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:

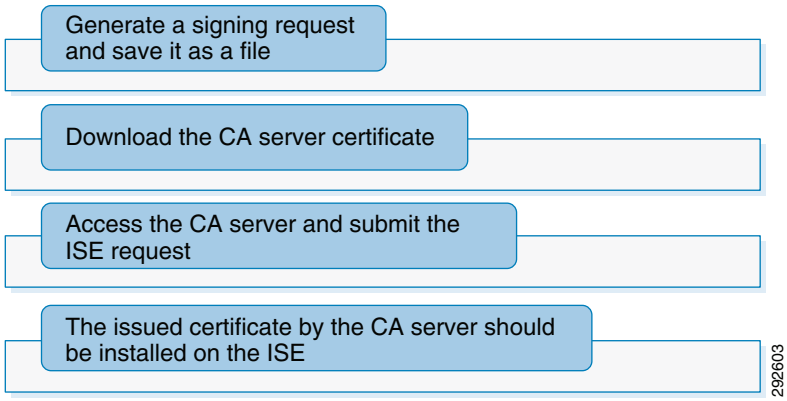
- Administration—The administration node handles all system level configuration. There can be one primary and one secondary administration node in a distributed deployment.
- Monitoring—The monitoring node handles log collection and provides monitoring and troubleshooting tools. There can be one primary 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



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

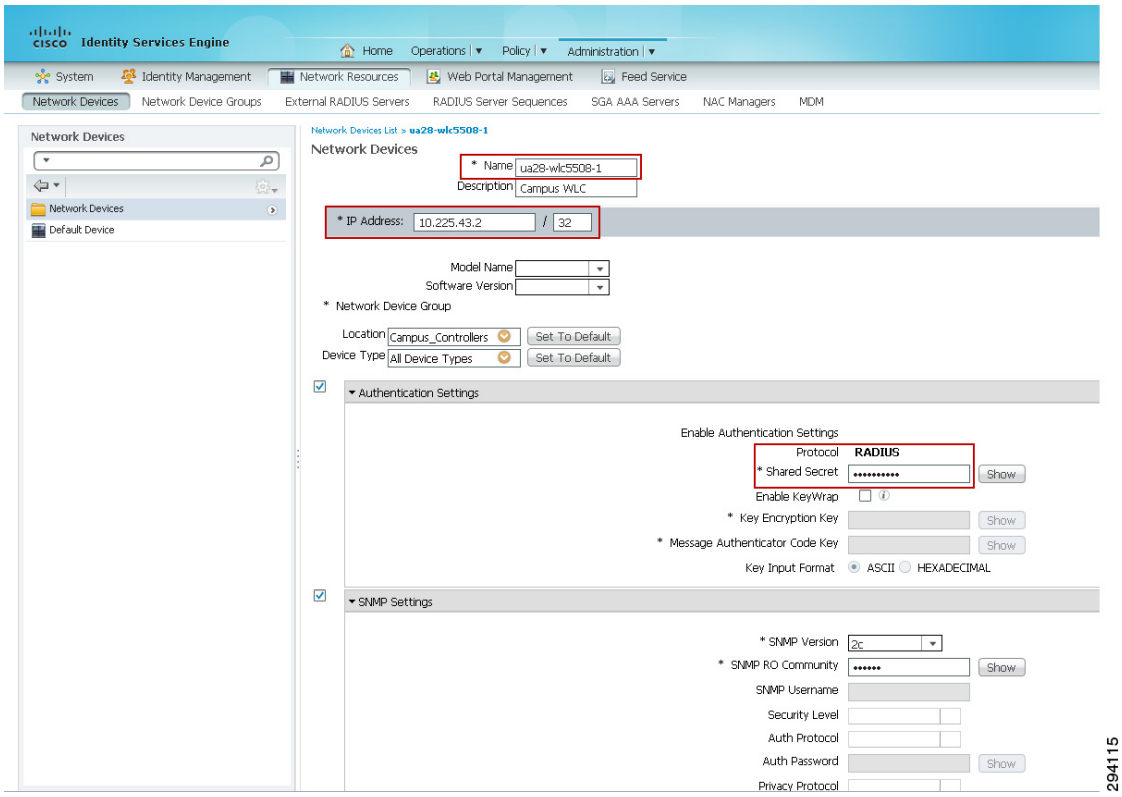
A network device is an authentication, authorization, and accounting (AAA) client through which AAA service requests are attempted, for example, switches, routers, and so on. The network device definition enables the Cisco Identity Services Engine (Cisco ISE) to interact with the network devices that 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

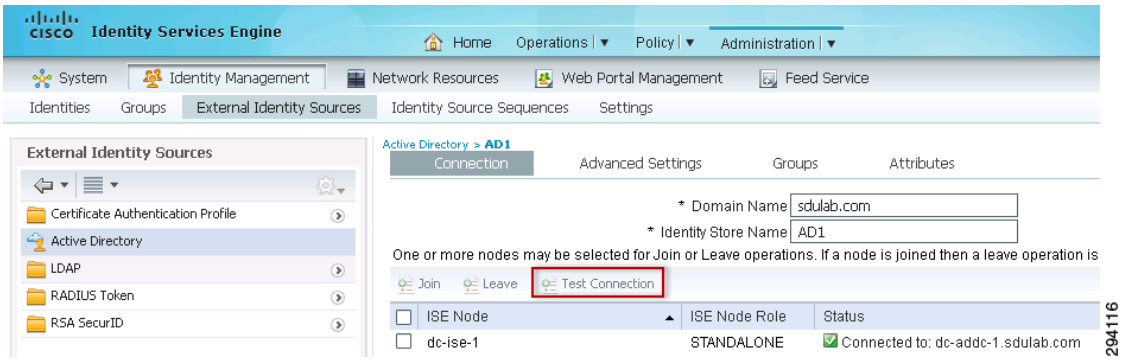


ISE Integration with Active Directory

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



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.

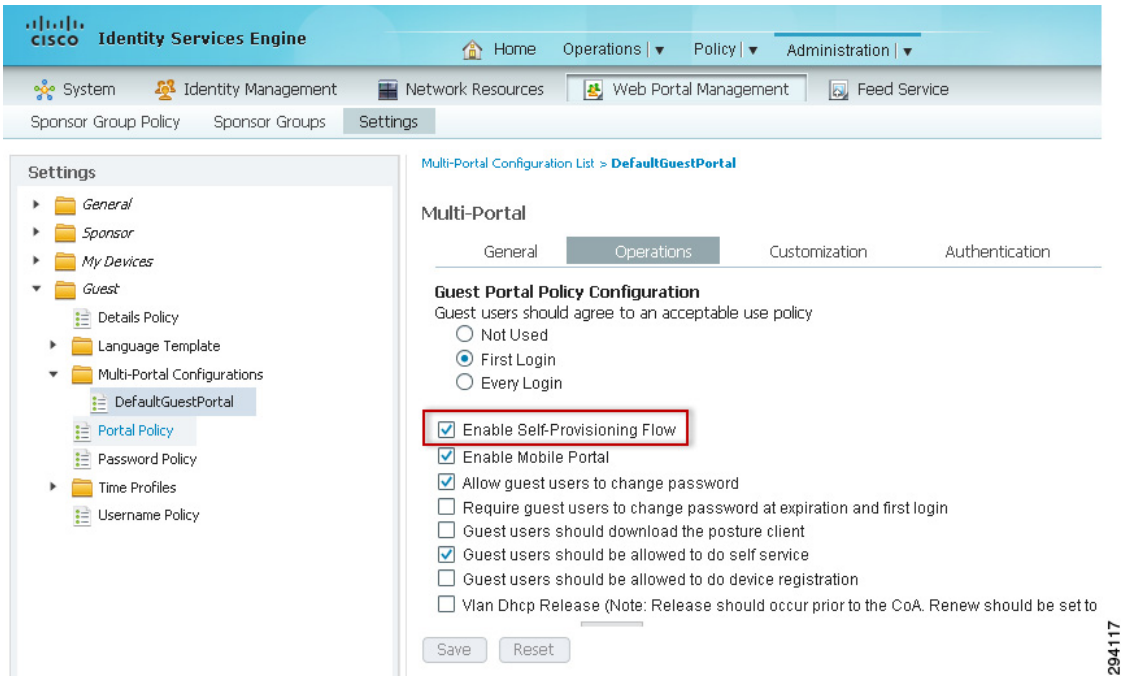
ISE enables self-provisioning, which allows employees to register their personal devices. The ISE provisions the device with its native supplicant during device registration.

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

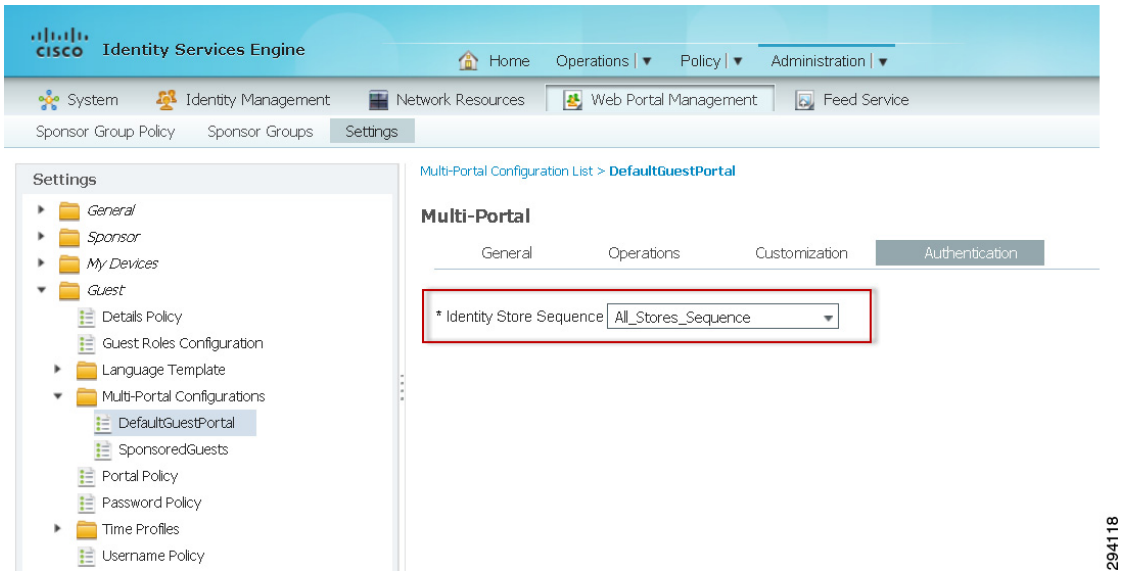


The DefaultGuestPortal refers to the portal used for self-registration—otherwise known as the Self-Registration portal in this document.

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.

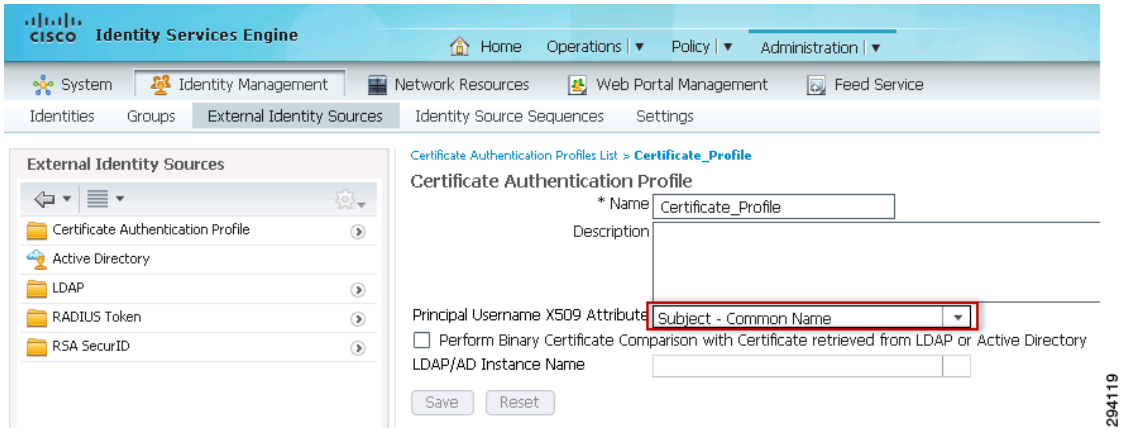
Figure 10-5 Authentication Portal Settings



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

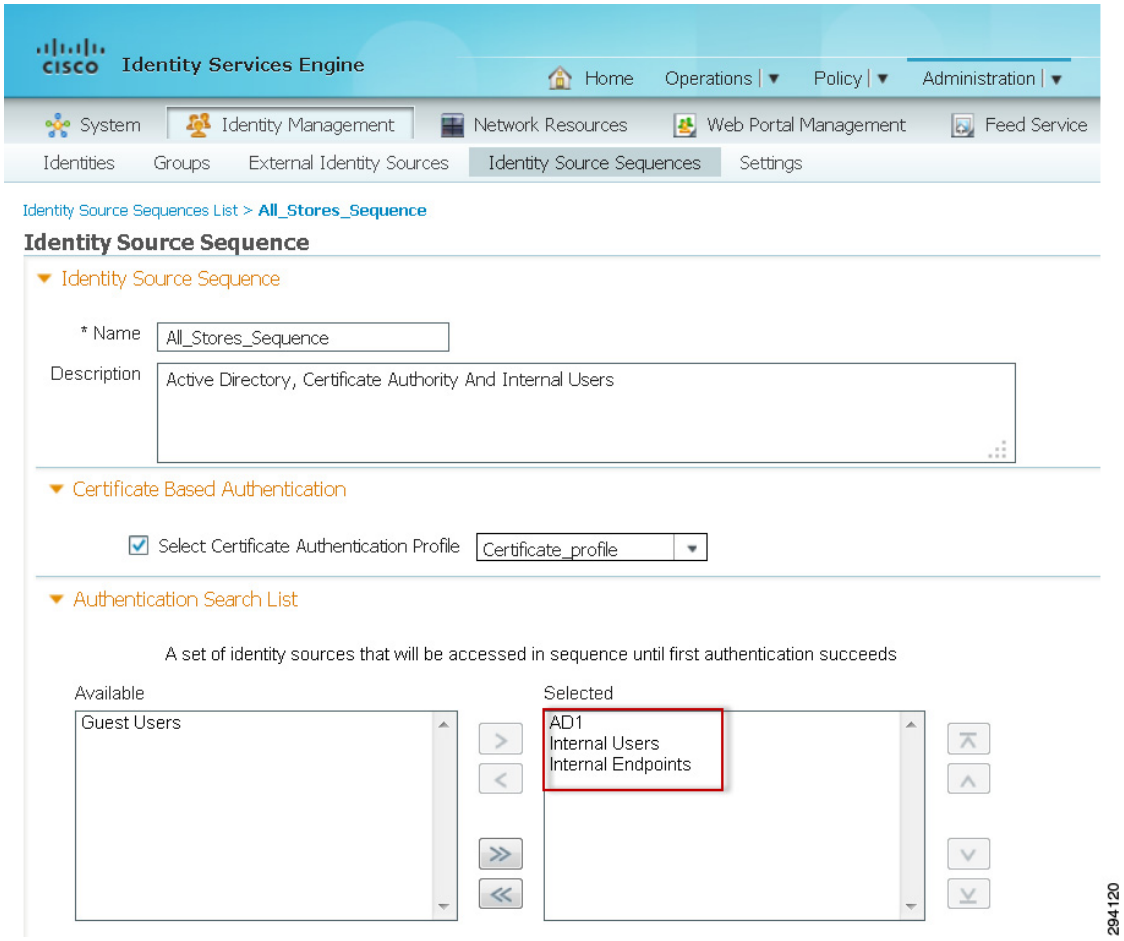


Identity Source Sequences

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

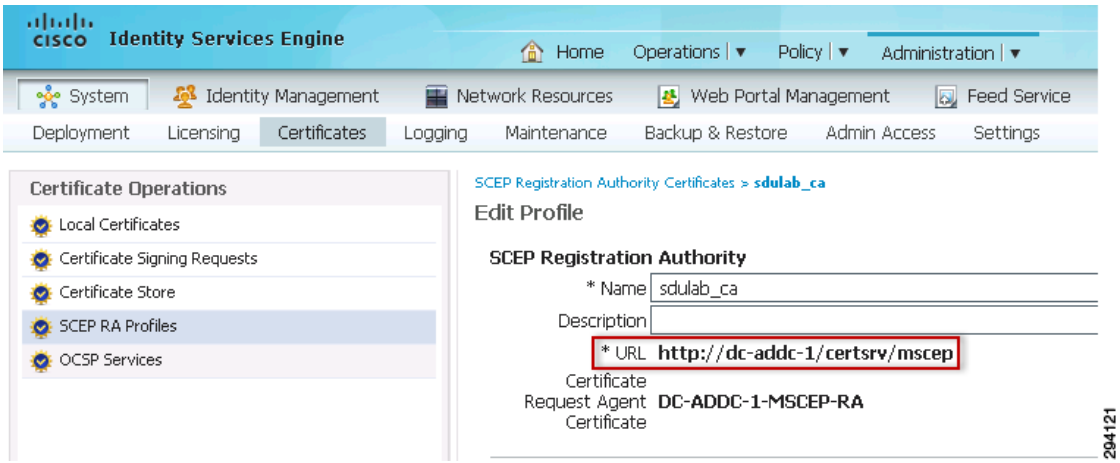


SCEP Profile Configuration on ISE

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.

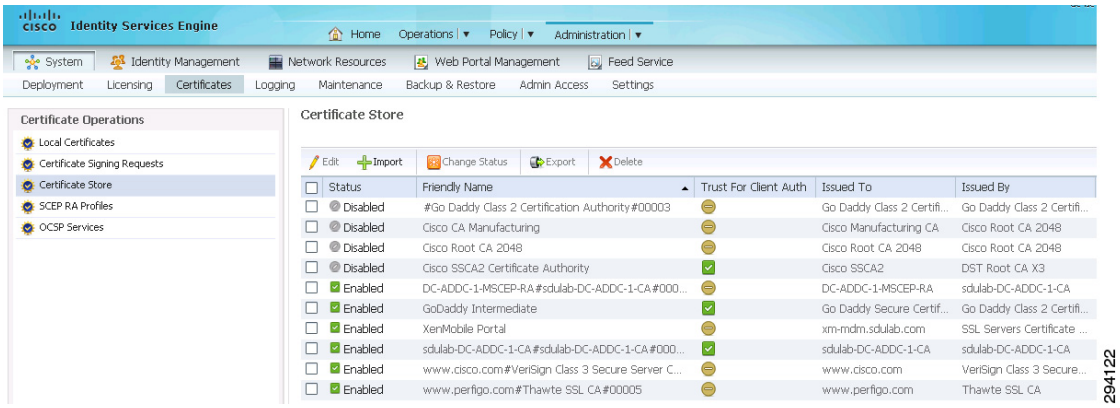
To configure SCEP profile on the ISE, click **Administration > Certificates > SCEP RA Profiles > Add**. Define the SCEP profile, as shown in Figure 10-8.

Figure 10-8 SCEP Profile Configuration



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



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
```

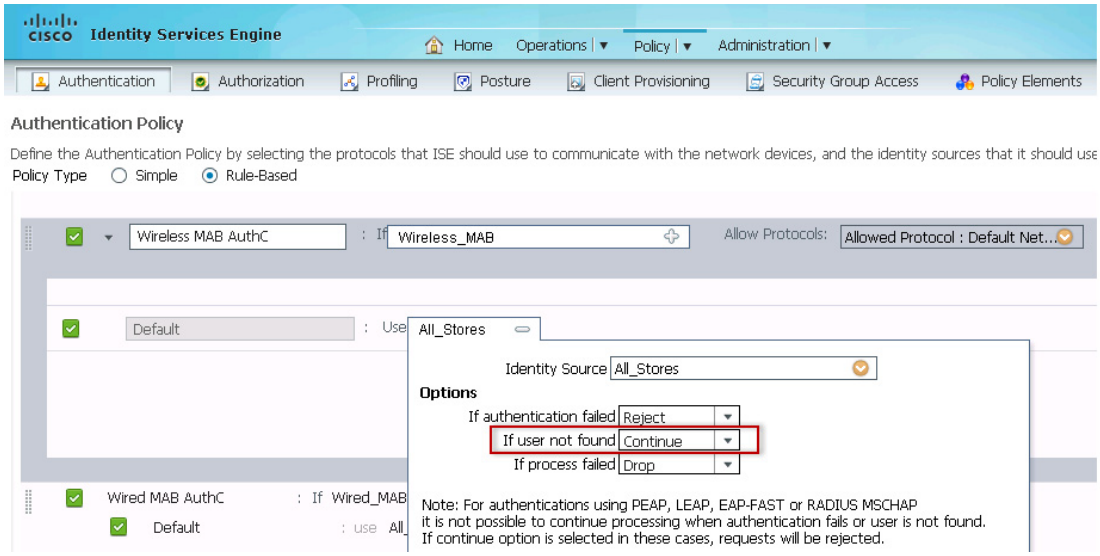
```
Else
     Use Default Rule
```

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



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

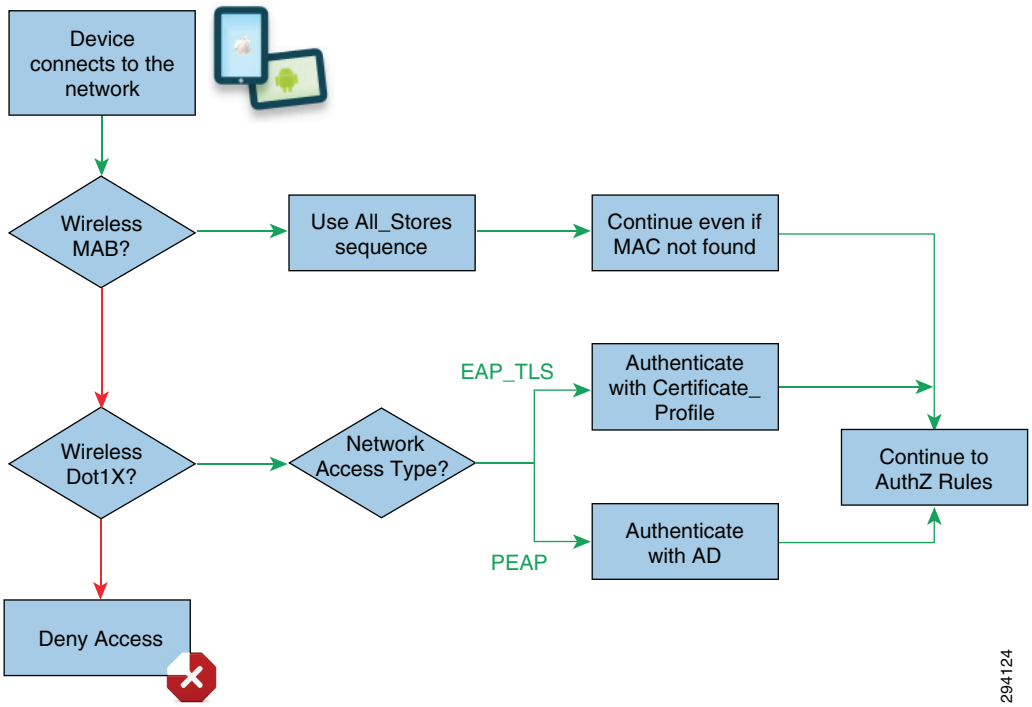


Table 10-1 explains how these rules are implemented in this design guide.

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

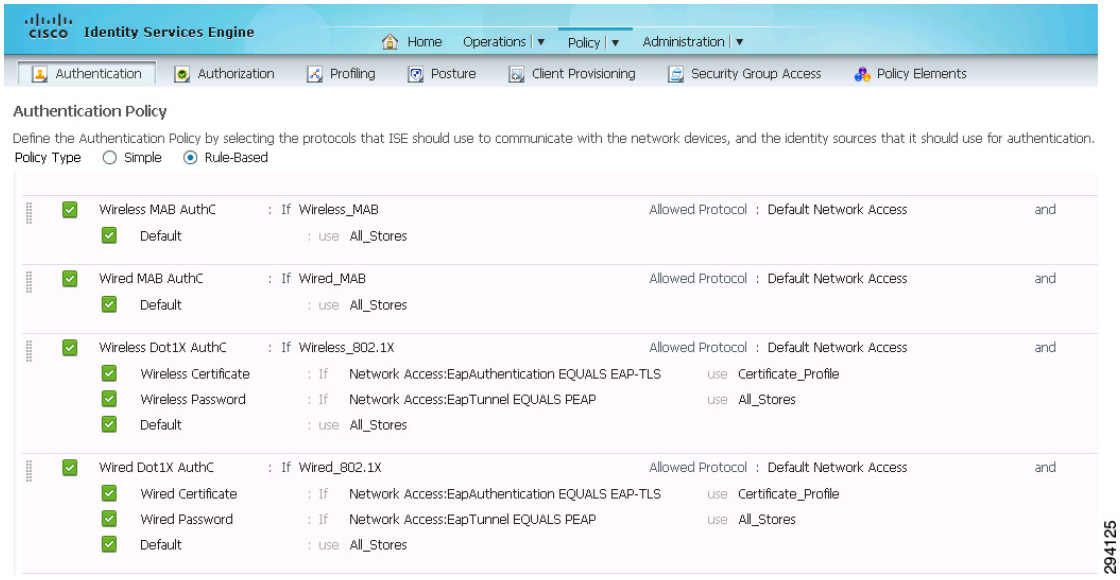
The endpoint devices could use either MAB or dot1x protocol when connecting to the wireless network. The authentication policy for wireless networks using MAB is explained in the previous section. This section explains the authentication policy for wireless medium using dot1X protocol, as shown in Table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



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

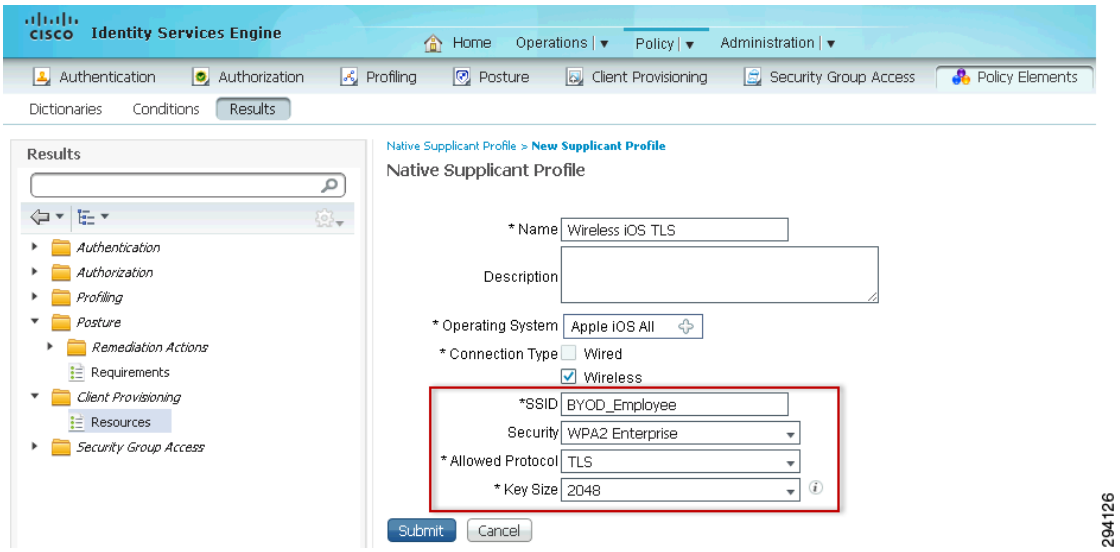
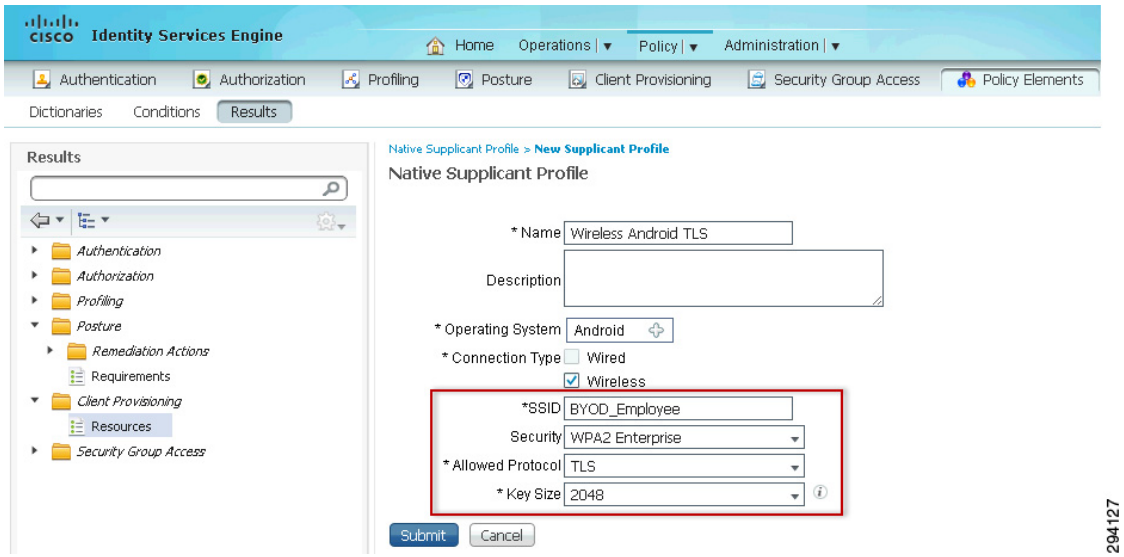


Figure 10-14 shows the configuration details for the Wireless Android TLS profile used by Android devices.

Figure 10-14 Wireless Android TLS

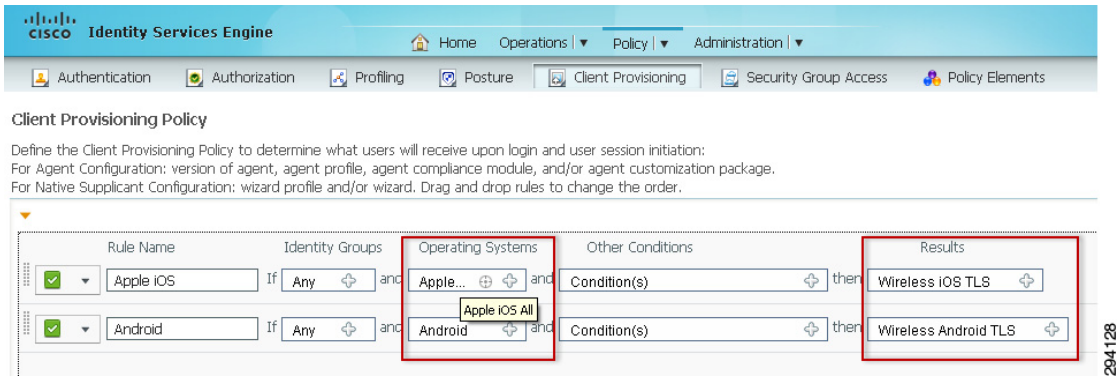


Client Provisioning Policy—Apple iOS and Android Devices

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



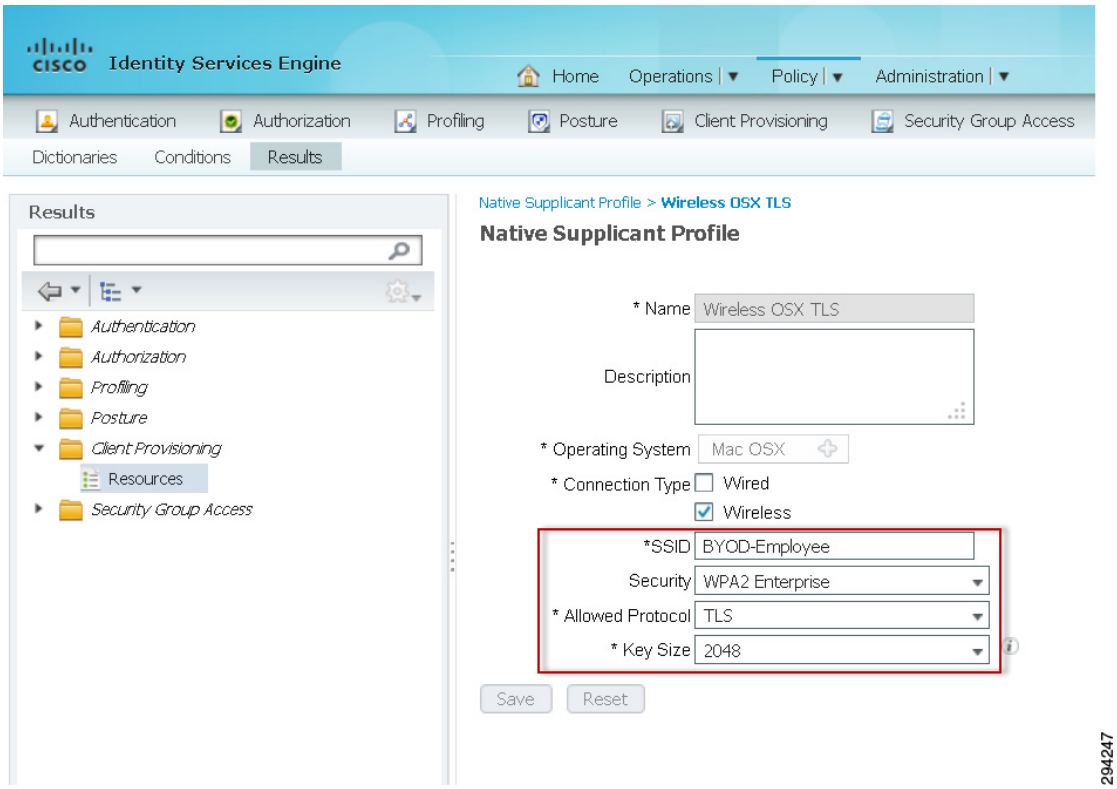
It is important to note that for Android devices the user is also required to download the software from Google's Play Store, since it cannot be distributed by ISE.

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.

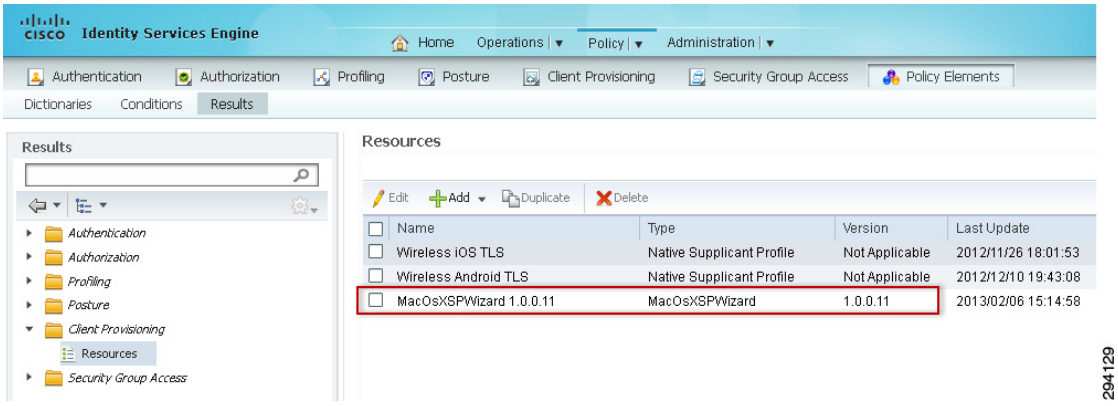
Figure 10-16 Native Supplicant Profile for Mac OSX Devices



- 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



Client Provisioning Policy for Mac OS Devices—Wireless

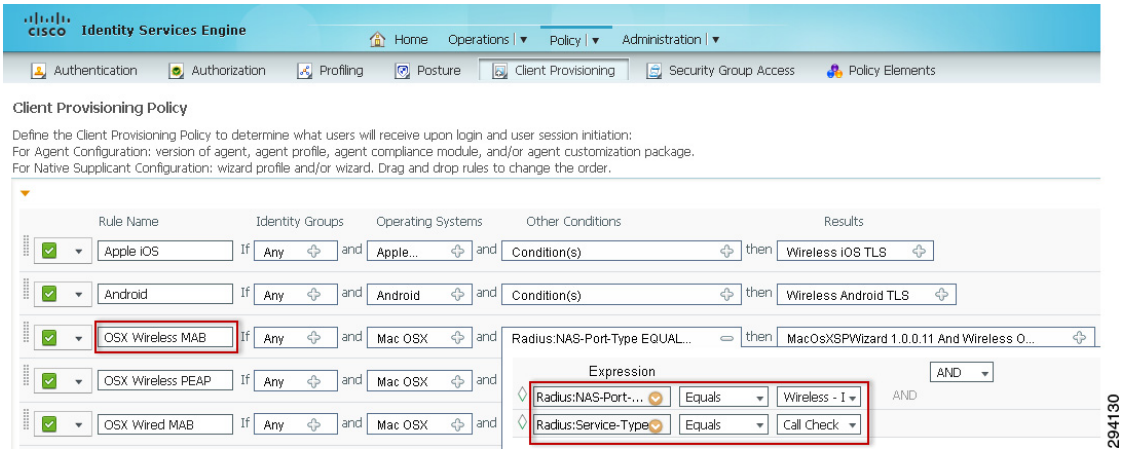
The previous section discussed the resources needed for provisioning Mac OS devices. Once the resources have been configured, the next step is to define under what conditions these resources will be used. The Mac OS X devices can use either MAB or PEAP protocol during the provisioning process. Therefore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

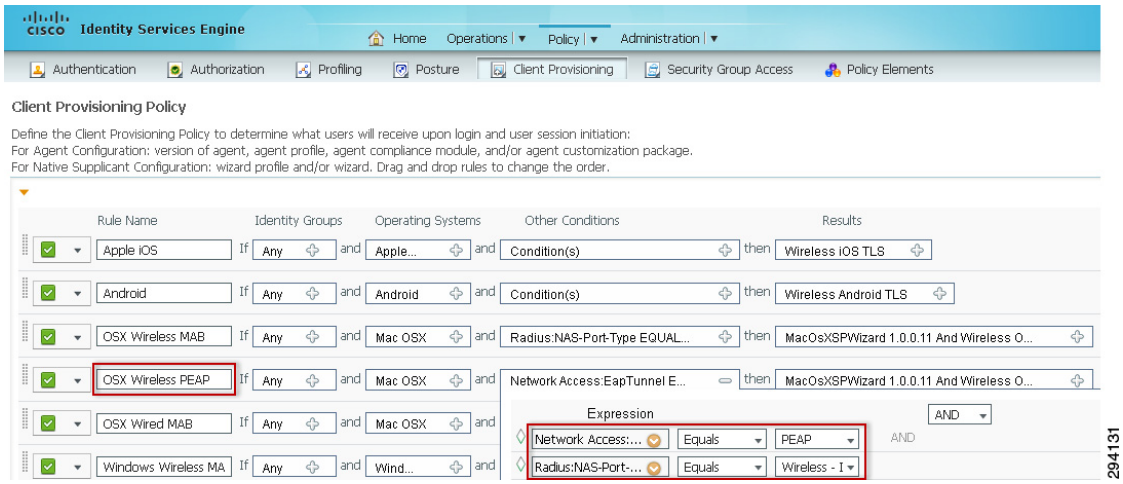


To match a Mac device using the PEAP protocol, the following conditions are needed:

- 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

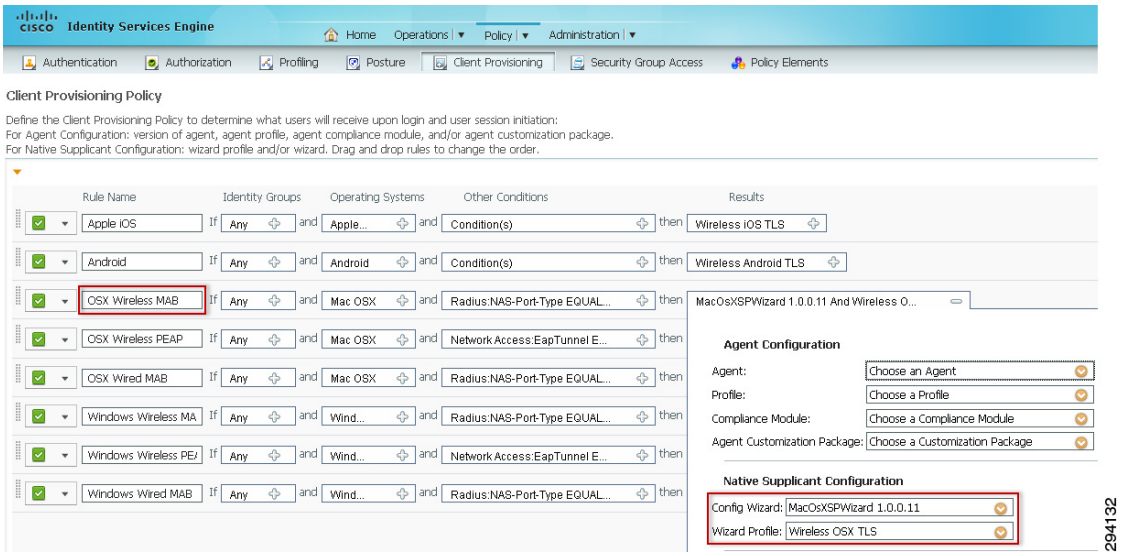


To complete a Client Provisioning policy for MAC_OSX_Wireless devices, the following must be defined:

- 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 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

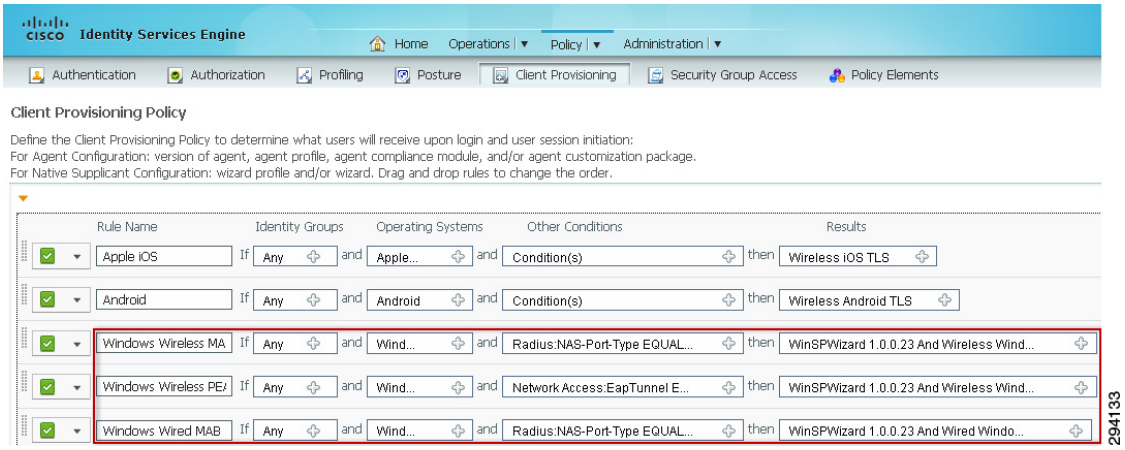
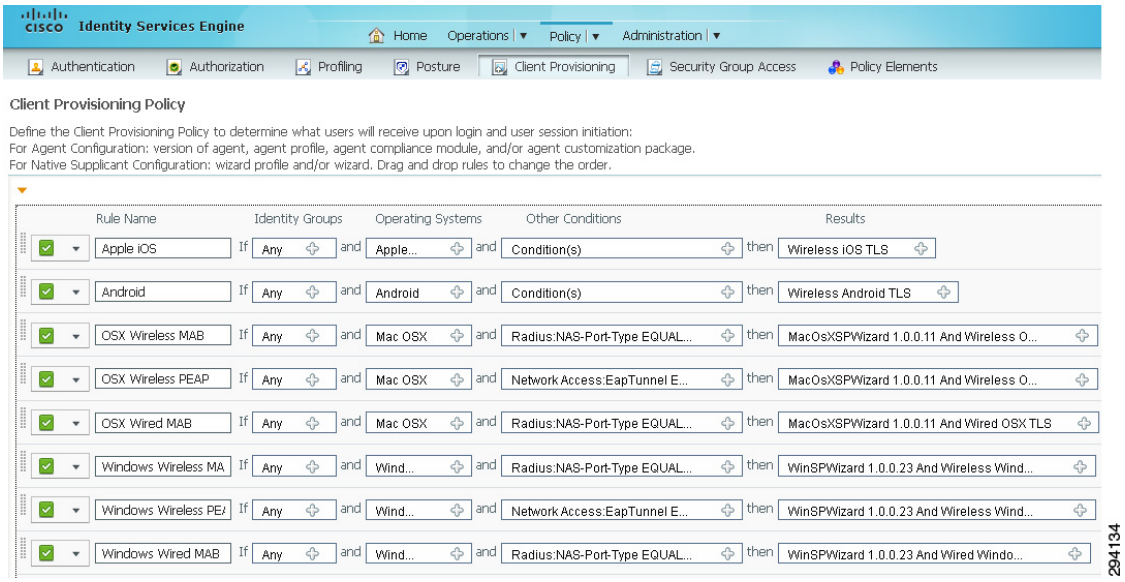


Figure 10-22 shows the complete client provisioning policy used during testing.

Figure 10-22 Complete Client Provisioning Policy



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.

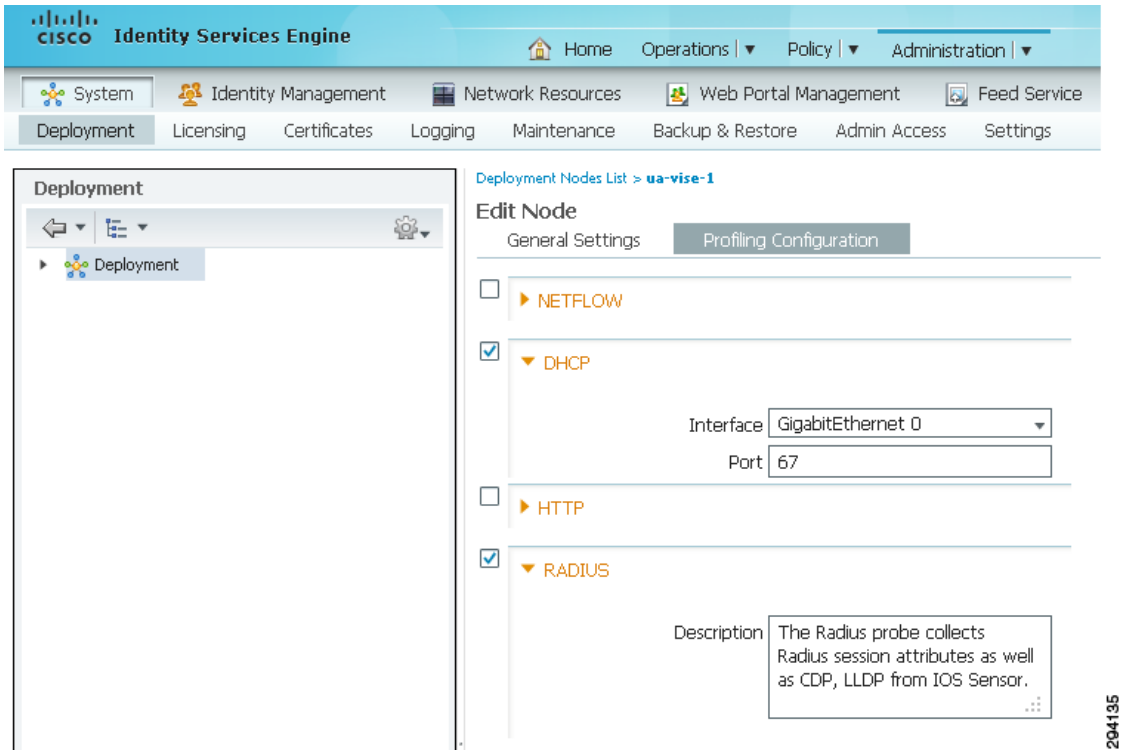
The ISE supports a number of sensors to capture endpoint attributes and classify them according to their profiles. The sensors rely on a number of probes that capture network packets by querying network access devices. Once the endpoints are profiled, different authentication and authorization policies 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

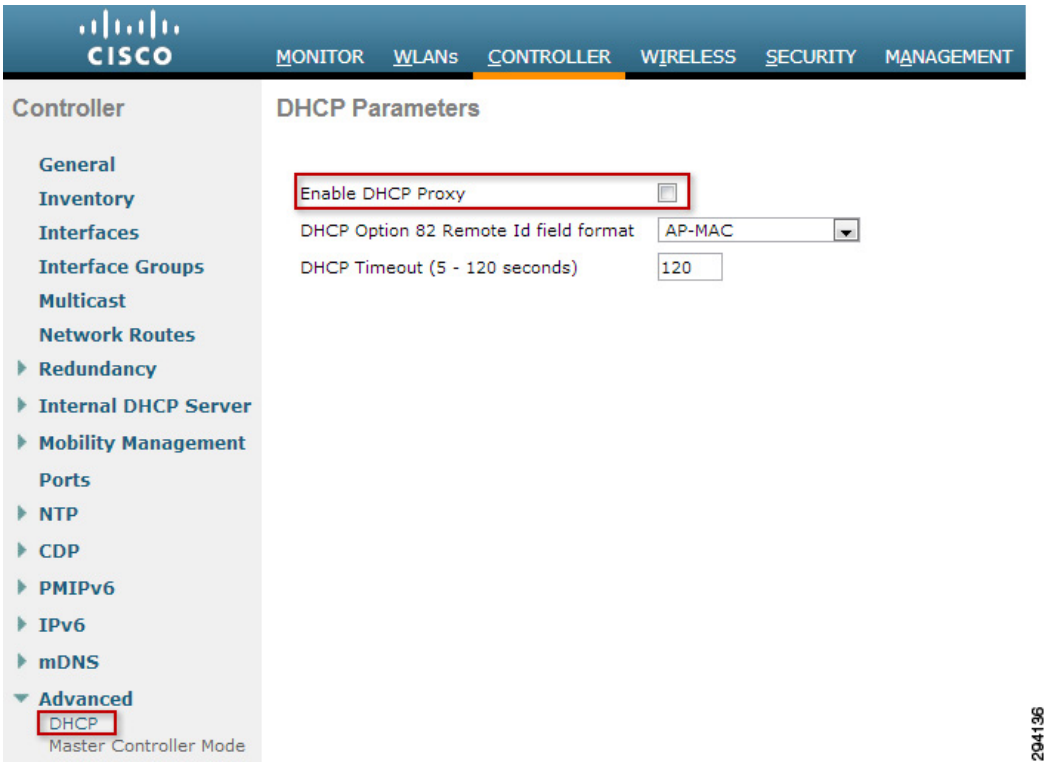
To enable profiling on the ISE, click **Administration > System > Deployment**. Click the ISE hostname and click **Profiling Configuration**. Enable the appropriated probes to listen to packets forwarded from the LAN switch or Wireless LAN Controller, as shown in Figure 10-23.

Figure 10-23 Profiling Probes



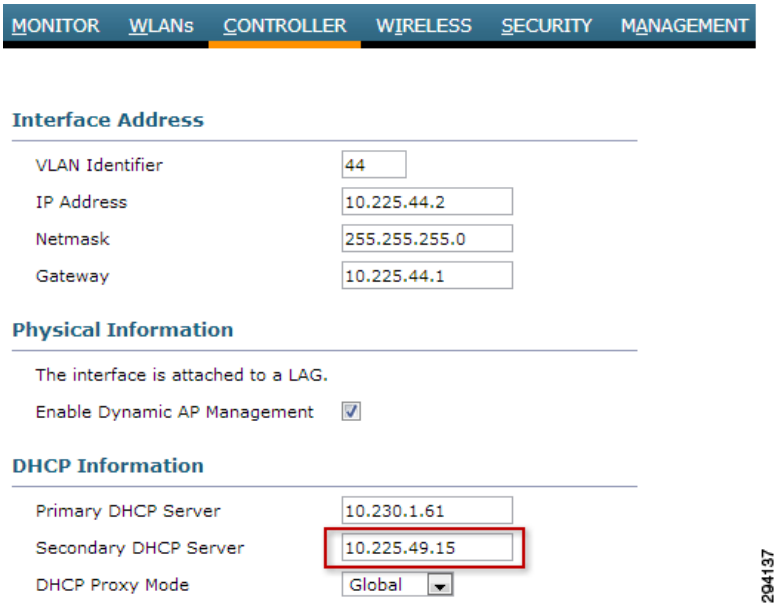
The Wireless LAN Controller should be configured in DHCP bridging mode to forward DHCP packets from the wireless endpoints to the ISE. Click **Controller > Advanced > DHCP** and clear the Enable DHCP Proxy check box, as shown in Figure 10-24.

Figure 10-24 Disable DHCP Proxy



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.

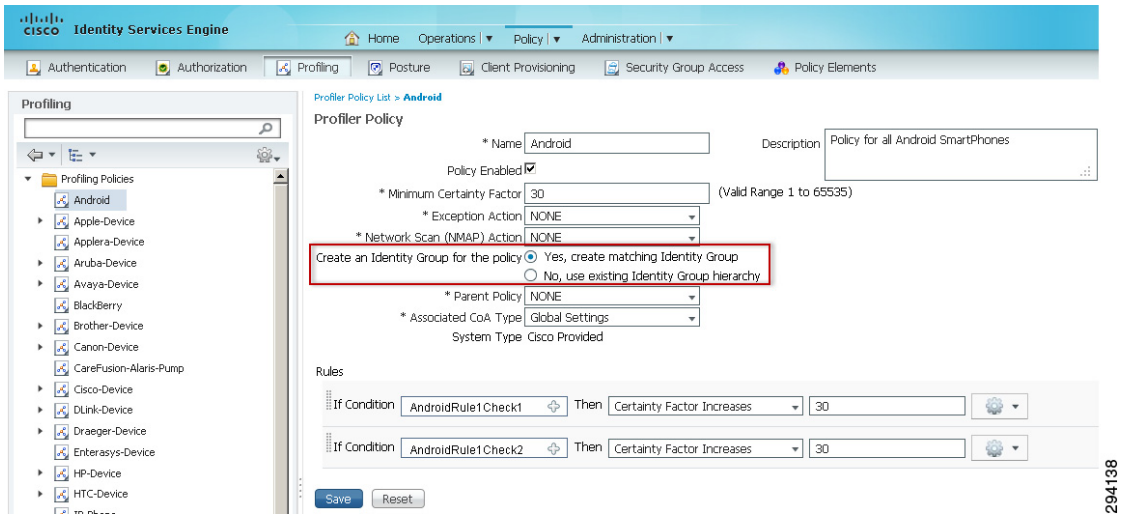
Figure 10-25 Secondary DHCP Server



Profiling Android Devices

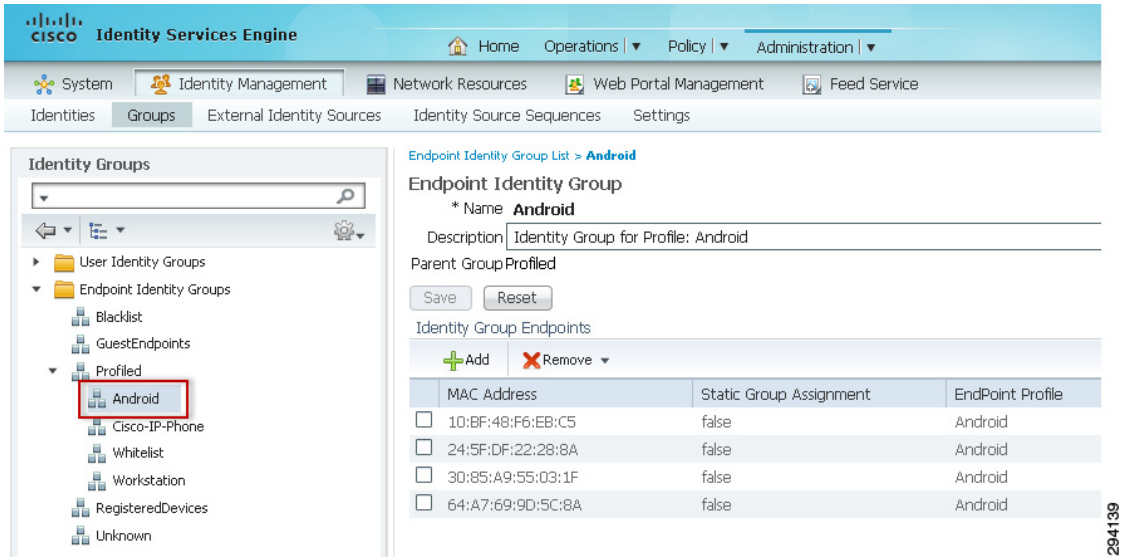
To create an identity group based on the Android policy, click **Policy > Profiling > Profiling Policies > Android** and enable the Create Matching Identity Group, as shown in Figure 10-26.

Figure 10-26 Android Profiling Policy



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



Logical Profiles

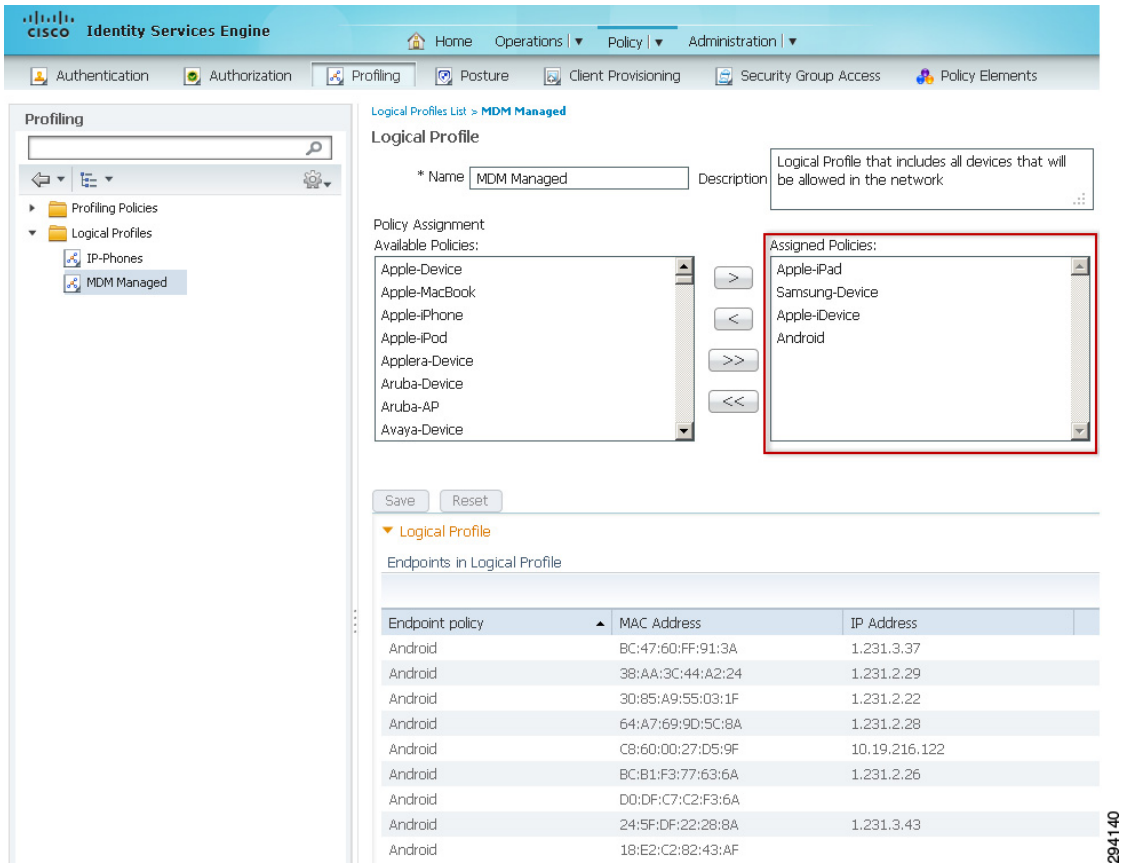
Logical profiles are containers that group different profiles to create an overall category of profiles. Logical profiles provide additional flexibility to the authorization policies, enhancing the overall network access policy.

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.

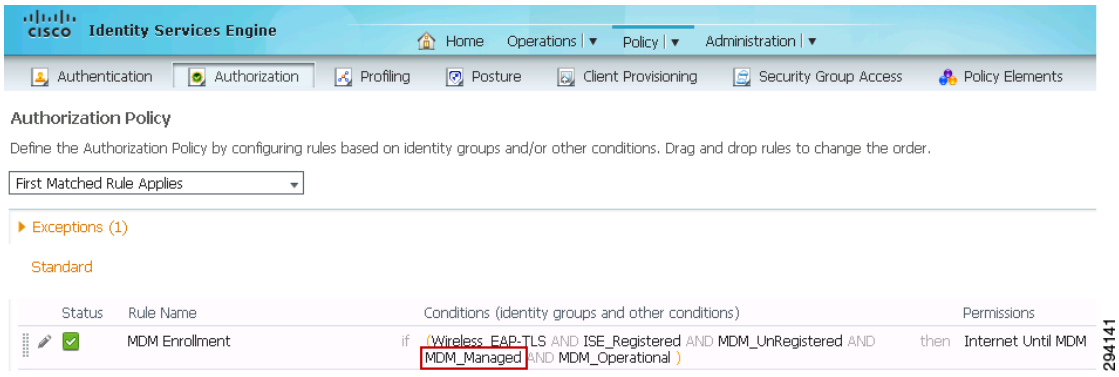
Figure 10-28 MDM Managed Logical Profile



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 Policies and Profiles

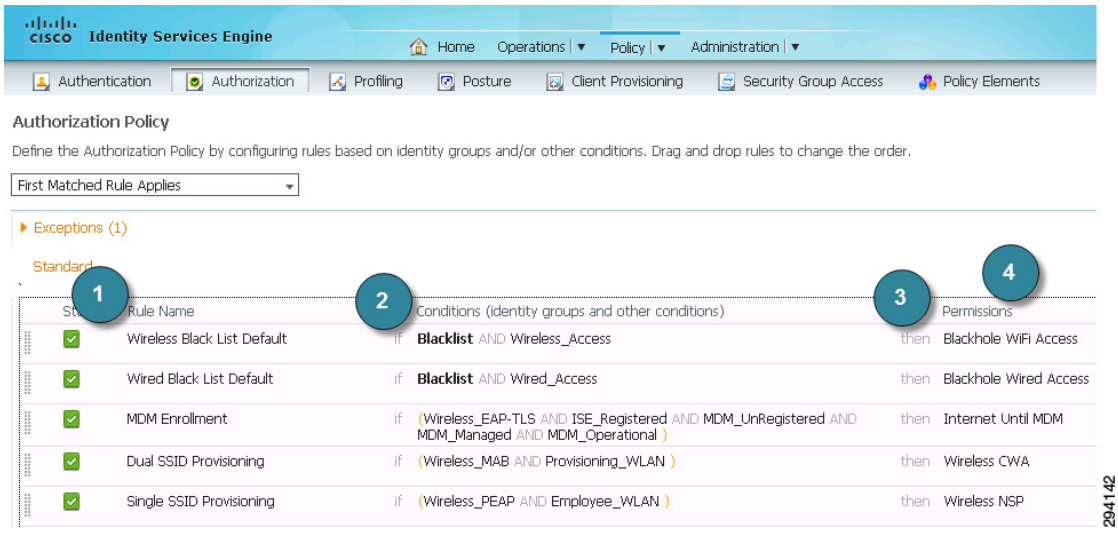
Authorization policies define the overall security policy to access the network. Network authorization controls user access to the network and its resources and what each device can do on the system with those resources. An Authorization Policy is composed of multiple rules.

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 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.

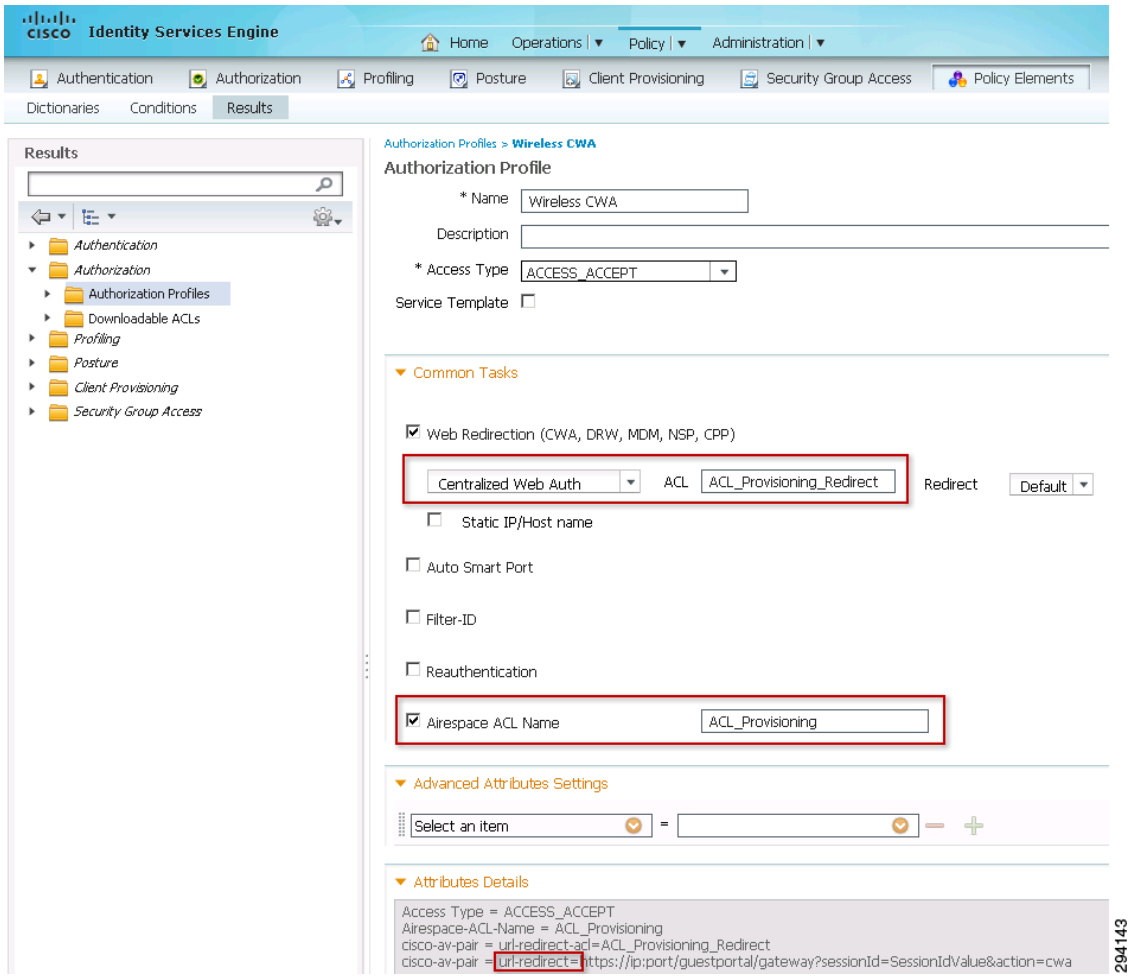
Wireless CWA Authorization Profile for Dual SSID Provisioning

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



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).

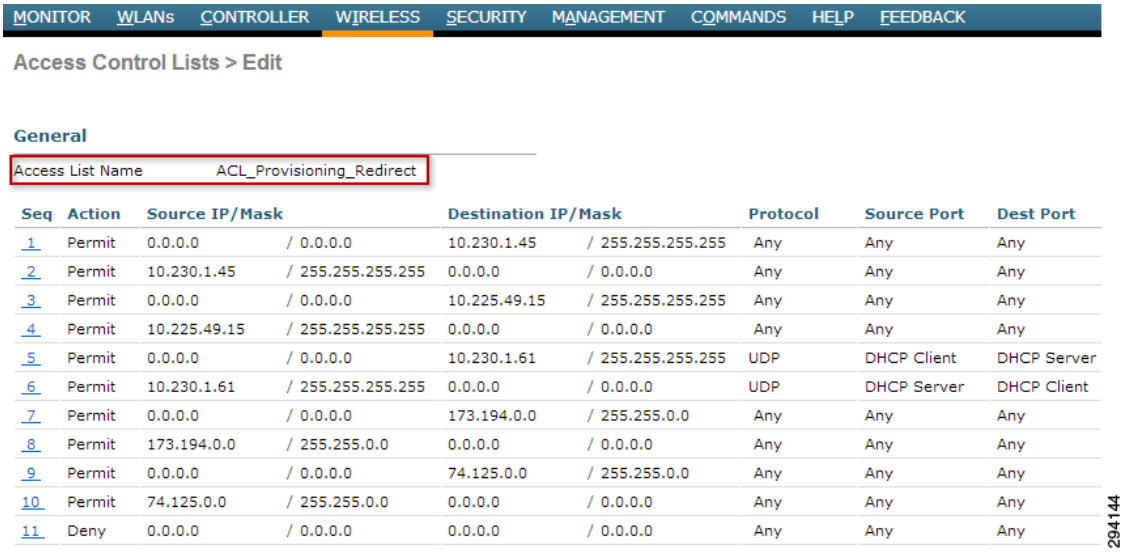
The behavior of the two ACLs is slightly different between wireless controllers:

- 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



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:

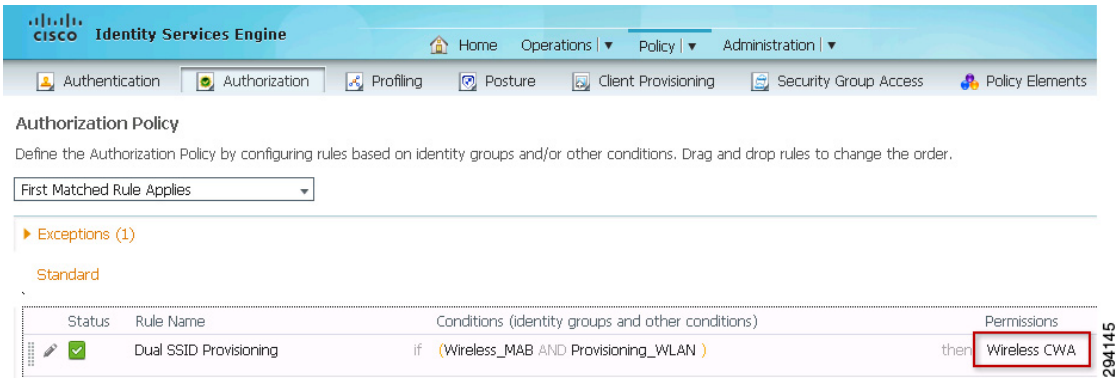
- Deny (do not redirect) IP access to and from the DNS server (10.230.1.45).

- 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

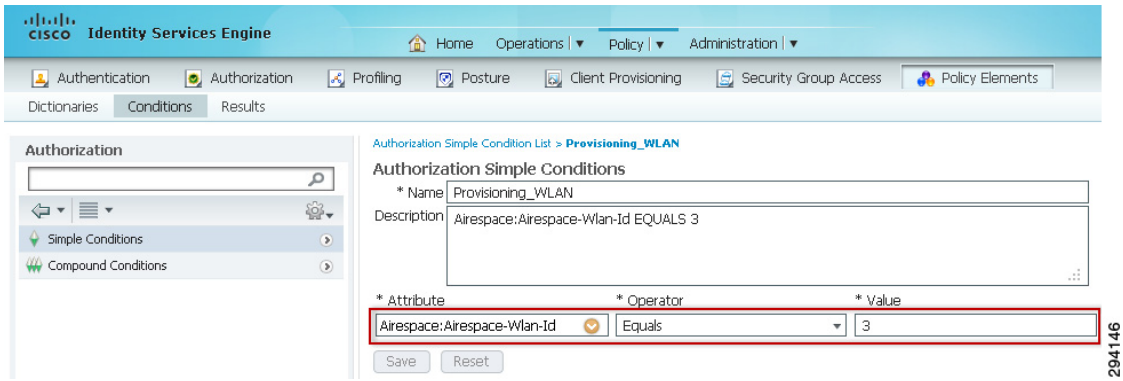
The Dual SSID Provisioning rule links the Wireless CWA authorization profile to the conditions that authorize MAB devices into the Provisioning SSID, as shown in Figure 10-33. It includes two conditions: Wireless_MAB and Provisioning_WLAN.

Figure 10-33 Dual SSID Authorization Rule



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



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.

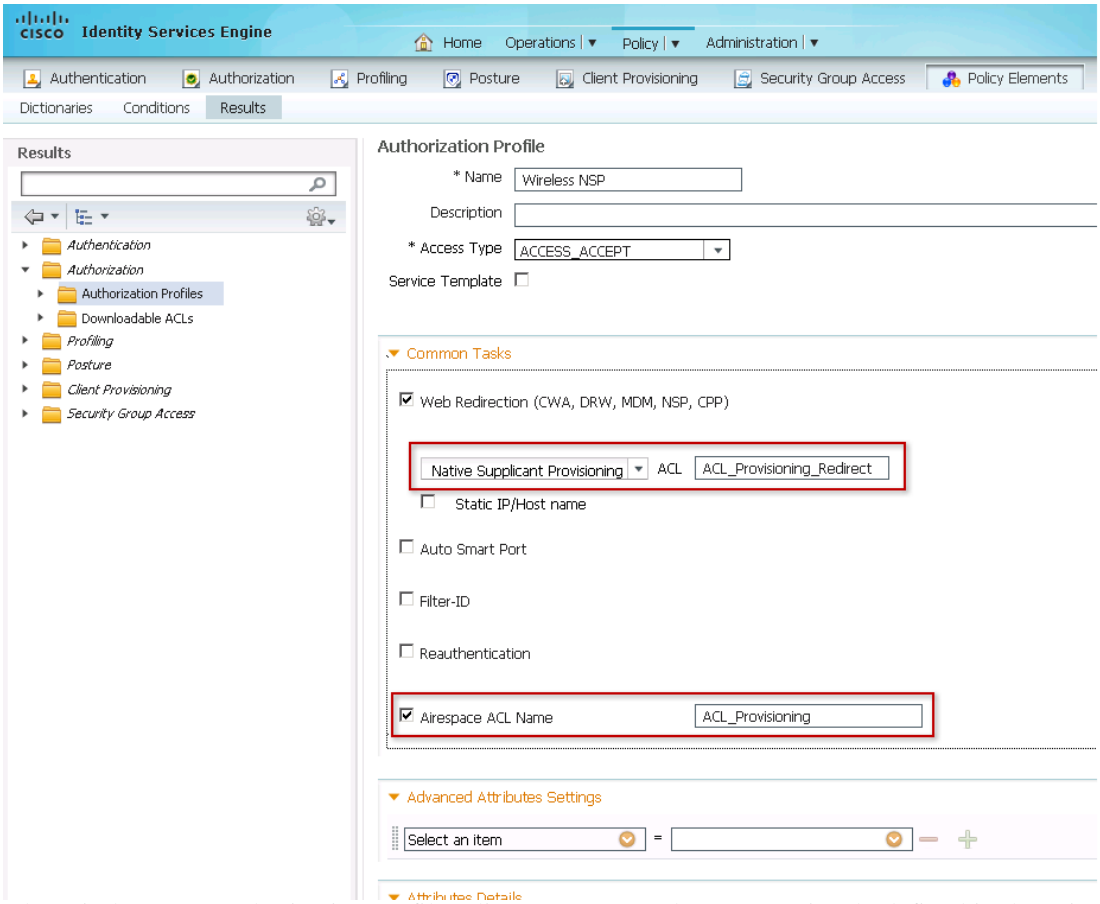
Wireless NSP Authorization Profile for Single SSID Provisioning

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



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

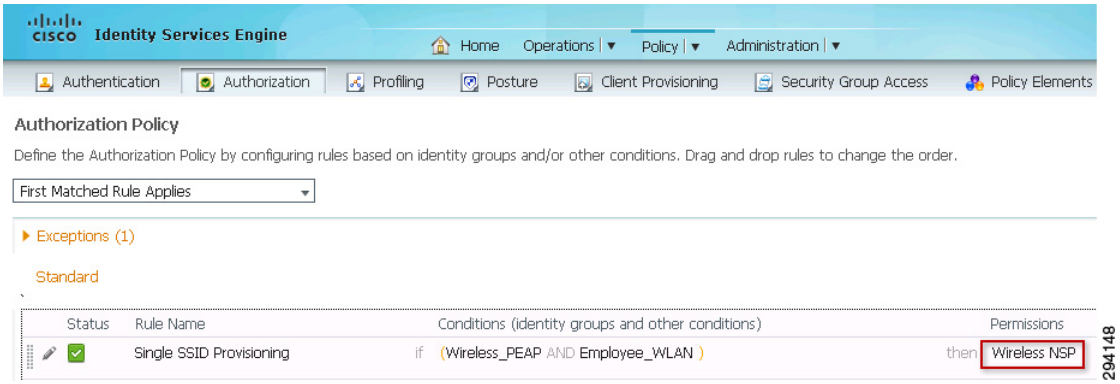
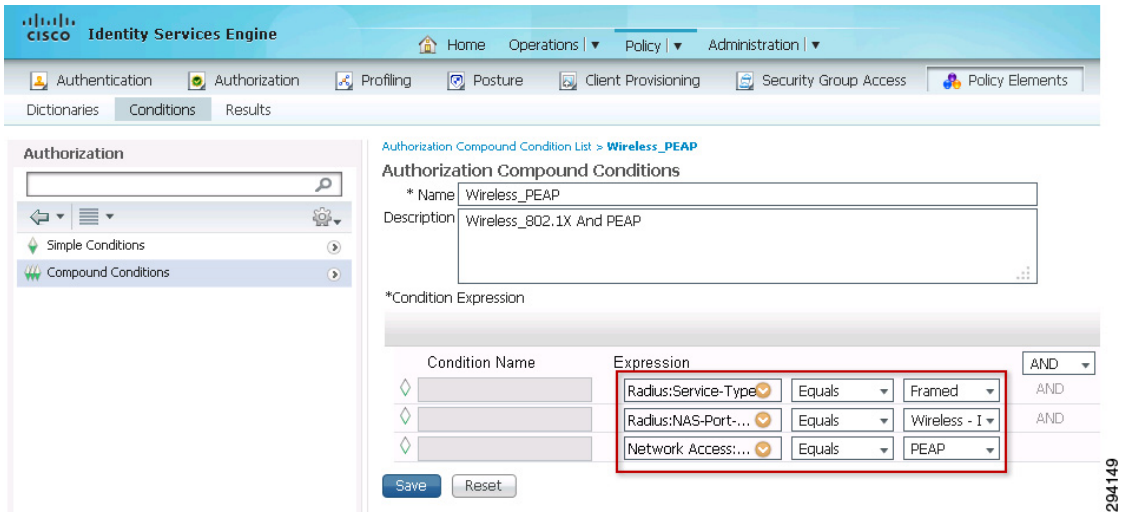


Figure 10-37 shows the Wireless_PEAP compound condition in ISE, which includes these expressions:

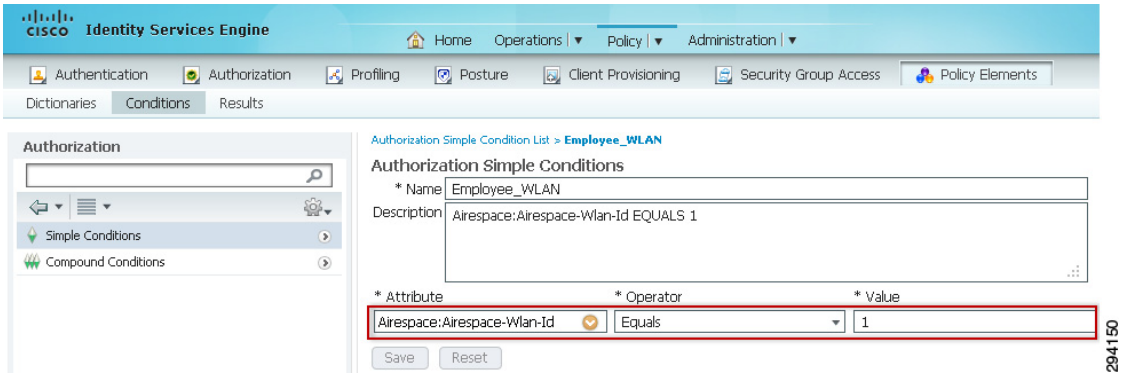
- Radius:Service-Type Equals Framed
- Radius:NAS-Port-Type Equals Wireless—IEEE 802.11
- Network Access: EapTunnel Equals PEAP

Figure 10-37 Wireless_PEAP Compound Condition



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



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

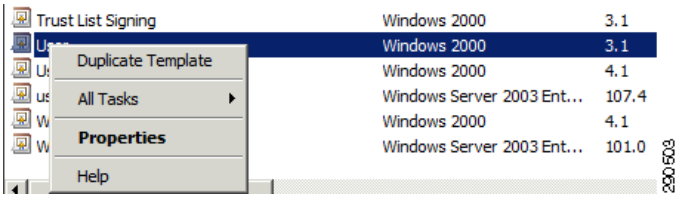
Digital certificates can be used for different purposes like server authentication, secure email, encrypting the file system, and client authentication. Hence it is important that a client is issued a certificate which serves its purpose. For example, a web server may need a certificate for server authentication. 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

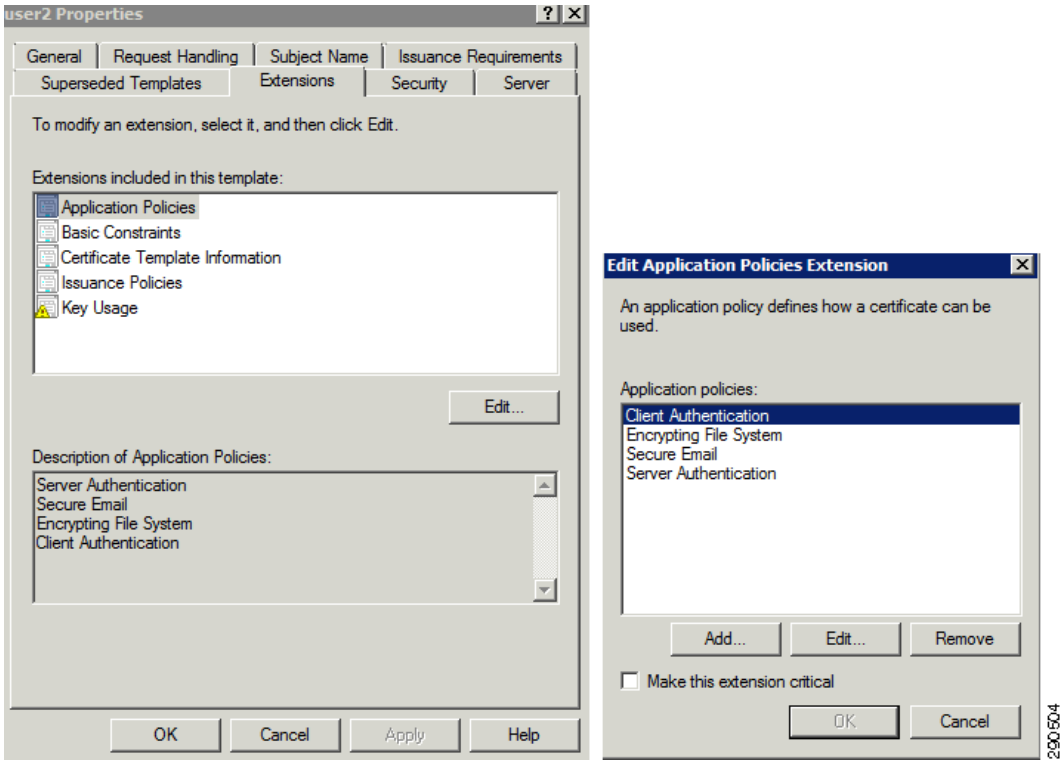


The default "User" template was copied and renamed "user2". Then the "user2" template was used to auto-enroll AnyConnect VPN clients with client certificates using this newly created template.

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.

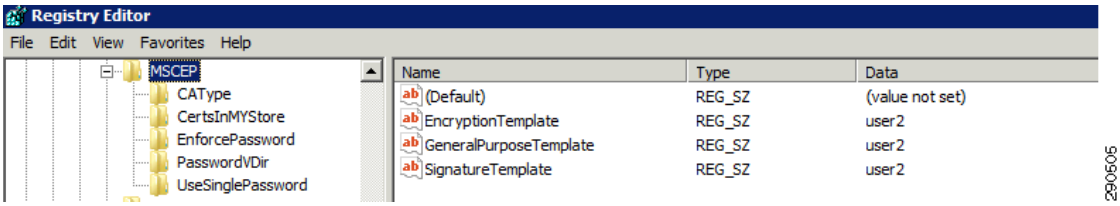
Figure 10-40 Configuring Extended Properties for Certificates



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.

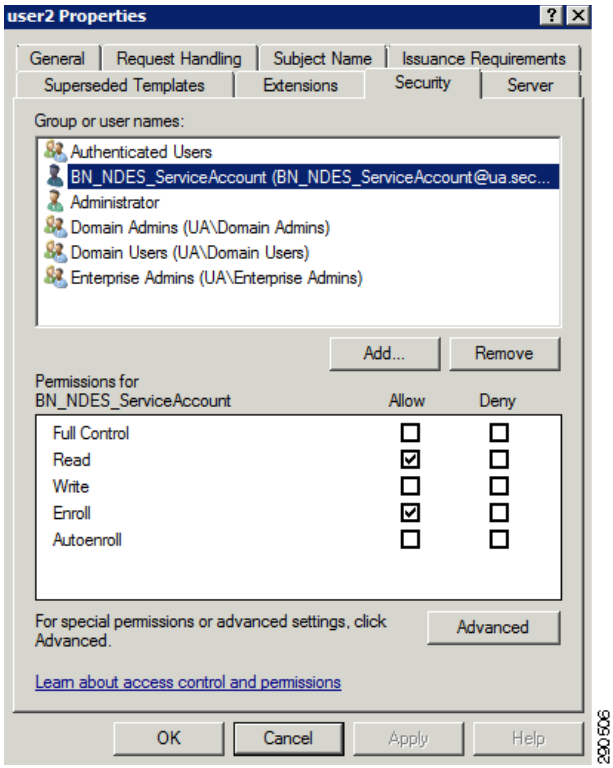
Figure 10-41 describes how the registry setting must be modified to reflect the newly-created template “user2”.

Figure 10-41 Modifying the Registry



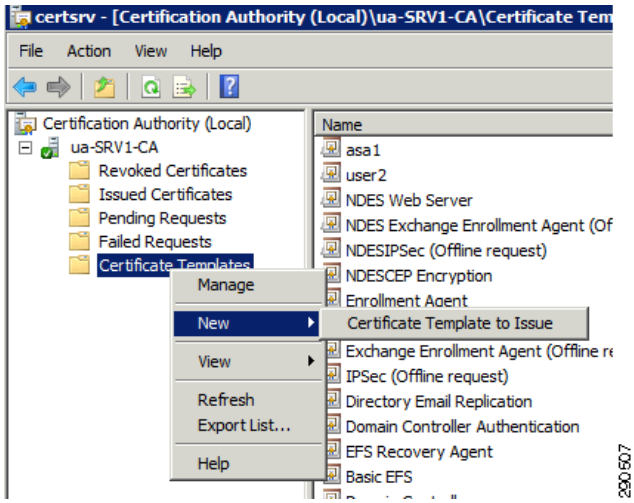
Once the template has been duplicated, the permissions are set for the NDES_ServiceAccount on the “user2” template to Read and Enroll. Figure 10-42 displays the Read and Enroll permissions that have been set for the NDES_ServiceAccount on the “user2” template.

Figure 10-42 Read and Enroll Permissions



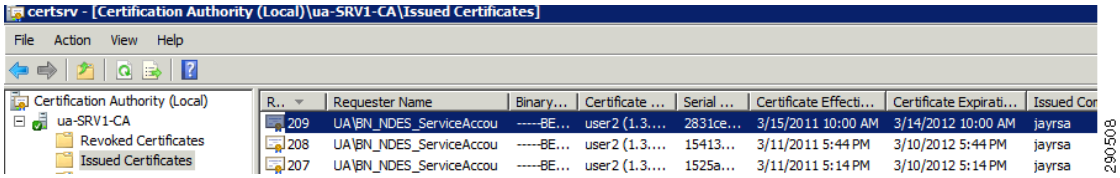
Ensure that the newly created "user2" template is available to be issued via the CA. Right click "user2" and choose the newly-created "User2 Certificate", as shown in Figure 10-43.

Figure 10-43 Ensuring Template is Available From CA



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



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.