profiler Policy List > Android

Profiler Policy

* Name: Android

Description: Policy for all Android SmartPhones

Policy Enabled ☑

* Minimum Certainty Factor: 30 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: ● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy

* Parent Policy: NONE

* Associated CoA Type: Global Settings

System Type: Cisco Provided

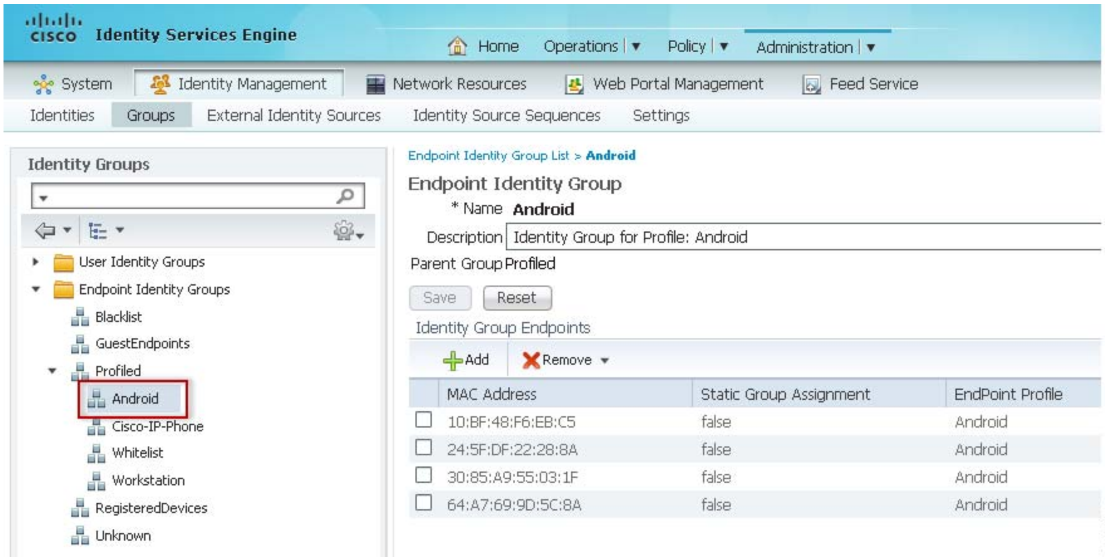
Rules

If Condition AndroidRule1Check1 Then Certainty Factor Increases 30

If Condition AndroidRule1Check2 Then Certainty Factor Increases 30

The Android profiling policy should be listed under Endpoint Identity Groups > Profiled. Click **Administration > Identity Management > Groups** to see a list of Android devices that have been profiled by the ISE, as shown in Figure 10-27.

Figure 10-27 Android Identity Group



Endpoint Identity Group List > Android

Endpoint Identity Group

* Name: Android

Description: Identity Group for Profile: Android

Parent Group: Profiled

Identity Group Endpoints

	MAC Address	Static Group Assignment	EndPoint Profile
□	10:BF:48:F6:EB:C5	false	Android
□	24:5F:DF:22:28:8A	false	Android
□	30:85:A9:55:03:1F	false	Android
□	64:A7:69:9D:5C:8A	false	Android

Logical Profiles

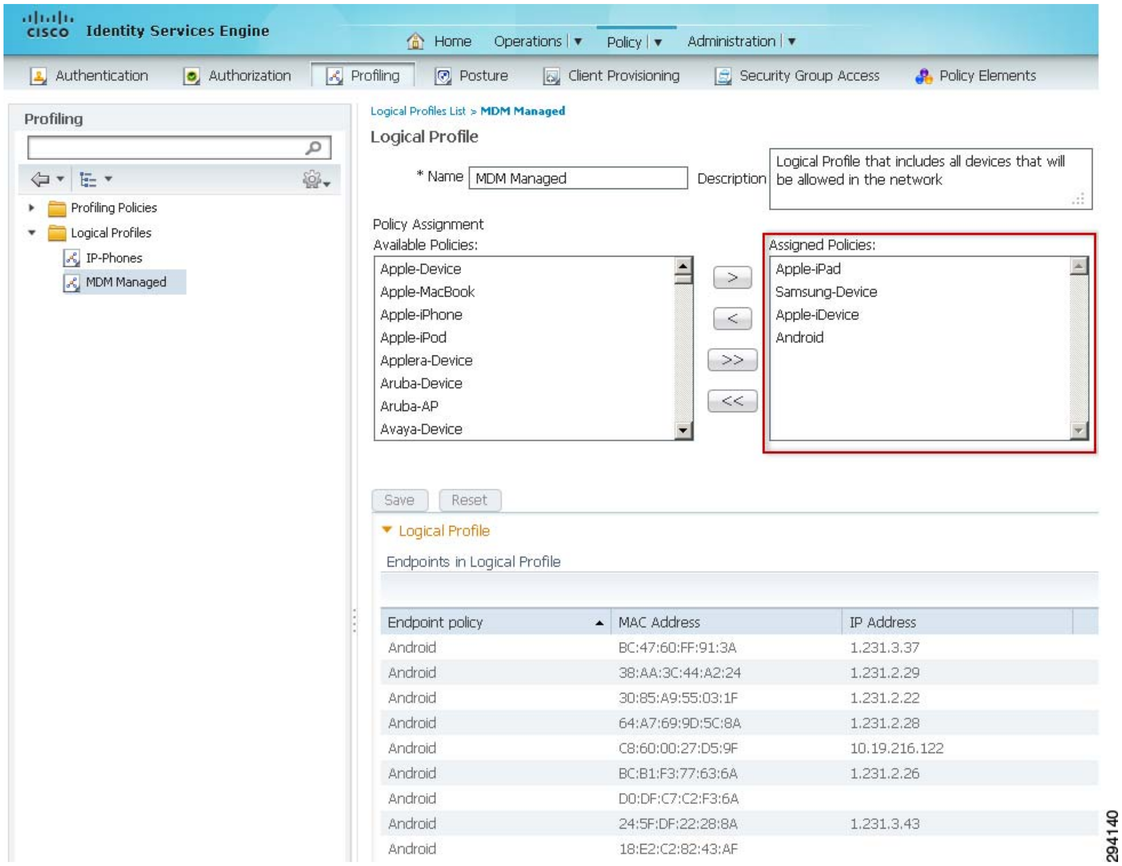
Logical profiles are containers that group different profiles to create an overall category of profiles. Logical profiles provide additional flexibility to the authorization policies, enhancing the overall network access policy.

With logical profiles, a single entry in the authorization rule is able to include several profiles. Before logical profiles were available, a matching identity groups had to be created for each device type.

In this design guide, a logical profile was created to group the mobile devices that are managed by the MDM. This profile combines some mobile devices into a single logical profile that may be invoked from the authorization rules.

To create a logical profile, click **Policy > Profiling > Profiling > Logical Profiles**, as shown in Figure 10-28.

Figure 10-28 MDM Managed Logical Profile



Logical Profiles List > MDM Managed

Logical Profile

* Name: MDM Managed

Description: Logical Profile that includes all devices that will be allowed in the network

Policy Assignment

Available Policies:
Apple-Device
Apple-MacBook
Apple-iPhone
Apple-iPod
Applera-Device
Aruba-Device
Aruba-AP
Avaya-Device

Assigned Policies:
Apple-iPad
Samsung-Device
Apple-iDevice
Android

Logical Profile

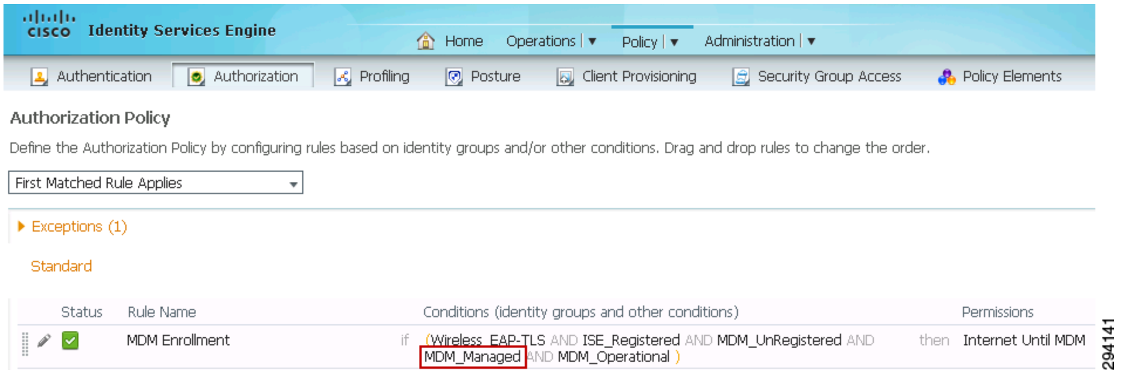
Endpoints in Logical Profile

Endpoint policy	MAC Address	IP Address
Android	BC:47:60:FF:91:3A	1.231.3.37
Android	38:AA:3C:44:A2:24	1.231.2.29
Android	30:85:A9:55:03:1F	1.231.2.22
Android	64:A7:69:9D:5C:8A	1.231.2.28
Android	C8:60:00:27:D5:9F	10.19.216.122
Android	BC:B1:F3:77:63:6A	1.231.2.26
Android	D0:DF:C7:C2:F3:6A	
Android	24:5F:DF:22:28:8A	1.231.3.43
Android	18:E2:C2:82:43:AF	

This logical profile provides the flexibility to add new devices at any time without modifying the authorization rules. Figure 10-29 shows how the MDM Managed Logical Profile is used to identify devices supported by the MDM.

This and other authorization rules are explained in more detail later in this design guide.

Figure 10-29 MDM Enrollment Authorization Rule



Authorization Policy

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

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	MDM Enrollment	if	(Wireless_EAP-TLS AND ISE_Registered AND MDM_UnRegistered AND MDM_Managed AND MDM_Operational)	then	Internet Until MDM

Authorization Policies and Profiles

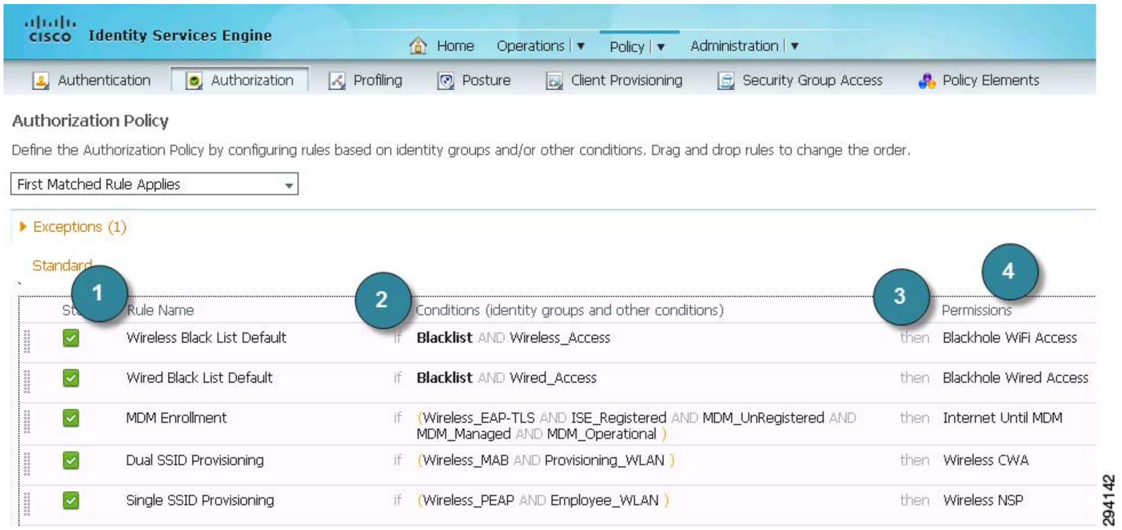
Authorization policies define the overall security policy to access the network. Network authorization controls user access to the network and its resources and what each device can do on the system with those resources. An Authorization Policy is composed of multiple rules.

Authorization rules are defined by three main elements, as shown in Figure 10-30:

- Names (1)
- Conditions (2)
- Permissions (3)
- Authorization Profiles (4)

Permissions are enforced by authorization profiles (4). Similar to the authentication rules, authorization rules are processed from the top down. When the first condition is met, processing stops and the assigned permission dictates what authorization profile to use.

Figure 10-30 Authorization Policy



Authorization Policy

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

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Wireless Black List Default	if	Blacklist AND Wireless_Access	then	Blackhole WiFi Access
☑	Wired Black List Default	if	Blacklist AND Wired_Access	then	Blackhole Wired Access
☑	MDM Enrollment	if	(Wireless_EAP-TLS AND ISE_Registered AND MDM_UnRegistered AND MDM_Managed AND MDM_Operational)	then	Internet Until MDM
☑	Dual SSID Provisioning	if	(Wireless_MAB AND Provisioning_WLAN)	then	Wireless CWA
☑	Single SSID Provisioning	if	(Wireless_PEAP AND Employee_WLAN)	then	Wireless NSP

Authorization Profiles

An authorization profile acts as a container where a number of specific permissions allow access to a set of network services. The authorization profile is where a set of permissions to be granted is defined and can include:

- An associated VLAN.
- An associated downloadable ACL (DACL).
- Wireless LAN Controller attributes such as the use of a Named ACL or Security Group Tag for policy enforcement.
- Advanced settings using attributes contained in dictionaries.

In addition to the standard PermitAccess and DenyAccess authorization profiles, the following are some of the profiles that are defined within this design guide:

- Wireless CWA—This profile is used for redirection of wireless devices to the registration portal for devices using MAB and dual SSIDs.
- Wireless NSP—This profile is used to redirect wireless users to the registration portal when they access the network using dot1x or a single SSID.
- Blackhole WiFi Access—Used to block access to devices reported lost (for more information, see Chapter 22, "Managing a Lost or Stolen Device").

Several other authorization profiles are explained in other chapters of this design guide.

Note Cisco has been made aware of potential incompatibilities introduced by Apple iOS 7. We are working to understand the limitations and design updates will be made to this publication.

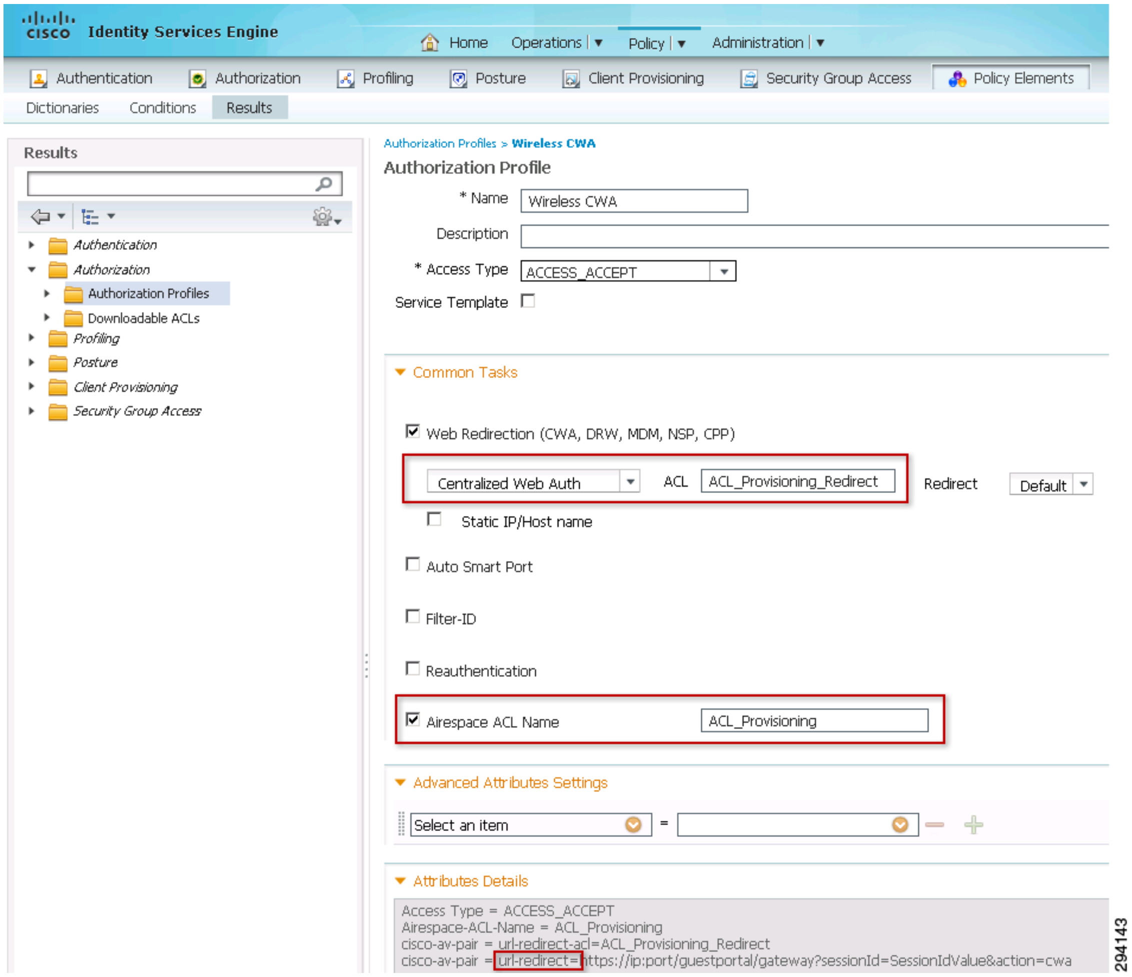
Wireless CWA Authorization Profile for Dual SSID Provisioning

This policy is used in dual SSID configurations to redirect wireless devices to the Self-Registration portal upon connecting to the network. This authorization profile restricts access by triggering the ACL_Provisioning_Redirect access list, which is defined in advance in the Wireless LAN Controller.

When implementing dual SSIDs, the provisioning SSID can be either open or password-protected with Active Directory credentials. In this design guide, the provisioning SSID is open and relies on MAC Authentication Bypass (MAB) to grant access to the network.

To configure this authorization policy, click **Policy > Policy Elements > Results > Authorization Profiles**, as shown in Figure 10-31.

Figure 10-31 Wireless CWA Authorization Profile



Authorization Profile

* Name: Wireless CWA
Description:
* Access Type: ACCESS_ACCEPT
Service Template □

☑ Web Redirection (CWA, DRW, MDM, NSP, CPP)
Centralized Web Auth ACL ACL_Provisioning_Redirect Redirect Default
□ Static IP/Host name
□ Auto Smart Port
□ Filter-ID
□ Reauthentication
☑ Airespace ACL Name ACL_Provisioning

```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = ACL_Provisioning
cisco-av-pair = url-redirect-acl=ACL_Provisioning_Redirect
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

To force devices to the self-registration portal, a redirect URL is created with a unique Session ID and pushed to the device:

https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

When the user launches a web browser, the device is redirected to the Self-Registration portal. To prevent the user from staying connected to the provisioning SSID, the ACL_Provisioning_Redirect ACL only permits access to the Cisco ISE, DHCP, and Domain Name System (DNS) services.

The Wireless CWA authorization profile relies on two named ACLs previously defined in the Wireless LAN Controller:

- ACL_Provisioning_Redirect—Applied to the Centralized Web Auth setting.
- ACL_Provisioning—Sent to the wireless controller via the Radius:Airespace-ACL-Name attribute value (AV).

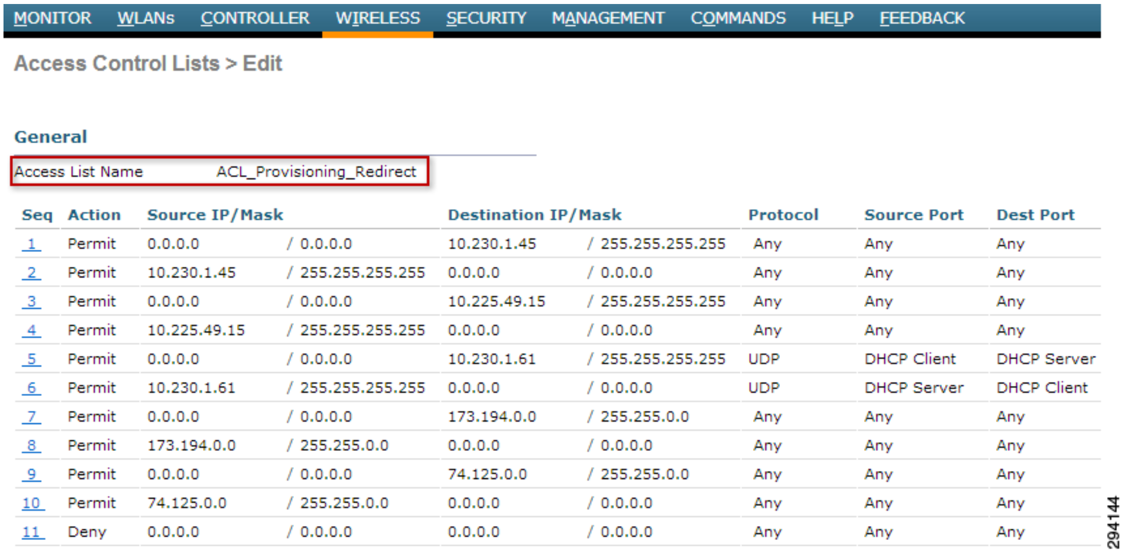
The behavior of the two ACLs is slightly different between wireless controllers:

- For CUWN wireless controllers (e.g., CT5508 and Flex 7500), ACL_Provisioning_Redirect functions as both the ACL which controls web redirection and as the ACL which controls access on the network. ACL_Provisioning serves simply as an extra security configuration and is not used when URL redirection is specified. For CUWN wireless controllers the ACL_Provisioning _Redirect ACL shown in Figure 10-32 can be the same as the ACL_Provisioning.

- For Cisco IOS XE based wireless controllers (e.g., CT5760 and Catalyst 3850), ACL_Provisioning_Redirect functions strictly as the ACL which controls web redirection. ACL_Provisioning functions as the ACL, which controls what the wireless client is allowed to access on the network. Hence IOS XE based wireless controllers make use of both ACLs when URL redirection is specified.

Figure 10-32 displays the configuration for ACL_Provisioning_Redirect on the WLC. This is just an example, since each organization will have unique business policies and security requirements.

Figure 10-32 WLC Access List for Provisioning



Access Control Lists > Edit

General

Access List Name ACL_Provisioning_Redirect

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	173.194.0.0	/ 255.255.0.0	Any	Any	Any
8	Permit	173.194.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	74.125.0.0	/ 255.255.0.0	Any	Any	Any
10	Permit	74.125.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

The ACL_Provisioning_Redirect ACL specifies the following access:

- Allow IP access to and from the DNS server (10.230.1.45).
- Allow IP access to and from the ISE Server (10.225.49.15).
- Allow IP access to and from the DHCP server (10.230.1.61).
- Access to Google Play.

Note Android devices require access to the Google Play Store to download the SPW package. Modify the ACL to allow endpoints to download the SPW. Analyzing the DNS transactions between the DNS server and the device is one approach to develop and troubleshoot ACL_Provisioning_Redirect.

On the Catalyst 3850 or the CT5760 Controller, the ACL_Provisioning_Redirect is defined as follows:

```
ip access-list extended ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 permit tcp any any eq www
 permit tcp any any eq 443
```

The ACL_Provisioning_Redirect ACL specifies the following access:

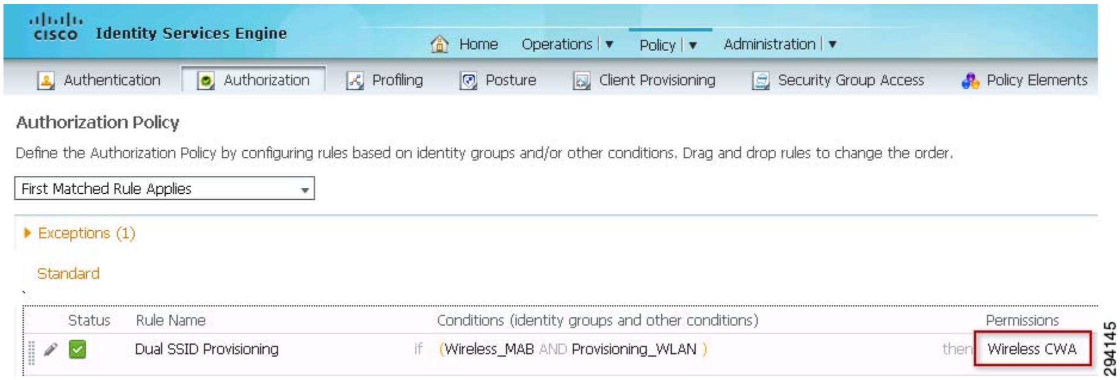
- Deny (do not redirect) IP access to and from the DNS server (10.230.1.45).

- Deny (do not redirect) IP access to and from the ISE Server (10.225.49.15).
- Deny (do not redirect) DHCP Access (bootpc and bootps).
- Permit (redirect) TCP access to any web host.
- Permit (redirect) TCP access to any secure web host.
- Deny (do not redirect) all other access to the Internet.

Dual SSID Provisioning Authorization Rule

The Dual SSID Provisioning rule links the Wireless CWA authorization profile to the conditions that authorize MAB devices into the Provisioning SSID, as shown in Figure 10-33. It includes two conditions: Wireless_MAB and Provisioning_WLAN.

Figure 10-33 Dual SSID Authorization Rule



Authorization Policy

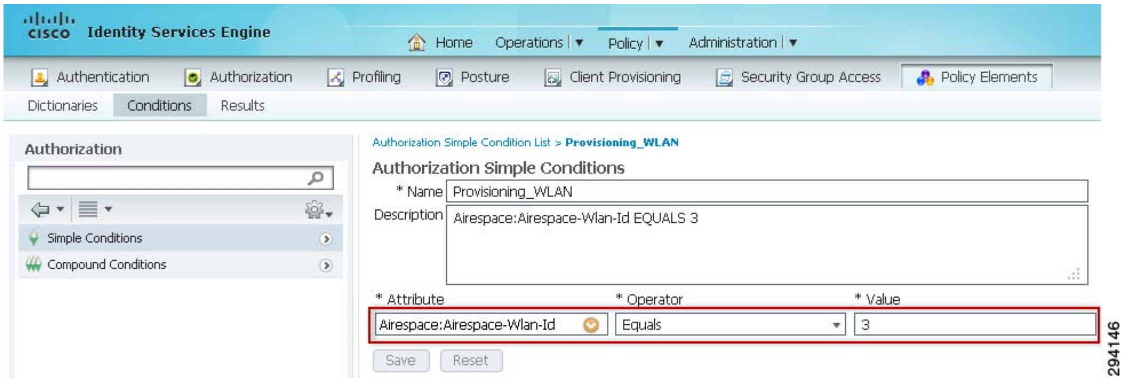
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Dual SSID Provisioning	if (Wireless_MAB AND Provisioning_WLAN)	then Wireless CWA

The Wireless_MAB condition is a predefined condition in ISE, while the Provisioning_WLAN condition was defined from the menu **Policy > Conditions > Simple Conditions**, as shown in Figure 10-34.

Figure 10-34 Provisioning_WLAN Condition



Authorization Simple Condition List > **Provisioning_WLAN**

Authorization Simple Conditions

* Name: Provisioning_WLAN

Description: Airespace:Airespace-Wlan-Id EQUALS 3

* Attribute	* Operator	* Value
Airespace:Airespace-Wlan-Id	Equals	3

For the purposes of this CVD, the BYOD_Provisioning SSID number was defined as 3 during testing. The simple condition Provisioning_WLAN matches when the SSID number is 3. The condition is created to improve readability of the rules.

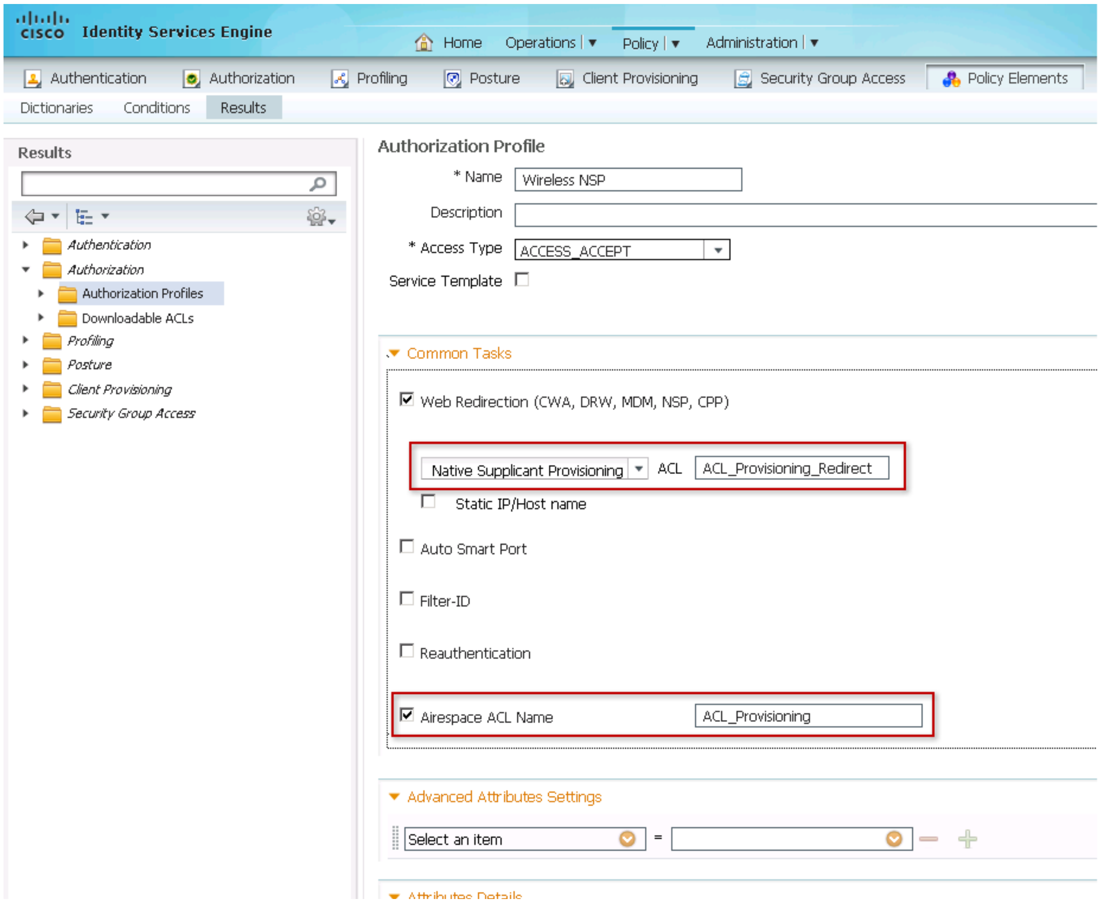
Wireless NSP Authorization Profile for Single SSID Provisioning

The native supplicant flow starts similarly regardless of device type by redirecting employees using a supported personal device to the Guest portal where they are required to enter their user credentials. From there, they are redirected to the Self-Provisioning portal to confirm their device information.

The Wireless NSP authorization profile is used in single SSID configurations to redirect devices to the Guest portal using the PEAP authentication protocol.

To configure this authorization policy, click **Policy > Policy Elements > Results > Authorization Profiles**, as shown in Figure 10-35.

Figure 10-35 Wireless NSP Authorization Profile



Authorization Profile

* Name: Wireless NSP

Description:

* Access Type: ACCESS_ACCEPT

Service Template: □

Common Tasks

☑ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Native Supplicant Provisioning ACL ACL_Provisioning_Redirect

□ Static IP/Host name

□ Auto Smart Port

□ Filter-ID

□ Reauthentication

☑ Airespace ACL Name ACL_Provisioning

Advanced Attributes Settings

Select an item =

The Wireless NSP authorization profile relies on two named ACLs previously defined in the Wireless LAN Controller:

- ACL_Provisioning_Redirect—Applied to the Centralized Web Auth setting.
- ACL_Provisioning—Sent to the wireless controller via the Radius:Airespace-ACL-Name attribute value (AV).

The behavior of the two ACLs is slightly different between wireless controllers:

- For CUWN wireless controllers (e.g., CT5508 and Flex 7500), ACL_Provisioning_Redirect functions as both the ACL which controls web redirection and as the ACL which controls access on the network. ACL_Provisioning serves simply as an extra security configuration and is not used when URL redirection is specified. For CUWN wireless controllers the ACL_Provisioning _Redirect ACL shown in Figure 10-32 can be the same as the ACL_Provisioning.
- For Cisco IOS XE based wireless controllers (e.g., CT5760 and Catalyst 3850), ACL_Provisioning_Redirect functions strictly as the ACL which controls web redirection. ACL_Provisioning functions as the ACL which controls what the wireless client is allowed to access on the network. Hence IOS XE based wireless controllers make use of both ACLs when URL redirection is specified.

Single SSID Provisioning Authorization Rule

The Single SSID Provisioning rule links the Wireless NSP authorization profile to the conditions that authorize wireless devices authenticating via PEAP.

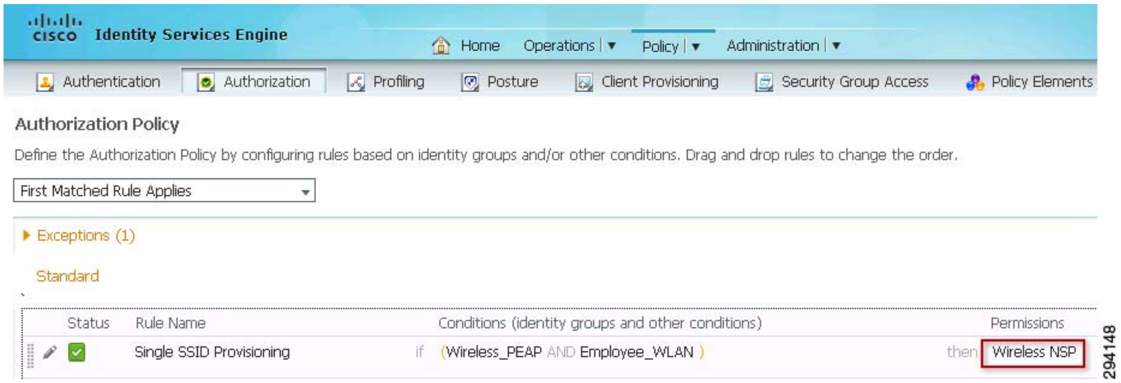
To force devices to the self-registration portal, a redirect URL is created with a unique Session ID and pushed to the device:

https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp

When the user launches a web browser, the device is redirected to the Self-Registration portal.

Figure 10-36 shows the authorization rule defined under the authorization policies. This rule includes two conditions: Wireless_PEAP and Employee_WLAN.

Figure 10-36 Single SSID Provisioning Authorization Rule



Authorization Policy

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

First Matched Rule Applies

Exceptions (1)

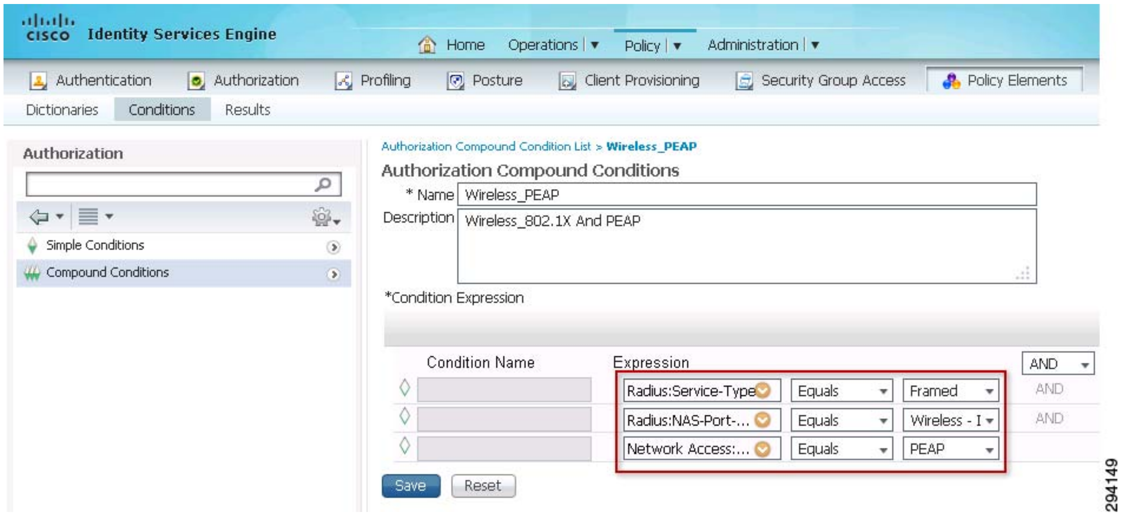
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Single SSID Provisioning	if	(Wireless_PEAP AND Employee_WLAN)	then	Wireless NSP

Figure 10-37 shows the Wireless_PEAP compound condition in ISE, which includes these expressions:

- Radius:Service-Type Equals Framed
- Radius:NAS-Port-Type Equals Wireless—IEEE 802.11
- Network Access: EapTunnel Equals PEAP

Figure 10-37 Wireless_PEAP Compound Condition



* Name Wireless_PEAP

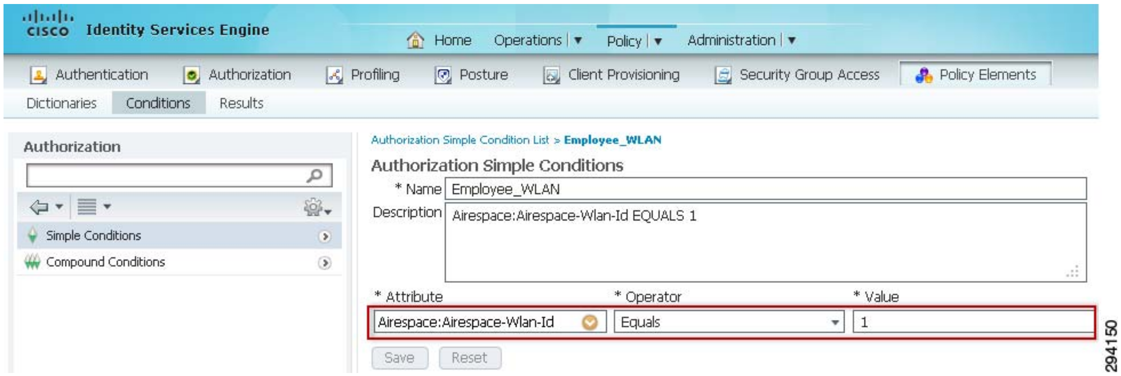
Description Wireless_802.1X And PEAP

*Condition Expression

Expression			AND
Radius:Service-Type	Equals	Framed	AND
Radius:NAS-Port-...	Equals	Wireless - I	AND
Network Access:...	Equals	PEAP	

For the purposes of this CVD, the BYOD_Employee SSID number was defined as 1 during testing. The simple condition Employee_WLAN matches when the SSID number is 1. The condition is created to improve readability of the rules.

Figure 10-38 Employee_WLAN Condition



* Name Employee_WLAN

Description Airespace:Airespace-Wlan-Id EQUALS 1

* Attribute	* Operator	* Value
Airespace:Airespace-Wlan-Id	Equals	1

Certificate Authority Server

The Certificate Authority server is the central authority for distributing digital certificates. A Windows 2008 CA server was used as the CA server for this solution. This section focuses on:

- Network Device Enrollment Service, which is Microsoft's implementation of SCEP.
- Certificate Templates and how to design them.

NDES Server Configuration for SCEP

The Network Device Enrollment Service (NDES) is the Microsoft implementation of the SCEP, a communication protocol that makes it possible for network devices to enroll for X.509 certificates from a CA. To distribute and deploy digital x.509 client certificates to users, the Microsoft Network Device Enrollment Service (NDES) was utilized in conjunction with a Microsoft CA Server. For more details on how to implement NDES, see:
http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx.

By default, the NDES service is configured to present one-time enrollment passwords for certificate enrollment. The use of one-time passwords by the NDES service is typically used to allow network and IT administrators to enroll certificates for network devices within the IT organization. However, in this solution this feature is disabled because remote endpoints are authenticated by using their RSA SecurID tokens.

Disabling the "one-time password" on the NDES server is configured in the following registry key:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword.

EnforcePassword value data is set to "0", which ensures no password is requested by NDES.

Note Windows Server 2003, Microsoft SCEP (MSCEP) required a Resource Kit add-on to be installed on the same computer as the CA. In Windows Server 2008, MSCEP support has been renamed NDES and is part of the operating system. NDES may be installed on a different computer than the CA (http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx).

The NDES extension to IIS uses the registry to store configuration settings. All settings are stored under one registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP

Note It is possible for the ISE to generate URLs which are too long for the IIS. To avoid this problem, the default IIS configuration may be modified to allow longer URLs.

The following command should be run on a command line with administrative privileges:

```
%systemroot%\system32\inetsrv\appcmd.exe set config
  /section:system.webServer/security/requestFiltering
  /requestLimits.maxQueryString:"6044"
  /commit:apphost
```

Certificate Template

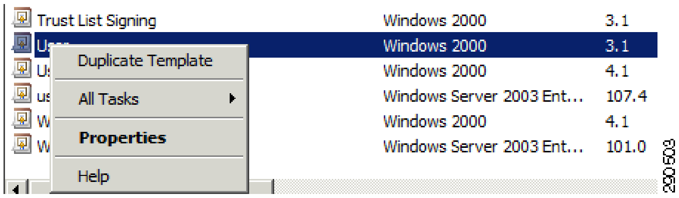
Digital certificates can be used for different purposes like server authentication, secure email, encrypting the file system, and client authentication. Hence it is important that a client is issued a certificate which serves its purpose. For example, a web server may need a certificate for server authentication. Similarly, a normal client needs a certificate mainly for client authentication. Therefore, certificate templates are needed to properly distribute certificates to users based on their specific needs. In this solution, a security template has been created on the Microsoft Windows 2008 CA server so that users can obtain the proper certificate. This section describes important steps to set up the certificate template on the Windows CA server and specific actions needed by the user.

For more information on certificate templates, see: http://technet.microsoft.com/en-us/library/cc730826%28WS.10%29.aspx.

SCEP is used as a protocol by the endpoints to obtain their digital certificates from the CA server. The endpoints send the certificate requests to ISE, which forwards the requests to the CA server. ISE is configured as SCEP Proxy to handle these requests and once the CA server issues the certificates, ISE sends the certificates back to the clients. The properties of the "User" template are being used. That is a default template in the Microsoft Server 2008 R2 CA Server deployment. Default templates in Microsoft Server 2008 R2 cannot be edited. Therefore, a customized template can be built that gives an administrator more flexibility in defining the certificate options. This section describes how to create a customized template named "user2" in this example.

The first step is to create a duplicate template from the pre-defined list of templates. Figure 10-39 shows how to create a duplicate template.

Figure 10-39 Creating a Duplicate Template

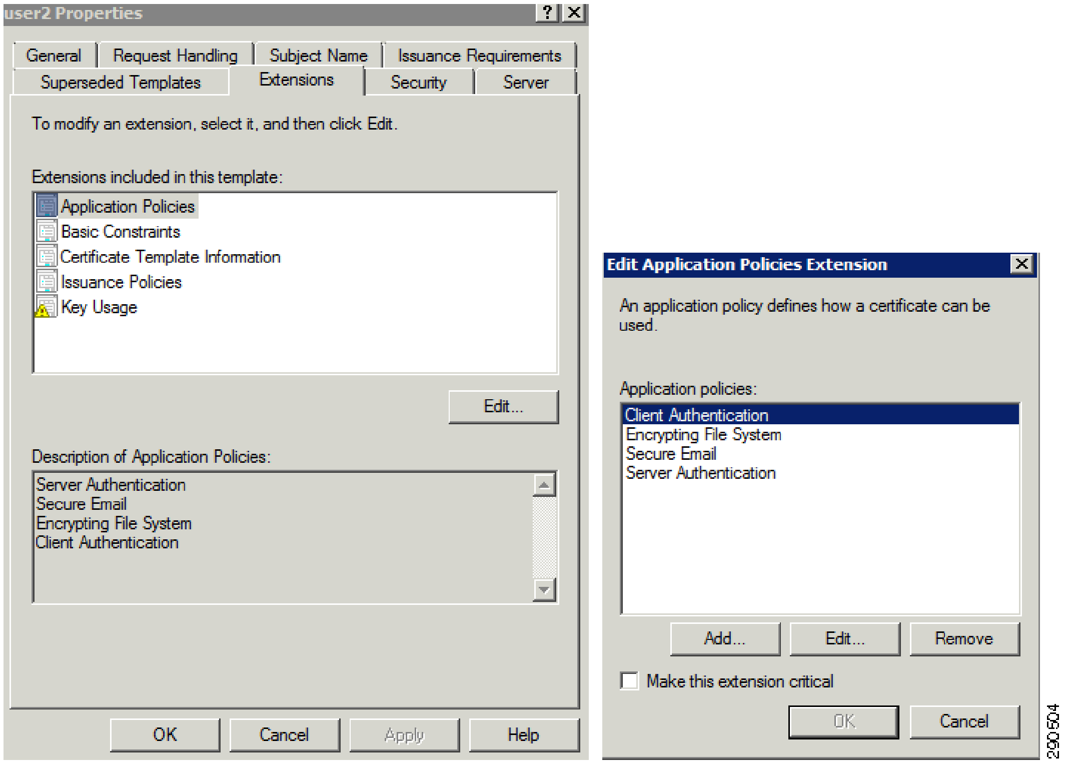


The default "User" template was copied and renamed "user2". Then the "user2" template was used to auto-enroll AnyConnect VPN clients with client certificates using this newly created template.

The next step is to configure the extensions of the certificates that are derived from the "user2" template. The EKU extension and extended property specify and limit the valid uses of a certificate. The extensions are part of the certificate itself. They are set by the issuer of the certificate and are read-only. Certificate-extended properties are values associated with a certificate that can be set in an application. To obtain more information about extended properties, see: http://msdn.microsoft.com/en-us/library/aa380252%28v=vs.85%29.aspx.

Figure 10-40 describes how to configure the extended properties for the certificates.

Figure 10-40 Configuring Extended Properties for Certificates



user2 Properties

To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Server Authentication
Secure Email
Encrypting File System
Client Authentication

Edit Application Policies Extension

An application policy defines how a certificate can be used.

Application policies:

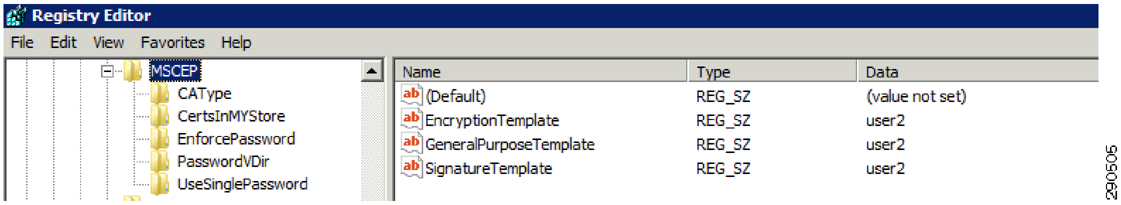
- Client Authentication
- Encrypting File System
- Secure Email
- Server Authentication

□ Make this extension critical

Notice the template named “user2”. This value must be set in the registry as it correlates to the “user2” template, which was copied from the “User” template in the Certificate Templates Console on the CA Server.

Figure 10-41 describes how the registry setting must be modified to reflect the newly-created template “user2”.

Figure 10-41 Modifying the Registry



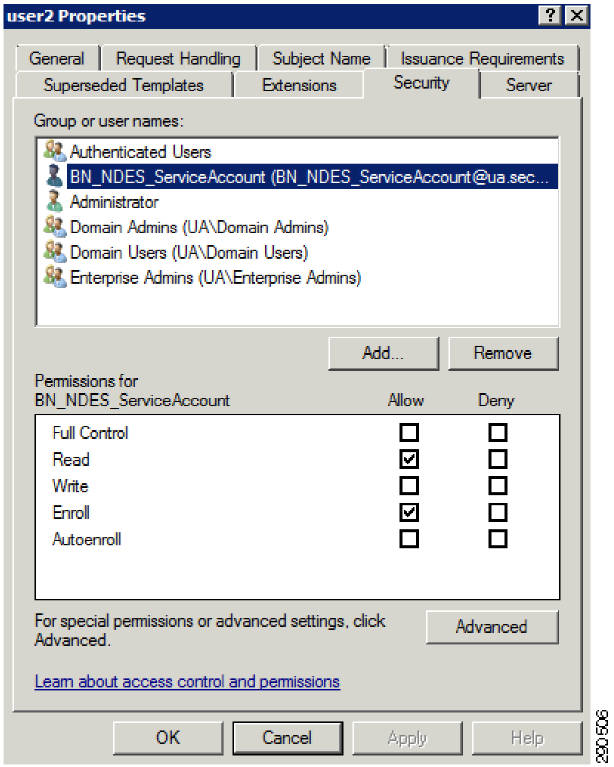
Registry Editor

MSCEP
- CAType
- CertsInMYStore
- EnforcePassword
- PasswordVDir
- UseSinglePassword

Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	user2
GeneralPurposeTemplate	REG_SZ	user2
SignatureTemplate	REG_SZ	user2

Once the template has been duplicated, the permissions are set for the NDES_ServiceAccount on the “user2” template to Read and Enroll. Figure 10-42 displays the Read and Enroll permissions that have been set for the NDES_ServiceAccount on the “user2” template.

Figure 10-42 Read and Enroll Permissions



Group or user names:

- Authenticated Users
- BN_NDES_ServiceAccount (BN_NDES_ServiceAccount@ua.sec...
- Administrator
- Domain Admins (UA\Domain Admins)
- Domain Users (UA\Domain Users)
- Enterprise Admins (UA\Enterprise Admins)

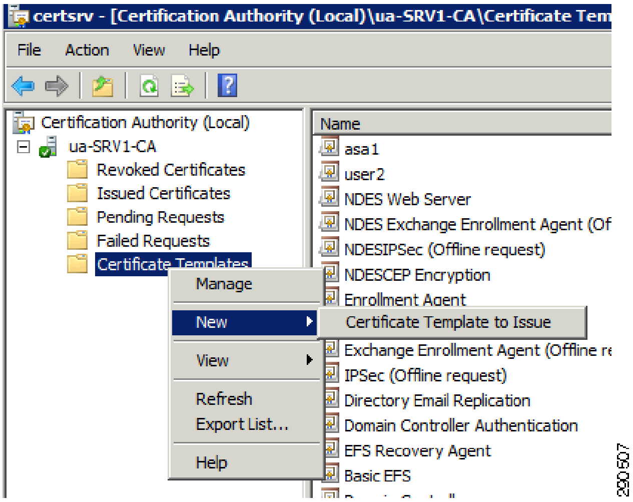
Permissions for BN_NDES_ServiceAccount	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Ensure that the newly created "user2" template is available to be issued via the CA. Right click "user2" and choose the newly-created "User2 Certificate", as shown in Figure 10-43.

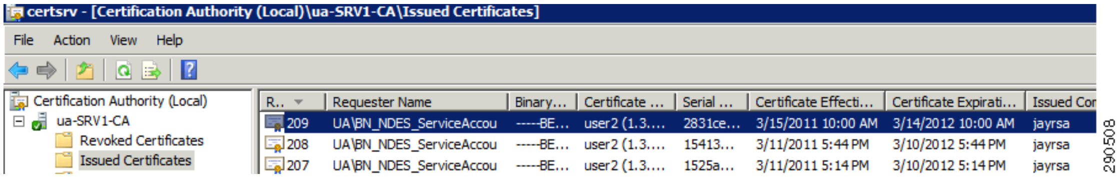
Figure 10-43 Ensuring Template is Available From CA



- asa1
- user2
- NDES Web Server
- NDES Exchange Enrollment Agent (Of
- NDESIPSec (Offline request)
- NDESCEP Encryption
- Enrollment Agent
- Exchange Enrollment Agent (Offline re
- IPSec (Offline request)
- Directory Email Replication
- Domain Controller Authentication
- EFS Recovery Agent
- Basic EFS

Now the certificate template is fully configured and can be used by users to submit enrollment requests. Figure 10-44 shows a successful enrollment request to the "user2" template that was submitted by a user, "jayrsa".

Figure 10-44 Successful Enrollment Request



certsrv - [Certification Authority (Local)\ua-SRV1-CA\Issued Certificates]

R..	Requester Name	Binary…	Certificate …	Serial …	Certificate Effecti…	Certificate Expirati…	Issued Cor
209	UA\BN_NDES_ServiceAccou	-----BE…	user2 (1.3.…	2831ce…	3/15/2011 10:00 AM	3/14/2012 10:00 AM	jayrsa
208	UA\BN_NDES_ServiceAccou	-----BE…	user2 (1.3.…	15413…	3/11/2011 5:44 PM	3/10/2012 5:44 PM	jayrsa
207	UA\BN_NDES_ServiceAccou	-----BE…	user2 (1.3.…	1525a…	3/11/2011 5:14 PM	3/10/2012 5:14 PM	jayrsa

A successful auto-enrollment request has occurred on the CA Server. Notice that the requester name is the NDES Service Account that is configured for Read and Enroll permissions and also notice that the "user2" certificate template was chosen.

BYOD Wired Infrastructure Design

Revised: August 7, 2013

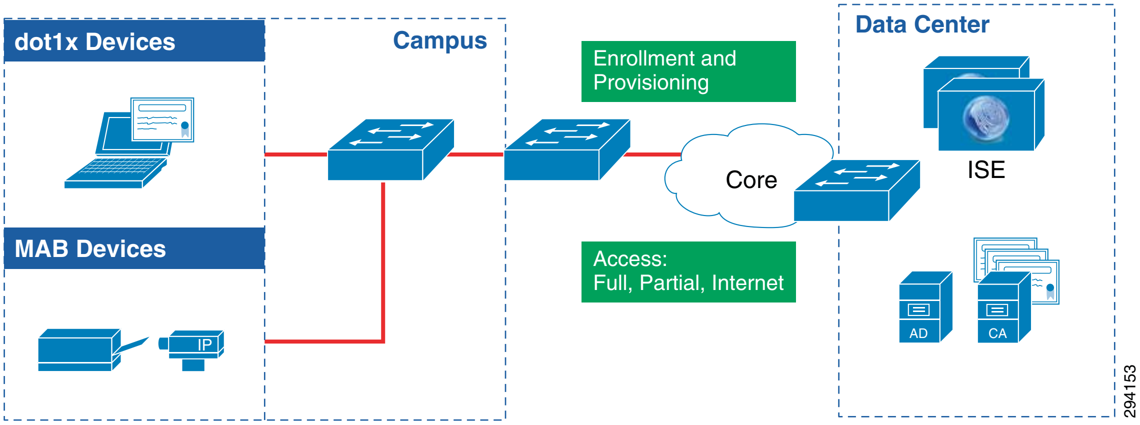
The previous sections discussed how BYOD devices can be on-boarded to the network and also how different policies can be enforced for mobile devices using wireless medium. This section discusses how to design and configure on-boarding and enforcing network access policies for wired devices. These devices can be located at Campus or at Branch location. Moreover, wired devices can connect using either converged access layer switches or by using non-converged access layer switches. This section discusses the design and configuration details for following network architectures:

- Campus (Both Converged Access and non-Converged Access)
- Branch (Both Converged Access and non-Converged Access)

Campus Wired Design

At the campus location there are 802.1X-capable clients that go through the provisioning/enrollment process and there are other types of devices like printers, cameras, etc. which do not have 802.1X capabilities and can only provide their MAC address as their source of authentication. These devices also will need to access the network and this design allows them to authenticate/authorize and obtain their authorization policy from ISE. Figure 11-1 shows an end-to-end network architecture diagram that includes wired device access from campus:

Figure 11-1 Network Diagram for Wired Devices at Campus Location



VLAN Design for Wired Switches at Campus

In the campus BYOD wired designs presented in this document, the VLAN assignment is same for all types of access—Full, Partial, or Internet. This means that the VLAN assignment to the port does not change when the device accessing the port changes. For example, the corporate-owned asset and the personal device would still use the same VLAN number. The policy enforcement is done by a DACL which is pushed from the ISE for non-Converged Access switches. On the other hand, policy enforcement in Converged Access switches is done using a named ACL instead of a DACL. To obtain more information about the different types of DACLs or named ACLs, refer to Chapter 16, "BYOD Limited Use Case—Corporate Devices" or Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices." The following is an example configuration of Layer 2 interface of the access layer switch and is the same either on centralized campus or a converged access campus switch:

```
interface GigabitEthernet1/0/2
 switchport access vlan 42    ! VLAN used in this design is 42
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

IP Address Design for Campus Wired Infrastructure

In the campus wired network designs discussed in this design guide, the access layer switch performs Layer 2 functions only. The aggregation switch performs Layer 3 routing. The following is an example of part of the configuration of the Layer 3 aggregation switch:

```
ua31-6500-1#show running-config interface vlan 42
Building configuration...

Current configuration : 91 bytes
!
interface Vlan42
 ip address 10.207.42.1 255.255.255.0
 ip helper-address 10.230.1.61
end

ua31-6500-1#
```

As seen above, the Layer 3 interfaces are configured with the ip-helper address command, which helps clients obtain an IP address. For the purposes of this design guide, the DHCP server is located in the data center.

Policy Enforcement in the Campus for Wired Devices

ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the campus. There are two distinct sets of ACLs used:

- ACLs for managing the device—These ACLs are used for provisioning the device or managing the device like Blacklisting.
- ACLs that are mainly for enforcing the policies.

The policy enforcement method at campus non-Converged Access switches is done by defining DACLs in the ISE based on the authZ policy and pushing that DACL to the port on the access layer switch. In Converged Access switches, policy enforcement is done through a named ACL sent by the ISE based on the authZ policy. The named ACL must be previously configured on the Converged Access Catalyst 3850 switch. To obtain more information on the authZ profiles used in this design guide, refer to either Chapter 16, "BYOD Limited Use Case—Corporate Devices" or Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices."

ACL Design for Campus Access Layer Switches

This section discusses the set of ACLs that are used for provisioning devices onto the network, protecting against unauthorized access, and blacklisting the device. The ACLs discussed in this section apply to both Converged access layer switches and non-converged access layer switches. Table 11-1 summarizes these ACLs and their purpose.

Table 11-1 Campus ACLs and Purpose

ACL Name	Where it Applies	Purpose
ACL-DEFAULT	Access Layer Switch	To protect against unauthorized access through the switch port
ACL_Provisioning	ISE	To allow an endpoint access to complete on-boarding process
ACL_Provisioning_Redirect	Access Layer Switch	Redirect web traffic initiated by new devices accessing the network. This ACL is a named ACL that is present on the access layer switch.
ACL_BLACKHOLE_Redirect	Access Layer Switch	Redirect web traffic initiated by black listed devices

ACL-DEFAULT—This ACL is configured on the access layer switch and used as a default ACL on the port. Its purpose is to prevent un-authorized access. In an 802.1X authentication/authorization scenario, after the device is authenticated and authorized, if there is no DACL applied to the port or if there is a mistake in the syntax of the downloadable ACL and the switch rejects the DACL sent by ISE, ACL-DEFAULT protects the port in the above mentioned scenarios. In the converged access design, the ACL is a named ACL and is configured on the Catalyst 3850 switch. The ISE sends the name of the ACL to be applied at the port. Again, if the switch rejects the named ACL sent by ISE, ACL-DEFAULT protects the port.

An example of a default ACL on a campus access layer switch is shown below:

```
Extended IP access list ACL-DEFAULT
    10 permit udp any eq bootpc any eq bootps log (2604 matches)
    20 permit udp any host 10.230.1.45 eq domain
    30 permit icmp any any
    40 permit udp any any eq tftp
    50 deny ip any any log (40 matches)
```

As seen from the output above, ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

ACL_Provisioning_Redirect—This ACL is used during on-boarding of wired devices. The ACL triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere, which means that when the user opens a web browser and attempts to access any website, that traffic is re-directed. The example shown below redirects any web traffic initiated by the user. However, this ACL can be modified to allow only certain traffic to be redirected to ISE portal. The underlying assumption in this design is that all the devices must be registered with ISE, therefore when an un-registered device accesses the network, it is redirected to ISE.

An example of ACL_Provisioning_Redirect ACL on a campus switch is shown below:

```
Extended IP access list ACL_Provisioning_Redirect
    10 deny udp any eq bootpc any eq bootps log
    20 deny udp any host 10.230.1.45 eq domain (43 matches)
    30 deny ip any host 10.225.42.15 (27 matches)
    40 permit tcp any any eq www (30 matches)
    50 permit tcp any any eq 443 (240 matches)
```

ACL_BLACKHOLE_Redirect—This ACL is used to redirect devices that have been blacklisted to the ISE portal to let the user know that the device in use has been blacklisted. This ACL is similar to the ACL_Provisioning_Redirect ACL.

An example of ACL_BLACKHOLE_Redirect on a campus switch is shown below:

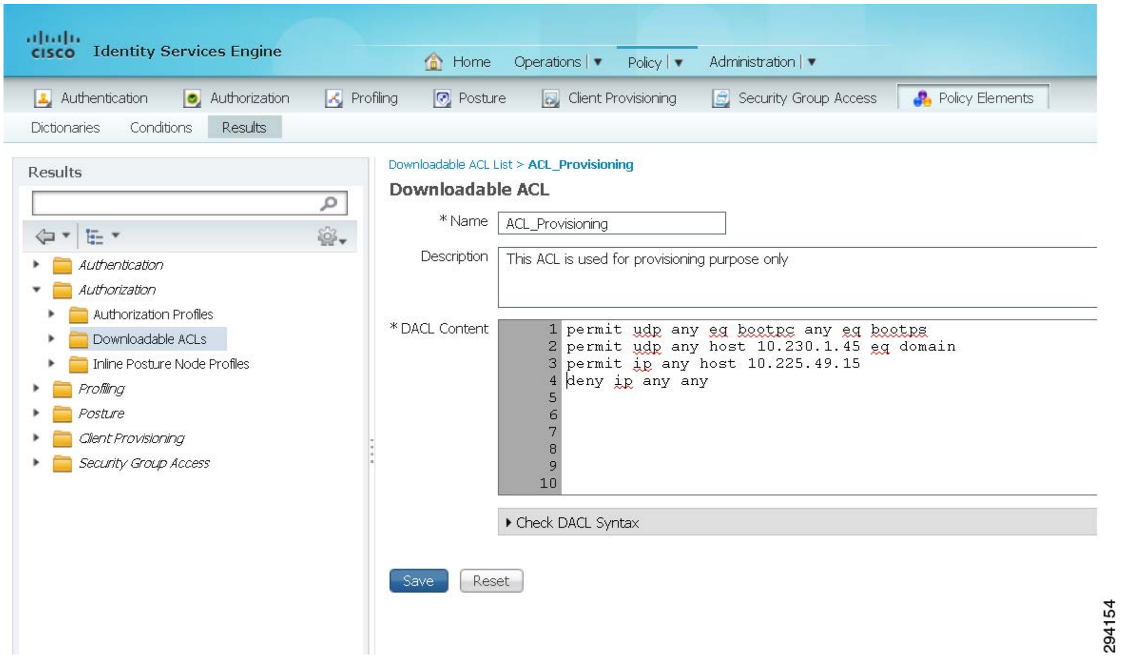
```
Extended IP access list ACL_BLACKHOLE_Redirect
    10 deny udp any eq bootpc any eq bootps
    20 deny udp any host 10.230.1.45 eq domain
    35 deny ip any host 10.225.49.15
    40 permit ip any any
```

Note The converged access layer switches use the same ACL_BLACKHOLE_Redirect for redirecting black listed wired devices.

Provisioning ACL

This ACL is also used during the on-boarding of wired devices. This DACL is downloaded from the ISE and restricts access to only the ISE, DNS, and DHCP server. This ACL is defined on the ISE, as shown in Figure 11-2.

Figure 11-2 ACL_Provisioning



Downloadable ACL List > ACL_Provisioning

Downloadable ACL

* Name: ACL_Provisioning

Description: This ACL is used for provisioning purpose only

* DACL Content

```
permit udp any eq bootpc any eq bootps
permit udp any host 10.230.1.45 eq domain
permit ip any host 10.225.49.15
deny ip any any
```

Note The ACL_Provisioning ACL is also used for Converged access layer switches.

802.1X and AAA Configuration for Campus Switches

A Cisco Catalyst Switch is used to provide end user Ethernet connectivity into the network in this design guide. The access layer switch enables 802.1X authentication for the client devices and interacts with the Identity Services Engine using the RADIUS protocol. Based on the results from the authentication process, a user may be allowed restricted or full access into the network using a VLAN assignment and a downloadable Access Control List (DACL). The flex-authentication configuration described below allows for using both 802.1X and MAC Authentication Bypass (MAB) as a fallback mechanism. Flex-auth is useful for devices that do not have 802.1X support such as printers.

This section discusses on the configuration details of enabling AAA on the campus access layer switches, and these switches can be either converged access layer switches non-converged access layer switches.

The following steps are required to configure the access switch for AAA on the Campus Switch:

Step 1 Enable Authentication, Authorization, and Accounting (AAA):

```
ACL(config)# aaa new-model
```

Step 2 Create an authentication method for 802.1X (default use all RADIUS servers for authentication):

```
ACL(config)# aaa authentication dot1x default group radius
```

Step 3 Create an authorization method for 802.1X (enables RADIUS for policy enforcement):

```
ACL(config)# aaa authorization network default group radius
```

Step 4 Create an accounting method for 802.1X (provides additional information about sessions to ISE):

```
ACL(config)# aaa accounting dot1x default start-stop group radius
```

The following steps are required to configure the access switch for RADIUS:

Step 1 Add ISE server to the RADIUS group:

```
ACL(config)# radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key
shared-secret
```

Step 2 Configure ISE server dead time (15 seconds total-3 retries of 5 second timeout):

```
ACL(config)# radius-server dead-criteria time 5 tries 3
```

Step 3 Configure the switch to send Cisco Vendor-Specific attributes:

```
ACL(config)# radius-server vsa send accounting
ACL(config)# radius-server vsa send authentication
```

Step 4 Configure the Cisco Vendor-Specific attributes:

```
ACL(config)# radius-server attribute 6 on-for-login-auth
ACL(config)# radius-server attribute 8 include-in-access-req
ACL(config)# radius-server attribute 25 access-request include
```

Step 5 Configure IP address to be used to source RADIUS messages:

```
ACL(config)# ip radius source-interface interface-name Vlan4093
```

The following steps are required to configure the access switch for 802.1X:

Step 1 Enable 802.1X globally (command by itself does not enable authentication on the switchports):

```
ACL(config)# dot1x system-auth-control
```

Step 2 Enable IP device tracking:

```
ACL(config)# ip device tracking
```

The following interface level commands enable 802.1X for Flex-Auth:

Step 1 Configure the authentication method priority (dot1x has higher priority over MAB):

```
ACL(config-if)# authentication priority dot1x mab
```

Step 2 Configure the authentication method order (dot1x first):

```
ACL(config-if)# authentication order dot1x mab
```

Step 3 Enable Flex-Auth:

```
ACL(config-if)# authentication event fail action next-method
```

Step 4 Enable support for more than one MAC address on the physical port:

```
ACL(config-if)# authentication host-mode multi-auth
```

Step 5 Configure the violation action (restrict access for additional devices that may fail authentication):

```
ACL(config-if)# authentication violation restrict
```

Step 6 Enable port for 802.1X:

```
ACL(config-if)# dot1x pae authenticator
```

Step 7 Enable port for MAB:

```
ACL(config-if)# mab
```

Step 8 Configure timers (30 seconds (10x3) until falling back to MAB):

```
ACL(config-if)# dot1x timeout tx-period 3
```

Step 9 Turn authentication on:

```
ACL(config-if)# authentication port-control auto
```

Step 10 Enable the ACL-DEFAULT to the port

```
ACL(config-if)# ip access-group ACL-DEFAULT in
```

Step 11 Enable http and https server:

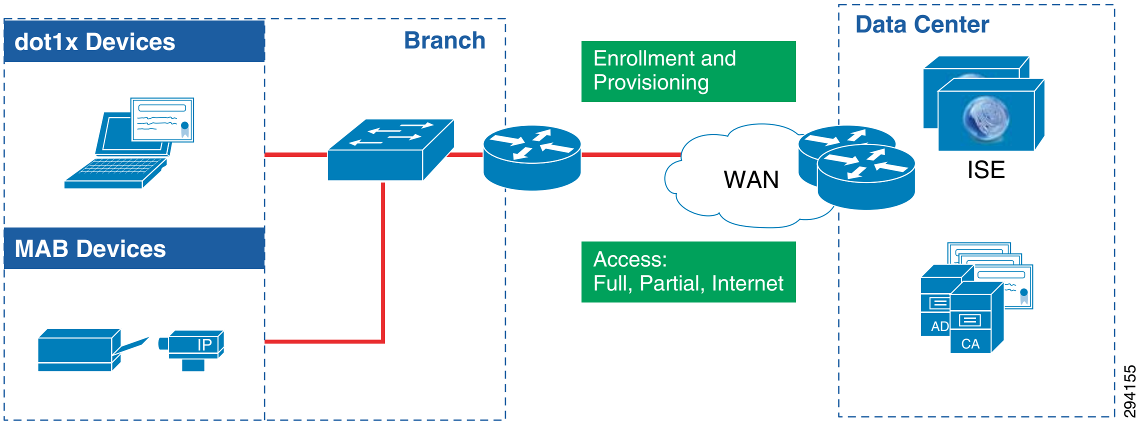
```
ACL (config)# ip http-server
ACL (config)# ip http secure-server
```

Branch Wired Design—Non-Converged Access

At a branch location, there are 802.1X capable clients that go through the provisioning/enrollment process and there are also other types of devices such as printers, cameras, etc. which do not have 802.1X capabilities and can only provide their MAC address as their source of authentication. These devices also need to access the network and this design allows them to authenticate/authorize and obtain their authorization policy from ISE. This section discusses wired designs for branches which do not deploy Converged Access (Catalyst 3850) switches. The branch wired design discussed in this section is meant to accompany FlexConnect-based wireless branch designs. The Converged Access branch wired design is discussed in Branch Wired Design—Converged Access.

Figure 11-3 shows an end-to-end network architecture diagram that includes wired device access from the branch.

Figure 11-3 Network Diagram for Wired Access at Branch Location



VLAN Design at Branch Locations

Four VLANs are implemented for wired devices at the non-Converged Access branch location. Table 11-2 illustrates the names of these VLANs and their purpose.

Table 11-2 VLANs and their Purpose

VLAN Name	VLAN Number	Description
Wired_Full	13	Devices placed in this VLAN get full access to corporate resources and branch local servers.
Wired_Partial	14	Devices placed in this VLAN get restricted access to resources.
Wired_Internet	15	Devices placed in this VLAN get only Internet access only.
Branch_Server	16	Local Servers at branch location are placed in this VLAN.

IP Address Allocation at Branch Location

In the non-converged access branch network design discussed in this design guide, the switch performs Layer 2 functions only and the branch router performs Layer 3 routing. Hence, all the Layer 3 interfaces for the VLANs mentioned above are implemented at the branch router. The following is an example configuration of the branch router:

```
interface GigabitEthernet0/1.13
 encapsulation dot1Q 13
 ip address 10.200.13.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 13 ip 10.200.13.1
 standby 13 priority 110
 standby 13 preempt
!
interface GigabitEthernet0/1.14
 encapsulation dot1Q 14
 ip address 10.200.14.2 255.255.255.0
 ip access-group Branch1_ACL_Partial_Access in
 ip helper-address 10.230.1.61
 standby 14 ip 10.200.14.1
 standby 14 priority 110
 standby 14 preempt
!
interface GigabitEthernet0/1.15
 encapsulation dot1Q 15
 ip address 10.200.15.2 255.255.255.0
 ip access-group ACL_Internet_Only in
 ip helper-address 10.230.1.61
 standby 15 ip 10.200.15.1
 standby 15 priority 110
 standby 15 preempt
!
interface GigabitEthernet0/1.16
 encapsulation dot1Q 16
 ip address 10.200.16.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 16 ip 10.200.16.1
 standby 16 priority 110
 standby 16 preempt
!
```

As seen above, the Layer 3 interfaces are configured with the **ip-helper address** command, which helps branch clients obtain an IP address. For the purposes of this design guide, the DHCP server is in a data center location.

Policy Enforcement in the Branch for Wired Devices

ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the branch. There are two distinct sets of ACLs used:

- ACLs for managing the device—These ACLs are used for provisioning the device or managing the device like Blacklisting.
- ACLs that are mainly for enforcing the policies.

When designing the ACLs for branch the following should be considered:

- Configuring static ACLs at every branch router in the network.
- Configuring the ISE to push downloadable ACLs to access layer switches at every branch location.

Table 11-3 gives the advantages and disadvantages of each approach.

Table 11-3 ACL Policy Enforcement

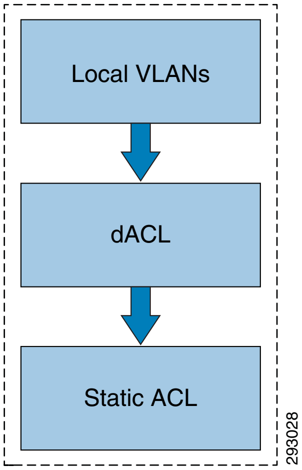
Method	Advantages	Disadvantages
Static ACLs	Modify the ACL based on the branch's needs	Hard to manage each branch policy individually
Downloadable ACLs	Centralized access control	Creating an individual policy at ISE for every branch location would make the policy very large from an administrative perspective. For example, to manage 500 unique branches, 500 ACLs, 500 authZ profiles, and 500 authZ policy rules would need to be defined on the ISE.

Each of the above methods has advantages and disadvantages. This design guide focuses on a combination that includes both methods. The static ACLs are the primary method by which access is restricted. However, the static ACLs are applied at the router only; to override the ACL called

"DEFAULT-ACL" which is present on every port of the access layer switch, a DACL (permit all traffic) is downloaded from ISE. This DACL from the ISE allows the traffic to flow upstream from the access layer switch to the Branch router. The Branch router is pre-configured with the different ACLs that restrict access. These ACLs either provide full, partial, or Internet access to the users.

Figure 11-4 shows how the authorization policy pushes the VLAN information and the DACL (permit all traffic) to the port on the access layer switch, thereby allowing the traffic to reach from the access layer switch up to the router where the traffic will be filtered.

Figure 11-4 Enforcing Permissions



ACL Design at Branch Location

ACLs are very important at the branch location, since they are the main method used to enforce policies. Some ACLs are defined on the Layer 2 switch for provisioning purposes, while others are defined on the branch router. In addition, some ACLs may be downloaded from the ISE.

Table 11-4 summarizes the various ACLs at branch locations and their purpose.

Table 11-4 Branch ACLs and Purpose

ACL Name	Where it Applies	Purpose
ACL_DEFAULT	Switch	To protect against unauthorized access through the switch port
ACL_Provisioning_Redirect	Switch	Redirect web traffic initiated by new devices accessing the network.
ACL_Blackhole	Switch	Redirect web traffic initiated by black listed devices
ACL_Internet_Only	Branch Router	Allow only Internet traffic
ACL_Provisioning	ISE	Used during provisioning process
ACL_Partial_Access	Branch Router	Allow partial access to certain resources

ACL_DEFAULT—This ACL is used as a default ACL on the port and its purpose is to prevent un-authorized access. In an 802.1X authentication/authorization scenario, after the device is authenticated and authorized, if there is no DACL applied to the port or if there is a mistake in the syntax of the downloadable ACL and the switch rejects the DACL sent by ISE, ACL_DEFAULT protects the port in the above mentioned scenarios. An example of a default ACL is shown below:

```
bn22-3750x-1#show ip access-lists
Load for five secs: 13%/0%; one minute: 16%; five minutes: 16%
Time source is NTP, 16:24:50.872 EDT Wed Sep 19 2012

Extended IP access list ACL-DEFAULT
  10 permit udp any eq bootpc any eq bootps
  20 permit udp any any eq domain
  30 permit icmp any any
  40 permit udp any any eq tftp
  50 deny ip any any log
```

As seen from the output above, ACL_DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

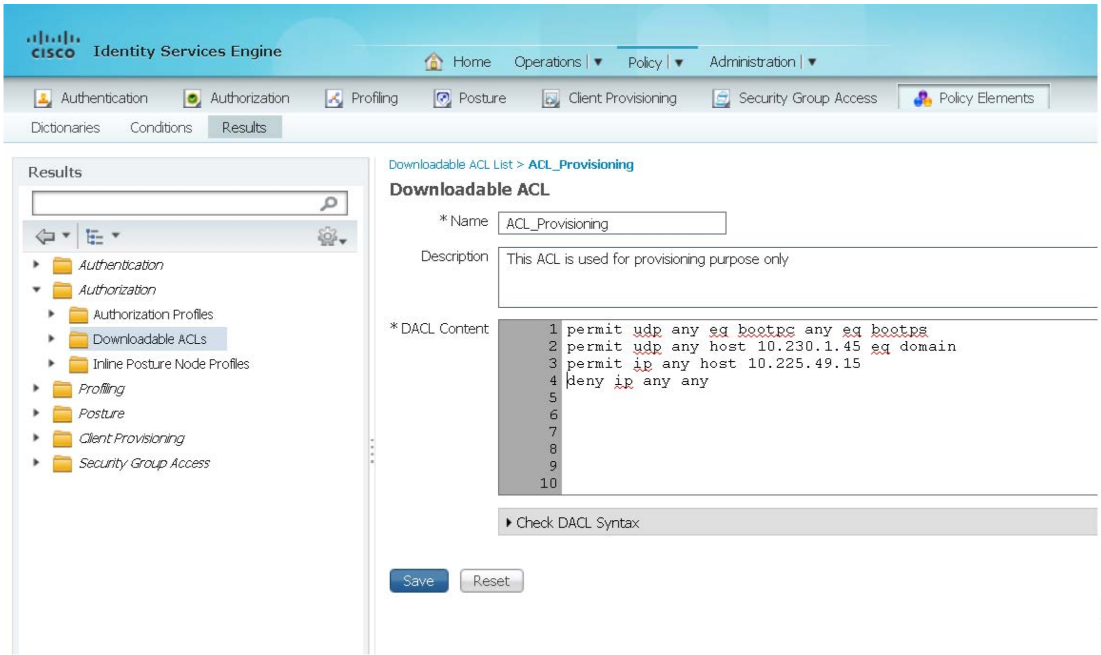
ACL_Provisioning_Redirect—This ACL is used during the on-boarding of wired devices. This ACL triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere, which means that when the user opens a web browser and attempts to access any website, that traffic is re-directed. The example shown below redirects any web traffic initiated by the user. However this ACL can be modified to allow only certain traffic to be redirected to ISE portal. The underlying assumption in this design is that all the devices must be registered with ISE, therefore when an un-registered device accesses the network, it is redirected to ISE.

```
uasl-3750x-1#show ip access-lists | begin ACL_Provisioning_Redirect
Extended IP access list ACL_Provisioning_Redirect
    10 deny udp any eq bootpc any eq bootps log
    20 deny udp any host 10.230.1.45 eq domain (1865 matches)
    30 deny ip any host 10.225.42.15 (839 matches)
    40 deny ip any host 10.225.49.15 (1853 matches)
    50 permit tcp any any eq www (3728 matches)
    60 permit tcp any any eq 443 (4140 matches)
uasl-3750x-1#
```

Provisioning ACL

This ACL is also used during the on-boarding of wired devices. This DACL is downloaded from the ISE and restricts access to only the ISE, DNS, and DHCP server. This ACL is defined on the ISE, as shown in Figure 11-5.

Figure 11-5 ACL_Provisioning



* Name: ACL_Provisioning

Description: This ACL is used for provisioning purpose only

* DACL Content:

```
permit udp any eq bootpc any eq bootps
permit udp any host 10.230.1.45 eq domain
permit ip any host 10.225.49.15
deny ip any any
```

802.1X and AAA Configuration for Branch Switches

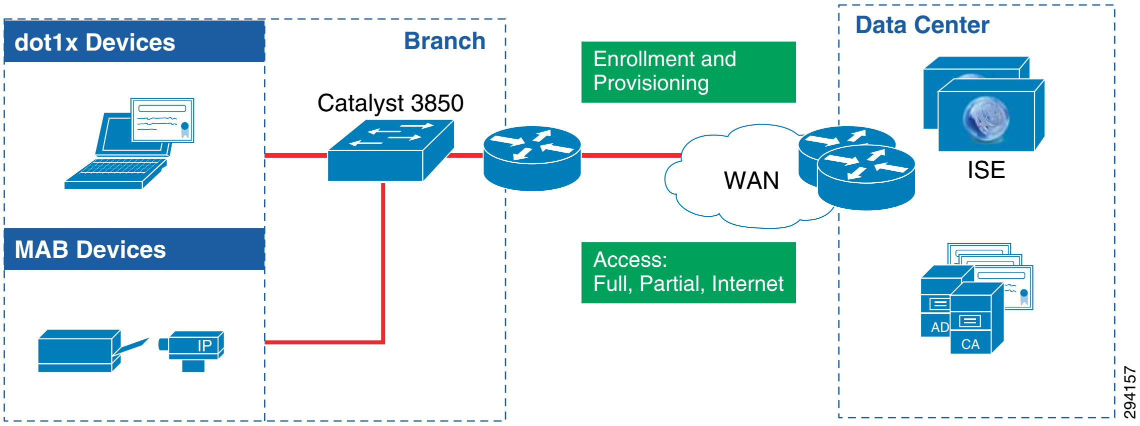
The configuration of 802.1X and AAA for branch non-Converged Access switches is exactly identical to the campus switches. Refer to 802.1X and AAA Configuration for Campus Switches for details.

Branch Wired Design—Converged Access

At a branch location, there are 802.1X capable clients that go through the provisioning/enrollment process and there are other types of devices like printers, cameras, etc. which do not have 802.1X capabilities and can only provide their MAC address as their source of authentication. These devices also need to access the network and this design allows them to authenticate/authorize and obtain their authorization policy from ISE. This section discusses wired designs for branches that deploy Converged Access (Catalyst 3850) switches.

Figure 11-6 shows an end-to-end network architecture diagram that includes wired device access from the branch.

Figure 11-6 Network Diagram for Wired Devices at Branch Location Using Converged Access Switches



VLAN Design at Branch Locations

In the Branch BYOD wired designs presented in this document, the VLAN assignment is same for all types of access—Full, Partial, or Internet. This means that the VLAN assignment to the port does not change when the device accessing the port changes. For example, the corporate-owned asset and the personal device would still use the same VLAN number. The policy enforcement in Converged Access switches is done using a named ACL instead of a DACL. Different named ACLs are applied to each device granting different access to the network. Since the named ACL is configured on the Catalyst 3850 switch specific to the particular branch, a single Cisco ISE policy can be implemented across multiple branches. However the Access Control Entries (ACEs) within the ACL for each branch can be unique to the IP addressing of the branch. This reduces the administrative complexity of the Cisco ISE policy, albeit at the expense of increased complexity of having to configure and maintain ACLs at each branch Catalyst 3850 Series switch.

Three VLANs are implemented for wired devices at the Converged Access branch location. Table 11-5 illustrates the names of these VLANs and their purpose.

Table 11-5 VLANs and their Purpose—Converged Access

VLAN Name	VLAN Number	Description
BYOD_Employee	10	Devices in this VLAN get access to either full, partial or limited access based on named ACL.
BYOD_Provisioning	11	Provisioning VLAN
Branch_Server	16	Local Servers at branch location are placed in this VLAN.

IP Address Allocation at Branch Location

In the converged access branch network design discussed in this design guide, the Catalyst 3850 switch performs Layer 2 functions only. There is no branch router, unlike Branch Wired design for non-Converged Access. The following is an example configuration of a Layer 2 interface of the access layer switch and is the same on either a centralized campus or a converged access campus switch:

```
interface GigabitEthernet1/0/2
 switchport access vlan 42   ! VLAN used in this design is 42
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

Layer 3 connectivity within the branch is provided by the ISR routers that also serve as the WAN connectivity point for the branch. The following is an example of part of the configuration of the Layer 3 router:

```
ua31-6500-1#show running-config interface vlan 42
Building configuration...

Current configuration : 91 bytes
!
interface Vlan42
 ip address 10.207.42.1 255.255.255.0
 ip helper-address 10.230.1.61
end
```

As seen above, the Layer 3 interfaces are configured with the **ip-helper address** command, which helps branch clients obtain an IP address.

Policy Enforcement at the Branch Using Converged Access Switches

ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the branch. There are two distinct sets of ACLs used:

- ACLs for managing the device—These ACLs are used for provisioning the device or managing the device like Blacklisting.
- ACLs that are mainly for enforcing the policies.

In Converged Access switches, policy enforcement is done through a named ACL sent by the ISE based on the authZ policy. The named ACL must be previously configured on the Converged Access Catalyst 3850 switch. To obtain more information on the authZ profiles used in this design guide, refer to either Chapter 16, "BYOD Limited Use Case—Corporate Devices" or Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices."

ACL Design at Branch Location for Converged Access Switches

This section discusses both sets of ACLs that are important for a converged access layer switch at a branch location:

- ACL that are used for provisioning.
- ACLs that are used for policy enforcement.

Table 11-6 summarizes the various ACLs in the Converged Access branch wired branch design and their purpose.

Table 11-6 Branch ACLs and Purpose

ACL Name	Where it Applies	Purpose
ACL_DEFAULT	Switch	To protect the switch port
ACL_Blackhole	Switch	Redirect web traffic initiated by black listed devices
ACL_Internet_Only	Switch	Allow only Internet traffic
ACL_Provisioning	ISE	Used during provisioning process
ACL_Partial_Access	Switch	Allow partial access to certain resources
ACL_Full_Access	Switch	Allow full access to all resources

ACL_Default—This ACL is used as a default ACL on the port and its purpose is to prevent un-authorized access. In the Converged Access Design this is done through a named ACL approach. The ACL_DEFAULT resides on the Catalyst 3850 switch.

```
Extended IP access list ACL_DEFAULT
  10 permit udp any eq bootpc any eq bootps
  20 permit udp any any eq domain
  30 permit icmp any any
  40 permit udp any any eq tftp
  50 deny ip any any
```

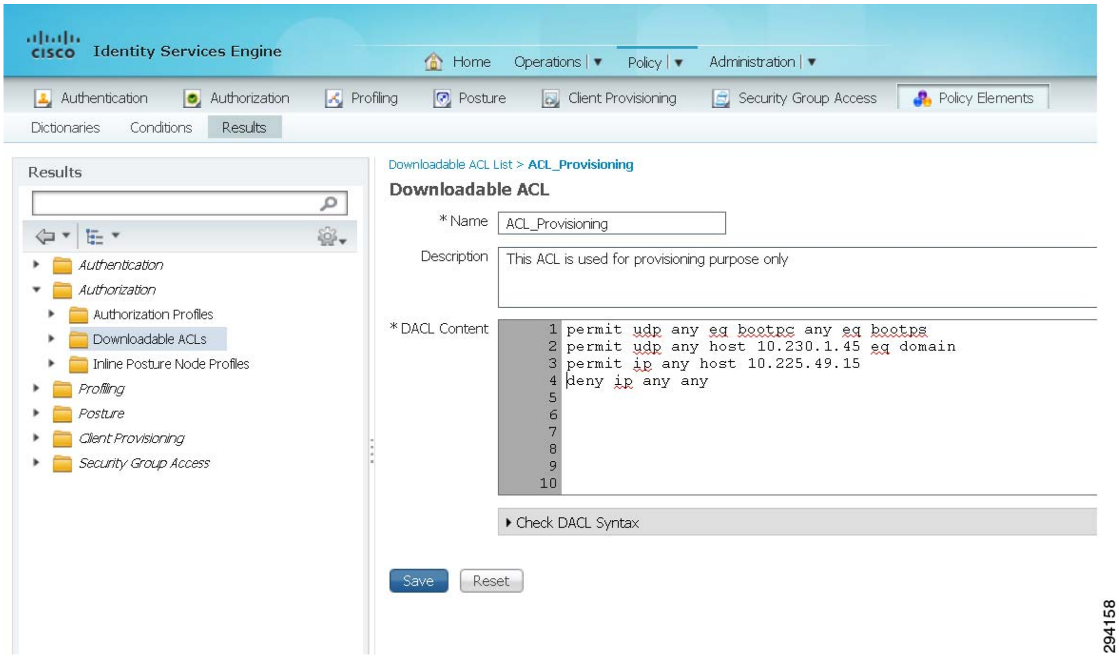
As seen from the output above, ACL_DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

ACL_Provisioning_Redirect—This ACL is used during the on-boarding of wired devices. This ACL triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere, which means that when the user opens a web browser and attempts to access any website, that traffic is re-directed. The example shown below redirects any web traffic initiated by the user. However, this ACL can be modified to allow only certain traffic to be redirected to ISE portal. The underlying assumption in this design is that all the devices must be registered with ISE, therefore when an un-registered device accesses the network, it is redirected to ISE.

```
Extended IP access list ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 permit tcp any any eq www
 permit tcp any any eq 443
```

ACL_Provisioning—This ACL is also used during the on-boarding of wired devices. This DACL is downloaded from the ISE and restricts access to only the ISE, DNS, and DHCP server. This ACL is defined on the ISE, as shown in Figure 11-7.

Figure 11-7 ACL_Provisioning



Downloadable ACL List > ACL_Provisioning

Downloadable ACL

* Name: ACL_Provisioning

Description: This ACL is used for provisioning purpose only

* DACL Content:

```
permit udp any eq bootpc any eq bootps
permit udp any host 10.230.1.45 eq domain
permit ip any host 10.225.49.15
deny ip any any
```

802.1X and AAA Configuration for Branch Switches

The configuration of 802.1X and AAA for branch switches is exactly identical to the campus switches. Refer to 802.1X and AAA Configuration for Campus Switches.

MAB Devices at Branch or at Campus Location

This section discusses how to design access for MAB devices using either converged access switches or traditional access layer switches. MAB devices can be present at either branch or campus locations.

MAB devices are generally those devices that cannot run 802.1X and can only present their mac-address for authentication. It is important to note that BYOD devices also use the MAB protocol during the provisioning process. During the provisioning process, BYOD devices are re-directed to the ISE guest portal to complete the registration process. MAB devices do not need to be registered and therefore do not need to be re-directed. The requirement for MAB devices is to authenticate the device and apply an authorization policy. Here are the high level steps that need to be performed for MAB devices:

1. Configure the access layer switch port or WLC to support the MAB protocol.
2. Import a MAC-address list of all MAB devices as an Identity group in ISE.
3. Configure an authentication policy for Wired and Wireless MAB devices. This same policy will be used to authenticate BYOD devices during provisioning.
4. Configure authorization policy rules in ISE for wired and wireless devices.

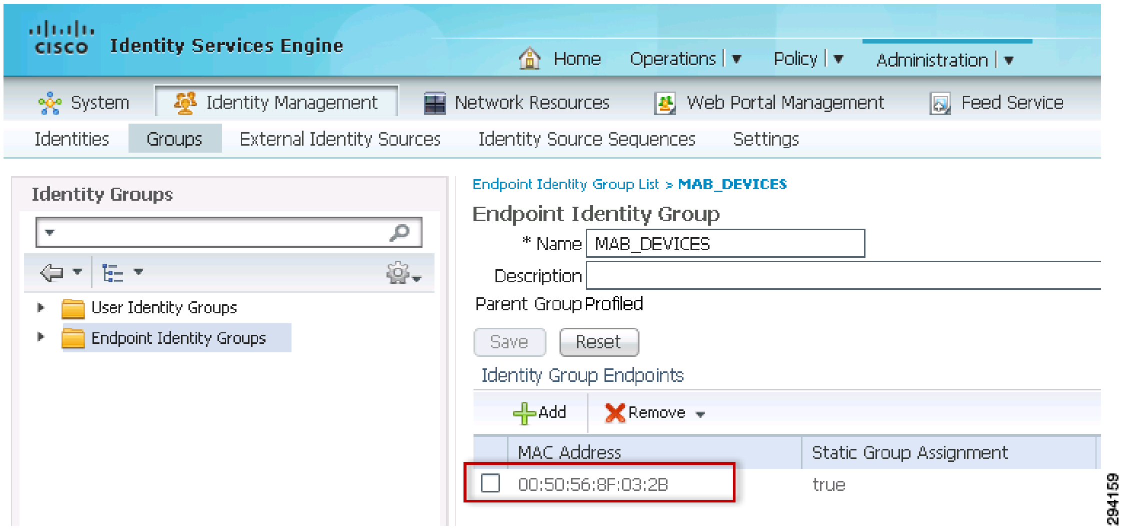
When a MAB device connects, the access layer switch sends the authentication request to the ISE using the MAC-address of the device as the source of authentication. An example is shown below.

```
Sep 25 11:09:50.741: %DOT1X-5-FAIL: Authentication failed for client (0050.568f.
1bb2) on Interface Gi1/0/10 AuditSessionID 0AC8130400000221292C2D59
```

```
Sep 25 11:09:50.741: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
 'dot1x' for client (0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC813
0400000221292C2D59
Sep 25 11:09:50.749: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client
0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC8130400000221292C2D59
Sep 25 11:09:50.749: %AUTHMGR-5-START: Starting 'mab' for client (0050.568f.032b
) on Interface Gi1/0/10 AuditSessionID 0AC8130400000221292C2D59
```

In this design, all the MAC addresses of MAB devices are placed in an internal identity group called MAB_DEVICES so ISE will know this device in advance. To add new MAC addresses to the MAB_DEVICES identity group, click **Administration > Groups > Endpoint Identity Groups**, as shown in Figure 11-8.

Figure 11-8 MAB_DEVICES Identity Group



Endpoint Identity Group List > MAB_DEVICES

Endpoint Identity Group

* Name MAB_DEVICES

Description

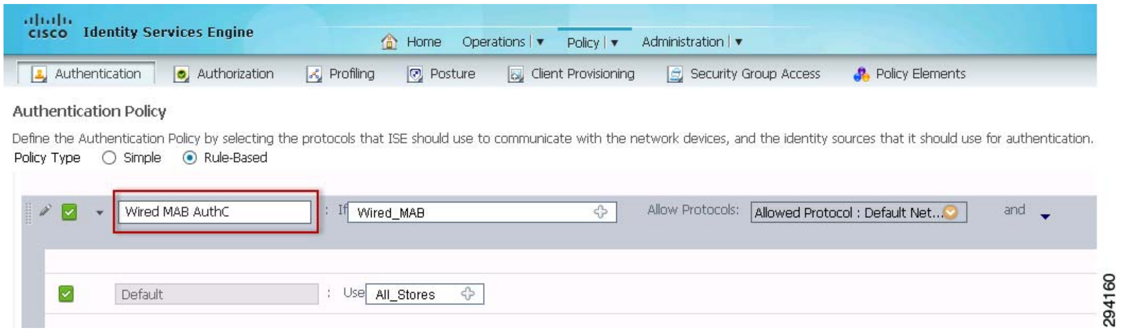
Parent Group Profiled

Identity Group Endpoints

	MAC Address	Static Group Assignment
□	00:50:56:8F:03:2B	true

Figure 11-9 shows the authentication policy defined on the ISE for wired MAB devices.

Figure 11-9 WIRED MAB AuthC



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

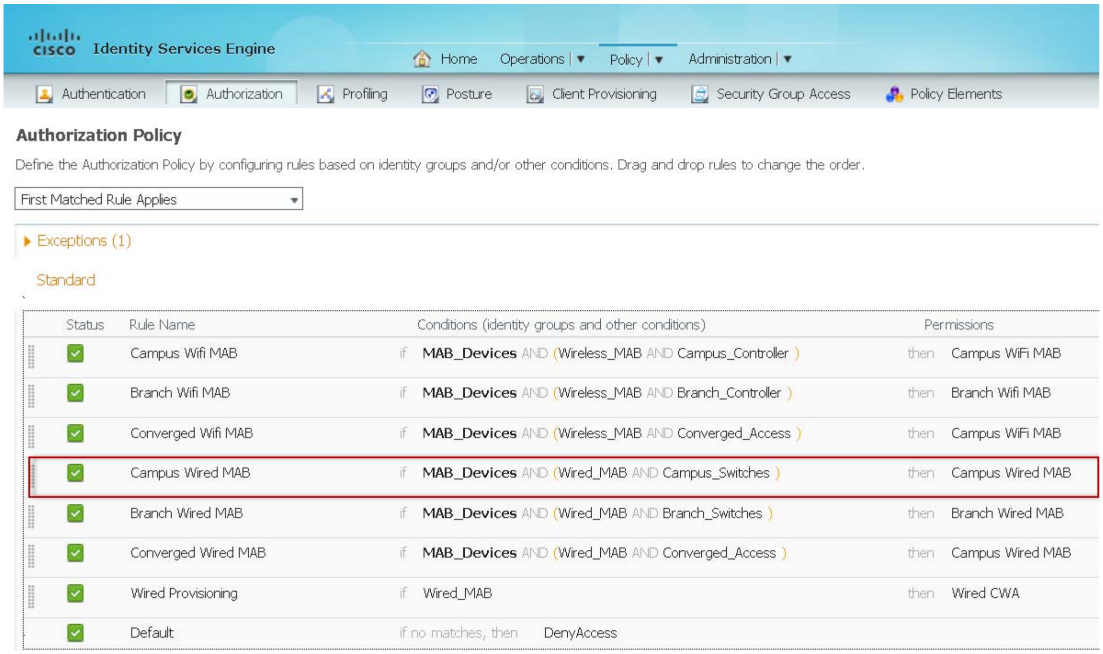
Policy Type ○ Simple ● Rule-Based

☑ Wired MAB AuthC : If Wired_MAB Allow Protocols: Allowed Protocol : Default Net... and

☑ Default : Use All_Stores

The authorization policy is different for MAB devices originating in the branch design with FlexConnect versus in the campus location. In the branch design in a FlexConnect model, every device is placed in different VLANs, but this is not done in the campus or a branch design with converged access. Hence there are different rules that are defined in the authZ policy to take care of location of the device-branch versus campus. Figure 11-10 shows how the policy rules are defined for campus devices.

Figure 11-10 Authorization Policy for MAB devices



Authorization Policy

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

First Matched Rule Applies ▾

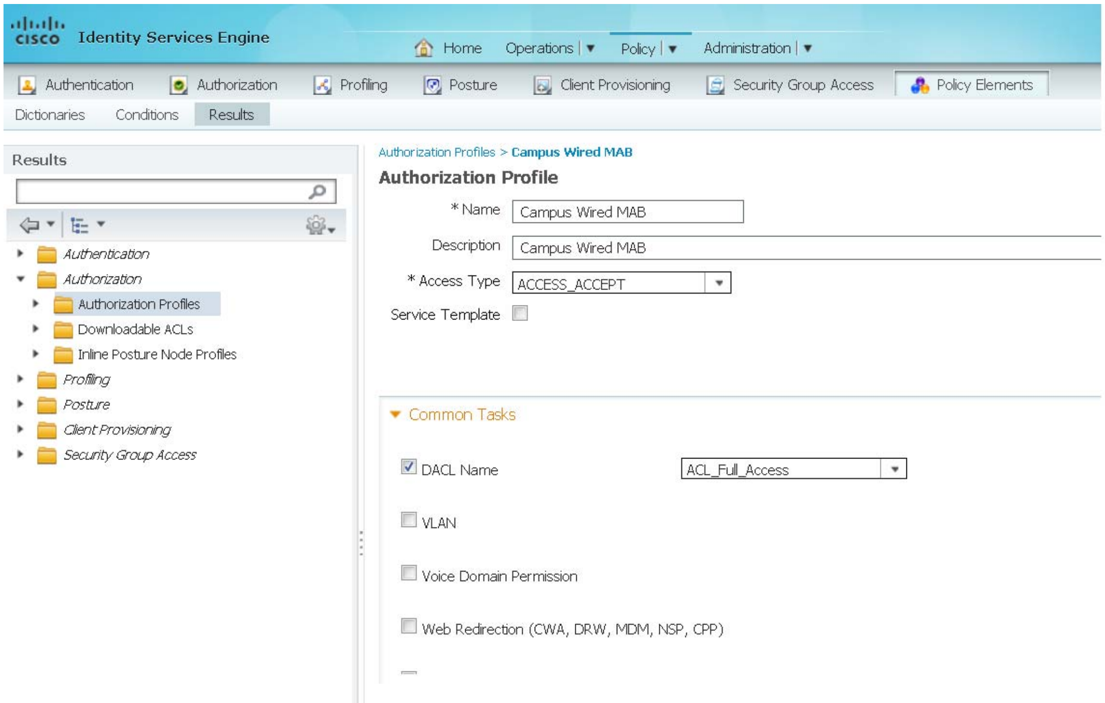
▸ Exceptions (1)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
☑	Campus Wifi MAB	if MAB_Devices AND (Wireless_MAB AND Campus_Controller)	then	Campus WiFi MAB
☑	Branch Wifi MAB	if MAB_Devices AND (Wireless_MAB AND Branch_Controller)	then	Branch Wifi MAB
☑	Converged Wifi MAB	if MAB_Devices AND (Wireless_MAB AND Converged_Access)	then	Campus WiFi MAB
☑	Campus Wired MAB	if MAB_Devices AND (Wired_MAB AND Campus_Switches)	then	Campus Wired MAB
☑	Branch Wired MAB	if MAB_Devices AND (Wired_MAB AND Branch_Switches)	then	Branch Wired MAB
☑	Converged Wired MAB	if MAB_Devices AND (Wired_MAB AND Converged_Access)	then	Campus Wired MAB
☑	Wired Provisioning	if Wired_MAB	then	Wired CWA
☑	Default	if no matches, then DenyAccess		

Campus Wired MAB is an authorization profile that pushes the appropriate settings to the access layer switch. Figure 11-11 shows the authorization profile details.

Figure 11-11 Campus Wired MAB Authorization Profile



Authorization Profiles > Campus Wired MAB

Authorization Profile

* Name: Campus Wired MAB

Description: Campus Wired MAB

* Access Type: ACCESS_ACCEPT ▾

Service Template: □

▾ Common Tasks

☑ DACL Name: ACL_Full_Access ▾

□ VLAN

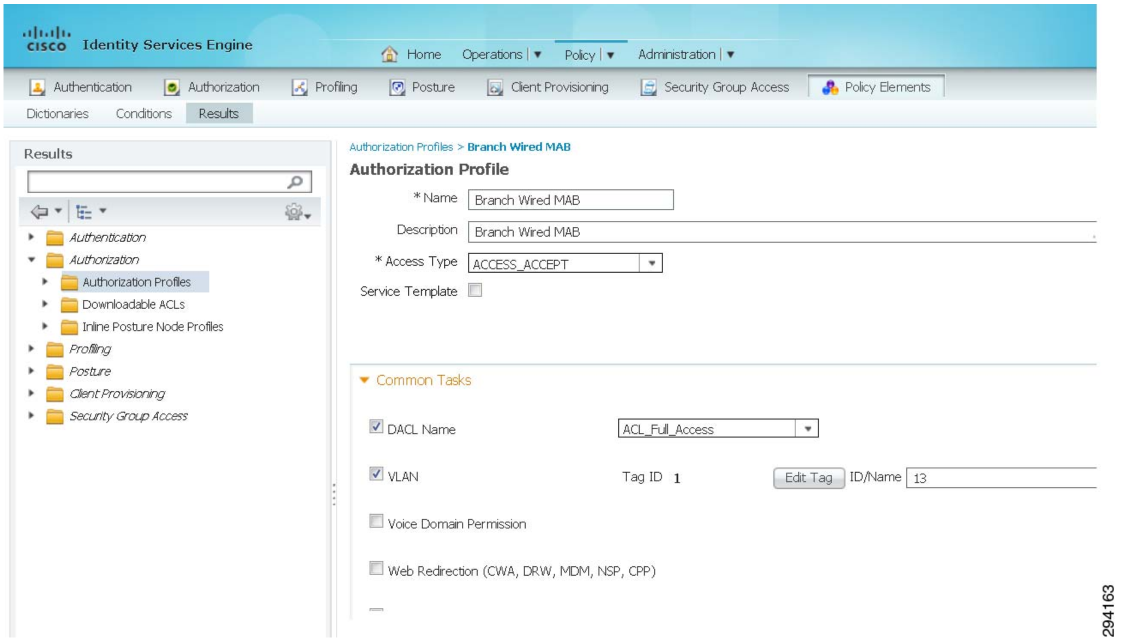
□ Voice Domain Permission

□ Web Redirection (CWA, DRW, MDM, NSP, CPP)

The Campus Wired MAB authorization profile does not push VLAN information, but rather applies a DACL to the port. The Converged Access design uses the same authorization profile as shown in the Figure 11-11. Also note that in the Converged Access design, for the authorization profile, a DACLs is used for both Campus and Branch designs.

Conversely, Branch_Wired_MAB authorization profile pushes the VLAN information to the access port on the wired switch for designs with branch with FlexConnect. Figure 11-12 shows the Branch_Wired_MAB profile configuration.

Figure 11-12 Branch_Wired_MAB Authorization Profile



Authorization Profile

* Name: Branch Wired MAB

Description: Branch Wired MAB

* Access Type: ACCESS_ACCEPT

Service Template ☐

Common Tasks

☑ DACL Name: ACL_Full_Access

☑ VLAN Tag ID 1 Edit Tag ID/Name 13

☐ Voice Domain Permission

☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)

The Converged Access Branch Design also uses same authorization profile for MAB devices as shown in the Figure 11-12.

CHAPTER 12

Security Group Access for BYOD

Revised: August 7, 2013

The following section describes the infrastructure used in this CVD and provides an outline of the two deployment scenarios used to enforce policies based on Security Group Tags. These deployment scenarios are not mutually exclusive and may be used together to satisfy an organization’s requirements. Configuration details for the infrastructure are also provided.

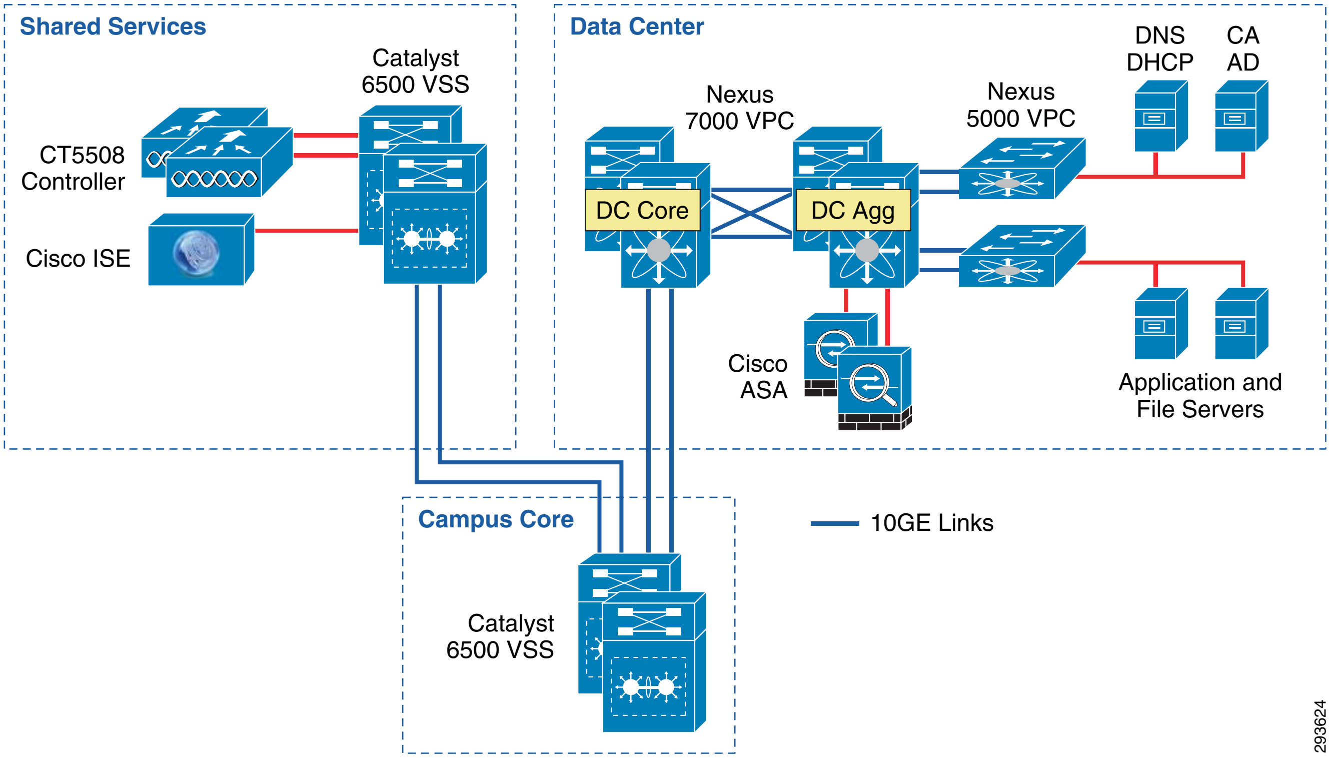
Unified Infrastructure Design to Support SGA

As described in SGT Deployment Scenarios in this CVD in Chapter 5, “Campus and Branch Network Design for BYOD,” two specific infrastructure deployment scenarios are examined in this CVD. The first use case uses the SGA Policy defined at the Identity Services Engine and the resulting SGACLs are dynamically exchanged with the Catalyst 6500 and Nexus 7000 infrastructure. The second use case also uses the SGA Policy defined at the Identity Services Engine, but enforces this policy through the configuration of Security Group Firewall (SG-FW) policies defined on an ASA providing secure access to data center resources.

In both scenarios, campus wireless users/devices connecting through centralized CUWN CT5508 controllers configured for local mode have access to data center resources based on their authorized roles and enforced through the use of SGT-based policies as implemented in the two deployment scenarios.

Figure 12-1 depicts the infrastructure that is used for purposes of SGA validation within the CVD.

Figure 12-1 TrustSec Infrastructure for BYOD v2.5 CVD

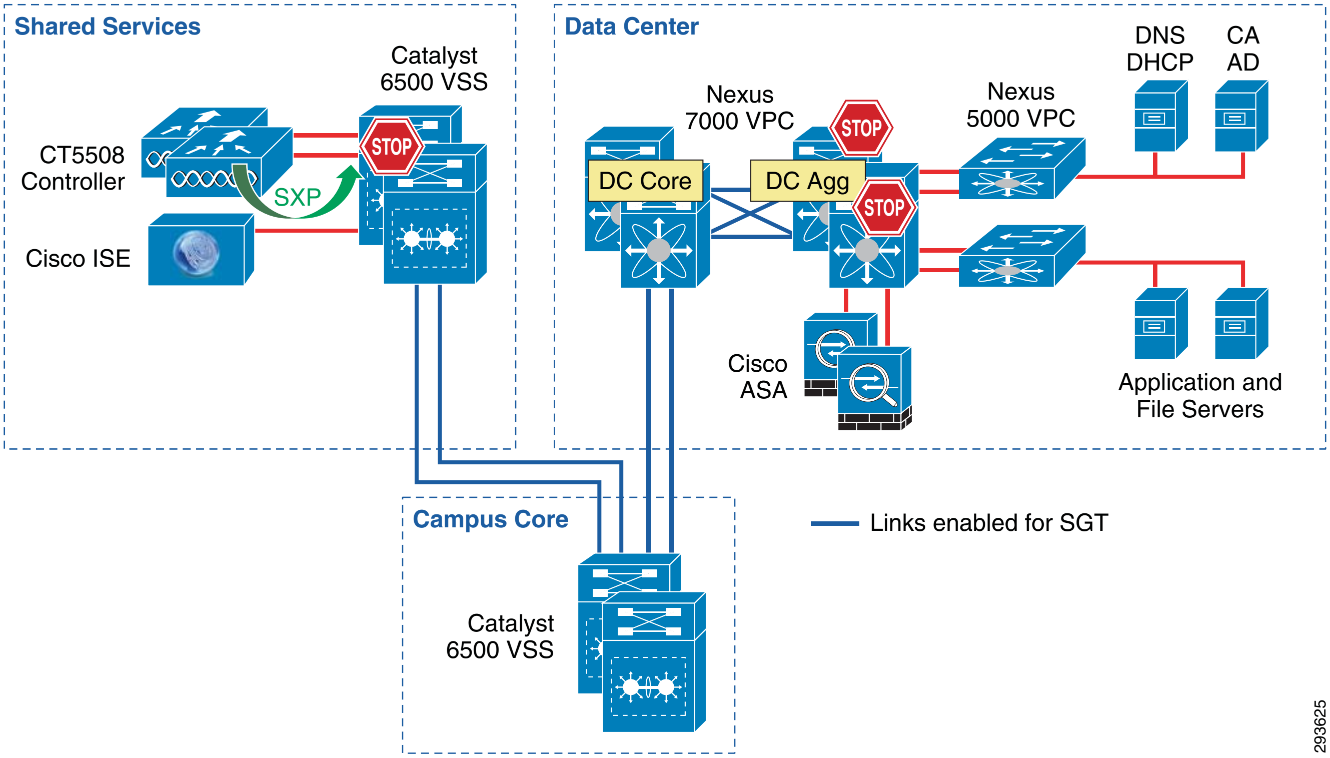


In Figure 12-1, the links extend between the Catalyst 6500 VSS in Shared Services to the Catalyst 6500 VSS in core and extends to the Nexus 7000 are 10GE links. On the Catalyst 6500s, WS-X6904 linecards with the FourX Adapters provide the 10GE interfaces while the N7K-M108X2-12L linecards provide the Nexus 7000 interfaces. The links between the Nexus 7000 and the Nexus 5548 are likewise connected to N7K-M108X2-12L linecards at the N7K and 10GE ports on the Nexus 5548. All other network connectivity for wireless controllers, ASA Firewalls, ISE, and the miscellaneous servers depicted are 1GE links.

Policy Configuration for SGACLs in Scenario 1

For Deployment Scenario 1, refer to Figure 12-2.

Figure 12-2 Infrastructure Deployment Scenario 1 SGT Enforcement



Deployment Scenario 1 requires that Security Group Tags are forwarded from the Shared Services Catalyst 6500 VSS, where the wireless controller is attached, through the core of the BYOD infrastructure enroute to servers located in the data center proper. In Figure 12-2, the links depicted in blue will be configured for SGT forwarding as well as manually configured for 802.1ae MACsec encryption. As previously discussed, the CT5508 wireless controller does not support native tagging on its 1GE interfaces, so a Security Group Tag Exchange Protocol (SXP) connection will be defined between the controller(s) and the Shared Services C6500 VSS switch as depicted above.

In this first scenario, wireless users, upon successful authentication and authorization, will be associated with a specific role and an IP to SGT mapping will be created on the wireless controller with the device's IP Address and the appropriate SGT. SXP will be used to communicate this mapping to the Shared Services Catalyst 6500s to which the wireless controllers are attached. As wireless user traffic egresses the Shared Services Catalyst 6500s, it will be tagged with the appropriate SGT learned via SXP from the wireless controller. As this traffic traverses the SGT-capable Core, this tag will be propagated hop-by-hop enroute to the Nexus 7000s comprising the data center switching infrastructure within which the various servers are located.

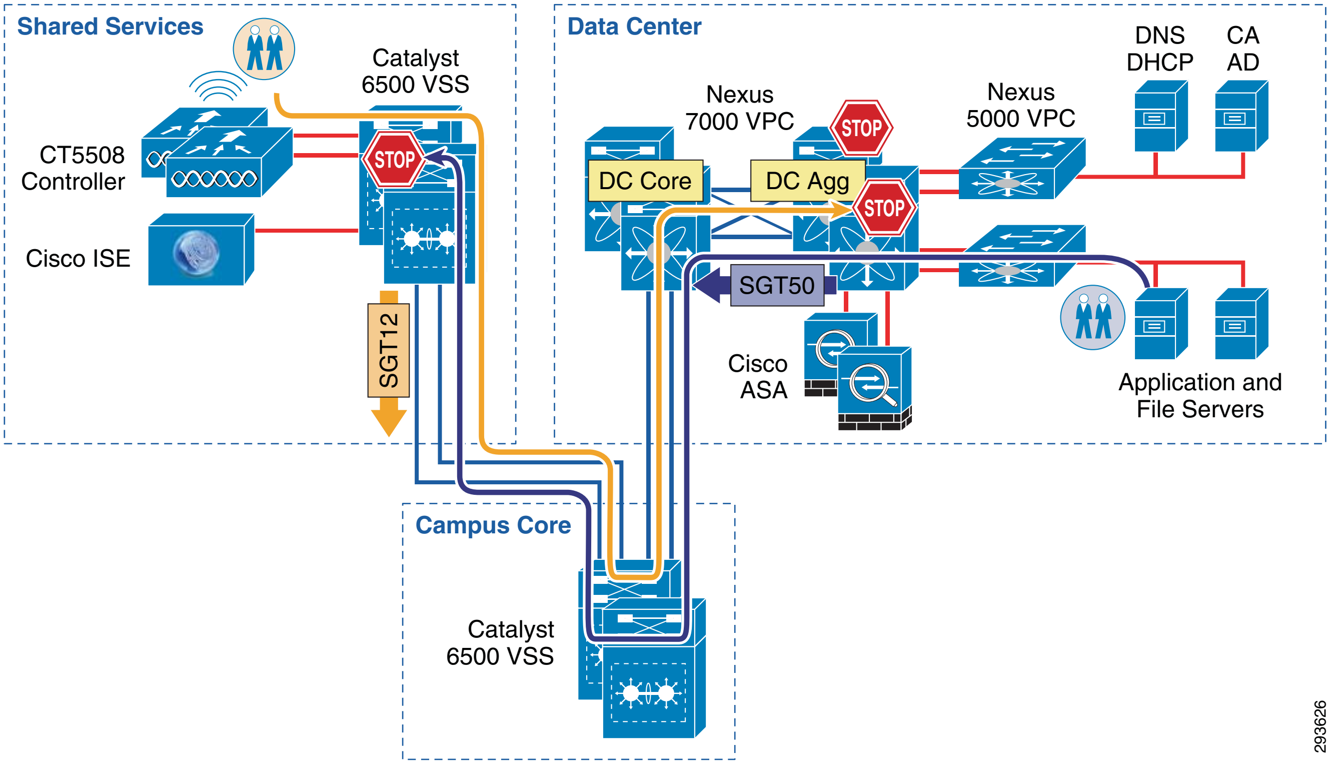
As 802.1X is not used to authenticate the servers residing in the Nexus data center infrastructure, the Server IP Address to SGT mapping can either be manually defined on the Nexus 7000 Data Center Aggregation switch or at the ISE server which would subsequently populate that mapping to the Nexus 7000. For purposes of the CVD, these mappings have been manually defined on the Nexus 7000 DC Aggregation Switch. As discussed in SGT Deployment Scenarios in this CVD in Chapter 5, "Campus and Branch Network Design for BYOD," there are other methods of associating traffic with a specific SGT on the Nexus 7000 platform.

As tagged user traffic arrives at the Nexus 7000 data center switch where the manual SGT mappings for the servers have been created, the traffic will be matched against TrustSec Policy (SGACL) defined either centrally at ISE or locally, as in the case of destination "Unknown" (SGT0), and will be either forwarded or dropped as applicable.

As discussed earlier, all server IP to SGT mappings have been manually created on the Nexus 7000 aggregation switches. As the servers are connected to the Nexus 5548 switches depicted in Figure 12-3, traffic from the Nexus 5548s egresses untagged as no mappings have been created there. Once this traffic passes through the Nexus 7000 Aggregation switch, the resident SGT mappings will be examined and the appropriate SGT imposed upon egress from the aggregation switch. In the event that traffic is initiated by a server associated with an SGT in the data center, the tagged traffic egresses the Nexus 7000 data center switches and traverses the Core and Shared Service infrastructure with the SGT propagated at each hop enroute to the destination, which is the wireless controller attached to the Shared Services 6500. Once the traffic arrives at the Shared Services 6500, the traffic will be matched against TrustSec Policy (SGACL) and will be either forwarded or dropped as defined.

Figure 12-3 depicts where SGACLs will be enforced in the Unified Access infrastructure.

Figure 12-3 Policy Enforcement in Deployment Scenario 1



The following major tasks are required for this deployment scenario and are outlined in the following sub-sections in Chapter 23, “BYOD Policy Enforcement Using Security Group Access”:

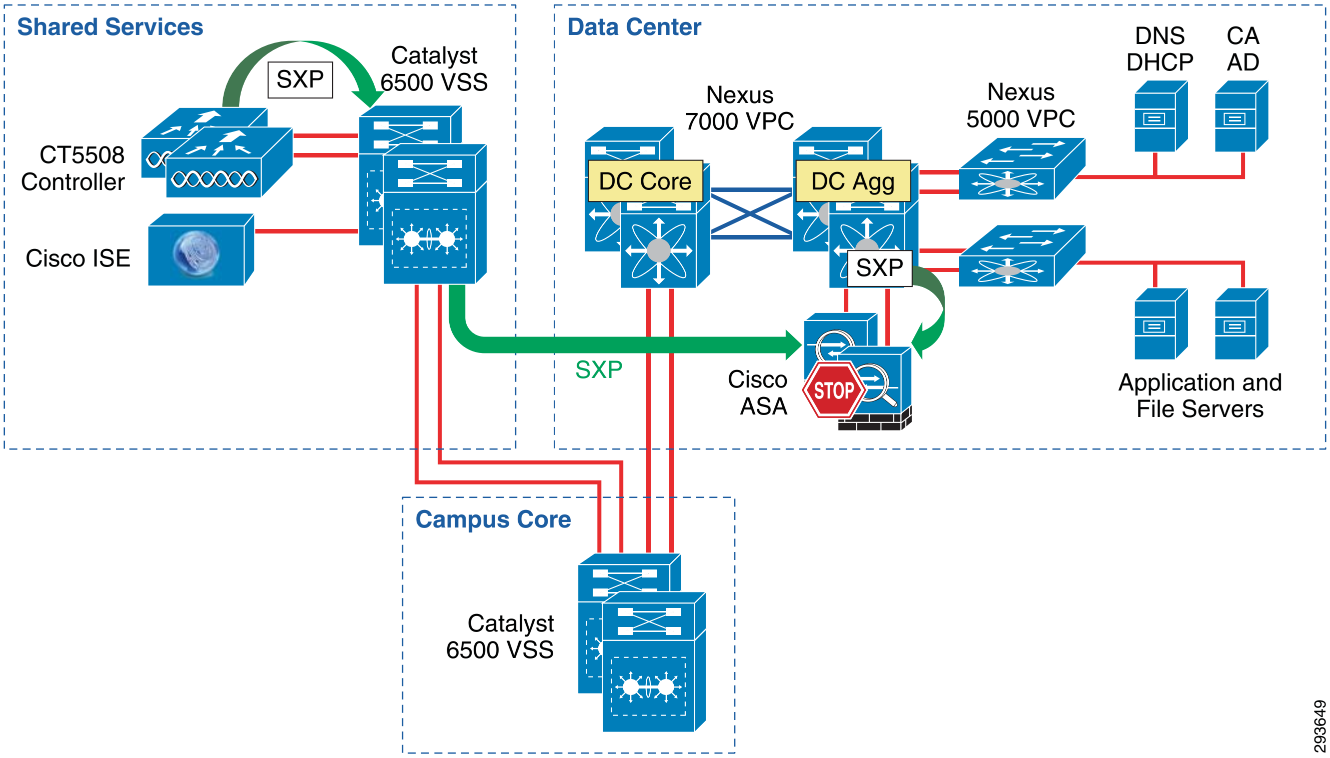
1. Configuring ISE to Support TrustSec
2. Configuring ISE for Network Access Device Authentication
3. Configuring Network Access Devices for Authentication at ISE
   a. RADIUS Server Configuration on the Wireless Controller
   b. RADIUS Server Configuration on the Catalyst 6500
   c. RADIUS Server Configuration on the Nexus 7000
4. Catalyst 6500 Platform Specific Considerations
5. Configuring Switching Infrastructure to Support TrustSec with 802.1ae MACsec Encryption

   a. Catalyst 6500 Commands
   b. Nexus 7000 Commands
6. Configuring Security Group Tag Exchange Protocol (SXP) for Wireless Controllers
   a. Wireless Controller Configuration
   b. Catalyst 6500 SXP Configuration
7. Configuring Static IP/SGT Bindings on Nexus Switches

Policy Configuration in Scenario 2

For the topology used in Deployment Scenario 2, refer to Figure 12-4.

Figure 12-4 Deployment Scenario 2 Configuration



With Deployment Scenario 2 an alternate means other than SGACLs is used to enforce SGA policy. In Scenario 2, the ASA running version 9.0 will be used as a Security Group Firewall (SG-FW) securing data center resources from outside access. As the ASA does not presently support Native SGT Tagging on its Ethernet interfaces, SXP must be used for it to learn IP/SGT mappings from other areas of the network where they have been dynamically learned or statically configured.

As in the case of the first deployment scenario, wireless users, upon successful authentication and authorization, will be associated with a specific role and an IP to SGT mapping will be created on the wireless controller with the device's IP Address and the appropriate SGT. Security Group Tag Exchange Protocol (SXP) will be used to communicate this mapping to the Shared Services Catalyst 6500s to which the wireless controllers are attached.

Unlike Scenario 1 however, the 10GE infrastructure between the Shared Services Catalyst 6500 VSS and the data center does not need to be enabled to support Security Group Tags or SGACLs. SXP will be used instead to re-advertise the mappings the Shared Services Catalyst 6500 VSS learned from the wireless controllers to the ASA Firewall.

The reason that a multi-hop SXP configuration is used from the wireless controller is primarily due to the fact that concentrating all of the controllers SXP advertisements at the 6500 VSS switch in Shared Services for single advertisement elsewhere in the network just provides a cleaner approach; it would be entirely possible to create the SXP peering directly between the wireless controller and the ASA firewall. The only other consideration lies in the fact that the WLC-5508 controllers used in this guide, as well as the WiSM2 only support four SXP connections, whereas the 6500 scales far beyond that.

In addition to the SXP Peering between the Shared Services 6500s and the ASA, the Nexus 7000 aggregation switches will require an SXP Peering to advertise SGT mappings that have been configured on them. It is by virtue of these SXP advertisements that the ASA is capable of inspecting the traffic from various devices and associating the appropriate tag for subsequent SG-FW policy enforcement as the ASA's interfaces are not TrustSec aware and incapable of manipulating the SGT.

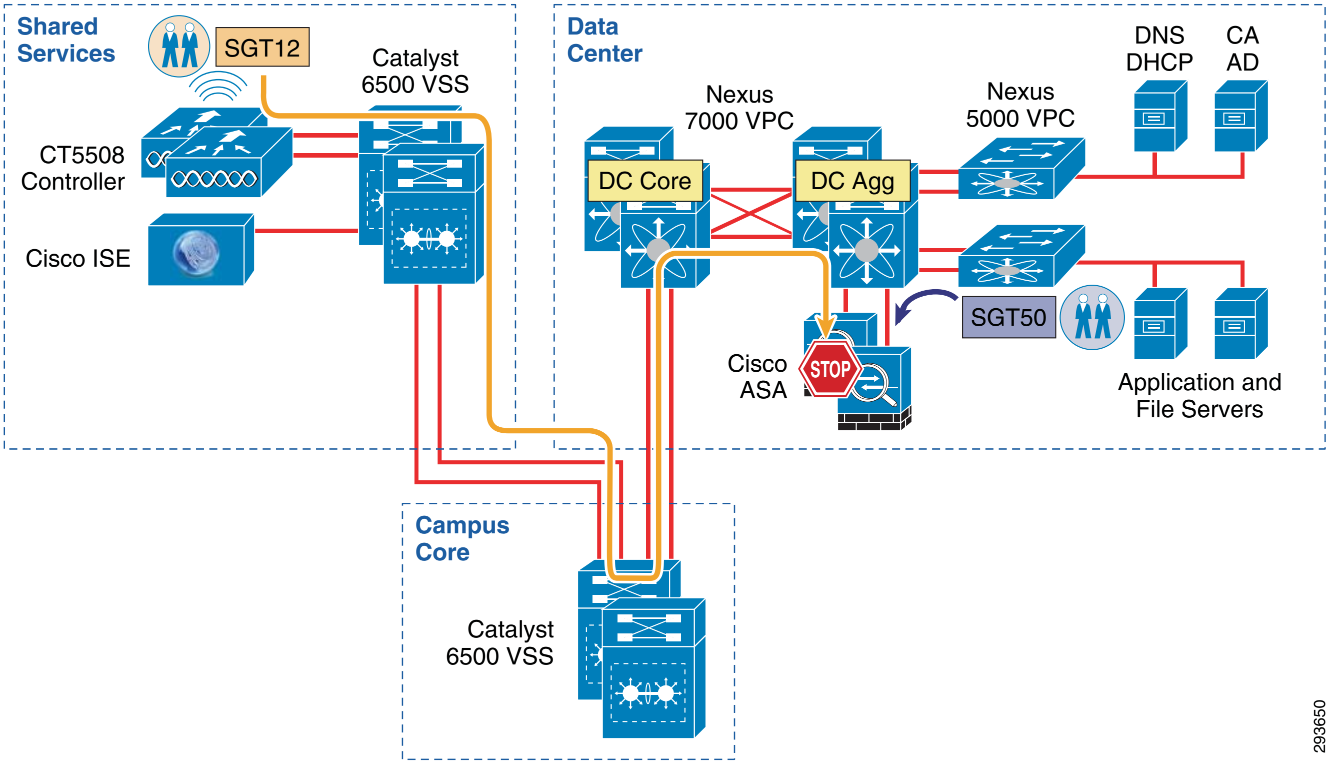
As previously discussed, the ASA Firewall that will be used to enforce SG-FW policies must be manually configured with SGT policies as Network Device Admission Control (NDAC) is presently not supported in the ASA and is therefore unable to acquire these policies dynamically from ISE. For more information regarding NDAC, refer to Chapter 23, "BYOD Policy Enforcement Using Security Group Access." These policies as defined in Chapter 23, "BYOD Policy Enforcement Using Security Group Access" for Deployment Scenario 2 can be configured via CLI, ASDM, or a management platform such as Cisco Security Manager.

As wireless traffic egresses the Shared Services Catalyst 6500s en route to the data center, the traffic will be untagged and will simply pass through the Core, enter the data center switching infrastructure, and ultimately arrive at the ASA Firewall where the appropriate SG-FW policy will be enforced.

Should any traffic be sourced from a server in the data center, it will likewise egress the Nexus 7000 aggregation switch untagged and be forwarded to the ASA firewall where any applicable SG-FW policy will be enforced.

Figure 12-5 depicts the infrastructure used in Deployment Scenario 2 and the means by which security group policies will be enforced.

Figure 12-5 SGA Policy Enforcement Using SXP and SG-FW



The following major tasks are required for this deployment scenario and are outlined in the following sub-sections in Chapter 23, "BYOD Policy Enforcement Using Security Group Access":

1. Configuring ISE to Support TrustSec
2. Configuring ISE for Network Access Device Authentication
3. ISE Configuring the Network Devices for Integration with ISE
    a. RADIUS Server Configuration on the Wireless Controller
    b. RADIUS Server Configuration on the ASA Firewall
    c. RADIUS Server Configuration on the Nexus 7000
4. Configuring Security Group Tag Exchange Protocol (SXP) for Wireless Controllers
    a. Wireless Controller Configuration
    b. Catalyst 6500 SXP Configuration
    c. Nexus 7000 SXP Configuration
    d. ASA SXP Configuration
5. Configuring Static IP/SGT Bindings on Nexus Switches
6. Configuring SG-FW Role-Based Policies at ASA

TrustSec Summary

For information regarding the detailed, platform-specific configuration steps, refer to the TrustSec section in Chapter 23, "BYOD Policy Enforcement Using Security Group Access."

Note Patch 1 for ISE 1.2 **MUST** be installed in order for NDAC (Network Device Admission Control) to function properly between the network device and ISE. Without Patch 1, the network device will be unable to authenticate with ISE in order to derive TrustSec environment data, PAC file, and security group policies when CTS Manual Mode is configured and, additionally, the credentials required to authenticate peers/TrustSec links when CTS Dot1x Mode is configured. Refer to the ISE 1.2 Release Notes for additional information regarding this **very important** information.

Mobile Device Manager Integration for BYOD

Revised: August 7, 2013

The Cisco ISE can be configured to integrate with third-party Mobile Device Manager (MDM) products through an XML-based API. This allows network policy decisions based on mobile device posture that can include PIN lock, storage encryption, or registration status. In this release, both Apple and Android devices are supported. Configuring the infrastructure to support this functionality involves setting up ISE to send API requests to the MDM and configuring the MDM to accept these requests. Chapter 6, "Mobile Device Managers for BYOD" includes a discussion of the communications between the various components. Some MDM configurations, including device compliance policy, are discussed in general terms in this section. Detailed partner specific information can be found in supporting documentation at: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/own_device.html.

An overview of the topology common with the MDM architecture is presented below. The two basic models that are detailed in this section are an On-Premise model and a Cloud-based SaaS model. The components are similar except that the cloud model can also include an on-premise component to facilitate the integration with the enterprise.

Establishing IP Connectivity for an On-Premise MDM

Typically the on-premise MDM resides in the DMZ or some location where mobile devices can establish inbound connections. This allows the MDM to monitor the device's posture while the device is on the outside of the firewall. Without this access, the device would need to be placed on the network and interrogated prior to establishing the posture compliance of the device. The device does not automatically update the server whenever it joins a new network, therefore this interrogation would need to be manually initiated by the enterprise. If the MDM is located in the data center, some provision is required to allow inbound TCP sockets from the Internet. The specific ports vary based on the MDM partner and are detailed in the supporting documentation on Design Zone.

In addition to inbound sessions from the devices, the MDM needs to establish outbound connections to the push servers. The MDM uses the push service to locate and notify the device of changes to the MDM policy. Apple refers their service as the Apple Push Notification Service (APNS) and requires an Apple signed certificate to authenticate the MDM. Google refers to their service as Google Cloud Messaging for Android (GCM). This service replaces the older Cloud to Device Messaging Framework (C2DM). Both Apple and Android incorporate the push service into the device's operating system (OS) to allow the MDM server to communicate with the MDM client application. Apple devices also allow the MDM to communicate with the OS MDM API with the appropriate credentials. Both require the end user to establish an account with either Google or Apple respectively. This account effectively binds a device list to a user.

The MDM will also host a user-centric My Devices Portal to allow users to log into the MDM and manage some aspects of their device. This is similar but distinct from the My Devices Portal offered by ISE and serves a different purpose. Users may attach from either the mobile device or their standard desktop. The MDM web server can be configured with ACLs to restrict access to the My Devices Portal page from specific source address. For example, it is possible to block Internet access to the portal. The same is true for the administrator website.

The MDM will also receive inbound HTTPS session on port 443 by default to support the API used by ISE. In contrast to the MDM placement, ISE should be located in the data center. Firewall policy should be set to allow TCP 443 sessions that are initiated from ISE towards the MDM server. The MDM will have a default route pointing towards an outbound firewall and a more specific route to ISE pointing towards an inbound firewall. The majority of MDM partners support on-premise deployments on VM servers that may support multiple interfaces. It is possible that the route to ISE may be over a dedicated link. The topology of the DMZ should match the established corporate policy for servers. Typically the MDM will also allow the administrator to protect the API with an ACL. In this case, the ACL could be configured to permit ISE but deny any other connections.

ISE supports the use of a proxy for external connections. Currently the proxy configuration is globally configured. If ISE is required to use a proxy for the feed service, then it will also direct MDM requests to the proxy. This could cause connectivity issues between ISE and an on-premise MDM. In this scenario, the proxy configuration will require careful review to ensure that the ISE can connect to the MDM via the proxy.

Establishing IP Connectivity for a Cloud-Based MDM

Subscribing to an online MDM service simplifies many of the connectivity issues, especially between the mobile devices and the device manager. Because personal mobile devices spend the majority of time connected to the public Internet, choosing this model offers some advantages over a traditional on-premise model. The Apple APNS or Google GCM are also simplified when a cloud model is in use. The enterprise will still need to generate a certificate-signing request and present that to Apple prior to using the APNS service. This is explained in the partner-specific supporting documentation. However with the advantages realized with a cloud deployment, there are also challenges with respect to enterprise integration, specifically the corporate directory structure. Without any integration, a separate and dedicated user database would need to be established and maintained on the MDM servers. Typically in the cloud model, the enterprise will establish a small integration server that resides in the DMZ and serves as a proxy to a secure LDAP binding. This is explained in the partner-specific supporting documentation. With the exception of this additional server, all of the other components found in the on-premise model are present in a cloud model.

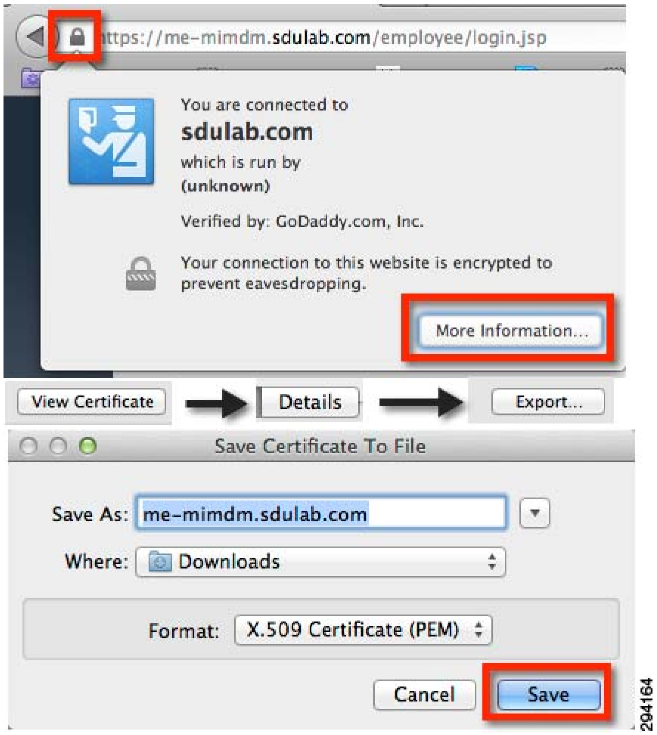
The primary concern is the HTTPS connection between ISE and the cloud-based MDM server, which is outbound from ISE. Corporate firewalls need to allow the ISE server siting in the data center to establish outbound HTTPS servers to the MDM server. The MDM partner may be able to provide a range of destination subnets if outbound sessions are restricted from data center servers such as ISE. Before ISE will trust the MDM server, the MDM server’s certificate should be imported into the local ISE certificate store (this is explained below). The MDM service will provide the URL of the API. It is this certificate on this site that should be imported. In addition, users will need to be able to establish outbound HTTPS connections to the My Devices Portal page on the cloud-based MDM server. This would only be a concern in environments where users are not allowed access to Internet websites. If WCS or ScanSafe is in use, then the enterprise should confirm that the MDM site has a reputation score that exceeds the threshold needed for access or the site should be manually added to the permitted whitelist. Routing is straightforward. ISE and the user devices will follow the default route towards the Internet. The session may flow over NAT boundaries without requiring a NAT fix-up.

Connectivity must also be provided to mobile clients that have been quarantined to the MDM and to either the Apple Push Service or Google Cloud Messaging Servers. This allows the MDM to communicate with the device as needed to update the device's posture information on the server. In some situations, the mobile client may also need access to Google Play and the Apple AppStore to download required applications such as the MDM mobile client.

Configure ISE to Authenticate the MDM API

Prior to configuring the MDM, ISE must trust the HTTPS certificate presented by the MDM website. In either the cloud or on-premise deployment model, this can be accomplished by installing the MDM's HTTPS certificate in the ISE certificate store. The easiest method is to browse to the MDM server, export the HTTPS certificate, and then import it into ISE. Figure 13-1 shows this in Firefox, however the procedure may be different for other browsers.

Figure 13-1 Exporting MDM Certificate



ttps://me-mimdm.sdulab.com/employee/login.jsp

You are connected to
sdulab.com
which is run by
(unknown)

Verified by: GoDaddy.com, Inc.

Your connection to this website is encrypted to prevent eavesdropping.

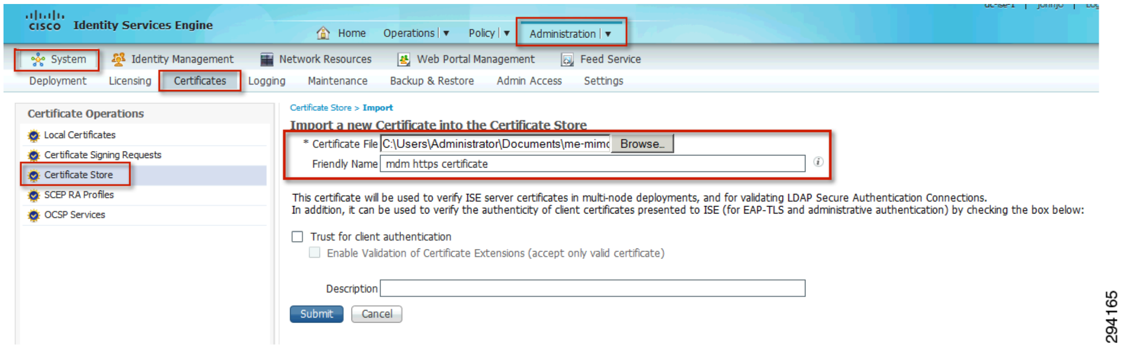
Save As: me-mimdm.sdulab.com

Where: Downloads

Format: X.509 Certificate (PEM)

Once the certificate has been saved to the local disk, the user will import it into the local certificate store on ISE. By default, the browser will save the certificate file with a name based on identity contained in the certificate, which is typically the FQDN of the site. The file extension could be .com, which is a well-known MS-DOS extension, making the cert more difficult to locate. While this does not affect importing the certificate, it could make browsing for the file on the hard drive less obvious. Importing the certificate into ISE is shown in Figure 13-2.

Figure 13-2 Importing Certificate into ISE



Import a new Certificate into the Certificate Store

* Certificate File: C:\Users\Administrator\Documents\me-mimc

Friendly Name: mdm https certificate

This certificate will be used to verify ISE server certificates in multi-node deployments, and for validating LDAP Secure Authentication Connections.
In addition, it can be used to verify the authenticity of client certificates presented to ISE (for EAP-TLS and administrative authentication) by checking the box below:

□ Trust for client authentication

□ Enable Validation of Certificate Extensions (accept only valid certificate)

Description:

If ISE and the MDM are using the same CA, then importing the MDM SSL certificate may not be required. ISE does not maintain a system list of well-known public root certificates, therefore all trust relationships must be established by the administrator. Installing the MDM SSL certificate is the simplest approach and is shown here to ensure success.

Creating the MDM API User Account

In addition to the certificate, ISE will need a user account on the MDM that will allow access to the API. The previously installed certificate allows ISE to attach to the MDM via HTTPS, which will encrypt all data exchanges between ISE and the MDM, including the API credentials. All of the MDM partners support a local user account that can be granted API privileges. Some vendors may allow the account to be defined in an external data store such as Active Directory. This could be useful if ISE is using the same account to access AD or other resources and centralized machine account management is in use. In all cases, the API user account should be protected by strong passwords. For specific guidance on setting up this account, refer to the partner-specific supporting documentation or the partner MDM Administrator guide.

There are two account issues that may prevent the API from functioning properly:

- Incorrect username or password combination
- Defined user has not been granted API access

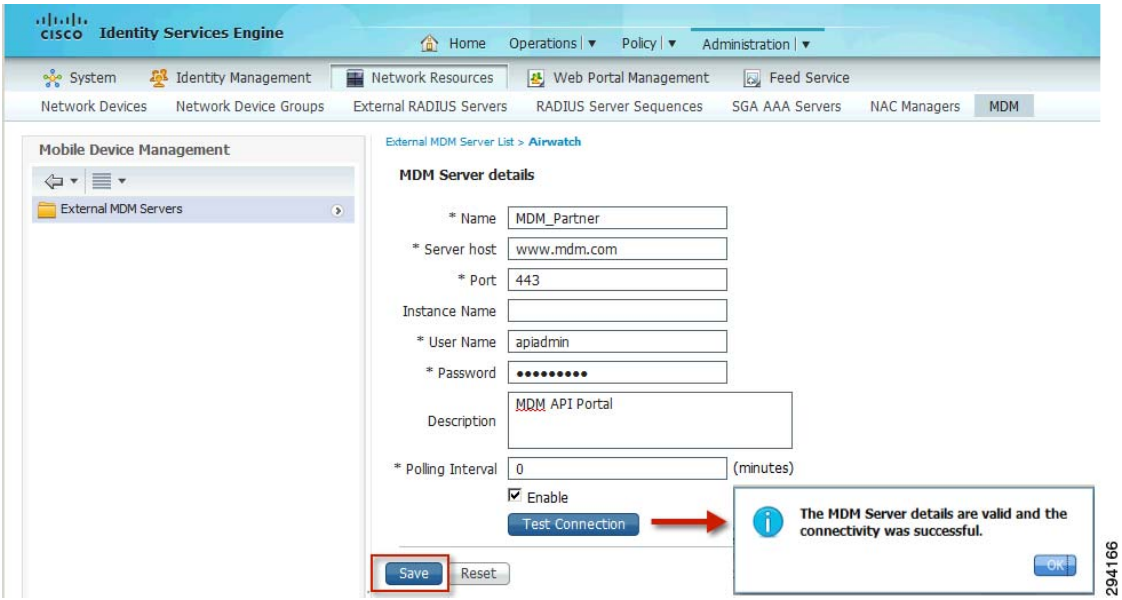
Setting Up the MDM Connection

ISE will contact the MDM to gather posture information about devices or to issue device commands such as corporate wipe or lock. The session is initiated from ISE towards the MDM server. The URL for the MDM server is typically the same as the admin page and will be the same website used to export the certificate. The directory path is handled automatically by the system and is not specified as part of the configuration. The instance is used in multi-tenant deployments more commonly found when subscribing to a cloud service. The field should be left blank unless the cloud provider has instructed otherwise. The port will typically be TCP 443 for HTTPS. Typically the MDM cannot be configured to listen on a specific port for API users. Any change will also impact both the admin and user portal pages.

The polling interval specifies how often ISE will query the MDM for changes to device posture. By default, this is set to 0 minutes, effectively disabling polling. Polling can be enabled to periodically check the MDM compliance posture of an endpoint. If the device is found to be out of compliance and the device is associated to the network, then ISE will issue a CoA forcing the device to re-authenticate. Likely the device will need to remediate with the MDM, although this will depend on how the policy is configured. Note that MDM compliance requirements are configured on the MDM and are independent of the policy configured on ISE. It is possible, although not practical, to set the polling interval even if the ISE policy does not consider this dictionary attribute. The advantage of polling is that if a user takes the device out of MDM compliance, they will be forced to reauthorize that device. The shorter the window, the quicker ISE will discover the condition. There are some considerations to be aware of before setting this value to an aggressively low value. The MDM compliance posture could include a wide range of conditions not specific to network access. For example, the device administrator may want to know when an employee on a corporate device had exceeded 80% of the data plan to avoid overage charges. In this case, blocking network access based solely on this attribute would aggravate the MDM compliance condition and run counter the device administrator intentions. In addition, the CoA will interrupt the user WiFi session, possibly terminating real-time applications such as VoIP calls. The recommendation is to leave the polling interval at 0 until a full understanding of the MDM's configuration is complete. If the polling interval is set, then it should match the device check-in period defined on the MDM. For example, if the MDM is configured such that devices will report their status every four hours, then ISE should be set to the same value and not less than half of this value. Over sampling the device posture will create unnecessary loads on the MDM server and reduced battery life on the mobile devices.

Finally, the enable check box will be set to active on one MDM server. It is possible to save multiple configurations, but only one can be active at a time. Figure 13-3 shows a typical configuration.

Figure 13-3 MDM Server Details



MDM Server details

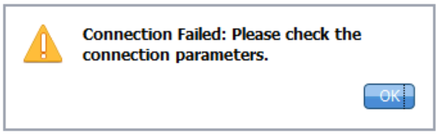
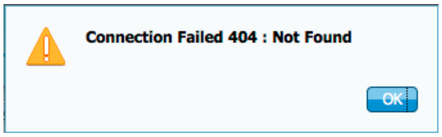
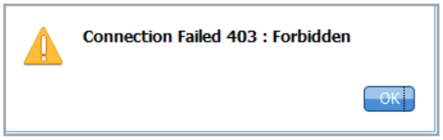
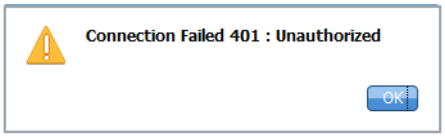
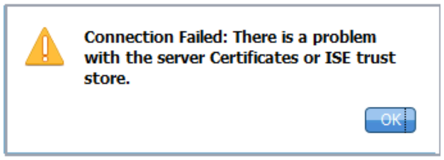
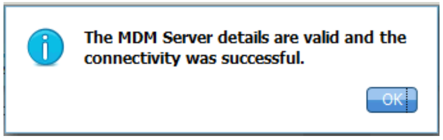
* Name: MDM_Partner
* Server host: www.mdm.com
* Port: 443
Instance Name:
* User Name: apiadmin
* Password: •••••••••
Description: MDM API Portal
* Polling Interval: 0 (minutes)
☑ Enable

The MDM Server details are valid and the connectivity was successful.

Verifying the MDM Connection

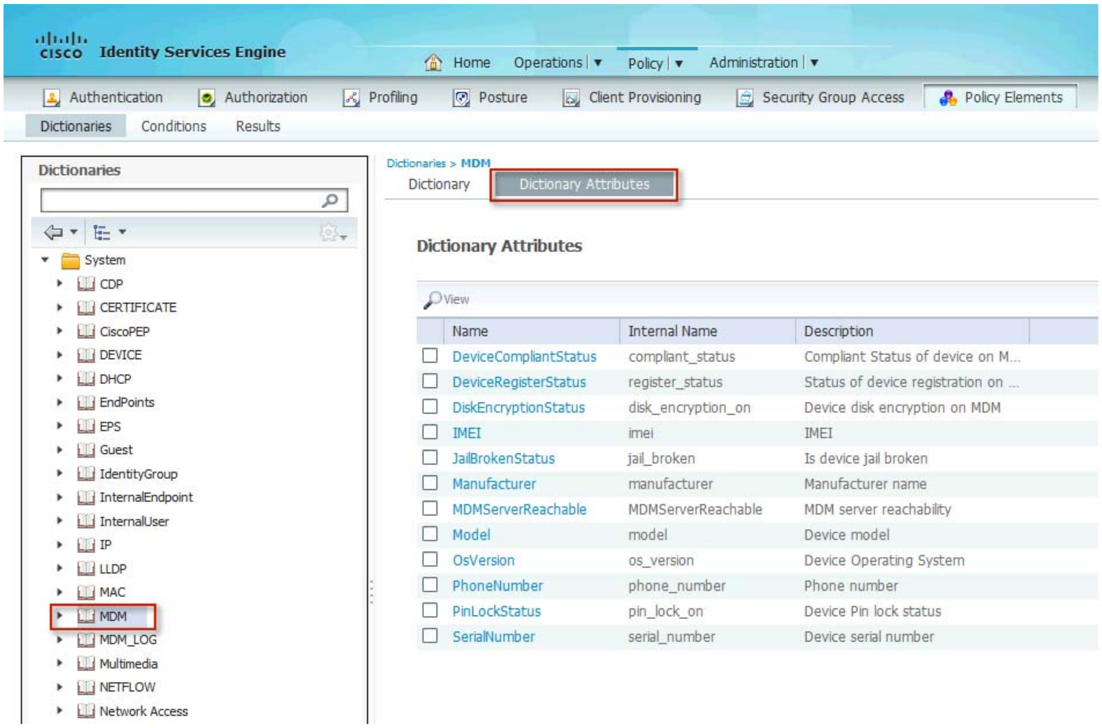
The test button will establish a connection to the MDM and attempt to authenticate using the configured credentials. This should be complete prior to saving the settings. If not, then the save button will validate the settings. If any errors are encountered, the MDM Enable button will be deselected prior to saving. If any error messages are presented, the administrator can refer to Table 13-1 for guidance in correcting the setup. In order to re-run the test on a previously validated server, the user should deselect the Enable checkbox, save, and then re-enable the checkbox.

Table 13-1 Common MDM Connection Error Codes

 Connection Failed: Please check the connection parameters.	A routing or firewall problem exists between ISE located in the data center and the MDM located in either the DMZ or Cloud. The firewall's configuration should be checked to confirm HTTPS is allowed in this direction.
 Connection Failed 404 : Not Found	The most likely cause of an HTML 404 error code is that an instance was configured when it was not required, or that the wrong instance has been configured.
 Connection Failed 403 : Forbidden	The user account setup on the MDM server does not have the proper roles associated to it. Validate that the account being used by ISE is assigned the REST API MDM roles as shown above.
 Connection Failed 401 : Unauthorized	The user name or password is not correct for the account being used by ISE. Another less likely scenario is that the URL entered is a valid MDM site, but not the same site used to configure the MDM account above. Either of these could result in the MDM server returning an HTML code 401 to ISE.
 Connection Failed: There is a problem with the server Certificates or ISE trust store.	ISE does not trust the certificate presented by the MDM website. This indicates the certificate was not imported to the ISE certificate store as described above or the certificate has expired since it was imported.
 The MDM Server details are valid and the connectivity was successful.	The connection has successfully been tested. The administrator should also verify the MDM dictionary has been populated with attributes.

After successfully configuring the MDM, the ISE policy dictionary will contain the attributes needed to create policy. The user can verify the dictionary by clicking **Policy > Dictionaries > System > MDM**, as shown in Figure 13-4.

Figure 13-4 Dictionary Attributes



Dictionary Attributes

	Name	Internal Name	Description
□	DeviceCompliantStatus	compliant_status	Compliant Status of device on M...
□	DeviceRegisterStatus	register_status	Status of device registration on ...
□	DiskEncryptionStatus	disk_encryption_on	Device disk encryption on MDM
□	IMEI	imei	IMEI
□	JailBrokenStatus	jail_broken	Is device jail broken
□	Manufacturer	manufacturer	Manufacturer name
□	MDMServerReachable	MDMServerReachable	MDM server reachability
□	Model	model	Device model
□	OsVersion	os_version	Device Operating System
□	PhoneNumber	phone_number	Phone number
□	PinLockStatus	pin_lock_on	Device Pin lock status
□	SerialNumber	serial_number	Device serial number

Configuring the MDM

In addition to the API user account needed for ISE, there are several other administrative tasks that need to be accomplished on the MDM, such as signing and installing the APNS certificates before ISE can issue device actions through the API. The partner-specific supporting documentation has additional details on the minimum requirements. The MDM can also be configured to integrate with the corporate directory structure through LDAP. The administrator should review the MDM installation and administration guides to bring the MDM system into a fully functional state.