



## **PART 4**

### **BYOD Use Cases**





## Summary of BYOD Use Cases

---

**Revised: August 7, 2013**

This part of the CVD focuses on implementing the rules previously defined in business policies. These rules translate into four different use cases that focus in providing differentiated access to corporate, personal-owned, and guest devices and highlight the network infrastructure as the enforcement point for BYOD policies.

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 configuration steps are discussed to support different BYOD use cases:

- Digital Certificates
- Microsoft Active Director authentication
- Wireless Controllers (Unified and Converged Access)
- Identity Services Engine
- Access Layer Switches
- API Integration with Mobile Device Managers

This part of the CVD includes the following chapters:

- **BYOD Enhanced Use Case—Personal and Corporate Devices**—This use case provides network access for personal devices and corporate-issued devices. It provides unique access (Full, Partial, and Internet Only) based on different conditions analyzed by the ISE. ISE relies on the network infrastructure to enforce unique permissions.
- **BYOD Limited Use Case—Corporate Devices**—This use case focuses on identifying corporate-issued devices and providing Full Access to Network Resources.
- **BYOD Advanced Use Case—Mobile Device Manager Integration**—The API integration with third party Mobile Device Managers allows the ISE to query for additional posture information on endpoints. This information translates into more granular authorization rules and allows for more visibility into the endpoint.
- **BYOD Basic Access Use Case**—An extension all the traditional wireless guest access, this use case presents an alternative where the business policy is not to on-board personal wireless devices but still provides access to network resources.

- [User Experience—How To On-board a BYOD Device](#)—Providing a positive user experience is important for any BYOD deployment. Employees should be provided with a simple way to on-board their devices and enable the necessary security features with minimum manual intervention. This chapter captures a typical user interaction with ISE during the on-boarding process.





# BYOD Enhanced Use Case—Personal and Corporate Devices

---

**Revised: March 6, 2014**

**What's New:** In the previous version of the BYOD CVD, the authorization policies for a user accessing the network with a personal device and enforced with the security group tags supported only a Centralized Unified Wireless Network (CUWN) architecture with CT-5508 as a controller.

In this version of the BYOD CVD, the authorization policies for a user accessing the network with a personal device and enforced with security group tags support:

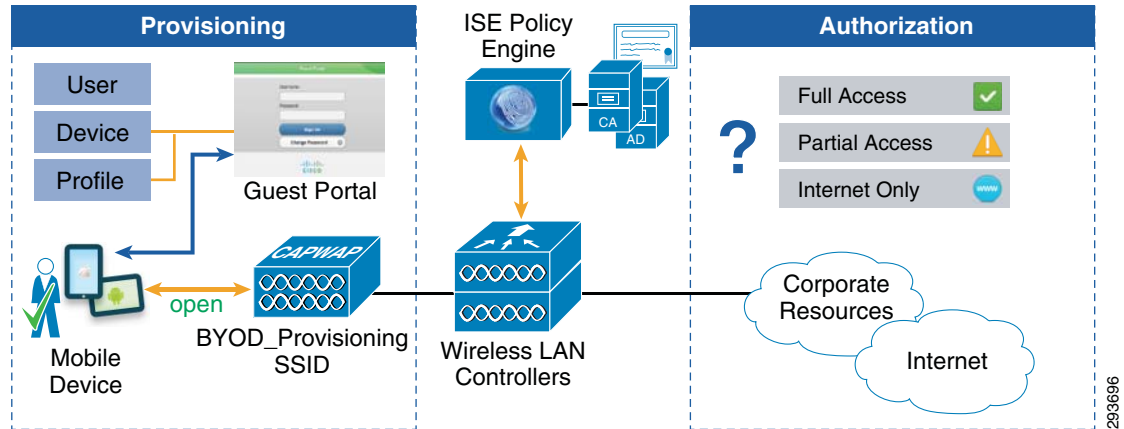
- CUWN architecture using CT-5508 and CT-5760 controllers
- Converged Access wireless design using Catalyst 3850

The BYOD Enhanced use case is a super-set of the BYOD Limited use case, covering both personal and corporate devices. This chapter defines the design scenarios for deploying BYOD for personal device access and the design considerations for each scenario. It also highlights how to deny access to personal devices based on their device type. [Chapter 16, “BYOD Limited Use Case—Corporate Devices”](#) provides the same design guidance for corporate devices. Hence the design guidance for corporate devices is not duplicated in this chapter.

One of the main objectives of a BYOD solution is to provide a simple way for employees to on-board their personal devices without requiring assistance from IT. Since the BYOD needs of the majority of employees will be met with either simple Internet access or Partial access, the only time an employee requires assistance from IT is when they may require full access to corporate resources.

Cisco ISE provides different ways to define security policies and determine what network resources each employee is allowed to access. The security policies are then enforced throughout the network infrastructure. The ISE feature set is extremely flexible, enabling different business policies to be enforced. This chapter explains the steps to on-board personal devices and how to apply different policies.

[Figure 15-1](#) shows how a personal device is profiled and registered by ISE and the different network components (WLC, AD, CA) that play a role in the process. Different conditions are evaluated to provide the proper authorization and access to network resources, including digital certificates, Active Directory groups, etc.

**Figure 15-1** Provisioning Personal Devices**Note**

Unless otherwise specified, in the figures throughout this chapter “Wireless LAN Controllers” refers to either standalone devices such as the Cisco Flex 7500, CT5508, and CT5760 wireless controller or to wireless LAN controller functionality integrated within Catalyst 3850 Series converged access switches.

Figure 15-2 shows how a personal device is restricted from accessing the network. Once the device connects and regardless of user authentication, ISE profiles the device and enforces the DenyAccess authorization rule.

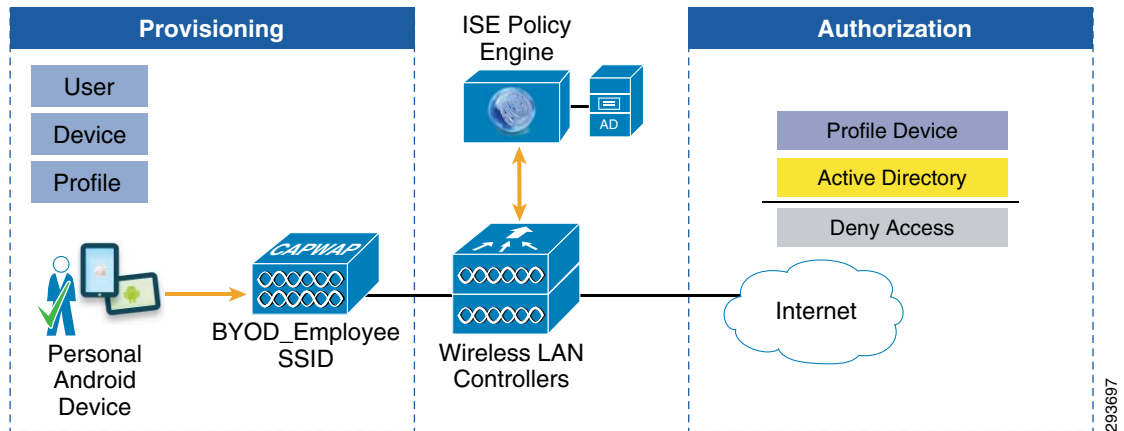




**Figure 15-2** Deny Access

Figure 15-3 shows the different permission levels configured in this chapter. These access levels are enforced using various mechanisms, including Access Control Lists (ACLs) in the Wireless LAN Controllers (WLCs) or Catalyst switches, Security Group Tag (SGT) assignment in the WLCs, and VLAN assignment in the Catalyst switches along with FlexConnect ACLs in access points.

**Figure 15-3** *Permission Levels for Personal Devices*

	Permission	Access
	Full Access	Internet plus all corporate resources
	Partial Access	Internet plus some corporate applications
	Internet Only	Internet Only
	Deny Access	Explicitly deny network access

292642

## Active Directory Groups





Active Directory groups can be used as an additional way to grant differentiated access to users. This chapter relies on the following three AD groups:

- **BYOD\_Full\_Access**—Members of this group are granted full access to network resources.
- **BYOD\_Partial\_Access**—Members of this group are granted partial access to network resources. With this permission, users are able to access the Internet and a subset of corporate applications, such as email, corporate directory, travel tools, etc.
- **Domain Users**—All users are members of this system-generated group by default. Employees that are not members of the above mentioned groups are granted Internet access.

This model could easily be expanded to include other user groups with similar access requirements. A good example would be to create a new group and access list to grant access to contractors or partners.

Figure 15-4 highlights the different access policies validated for this chapter, along with the different requirements and permissions granted by each policy. These policies, along with detailed configurations, are explained later in this chapter.

**Figure 15-4** *Access Policies and Permissions*

Policy	Location	AD Group	Profile	Permission
Full Access	Campus/Branch/SGT	BYOD_Full_Access		Full 
Partial Access	Campus/Branch/SGT	BYOD_Partial_Access		Partial 
Internet Only	Campus/Branch/SGT	Domain Users		Internet Only 
Deny Android Devices			Android	Deny 

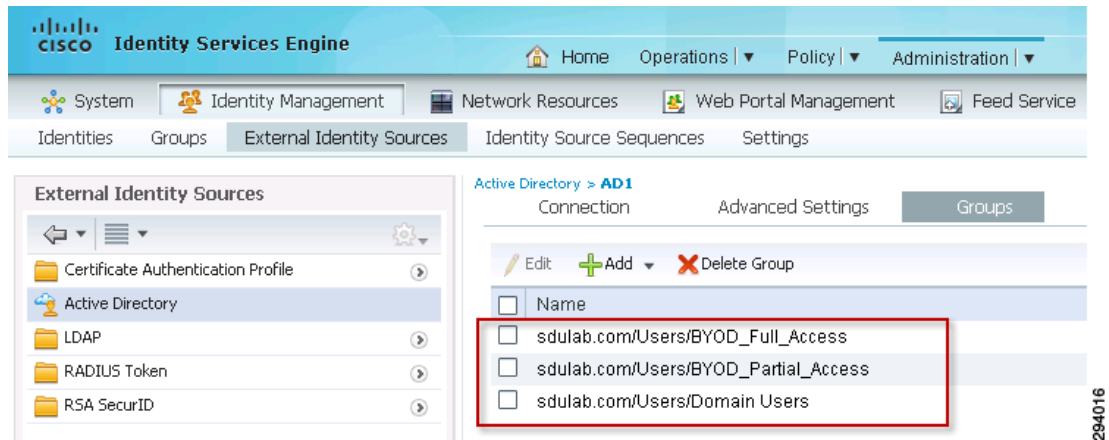
293698



### Note

The location SGT refers to a Wireless LAN Controller which is dedicated for the purpose doing SGT only.

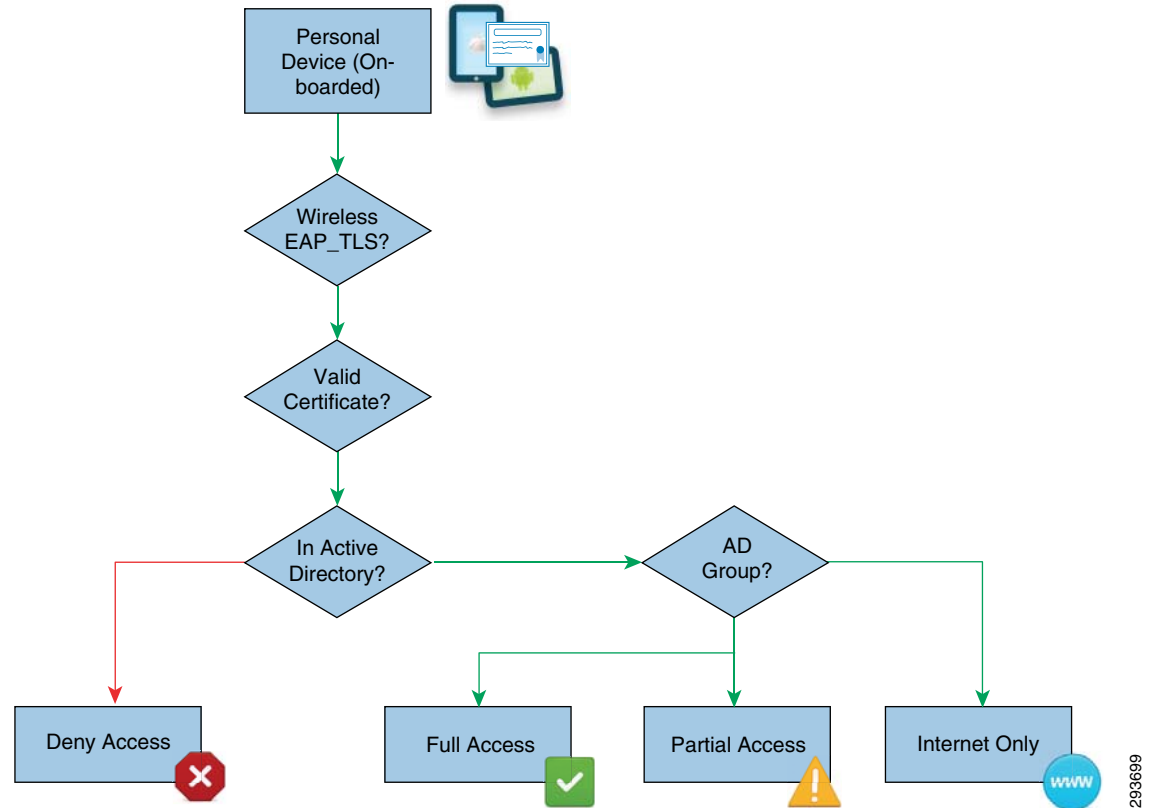
To configure the Active Directory groups that can be available for use in the authorization policy conditions, click **Administration > Identity Management > External Identity Sources > Active Directory > Groups** and check the boxes next to the groups that will be used in the policy conditions and rules. Figure 15-5 includes the groups used in this design guide.

**Figure 15-5** Active Directory Groups

This chapter assumes that after employees have on-boarded their devices, they will connect to the BYOD\_Employee SSID. Figure 15-6 highlights the connectivity flow for personal devices.

If the endpoint connected from a wireless 802.1X EAP-TLS SSID and has a valid certificate, based on their AD group membership, employees will get:

- Full Access if they belong to the BYOD\_Full\_Access group.
- Partial Access if they belong to the BYOD\_Partial\_Access group.
- Internet Access if they are a valid Active Directory member (Domain Users group)

**Figure 15-6** *Personal Device BYOD Access*

## Distributing Digital Certificates

Digital signatures, enabled by public key cryptography, provide a means to authenticate devices and users. In public key cryptography, such as the RSA encryption system, each user has a key pair containing both a public and a private key. The keys act as complements and anything encrypted with one of the keys can be decrypted with the other.

A digital signature is encrypted with the sender's private key. The signature must be verified to confirm the sender's identity. This is done by the receiver, who decrypts the signature with the sender's public key. If the signature sent with the data matches the result of applying the public key to the data, the validity of the message is established.

This process relies on the receiver having a copy of the public key of the sender and a high degree of certainty that this key belongs to the sender, not to someone pretending to be the sender.

Deploying digital certificates on mobile devices requires a unique process, as many of these devices do not natively support all the features and functionality to create, download, and install digital client certificates in the same manner as traditional PC-based devices. At the same time, some endpoints do not support Simple Certificate Enrollment Protocol (SCEP) natively.

For example, for users to install digital client certificates using SCEP on Apple iOS devices, the IT administrator needs to manually create the configuration profile using the iPhone Configuration Utility and distribute the profile to user devices via email, USB, or web pages.

Traditional full-featured PC-based devices are more apt to take advantage of the many services, such as Microsoft's NDES, to provide certificate enrollment. However, with the onset of many Android and Apple iOS devices on the market, it cannot be assumed that these devices can natively interoperate with many of the enterprise services currently deployed.

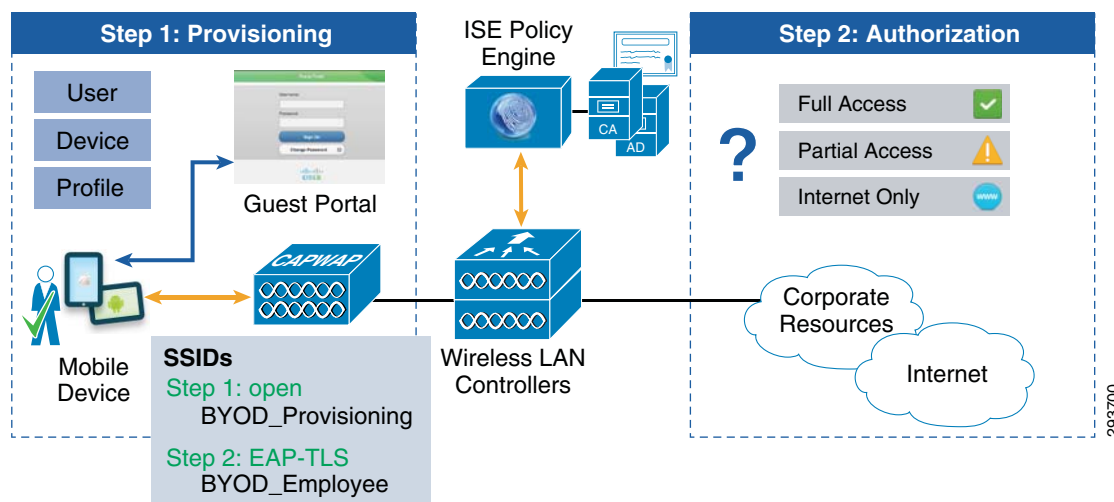
ISE solves this problem by distributing digital certificates to endpoints using the SCEP Proxy feature, which allows endpoints to obtain digital certificates through ISE. Moreover, this feature is combined during the initial registration process, thereby preventing different registration steps. The next section on mobile devices discusses how the endpoints obtain their digital certificates during the registration process.

## Mobile Device On-boarding

Deploying digital certificates to endpoint devices requires a network infrastructure that provides the security and flexibility to enforce different security policies. Figure 15-7 highlights the general steps that are followed when a mobile device connects to the network using dual SSIDs.

1. A new device connects to a provisioning SSID. This SSID (open or secured with PEAP) is configured to redirect the user to the Guest Registration portal.
2. The certificate enrollment and profile provisioning begins once the user is properly authenticated.
3. The provisioning service requests information from the mobile device user and provisions the configuration profile, which includes a WiFi profile with the required parameters to connect to the secured Employee SSID.
4. For subsequent connections, the device uses the Employee SSID and is granted access to network resources based on different ISE authorization rules.

**Figure 15-7 Enrollment and Provisioning—Dual SSID**



The on-boarding steps may also be configured with a single SSID used for provisioning and secure access. The general steps followed when the mobile device connects are similar, redirecting the user to the Guest registration portal and provisioning the device with a digital certificate and configuration profiles.

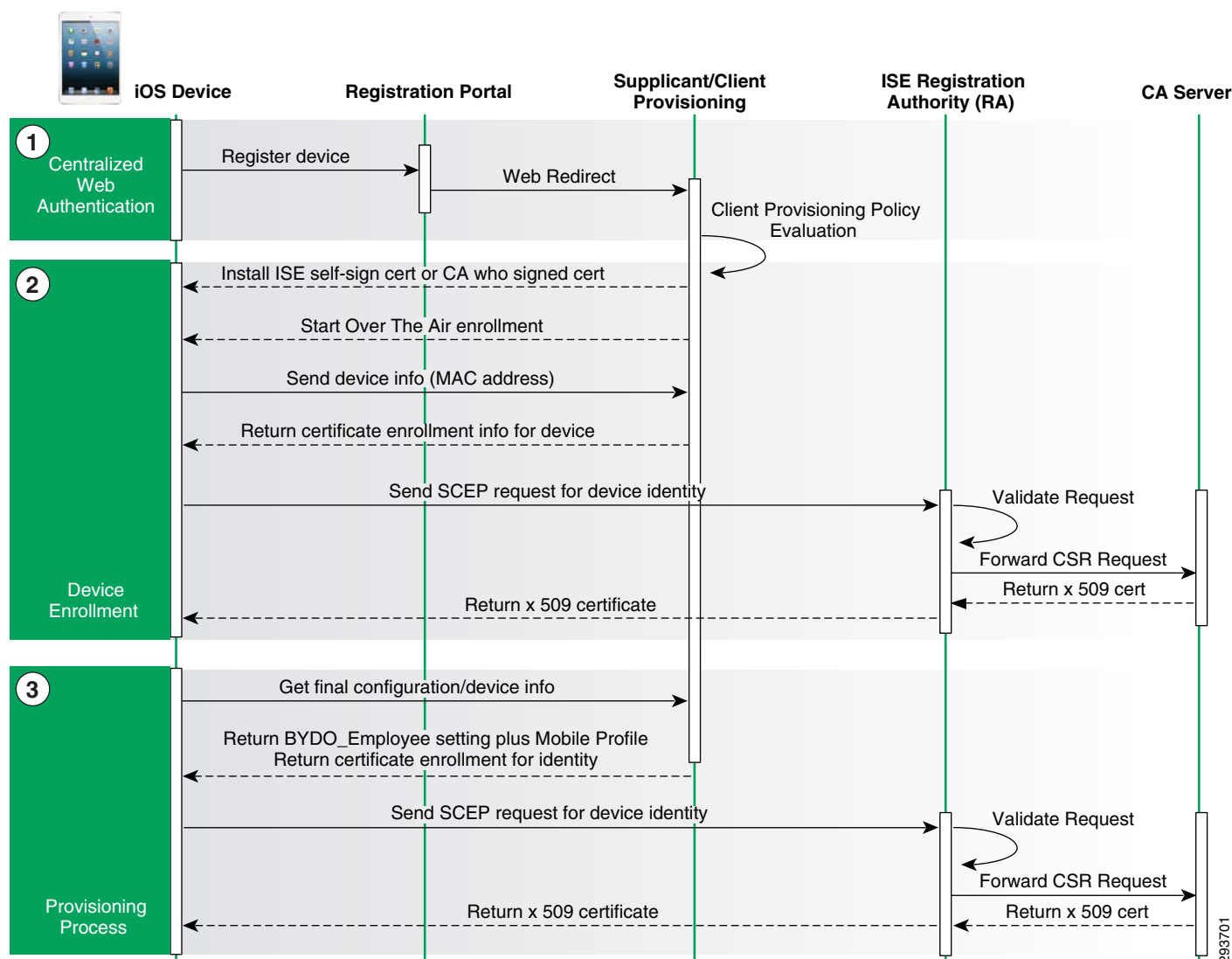
# Provisioning Flows

This section explains the interaction between the endpoints and the Guest Registration portal and the steps required to enroll the digital certificate and configuration profile. The way Windows and Mac devices are provisioned is similar. [Chapter 8, “Summary of Configuring the Infrastructure”](#) points to the chapters with the steps required to configure the different network components.

## Provisioning Apple iOS Devices

The following steps take place while provisioning Apple iOS devices:

- The device is redirected to the Guest Registration Portal.
- After successful authentication, the Over-The-Air (OTA) enrollment begins.
- Device sends unique identifier (MAC address) and other information.
- Certificate enrollment information is sent to the device.
- A SCEP request is made to ISE, which returns a certificate.
- Wireless profile for BYOD\_Employee is sent to the device.
- Once the enrollment is complete, the user manually connects to BYOD\_Employee SSID.

**Figure 15-8** Provisioning Flow for Apple iOS Devices

For more details on Over-the-Air Enrollment and configuration for iOS devices, review the iPhone OS Enterprise Deployment Guide:

[http://manuals.info.apple.com/en\\_US/Enterprise\\_Deployment\\_Guide.pdf](http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf).

## Provisioning Android Devices

The following steps take place while provisioning Android devices:

- The device is redirected to the Guest Registration portal.
- After successful authentication, the self-registration portal page redirects the user to the Google Play.
- The user installs the Supplicant Provisioning Wizard (SPW).
- The SPW is launched to perform provisioning of the supplicant. The SPW performs the following functions:



- Discovers the ISE and downloads the profile from the ISE.
  - Creates a certificate/key pair for EAP TLS.
  - Makes a SCEP proxy request to ISE and gets the certificate.
  - Applies the wireless profile to allow connectivity to BYOD\_Employee SSID.
- The SPW triggers re-authentication and connects to BYOD\_Employee SSID automatically.

**Note**

---

The Android agent must be downloaded from Google Play and is not provisioned by the ISE. Endpoints must be able to reach Google Play on the Internet.

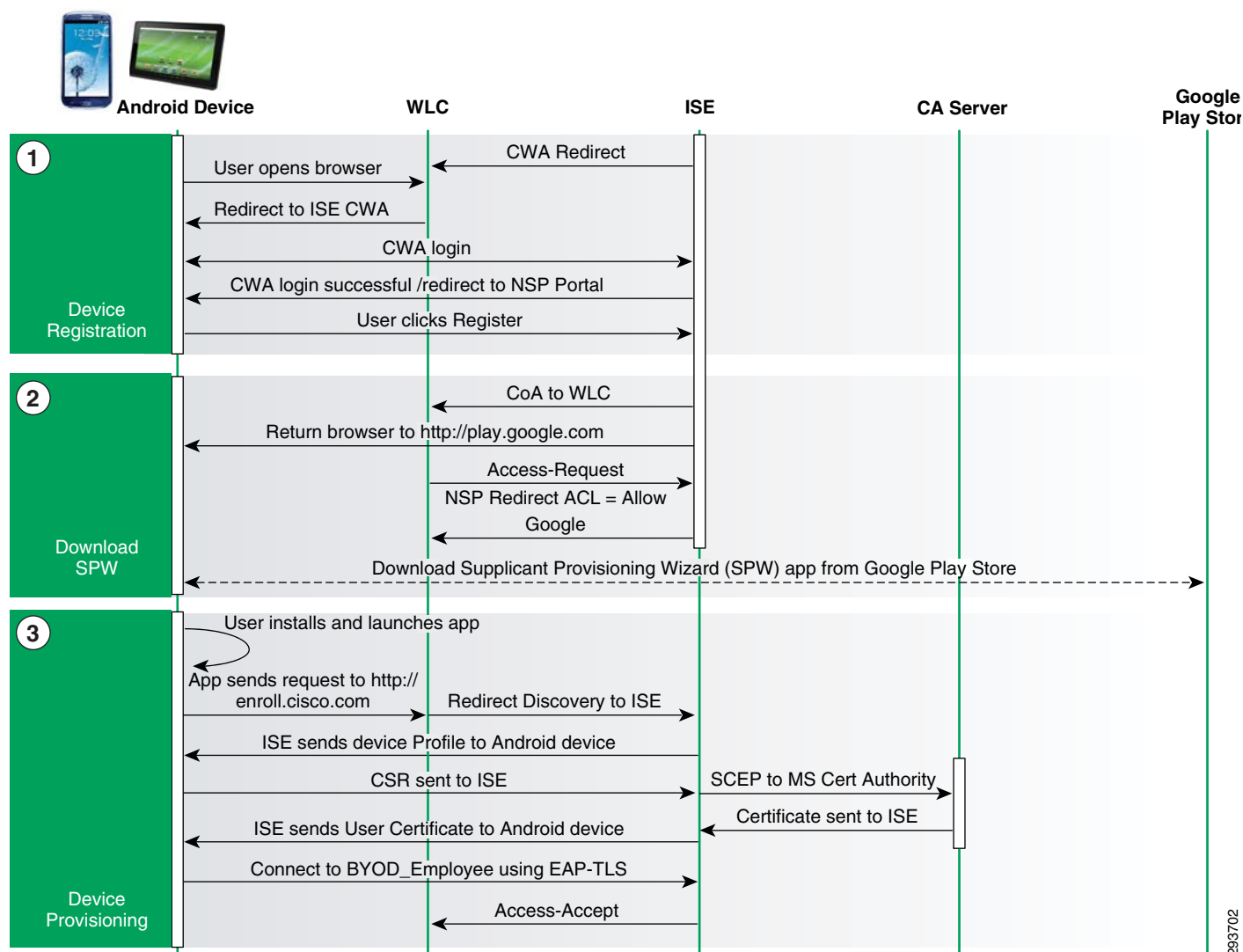
---

**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 ISE server. This is shown as part of step 3 in [Figure 15-9](#). This is not a concern if the guidance presented in the CVD is followed since all Internet traffic except Google Play is redirected back to ISE.

---

**Figure 15-9** Provisioning Flow for Android Devices

293702

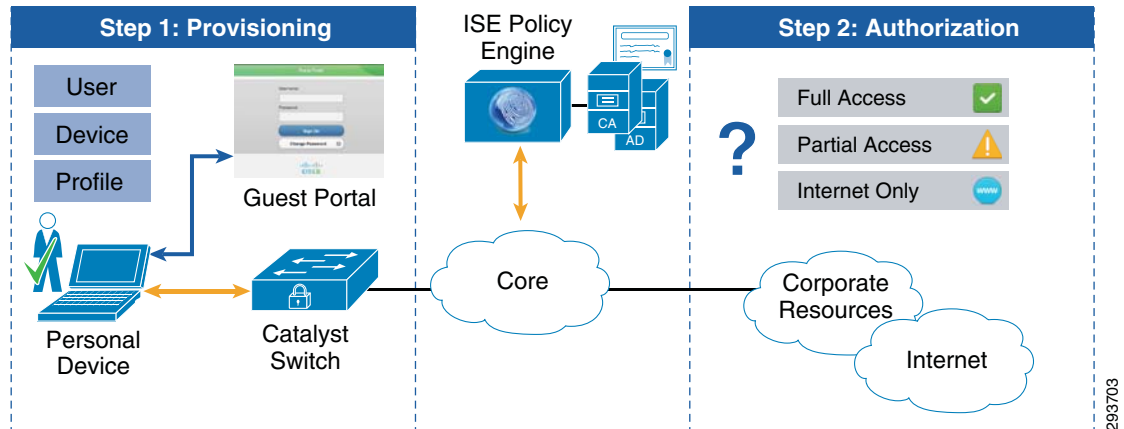
## Provisioning Wired Devices

BYOD applies to both wired and wireless devices. Wired devices can be provisioned, registered, authenticated, and authorized in much the same way as wireless devices. The following are some of the advantages of provisioning wired devices:

- Certificate provisioning can be done during the provisioning process, which alleviates the burden on IT to support another model to provision certificates on the devices.
- The native supplicants on the device can be configured with the right protocols during the provisioning process. If this is left to the user, it may often lead to incorrect configurations and additional management overhead for IT.
- Provides easier methods for IT to obtain visibility into who is accessing the network and also methods to remove network access for devices that are lost or stolen.

Figure 15-10 shows a high-level overview of the components used to deploy wired devices. ISE uses several building blocks, such as AD group membership, the EndPoints:BYODRegistration attribute, and Digital Certificates to authenticate and authorize devices. Examples on how to construct these policies are explained in this design guide.

**Figure 15-10**     **Wired Device Deployment**



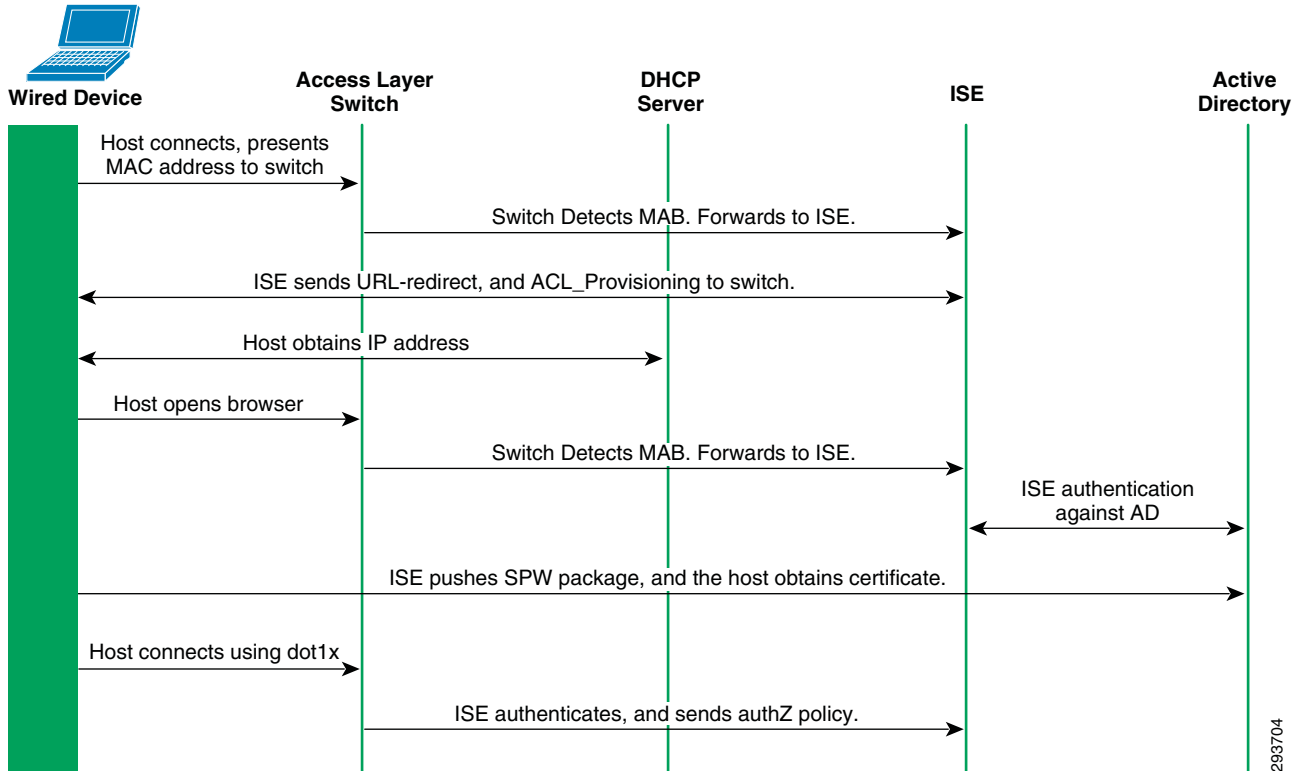
**Note**

Unless otherwise specified, in the figures throughout this chapter “Access Layer Switches” refers to either switches such as the Catalyst 3750X Series and Catalyst 4500 Series or to Catalyst 3850 Series converged access switches.

The following are high-level steps that occur when a wired device connects to the access layer switch:

1. The switch must detect that the wired endpoint is not configured for dot1x and should authenticate using MAB.
2. The ACL\_Provisioning\_Redirect ACL is used to match web traffic.
3. The URL redirect must point to the ISE Guest Registration portal.
4. The ACL\_Provisioning ACL must be downloaded on the port that restricts access in this state.
5. The user opens a browser and attempts to access any resource.
6. The switch redirects the user to an ISE self-registration portal.
7. ISE authenticates the user against AD and pushes the SPW package.
8. The SPW package helps the user register and obtain a digital certificate from ISE.
9. CoA occurs and the user reconnects to the network using the obtained digital certificate.

Figure 15-11 illustrates the flow for wired device provisioning.

**Figure 15-11** *Wired Device Provisioning Flow*

## Key and Certificate Storage

Being able to store digital certificates and their associated keys safely is critical for every device. Storage is implemented differently, depending on the operating system or media used. [Table 15-1](#) shows the different platforms tested in this design guide and their certificate stores.

**Table 15-1** *Platform and Certificate Storage*

Device	Certificate Store	How to Access
Microsoft Windows	Machine Certificate Store	Use the Certificates snap-in from the mmc.exe utility
Mac OS	Device Certificate Store	Use the Keychain Access application
Apple iPad	Device Certificate Store	Settings > General > Profile
Android	Credential Storage	Settings > Location & Security

Once provisioned, the certificates have the following attributes, which can be used by ISE to enforce different permissions:

**Common Name (CN) of the Subject:**

User identity used for authentication

**Subject Alternative Name:**

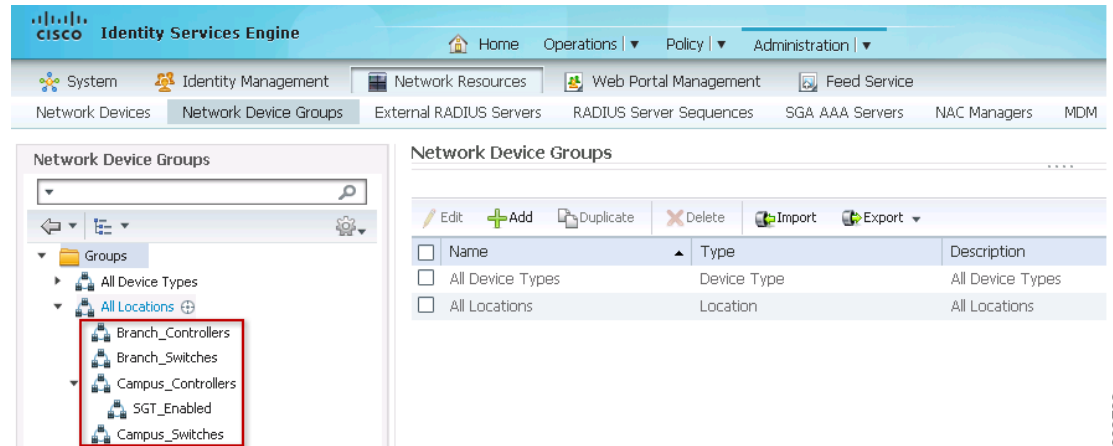
MAC address(es) of the endpoint.

# Network Device Groups

To differentiate between different connections, the ISE relies on Network Device Groups to group WLCs based on their location or device type. This allows a single ISE to enforce policies across different groups of devices. Click **Administration > Network Resources > Network Device Groups** to define locations for branch, campus, and SGT enabled controllers.

Figure 15-12 shows the different locations used in the authorization policy.

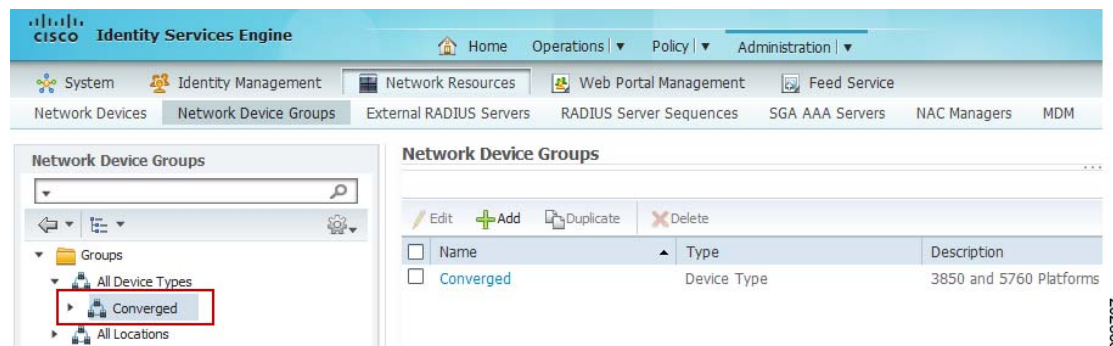
**Figure 15-12 ISE Device Groups—Locations**



293706

Similarly, Figure 15-13 shows a device type called **Converged** which can be created for Catalyst 3850 Series switches and CT5760 wireless controllers and used in the authorization policy.

**Figure 15-13 ISE Device Groups—Device Types**



293707



## Note

One of the reasons a device type is used instead of a location for Converged Access designs is that the same authorization policy rules are used for Converged Access branch and campus designs within this design guide. Hence location—campus versus branch—is not particularly relevant from a Cisco ISE perspective to Converged Access designs presented in this design guide. Note that if location is relevant, the customer can always modify the design presented here and choose to deploy separate authorization policy rules for branch and campus Converged Access designs as well.

Each Wireless LAN Controller, previously defined as a Network Device, needs to be added to the proper device group by clicking **Administration > Network Resources > Network Devices** and specifying the proper location or device type from the pull-down menu.

Figure 15-14 shows how the dc-wlc-1 Wireless LAN Controller belongs to the Campus\_Controllers Network Device Group.

**Figure 15-14 ISE Network Devices—Campus Controller**

The screenshot displays the Cisco Identity Services Engine (ISE) web interface for configuring a Network Device. The breadcrumb trail is **Administration > Network Resources > Network Devices**. The left sidebar shows a tree view with **Network Devices** selected. The main content area is titled **Network Devices List > dc-wlc-1**. The configuration form includes the following fields:

- Name:** dc-wlc-1
- Description:** (empty)
- IP Address:** 10.225.44.2 / 32
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
  - Device Type:** WLC (dropdown)
  - Location:** Campus\_Controllers (dropdown, highlighted with a red box)
- Authentication Settings:** (expanded)
  - Enable Authn:** (checkbox, checked)
  - Message Authn:** (checkbox, unchecked)

An **All Locations** dropdown menu is open, showing a list of locations: Branch\_Controllers, Branch\_Switches, Campus\_Controllers (selected), Campus\_Switches, Core, and DMZ. Each location has a corresponding **Show** button.

These device groups will be used in the authorization rules of the following sections to enforce full, partial, or Internet only access.

## Policy Enforcement for Security Group Access

Enforcing policies for SGA in BYOD architecture consist of two main components:

- Defining tags for the endpoints and the destination servers.
- Defining and implementing the Security Group ACL or Security Group Firewall (SG-FW) policy.

In this design, the Security Group ACL is implemented either on the Catalyst and Nexus Data Center switching infrastructure or on the ASA Firewall as an SG-FW policy. These two choices are discussed in Chapter 5, “Campus and Branch Network Design for BYOD” as two different deployment scenarios.

## Security Group Access Tags

The basic idea of Security Group Access is to associate a device or server's IP address with a Security Group Tag and then create role-based policies that either permit or deny traffic flows based on these source and destination SGTs. For example: are devices tagged with an SGT 10 allowed to communicate with a server tagged with an SGT 40? This flow is either allowed or blocked at the enforcement point.

Using this tagging concept, unique tags have been defined for each device accessing the network as a client. As explained in [Chapter 5, “Campus and Branch Network Design for BYOD”](#) unique permissions are granted to personal and corporate devices and hence unique tags have been defined for each use case.

[Table 15-2](#) illustrates how tags are assigned to different devices.

**Table 15-2**      **Source Tags**

Device Type	Tag
Corporate device with Full Access	SGT 10
Personal device with Full Access	SGT 11
Personal device with Partial Access	SGT 12

Similarly, the destination servers also need to be associated with a particular tag. [Table 15-3](#) illustrates how based on their role, servers are assigned with a different tag.

**Table 15-3**      **Destination Tags**

Destination Server	Tag
Open Access	SGT 40
Corporate Server	SGT 50

## Security Group ACL

After defining the source tags and destination tags, the next logical step is to define the egress policy matrix that defines the enforcement policy between a source and destination tag. [Table 15-4](#) illustrates the egress policy matrix.

**Table 15-4**      **Egress Policy Matrix**

	Device Type	SGT 40	SGT 50
SGT 10	Corporate device with Full Access	Yes	Yes
SGT 11	Personal device with Full Access	Yes	Yes
SGT 12	Personal device with Partial Access	Yes	No

As shown in [Table 15-4](#), corporate or personal devices granted full access will be allowed to reach servers that have been tagged with SGT 40 or SGT 50. Similarly, a personal device with partial access is only allowed to connect with a server tagged with SGT 40.

The implementation of the SGACL depends upon the type of the deployment scenario. For the deployment scenario where Nexus is the enforcement point the SGACL is defined in ISE and pushed to the Nexus switch whereas when the deployment scenario is using ASA as the enforcement point then an SGT-based access rule is configured manually on the ASA firewall.

## Authorization Policies for SGT

Based on policy matches and authorization profiles, the ISE assigns an SGT tag to endpoints. [Centralized Campus with SGT](#), found later in this chapter, provides information as to the criteria used to determine when an ACL versus an SGT should be returned upon successful authorization based on the network device type of the wireless controller defined in ISE.

For the destination tags assigned to servers, the configuration is done manually at the data center switch, and the actual enforcement happens based on the deployment scenario. To obtain more information on how to configure tags for servers and on the ASA, refer to [Chapter 12, “Security Group Access for BYOD.”](#)

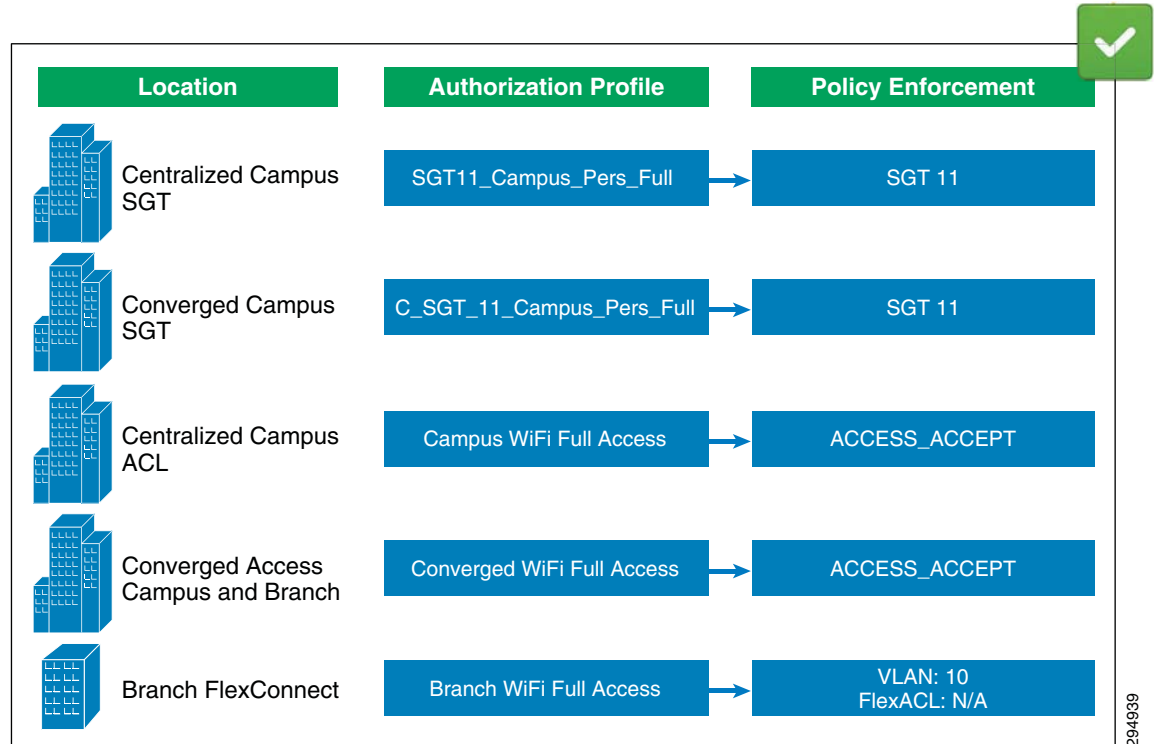
## Personal Wireless Devices—Full Access

To provide full access to personal devices, the Cisco ISE verifies the following:

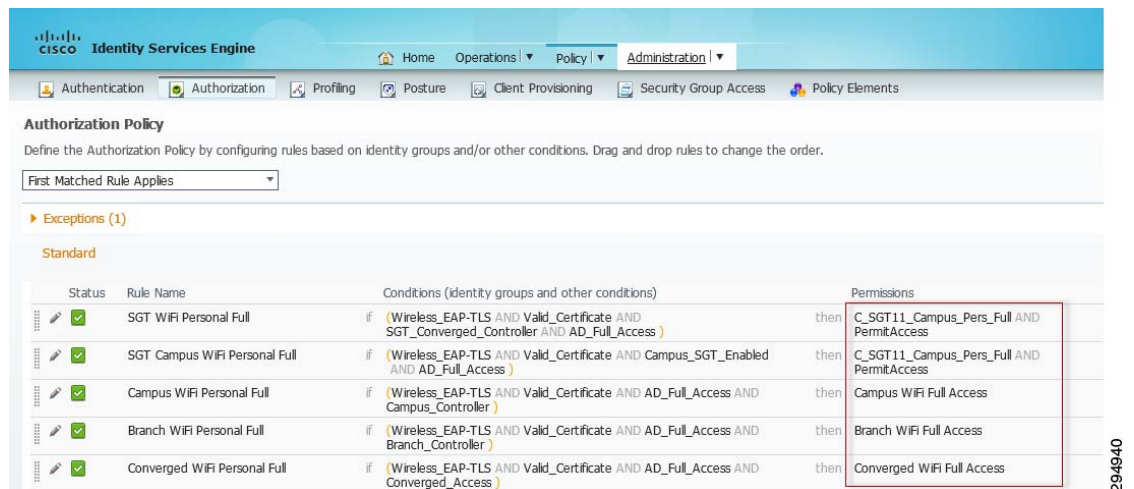
- The employee has completed the on-boarding process through the Guest Registration portal.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate.
- The connection originated using EAP-TLS authentication.
- The user is a member of the BYOD\_Full\_Access Active Directory group.

Since the wireless designs presented in this design guide rely on different WLCs for FlexConnect branches, centralized controller campuses, and Converged Access campuses and branches; unique authorization rules are created for connections originating from each design. At a high level, [Figure 15-15](#) shows how different authorization profiles are selected for connections originating from different locations with different wireless designs. Each authorization profile in turn enforces a unique permission.



**Figure 15-15 Full Access Enforcement**

To configure the authorization rules in ISE, click **Policy > Authorization**. Figure 15-16 highlights the authorization policy to grant full access to personal devices.

**Figure 15-16 Authorization Policies for Full Access**

Looking at the rules in more detail, ISE evaluates the following conditions:

- Wireless\_EAP-TLS—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).
- The user belongs to a specific Active Directory group (defined as a simple condition).

- The RADIUS authentication originated from a wireless controller which was a member of one of the following device groups—SGT\_Converged\_Controller, Campus\_Controller, SGT\_Controller, Branch\_Controller, or Converged\_Access (defined as a simple condition).

**Note**

A wireless controller which is a member of the Converged\_Access device group could be either a standalone device, such as a Cisco CT5760 wireless controller, or a switch with integrated wireless controller functionality, such as the Catalyst 3850.

## Simple and Compound Conditions

To improve the readability of the authorization policy, simple and compound authorization conditions were defined to group different conditions. These conditions may be reused and modified without changing every authorization rule.

Table 15-5 shows the conditions used in the authorization rules:

**Table 15-5 Simple and Compound Conditions**

<b>Wireless EAP-TLS (Compound)</b>	
Wireless_EAP-TLS (See Figure 15-18)	Radius:Service-Type Equals Framed AND
	Radius:NAS-Port-Type Equals Wireless - IEEE 802.11 AND
	Network Access:EapAuthentication Equals EAP-TLS
<b>Check for Valid Certificate (Simple)</b>	
Valid_Certificate (See Figure 15-19)	Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name
<b>Active Directory Group (Simple)</b>	
AD_Full_Access	AD1:ExternalGroups EQUALS sdulab.com/Users/BYOD_Full_Access
AD_Partial_Access	AD1:ExternalGroups EQUALS
AD_Domain_users	sdulab.com/Users/BYOD_Partial_Access
	AD1:ExternalGroups EQUALS sdulab.com/Users/Domain User
<b>WLC Location or Device Type (Simple)</b>	
SGT_Controller	DEVICE:Location EQUALS All
Campus_Controller	Locations#Campus_Controllers#SGT_Enabled
Branch_Controller	DEVICE:Location EQUALS All Locations#Campus_Controllers
Converged_Access	DEVICE:Location EQUALS All Locations#Branch_Controllers
	DEVICE:Device Type EQUALS All Device Types#Converged

To illustrate the value of using simple/compound conditions, Figure 15-17 shows how much longer and harder to read a rule can be when simple/compound conditions are not implemented.

Cisco Identity Services Engine

Home
Operations
Policy
Administration

Authentication
Authorization
Profiling
Posture
Client Provisioning
Security Group Access
Policy Elements

### Authorization Policy

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

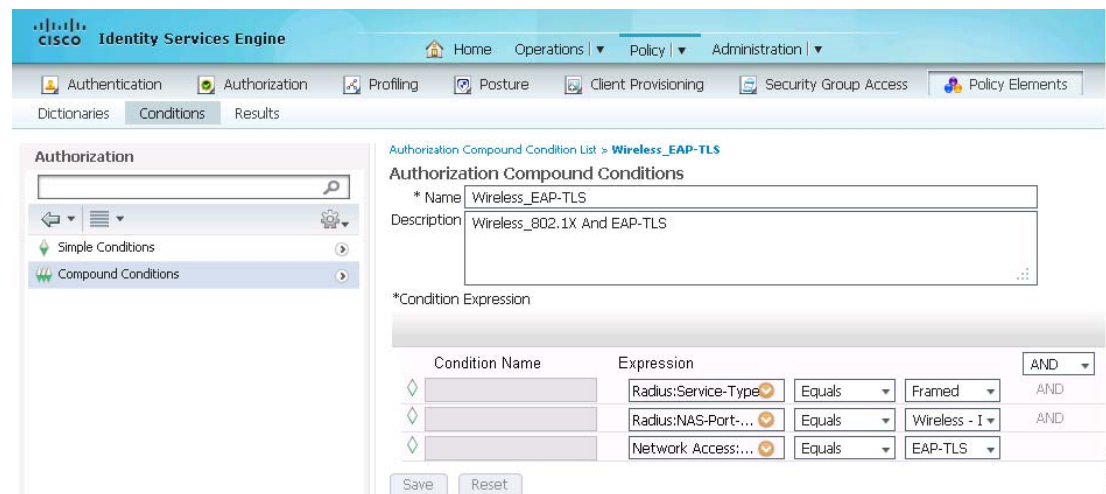
First Matched Rule Applies

Exceptions (1)

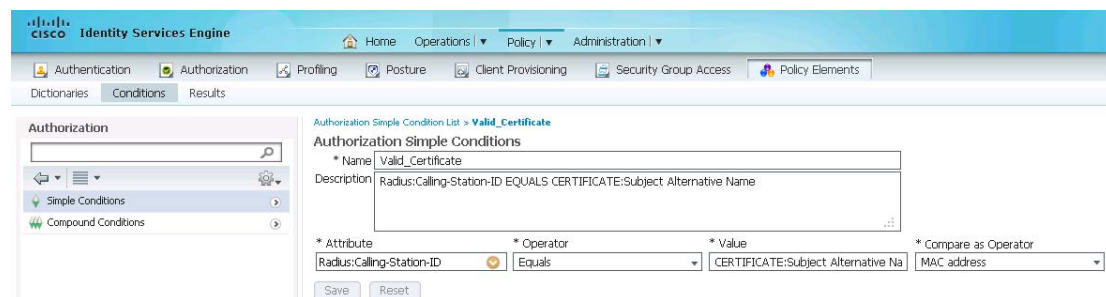
Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	SGTCampus WIFI Personal Full	if (Radius:Service-Type EQUALS Framed AND Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 AND AD1:ExternalGroups EQUALS sduilab.com/Users/BYOD_Full_Access AND Network Access:EapAuthentication EQUALS EAP-TLS AND DEVICE:Location EQUALS All Locations#Campus_Controller#SGT_Enabled AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name)	then SGT11_Campus_Pers_Full AND PermitAccess

**Figure 15-18**      **Wireless\_EAP-TLS Condition**



**Figure 15-19**     *Valid\_Certificate Condition*



15-19

**Figure 15-20** AD\_Full\_Access Condition

Authorization Simple Condition List > AD\_Full\_Access

**Authorization Simple Conditions**

\* Name: AD\_Full\_Access

Description: AD1:ExternalGroups EQUALS Sdulab.com/Users/BYOD\_Full\_Access

* Attribute	* Operator	* Value
AD1:ExternalGroups	Equals	sdulab.com/Users/BYOD_Full_Acc

Save Reset

The remaining conditions mentioned in Table 5 are defined in a similar way.

## Permissions

Permission is a result of an authorization policy match, and the permission can be of different types such as an authorization profile, or a standard result. Table 15-6 explains the permissions used for full access.

**Table 15-6** Permissions for Full Access

Permission name	Permission type	Purpose
C_SGT11_Campus_Pers_Full	Standard result	To Assign a SGT for 802.1X wireless devices connecting from a Converged Access SGT enabled controller and allowing full access.
SGT11_Campus_Pers_Full	Standard result	To Assign a SGT for 802.1X wireless devices connecting from an SGT-enabled controller allowing full access.
Campus WiFi Full Access	Authorization profile	Provides Full Access for 802.1X wireless devices connecting from a centralized campus controller.
Branch WiFi Full Access	Authorization profile	To push a VLAN for 802.1X wireless devices connecting from a FlexConnect branch controller
Converged WiFi Full Access	Authorization profile	Provides Full Access for 802.1X wireless devices connecting from a Converged Access controller.



### Note

A Converged Access infrastructure refers to a branch or campus deployment with Catalyst 3850 Series switches and/or CT5760 wireless controllers within this design guide.

## Centralized Campus with SGT

As explained in [Policy Enforcement for Security Group Access](#), the personal device with permissions for full access will be assigned an SGT value of 11. Once the personal device obtains the tag value of 11, it can then connect with all the servers in the data center.



### Note

Centralized Campus with SGT refers to a Wireless LAN Controller which is part of Centralized Wireless LAN Architecture and is enabled with SGT capability.

[Figure 15-21](#) shows how the SGT11\_Campus\_Pers\_Full authorization profile uses SGT 11 for personal devices granted full access.

**Figure 15-21 SGT11\_Campus\_Pers\_Full**

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a security group. The breadcrumb trail at the top indicates the path: Home > Operations > Policy > Administration > Security Groups. The left-hand navigation pane shows a tree structure with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, Security Group ACLs, Security Groups, and Security Group Mappings. The 'Security Groups' category is selected, and the specific group 'SGT11\_Campus\_Pers\_Full' is chosen from the 'Security Groups List'. The main configuration area shows the group's name as 'SGT11\_Campus\_Pers' and its description as 'Personal Devices With A Full Access Get A Tag Value Of 11.' Below this, there are two radio button options: 'Allow system to automatically generate tag' (which is unselected) and 'Select value from reserved range' (which is selected). Under the selected option, the 'Tag Value' is set to '11' in a text box, which is highlighted with a red rectangle. To the right of the text box is a hint: 'Enter value between 5 and 80'. At the bottom of the configuration area are 'Save' and 'Reset' buttons. The bottom right corner of the screenshot contains the number '293714'.

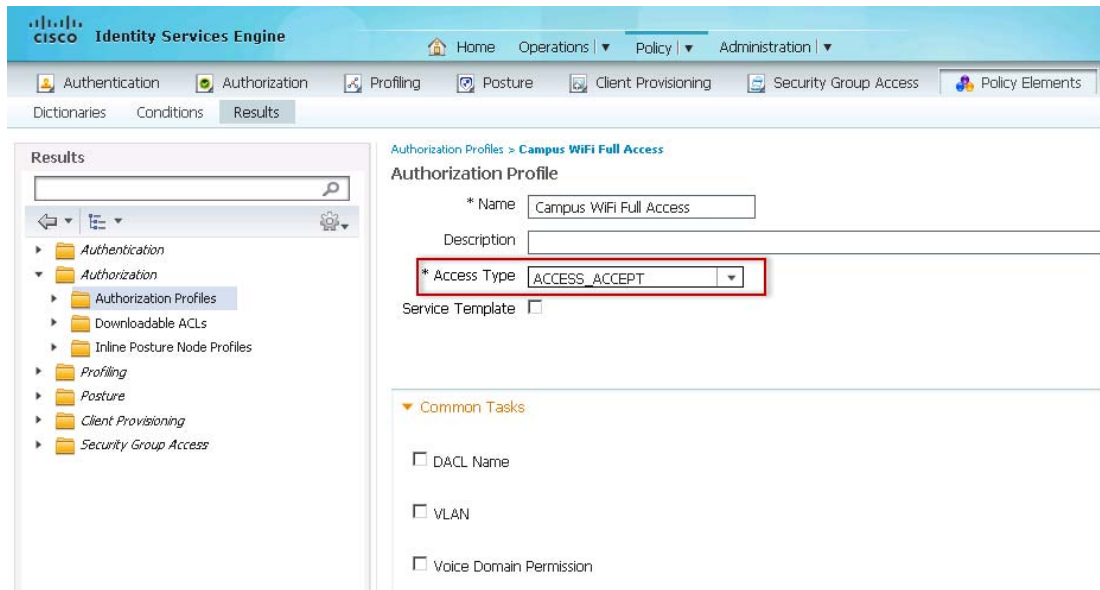
See [Policy Enforcement for Security Group Access](#) for details regarding the SGT egress policy matrix which defines the permissions for SGT11 allowing full access for a campus which implements a centralized controller (Local Mode) design with SGTs.

## Converged Access Campus with SGT

The authorization result used in this rule is same as the one used in the Centralized Campus with SGT, but the key difference is that it is initiated by a Converged Access Switch in a Campus network. The Conditions that are part of this rule match for Converged Access Switches only.

## Centralized Campus with ACLs

[Figure 15-22](#) shows how the Campus WiFi Full Access authorization profile is using the ACCESS\_ACCEPT Access Type to allow full access.

**Figure 15-22** *Campus WiFi Full Access*

Since full access is allowed with this authorization profile, no Named ACL for access control needs to be specified by ISE.

## Branch with FlexConnect

Endpoints connecting from a branch location which implements FlexConnect dynamically get assigned to VLAN 10, which has been configured to provide full access. [Figure 15-23](#) shows the Branch WiFi Full Access authorization profile.

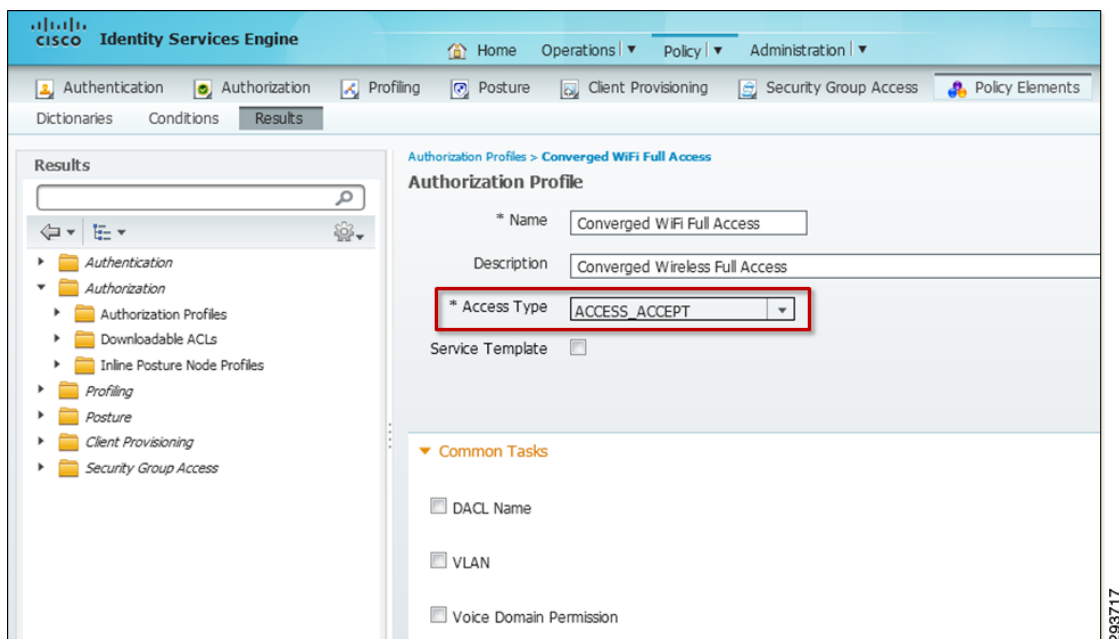
**Figure 15-23** *Branch WiFi Full Access*

The screenshot displays the Cisco Identity Services Engine (ISE) configuration page for an authorization profile named "Branch WiFi Full Access". The interface includes a navigation pane on the left with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. The main content area shows the configuration for the selected profile, including fields for Name, Description, Access Type (set to ACCESS\_ACCEPT), and Service Template. Under "Common Tasks", the "VLAN" checkbox is checked, showing a Tag ID of 1 and an ID/Name of 10. The "Advanced Attributes Settings" section shows a list of attributes, and the "Attributes Details" section displays the resulting configuration: Access Type = ACCESS\_ACCEPT, Tunnel-Private-Group-ID = 1:10, Tunnel-Type=1:13, and Tunnel-Medium-Type=1:6.

Since full access is allowed with this authorization profile, no FlexConnect ACL for access control needs to be associated with VLAN 10 on the access point.

## Converged Access Branch or Campus

Figure 15-24 shows how the Converged WiFi Full Access authorization profile is using the ACCESS\_ACCEPT Access Type to allow full access.

**Figure 15-24** Converged WiFi Full Access

Again, since full access is allowed with this authorization profile, no Named ACL for access control needs to be specified by ISE.

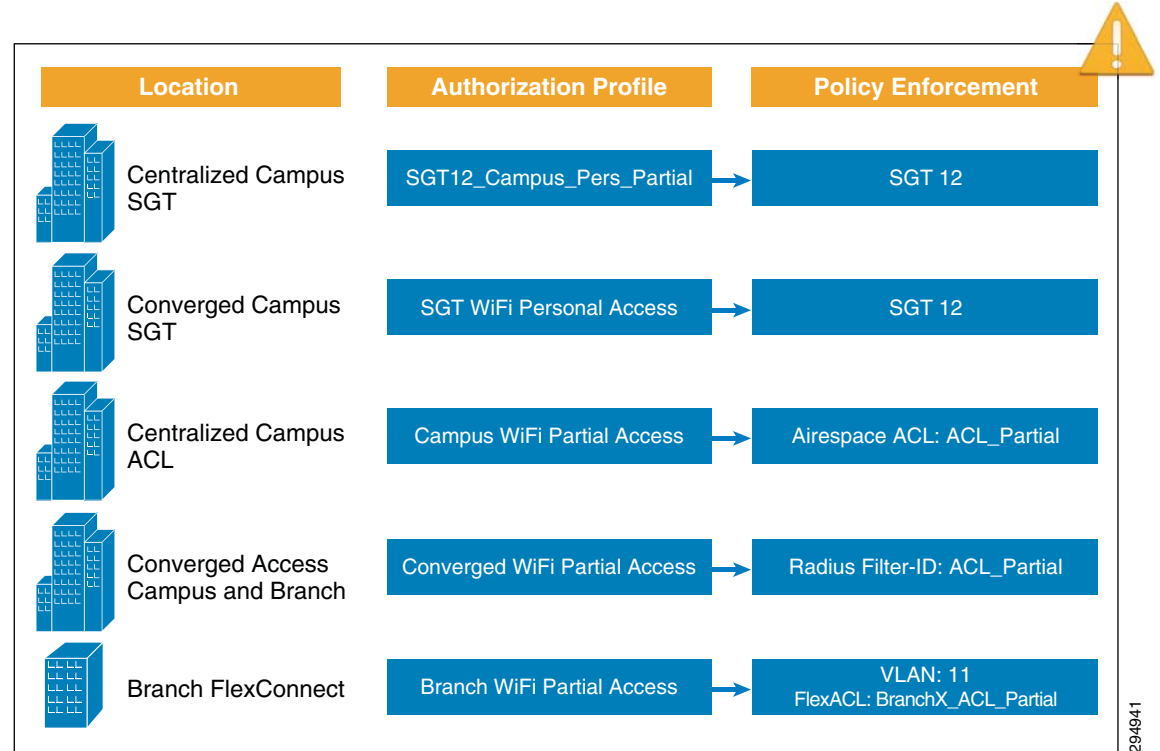
## Personal Wireless Devices—Partial Access

To provide partial access to personal devices, the Cisco ISE verifies the following:

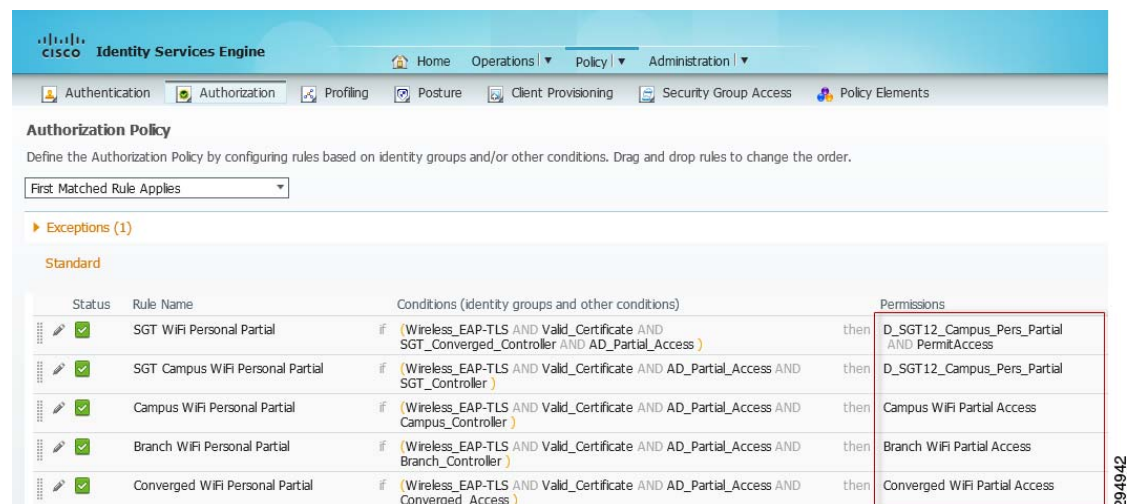
- The employee has completed the on-boarding process through the Guest Registration portal.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is member of the BYOD\_Partial\_Access Active Directory group.

At a high level, [Figure 15-25](#) shows how different authorization profiles are selected for devices accessing the network from different locations with different wireless designs. Each authorization profile in turn enforces a unique permission using either VLANs, SGTs, dynamic ACLs, FlexConnect ACLs, etc.



**Figure 15-25** Partial Access Enforcement

To configure the authorization rules in ISE, click **Policy > Authorization**. Figure 15-26 highlights the authorization policy to grant partial access to personal devices.

**Figure 15-26** Authorization Policies for Partial Access

Looking at the rules in more detail, ISE evaluates the following conditions:

- **Wireless\_EAP-TLS**—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).

- The user belongs to a specific Active Directory group (defined as a simple condition).
- The RADIUS authentication originated from a wireless controller which was a member of one of the following device groups—SGT\_Converged\_Controller, Campus\_Controller, SGT\_Controller, Branch\_Controller, or Converged\_Access (defined as a simple condition).

[Simple and Compound Conditions](#) explains the different conditions used in the rules.

## Permissions

Permission is a result of an authorization policy match and the permission can be of different types such as an authorization profile or a standard result. [Table 15-7](#) explains the permissions used for partial access.

**Table 15-7** *Permissions Used for Wireless Partial Access*

Permission name	Permission type	Purpose
SGT12_Campus_Pers_partial	Standard result	To Assign a SGT for 802.1X wireless devices connecting from an SGT-enabled controller granting partial access to some servers in the data center.
Converged Campus SGT	Standard result	To Assign a SGT for 802.1X wireless devices connecting from a Converged Access SGT enabled controller and allowing partial access.
Campus WiFi Partial Access	Authorization profile	To push a named ACL for 802.1X wireless devices connecting from a centralized campus controller.
Branch WiFi Partial Access	Authorization profile	To push a VLAN for 802.1X wireless devices connecting from a FlexConnect branch controller
Converged WiFi Partial Access	Authorization profile	To push a named ACL for 802.1X wireless devices connecting from either a campus or branch location with Converged Access

## Centralized Campus with SGT

As explained in [Policy Enforcement for Security Group Access](#), the personal device with permissions for partial access will be assigned an SGT value of 12. Once the personal device obtains the tag value of 12 it can then connect with only those servers with an SGT of 50 in the data center.

[Figure 15-27](#) shows how the SGT12\_Campus\_Pers\_Partial authorization profile is configured to assign SGT 12 to personal devices thus allowing partial access.

**Figure 15-27 SGT12\_Campus\_Pers\_Partial**

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, and Administration. The left sidebar shows a tree view of configuration objects, with Security Groups expanded. The main content area displays the configuration for the Security Group 'SGT12\_Campus\_Pers'. The 'Name' field is 'SGT12\_Campus\_Pers' and the 'Generation Id' is 7. The 'Description' field contains the text 'Personal Devices With Partial Access Get A Tag Value Of 12.' Below the description, there are two radio buttons: 'Allow system to automatically generate tag' (unselected) and 'Select value from reserved range' (selected). A 'Tag Value' field is highlighted with a red box, containing the value '12'. To the right of the field is the text 'Enter value between 5 and 80'. At the bottom of the configuration area are 'Save' and 'Reset' buttons.

See [Policy Enforcement for Security Group Access](#) for details regarding the SGT egress policy matrix which defines the permissions for SGT12 allowing full access for a campus which implements a centralized controller (Local Mode) design with SGTs.

## Converged Access Campus with SGT

This authorization result used in this rule is same as the one used in the Centralized Campus with SGT, but the key difference is that it is initiated by a Converged Access Switch in a Campus network. The Conditions that are part of this rule match for Converged Access Switches only.

## Centralized Campus with ACLs

For devices connecting from a campus location which implements a centralized (Local Mode) wireless design, the Campus WiFi Partial Access authorization profile relies on the ACL\_Partial\_Access access list, enforced by the WLC. [Figure 15-28](#) shows the authorization profile.

**Figure 15-28** Campus WiFi Partial Access

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, a secondary navigation bar shows 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Results' tab is selected in the left sidebar, which also lists 'Authentication', 'Authorization', 'Downloadable ACLs', 'Inline Posture Node Profiles', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'.

The main content area is titled 'Authorization Profiles > Campus WiFi Partial Access'. It shows the configuration for an 'Authorization Profile' with the following details:

- Name:** Campus WiFi Partial Access
- Description:** Campus WiFi Partial Access
- Access Type:** ACCESS\_ACCEPT
- Service Template:** (unchecked)

Under the 'Common Tasks' section, several checkboxes are visible: 'MACSec Policy' (unchecked), 'NEAT' (unchecked), 'Web Authentication (Local Web Auth)' (unchecked), 'Airespace ACL Name' (checked), and 'ASA VPN' (unchecked). The 'Airespace ACL Name' checkbox is highlighted with a red rectangle, and its value is 'ACL\_Partial\_Access'.

The 'Advanced Attributes Settings' section shows a dropdown menu with 'Select an item' and a plus sign. The 'Attributes Details' section at the bottom shows the following attributes:

- Access Type = ACCESS\_ACCEPT
- Airespace-ACL-Name = ACL\_Partial\_Access

The page number '293721' is visible in the bottom right corner.

Cisco Wireless LAN Controllers support named ACLs, meaning that the ACL must be previously configured on the controller rather than being downloaded from ISE. Using the RADIUS Airespace-ACL Name attribute-value pair, ISE instructs the WLC to apply the ACL\_Partial\_Access ACL. Figure 15-29 shows the contents of this ACL, as defined in the CT5508 WLC campus controller.

**Figure 15-29** *ACL\_Partial\_Access on Wireless Controller*

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK										
Access Control Lists > Edit										
General										
Access List Name		ACL_Partial_Access								
Deny Counters		0								
Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction
<a href="#">1</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any	Any	Inbound
<a href="#">2</a>	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Outbound
<a href="#">3</a>	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any	Any	Inbound
<a href="#">4</a>	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Outbound
<a href="#">5</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server	Any	Inbound
<a href="#">6</a>	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client	Any	Outbound
<a href="#">7</a>	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any	Any	Inbound
<a href="#">8</a>	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Outbound
<a href="#">9</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.4.0	/ 255.255.255.0	Any	Any	Any	Any	Inbound
<a href="#">10</a>	Permit	10.230.4.0	/ 255.255.255.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Outbound
<a href="#">11</a>	Deny	0.0.0.0	/ 0.0.0.0	10.230.0.0	/ 255.255.0.0	Any	Any	Any	Any	Inbound
<a href="#">12</a>	Deny	10.230.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Outbound
<a href="#">13</a>	Deny	0.0.0.0	/ 0.0.0.0	10.225.0.0	/ 255.255.0.0	Any	Any	Any	Any	Inbound
<a href="#">14</a>	Deny	10.225.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Outbound
<a href="#">15</a>	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any

293722

The access-list shown in [Figure 15-29](#) 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).
- Allow IP access to and from the MDM Server (203.0.113.10).
- Allow IP access to and from specific subnet (10.230.4.0 /24).
- Deny IP access to and from data center subnets (10.230.0.0 /16).
- Deny IP access to and from campus subnets (10.225.0.0 /16).
- Allow access to and from all other subnets (Internet access).

**Note**

Note that Access Control Entries (ACEs) for the MDM server are included within the ACLs in this chapter. These are not used for the Enhanced Access use case discussed within this chapter. The Advanced Access use case, discussed in [Chapter 17, “BYOD Advanced Use Case—Mobile Device Manager Integration,”](#) makes use of the same authorization policy rules and authorization profiles.

The access list shown in [Figure 15-29](#) is a generic example used to enforce a hypothetical use case and is not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

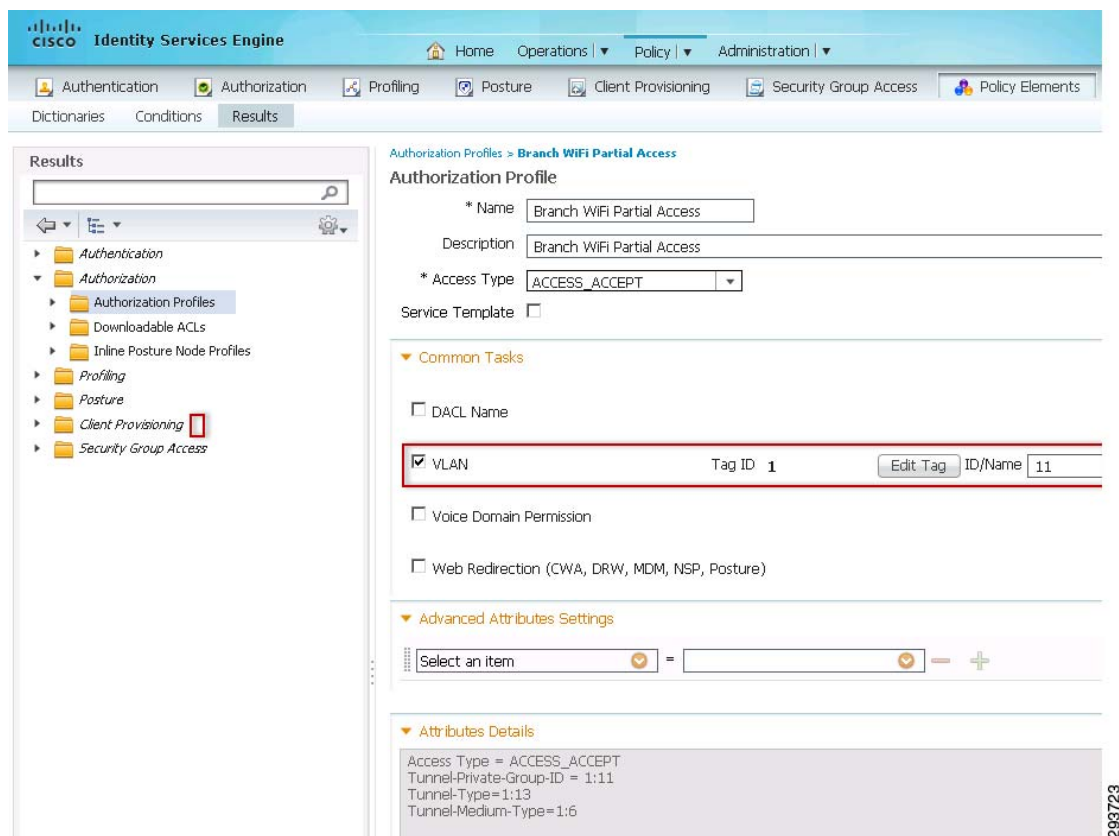
**Note**

The CT5508 WLC supports a maximum of 64 ACLs with a maximum of 64 lines per ACL.

## Branches with FlexConnect

For devices connecting from a branch location which implements a FlexConnect wireless design, the Branch WiFi Partial Access authorization profile dynamically assigns the device to VLAN11, which is dedicated for devices obtaining Partial Access. Figure 15-30 shows this authorization profile.

**Figure 15-30** Branch WiFi Partial Access



Deploying ACLs on the branch is slightly different than using ACLs with a centralized WLC. For branch locations, the Cisco 7500 Flex Wireless Controller relies on FlexConnect ACLs to enforce policy permissions within this design guide. FlexConnect ACLs are created on the WLC and configured with the VLAN defined on the AP or the FlexConnect Group using the VLAN-ACL mapping for dynamic or AAA override VLANs. These FlexConnect ACLs are pushed to the APs when the authorization policy matches. This design guide relies on FlexConnect groups to enforce Flex ACLs for each VLAN. The steps are as follows:

1. Create a FlexConnect ACL for each branch.
2. Apply the FlexConnect ACL on the FlexConnect group for each branch.
3. Define the VLAN-ACL mapping for each VLAN.

On the FlexConnect 7500 Controller, click **Security > Access Control Lists > FlexConnect ACLs** and define the ACL rules for Partial Access. Figure 15-31 shows the Branch1\_ACL\_Partial\_Access ACL, which allows access to the Internet and some internal resources.

**Note**

A unique ACL may be needed for each branch since each branch location may have its own local resources and unique IP address space.

**Figure 15-31** *Branch1\_ACL\_Partial\_Access*

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK									
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	
<a href="#">1</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any	
<a href="#">2</a>	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">3</a>	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any	
<a href="#">4</a>	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">5</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server	
<a href="#">6</a>	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client	
<a href="#">7</a>	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any	
<a href="#">8</a>	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">9</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.4.0	/ 255.255.255.0	Any	Any	Any	
<a href="#">10</a>	Permit	10.230.4.0	/ 255.255.255.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">11</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.0.0	/ 255.255.0.0	Any	Any	Any	
<a href="#">12</a>	Permit	10.230.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">13</a>	Permit	0.0.0.0	/ 0.0.0.0	10.225.0.0	/ 255.255.0.0	Any	Any	Any	
<a href="#">14</a>	Permit	10.225.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">15</a>	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	

293724

The above 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).
- Allow IP access to and from the MDM Server (203.0.113.10).
- Allow IP access to and from specific subnet (10.230.4.0 /24). Similar ACL entries could be added to allow access to Branch1 subnets/servers.
- Deny IP access to and from data center subnets (10.230.0.0 /16).
- Deny IP access to and from campus subnets (10.225.0.0 /16).
- Allow access to and from all other subnets (Internet access).

**Note**

The access list shown is a generic example used to implement an arbitrary use case and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

For the purposes of this design guide, a FlexConnect group is defined for each branch, which allows for multiple FlexConnect access points in the branch to share configuration parameters.

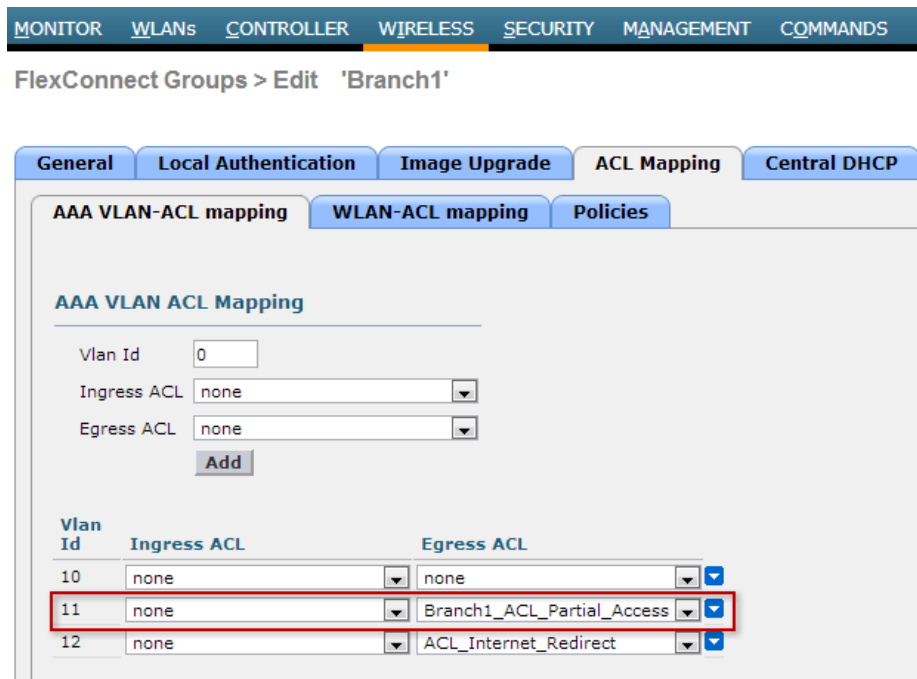
On the FlexConnect 7500 controller, click **Wireless > FlexConnect Groups** and select the FlexConnect group for a particular branch location, as shown in Figure 15-32.

**Figure 15-32 FlexConnect Groups**



In Figure 15-33, the FlexConnect group for Branch1 is applying the Branch1\_ACL\_Partial\_Access ACL to endpoints connecting to VLAN 11.

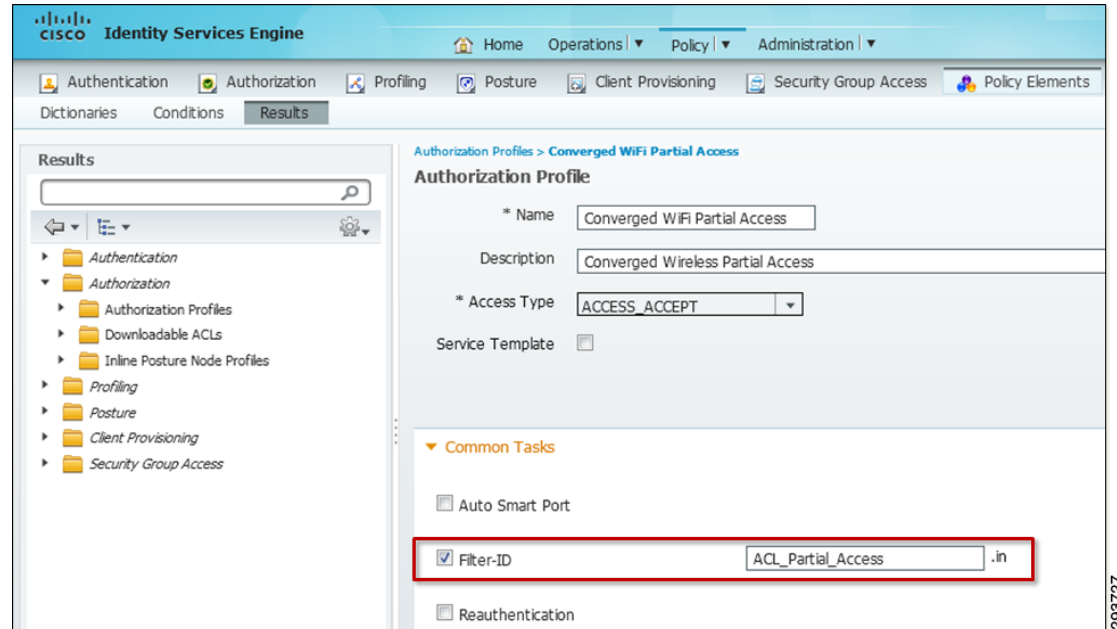
**Figure 15-33 FlexConnect Group for Branch1**



## Converged Access Branch or Campus

For devices connecting from campus or branch locations which implement a Converged Access design, the Converged WiFi Partial Access authorization profile relies on the ACL\_Partial\_Access access list, enforced by the Catalyst 3850 Series switch. Figure 15-34 shows the authorization profile.



**Figure 15-34** Converged WiFi Partial Access

Cisco Catalyst 3850 Series switches (and CT5760 wireless controllers) support both named ACLs and downloadable ACLs. For the Converged Access design a named ACL is implemented, meaning that the ACL must be configured on the Catalyst 3850 switch rather than being downloaded from ISE. Using the RADIUS Filter-ID attribute-value pair, ISE instructs the WLC to apply the ACL\_Partial\_Access ACL. The following configuration example shows the contents of this ACL, as defined in the Catalyst 3850 switch.

```
!
ip access-list extended ACL_Partial_Access
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 203.0.113.10
 permit ip any 10.230.4.0 0.0.0.255
 permit ip any host 10.230.6.2
 permit ip any host 10.225.100.10
 deny ip any 10.230.0.0 0.0.255.255
 deny ip any 10.225.0.0 0.0.255.255
 deny ip any 10.200.0.0 0.0.255.255
 permit ip any any
!
```

The access list shown in above similar to the access list shown in [Figure 15-29](#), but configured on a Catalyst switch instead of a wireless controller. Hence the structure of the access list is slightly different. The access list 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 MDM Server (203.0.113.10).
- Allow IP access to and from specific servers (10.230.6.2 and 10.225.100.10).
- Deny IP access to and from data center subnets (10.230.0.0 /16).
- Deny IP access to and from campus subnets (10.225.0.0 /16).

- Deny IP access to and from branch subnets (10.200.0.0 /16).
- Allow access to and from all other subnets (Internet access).

Again, the access list shown in this example is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

**Note**

This design guide shows the use of the Radius:Airespace-ACL-Name AV pair for specifying a named ACL on CUWN wireless controller platforms, such as the CT5508 and Flex 7500 wireless controllers. However, it shows the use of the Radius:Filter-Id AV pair for specifying a named ACL on Cisco IOS-based wireless controller platforms, such as the CT5760 wireless controller and Catalyst 3850 Series switch. For wireless devices, this is simply to highlight the fact that the network administrator can utilize the legacy Airespace-ACL-Name AV pair or the RADIUS standard method of the Filter-Id AV pair within the BYOD implementation. It is recommended that the network administrator standardize on one of the two methods to specify a named ACL where possible in actual deployments.

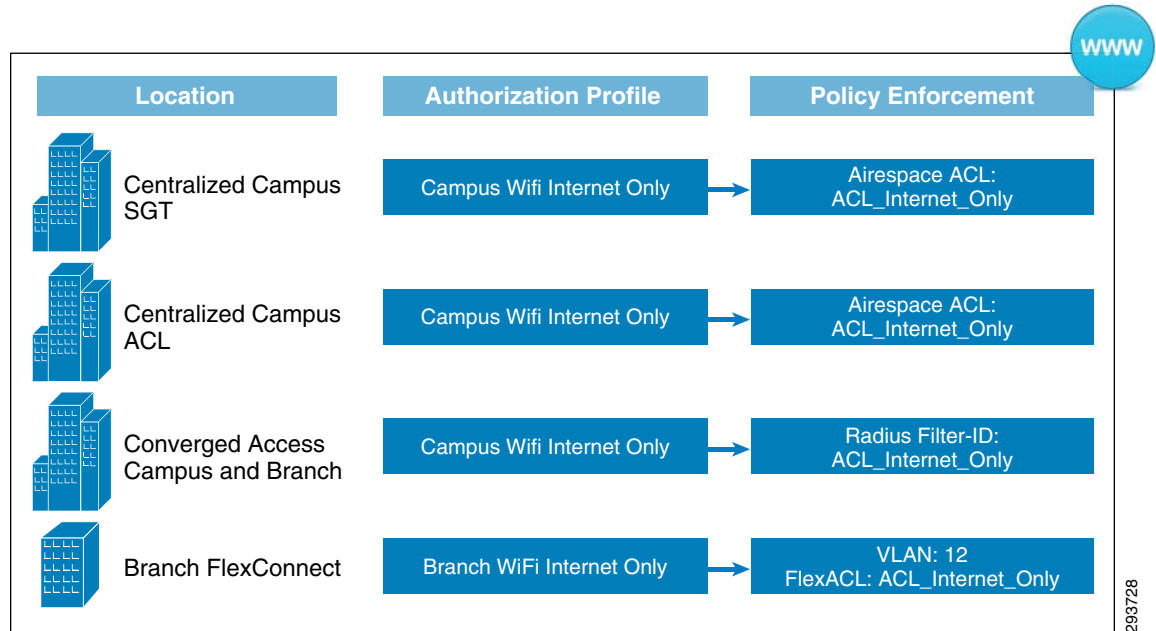
Since a single ISE policy rule is defined for partial access of personal wireless devices from either a branch or campus with a converged access infrastructure, the access list can be customized to the specific branch or campus location as needed. The specific example ACL shown above is consistent with the ACL discussed in the campus centralized (Local Mode) controller design previously discussed.

## Personal Wireless Devices—Internet Only Access

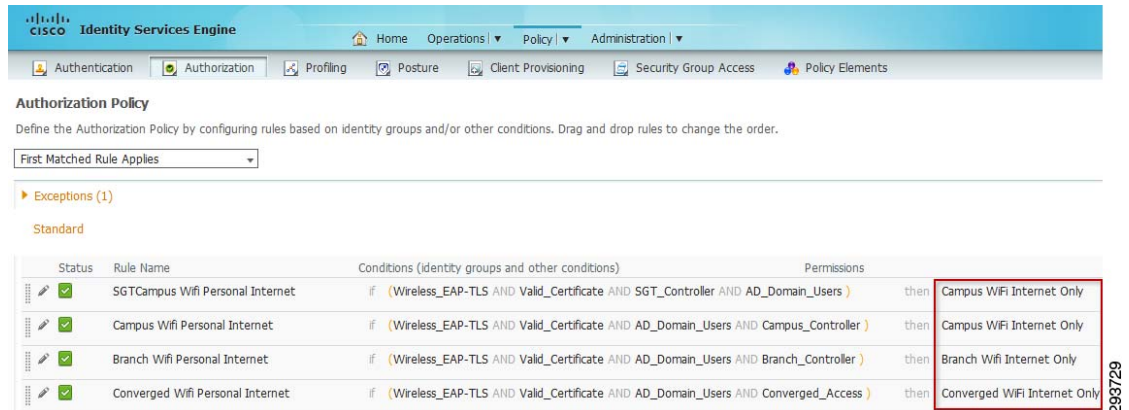
To provide Internet Only access to personal devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the Guest Registration portal.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the Domain Users Active Directory group.

At a high level, [Figure 15-35](#) shows how different authorization profiles are selected for devices coming from different locations with different wireless designs. Each authorization profile in turn enforces a unique permission using VLANs, SGTs, named ACLs, FlexConnect ACLs, etc.

**Figure 15-35 Internet Only Enforcement**

To configure the authorization rules in ISE, click **Policy > Authorization**. [Figure 15-36](#) highlights the authorization policy to grant Internet Only access to personal devices.

**Figure 15-36 Authorization Policies for Internet Only Access**

Looking at the rules in more detail, ISE evaluates the following conditions:

- **Wireless\_EAP-TLS**—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).
- The user belongs to the Domain Users Active Directory group (defined as a simple condition).
- The RADIUS authentication originated from a wireless controller which was a member of one of the following device groups—Campus\_Controller, SGT\_Controller, Branch\_Controller, or Converged\_Access (defined as a simple condition).

[Simple and Compound Conditions](#) explains the different conditions used in the rules.

## Permissions

When all conditions in the authorization policy rules match, the rule invokes the proper permission. In the previous sections the permission result was either an authorization profile (non-SGT based access), or a standard result for SGT based access. However, in this section only the authorization profile will be used for the reasons explained below.

- Campus WiFi Internet Only for 802.1X wireless devices connecting from a SGT\_enabled controller or from a campus location with a centralized (Local Mode) wireless design. Both the campus controller and the SGT\_enabled controller use the same authorization profiles. SGTs are not used to tag Internet only traffic since SGT relies on source and destination tags and the destination tag for the Internet is unknown.
- Branch Wireless Internet Only for 802.1X wireless devices connecting from a branch location which implements a Flexconnect wireless design.
- Converged WiFi Internet Only for 802.1X wireless devices connecting from either a campus or branch location which implements a Converged Access infrastructure design.

## Centralized Campus with SGT or ACLs

For devices connecting from a campus location which implements a centralized (Local Mode) wireless design or from a SGT\_enabled controller, the Campus WiFi Internet Only authorization profile relies on the ACL\_Internet\_Only access list enforced by the WLC. [Figure 15-37](#) shows how the authorization profile instructs the WLC to apply the ACL.

**Figure 15-37** *Campus WiFi Internet Only*

**Results**

- Authentication
- Authorization
  - Authorization Profiles
  - Downloadable ACLs
  - Inline Posture Node Profiles
- Profiling
- Posture
- Client Provisioning
- Security Group Access

**Authorization Profiles > Campus WiFi Internet Only**

**Authorization Profile**

\* Name: Campus WiFi Internet Only

Description:

\* Access Type: ACCESS\_ACCEPT

Service Template: ☐

**Common Tasks**

- ☐ MACSec Policy
- ☐ NEAT
- ☐ Web Authentication (Local Web Auth)
- ☒ Airespace ACL Name: ACL\_Internet\_Only
- ☐ ASA VPN

**Advanced Attributes Settings**

Select an item = +

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Airespace-ACL-Name = ACL\_Internet\_Only

Cisco Wireless LAN Controllers support named ACLs, meaning the ACL must be previously configured on the controller, rather than being downloaded from ISE. Using the RADIUS Airespace-ACL Name attribute-value pair, ISE instructs the WLC to apply the ACL\_Internet\_Only ACL.

Figure 15-38 shows the contents of this ACL, as defined in the CT5508 WLC campus controller.

**Figure 15-38 ACL\_Internet\_Only**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK									
Access Control Lists > Edit									
<b>General</b>									
Access List Name		ACL_Internet_Only							
Deny Counters		0							
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
<a href="#">1</a>	Permit	0.0.0.0 / 0.0.0.0	10.230.1.45 / 255.255.255.255	Any	Any	Any	Any	Inbound	
<a href="#">2</a>	Permit	10.230.1.45 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	
<a href="#">3</a>	Permit	0.0.0.0 / 0.0.0.0	10.225.49.15 / 255.255.255.255	Any	Any	Any	Any	Inbound	
<a href="#">4</a>	Permit	10.225.49.15 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	
<a href="#">5</a>	Permit	0.0.0.0 / 0.0.0.0	10.230.1.61 / 255.255.255.255	UDP	DHCP Client	DHCP Server	Any	Inbound	
<a href="#">6</a>	Permit	10.230.1.61 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DHCP Server	DHCP Client	Any	Outbound	
<a href="#">7</a>	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	
<a href="#">8</a>	Deny	10.0.0.0 / 255.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	
<a href="#">9</a>	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	
<a href="#">10</a>	Deny	172.16.0.0 / 255.240.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	
<a href="#">11</a>	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	
<a href="#">12</a>	Deny	192.168.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	
<a href="#">13</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	

293731

The access list 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).
- Deny IP access to and from internal network address space (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
- Allow access to and from all other subnets (Internet access).

Once again, the access list is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

## Branches with FlexConnect

For devices connecting from a branch location which implements a FlexConnect wireless design, the Branch WiFi Internet Only authorization profile dynamically assigns the device to VLAN12, which is dedicated for devices obtaining Internet\_Only access.

Figure 15-39 shows this authorization profile.

**Figure 15-39** Branch WiFi Internet Only

**Results**

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

**Authorization Profiles > Branch WiFi Internet Only**

**Authorization Profile**

\* Name: Branch WiFi Internet Only

Description:

\* Access Type: ACCESS\_ACCEPT

Service Template: ☐

**Common Tasks**

☐ DACL Name

☒ VLAN Tag ID 1 Edit Tag ID/Name 12

☐ Voice Domain Permission

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

**Advanced Attributes Settings**

Select an item =

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Tunnel-Private-Group-ID = 1:12  
Tunnel-Type=1:13  
Tunnel-Medium-Type=1:6

For branch locations which implement FlexConnect wireless designs, the Cisco 7500 Flex Wireless Controller relies on FlexConnect ACLs to enforce policy permissions. FlexConnect ACLs are created on the WLC and configured with the VLAN defined on the AP or the FlexConnect Group using the VLAN-ACL mapping for dynamic or AAA override VLANs. These FlexConnect ACLs are pushed to the APs when the authorization policy matches.

1. Create a FlexConnect ACL for each branch.
2. Apply the FlexConnect ACL on the FlexConnect group for each branch.
3. Define the VLAN-ACL mapping for each VLAN.

On the FlexConnect 7500 Controller, click **Security > Access Control Lists > FlexConnect ACLs** and define the ACL rules for Internet\_Only access. Figure 15-40 shows an example of the Branch\_ACL\_Internet\_Only ACL, which only allows access to the Internet. This ACL is the same for all branches.

**Figure 15-40 Branch\_ACL\_Internet\_Only**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK									
Access Control Lists > Edit									
General									
Access List Name		Branch_ACL_Internet_Only							
Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	
<a href="#">1</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any	
<a href="#">2</a>	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">3</a>	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any	
<a href="#">4</a>	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">5</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server	
<a href="#">6</a>	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client	
<a href="#">7</a>	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any	
<a href="#">8</a>	Deny	10.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">9</a>	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any	
<a href="#">10</a>	Deny	172.16.0.0	/ 255.240.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">11</a>	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any	
<a href="#">12</a>	Deny	192.168.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">13</a>	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	

293733

The access list 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).
- Deny IP access to and from internal network address space (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
- Allow access to and from all other subnets (Internet access).

The access list is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

For the purposes of this design guide, a FlexConnect group is defined for each branch, which allows for multiple FlexConnect access points in the branch to share configuration parameters.

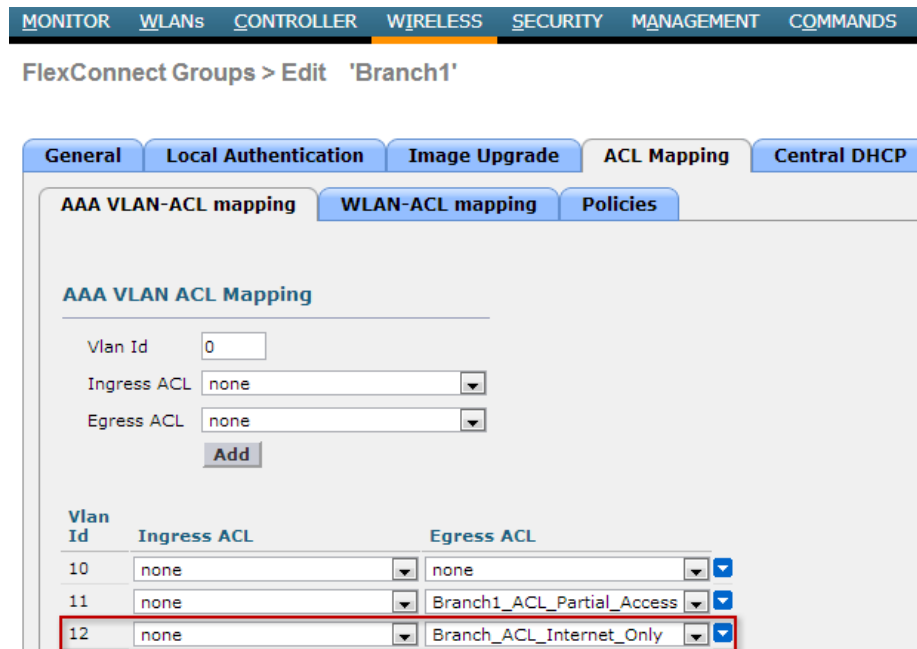
On the FlexConnect 7500 controller, click **Wireless > FlexConnect Groups** and select the FlexConnect group for a particular branch location, as shown in [Figure 15-41](#).



**Figure 15-41 FlexConnect Groups**

203734

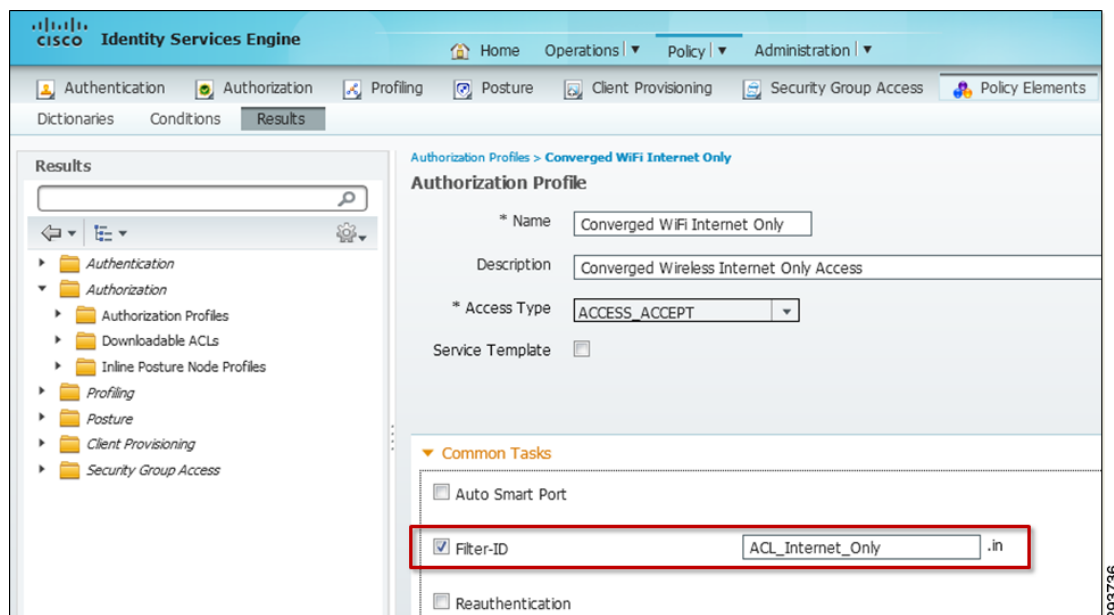
In [Figure 15-42](#), the FlexConnect group for Branch1 is applying the Branch\_ACL\_Internet\_Only ACL to endpoints connecting to VLAN 12.

**Figure 15-42 FlexConnect Group for Branch1 Internet Only**

203735

## Converged Access Branch or Campus

For devices connecting from campus or branch locations which implement a Converged Access design, the Converged WiFi Internet Only authorization profile relies on the ACL\_Internet\_Only access list, enforced by the Catalyst 3850 Series switch. [Figure 15-43](#) shows the authorization profile.

**Figure 15-43** Converged WiFi Internet Only

Cisco Catalyst 3850 Series switches (and CT5760 wireless controllers) support both named ACLs and downloadable ACLs. For the Converged Access design a named ACL is implemented, meaning that the ACL must be configured on the Catalyst 3850 switch rather than being downloaded from ISE. Using the RADIUS Filter-ID attribute-value pair, ISE instructs the WLC to apply the ACL\_Internet\_Only ACL. The following configuration example shows the contents of this ACL, as defined in the Catalyst 3850 switch.

```
ip access-list extended ACL_Internet_Only
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.225.100.10
 deny ip any 10.0.0.0 0.255.255.255
 deny ip any 172.16.0.0 0.15.255.255
 deny ip any 192.168.0.0 0.0.255.255
 permit ip any any
!
```

The access-list shown in above is similar to the access list shown in [Figure 15-38](#), but configured on a Catalyst switch instead of a wireless controller. Hence the structure of the access-list is slightly different. However the access-list specifies the following access:

- Allow DHCP access (bootpc and bootps).
- 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).
- Deny IP access to and from the rest of the internal network IP address space (10.0.0.0 /8, 172.16.0.0 /12, 192.168.0.0 /16).
- Allow access to all other addresses (Internet addresses).

**Note**

The MDM above is shown with private RFC1918 address. In practice, the MDM must be reachable from the public Internet and may not require a specific line entry in the ACL.

Again, the access list shown in this example is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

## Personal Wired Devices—Full Access

To provide full access to personal wired devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the Guest Registration portal.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the BYOD\_Full\_Access Active Directory group.

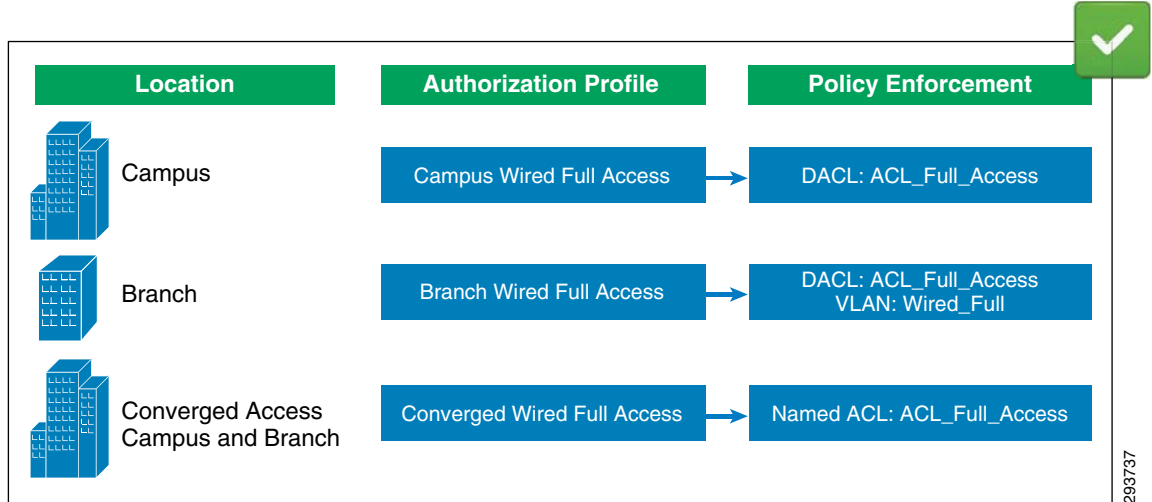
Since the wired designs presented in this design guide rely on slightly different access control mechanisms for Converged Access campuses and branches, for campuses and branches which do not implement Converged Access infrastructures, unique authorization rules are created for connections originating from each design.



### Note

For the purpose of clarity within this design guide, Converged Access branches refer to designs in which Catalyst 3850 Series switches are deployed at the access-layer of the branch network. From a wired perspective, branches which do not implement Converged Access infrastructures are branches which deploy other Catalyst access-layer switches, such as the Catalyst 3750X Series. Unless otherwise specified, these will be referred to simply as “branches” within the design guide. Similarly, Converged Access campuses refer to designs in which Catalyst 3850 Series switches are deployed at the access-layer of building distribution modules within the campus. From a wired perspective, campuses which do not implement Converged Access infrastructures are campuses which deploy other Catalyst access-layer switches, such as the Catalyst 3750X Series. Unless otherwise specified, these will be referred to simply as “campuses” within this design guide. This is in order to minimize the use of verbose phrases such as “branches which do not implement Converged Access infrastructure” and “campuses which do not implement Converged Access infrastructure”.

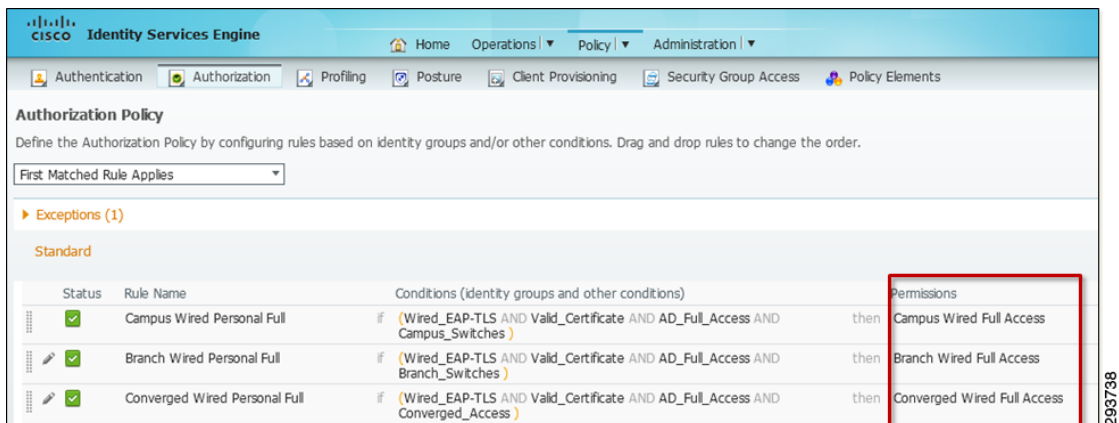
At a high level, [Figure 15-44](#) shows how different authorization profiles are selected for connections originating from different locations with different infrastructure designs. Each authorization profile in turn enforces a unique permission using VLANs, dynamic ACLs (either named or downloadable [DACL]), etc.

**Figure 15-44 Full Access Wired Enforcement****Note**

Wired assignment of Security Group Tags (SGTs) is not discussed within this version of the design guide. Hence, there is no wired policy enforcement via SGTs in Figure 15-44. Future versions of this design guide may address wired SGT assignment.

To differentiate these connections, the ISE relies on Network Device Groups to group Catalyst switches based on their location or device type. This allows a single ISE to enforce policies across different groups of devices. Each Catalyst switch needs to be added to the proper device group by clicking **Administration > Network Resources > Network Devices** and specifying the proper location or device type from the pull-down menu.

Figure 15-45 shows the details of authorization profile configured in ISE for wired devices.

**Figure 15-45 Authorization Policies for Wired Full Access**

Looking at the rules in more detail, ISE evaluates the following conditions:

- Wired\_EAP-TLS—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).

- The user belongs to a specific Active Directory group (defined as a simple condition).
- The RADIUS authentication originated from a Catalyst switch which was a member of one of the following device groups—Campus\_Switches, Branch\_Switches, or Converged\_Access (defined as a simple condition).

## Wired Simple and Compound Conditions

To improve the readability of the authorization policy, simple and compound authorization conditions were defined to group different conditions. These conditions may be reused and modified without changing every authorization rule.

Table 15-8 shows the conditions used in the authorization rules.

**Table 15-8 Simple and Compound Conditions**

<b>Wired EAP-TLS (Compound)</b>	
Wired_EAP-TLS	Radius:Service-Type Equals Framed Radius:NAS-Port-Type Equals Ethernet Network Access:EapAuthentication Equals EAP-TLS
<b>Check for Valid Certificate (Simple)</b>	
Valid_Certificate	Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name
<b>Active Directory Group (Simple)</b>	
AD_Full_Access	AD1:ExternalGroups EQUALS sdulab.com/Users/BYOD_Full_Access
AD_Partial_Access	AD1:ExternalGroups EQUALS sdulab.com/Users/BYOD_Partial_Access
AD_Domain_users	AD1:ExternalGroups EQUALS sdulab.com/Users/Domain User
<b>WLC Location or Device Type (Simple)</b>	
Campus_Switches	DEVICE:Location EQUALS All Locations#Campus_Switches
Branch_Switches	DEVICE:Location EQUALS All Locations#Branch_Switches
Converged_Access	DEVICE:Device Type EQUALS All Device Types#Converged

## Permission

When all conditions in the authorization policy rule match, the rule invokes the proper permission. The permissions can be of different forms such as an authorization profile or a standard result. In this design guide, for wired access the authorization policy is used as permission to the policy rules match.

Table 15-9 explains the permissions used for the full access for wired users.

**Table 15-9** Permissions Used for Wired Full Access

Permission name	Permission type	Purpose
Campus Wired Full Access	Authorization profile	Provides Full Access for 802.1X wired devices connecting from campus location.
Branch Wired Full Access	Authorization profile	To push a VLAN for 802.1X wired devices connecting from a branch location.
Converged Wired Full Access	Authorization profile	To push a named ACL for 802.1X wired devices connecting from either a campus or branch location with Converged Access.

## Campus Wired

Figure 15-46 shows how the Campus Wired Full Access authorization profile is defined in ISE.

**Figure 15-46** Campus Wired Full Access Authorization Profile

The screenshot displays the Cisco Identity Services Engine (ISE) configuration page for the 'Campus Wired Full Access' authorization profile. The interface includes a top navigation bar with tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The left-hand pane shows a hierarchical tree of authorization profiles, with 'Campus Wired Full Access' highlighted. The main configuration area on the right shows the following details:

- Name:** Campus Wired Full Access
- Description:** Campus Wired Full Access
- Access Type:** ACCESS\_ACCEPT
- Service Template:** (unchecked)
- Common Tasks:**
  - ☒ **DACL Name:** ACL\_Full\_Access
  - ☐ VLAN
  - ☐ Voice Domain Permission
  - ☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)
- Advanced Attributes Settings:** (partially visible)



### Note

Cisco Catalyst switches support both downloadable ACLs (DACLS) and named ACLs. This design guide shows the use of downloadable ACLs for access control of wired devices when implementing a non-Converged Access infrastructure and the use of named ACLs for access control of wired devices when implementing a Converged Access infrastructure. This is done to show the range of capabilities for access control available on Cisco IOS-based platforms. The same wired policy enforcement for Converged Access and non-Converged Access infrastructure can be achieved if the customer desires, simply by using either downloadable ACLs (DACLS) or named ACLs for both designs. Both downloadable and named ACLs have advantages and disadvantages, depending upon where they are

deployed within the network. Chapter 5, “Campus and Branch Network Design for BYOD” discusses some of these advantages and disadvantages.

The downloadable ACL (dACL), which allows all IP traffic, overrides the default-ACL configured on the switch port. The default-ACL is used as an additional preventative measure in case the downloadable ACL is not applied to the switch port for some reason. Figure 15-47 shows the dACL definition which must be configured in ISE:

**Figure 15-47** dACL Definition in ISE that Grants Full Access to the Users

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The left sidebar shows a tree view with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. Under 'Authorization', 'Downloadable ACLs' is selected. The main content area displays the configuration for a 'Downloadable ACL' named 'ACL\_Full\_Access'. The 'Description' is 'Allow all Traffic'. The 'DACL Content' field contains the text 'permit ip any any'. Below this field is a 'Check DACL Syntax' button. At the bottom of the configuration area are 'Save' and 'Reset' buttons.



**Note**

ISE 1.2 has the ability to check the dACL syntax. This feature should be utilized in order to minimize the possibility that the dACL is not applied due to a syntax error.

## Branch Wired

Figure 15-48 shows how a similar authorization profile is constructed for devices connected at a branch which does not have a Converged Access infrastructure. The authorization profile pushes VLAN information—in this case the VLAN name—along with the ACL information.

**Figure 15-48 Branch Wired Full Access Authorization Profile**

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The left sidebar displays a tree view of authorization profiles, with 'Branch Wired Full Access' selected. The main content area shows the configuration for this profile. The 'Name' field is 'Branch Wired Full Access', and the 'Description' is 'Branch Wired Full Access'. The 'Access Type' is set to 'ACCESS\_ACCEPT'. Under the 'Common Tasks' section, the 'DACI Name' is 'ACL\_Full\_Access' and 'VLAN' is checked with 'Tag ID' set to '1'. The 'ID/Name' field for the VLAN is '13'. Other options like 'Voice Domain Permission' and 'Web Redirection' are unchecked.

293740

Once this profile is downloaded to the Catalyst switch, the endpoint gets full access to the network. Figure 15-49 shows an example of the state of the port when this profile is downloaded by using the switch command **show authentication session interface Gi0/23**.

**Figure 15-49 Catalyst Switch Port**

```

Interface: GigabitEthernet0/23
MAC Address: 0050.568f.0020
IP Address: 10.11.31.14
User-Name: user1
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Group: N/A
ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4f6095bc
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 96010101000002B00155A3
Acct Session ID: 0x0000002F
Handle: 0x9E00002C

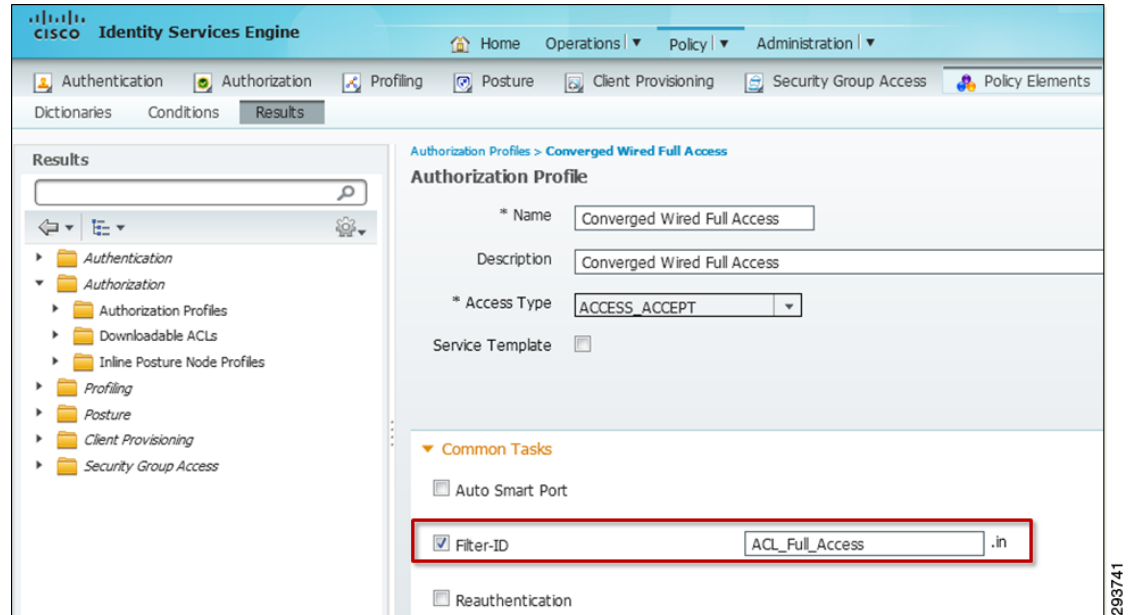
```

293854

## Converged Access Branch or Campus

Figure 15-50 shows how the Converged Wired Full Access authorization profile is defined in ISE.



**Figure 15-50** Converged Wired Full Access Authorization Profile

For the Converged Access design a named ACL is implemented, meaning that the ACL must be configured on the Catalyst 3850 switch rather than being downloaded from ISE. Using the RADIUS Filter-ID attribute-value pair, ISE instructs the converged access switch to apply the ACL\_Full\_Access ACL. The following configuration example shows the contents of this ACL, as defined in the Catalyst 3850 switch.

```
!
ip access-list extended ACL_Full_Access
 permit ip any any
!
```

This ACL is used to override the default-ACL configured on the switch port. The default-ACL is used as an additional preventative measure in case ACL\_Full\_Access is not configured on the switch.

## Personal Wired Devices—Partial Access

Partial Access grants access to corporate resources, in addition to Internet access. As mentioned in [Personal Wireless Devices—Partial Access](#), once a device authenticates to ISE, an authorization profile is applied. For wired devices, the authorization profile is applied to the access layer switch.

To provide partial access to personal wired devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the Guest Registration portal.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the AD\_Partial\_Access Active Directory group.

At a high level, [Figure 15-51](#) shows how different authorization profiles are selected for devices coming from different locations with different wired infrastructure designs. Each authorization profile in turn enforces a unique permission using VLANs, dynamic ACLs (either named or downloadable [DACL]), etc.

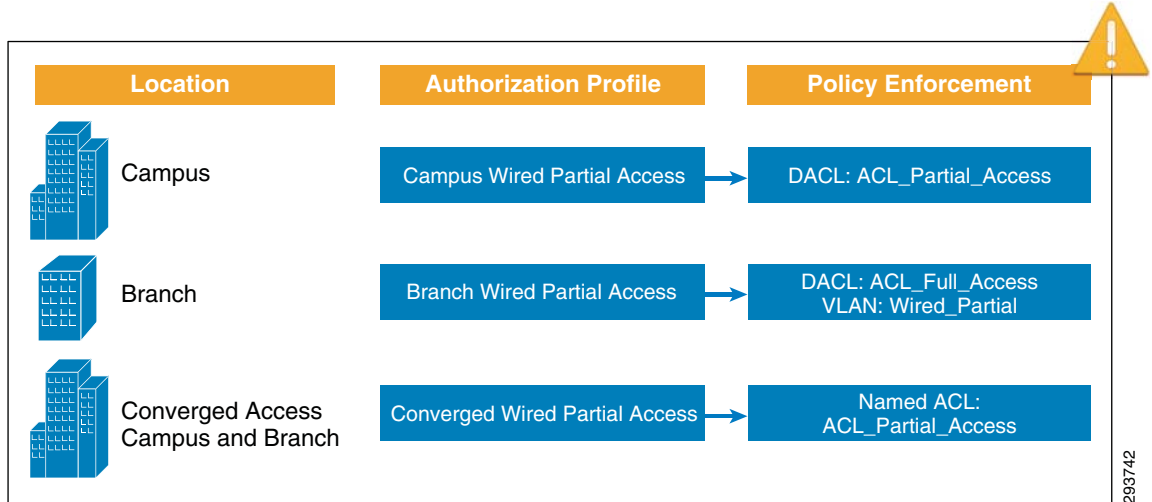
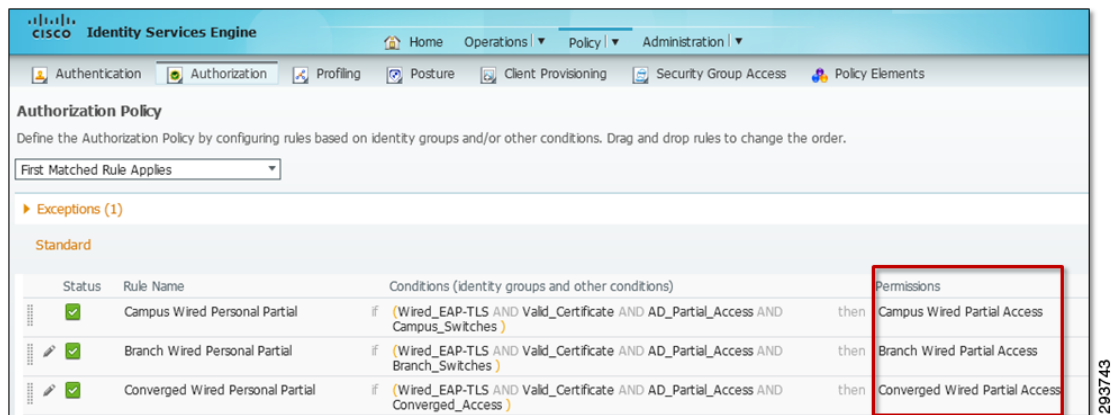
**Figure 15-51** *Wired Partial Access Enforcement*

Figure 15-52 shows the details of authorization profile configured in ISE for wired devices.

**Figure 15-52** *Authorization Policies for Wired Partial Access*

Looking at the rules in more detail, ISE evaluates the following conditions:

- **Wired\_EAP-TLS**—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).
- The user belongs to a specific Active Directory group (defined as a simple condition).
- The RADIUS authentication originated from a Catalyst switch which was a member of one of the following device groups—Campus\_Switches, Branch\_Switches, or Converged\_Access (defined as a simple condition).

[Wired Simple and Compound Conditions](#) explains the different conditions used in the rules.

## Permissions

When all conditions in the authorization policy rule match, the rule invokes the proper permission. The permissions can be of different forms such as an authorization profile or a standard result. In this design guide, for wired access the authorization policy is used as permission to the policy rules match.

Table 15-10 explains the permissions used for the partial access for wired users.

**Table 15-10 Permissions Used for Wired Partial Access**

Permission name	Permission type	Purpose
Campus Wired Partial Access	Authorization profile	To push a dACL for 802.1X wired devices connecting from campus location.
Branch Wired Partial Access	Authorization profile	To push a VLAN for 802.1X wired devices connecting from a branch location.
Converged Wired Partial Access	Authorization profile	To push a named ACL for 802.1X wired devices connecting from either a campus or branch location with Converged Access.

## Campus Wired

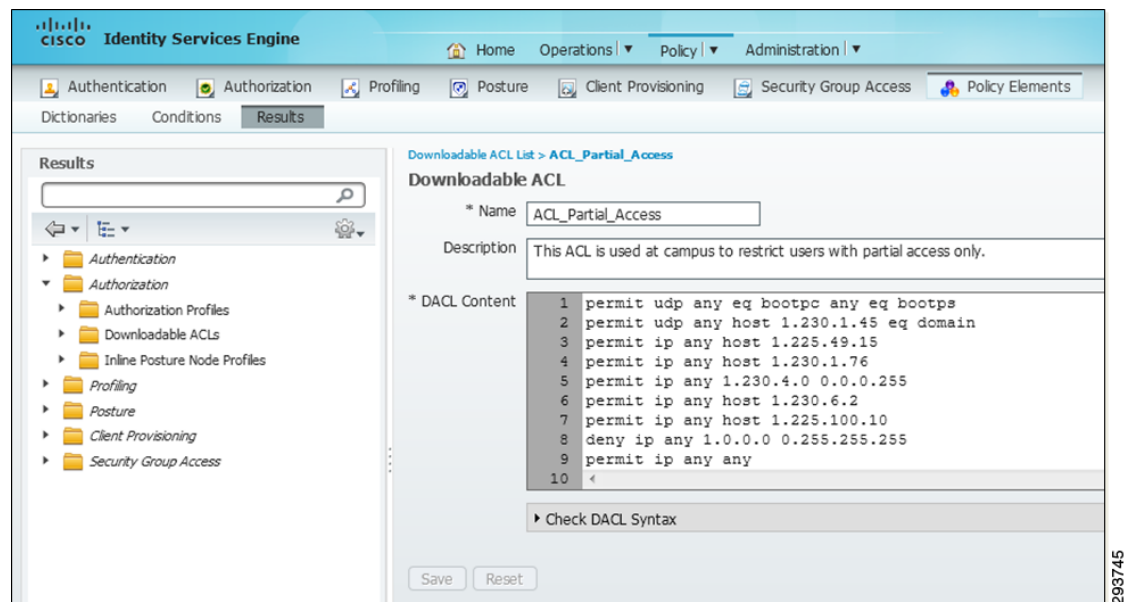
For devices connecting from a campus location, the Campus Wired Partial Access authorization uses a DACL named ACL\_Partial\_Access enforced by the access layer switch, as shown in Figure 15-53.

**Figure 15-53 Campus Wired Partial Access**

The screenshot displays the Cisco Identity Services Engine (ISE) configuration page for the 'Campus Wired Partial Access' authorization profile. The left sidebar shows the navigation tree with 'Authorization' > 'Authorization Profiles' selected. The main content area shows the configuration for the 'Campus Wired Partial Access' profile. The 'Common Tasks' section is expanded, showing the 'DACL Name' field set to 'ACL\_Partial\_Access'. The 'Advanced Attributes Settings' section shows a list of attributes with 'Access Type' set to 'ACCESS\_ACCEPT' and 'DACL' set to 'ACL\_Partial\_Access'. The 'Attributes Details' section shows the final configuration: 'Access Type = ACCESS\_ACCEPT' and 'DACL = ACL\_Partial\_Access'.

The dACL overrides the default-ACL configured on the switch. [Figure 15-54](#) shows an example of this ACL, which is configured within ISE.

**Figure 15-54** *ACL\_Partial\_Access within ISE*



The above ACL specifies the following access:

- Allow DHCP access (bootpc and bootps).
- Allow DNS access to 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 specific subnet (10.230.4.0 /24).
- Allow IP access to and from specific servers (10.230.6.2 and 10.225.100.10).
- Deny IP access to and from internal network address space (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
- Allow access to and from all other subnets (Internet access).

## Branch Wired

For devices connecting from a branch location, the Branch Wired Partial Access authorization pushes a VLAN assignment along with a downloadable ACL.

[Figure 15-55](#) shows the details of the authorization profile configured in ISE.

**Figure 15-55** Branch Wired Partial Access Authorization Profile

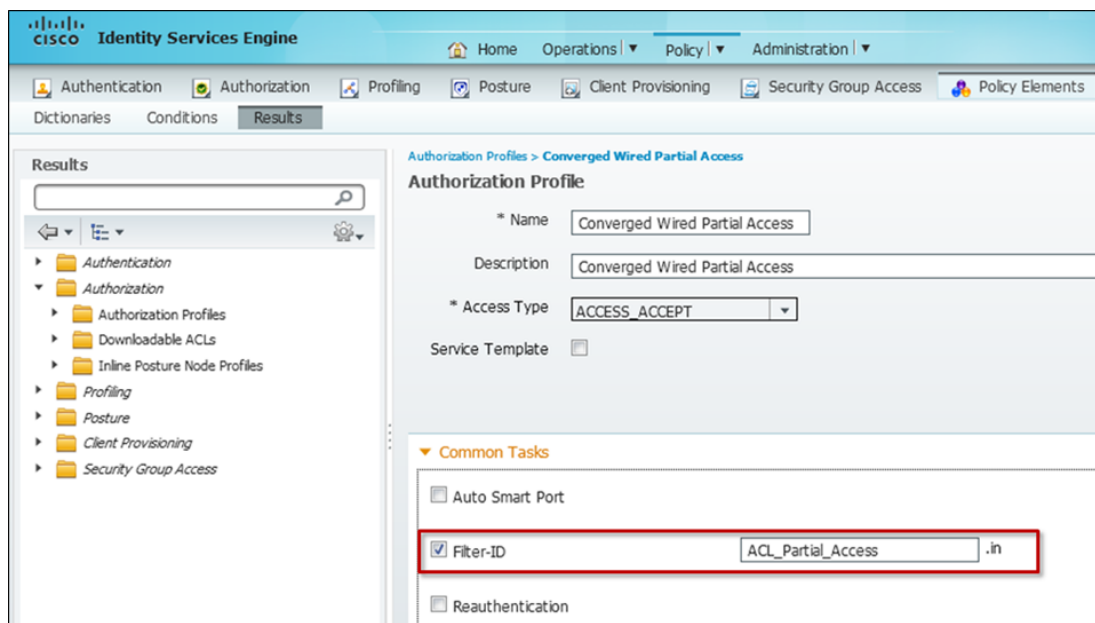
The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Policy' tab is active, showing sub-tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Results' sub-tab is selected. On the left, a tree view under 'Results' shows 'Authorization Profiles' expanded, with 'Branch Wired Partial Access' highlighted. The main configuration area for the 'Branch Wired Partial Access' profile is shown. It includes fields for 'Name' (Branch Wired Partial Access), 'Description' (Branch Wired Partial Access), 'Access Type' (ACCESS\_ACCEPT), and 'Service Template' (unchecked). Under the 'Common Tasks' section, 'DACL Name' is set to 'ACL\_Full\_Access' and 'VLAN' is checked, with 'Tag ID' 1 and 'ID/Name' 14. Other options like 'Voice Domain Permission' and 'Web Redirection' are unchecked.

The DACL allows all IP traffic, so that the traffic initiated by the host reaches the branch router where the router-ACL is applied.

See [VLAN Design at Branch Locations](#) in [Chapter 11, “BYOD Wired Infrastructure Design”](#) for details regarding how this assignment of VLAN 14 is given full access for a branch which does not implement a Converged Access infrastructure.

## Converged Access Branch and Campus

[Figure 15-56](#) shows how the Converge Wired Partial Access authorization profile is defined in ISE.

**Figure 15-56** Converged Wired Partial Access Authorization Profile

For the Converged Access design a named ACL is implemented. Using the RADIUS Filter-ID attribute-value pair, ISE instructs the converged access switch to apply the ACL\_Partial\_Access ACL. This is the same ACL discussed for converged access infrastructure in [Personal Wireless Devices—Partial Access](#). For wired devices, the ACL is used to override the default-ACL configured on the switch port. The default-ACL is used as an additional preventative measure in case ACL\_Partial\_Access is not configured on the switch.

## Personal Wired Devices—Internet Only Access

To provide Internet Only access to personal devices, the Cisco ISE verifies the following:

- The employee has completed the on-boarding process through the Guest Registration portal.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.
- The user is a member of the Domain Users Active Directory group.

At a high level, [Figure 15-57](#) shows how different authorization profiles are selected for devices coming from different locations with different wired infrastructure designs. Each authorization profile in turn enforces a unique permission using VLANs, dynamic ACLs (either named or downloadable [DACL]), etc.

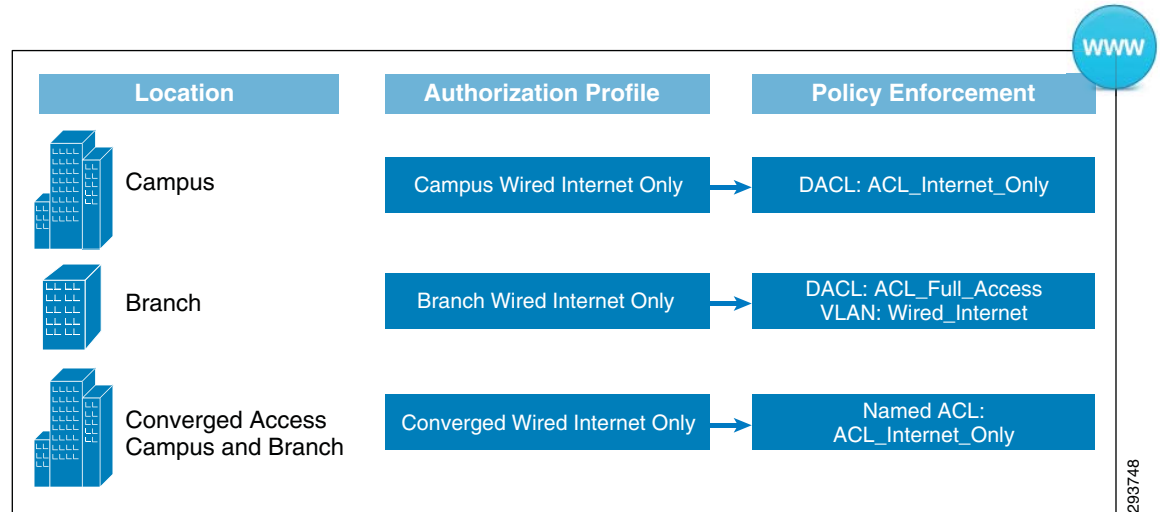
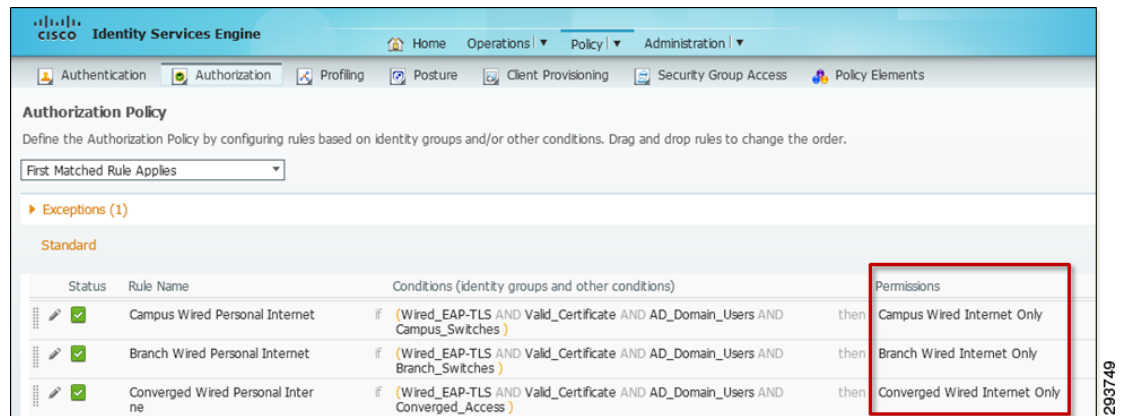
**Figure 15-57** *Wired Internet Only Access Enforcement*

Figure 15-58 highlights the authorization policy to grant Internet Only access to personal wired devices.

**Figure 15-58** *Authorization Policies for Wired Internet Only Access*

Looking at the rules in more detail, ISE evaluates the following conditions:

- **Wired\_EAP-TLS**—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).
- The user belongs to a specific Active Directory group (defined as a simple condition).
- The RADIUS authentication originated from a Catalyst switch which was a member of one of the following device groups—Campus\_Switches, Branch\_Switches, or Converged\_Access (defined as a simple condition).

[Wired Simple and Compound Conditions](#) explains the different conditions used in the rules.

## Permissions

When all conditions in the authorization policy rule match, the rule invokes the proper permission. The permissions can be of different forms such as an authorization profile or a standard result. In this design guide, for wired access the authorization policy is used as permission to the policy rules match.

[Table 15-11](#) explains the permissions used for Internet access.

**Table 15-11** *Permissions Used for Wired Internet Access*

Permission name	Permission type	Purpose
Campus Wired Internet Only	Authorization profile	To push a dACL for 802.1X wired devices connecting from a campus location.
Branch Wired Internet Only	Authorization profile	To push a VLAN for 802.1X wired devices connecting from a branch location.
Converged Wired Internet Only	Authorization profile	To push a named ACL for 802.1X wired devices connecting from either a campus or branch location with Converged Access

## Wired Campus

For devices connecting from a campus location, the Campus Wired Internet Only authorization profile uses the DACL named ACL\_Internet\_Only, which is pushed to the access layer switch port.

[Figure 15-59](#) shows the Authorization profile.



**Figure 15-59** *Campus Wired Internet Only Authorization Profile*

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The left sidebar shows a tree view with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. The main content area is titled 'Authorization Profiles > Campus Wired Internet Only'. It shows the configuration for an 'Authorization Profile' with the following details:

- Name:** Campus Wired Internet Only
- Description:** (empty field)
- Access Type:** ACCESS\_ACCEPT
- Service Template:** (unchecked)
- Common Tasks:**
  - ☒ **DACL Name:** ACL\_Internet\_Only
  - ☐ VLAN
  - ☐ Voice Domain Permission
  - ☐ Web Redirection (CWA, DRW, MDM, NSP, Posture)
- Advanced Attributes Settings:** (empty)
- Attributes Details:**
  - Access Type = ACCESS\_ACCEPT
  - DACL = ACL\_Internet\_Only

The DACL overrides the default-ACL configured on the switch. Figure 15-60 shows an example of this ACL, which is configured within ISE.

**Figure 15-60** *ACL\_Internet\_Only DACL*

The screenshot displays the Cisco Identity Services Engine (ISE) web interface for configuring a 'Downloadable ACL'. The left sidebar shows a tree view with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. The main content area is titled 'Downloadable ACL List > ACL\_Internet\_Only'. It shows the configuration for a 'Downloadable ACL' with the following details:

- Name:** ACL\_Internet\_Only
- Description:** This ACL is used at campus to restrict access for Internet Only
- DACL Content:**

```

1 permit udp any eq bootpc any eq bootps
2 permit udp any host 1.230.1.45 eq domain
3 permit ip any host 1.225.49.15
4 permit ip any host 1.230.1.76
5 permit ip any host 1.225.100.10
6 deny ip any 1.0.0.0 0.255.255.255
7 permit ip any any
8
9
10

```
- Check DACL Syntax:** (button)
- Buttons:** Save, Reset

The access list specifies the following access:

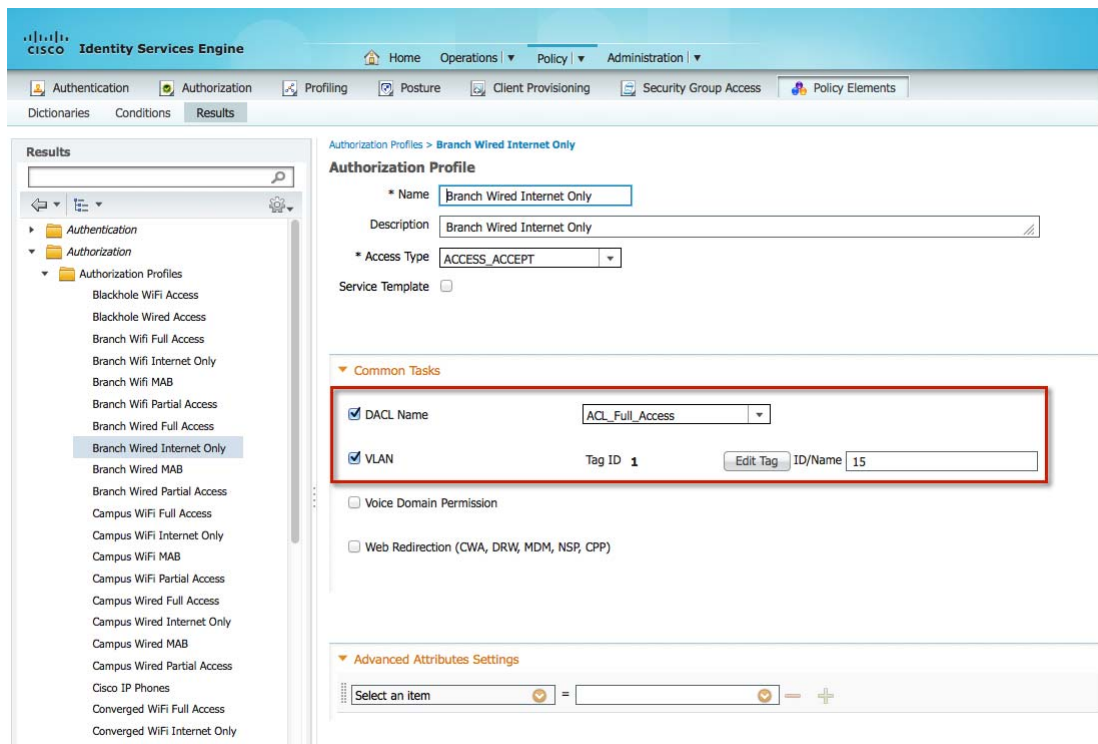
- Allow DHCP access (bootpc and bootps).
- Allow DNS access to the DNS server (10.230.1.45).
- Allow IP access to and from the ISE Server (10.225.49.15).
- Deny IP access to and from internal network address space (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
- Allow access to and from all other subnets (Internet access).

This access list is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

## Branch Wired

For devices connecting from a branch location, the Branch Wired Internet Only authorization pushes a VLAN assignment along with a downloadable ACL. [Figure 15-61](#) illustrates the Branch Wired Internet\_Only authorization profile, used to grant Internet\_Only access to personal devices connecting from the branch.

**Figure 15-61** Branch Wired Internet Only Authorization Profile



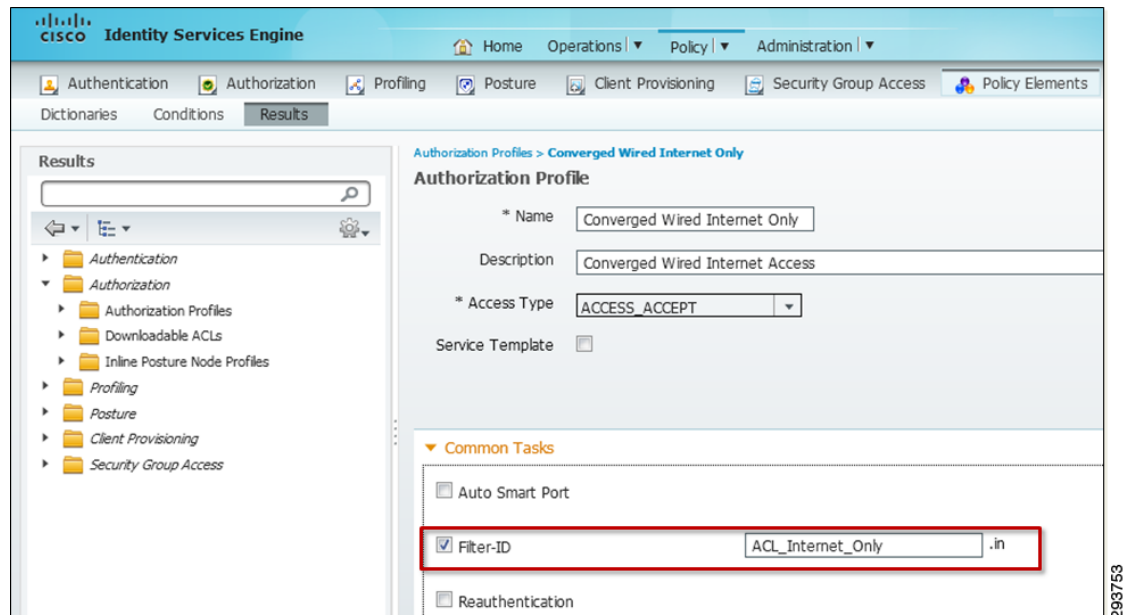
The ACL\_Full\_Access DACL is pushed to the access-layer switch to override the default-ACL on the port and allow all IP traffic to flow up to the branch router.

See [VLAN Design at Branch Locations](#) in [Chapter 11, “BYOD Wired Infrastructure Design”](#) for details regarding how this assignment of VLAN 15 is given full access for a branch which does not implement a Converged Access infrastructure.

## Converged Access Branch and Campus

Figure 15-62 shows how the Converge Wired Internet Only authorization profile is defined in ISE.

**Figure 15-62** Converged Wired Internet Only Authorization Profile



For the Converged Access design a named ACL is implemented. Using the RADIUS Filter-ID attribute-value pair, ISE instructs the converged access switch to apply the ACL\_Internet\_Only ACL. This is the same ACL discussed for converged access infrastructure in [Personal Wireless Devices—Internet Only Access](#). For wired devices, the ACL is used to override the default-ACL configured on the switch port. The default-ACL is used as an additional preventative measure in case ACL\_Internet\_Only is not configured on the switch.

## Android Devices—Deny Access

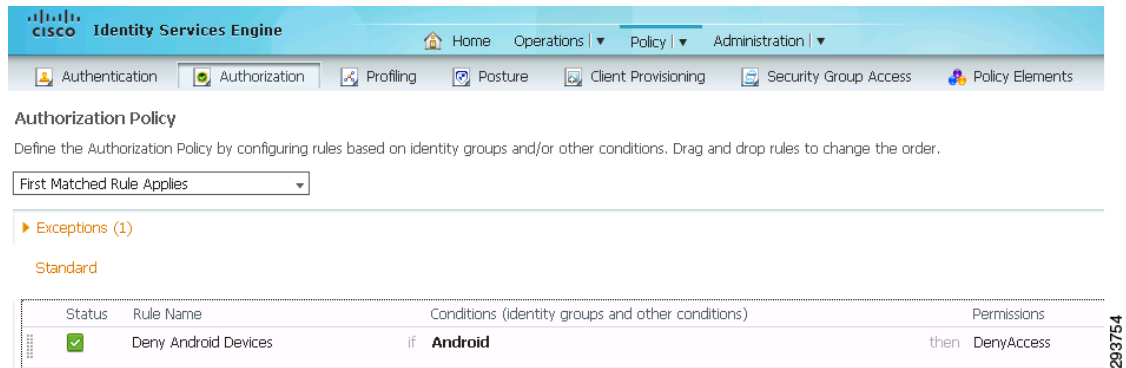
Rather than allowing differentiated access to the network which was depicted in the previous use cases, this use case discusses on how to deny access permission for some BYOD devices from connecting to the network. For example, some organizations may decide to have a more restrictive BYOD environment and grant access only to a specific type of device (e.g., Android, Apple iOS, etc.).

This example focuses on denying access to Android devices, relying on the profiling capabilities of ISE.

To deny access to Android devices, the Cisco ISE verifies the following:

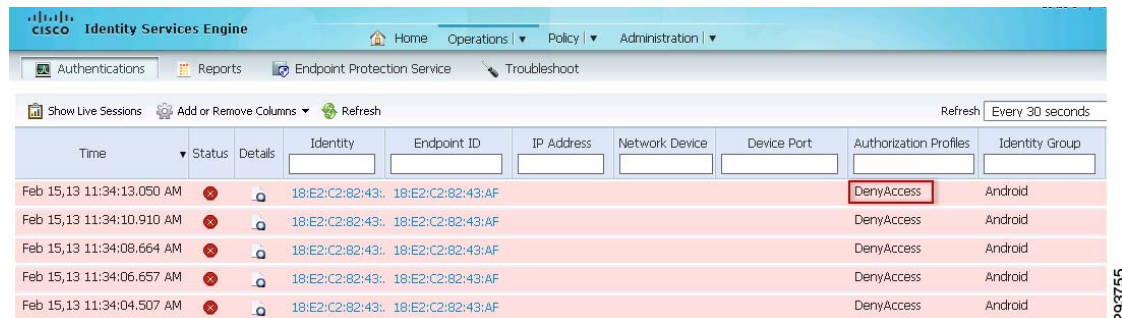
- The employee attempts to connect to the network.
- The ISE profiler identifies the device type.
- If the device type is Android, deny access.

To configure the authorization rules in ISE, click **Policy > Authorization**. Figure 15-63 highlights the authorization policy to deny access to Android devices.

**Figure 15-63 Deny Android Devices**

The DenyAccess authorization profile is used to enforce the permissions and deny access to Android devices. The DenyAccess profile is a standard ISE profile and cannot be edited. This reserved profile cannot be edited but may be found under **Policy > Results > Authorization Profiles**.

Figure 15-64 shows an entry from ISE's log, highlighting the fact that the device has been profiled as an Android device and the DenyAccess authorization rule has been enforced.

**Figure 15-64 DenyAccess**

## ISE Authorization Policy

For reference purposes, the complete authorization policy used during validation is shown in Figure 15-65. The figure highlights the following sections:

1. Used for blacklisting lost or stolen devices.
2. On-boarding and MDM registration/remediation (required for the advanced use case).
3. Wireless devices connecting from an access point in a SGT\_Enabled location.
4. Wireless devices connecting from an access point in the campus or branch locations.
5. Wired devices connecting from a campus or branch locations.
6. Wired and Wireless devices connecting from a converged location.
7. Guest and Basic Access.

Figure 15-65 Complete 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
1	Wireless Black List Default ISE	Blacklist AND Wireless_Access	then Blackhole WiFi Access
	Wired Black List Default	Blacklist AND Wired_Access	then Blackhole Wired Access
	MDM Enrollment	(Wireless_EAP-TLS AND ISE_Registered AND MDM_UnRegistered AND MDM_Managed AND MDM_Operational)	then Internet Until MDM
	Dual SSID Provisioning	(Wireless_MAB AND Provisioning_WLAN)	then Wireless CWA
2	Single SSID Provisioning	(Wireless_PEAP AND Employee_WLAN)	then Wireless NSP
	Remediate Non ISE Compliant	(Wireless_EAP-TLS AND ISE_NonCompliant AND MDM_Managed AND MDM_Operational)	then ISE Quarantine
	Remediate Non MDM Compliant	(Wireless_EAP-TLS AND MDM_NonCompliant AND MDM_Managed AND MDM_Operational)	then MDM Quarantine
	SGTCampus Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller)	then SGT10_Campus_Corp AND PermitAccess
	SGTCampus Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Full_Access)	then SGT11_Campus_Pers_Full AND PermitAccess
3	SGTCampus Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Partial_Access)	then SGT12_Campus_Pers_Partial AND PermitAccess
	SGTCampus Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Domain_Users)	then Campus WiFi Internet Only
	Campus Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Campus_Controller)	then Campus WiFi Full Access
	Campus Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND Campus_Controller AND AD_Full_Access)	then Campus WiFi Full Access
	Campus Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Campus_Controller)	then Campus WiFi Partial Access
4	Campus Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Campus_Controller)	then Campus WiFi Internet Only
	Branch Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Branch_Controller)	then Branch WiFi Full Access
	Branch Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND Branch_Controller AND AD_Full_Access)	then Branch WiFi Full Access
	Branch Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Branch_Controller)	then Branch WiFi Partial Access
	Branch Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Branch_Controller)	then Branch WiFi Internet Only
	Campus Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Campus_Switches)	then Campus Wired Full Access
	Campus Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND Campus_Switches AND AD_Full_Access)	then Campus Wired Full Access
	Campus Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Campus_Switches)	then Campus Wired Partial Access
	Campus Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Campus_Switches)	then Campus Wired Internet Only
	Branch Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Branch_Switches)	then Branch Wired Full Access
	Branch Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Branch_Switches)	then Branch Wired Full Access
	Branch Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Branch_Switches)	then Branch Wired Partial Access
	Branch Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Branch_Switches)	then Branch Wired Internet Only
	Converged Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Converged_Access)	then Converged WiFi Full Access
	Converged Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Converged_Access)	then Converged WiFi Full Access
	Converged Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Converged_Access)	then Converged WiFi Partial Access
	Converged Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Converged_Access)	then Converged WiFi Internet Only
6	Converged Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Converged_Access)	then Converged Wired Full Access
	Converged Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Converged_Access)	then Converged Wired Full Access
	Converged Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Converged_Access)	then Converged Wired Partial Access
	Converged Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Converged_Access)	then Converged Wired Internet Only
7	Wifi Guest	(WLC_Web_Authentication AND Guest_WLAN)	then PermitAccess
	Wifi Basic Access	(Wireless_PEAP AND Personal_Device_WLAN)	then PermitAccess

293756







## BYOD Limited Use Case—Corporate Devices

---

**Revised: March 6, 2014**

**What's New:** In the previous version of the BYOD CVD, the authorization policies for a user accessing the network with a corporate device and enforced with the security group tags supported only a Centralized Unified Wireless Network (CUWN) architecture with CT-5508 as a controller.

In this version of the BYOD CVD, the authorization policies for a user accessing the network with a corporate device and enforced with security group tags support:

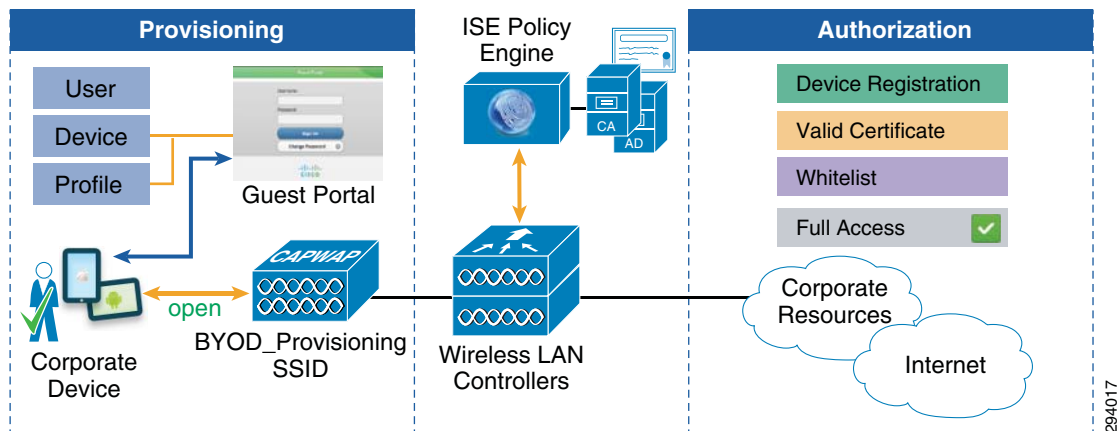
- CUWN architecture using CT-5508 and CT-5760 controllers
- Converged Access wireless design using Catalyst 3850

This chapter discusses design considerations and the construction of policy rules for providing network access to corporate devices, as well as the security policies enforced by the Cisco ISE. A corporate device is a corporate asset that is provided by the organization and has the approved configuration profiles and digital certificate to access the network. ISE allows the employee to on-board their corporate devices in a similar way personal devices are on-boarded, as discussed in [Chapter 15, “BYOD Enhanced Use Case—Personal and Corporate Devices.”](#)

Cisco ISE provides many ways to enforce security policies and determines what network resources each device is allowed to access. This chapter focuses on allowing full access to corporate devices. The ISE feature set is extremely flexible to meet diverse business requirements. The goal of this chapter is to highlight this flexibility of ISE and explain the steps to restrict access for corporate devices.

[Figure 16-1](#) shows the different authorization rules used by ISE to grant full access to corporate devices. Different network components play a role in this process, including the wireless infrastructure, Active Directory, a CA server, etc.

Figure 16-1 Provisioning Corporate Devices



## Whitelist Identity Group

An identity group is a logical list used to group endpoints according to their profiles and is an efficient way for ISE to enforce different permissions to different types of devices.

For this design guide, the Whitelist identity group was created for the purpose of uniquely identifying corporate devices. This identity group maintains a list of devices owned by the corporation. The Whitelist is manually updated by the IT administrator and contains the MAC addresses of devices that are granted full access. The assumption is that IT has added the devices to the Whitelist in advance.

The identity group provides an additional check when enforcing authorization rules. Endpoints may be moved to other identity groups, such as the Whitelist identity group or the Blacklist identity group, used when a device is lost or stolen. [Chapter 22, “Managing a Lost or Stolen Device”](#) has more details on the Blacklist identity group.

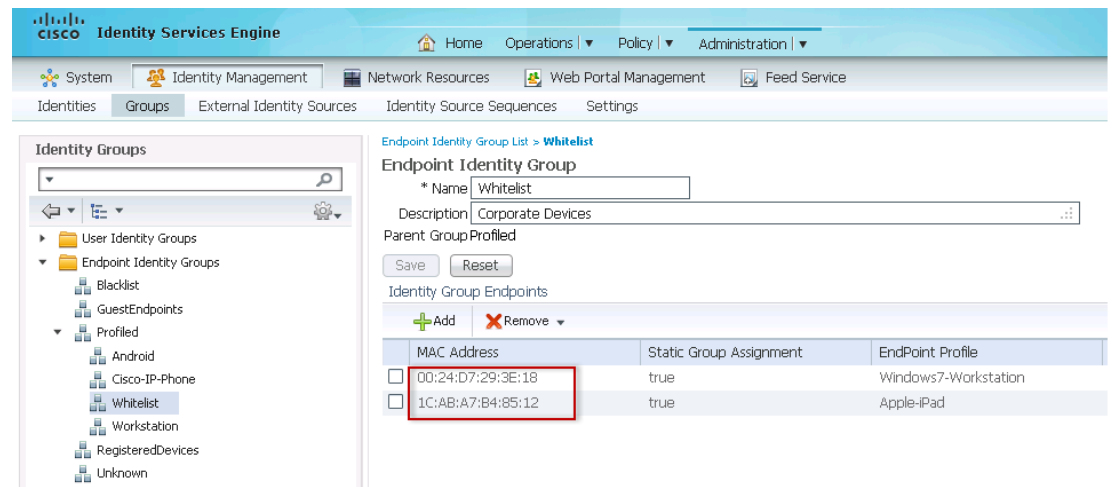


### Note

Endpoints can only be members of one identity group at a time.

To update an endpoint's identity group, click **Administration > Groups > Endpoint Identity Groups**. [Figure 16-2](#) shows endpoints as members of the Whitelist identity group.



**Figure 16-2** *Whitelist Identity Group*

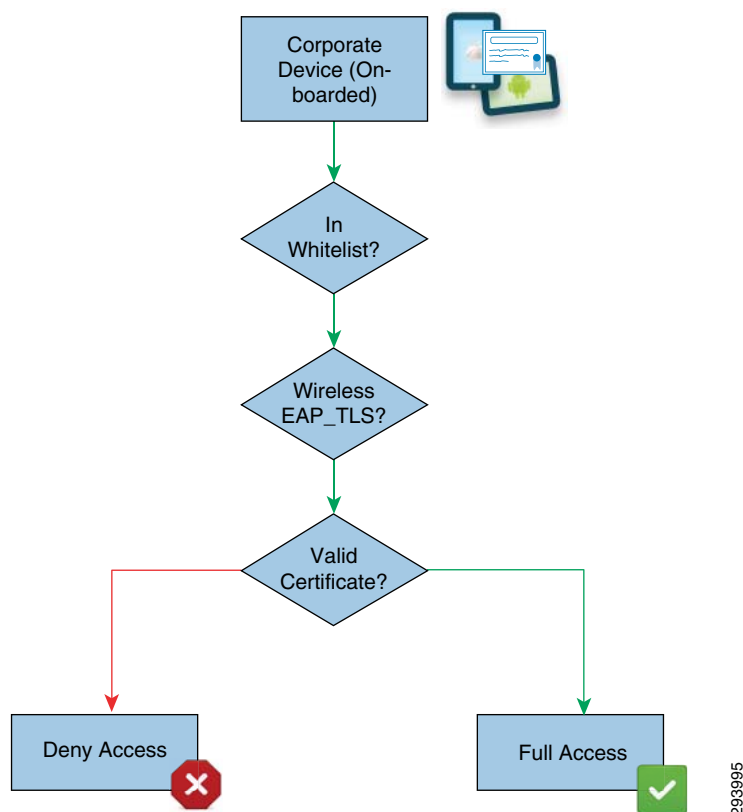
An Active Directory group could be used as an additional check, but for the purpose of this design guide the Whitelist identity group identifies a device as a corporate device. This model could easily be expanded to include AD groups to enforce additional policy requirements.

Figure 16-3 highlights the policy tested in this chapter, along with the different requirements and permissions. This policies, along with detailed configurations, is explained in this chapter.

**Figure 16-3** *Access Policies and Permissions*

Policy	Identity Group	Location	Permission
Corporate Owned	Whitelist	Campus/Branch/ <u>SGT</u>	Full

This chapter assumes that after employees have on-boarded their devices, they'll connect to the BYOD\_Employee. Figure 16-4 highlights the connectivity flow granting full access to corporate devices. If the device has been on-boarded, it belongs to the Whitelist identity group and has a digital certificate, the device is granted full access.

**Figure 16-4 Corporate Device BYOD Access**

## Policy Enforcement for Security Group Access

A new addition to this CVD is the use of Security Group Tags in creating role-based policies in addition to ACLs to enforce policies for campus wireless users. Enforcing policies for SGA in BYOD architecture consist of three main components:

- Defining tags for the endpoints and the destination servers.
- Defining and implementing the Security Group ACL in the switching infrastructure.
- Defining firewall policies based on Security Group Tags if Security Group Firewall is implemented.

Depending on the SGA deployment scenario followed, the Security Group Egress Policy can be defined at the ISE and dynamically pushed to Catalyst 6500 infrastructure switches and the Nexus Data Center switches as Security Group ACLs (SGACL) or configured at the ASA Firewall as a SGT-based policy. These two choices are discussed in [Chapter 23, “BYOD Policy Enforcement Using Security Group Access”](#) as two different deployment scenarios.

## Security Group Access Tags

The basic idea of Security Group Access is to define the tags for source and destination traffic flows and specify what source tags are able to reach other destination tags. For example, are devices tagged with an SGT 10 allowed to communicate with a server tagged with an SGT 40? This flow is either allowed or blocked at the enforcement point.

Using this tagging concept, unique tags have been defined for different types of source traffic generated by the endpoints. As explained in [Chapter 12, “Security Group Access for BYOD,”](#) unique permissions are established for personal and corporate devices and unique tags have been defined for each use case.

[Table 16-1](#) illustrates how tags are assigned to different devices.

**Table 16-1 Source Tags**

Device Type	Tag
Corporate device with Full Access	SGT 10
Personal device with Full Access	SGT 11
Personal device with Partial Access	SGT 12

Similarly, the destination servers also need to be associated with a particular tag. [Table 16-2](#) illustrates how, based on their role, servers are assigned with a different tag.

**Table 16-2 Destination Tags**

Destination Server	Tag
Open Access	SGT 40
Corporate Server	SGT 50

## Security Group ACL

After defining the source and destination tags, the next logical step is to define the egress policy that establishes the permissions for traffic between those tags. [Table 16-3](#) illustrates the egress policy as an enforcement matrix.

**Table 16-3 Enforcement Matrix**

	Device Type	SGT 40	SGT 50
SGT 10	Corporate device with Full Access	Yes	Yes
SGT 11	Personal device with Full Access	Yes	Yes
SGT 12	Personal device with Partial Access	Yes	No

As shown in [Table 16-3](#), corporate or personal devices granted full access will be allowed to reach servers that have been tagged with SGT 40 or SGT 50. Similarly, a personal device with a partial access is only allowed to connect with a server tagged with SGT 40.

The implementation of the SGACL depends upon the type of the deployment scenario. For the deployment scenario where Nexus is the enforcement point, the SGACL is designed in ISE and pushed to the Nexus switch. When the deployment scenario is using ASA as the enforcement point, then an SGT-based access rule is configured manually on the ASA firewall.

## Authorization Polices for SGT

Based on policy matches and authorization profiles, the ISE assigns an SGT to campus wireless devices. [Centralized Campus—Policy Enforcement using TrustSec](#) in [Chapter 9, “BYOD Wireless Infrastructure Design”](#) provides information about the criteria used to determine when, based on the network device type of the wireless controller defined in ISE, an ACL versus an SGT should be returned upon successful authorization.

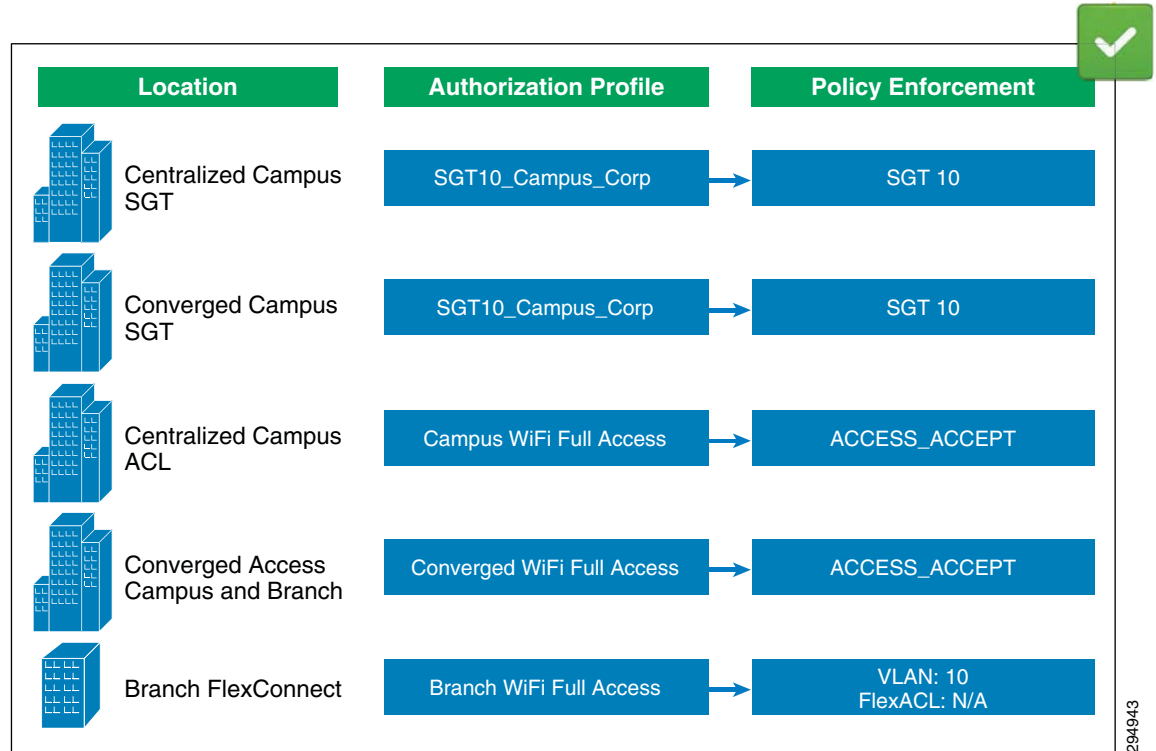
For the destination server tags, the configuration is done manually at the data center switch and the actual enforcement happens based on the deployment scenario. For more information about configuring tags for servers and the ASA, see [Chapter 23, “BYOD Policy Enforcement Using Security Group Access.”](#)

## Corporate Devices—Full Access

To provide full access to corporate devices, the Cisco ISE verifies the following:

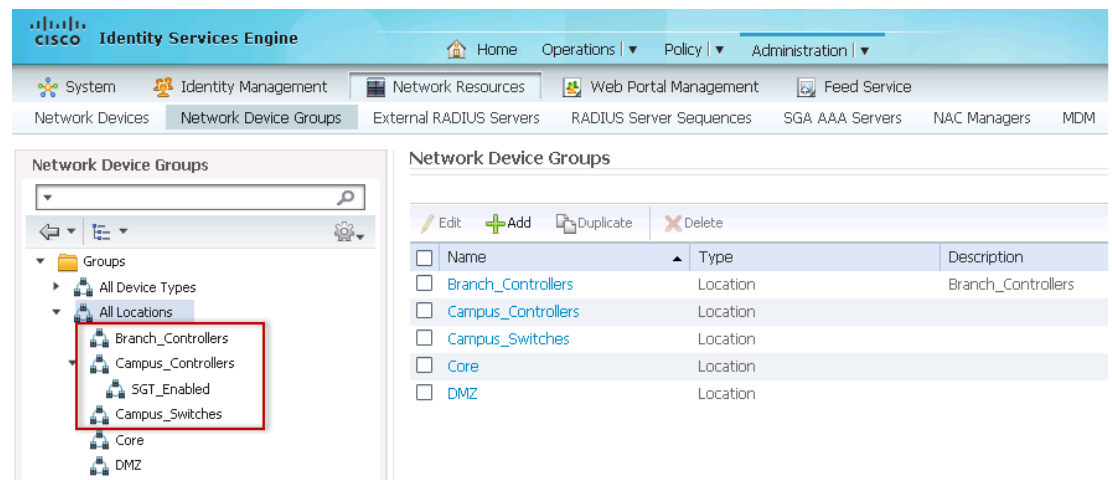
- The device has been on-boarded and has the right certificate and profile configurations.
- The device has been added to the Whitelist identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate.
- The connection originated using EAP-TLS authentication.

Since the wireless designs presented in this design guide rely on different WLCs for FlexConnect branches, Centralized Controller campuses, and Converged Access campuses and branches, unique authorization rules are created for connections originating from each design. At a high level, [Figure 16-5](#) shows how different authorization profiles are selected for connections originating from different locations with different wireless designs. Each authorization profile in turn enforces a unique permission using VLANs, SGTs, dynamic ACLs (either named or downloadable [DACL]), FlexConnect ACLs, etc.

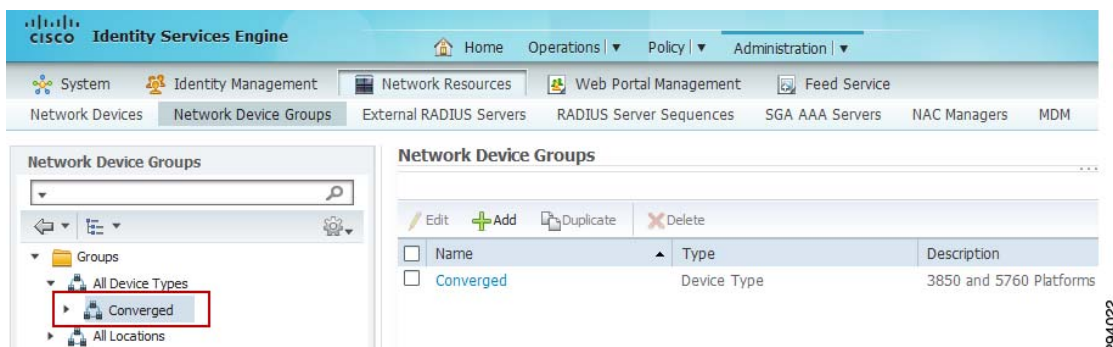
**Figure 16-5 Full Access Enforcement**

To differentiate these connections, the ISE relies on Network Device Groups to group WLCs based on their location or device type. This allows a single ISE to enforce policies across different groups of devices.

Figure 16-6 shows the different locations created for branch and campus devices.

**Figure 16-6 ISE Device Groups—Locations**

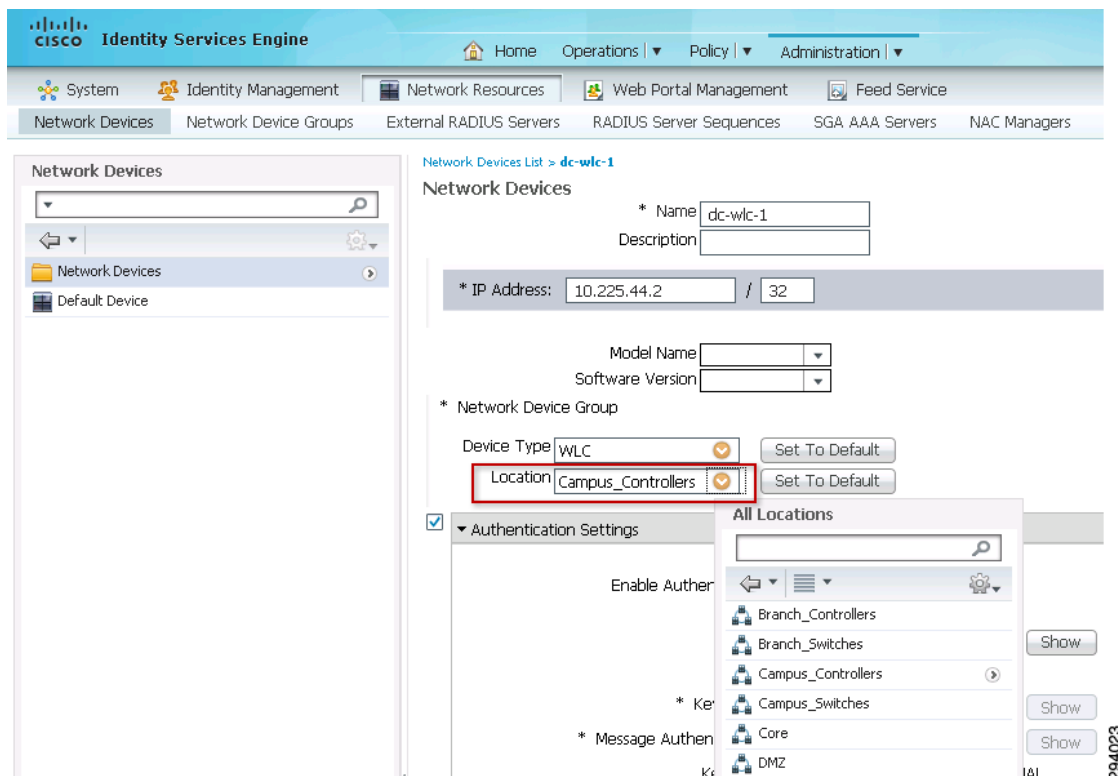
Similarly, Figure 16-7 shows a device type called Converged which can be created for Catalyst 3850 Series switches and CT5760 wireless controllers and used in the authorization policy.

**Figure 16-7 ISE Device Groups—Device Types****Note**

One of the reasons a device type is used instead of a location for Converged Access designs is that the same authorization policy rules are used for Converged Access branch and campus designs within this design guide. Hence location—campus versus branch—is not particularly relevant from a Cisco ISE perspective to converged access designs presented in this design guide.

Each Wireless LAN Controller needs to be added to the proper device group by clicking **Administration > Network Resources > Network Devices** and specifying the proper location or device type from the pull-down menu.

Figure 16-8 shows how the dc-wlc-1 belongs to the Campus\_Controllers location.

**Figure 16-8 Campus Controller**

Wireless LAN Controllers implementing a centralized (Local Mode) campus wireless design are assigned to the Campus\_Controllers group.

To configure the authorization rules in ISE, click **Policy > Authorization**. Figure 16-9 highlights the authorization policy to grant full access to corporate devices.

**Figure 16-9 Authorization Policies for Full Access**

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Centralized Campus SGT	if <b>Whitelist</b> AND <b>Wireless_EAP-TLS</b> AND <b>Valid_Certificate</b> AND <b>Campus_SGT_Enabled</b>	then SGT10_Campus_Corp AND PermitAccess
✓	SGT WIFI Corporate Full	if <b>Whitelist</b> AND <b>Wireless_EAP-TLS</b> AND <b>Valid_Certificate</b> AND <b>SGT_Converged_Controller</b>	then SGT10_Campus_Corp AND PermitAccess
✓	Campus WIFI Corporate Full	if <b>Whitelist</b> AND <b>Wireless_EAP-TLS</b> AND <b>Valid_Certificate</b> AND <b>Campus_Controller</b>	then Campus WIFI Full Access
✓	Converged WIFI Corporate Full	if <b>Whitelist</b> AND <b>Wireless_EAP-TLS</b> AND <b>Valid_Certificate</b> AND <b>Converged_Access</b>	then Converged WIFI Full Access
✓	Branch WIFI Corporate Full	if <b>Whitelist</b> AND <b>Wireless_EAP-TLS</b> AND <b>Valid_Certificate</b> AND <b>Branch_Controller</b>	then Branch WIFI Full Access

Looking at the first rule in more detail, ISE evaluates these conditions:

- **Whitelist**—The endpoint has been added by an IT Administrator to the Whitelist identity group.
- **Wireless\_EAP-TLS**—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).
- The RADIUS authentication originated from a wireless controller which was a member of one of the following device groups: Campus\_Controller, SGT\_Controller, Branch\_Controller, or Converged\_Access (defined as a simple condition).



#### Note

A wireless controller which is a member of the Converged\_Access device group could be either a standalone device, such as a Cisco CT5760 wireless controller, or a switch with integrated wireless controller functionality, such as the Catalyst 3850.

## Simple and Compound Conditions

To improve the readability of the authorization policy, simple and compound authorization conditions were defined to group different conditions. These conditions may be reused and modified without changing every authorization rule.

Table 16-4 shows the conditions used in the authorization rules.

**Table 16-4**      **Wireless Simple and Compound Conditions****Wireless EAP-TLS (Compound)**

Wireless_EAP-TLS (See <a href="#">Figure 16-11</a> )	Radius:Service-Type Equals Framed
	Radius:NAS-Port-Type Equals Wireless - IEEE 802.11
	Network Access:EapAuthentication Equals EAP-TLS

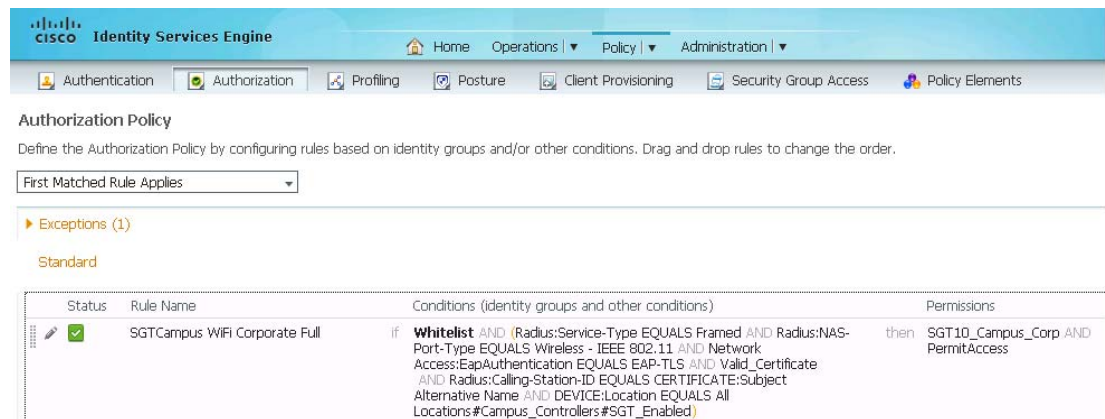
**Check for Valid Certificate (Simple)**

Valid_Certificate (See <a href="#">Figure 16-12</a> )	Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name
---	---

**WLC Location or Device Type (Simple)**

SGT_Controller	DEVICE:Location EQUALS All Locations#Campus_Controllers#SGT_Enabled
Campus_Controller	DEVICE:Location EQUALS All Locations#Campus_Controllers
Branch_Controller	DEVICE:Location EQUALS All Locations#Branch_Controllers
Converged_Access	DEVICE:Device Type EQUALS All Device Types#Converged

To illustrate the value of using simple/compound conditions, [Figure 16-10](#) shows how much longer and harder to read a rule can be when simple/compound conditions are not implemented.

**Figure 16-10**      **Authorization Rule without Conditions**

To define a new compound condition, click **Policy > Conditions > Authorization > Compound Conditions**. [Figure 16-11](#) shows how the Wireless\_EAP-TLS condition combines several conditions into one.



**Figure 16-11** *Wireless\_EAP-TLS Condition*

Authorization Compound Condition List > **Wireless\_EAP-TLS**

Authorization Compound Conditions

\* Name: Wireless\_EAP-TLS

Description: Wireless\_802.1X And EAP-TLS

\*Condition Expression

Condition Name	Expression	Operator	Value	Compare as Operator
Radius:Service-Type	Equals	Framed	AND	AND
Radius:NAS-Port-...	Equals	Wireless - I	AND	AND
Network Access:...	Equals	EAP-TLS		

Save Reset

Figure 16-12 shows the Valid\_Certificate simple condition.

**Figure 16-12** *Valid\_Certificate Condition*

Authorization Simple Condition List > **Valid\_Certificate**

Authorization Simple Conditions

\* Name: Valid\_Certificate

Description: Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name

\* Attribute \* Operator \* Value \* Compare as Operator

Radius:Calling-Station-ID	Equals	CERTIFICATE:Subject Alternative Na	MAC address
---------------------------	--------	------------------------------------	-------------

Save Reset

The remaining conditions shown in Table 16-4 are defined in a similar way.

## Permissions for Wireless Users

When all conditions in the authorization policy rule match, the rule invokes the proper permissions to provide Full Access, as shown in Table 16-5.

**Table 16-5** *Permissions for Full Access*

Permission name	Permission type	Purpose
SGT10_Campus_Corp	Standard result	To assign a SGT for 802.1X wireless devices connecting from an SGT-enabled controller.
Campus WiFi Full Access	Authorization profile	Provides Full Access for 802.1X wireless devices connecting from a centralized campus controller.

**Table 16-5** *Permissions for Full Access*

Permission name	Permission type	Purpose
Branch WiFi Full Access	Authorization profile	To push a VLAN for 802.1X wireless devices connecting from a FlexConnect branch controller.
Converged WiFi Full Access	Authorization profile	Provides Full Access for 802.1X wireless devices connecting from a Converged Access controller.

**Note**

A Converged Access infrastructure refers to a branch or campus deployment with Catalyst 3850 Series switches and/or CT5760 wireless controllers within this design guide.

## Centralized Campus with SGTs

Figure 16-13 shows how the SGT10\_Campus\_Corp authorization profile is pushing the Security Group Tag whose value is 10 for a user of a corporate device, who is allowed to obtain full access.

**Figure 16-13** *SGT10\_Campus\_Corp*

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for the Security Group **SGT10\_Campus\_Corp**. The left-hand navigation pane shows a tree structure with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, Security Group ACLs, and Security Groups. Under Security Groups, several groups are listed, including **SGT10\_Campus\_Corp**, which is currently selected. The main configuration area on the right shows the details for this group: Name is **SGT10\_Campus\_Corp**, Description is **Corporate Users Get A Tag Value Of 10**, and the Tag Value is set to **10**. The Tag Value field is highlighted with a red rectangular box. Below the Tag Value field, there are **Save** and **Reset** buttons. The interface also shows a **Generation Id: 6** and a note to 'Enter value between 2 and 65519'.

See Chapter 23, “BYOD Policy Enforcement Using Security Group Access” for details regarding how SGT 10 is given full access for a campus which implements a centralized controller (Local Mode) design with SGTs.

## Centralized Campus with ACLs

Figure 16-14 shows how the Campus WiFi Full Access authorization profile is using the ACCESS\_ACCEPT Access Type to allow full access.

**Figure 16-14** *Campus WiFi Full Access*

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring an authorization profile. The left sidebar shows a tree view with categories like Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. The main area is titled 'Authorization Profiles > Campus WiFi Full Access'. The 'Authorization Profile' section shows the profile name 'Campus WiFi Full Access' and a description field. The 'Access Type' is set to 'ACCESS\_ACCEPT', which is highlighted with a red box. Below this, the 'Service Template' checkbox is unchecked. The 'Common Tasks' section includes checkboxes for 'DACL Name', 'VLAN', 'Voice Domain Permission', and 'Web Redirection (CWA, DRW, MDM, NSP, Posture)'. The 'Advanced Attributes Settings' section shows a dropdown menu for 'Select an item'. The 'Attributes Details' section shows 'Access Type = ACCESS\_ACCEPT'.

Since full access is allowed with this authorization profile, no Named ACL for access control needs to be specified by ISE.

## Branch with FlexConnect

Endpoints connecting from a branch location dynamically get assigned to VLAN 10, which has been configured without an ACLs thus providing full access.

**Figure 16-15** Branch WiFi Full Access

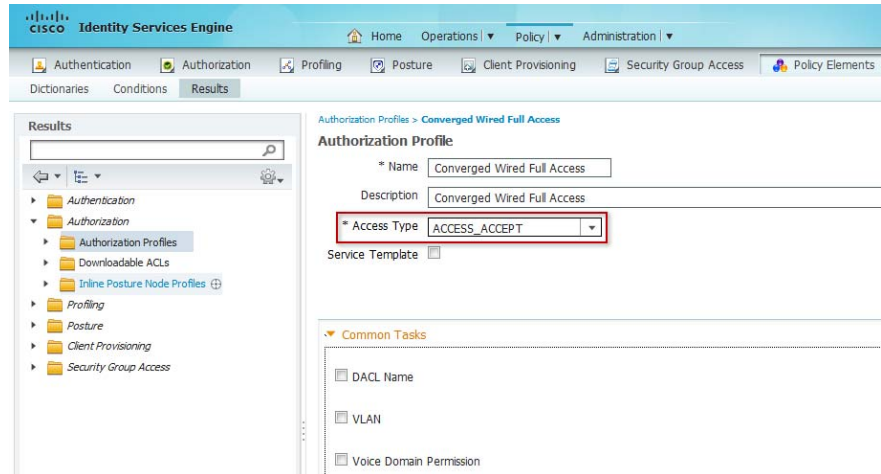
The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Policy' tab is active, showing a breadcrumb trail: 'Authorization Profiles > Branch WiFi Full Access'. The left sidebar contains a tree view of configuration objects, with 'Authorization' expanded to show 'Authorization Profiles'. The main content area is titled 'Authorization Profile' and shows the configuration for 'Branch WiFi Full Access'. The 'Access Type' is set to 'ACCESS\_ACCEPT'. Under 'Common Tasks', the 'VLAN' checkbox is checked, with 'Tag ID' set to 1 and 'ID/Name' set to 10. The 'Advanced Attributes Settings' section shows a dropdown menu with 'Select an item' and a plus sign. The 'Attributes Details' section lists the following attributes: 'Access Type = ACCESS\_ACCEPT', 'Tunnel-Private-Group-ID = 1:10', 'Tunnel-Type=1:13', and 'Tunnel-Medium-Type=1:6'.

294030

## Converged Access Branch or Campus

Within this design guide, a Converged Access infrastructure refers to a branch or campus deployment with Catalyst 3850 Series switches and/or CT5760 wireless controllers.

Figure 16-16 shows how the Converged WiFi Full Access authorization profile is using the ACCESS\_ACCEPT Access Type to allow full access.

**Figure 16-16** Converged WiFi Full Access

Again, since full access is allowed with this authorization profile, no Named ACL for access control needs to be specified by ISE.

## Corporate Wired Devices—Full Access

The authorization policy rules for wired devices follow the same logic as wireless devices. Corporate approved wired devices are assumed to be pre-configured with the correct configuration profiles after being on-boarded.

To provide full access to corporate wired devices, the Cisco ISE verifies the following:

- The device has been on-boarded and has the right certificate and profile configurations.
- The device has been added to the Whitelist identity group.
- To uniquely identify the device and prevent spoofing, the Calling-Station-ID matches the Subject Alternative Name of the certificate, in this case, the MAC address of the endpoint.
- The connection originated using EAP-TLS authentication.

Since the wired designs presented in this design guide rely on slightly different access control mechanisms for converged access campuses and branches, for campuses and branches that do not implement converged access infrastructures unique authorization rules are created for connections originating from each design.



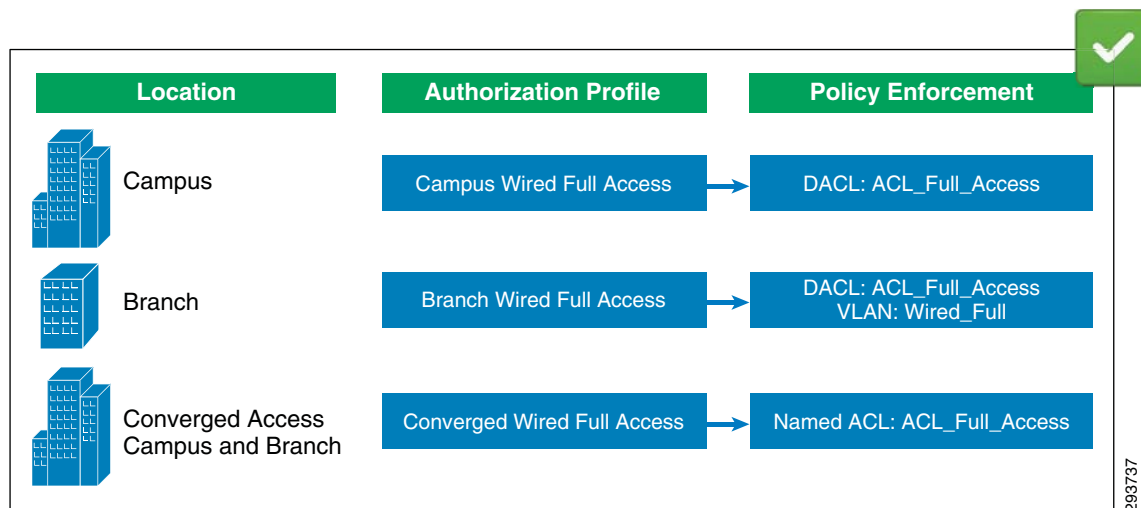
### Note

For the purpose of clarity within this design guide, converged access branches refer to designs in which Catalyst 3850 Series switches are deployed at the access-layer of the branch network. From a wired perspective, branches which do not implement converged access infrastructures are branches which deploy other Catalyst access-layer switches, such as the Catalyst 3750X Series. Unless otherwise specified, these are referred to simply as “branches” within the design guide. Similarly, converged access campuses refer to designs in which Catalyst 3850 Series switches are deployed at the access-layer of building distribution modules within the campus. From a wired perspective, campuses which do not implement converged access infrastructures are campuses which deploy other Catalyst access-layer switches, such as the Catalyst 3750X Series. Unless otherwise specified, these are referred to simply as

“campuses” within this design guide. This is in order to reduce the use of verbose phrases such as “branches which do not implement converged access infrastructure” and “campuses which do not implement converged access infrastructure”.

At a high level, [Figure 16-17](#) shows how different authorization profiles are selected for connections originating from different locations with different infrastructure (converged access versus non-converged access) designs. Each authorization profile in turn enforces a unique permission using VLANs, dynamic ACLs (either named or downloadable [DACL]), etc.

**Figure 16-17 Full Access Wired Enforcement**



**Note**

Wired assignment of Security Group Tags (SGTs) is not discussed within the design guide. Hence there is no wired policy enforcement via SGTs in [Figure 16-17](#). Future versions of this design guide may address wired SGT assignment.

To differentiate these connections, the ISE relies on Network Device Groups to group Catalyst switches based on their location or device type. This allows a single ISE to enforce policies across different groups of devices. Each Catalyst switch needs to be added to the proper device group by clicking **Administration > Network Resources > Network Devices** and specifying the proper location or device type from the pull-down menu.

[Figure 16-18](#) shows the details of authorization profile configured in ISE for wired devices.

**Figure 16-18 Authorization Policies for Wired Full Access**

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Campus Wired Corporate Full	if <b>Whitelist</b> AND (Wired_EAP-TLS AND Valid_Certificate AND Campus_Switches )	then Campus Wired Full Access
✓	Branch Wired Corporate Full	if <b>Whitelist</b> AND (Wired_EAP-TLS AND Valid_Certificate AND Branch_Switches )	then Branch Wired Full Access
✓	Converged Wired Corporate Full	if <b>Whitelist</b> AND (Wired_EAP-TLS AND Valid_Certificate AND Converged_Access )	then Converged Wired Full Access

Looking at the rules in more detail, ISE evaluates the following conditions:

- **WhiteList**—The endpoint has been added by an IT Administrator to the WhiteList identity group.
- **Wired\_EAP-TLS**—The endpoint connected using EAP-TLS (defined as a compound condition).
- The endpoint has a valid certificate. The Calling-Station-ID matches the MAC address included in the certificate's Subject Alternative Name (defined as a simple condition).
- The RADIUS authentication originated from a Catalyst switch which was a member of one of the following device groups: Campus\_Switches, Branch\_Switches, or Converged\_Access (defined as a simple condition).

## Wired Simple and Compound Conditions

To improve the readability of the authorization policy, simple and compound authorization conditions were defined to group different conditions. These conditions may be reused and modified without changing every authorization rule.

Table 16-6 shows the conditions used in the authorization rules.

**Table 16-6 Wired Simple and Compound Conditions**

Wired EAP-TLS (Compound)	
Wired_EAP-TLS	Radius:Service-Type Equals Framed Radius:NAS-Port-Type Equals Ethernet Network Access:EapAuthentication Equals EAP-TLS
Check for Valid Certificate (Simple)	
Valid_Certificate	Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name
WLC Location or Device Type (Simple)	
Campus_Switches	DEVICE:Location EQUALS All Locations#Campus_Switches
Branch_Switches	DEVICE:Location EQUALS All Locations#Branch_Switches
Converged_Access	DEVICE:Device Type EQUALS All Device Types#Converged

# Permissions for Wired Users

When all conditions in the authorization policy rule match, the rule invokes the proper permission. The permissions can be of different forms, such as an authorization profile or a standard result. In this design guide, for wired access the authorization policy is used as permission to the policy rules match. [Table 16-7](#) explains the permissions used for the full access for wired users.

**Table 16-7      Permissions Used for Wired Full Access**

Permission Name	Permission Type	Purpose
Campus Wired Full Access	Authorization profile	Provides Full Access for 802.1X wired devices connecting from campus location.
Branch Wired Full Access	Authorization profile	To push a VLAN for 802.1X wired devices connecting from a branch location.
Converged Wired Full Access	Authorization profile	To push a named ACL for 802.1X wired devices connecting from either a campus or branch location with Converged Access.

## Campus Wired

[Figure 16-19](#) shows how the Campus Wired Full Access authorization profile is defined in ISE.



**Figure 16-19** Campus Wired Full Access Authorization Profile

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Operations, Policy, and Administration. Below this is a secondary navigation bar with icons for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The 'Results' tab is selected in the left-hand navigation pane. The main content area is titled 'Authorization Profiles > Campus Wired Full Access'. It shows the configuration for an 'Authorization Profile' with the following details:

- Name:** Campus Wired Full Access
- Description:** (empty field)
- Access Type:** ACCESS\_ACCEPT (dropdown menu)
- Service Template:** (checkbox, unchecked)
- Common Tasks:**
  - ☒ DACL Name: PERMIT\_ALL\_TRAFFIC (dropdown menu)
  - ☐ VLAN
  - ☐ Voice Domain Permission
  - ☐ Web Redirection (CWA, DRW, MDM, NSP, Posture)
- Advanced Attributes Settings:**
  - Select an item (dropdown menu) = (empty field) (dropdown menu)
- Attributes Details:**
  - Access Type = ACCESS\_ACCEPT
  - DACL = PERMIT\_ALL\_TRAFFIC

**Note**

Cisco Catalyst switches support both downloadable ACLs (DACLs) and named ACLs. This design guide shows and validates the use of downloadable ACLs for access control of wired devices when implementing a non-converged access infrastructure and the use of named ACLs for access control of wired devices when implementing a converged access infrastructure. This is done to show the depth and range of capabilities for access control available on Cisco IOS-based platforms. Note that the same wired policy enforcement for converged access and non-converged access designs can be achieved if the customer desires by simply using either downloadable ACLs (DACLs) or named ACLs for both designs. Both downloadable and named ACLs have advantages and disadvantages, depending upon where they are deployed within the network. [ACL Complexity and Considerations](#) in Chapter 5, “Campus and Branch Network Design for BYOD” discusses some of these advantages and disadvantages.

The downloadable ACL (DACL), which allows all IP traffic, overrides the default-ACL configured on the switch port. The default-ACL is used as an additional preventative measure in case the downloadable ACL is not applied to the switch port for some reason.

**Note**

ISE 1.2 has the ability to check the DACL syntax. This feature should be utilized in order to minimize the possibility that the DACL is not applied due to a syntax error.

## Branch Wired

Figure 16-20 shows how a similar authorization profile is constructed for devices connected at a branch which does not have a Converged Access infrastructure. The authorization profile pushes VLAN information along with the ACL information.

**Figure 16-20 Branch Wired Full Access Authorization Profile**

The screenshot displays the Cisco Identity Services Engine (ISE) configuration page for an Authorization Profile. The breadcrumb trail indicates the path: Authorization Profiles > Branch Wired Full Access. The main configuration area is titled 'Authorization Profile' and includes the following fields:

- \* Name:** Branch Wired Full Access
- Description:** Branch Wired Full Access
- \* Access Type:** ACCESS\_ACCEPT (selected from a dropdown)
- Service Template:** (empty checkbox)

Below these fields is a section titled 'Common Tasks' which contains several configuration options:

- ☒ **DACL Name:** ACL\_Full\_Access (selected from a dropdown)
- ☒ **VLAN:** Tag ID 1, ID/Name 13 (with an 'Edit Tag' button)
- ☐ **Voice Domain Permission:** (unchecked)

A red rectangular box highlights the 'DACL Name' and 'VLAN' configuration options. On the right side of the interface, the number 294034 is visible.

Once this profile is downloaded to the Catalyst switch, the endpoint gets full access to the network.

## Converged Access Branch or Campus

Figure 16-21 shows how the Converged Access Wired Full Access authorization profile is defined in ISE.

**Figure 16-21 Converged Wired Full Access Authorization Profile**

For the converged access design, a named ACL is implemented, meaning that the ACL must be configured on the Catalyst 3850 switch rather than being downloaded from ISE. Using the RADIUS Filter-ID attribute-value pair, ISE instructs the Catalyst 3850 to apply the ACL\_Full\_Access ACL. The following configuration example shows the contents of this ACL as defined in the Catalyst 3850 switch.

```
!
ip access-list extended ACL_Full_Access
 permit ip any any
!
```

## ISE Authorization Policy

For reference purposes, the complete authorization policy used during testing is shown in [Figure 16-22](#). The figure highlights the following sections:

1. Used for blacklisting lost or stolen devices.
2. On-boarding and MDM registration/remediation.
3. Wireless devices connecting from an access point in a SGT\_Enabled location.
4. Wireless devices connecting from an access point in the campus or branch locations.
5. Wired devices connecting from a campus or branch locations.

6. Wired and Wireless devices connecting from a converged location.
7. Guest and Basic Access.

**Figure 16-22 Complete Authorization Policy**

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default ISE	Blacklist AND Wireless_Access	then Blackhole Wifi Access
✓	Wired Black List Default	Blacklist AND Wired_Access	then Blackhole Wired Access
✓	MDM Enrollment	(Wireless_EAP-TLS AND ISE_Registered AND MDM_UnRegistered AND MDM_Managed AND MDM_Operational)	then Internet Until MDM
✓	Dual SSID Provisioning	(Wireless_MAB AND Provisioning_WLAN)	then Wireless CWA
✓	Single SSID Provisioning	(Wireless_PEAP AND Employee_WLAN)	then Wireless NSP
✓	Remediate Non ISE Compliant	(Wireless_EAP-TLS AND ISE_NonCompliant AND MDM_Managed AND MDM_Operational)	then ISE Quarantine
✓	Remediate Non MDM Compliant	(Wireless_EAP-TLS AND MDM_NonCompliant AND MDM_Managed AND MDM_Operational)	then MDM Quarantine
✓	SGTCampus Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller)	then SGT10_Campus_Corp AND PermitAccess
✓	SGTCampus Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Full_Access)	then SGT11_Campus_Pers_Full AND PermitAccess
✓	SGTCampus Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Partial_Access)	then SGT12_Campus_Pers_Partial AND PermitAccess
✓	SGTCampus Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Domain_Users)	then Campus Wifi Internet Only
✓	Campus Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Campus_Controller)	then Campus Wifi Full Access
✓	Campus Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND Campus_Controller AND AD_Full_Access)	then Campus Wifi Full Access
✓	Campus Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Campus_Controller)	then Campus Wifi Partial Access
✓	Campus Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Campus_Controller)	then Campus Wifi Internet Only
✓	Branch Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Branch_Controller)	then Branch Wifi Full Access
✓	Branch Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND Branch_Controller AND AD_Full_Access)	then Branch Wifi Full Access
✓	Branch Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Branch_Controller)	then Branch Wifi Partial Access
✓	Branch Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Branch_Controller)	then Branch Wifi Internet Only
✓	Campus Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Campus_Switches)	then Campus Wired Full Access
✓	Campus Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND Campus_Switches AND AD_Full_Access)	then Campus Wired Full Access
✓	Campus Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Campus_Switches)	then Campus Wired Partial Access
✓	Campus Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Campus_Switches)	then Campus Wired Internet Only
✓	Branch Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Branch_Switches)	then Branch Wired Full Access
✓	Branch Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Branch_Switches)	then Branch Wired Full Access
✓	Branch Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Branch_Switches)	then Branch Wired Partial Access
✓	Branch Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Branch_Switches)	then Branch Wired Internet Only
✓	Converged Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Converged_Access)	then Converged Wifi Full Access
✓	Converged Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Converged_Access)	then Converged Wifi Full Access
✓	Converged Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Converged_Access)	then Converged Wifi Partial Access
✓	Converged Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Converged_Access)	then Converged Wifi Internet Only
✓	Converged Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Converged_Access)	then Converged Wired Full Access
✓	Converged Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Converged_Access)	then Converged Wired Full Access
✓	Converged Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Converged_Access)	then Converged Wired Partial Access
✓	Converged Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Converged_Access)	then Converged Wired Internet Only
✓	Wifi Guest	WLC_Web_Authentication AND Guest_WLAN	then PermitAccess
✓	Wifi Basic Access	(Wireless_PEAP AND Personal_Device_WLAN)	then PermitAccess

293792



# BYOD Advanced Use Case—Mobile Device Manager Integration

---

**Revised:** July 11, 2014

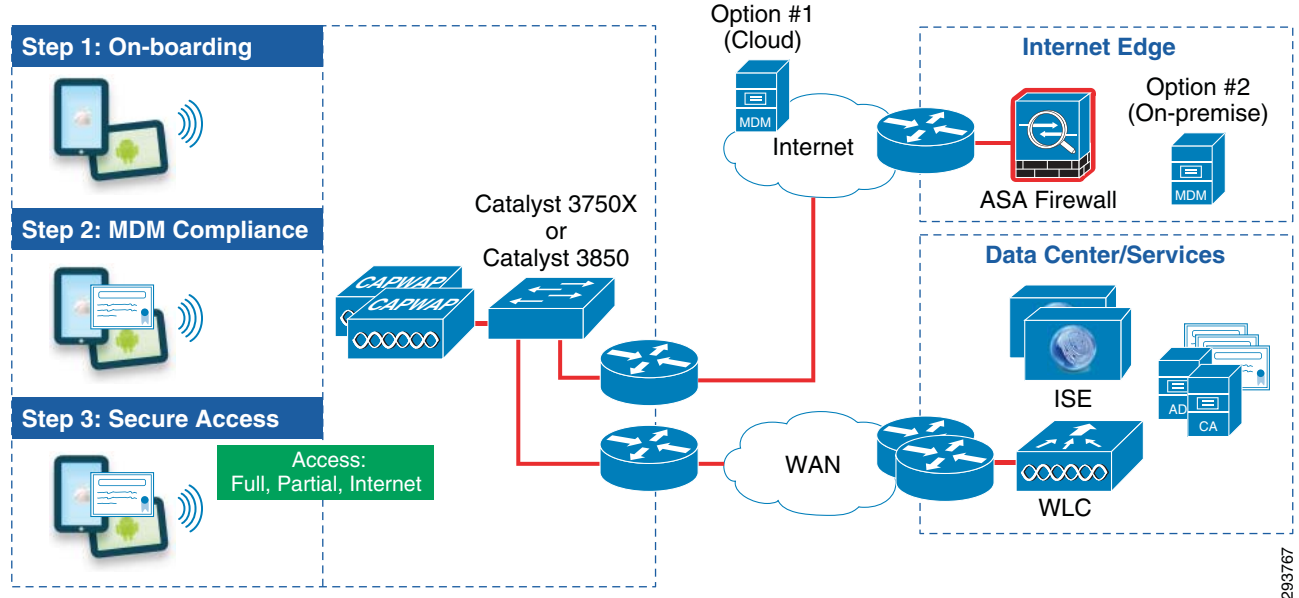
**What's New:** Added notes about how ACL behavior has changed in version 7.5+ of the Wireless LAN Controller.

This chapter focuses on getting additional posture information from the integration with third-party Mobile Device Managers (MDMs). While previous chapters focused on on-boarding corporate and personal devices and providing differentiated access, this chapter makes use of more detailed endpoint information to enforce authorization policies.

MDM servers secure, monitor, manage, and support mobile devices to secure and control the use of mobile applications. The network is the only entity that can provide granular access to endpoints based on VLAN assignment, ACLs (named or downloadable [DACL]), SGTs, FlexConnect ACLs, etc. By integrating with third-party MDM servers, the Cisco ISE receives the necessary device attributes to enforce a more granular network access to those endpoints.

[Figure 17-1](#) shows the interoperability between MDMs and the Cisco ISE. Once a device has been on-boarded with ISE, ISE queries the MDM for additional endpoint information. If the endpoint is registered and compliant with MDM policies, the device is granted access, based on other attributes, as described in the previous sections.

Notice that the MDM server can be deployed on-premise or in the cloud.

**Figure 17-1 MDM Interoperability**

The following steps take place when checking for device compliance:

1. The user connects to an on-boarding SSID and is guided through the registration and on-boarding process with ISE.
2. Once the user has been on-boarded with the proper certificate/profiles, the user connects to the secure Employee SSID.
3. ISE makes an API call to the MDM server. If the device is not registered with the MDM, the user is presented with the appropriate page to proceed to their MDM enrollment page.
4. Once the user completes the enrollment with the MDM server, they return to an enrollment redirect page that includes a continue button. When the user selects the continue option from the page, ISE will issue a Change of Authorization (CoA), forcing the user to re-authenticate. The API should now indicate the user has enrolled with the MDM. The MDM API results are cached by ISE for the duration of the authorization flow.
5. ISE uses the cached MDM information for the specific MAC address to verify the device's posture including its MDM compliance status. If the device is not in compliance with the MDM policies, the user is once again informed and is asked to become compliant.
6. Once the device becomes compliant, the user is authorized to access the network based on the assigned permissions (Full, Partial Access, or Internet Access).
7. ISE can poll the MDM server periodically to get compliance information.

Chapter 13, "Mobile Device Manager Integration for BYOD" provides more details on how to configure the integration between ISE and the MDM.



## Supported MDM Functions

Cisco ISE relies on REST API calls to query the external MDM server for additional endpoint information. The communication between ISE and the MDM is mostly unidirectional, where ISE sends different commands to the MDM. Some commands query for device information (model, compliance status, serial number, etc.) while others can invoke an action on the device (Corporate Wipe, Full Wipe, PIN lock, etc.).

The following are some of the functions that ISE performs in conjunction with an MDM server:

- Device registration—Unregistered endpoints connecting to the network are redirected to a web page hosted on the MDM server to initiate the MDM enrollment process.
- Device remediation—Cisco ISE imposes a captive portal on noncompliant endpoints. The user is redirected to a web page hosted by ISE but populated with device posture information obtained via the MDM API. The page informs the user and what actions to take to become compliant.
- Periodic compliance checks—Cisco ISE polls the MDM server periodically for a list of non-MDM compliant devices. ISE will determine if any device on the list is currently associated with the network and will issue a CoA against those devices.
- Device instructions through the MDM server—Remote actions can be issued for users' devices through the MDM server.

The endpoint database is updated with additional information from the MDM server that cannot be collected using the Cisco ISE Profiler. The following device attributes can be obtained from the MDM:

- MDManufacturer
- MDModel
- MDOSVersion
- MDPhoneNumber
- MDSerialNumber
- MDIMEI

These attributes can be viewed by clicking **Administration > Identity Management > Identities > Endpoints**, as shown in [Figure 17-2](#).

**Figure 17-2 MDM Attributes**

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Operations, Policy, and Administration. Below this, a secondary navigation bar shows System, Identity Management, Network Resources, Web Portal Management, and Feed Service. The main content area is divided into two panels. The left panel, titled 'Identities', contains a search bar and a list of folders: Users, Endpoints, and Latest Manual Network Scan Results. The right panel, titled 'Endpoint List > 1C:AB:A7:B4:85:12', shows the details for a specific endpoint. The 'Endpoint' section includes fields for MAC Address (1C:AB:A7:B4:85:12), Static Assignment (unchecked), Policy Assignment (Apple-iPad), Static Group Assignment (checked), and Identity Group Assignment (RegisteredDevices). Below this is the 'Attribute List' table, which contains various attributes and their values. A red box highlights the MDM-related attributes: MDMManufacturer (Apple), MDMModel (iPad, 3rd gen), MDMOSVersion (iOS 6.0), MDMPHONEumber (PDA), and MDMSerialNumber (DLXH7HKMDVD1). Other attributes include BYODRegistration (Yes), Certificate Expiration Date (02-19-2014 16:27:08), Certificate Issue Date (02-19-2013 16:27:08), Certificate Issuer Name (CN=sdulab-DC-ADDC-1-CA, DC=sdulab, DC=com), Certificate Serial Number (1c906ef8000000000104), Description (White iPad), DeviceRegistrationStatus (Pending), EndPointPolicy (Apple-iPad), EndPointProfilerServer (dc-ise-1.sdulab.com), EndPointSource (DHCP Probe), IdentityGroup (RegisteredDevices), IdentityStoreName (AD1), MACAddress (1C:AB:A7:B4:85:12), MatchedPolicy (Apple-iPad), OUI (Apple, Inc.), and PolicyVersion (1).

Attribute List	
BYODRegistration	Yes
Certificate Expiration Date	02-19-2014 16:27:08
Certificate Issue Date	02-19-2013 16:27:08
Certificate Issuer Name	CN=sdulab-DC-ADDC-1-CA, DC=sdulab, DC=com
Certificate Serial Number	1c906ef8000000000104
Description	White iPad
DeviceRegistrationStatus	Pending
EndPointPolicy	Apple-iPad
EndPointProfilerServer	dc-ise-1.sdulab.com
EndPointSource	DHCP Probe
IdentityGroup	RegisteredDevices
IdentityStoreName	AD1
MACAddress	1C:AB:A7:B4:85:12
MDMManufacturer	Apple
MDMModel	iPad, 3rd gen
MDMOSVersion	iOS 6.0
MDMPHONEumber	PDA
MDMSerialNumber	DLXH7HKMDVD1
MatchedPolicy	Apple-iPad
OUI	Apple, Inc.
PolicyVersion	1

The integration with an MDM server allows the Cisco ISE to configure policies based on additional MDM attributes. The dictionary attributes can be found under **Policy > Dictionaries > MDM > Dictionary Attributes**, as shown in [Figure 17-3](#).



**Figure 17-3 Dictionary Attributes**

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Policy Elements' tab is selected, and the 'Dictionary Attributes' sub-tab is active. On the left, a 'Dictionaries' sidebar shows a tree structure with 'System' and 'User' folders. The main area displays the 'Dictionary Attributes' for the 'MDM' dictionary. A table lists various attributes with checkboxes, internal names, and descriptions.

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

Some of these attributes are used in several authorization rules in this design guide.

## Integration Process Flow

Figure 17-4 shows the integration process between ISE and the MDM:

1. The device has been on-boarded and the user connects to the BYOD\_Employee SSID.
2. Cisco ISE makes an API call to the MDM server to verify that the device has been registered with the MDM.
3. If the device is not registered and is required to be registered, the user is asked to enroll with the MDM. This may include installing the appropriate application from the Apple App Store or Google Play.
4. ISE enforces some device attributes before allowing network access. If the device is not ISE Compliant, quarantine the device (explained below).
5. If the device is not compliant with the MDM policies, quarantine the device.

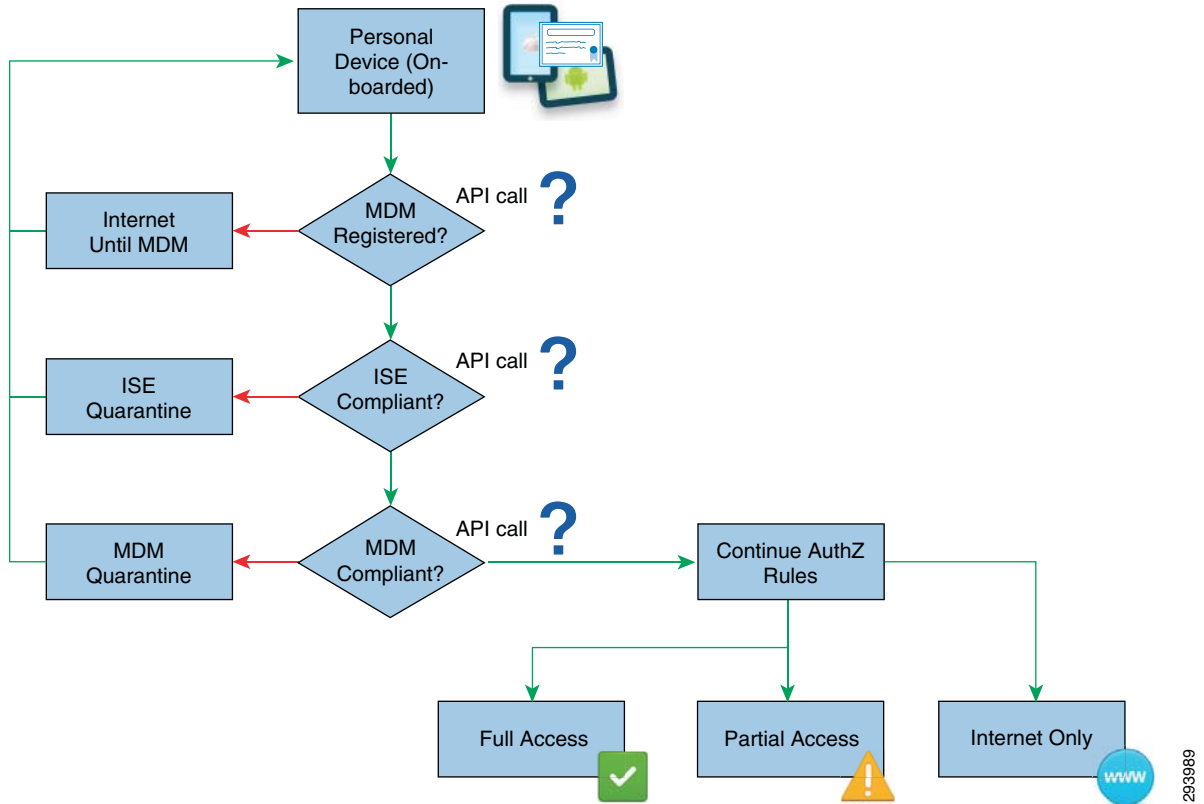
If the user has been on-boarded and is compliant with ISE and MDM policies, allow the proper permissions based on different rules.



### Note

The previous chapters explained how to grant Full Access, Partial Access and Internet Only access to personal and corporate devices.

Figure 17-4 MDM Compliance Checks



## ISE Compliance Check

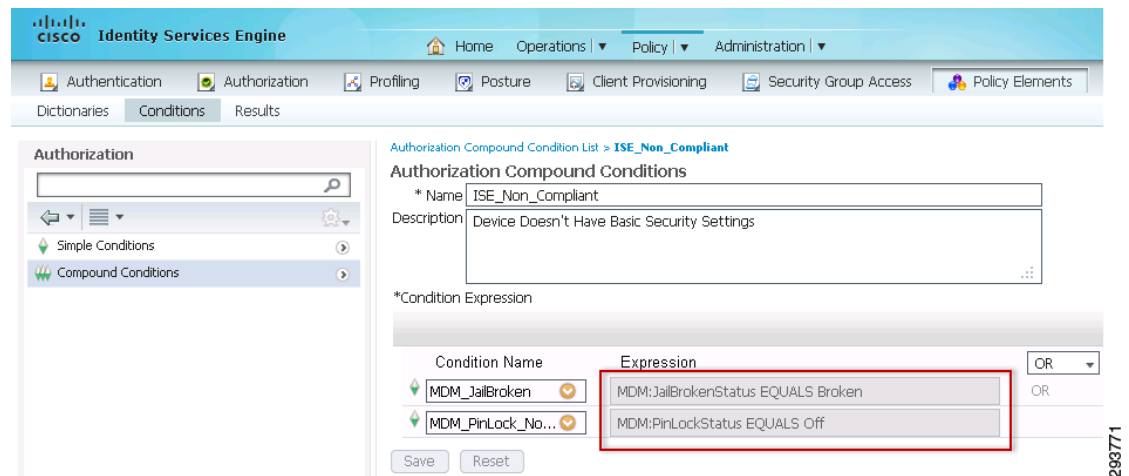
Once the device has been registered with the MDM, the ISE checks for certain device attributes before allowing access to the network. This can serve as an additional check and the first opportunity to verify some device attributes.

In this design guide, two device attributes were considered as the minimum for devices to obtain access to the network:

- Jailbroken or rooted devices—Not allowed into the network.
- PIN lock enforcement—Devices without a device PIN lock are denied access.

ISE makes the *JailBrokenStatus* and *PinLockStatus* API calls to the MDM to verify these attributes.

A compound condition was defined in the ISE to check for these two attributes. To define this compound condition click **Policy > Policy Elements > Conditions > Compound Conditions**, as shown in Figure 17-5.

**Figure 17-5 ISE\_Non\_Compliant**

Additional dictionary attributes could be added to accommodate the security policies of each organization.

## MDM Compliance Check

For devices that have been on-boarded and have met the ISE compliance check, an additional API call is made to the MDM to make sure the device has met all the compliance requirements established by the MDM.

If the device is not fully compliant with the MDM, ISE grants access to the Internet and denies access to all internal resources. When the user tries to access an internal resource, ISE redirects the session to a portal, highlighting the steps required to be completed to meet the MDM compliance rules.

ISE makes the DeviceCompliantStatus API call to the MDM to verify compliance. The MDM establishes what conditions result in a device being non-compliant.

## ISE Configuration

Several ISE features play a role in verifying for ISE and MDM compliance before permissions can be applied. Some of them include Logical Profiles, authorization rules, ACLs, and API calls to the MDM to receive endpoint attributes.

## Logical Profile

The profiling service in the Cisco ISE is able to identify devices connecting to the network to grant the appropriate access to endpoints based on their device type. By collecting attributes of endpoints and grouping them according to their profiles, unique policies may be enforced for specific type of devices.

A logical profile is a virtual container of objects that share a common attribute. One example of a logical profile is a set of devices that includes all tablets or all smartphones. A second example is a set of all Android or Apple devices. For the purposes of this design guide, a logical profile was created to include the devices that are managed by the MDM. This allows the administrator to dynamically add or remove devices managed by the MDM.

Figure 17-6 shows the MDM Managed logical profile used to group devices allowed and managed or licensed by the MDM. This logical profile is used when defining the ISE authorization policy and includes devices profiled as Android, Samsung-Device, and Apple-Device. To configure this logical profile on the ISE, click **Policy > Profiling > Logical Profiles**.

**Figure 17-6 MDM Managed Logical Profile**

The screenshot shows the Cisco Identity Services Engine (ISE) Profiling Logical Profiles configuration page. The 'MDM Managed' logical profile is selected. The 'Available Policies' list includes Apple-MacBook, Apple-iDevice, Apple-iPad, Apple-iPhone, Apple-iPod, Appera-Device, Aruba-Device, and Aruba-AP. The 'Assigned Policies' list includes Android, Samsung-Device, and Apple-Device. A table below shows endpoints in the logical profile with columns for Endpoint policy, MAC Address, and IP Address.

Endpoint policy	MAC Address	IP Address
Android	30:85:A9:60:08:CF	64.100.57.129
Android	18:E2:C2:82:43:AF	10.31.1.127
Android	C8:60:00:27:D5:9F	10.31.1.131
Android	10:F9:6F:B4:68:5E	10.31.1.134
Android	18:46:17:E3:43:68	10.31.1.131
Android	00:01:36:70:C1:04	
Apple-Device	34:51:C9:93:CB:8A	10.31.1.121
Apple-Device	B8:17:C2:11:BB:3F	10.31.1.121
Apple-Device	CC:08:E0:48:82:B7	192.168.1.149

The logical profile could be easily expanded to include other devices supported and managed by the MDM without modifying the ISE authorization policy.

## Authorization Policy

Figure 17-7 shows the ISE authorization rules used to enforce MDM and ISE compliance. These authorization rules are executed after the user has on-boarded the mobile device and before additional access (e.g., Full, Partial, Internet) to the network is granted.

**Figure 17-7 MDM Compliance Authorization Rules**

**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
<input checked="" type="checkbox"/>	MDM Enrollment	if (Wireless_EAP-TLS AND ISE_Registered AND MDM_UnRegistered AND MDM_Managed AND MDM_Operational )	then Internet Until MDM
<input checked="" type="checkbox"/>	Remediate Non ISE Compliant	if (Wireless_EAP-TLS AND ISE_NonCompliant AND MDM_Managed AND MDM_Operational )	then ISE Quarantine
<input checked="" type="checkbox"/>	Remediate Non MDM Compliant	if (Wireless_EAP-TLS AND MDM_NonCompliant AND MDM_Managed AND MDM_Operational )	then MDM Quarantine

293773

## MDM Enrollment Rule

This rule matches when the following conditions are met:

- The endpoint connected via a wireless 802.1X SSID.
- Logical Profile equals MDM Managed—The device is managed and supported by the MDM.
- The device has gone through the on-boarding process and registered with ISE.
- The device has **not** registered with the MDM.

If these conditions match, the *Internet Until MDM* authorization profile is used. This profile is configured to redirect nonregistered devices to the redirect URL highlighted in [Figure 17-8](#).

**Figure 17-8** Internet Until MDM

**Results**

- Authentication
- Authorization
  - Authorization Profiles
  - Downloadable ACLs
  - Inline Posture Node Profiles
- Profiling
- Posture
- Client Provisioning
- Security Group Access

**Authorization Profiles > Internet Until MDM**

**Authorization Profile**

\* Name: Internet Until MDM

Description:

\* Access Type: ACCESS\_ACCEPT

Service Template: ☐

**Common Tasks**

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

MDM Redirect:  ACL: ACL\_Internet\_Redirect

☐ Static IP/Host name

☐ Auto Smart Port

☐ Filter-ID

**Advanced Attributes Settings**

Select an item =

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
 Airespace-ACL-Name = ACL\_Internet\_Only  
 disco-av-pair = url-redirect-ACL=ACL\_Internet\_Redirect  
 disco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=mdm

The authorization profile relies on two named ACLs previously defined in the Wireless LAN Controller: ACL\_Internet\_Redirect and ACL\_Internet\_Only. ACL\_Internet\_Redirect is shown as being applied to the MDM Redirect setting in the figure above. ACL\_Internet\_Only is shown as being sent to the wireless controller via the Radius:Airespace-ACL-Name attribute value (AV) pair in Figure 17-8. The behavior of the two ACLs is slightly different between CUWN wireless controllers, such as the CT5508 and Flex 7500, and IOS XE based controllers, such as the CT5760 and Catalyst 3850.

**Note**

Within this document, wireless LAN Controller refers to either a standalone appliance such as the Cisco CT5508, Flex 7500, or CT5760 wireless controllers or to wireless controller functionality integrated within the Catalyst 3850 Series switch.

For CUWN wireless controllers, ACL\_Internet\_Redirect functions as both the ACL which controls web redirection, as well as the ACL which controls what the wireless client is allowed to access on the network. ACL\_Internet\_Only serves simply as a extra security configuration. CUWN wireless controllers do not make use of this ACL when URL redirection is specified. For CUWN wireless controllers the ACL\_Internet\_Redirect ACL shown in Figure 17-9 can be the same as the ACL\_Internet\_Only ACL discussed in the previous chapters.

**Figure 17-9** *ACL\_Internet\_Redirect*

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK									
Access Control Lists > Edit									
General									
Access List Name		ACL_Internet_Redirect							
Deny Counters		0							
Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	
<a href="#">1</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any	
<a href="#">2</a>	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">3</a>	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any	
<a href="#">4</a>	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">5</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server	
<a href="#">6</a>	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client	
<a href="#">7</a>	Deny	0.0.0.0	/ 0.0.0.0	10.0.0.0	/ 255.0.0.0	Any	Any	Any	
<a href="#">8</a>	Deny	10.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">9</a>	Deny	0.0.0.0	/ 0.0.0.0	172.16.0.0	/ 255.240.0.0	Any	Any	Any	
<a href="#">10</a>	Deny	172.16.0.0	/ 255.240.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">11</a>	Deny	0.0.0.0	/ 0.0.0.0	192.168.0.0	/ 255.255.0.0	Any	Any	Any	
<a href="#">12</a>	Deny	192.168.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	
<a href="#">13</a>	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	

293775

The 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).
- Deny IP access to and from internal network address space (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
- Allow access to and from all other subnets (Internet access).

**Note**

The ACL behavior has changed in version 7.5+ of the Wireless LAN Controller. The presence of an Airespace ACL Name in the authorization profile affects the webauth redirect functionality for access points operating in FlexConnect mode.

For FlexConnect deployments, the ACL\_Provisioning Airespace ACL must be removed from the configuration. This implies that there needs to be two independent authorization profiles for provisioning: one for FlexConnect and CUWN wireless controllers and another one for and Converged Access wireless controllers.

Refer to [Appendix E, “Airespace ACLs in WLC 7.5+”](#) for sample configurations.

For Cisco IOS XE based wireless controllers, ACL\_Internet\_Redirect functions strictly as the ACL which controls web redirection. ACL\_Internet\_Only 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. An example of the ACL\_Internet\_Redirect ACL for Cisco IOS XE based wireless controllers is shown in [Example 17-1](#).

**Example 17-1 Internet Redirect ACL for IOS XE Based Controllers**

```
!
ip access-list extended ACL_Internet_Redirect
deny    udp any eq bootpc any eq bootps
```

```
deny ip any host 10.230.1.45
deny ip any host 10.225.49.15
permit ip any 10.0.0.0 0.255.255.255
permit ip any 172.16.0.0 0.15.255.255
permit ip any 192.168.0.0 0.0.255.255
deny ip any any
!
```

The above ACL specifies the following access:

- Deny (do not redirect) DHCP access (bootpc and bootps).
- 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).
- Allow (redirect) IP access to and from the rest of the internal network IP address space (10.0.0.0 /8, 172.16.0.0 /12, 192.168.0.0 /16).
- Deny (do not redirect) all other access to the Internet.

An example of the ACL\_Internet\_Only ACL for Cisco IOS XE based wireless controllers is shown in [Example 17-2](#).

#### **Example 17-2 Access ACL for IOS XE Based Controllers**

```
!
ip access-list extended ACL_Internet_Only
permit udp any eq bootpc any eq bootps
permit ip any host 10.230.1.45
permit ip any host 10.225.49.15
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
permit ip any any
!
```

The above access-list specifies the following access:

- Allow DHCP access (bootpc and bootps).
- Allow IP access to and from the DNS server (1.230.1.45).
- Allow IP access to and from the ISE server (1.225.49.15).
- Deny IP access to and from the rest of the internal network IP address space (10.0.0.0 /8, 172.16.0.0 /12, 192.168.0.0 /16).
- Allow access to all other addresses (Internet addresses).

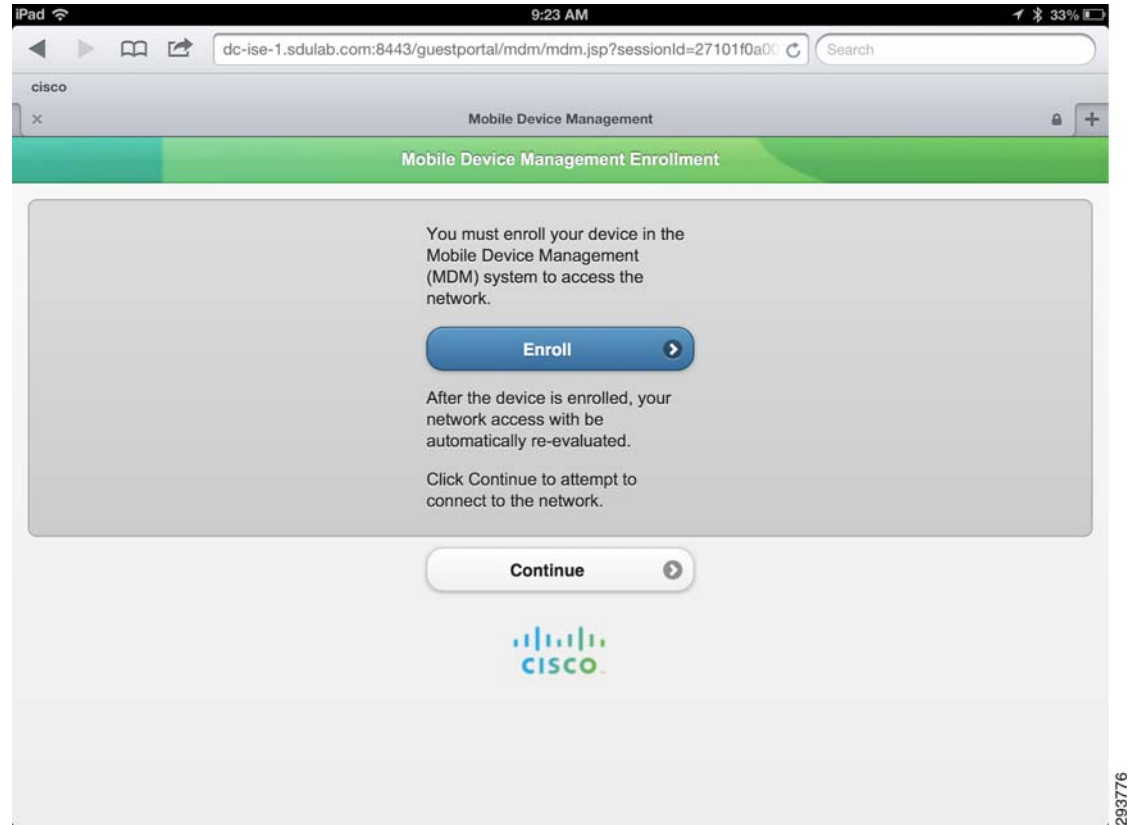


#### **Note**

The access list shown in [Example 17-2](#) is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

The first time the user tries to browse an internal resource, the session is redirected to a page similar to the one in [Figure 17-10](#) providing a link to register with the appropriate MDM.



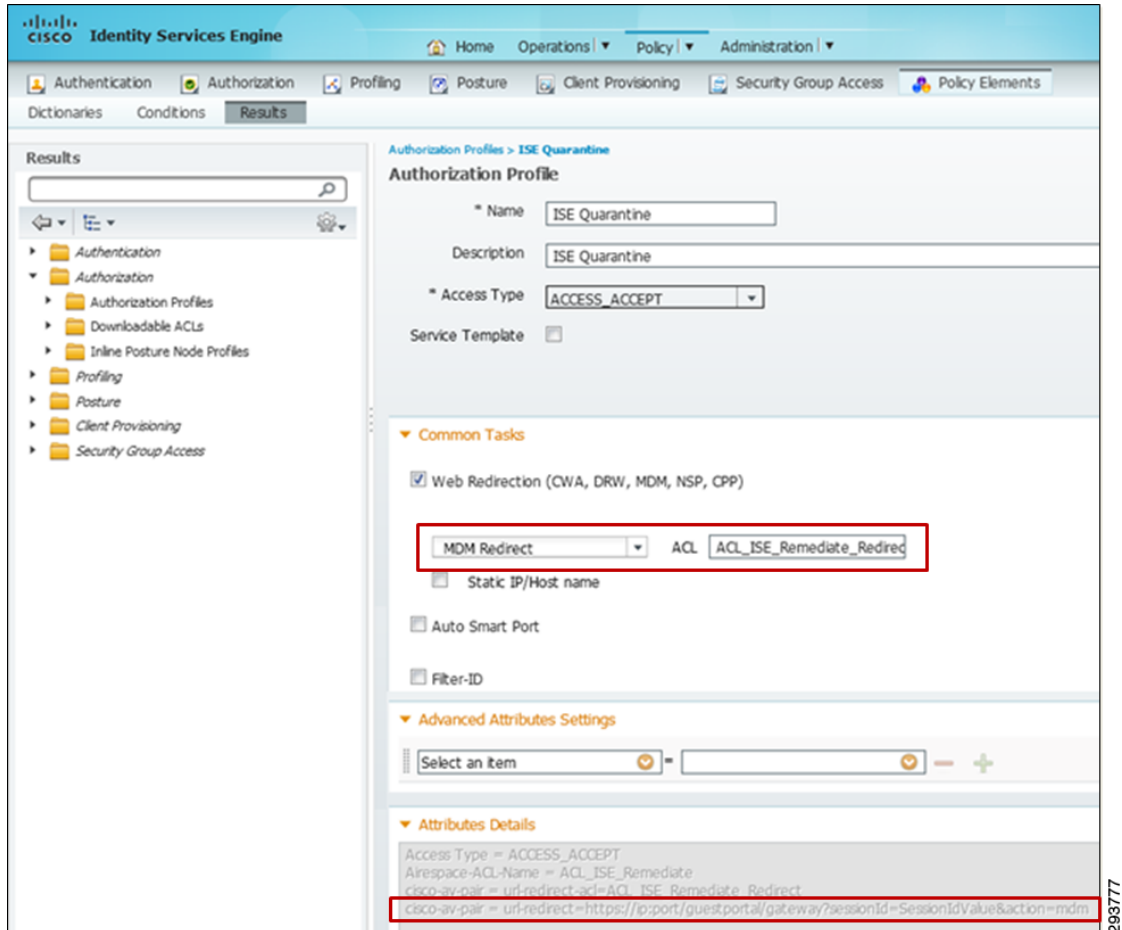
**Figure 17-10 Register with MDM**

## Remediate Non-ISE Compliant Rule

This rule matches when the following conditions are met:

- The connection originated using EAP-TLS authentication (defined as a compound condition, see below).
- The device does not comply with ISE requirements. The ISE\_Non\_Compliant compound condition is highlighted in [Figure 17-5](#).
- Logical Profile equals MDM Managed—The device is managed and supported by the MDM and is shown in [Figure 17-6](#).
- If these conditions match, the ISE Quarantine authorization profile is used. This profile is configured to redirect nonregistered devices to the redirect URL highlighted in [Figure 17-11](#).

Figure 17-11 ISE Quarantine Authorization Profile



The authorization profile relies on two named ACLs, previously defined in the Wireless LAN Controller: ACL\_ISE\_Remediate\_Redirect and ACL\_ISE\_Remediate. ACL\_ISE\_Remediate\_Redirect is shown as being applied to the MDM Redirect setting in Figure 17-11. ACL\_ISE\_Remediate is shown as being sent to the wireless controller via the Radius:Airespace-ACL-Name attribute value (AV) pair in Figure 17-11. The behavior of the two ACLs is slightly different between CUWN wireless controllers, such as the CT5508 and Flex 7500, and IOS XE based controllers such as the CT5760 and Catalyst 3850.

For CUWN wireless controllers, ACL\_ISE\_Remediate\_Redirect functions as both the ACL which controls web redirection, as well as the ACL which controls what the wireless client is allowed to access on the network. ACL\_ISE\_Remediate serves simply as a extra security configuration. CUWN wireless controllers do not make use of this ACL when URL redirection is specified.

For CUWN wireless controllers the ACL\_ISE\_Remediate and ACL\_ISE\_Remediate\_Redirect ACLs can be the same. An example of the ACL\_ISE\_Remediate ACL is shown in Figure 17-12.

**Figure 17-12 ACL\_ISE\_Remediate**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK								
Access Control Lists > Edit								
General								
Access List Name		ACL_ISE_Remediate						
Deny Counters		0						
Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
<a href="#">1</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
<a href="#">2</a>	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">3</a>	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
<a href="#">4</a>	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">5</a>	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
<a href="#">6</a>	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
<a href="#">7</a>	Permit	0.0.0.0	/ 0.0.0.0	203.0.113.10	/ 255.255.255.255	Any	Any	Any
<a href="#">8</a>	Permit	203.0.113.10	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">9</a>	Permit	0.0.0.0	/ 0.0.0.0	23.0.0.0	/ 255.0.0.0	Any	Any	Any
<a href="#">10</a>	Permit	23.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">11</a>	Permit	0.0.0.0	/ 0.0.0.0	17.0.0.0	/ 255.0.0.0	Any	Any	Any
<a href="#">12</a>	Permit	17.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">13</a>	Permit	0.0.0.0	/ 0.0.0.0	184.0.0.0	/ 255.0.0.0	Any	Any	Any
<a href="#">14</a>	Permit	184.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">15</a>	Permit	0.0.0.0	/ 0.0.0.0	8.0.0.0	/ 255.0.0.0	Any	Any	Any
<a href="#">16</a>	Permit	8.0.0.0	/ 255.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">17</a>	Permit	0.0.0.0	/ 0.0.0.0	173.194.0.0	/ 255.255.0.0	Any	Any	Any
<a href="#">18</a>	Permit	173.194.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">19</a>	Permit	0.0.0.0	/ 0.0.0.0	74.125.0.0	/ 255.255.0.0	Any	Any	Any
<a href="#">20</a>	Permit	74.125.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">21</a>	Permit	0.0.0.0	/ 0.0.0.0	206.111.0.0	/ 255.255.0.0	Any	Any	Any
<a href="#">22</a>	Permit	206.111.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
<a href="#">23</a>	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

293778

The 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).
- Allow IP access to and from the MDM server (203.0.113.10).
- Allow IP access to Apple Push Notification Server (23.0.0.0 /8 and 17.0.0.0 /8).
- Allow IP access to Google Cloud Messaging (184.0.0.0 /8, 8.0.0.0 /8, 173.194.0.0 /16, 74.125.0.0 /16, 206.111.0.0 /16).
- Deny IP access (redirect) to all other IP addresses.

**Note**

The ACL behavior has changed in version 7.5+ of the Wireless LAN Controller. The presence of an Airespace ACL Name in the authorization profile affects the webauth redirect functionality for access points operating in FlexConnect mode.

For FlexConnect deployments, the ACL\_Provisioning Airespace ACL must be removed from the configuration. This implies that there needs to be two independent authorization profiles for provisioning: one for FlexConnect and CUWN wireless controllers and another one for and Converged Access wireless controllers.

Refer to [Appendix E, “Airespace ACLs in WLC 7.5+”](#) for sample configurations.

For Cisco IOS XE based wireless controllers, ACL\_Internet\_Redirect functions strictly as the ACL which controls web redirection. ACL\_Internet\_Only 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. An example of the ACL\_Internet\_Redirect ACL for Cisco IOS XE based wireless controllers is shown in [Example 17-3](#).

**Example 17-3 Remediate Redirect ACL for IOS XE Controllers**

```
!
ip access-list extended ACL_ISE_Remediate_Redirect
deny  udp any eq bootpc any eq bootps
deny  ip any host 1.230.1.45
deny  ip any host 1.225.49.15
deny  ip any host 1.230.1.76
deny  ip any 63.128.76.0 0.0.0.255
deny  ip any 23.0.0.0 0.255.255.255
deny  ip any 17.0.0.0 0.255.255.255
deny  ip any 184.0.0.0 0.255.255.255
deny  ip any 8.0.0.0 0.255.255.255
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
deny  ip any host 1.225.100.10
permit ip any any
!
```

The above ACL specifies the following access:

- Deny (do not redirect) DHCP traffic.
- Deny IP access (do not redirect) to and from the DNS server (1.230.1.45).
- Deny IP access (do not redirect) to and from the ISE server (1.225.42.15).
- Deny IP access (do not redirect) to and from MDM servers (host 1.230.1.76 and subnet 63.128.76.0 /24).
- Deny IP access (do not redirect) to Apple Push Notification Server (23.0.0.0 /8 and 17.0.0.0 /8).
- Deny IP access (do not redirect) to Google Cloud Messaging (184.0.0.0 /8, 8.0.0.0 /8, 74.125.0.0 /16, 173.194.0.0 /16, 206.111.0.0 /16).
- Permit IP access (redirect) traffic to all other IP addresses.

An example of the ACL\_ISE\_Remediate ACL for Cisco IOS XE based wireless controllers is shown in [Example 17-4](#).

**Example 17-4 Remediate Access ACL for Cisco IOS XE Controller**

```
!
ip access-list extended ACL_ISE_Remediate
permit udp any eq bootpc any eq bootps
permit ip any host 1.230.1.45
permit ip any host 1.225.49.15
permit ip any host 1.230.1.76
permit ip any 63.128.76.0 0.0.0.255
permit ip any 23.0.0.0 0.255.255.255
permit ip any 17.0.0.0 0.255.255.255
permit ip any 184.0.0.0 0.255.255.255
permit ip any 8.0.0.0 0.255.255.255
permit ip any 74.125.0.0 0.0.255.255
```

```

permit ip any 173.194.0.0 0.0.255.255
permit ip any 206.111.0.0 0.0.255.255
deny ip any any
!

```

The above access-list specifies the following access:

- Allow DHCP traffic.
- Allow IP access to and from the DNS server (1.230.1.45).
- Allow IP access to and from the ISE server (1.225.42.15).
- Allow IP access to and from MDM servers (host 1.230.1.76 and subnet 63.128.76.0 /8).
- Allow IP access to Apple Push Notification Server (23.0.0.0 /8 and 17.0.0.0 /8).
- Allow IP access to Google Cloud Messaging (184.0.0.0 /8, 8.0.0.0 /8, 74.125.0.0 /16, 173.194.0.0 /16, 206.111.0.0 /16).
- Permit IP access to all other IP addresses.



#### Note

The access list shown in [Example 17-4](#) is generic and not intended to work for every organization. An ACL should be more specific and only allow access to specific IP addresses and protocols in the required direction. A common practice is to make the ACLs as detailed as possible and to define every entry down to the port level.

The Wireless\_EAP-TLS compound condition checks for the following conditions:

- Radius:Service-Type Equals Framed
- Radius:NAS-Port-Type Equals Wireless - IEEE 802.11
- Network Access:EapAuthentication Equals EAP-TLS

To define this compound condition, click **Policy > Conditions > Authorization > Compound Conditions**. [Figure 17-13](#) shows how the Wireless\_EAP-TLS condition combines several conditions into one.

**Figure 17-13** *Wireless\_EAP-TLS Condition*

The screenshot displays the Cisco Identity Services Engine (ISE) configuration page for the 'Wireless\_EAP-TLS' compound condition. The interface includes a top navigation bar with tabs for Home, Operations, Policy, and Administration. Below this is a sub-navigation bar with tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The main content area is divided into two sections: 'Authorization' on the left and 'Authorization Compound Condition List' on the right. The 'Authorization' section shows a search bar and a list of conditions, including 'Simple Conditions' and 'Compound Conditions'. The 'Authorization Compound Condition List' section shows the configuration for the 'Wireless\_EAP-TLS' condition. It includes a search bar, a list of conditions, and a table for defining the compound condition. The table has columns for 'Condition Name', 'Expression', and 'AND/OR'. The conditions are defined as follows:

Condition Name	Expression	AND/OR
Radius:Service-Type	Equals Framed	AND
Radius:NAS-Port-Type	Equals Wireless - IEEE 802.11	AND
Network Access:EapAuthentication	Equals EAP-TLS	AND

The 'Save' and 'Reset' buttons are located at the bottom of the configuration area.

## Remediate Non-MDM Compliant Rule

This rule matches when the following conditions are met:

- The connection originated using EAP-TLS authentication, as defined by the Wireless\_EAP-TLS compound condition highlighted in [Figure 17-13](#).
- The device does not comply with MDM policies. The ISE makes the DeviceCompliantStatus API call to the MDM to obtain this information.
- Logical Profile equals MDM Managed—The device is managed and supported by the MDM.

If these conditions match, the MDM Quarantine authorization profile is used. This profile is configured to redirect nonregistered devices to the redirect URL highlighted in [Figure 17-14](#).

**Figure 17-14** MDM Quarantine Authorization Profile

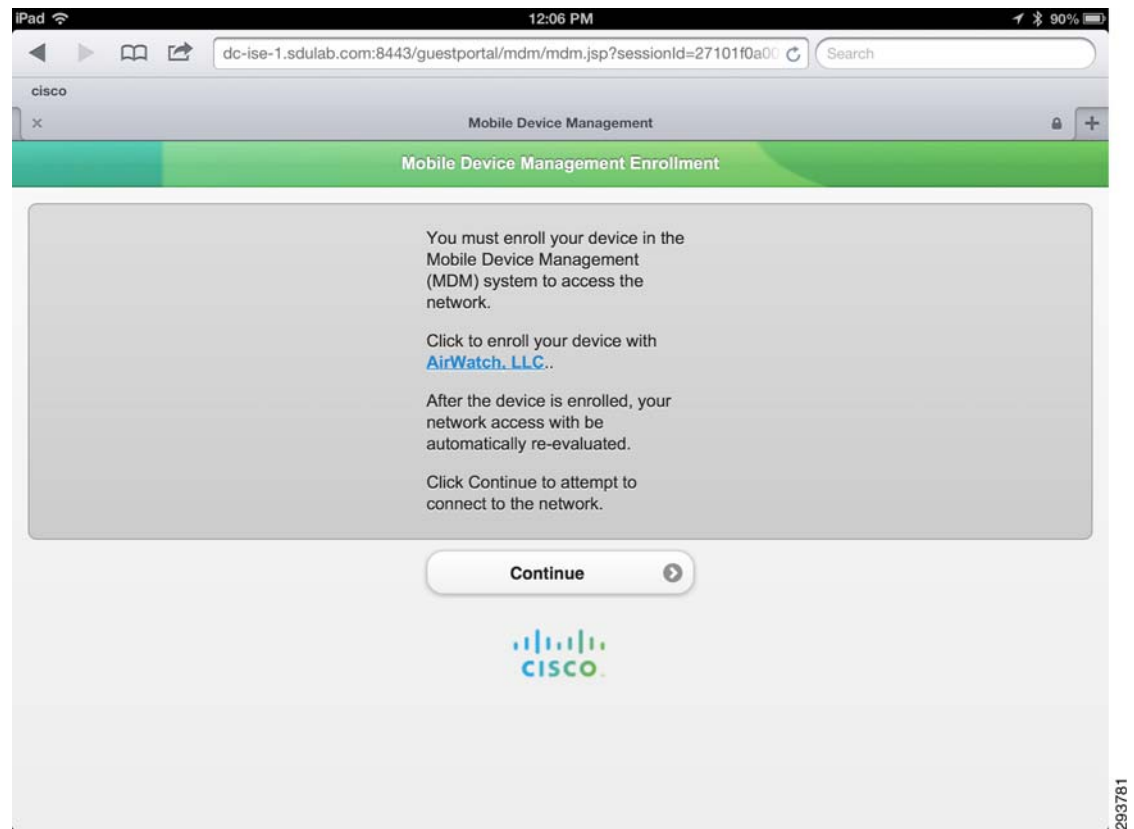
The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for the 'MDM Quarantine' authorization profile. The left sidebar shows the navigation tree with 'Authorization' selected. The main content area shows the profile configuration details:

- Name:** MDM Quarantine
- Description:** (empty)
- Access Type:** ACCESS\_ACCEPT
- Service Template:** (unchecked)
- Common Tasks:**
  - ☒ Web Redirection (CWA, DRW, MDM, NSP, CPP)
  - MDM Redirect:** ACL\_Internet\_Redirect
  - ☐ Static IP/Host name
  - ☐ Auto Smart Port
- Advanced Attributes Settings:**
  - Select an item = [dropdown] = [dropdown] +
- Attributes Details:**

```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = ACL_Internet_Only
cisco-av-pair = url-redirect-ad=ACL_Internet_Redirect
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionId&value&action=mdm
```

The authorization profile relies on the same two named ACLs: ACL\_Internet\_Redirect and ACL\_Internet\_Only previously discussed in [Remediate Non-ISE Compliant Rule](#).

When the user tries to browse an internal resource, the session is redirected to page similar to the one in [Figure 17-15](#), indicating why the device is not compliant with the MDM policies.

**Figure 17-15 MDM Quarantine**

For reference purposes, the complete authorization policy used during testing is shown in [Figure 17-16](#). The figure highlights the following sections:

1. Used for blacklisting lost or stolen devices.
2. On-boarding and MDM registration/remediation.
3. Wireless devices connecting from an access point in a SGT\_Enabled location.
4. Wireless devices connecting from an access point in the campus or branch locations.
5. Wired devices connecting from a campus or branch locations.
6. Wired and Wireless devices connecting from a converged location.
7. Guest and Basic Access.



Figure 17-16 Complete 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
1	Wireless Black List Default ISE	Blacklist AND Wireless_Access	then Blackhole WiFi Access
	Wired Black List Default	Blacklist AND Wired_Access	then Blackhole Wired Access
	MDM Enrollment	(Wireless_EAP-TLS AND ISE_Registered AND MDM_UnRegistered AND MDM_Managed AND MDM_Operational)	then Internet Until MDM
	Dual SSID Provisioning	(Wireless_MAB AND Provisioning_WLAN)	then Wireless CWA
2	Single SSID Provisioning	(Wireless_PEAP AND Employee_WLAN)	then Wireless NSP
	Remediate Non ISE Compliant	(Wireless_EAP-TLS AND ISE_NonCompliant AND MDM_Managed AND MDM_Operational)	then ISE Quarantine
	Remediate Non MDM Compliant	(Wireless_EAP-TLS AND MDM_NonCompliant AND MDM_Managed AND MDM_Operational)	then MDM Quarantine
	SGTCampus Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller)	then SGT10_Campus_Corp AND PermitAccess
	SGTCampus Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Full_Access)	then SGT11_Campus_Pers_Full AND PermitAccess
	SGTCampus Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Partial_Access)	then SGT12_Campus_Pers_Partial AND PermitAccess
	SGTCampus Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND SGT_Controller AND AD_Domain_Users)	then Campus WiFi Internet Only
	Campus Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Campus_Controller)	then Campus WiFi Full Access
	Campus Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND Campus_Controller AND AD_Full_Access)	then Campus WiFi Full Access
	Campus Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Campus_Controller)	then Campus WiFi Partial Access
	Campus Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Campus_Controller)	then Campus WiFi Internet Only
	Branch Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Branch_Controller)	then Branch WiFi Full Access
	Branch Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND Branch_Controller AND AD_Full_Access)	then Branch WiFi Full Access
	Branch Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Branch_Controller)	then Branch WiFi Partial Access
	Branch Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Branch_Controller)	then Branch WiFi Internet Only
	Campus Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Campus_Switches)	then Campus Wired Full Access
	Campus Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND Campus_Switches AND AD_Full_Access)	then Campus Wired Full Access
	Campus Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Campus_Switches)	then Campus Wired Partial Access
	Campus Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Campus_Switches)	then Campus Wired Internet Only
	Branch Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Branch_Switches)	then Branch Wired Full Access
	Branch Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Branch_Switches)	then Branch Wired Full Access
	Branch Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Branch_Switches)	then Branch Wired Partial Access
	Branch Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Branch_Switches)	then Branch Wired Internet Only
	Converged Wifi Corporate Full	Whitelist AND (Wireless_EAP-TLS AND Valid_Certificate AND Converged_Access)	then Converged WiFi Full Access
	Converged Wifi Personal Full	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Converged_Access)	then Converged WiFi Full Access
	Converged Wifi Personal Partial	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Converged_Access)	then Converged WiFi Partial Access
	Converged Wifi Personal Internet	(Wireless_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Converged_Access)	then Converged WiFi Internet Only
	Converged Wired Corporate Full	Whitelist AND (Wired_EAP-TLS AND Valid_Certificate AND Converged_Access)	then Converged Wired Full Access
	Converged Wired Personal Full	(Wired_EAP-TLS AND Valid_Certificate AND AD_Full_Access AND Converged_Access)	then Converged Wired Full Access
	Converged Wired Personal Partial	(Wired_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Converged_Access)	then Converged Wired Partial Access
	Converged Wired Personal Internet	(Wired_EAP-TLS AND Valid_Certificate AND AD_Domain_Users AND Converged_Access)	then Converged Wired Internet Only
	Wifi Guest	(WLC_Web_Authentication AND Guest_WLAN)	then PermitAccess
	Wifi Basic Access	(Wireless_PEAP AND Personal_Device_WLAN)	then PermitAccess

293782



# MDM Reports

Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting. Several reports provide information related to endpoints. In [Figure 17-17](#), the Mobile Device Management report shows the endpoints connected to the ISE, and several attributes collected from the MDM. Other reports provide additional information that may be used for reporting and troubleshooting.

**Figure 17-17** MDM Report

**Mobile Device Management**

From 02/22/2013 05:24:08 AM to 02/22/2013 05:24:07 PM

Endpoint ID	Endpoint OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer	Model
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✓	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✓	✓	✓	✓	Apple	iPad
68-96-7B-01-2E-11	iOS 6.1.2	✓	✓	✓	✓	✓	Apple	iPhone
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✓	✓	✓	✓	Apple	iPad
68-96-7B-01-2E-11	iOS 6.1.2	✓	✓	✓	✓	✓	Apple	iPhone
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
68-96-7B-01-2E-11	iOS 6.1.2	✓	✓	✓	✓	✓	Apple	iPhone
68-96-7B-01-2E-11	iOS 6.1.2	✓	✓	✓	✓	✓	Apple	iPhone
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
68-96-7B-01-2E-11	iOS 6.1.2	✓	✓	✓	✓	✓	Apple	iPhone
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
68-96-7B-01-2E-11	iOS 6.1.2	✓	✓	✓	✓	✓	Apple	iPhone
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad
1C-AB-A7-B4-85-12	iOS 6.0.0	✓	✗	✓	✓	✓	Apple	iPad

293783





## BYOD Basic Access Use Case

**Revised: August 7, 2013**

Previous chapters of this design guide have examined on-boarding employee personal devices to provide full, partial, or Internet only access. The use of digital certificates provides an additional level of authentication security by preventing the spoofing of device MAC addresses. Additionally, the use of the guest portal for self-registration and the My-Devices portal streamline the on-boarding and maintenance of employee personal devices, resulting in lower IT operating costs associated with providing BYOD services.

Despite these benefits, a subset of organizations may still decide on a business policy which does not on-board wireless employee personal devices, yet provides some access to corporate services and the Internet for such devices. This may be because of one or more of the following reasons:

- The organization does not have the desire or the ability to deploy digital certificates on employee personal devices.
- The employee may decide to opt-out of having the organization manage their personal device.
- The organization does not wish to administratively manage and maintain separate lists of registered corporate devices and BYOD devices which have full network access.
- The organization may wish to simply restrict employee personal devices to “outside” of the corporate firewall due to an unknown or un-trusted security posture of such devices.

Because of this, the following sections discuss design options for wireless employee personal devices which do not involve on-boarding such devices. The designs are based around extending traditional guest wireless access discussed in [Chapter 21, “BYOD Guest Wireless Access”](#) and providing similar guest-like wireless access for employee personal devices.



**Note**

Throughout this chapter, it is assumed that corporate-owned devices will still be on-boarded as discussed in [Chapter 16, “BYOD Limited Use Case—Corporate Devices.”](#) The use of a whitelist is still necessary to prevent employee personal devices from getting full access to the corporate network.

## Extending Guest Wireless Access to Employee Personal Devices

The following sections discuss two methods for extending guest wireless access, discussed in [Chapter 21, “BYOD Guest Wireless Access,”](#) to also allow employee personal devices access to the guest network:

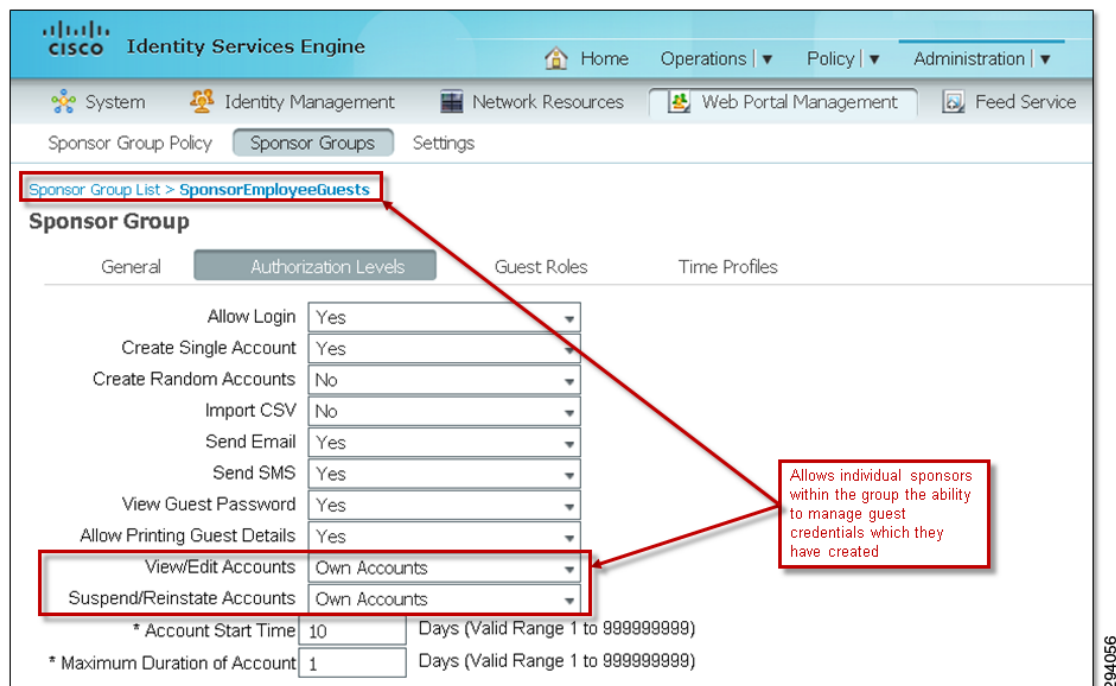
- Allowing employees to provision guest credentials for themselves.
- Extending guest web authentication (Web Auth) to also utilize the Microsoft Active Directory (AD) database when authenticating guests and employees using personal devices.

## Allowing Employees to Provision Guest Credentials for Themselves

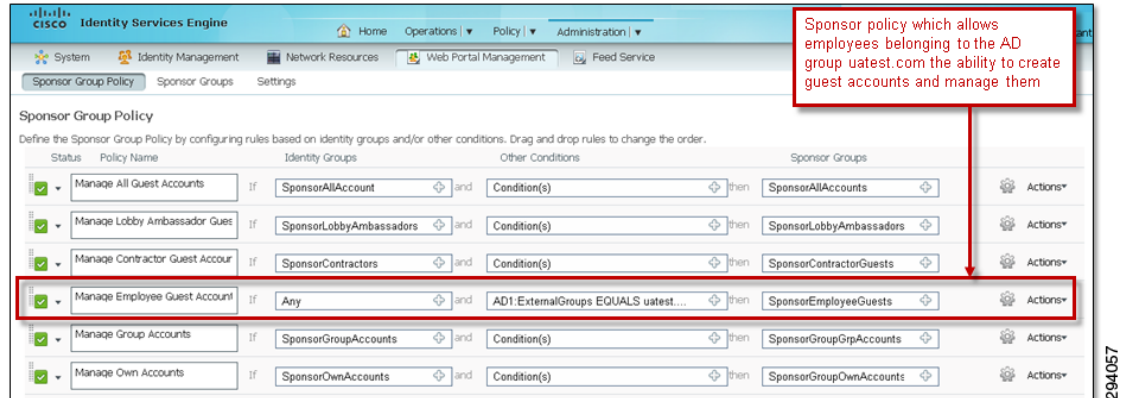
Chapter 21, “BYOD Guest Wireless Access,” discusses provisioning guest credentials with the Cisco ISE sponsor portal. The most basic form of extending guest wireless access to employee personal devices is simply to allow employees to sponsor themselves as guests. Employees then manually connect to the open guest SSID to utilize personal devices on the wireless guest network.

With the Cisco ISE sponsor portal, the sponsor authentication policy can be based on membership within a particular Microsoft AD group. This was discussed in [Configuring the Cisco ISE Sponsor Portal](#), which discussed the use of Microsoft AD groups within the ISE sponsor group policy as a means to limit sponsor access to the Cisco ISE server. This can equally be used to allow broader access to the ISE sponsor portal simply by adding additional employees to those Microsoft AD groups. Alternatively a new sponsor group can be created that allows individual employees to configure guest credentials yet restricts them to being able to only modify credentials that they provisioned. An example is shown in the figures below.

**Figure 18-1** Example ISE Sponsor Group for Employees to Create Self Guest Credentials



Membership to this ISE sponsor group can then be restricted to a Microsoft AD group via the ISE sponsor group policy, as shown in [Figure 18-2](#).

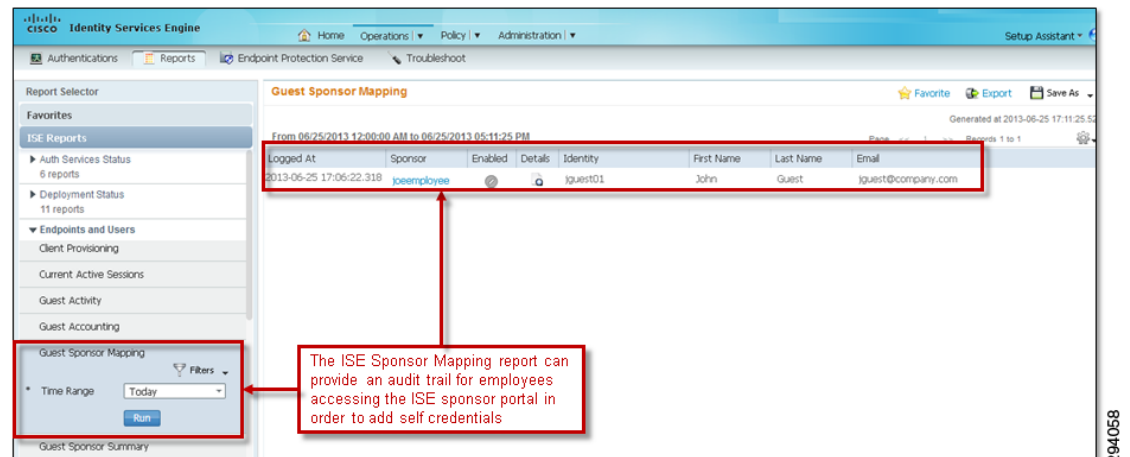
**Figure 18-2 Example ISE Sponsor Group Policy for Employees to Create Self Guest Credentials**

In this example, access to the sponsor group is limited to those members of the Microsoft Active Directory domain who are members of the group “Users/Domain Users”. The exact condition for the example is of the form:

```
AD1:ExternalGroups EQUALS uatest.com/Users/Domain Users
```

The Microsoft Active Directory domain is “uatest.com” in this example. Note that the Microsoft Active Directory server must be configured as an external identity source to select this option. In this example it is known by the name “AD1”.

One advantage of this design is that an audit trail exists through the ISE Reports for employees authenticating to the ISE sponsor portal. The ISE Sponsor Mapping report shows when the employee created a guest credential as well as the guest credential created. The ISE Sponsor Mapping report can be run over various time ranges from 30 minutes up to 30 days or a custom time range can be requested. This report can be used to gain a rough idea of which employees are accessing the ISE sponsor portal to create guest credentials and how often. An example is shown in Figure 18-3.

**Figure 18-3 Example of the Audit Trail for an Employee Accessing the ISE Sponsor Portal**

Note that this method of allowing employees the ability to create guest credentials for themselves does not prevent them from creating credentials for true guests who are visiting the organization. Corporate business policy should dictate that true guest credentials only be added by authorized members of sponsor groups, as discussed in Chapter 21, “BYOD Guest Wireless Access.” The next design option

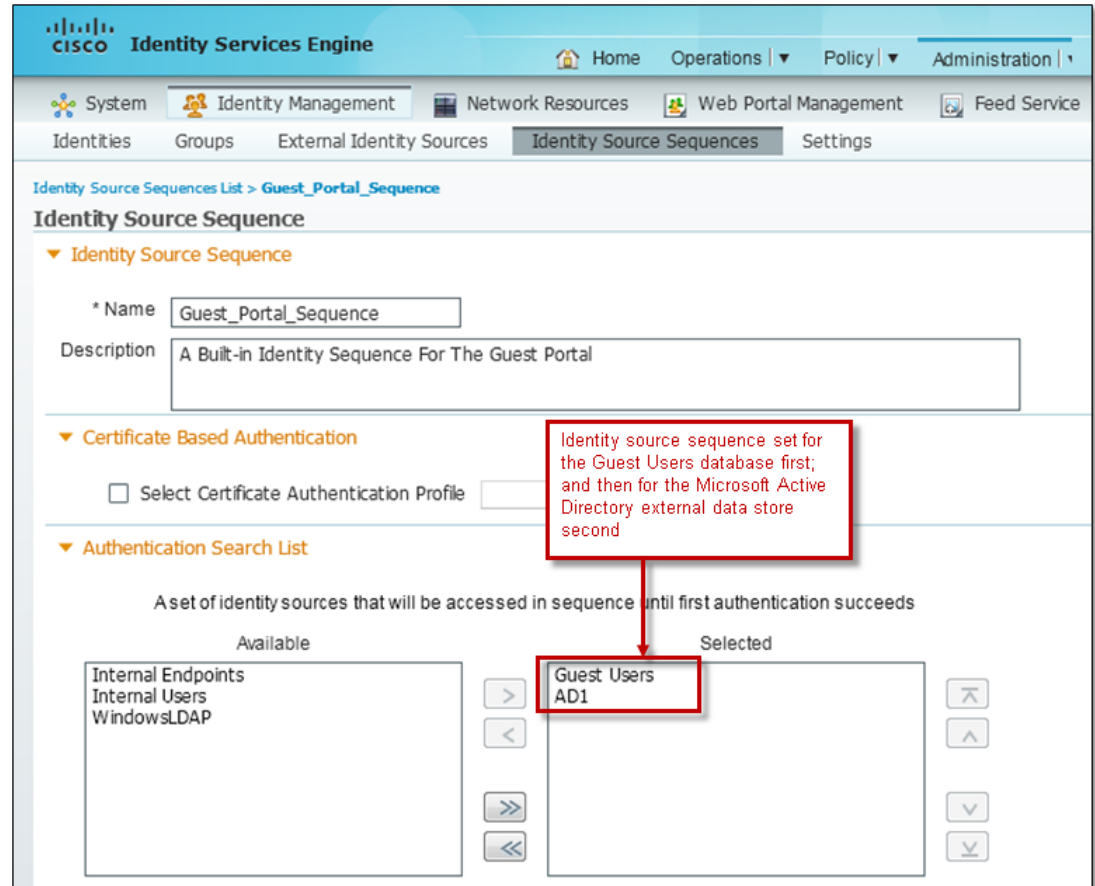
eliminates this issue by removing the ability for employees to create guest credentials for themselves altogether.

## Extending Web Auth to Use Microsoft AD when Authenticating Employees with Personal Devices

The previous section discussed the most basic way of extending guest wireless access to allow employees with personal devices to access the guest network. That method simply allows employees to configure guest credentials for themselves via the Cisco ISE sponsor portal. Although this provides several advantages over methods such as utilizing a shared sponsor account on the guest wireless controller for adding credentials, it still has several shortcomings. Employees must still provision temporary guest credentials for themselves. Finally, there is nothing preventing the employee from sponsoring a true guest, other than corporate business policy.

An alternative means of providing access to the guest wireless network for employee personal devices is to simply allow the ISE server to check multiple identity sources for credentials when performing web authentication (Web Auth). For example, the ISE server could first check its internal identity groups (local database) for guest credentials. If the credentials are not found there, then check the Microsoft AD external identity store to see if the person accessing the guest network is an employee instead of a guest.

[Cisco ISE Policy Configuration](#) in [Chapter 21, “BYOD Guest Wireless Access”](#) discusses the use of a user-defined identity source sequence called `Guest_Portal_Sequence` for authenticating guest access via Web Auth. The `Guest_Portal_Sequence` uses the Internal Users identity source only. This can easily be extended by adding a Microsoft Active Directory (AD1) external identity source to the sequence, as shown in [Figure 18-4](#).

**Figure 18-4** Example of Guest\_Portal\_Access Identity Source Sequence Extended to Include AD

This configuration now allows employees who are in the Microsoft Active Directory database to access the guest wireless network from their personal devices once they have performed web authentication and accepted the Acceptable Use Policy (AUP) or End User Agreement (EUA).

**Note**

This allows employees to access the guest wireless network from corporate-owned devices as well, since the authentication and authorization decision is based on Microsoft Active Directory userid and password only. The device itself is not considered within the authentication and authorization decision.

## Deploying Guest-Like Wireless Access for Employee Personal Devices

The previous sections discussed options for extending access to the wireless guest network for employees with personal devices, either by allowing employees to configure guest credentials for themselves or by extending Web Auth to also check the Microsoft AD database where employee credentials are kept. With these options, employee personal devices share the same wireless SSID as guest devices. Employee personal devices also share the same IP subnet address space as guest devices, since they terminate on the same DMZ segment of the ASA firewall. Essentially the employee's personal device is treated as a guest on the network, which can bring up potential concerns.



Since IP subnet space is shared between guest devices and employee personal devices, there can be some concern that employee personal devices could deplete the IP addressing space, limiting the ability of guest devices to gain access to the guest network or vice-versa.

The ASA firewall guest DMZ interface ingress policy can be modified to allow certain application flows inbound from the guest network to a mirror of the company website server, dedicated for employee personal devices, sitting on other DMZ segments. This is discussed further in [Accessing Corporate Resources](#). However, the ASA firewall policy would not be able to distinguish between guest devices and employee personal devices, since they share the same IP subnet address space. Therefore, application level access control at the mirror web server itself is necessary to prevent guests from accessing services on it. Likewise, the ASA firewall guest DMZ interface ingress policy could be modified to allow traffic from a virtual client—such as a Citrix or VMware client—inbound to internal Citrix or VMware servers. Again, the ASA firewall policy would not be able to distinguish between true guest devices and employee personal devices, since they share the same IP subnet address space. Application level access control at the Citrix or VMware server would be necessary to prevent guests from accessing these servers.

Since the guest SSID is typically open with no encryption, traffic from employee personal devices will be in the clear, unless the devices use either secure applications or some form of VPN tunneling, which encrypts the traffic. Although web traffic can be made secure simply by requiring the use of HTTPS, not all applications used by employee personal devices may be encrypted. This leaves some vulnerability which must be considered by security operations personnel, especially any site that authenticates using the employee's corporate login and password. If internal company data is being accessed from employee personal devices via the guest wireless network, then that information should be encrypted to prevent eavesdropping. Allowing employee devices to launch a VPN client to establish an IPsec VPN session—either directly to the ASA firewall or out to the Internet and back to another corporate VPN concentrator—may be one alternative. Another option is the establishment of an SSL VPN tunnel to the ASA firewall for employee devices. Both of these options may also require per-user authentication.

**Note**

---

Cisco's implementation of Web Auth uses HTTPS when redirecting the web session and requesting credentials.

---

Because of these concerns, security operations personnel may be hesitant to allow anything but Internet access for any device accessing the guest network, whether it is a true guest device or an employee personal device.

As in [Chapter 21, "BYOD Guest Wireless Access,"](#) two distinct terminologies are used in this chapter. The first pair of terminologies is guest controller and campus controller. The guest controller is a dedicated controller that is used for dealing with guest and employee personal device traffic. The campus controller is dedicated for handling internal traffic. Note that the term campus controller is used somewhat generically here. The campus controller discussed within this chapter may refer to a standalone wireless controller platform deployed within a campus location or wireless controller functionality integrated within Catalyst 3850 Series switches deployed within a branch location.

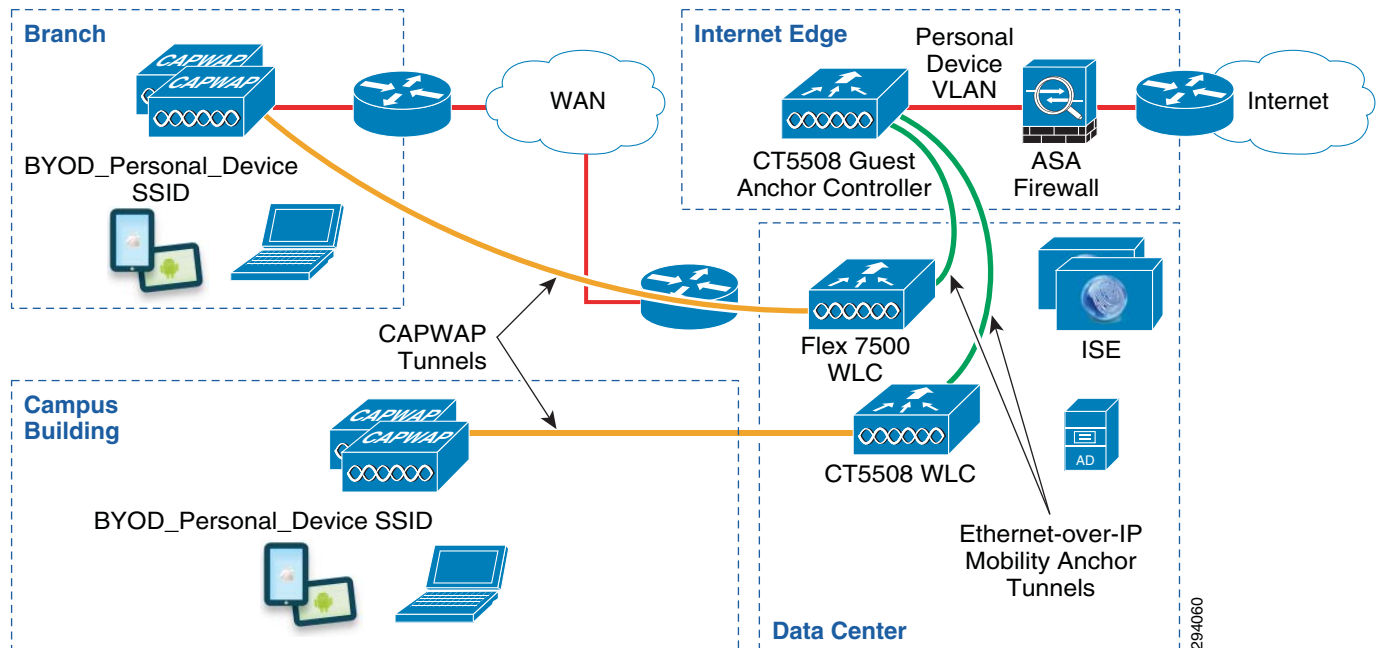
The second set of terminologies is foreign controller and anchor controller. These two terminologies are used when a user roams from one controller to another controller. The new controller to which the user associates is the foreign controller. This controller anchors all the traffic to the old controller, which becomes the anchor controller. These terminologies are used in this document.



## Dedicated SSID for Employee Personal Devices

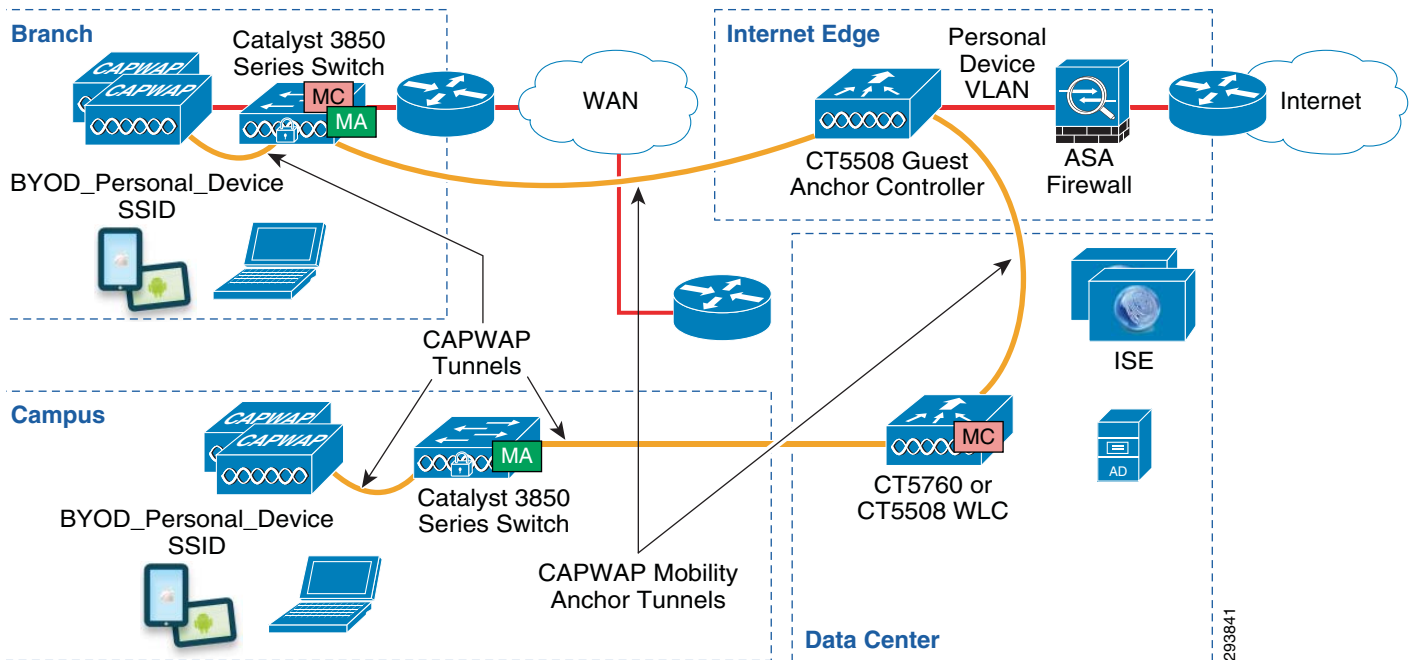
This section discusses another option in which a second guest-like wireless SSID is provisioned for employee personal devices. This SSID is auto-anchored to another DMZ segment off of the ASA firewall, in a similar fashion as the wireless guest SSID. An example of this design using CUWN infrastructure is shown in [Figure 18-5](#).

**Figure 18-5** Guest-Like Wireless Access for Employee Personal Devices Using CUWN Infrastructure



With the auto-anchor mobility feature of Cisco wireless controllers, packets from the wireless client are encapsulated through a mobility tunnel between the internal wireless controller (known as the foreign controller) to the guest wireless controller (known as the anchor controller), where they are de-capsulated and delivered to the wired network.

A similar example of this design using a Converged Access wireless infrastructure is shown in [Figure 18-6](#).

**Figure 18-6** Guest-Like Wireless Access for Employee Personal Devices Using Converged Access Infrastructure

The auto-anchor mobility feature also applies to the Converged Access Infrastructure. Note that with the Converged Access branch design shown in [Figure 18-6](#), the Catalyst 3850 switch within the branch implements both the Mobility Agent (MA) and Mobility Controller (MC) function. With the Converged Access campus design, the Catalyst 3850 switch only implements the MA function. The MC function is implemented by a dedicated CT5760 wireless controller. Since the auto-anchor tunnel is initiated from the MC within a Converged Access design, traffic is first tunneled from the campus Catalyst 3850 switch to the CT5760 wireless controller, where it is then auto-anchored to the guest anchor controller within the DMZ. For additional discussion regarding the MA and MC functionality within Converged Access infrastructure, see [Configuring the Infrastructure](#).

**Note**

In this version of the design guide, it is assumed that employees with personal devices would need to manually associate with this SSID. Future versions may investigate other alternatives that make use of RADIUS change-of-authentication (CoA) functionality or device profiles.

An advantage of implementing a dedicated SSID for employee personal devices is that the SSID does not have to be configured with open access and can be encrypted, unlike the guest SSID discussed throughout this design guide. Instead, the employee personal device SSID can be secured via mechanisms such as 802.1X authentication and WPA-2/AES encryption to prevent eavesdropping of traffic from employee personal devices. Employees can be authenticated via the Cisco ISE server using the external Microsoft AD identity source as they associate with the SSID.

Another advantage of implementing a dedicated SSID for employee personal devices is that the devices can be isolated from guest devices by provisioning separate VLANs for each SSID. Separate DMZ segments—implemented as separate physical interfaces off of the ASA firewall or as separate VLAN sub-interfaces off a single physical interface of the ASA firewall—can be deployed. Each DMZ interface now has a separate IP subnet address space and a separate access-control policy. This expands the IP addressing space deployed for guest devices as well as employee personal devices and removes the issue of employee personal devices causing IP address starvation issues for guest devices and vice-versa. The guest DMZ can be configured to allow only Internet access for guest devices. The employee personal

device DMZ can be configured to allow Internet access, as well as access to a mirror web server sitting on another DMZ segment. Additional access can be allowed by modifying the ASA firewall personal device DMZ interface ingress policy to allow traffic from a virtual client-such as a Citrix or VMware client-inbound to internal Citrix or VMware servers. Access can also be extended by allowing employee personal devices to launch a VPN client to establish an IPsec VPN session, either directly to the ASA firewall or out to the Internet and back to another corporate VPN concentrator. Another option is the establishment of an SSL VPN tunnel to the ASA firewall for employee personal devices.

## Wireless Controller Configuration

To deploy this option in which a second guest-like wireless SSID is provisioned for employee personal devices, both the campus (foreign) wireless controllers and the guest (anchor) controller need to be configured with a new WLAN for employee personal devices. This WLAN has a unique SSID different from the corporate WLAN and the guest WLAN.

### Campus Controller Configuration

This section discusses configurations when using either CUWN wireless controllers or Converged Access (IOS XE based) wireless controllers for the campus controller.

#### CUWN Wireless Controller Configuration

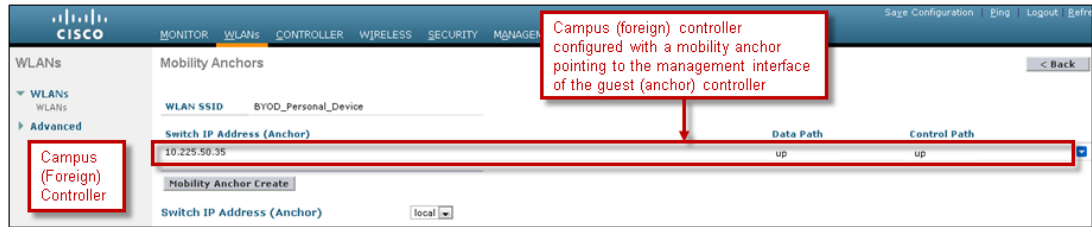
An example of a CUWN campus controller configuration is shown in [Figure 18-7](#), in which the new WLAN is called the BYOD\_Personal\_Device WLAN.

**Figure 18-7** Example Configuration of a CUWN Campus Wireless Controller for the Employee Personal Devices WLAN



The WLAN is configured for WPA2 security with AES as the cipher, along with 802.1X authenticated key management. Next, the WLAN on the campus (foreign) controller needs to be configured with a mobility anchor pointing at the management interface of the guest (anchor) controller. An example is shown in [Figure 18-8](#). Note that in branch scenarios which utilize a FlexConnect wireless design, the controller servicing branch APs will be the foreign controller for the branch personal device WLAN.

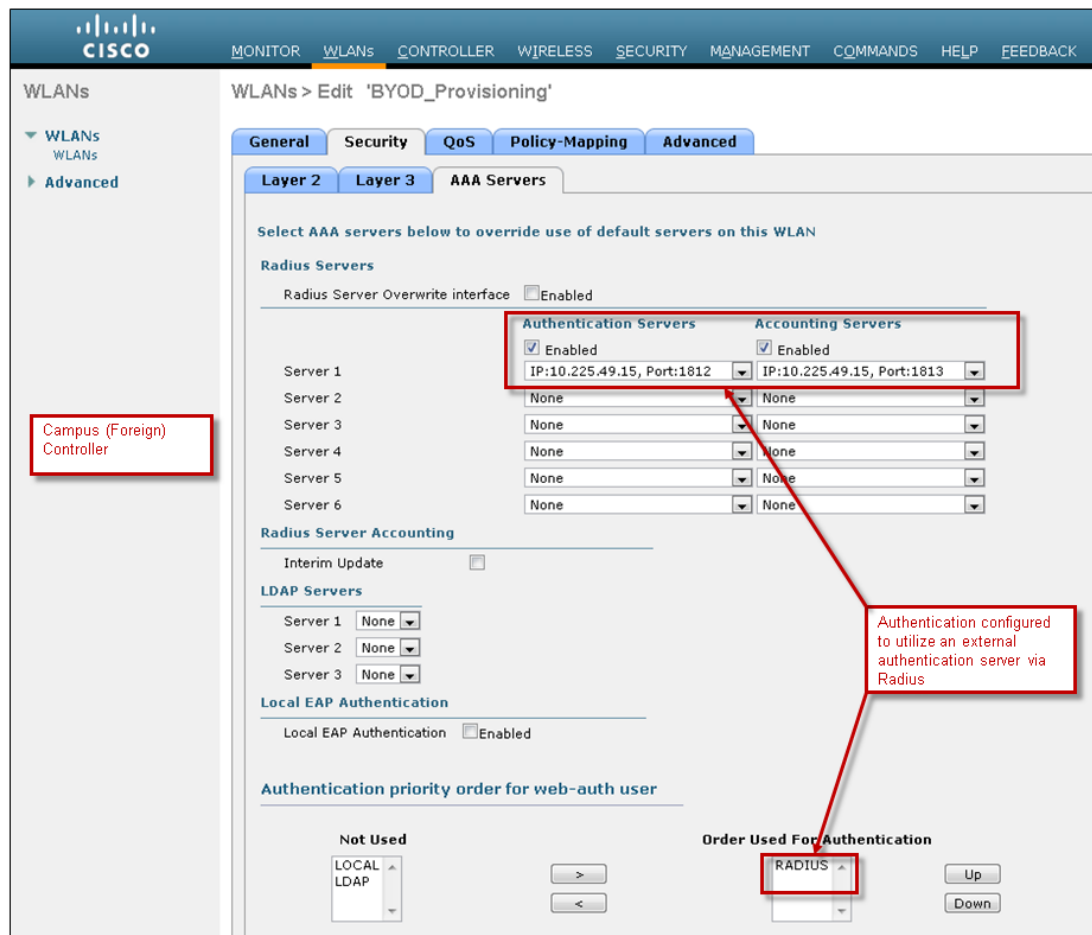
**Figure 18-8** Example Configuration of the Mobility Anchor on a Campus CUWN Wireless Controllers



Note that the campus controller and the guest controller must be part of the same mobility group before the mobility anchor can be configured. The mobility anchors establish the mobility tunnel through which packets from the wireless client are automatically encapsulated and sent from the campus controller to the guest controller where they are de-encapsulated and delivered to the wired network.

The network administrator must also configure the employee personal devices WLAN to use RADIUS within the campus controller for authentication. This is shown in Figure 18-9.

**Figure 18-9** Authentication via RADIUS for the Employee Personal Devices WLAN on the Campus Controller



Since Web Auth is not involved with this option, there is no redirection of web sessions to a guest portal and hence no configuration required within the guest controller for Web Auth or any requirement for a pre-authentication ACL. When an employee personal device connects to the SSID, the RADIUS session is initiated by the campus controller management interface to the Cisco ISE server for authentication and authorization. Upon successful authentication, the employee's personal device is then anchored to the guest controller.

### Converged Access (IOS XE Based) Wireless Controller Configuration

The following partial configuration shows an example of the employee personal devices WLAN along with part of the AAA server configuration on an IOS XE based wireless controller.

```
!
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
!
dot1x system-auth-control
!
ip http server
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 send nas-port-detail
radius-server dead-criteria time 5 tries 3
radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key 7 1237161E060E5D56797F71
!
                                /Radius server in the line above points to ISE
!
wlan BYOD_Personal_Device 4 BYOD_Personal_Device/Defines the personal devices WLAN and
SSID
  client vlan Guest/Static assignment to non-routed (isolated) VLAN
  mobility anchor 10.225.50.35/Creates an anchor tunnel to the guest wireless controller
  session-timeout 1800
  no shutdown /Enables the employee devices WLAN
!
```

By default WPA2 with AES as the cipher is enabled, along with 802.1X authenticated key management. Hence they do not show up in the configuration. The administrative-level **show wlan id <wlan ID number>** command can be used to display additional details regarding the configuration of the WLAN, including default values which do not appear within the configuration.

The employee devices WLAN must be configured on the device which functions as the Mobility Agent (MA) and on the device which functions as the Mobility Controller (MC). Therefore the configuration above is basically the same, regardless of whether a Catalyst 3850 Series switch is deployed as both the MA and MC within a branch deployment, a Catalyst 3850 Series switch is deployed as only an MA within a campus deployment, or a CT5760 wireless controller is deployed as an MA and MC within a campus deployment.

The Guest client VLAN in the configuration above is a VLAN which is isolated on the CT5760 wireless controller or Catalyst 3850 Series switch. It is not trunked to the adjacent Layer 3 device. This isolates any guest devices should the CAPWAP tunnel between the foreign and anchor controllers go down.

The following partial configuration example shows the configuration of the mobility group and mobility group members on an IOS XE based wireless controller.

```
!
wireless mobility group member ip 10.225.50.35 public-ip 10.225.50.35/Guest Controller
wireless mobility group name byod/Mobility group name
!
```

The mobility group name and mobility group peers must appear on the device which functions as the Mobility Controller (MC). Therefore, when a Catalyst 3850 Series switch is deployed as both the MA and MC within a branch deployment, the configuration must include the above two lines. A Catalyst 3850 Series switch deployed as only an MA within a campus deployment would not include the mobility group configuration. Instead the CT5760 wireless controller deployed as a MA and MC within a campus would contain the mobility group configuration. Note that since IOS XE based wireless controllers only support the new hierarchical mobility architecture; no configuration is required to enable it.



#### Note

Cisco wireless controllers currently support two different mobility architectures. The old mobility architecture relies on Ethernet-over-IP tunnels between wireless controllers. The new mobility architecture, also called the hierarchical mobility architecture, relies on CAPWAP tunnels between wireless controllers. The two mobility architectures are not compatible with each other. If mobility (including the auto-anchoring function) is required between wireless controllers, all wireless controllers must be running either the new mobility or the old mobility architecture. The new mobility architecture is supported on Cisco 5508 and WiSM2 wireless controllers with software release 7.3.112 and on the Cisco 5508, WiSM2, and 2504 wireless controllers with software release 7.5. The new mobility architecture is supported on the Cisco 5760 wireless controller and the Catalyst 3850 Series switch with IOS XE software releases 3.2.0SE and 3.2.2SE. CUWN wireless controller release 7.4 and releases below 7.3.112 support only the old mobility architecture. The Cisco Flex 7500, 8500, and vWLC do not support the new mobility architecture. IOS XE based wireless controllers do not support the old mobility architecture. Hence if a network contains both Flex 7500 wireless controllers and Converged Access controllers, then separate sets of guest wireless controllers must be deployed with the DMZ to support both mobility architectures with the guest wireless design discussed in this design guide.

## Guest Controller Configuration

The guest controller is the point where all the employee device traffic is terminated. For this version of the design guide, the discussion only includes a CT5508 CUWN wireless controller as the guest controller. An example of a guest controller configuration for the employee personal devices WLAN is shown in [Figure 18-10](#).

**Figure 18-10** Example Configuration of a Guest Wireless Controller for the Employee Personal Devices WLAN

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
2	WLAN	BYOD_Guest	BYOD_Guest	Enabled	Web-Auth
4	WLAN	BYOD_Personal_Device	BYOD_Personal_Device	Enabled	[WPA2][Auth(802.1X)]

As can be seen, the configuration of the WLAN on the guest controller must match the configuration of the WLAN on the campus controller.

The guest controller needs to be configured with a mobility anchor pointing at itself. An example is shown in Figure 18-11.

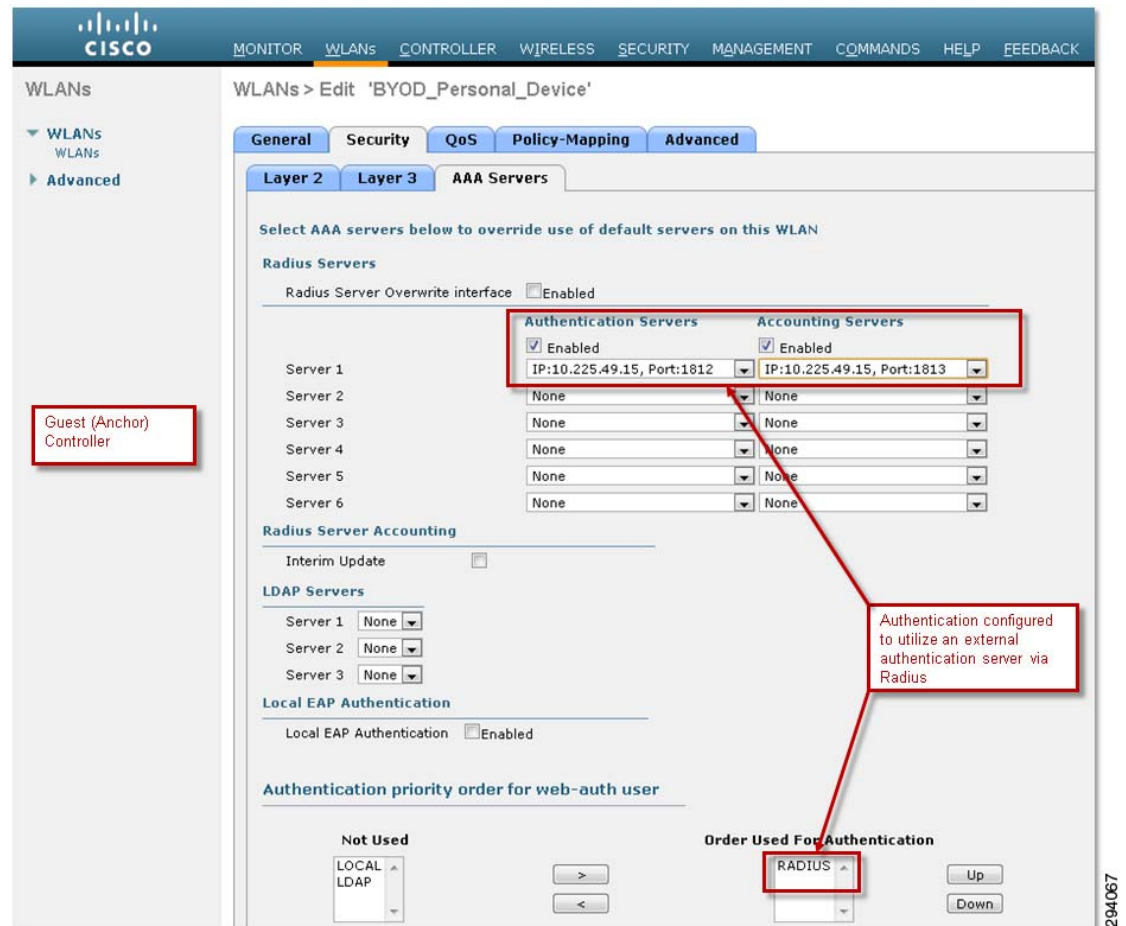
**Figure 18-11** Example Configuration of the Mobility Anchor on a Guest CUWN Wireless Controller



Again, this assumes the campus controller and the guest controller are configured to be part of the same mobility group before the mobility anchor is configured.

The network administrator must also configure the employee personal devices WLAN to use RADIUS within the guest controller for authentication. This is shown in Figure 18-12.

**Figure 18-12** Authentication via RADIUS for the Employee Personal Devices WLAN on the Guest Controller





Finally, in order to support the new mobility architecture (also referred to as the hierarchical mobility architecture), the network administrator must check the Enable Hierarchical Architecture option within the global mobility configuration of both the campus and guest controller. An example is shown in Figure 18-13.

**Figure 18-13 Enabling the Hierarchical Mobility Architecture**

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT

Global Configuration

**General**

Enable New Mobility (Converged Access) ☒ Enables the new hierarchical mobility architecture which uses CAPWAP for mobility tunnels

**Mobility Parameters**

Mobility Oracle ☐

Multicast Mode ☐

Multicast IP Address

Mobility Oracle IP Address

Mobility Controller Public IP Address

Mobility Keepalive Interval(1 to 30 sec)

Mobility Keepalive Count(3 to 20)

Mobility DSCP Value(0 to 63)

Guest (Anchor) Controller

204068



**Note**

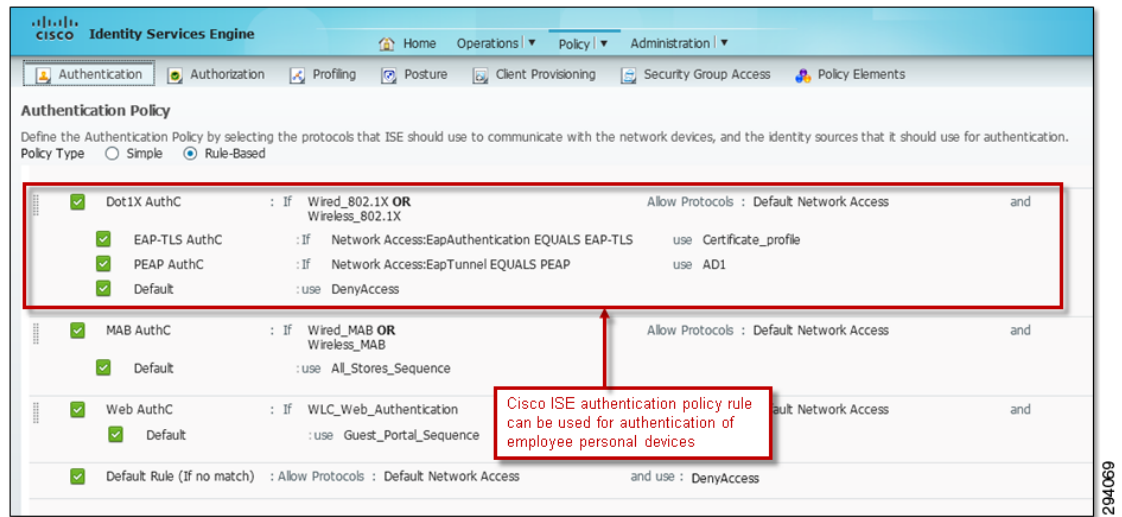
Since the Flex 7500 wireless controller does not support the new mobility architecture, this step can be skipped in deployments involving a Flex 7500 as the branch wireless controller.

## Cisco ISE Policy Configuration

From a Cisco ISE policy perspective, the existing authentication rule—which is used to support both the on-boarding of corporate-owned (IT-managed) devices and the authentication of on-boarded corporate-owned devices within the Limited Access use case—can also be used to support wireless employee personal devices for the Basic Access use case. An example of such a policy rule is shown in Figure 18-14.



**Figure 18-14** Example of Cisco ISE Authentication Policy Allowing Wireless Employee Personal Device Access



The logical format of the authentication policy rule for this example is:

```
IF (Wired_802.1X OR Wireless_802.1X)
  THEN (Allow Default Network Access AND
    IF Network Access:EapAuthentication EQUALS EAP-TLS USE Certificate_Profile
    IF Network Access:EapTunnel EQUALS PEAP USE AD1
    ELSE Default EQUALS DenyAccess)
```

**Wired\_802.1X** is a system-generated compound condition that is used here to match 802.1X-based authentication requests from switches. It matches the following two standard RADIUS attribute-value (AV) pairs:

```
Service-Type - [6] EQUALS Framed
NAS-Port-Type - [61] EQUALS Ethernet
```

**Wireless\_802.1X** is a system-generated compound condition that is used here to match 802.1X-based authentication requests from Cisco wireless controllers. It matches the following two standard RADIUS dictionary attribute-value (AV) pairs:

```
Service-Type - [6] EQUALS Framed
NAS-Port-Type - [61] EQUALS Wireless - IEEE 802.11
```

**Default Network Access** is a system-generated authentication result, which allows various EAP protocols to be used for authentication.

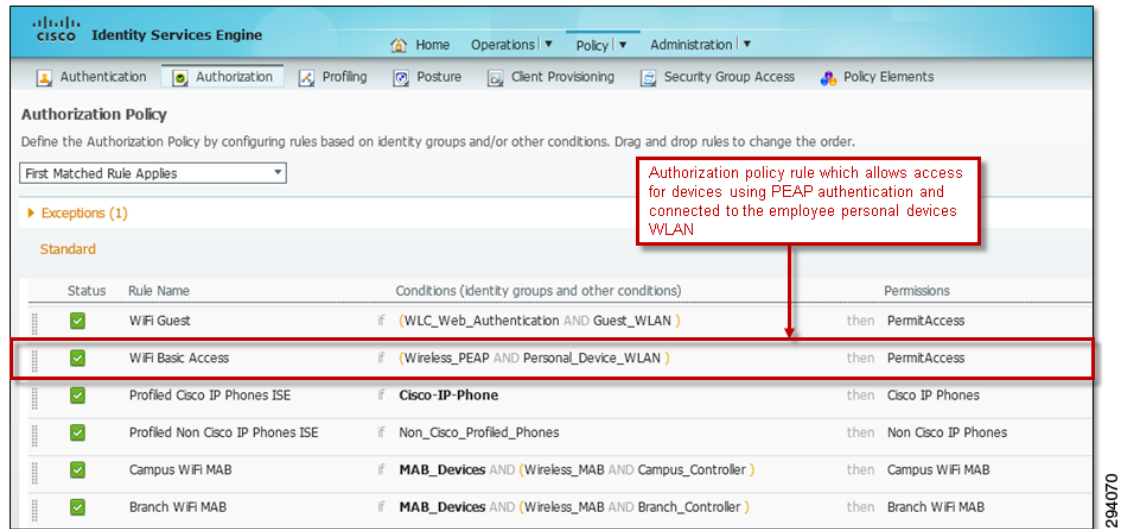
**Certificate\_Profile** is a user-defined Certificate Authentication Profile configured under the External Identity Sources section of the Cisco ISE server.

**AD1** corresponds to the Microsoft Active Directory identity store, where employee credentials are typically held within an organization.

For the Basic Access use case, wireless employee personal devices which use PEAP for authentication will match on the second condition—**IF Network Access:EapTunnel EQUALS PEAP USE AD1**—causing these devices to proceed to the authorization phase. Note that the example above works for employee personal devices which utilize PEAP authentication only. If the customer requires other authentication or EAP methods, additional conditions would need to be added to the above authentication policy rule. These conditions could also use the AD1 Microsoft Active Directory identity store to verify employee user credentials. Alternatively, the default condition could be changed from denying access to also using the AD1 identity store.

From a Cisco ISE policy perspective, an additional authorization rule needs to be added in order to support the Basic Access use case. This rule permits access for devices using PEAP authentication, which originate from the SSID corresponding to the employee personal devices WLAN. An example of the policy rule is shown in Figure 18-15.

**Figure 18-15** Example of Cisco ISE Authorization Policy Allowing Wireless Employee Personal Device Access



The logical format of the authorization policy rule for this example is:

```
IF (Wireless_PEAP AND Personal_Device_WLAN)
  THEN PermitAccess
```

**Wireless\_PEAP** is a user-defined compound authorization condition that is used here to match authentication requests from wireless PEAP devices. It matches the following two standard RADIUS dictionary attribute-value (AV) pairs, along with a Network Access condition which specifies the use of PEAP.

```
Service-Type - [6] EQUALS Framed
NAS-Port-Type - [61] EQUALS Wireless - IEEE 802.11
Network Access:EapTunnel EQUALS PEAP
```

**Personal\_Device\_WLAN** is a user-defined simple authorization condition for employee personal devices that access the network via the WLAN corresponding to the employee personal devices SSID. It matches the following RADIUS AV pair from the Airespace dictionary:

```
Airespace-Wlan-Id - [1] EQUALS 4
```

The Airespace-Wlan-Id is the identification number (WLAN ID) of the WLAN corresponding to the employee personal devices SSID. This is shown in Figure 18-16.

**Figure 18-16** Example Wireless Controller WLAN IDs Showing Employee Personal Devices WLAN and SSID

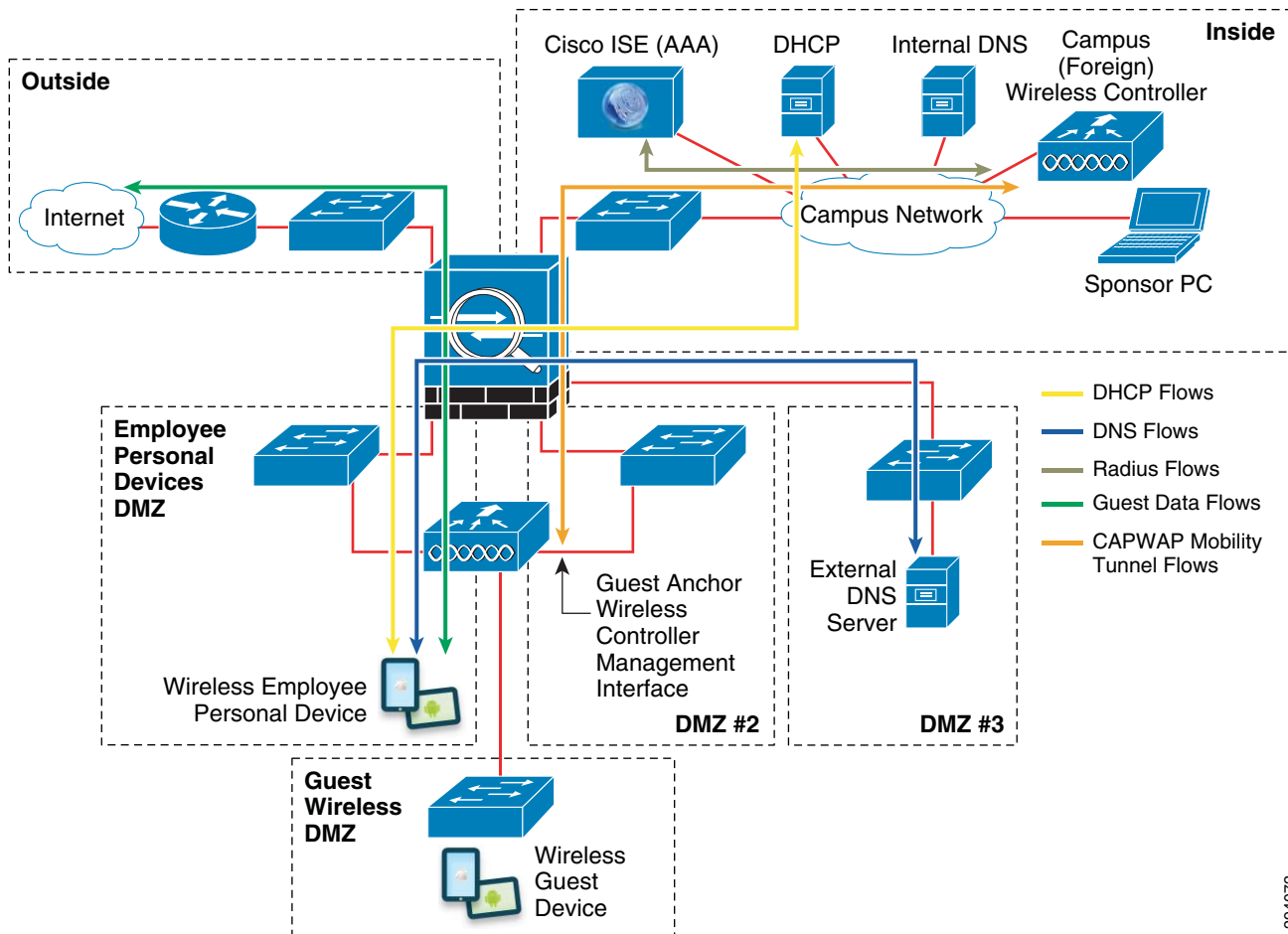


WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
2	WLAN	BYOD_Guest	BYOD_Guest	Enabled	Web-Auth
4	WLAN	BYOD_Personal_Device	BYOD_Personal_Device	Enabled	[WPA2][Auth(802.1X)]

Note that this WLAN ID must be consistent across the entire BYOD deployment. This rule allows the ISE authorization policy to differentiate 802.1X authentication requests coming from the employee personal devices SSID and simply permit access. A WLAN ID cannot be changed on an existing WLAN. To change a WLAN ID, the WLAN must be removed and created again.

## ASA Firewall Configuration

Figure 18-17 shows an example of the flows that need to pass through the Cisco ASA firewall to support this option.

**Figure 18-17** Example of Flows that Need to Pass Through the Cisco ASA Firewall for Employee Personal Devices

294072

The RADIUS session is initiated by the campus (foreign) wireless controller management interface to the Cisco ISE server for authentication and authorization. Therefore it does not need to be allowed through the ASA firewall for employees who are authenticating with personal devices. If using the newer hierarchical mobility architecture (as indicated in [Figure 18-17](#)), a CAPWAP auto-anchor mobility tunnel (UDP ports 5246 and 5247) between the management interfaces of the two wireless controllers must be allowed through the ASA firewall. If using the older mobility tunnel architecture, an Ethernet-over-IP (IP protocol 97) auto-anchor mobility tunnel, as well as the WLAN control port (UDP port 16666) between the management interfaces of the two wireless controllers, must be allowed through the ASA firewall.

Besides allowing DNS and DHCP (assuming the deployment of an internal DHCP server), the ASA firewall should be configured to block all other traffic generated from employee personal devices onto the internal network. Additional ports can be opened to accommodate the access of corporate resources as discussed in the following section and summarized in [Table 21-2](#).

**Note**

Additional ASA firewall ports may need to be opened to accommodate guest wireless access, depending upon the deployment model discussed in [Chapter 21, “BYOD Guest Wireless Access.”](#)

## Differentiated Quality of Service Treatment

With this deployment model, a separate QoS policy can be applied to employee personal devices, different from guest wireless devices. This is because wireless employee personal devices are terminated on a separate WLAN from wireless guest devices. For CUWN wireless controllers, as of software version 7.2, QoS is applied per WLAN by way of a profile, as shown in Figure 18-18.

**Figure 18-18** Example of QoS Profile Applied to a WLAN

The screenshot shows the Cisco WLAN configuration interface for the 'BYOD\_Personal\_Device' WLAN. The 'QoS' tab is selected, and the 'Quality of Service (QoS)' dropdown is set to 'Platinum (voice)'. A red box highlights this dropdown, and a red arrow points to it from a text box that reads: 'A QoS profile which allows a higher priority of traffic may be applied to the employee personal devices WLAN if desired'. Below the QoS section, there are two sections for 'Override Per-User Bandwidth Contracts (kbps)' with 'DownStream' and 'UpStream' settings for Average Data Rate, Burst Data Rate, Average Real-Time Rate, and Burst Real-Time Rate. At the bottom, the 'WMM' section shows 'WMM Policy' set to 'Allowed' and '7920 AP CAC' and '7920 Client CAC' both set to 'Enabled'.



### Note

IOS XE based wireless controllers support much more extensive QoS capabilities. However they also have the ability to support similar QoS per WLAN based on the older profiles model of CUWN wireless controllers. This version of the design guide does not address QoS on IOS XE based wireless controllers. Future versions will discuss this topic more thoroughly.

This may be desirable if employee personal devices are going to be allowed to run virtual desktop client applications such as a Citrix client or VMware client or if employee personal devices run collaboration clients such as Cisco Jabber.

**Note**

Chapter 21, “BYOD Guest Wireless Access” discusses rate limiting per-SSID and per-User. These features can be used for employee personal devices as they were for guest devices. Rate limiting is configured on the campus (foreign) controller and not the guest (anchor) controller.

## Accessing Corporate Resources

Because employee devices are associated to the network from a DMZ interface, which is effectively outside of the corporate firewall, they do not have access to company resources located inside the firewall. This may be perfectly acceptable and desirable. Employee devices still have access to the public Internet. This enables them to connect to cloud-based resources such as Cisco WebEx or partner websites. The employee device is afforded some level of usability, making the device useful as a productivity tool.

Companies may want to offer access to additional resources but still maintain the security offered by restricting employee devices to the guest side of the firewall. There are various options available to accomplish this objective, including:

- Setting up a mirror of the company website
- Allowing VPN access
- Allowing virtual desktop client access

## Securing Mirror Sites for Personal Devices

One approach to bringing services to employee personal devices accessing the guest network is to set up a mirror of the company website in another DMZ segment, referred to as an employee device security zone (EDSZ) within this section. If employee personal devices connect to the guest wireless network, the website will only be accessible after the user has completed the Web Auth process and accepted an Acceptable Use Policy (AUP) or End User Agreement (EUA). This website does not need to be an exact match of an internal website, but could contain relevant content that employees can use on their personal devices to make them more effective. In addition, the website could include content optimized for smaller mobile displays. Examples of applications that could be offered in the EDSZ include access to email, a team wiki page, or the company news site.

There are several methods available to setup a secure website. In general, the deployment is very similar to a typical DMZ web service, except that rather than residing in an Internet facing DMZ, the server is located on a subnet accessible by employee personal devices. The intent of this section is not to provide detailed guidance on the deployment of a presentation server, application server, and database server. Site administrators should be familiar with the approach that best fits their security environment. Some high level considerations when setting up the server include:

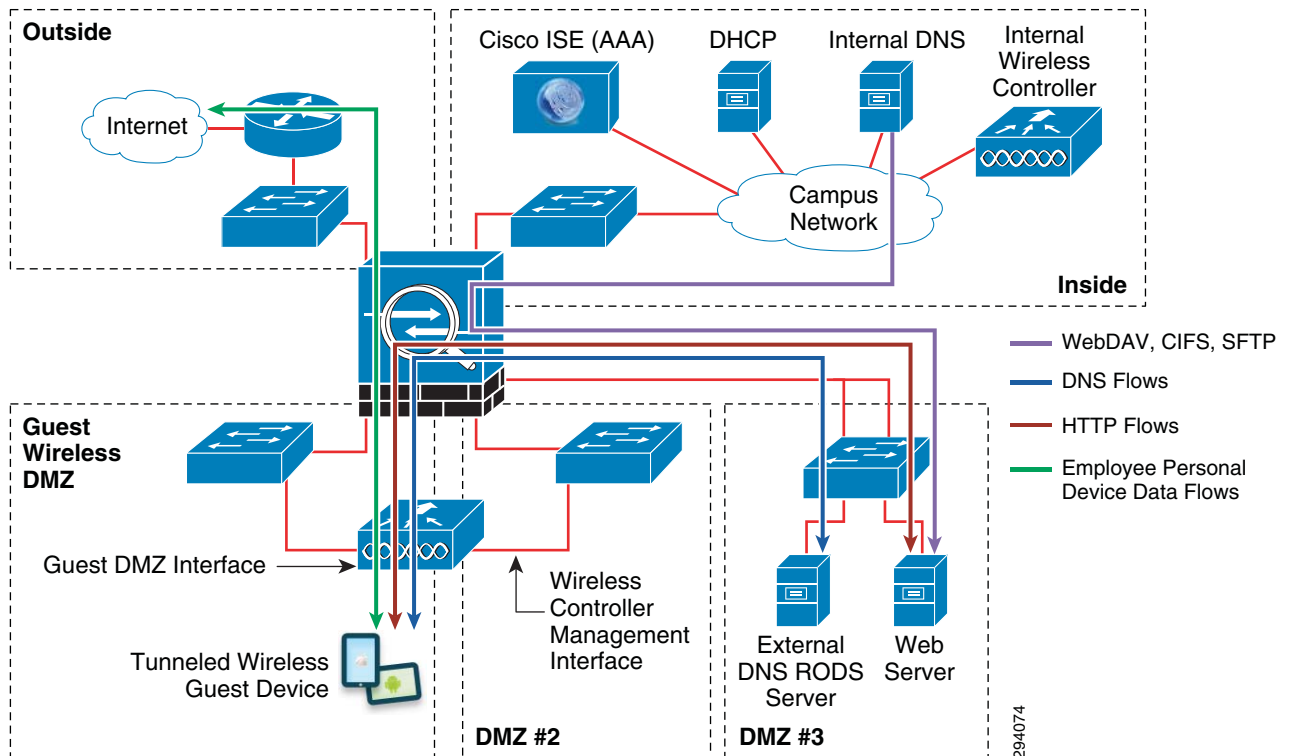
- Dual attachment—Usually this is considered to be more secure. The client-side NIC should implement firewall services that allow inbound connections on TCP port 80 or 443. Only session requests initiated by the client subnets should be allowed towards the server. Session requests initiated by the server should not be allowed towards the client subnets. If the employee device wireless network is encrypted, then some organizations may be comfortable allowing users to attach via HTTP.

- The back-end NIC should be used to move content between the server and the data store or application server. It may also be allowed for remote administration of the site. Single-attached servers are possible although usually a dedicated and secured gateway is setup for the server-to-server communications that is separate from the server-to-web client gateway.
- Content Delivery—Generally content is either static or dynamic. Static content can be pushed overnight or as needed to keep the website current. Dynamic content could allow the employee device to post information to the site. The website could use a local data store that is synchronized with an external data store or have a secured channel to an application server.
- User Authentication—Some method should be used to ensure only authorized and authenticated users are able to view site content. Utilizing Microsoft Active Directory or a local user database are two possible methods. Active Server pages (ASP.NET) can also be used to leverage the login controls used with Microsoft Internet Information Server (IIS) servers and provide a more sophisticated authentication model such as single sign-on (SSO). Local databases are easier to setup but require a high level of administrative overhead and are usually only appropriate in very small organizations.
- Secure Sockets—Websites in the employee device security zone (EDSZ) should implement secure socket layer (SSL) or transport layer security (TLS) if employees are sending sensitive information, such as their login credentials. This can be relaxed somewhat if the EDSZ has been implemented with wireless encryption. On the other hand, if employee devices reside in the traditional guest network where wireless packets are not typically protected with encryption and are co-mingled with actual guest traffic, then SSL/TLS websites are needed. This is particularly important if employees are passing their corporate credentials to a mirror website.
- Web Server software—There is a wide range of web server software available. Deciding which type of server to deploy impacts what security features are available. Common choices include Microsoft IIS, Apple, and Tomcat. Wikipedia has a comparison of web server software that can illustrate the choices available ([http://en.wikipedia.org/wiki/Comparison\\_of\\_web\\_server\\_software](http://en.wikipedia.org/wiki/Comparison_of_web_server_software)). It is also possible to host sites on a secure cloud service. This service could be restricted to IP addresses or require client side certificates. With proper security precautions, a cloud-based site could also allow mobile employees access to some traditional corporate resources such as payroll or benefits that are increasingly finding their way to the cloud.

Figure 18-19 illustrates a simple scenario where static content is deployed in a DMZ dedicated for employees using personal devices. A Windows 2008 server is deployed with Microsoft IIS 7.0 as well as some other network services specific to the DMZ, such as DNS and Read-Only Directory Services (RODS). Users are authenticated against the corporate Microsoft Active Directory server. The RODS service requires DNS to be installed on the same server. The web server is typically a dedicated box. However, in some situations it may be desirable to run RODS and IIS on the same server to simplify basic authentication using Microsoft AD. It is more appropriate when supporting a small-to-modest number of employee devices.



Figure 18-19 Example of a Mirror Website for Employee Personal Devices



Moving content to the secured server can be done by various means. One approach is to use FTP, however because FTP is not secured, a better approach is to use either SFTP or FTP over SSL. By default, Microsoft IIS does not ship with a secure FTP server. Microsoft supports FTP over SSL rather than SFTP. Administrators must copy the installation package from Microsoft's website (<http://learn.iis.net/page.aspx/310/what-is-new-for-microsoft-and-ftp-in-iis-7/>) and install the feature on their server. If FTP is already running, the administrator needs to deselect the FTP feature from the services manager prior to installing the FTP over SSL server. The improved FTP over SSL server offers additional tools not available in the standard FTP package that are used to manage access to the FTP site, as shown in Figure 18-20.

Figure 18-20 Example of Tools Available with the FTP over SSL Server

FTP Features	
FTP Authentication	Configure authentication settings for FTP sites
FTP Authorization Rules	Configure rules for authorizing users to access FTP sites
FTP Directory Browsing	Configure information to display in an FTP directory listing
FTP Firewall Support	Configure port ranges and external IP addresses for FTP connections
FTP IPv4 Address and ...	Restrict or grant access to FTP content based on IPv4 addresses or domain names
FTP Logging	Configure how IIS logs requests on the FTP server
FTP Messages	Configure the messages that the FTP server displays for user sessions
FTP Request Filtering	Use this feature to configure filtering rules for the FTP feature
FTP SSL Settings	Specify requirements for SSL
FTP User Isolation	Configure isolation settings for FTP sessions



Anonymous authentication should be disabled and at least basic authentication should be enabled. There are other options that may be appropriate from some organizations.

Instead of FTP over SSL, administrators can choose to use Web Distributed Authoring and Versioning (WebDAV). This method offers more flexibility than FTP because many operating systems allow the connection to be mounted to the file system. By providing a directory handle, web authoring applications as well as other applications can directly use the secured pipe. WebDAV is based on HTTP or HTTPS and provides the ability to authenticate and encrypt data. If employees are placed directly in the guest SSID, then WebDAV HTTPS should be used since passwords are sent. If employee devices are placed in an encrypted EDSZ, then WebDAV HTTPS could be used to provide an additional layer of encryption. The security considerations are detailed in section 20 of RFC4918.

Another option similar to WebDAV is CIFS. This protocol also allows local directory mounts of the remote site. It is commonly found in Microsoft environments, although Samba is available for non-Windows servers. Microsoft also supports SMB2 with Vista, Windows 7, and Windows 8, which is an update to CIFS. There are several other approaches that provide a secure path between either the web authoring site or the application server. A particular enterprise will likely leverage the same methods as the web servers located in the traditional DMZ.

## DNS Support

The employee devices need access to a DNS server. If the EDSZ web server is using RODS, then DNS is already available on the Directory Server. It is installed by default when the RODS is setup unless the administrator explicitly chooses not to. Dynamic updates are secured and zone transfers are not enabled. If the web server is not using AD for employee authentication, then DNS will be a standalone service.

## Outlook Web Access for Employee Devices

Email is a foundational service that can be offered to employee devices. This can be accomplished by deploying a web interface to the mail server such as Outlook Web Access (OWA) or ActiveSync for exchange environments. Some enterprises may already be offering this service for employees that need email while traveling. In this case, the employee devices can continue to use the current Internet facing OWA server.

Microsoft does not support the OWA server in a DMZ zone. Instead, the OWA server should be behind the firewall. Holes can be opened for port 443. Another option is to setup Apache in the EDSZ as a reverse proxy. The Microsoft recommended approach is to run OWA on the client access server (CAS) and publish the CAS with Microsoft's Internet security and acceleration (ISA) server into the EDSZ. This is a full blown deployment and may not be appropriate as a method to grant employee personal device access due to the complexity involved versus other methods, such as simply opening a hole in the EDSZ DMZ firewall for HTTPS to the enterprise CAS.

Another option is subscribing to Office365, which is Microsoft's cloud-based Exchange and Office environment. In this case, employees would use the public Internet service to gain access to their email or other cloud-based enterprise resources. At this time, there is not a native Office365 application for either Android or iOS devices and users would be restricted to HTTPS access unless they were using a Windows 8-based mobile device. This method would also allow Direct-To-Cloud over 3G/4G or off-premise accesses to the same resources. Microsoft is only one of many cloud based enterprise environments offering email services.

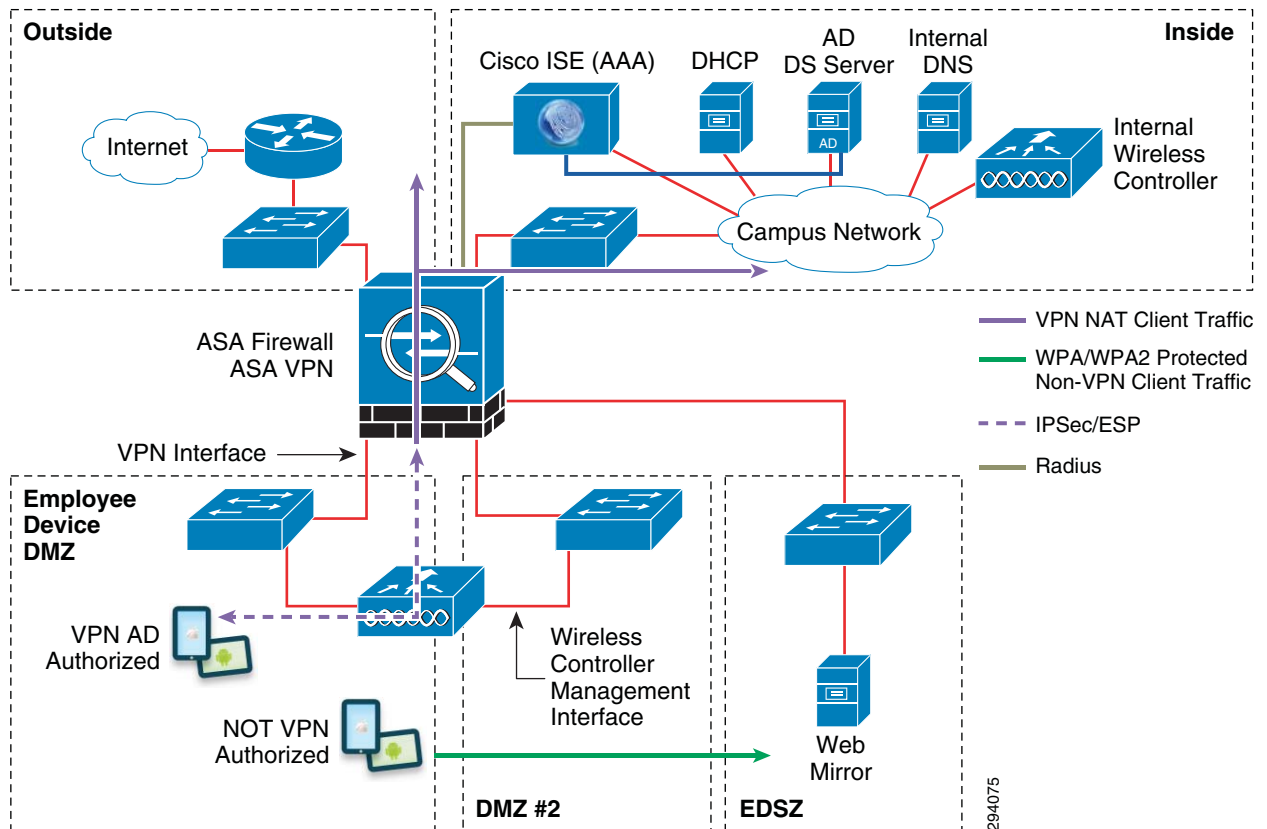
## ActiveSync Support

Future versions of this document will discuss mobile device managers (MDM) that are used to manage the configuration profiles of mobile devices and provide additional security features needed for lost or stolen devices. Some of the MDM functionality is licensed from Microsoft, including remote-wipe, PIN lock enforcement, and others. ActiveSync is used to synchronize email, calendar events, and contacts between the Microsoft Exchange server and the mobile device's email application. Administrators may be interested in providing ActiveSync to devices in the employee device security zone (EDSZ). When properly configured and certified, ActiveSync can also provide the MDM security features mentioned previously. Providing this support is similar to OWA. The firewall policy in the EDSZ can be set to allow connections to ActiveSync on the CAS that may be published on an ISA server. ActiveSync is supported by WebDAV and should be used over HTTPS (TCP port 443).

## VPN Client

Enterprises that restrict employee devices to a guest or dedicated EDSZ may want to allow a subset of these users the ability to launch the built-in VPN client to connect to the secured part of the network. There are two methods that can be employed. First, the device may already have access to the current Internet-facing VPN concentrator. In this case, the employee device would connect from the guest network out through the public Internet and then back in to the Internet DMZ where the VPN concentrator is located. If employee devices are co-mingled with actual guest traffic, then this may be the best approach. However, if a dedicated and secured SSID is deployed behind an ASA firewall specifically for employee personal devices, then this firewall could also provide VPN access for some privileged users. Alternatively, a dedicated VPN concentrator could be located in the EDSZ. After the device authenticates and joins the secured wireless domain, these users would connect to the VPN concentrator to gain additional secured access. Only employee devices in the dedicated security zone can reach the concentrator. The general layout of the network components are shown in [Figure 18-21](#).

Figure 18-21 Employee Zone VPN Network Components



Apple iOS devices include a built-in Cisco IPSec client allowing ESP tunnel mode and XAUTH. Both Apple and Android devices offer L2TP with IPsec and pre-shared key (PSK). The ASA can be setup to accept both types of VPN clients. For this discussion, the focus is the Cisco VPN client found on Apple iOS devices.

The employee needs to know the name of the VPN concentrator, group, and group secret to configure the VPN client. Future version of this document will illustrate how the VPN configuration can be pushed to the employee device without user intervention. Certificates can also be pushed to the employee device to further secure access to the VPN concentrator. The use of certificates negates the need for a group and group secret.

**Figure 18-22** iOS VPN Client Configuration

When the user connects to the VPN concentrator, they are asked for their Microsoft AD credentials. This information is passed by the Cisco ASA to the Cisco ISE server, where a policy decision can be made. This decision can include attributes from Microsoft Active Directory or any of the other parameters Cisco ISE can use to determine policy. If the user is authenticated and authorized by Cisco ISE, the ASA completes the VPN connection. Once connected, the ASA can apply additional security and access restrictions to the tunnel, further controlling what resources the employee device can reach. The ASA can also be used to monitor who is using the VPN portal, as shown in [Figure 18-23](#).

**Figure 18-23** ASA Management for VPN Connections

Filter By: IPsec(IKE v1) Remote Access -- All Sessio... Filter						
Username	Group Policy Connection Profile	Assigned IP Address Public(Peer) IP Address	Protocol Encryption	Login Time Duration	Client(Peer) Type Version	Bytes Tx Bytes Rx
joeemployee	EmpDevices	10.17.40.36	IKEv1 IPsec	08:56:16 PDT Wed May 16 201	iPhone OS	3504
	EmpDevices	10.17.34.13	AES128	0h:02m:23s	5.1.1	6983

ASA provides additional information for managing VPN connections.

## Virtual Desktop Client

Another available deployment model is to allow a virtual desktop to run on the employee device. The actual applications and associated data remain on the secured hosting server. Once the device disconnects from the network, the data is typically no longer available to the user. The enterprise can control which users are able to launch a virtual desktop and what applications are available on that desktop. The firewall between the EDSZ and the hosting server can be configured to allow specific connections.

There are a wide range of possibilities. In its simplest form, the employee could use VNC to connect back to their desktop or a dedicated server. A VNC client is available for both iOS and Android devices. This may be adequate for some small environments where availability and manageability are not a top priority. By default, the connection is not encrypted, which is a concern. Administrators may not have the necessary control over which applications are available on the hosting server. Employees may be tempted to attach to their desktop and send sensitive data to an external account via email or cloud file sharing services such as Dropbox and Google Drive. This temptation only arises as a means to bypass IT policy and should be considered before allowing remote desktops to attach to employee deployed VNC servers. The use case for employee devices with virtual VNC desktops needs careful review. The employee is likely sitting in front of the actual desktop, with a full keyboard and mouse and likely does not need a remote desktop. The best approach may be to block TCP port 5900 from traversing the firewall to unknown destinations.

Cisco also partners closely with Citrix in support of both the XenApp and XenDesktop products for deployment of a Virtual Desktop Infrastructure. Access to VDI for employee devices are best suited in environments where a centralized UCS server is securing and managing sessions. With VDI in place for corporate devices, extending access to employee devices may allow productivity gains. This can be done by opening the firewall to allow a connection to specific and well known servers. Beyond BYOD, virtual desktops are compelling because of the reduction in IT costs. Adding tablet support maximizes the benefit because the requirement for employee laptops is reduced. A small and lightweight VDI hardware appliance replaces the traditional desktop, and mobile device support un-tethers the employee from the cube. Tablets with virtual desktops can offer much of the same functionality as employee laptops, but at a reduced cost and with stronger tools to address lost and stolen devices plus centralized data security inherent in VDI.

Finally AnyConnect provides a centralized virtual desktop that integrates with the ASA firewall. This is a good approach because security is the foundation of the system. AnyConnect desktops attach to the ASA firewall via SSL. Virtual desktops are evolving in capabilities and will be covered in more detail the next release of this document.

## Summary

These types of alternate solutions offer a wide range of options to provide employees compute resources without compromising corporate data. Leveraging the guest environment can serve as part of a migration path to a fully certificate-based BYOD solution. Guest type deployments can be set up fairly quickly without the need to touch a large number of third-party devices and yet still meet the basic requirement of allowing employees to use their personal devices to increase the organization's productivity.





# User Experience—How To On-board a BYOD Device

---

**Revised: September 27, 2013**

The Cisco ISE allows employees to be in charge of on-boarding their own devices through a self-registration workflow and simplifies the automatic provisioning of supplicants as well as certificate enrollment for the most common BYOD devices. The workflow supports iOS, Android, Windows, and Mac OS devices and assists in transitioning these devices from an open environment to a secure network with the proper access based on device and user credentials.

The simple workflow provides a positive experience to employees provisioning their own device and allows IT to enforce the appropriate access policies.

## Apple iOS Devices

The employee connects to the provisioning SSID and is redirected to the Guest Registration portal for registration after opening a browser. The employee logs in using their Active Directory credentials.

If the device is not yet registered, the session is redirected to the self-registration portal, where the user is asked to enter a description for the new device. The employee is not allowed to change the Device ID (MAC address), which is automatically discovered by ISE.

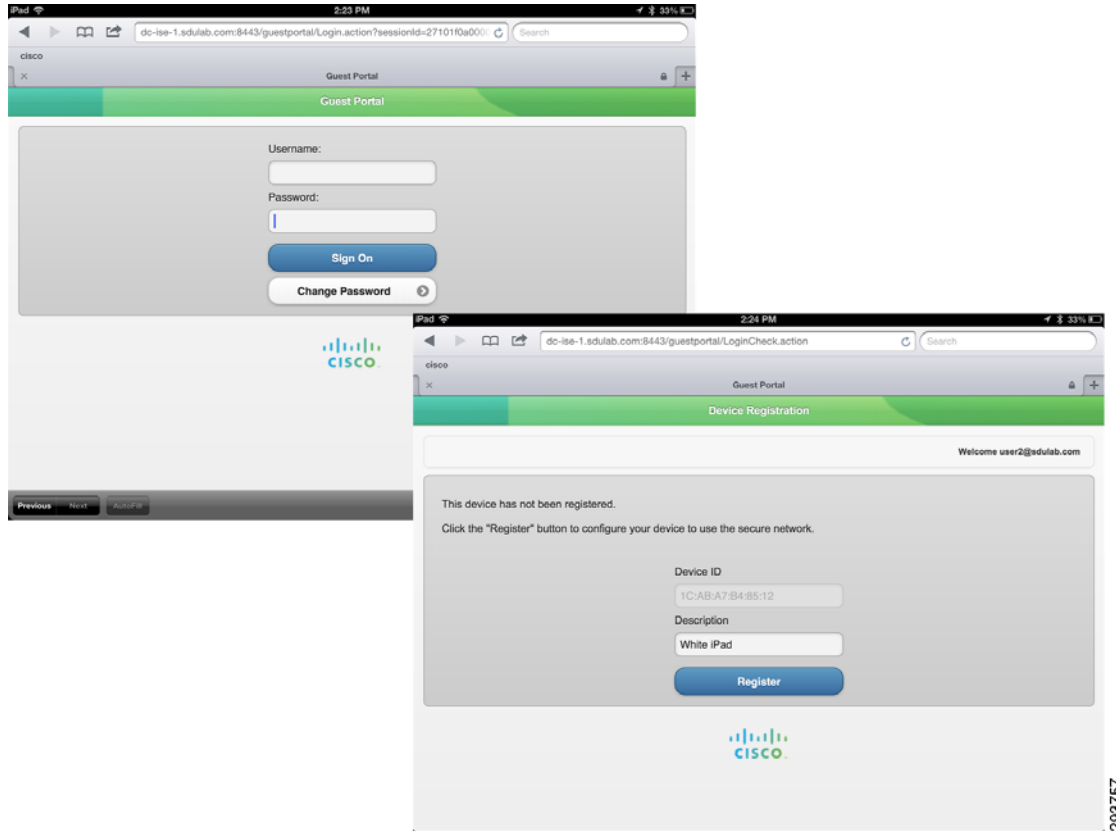


**Note**

---

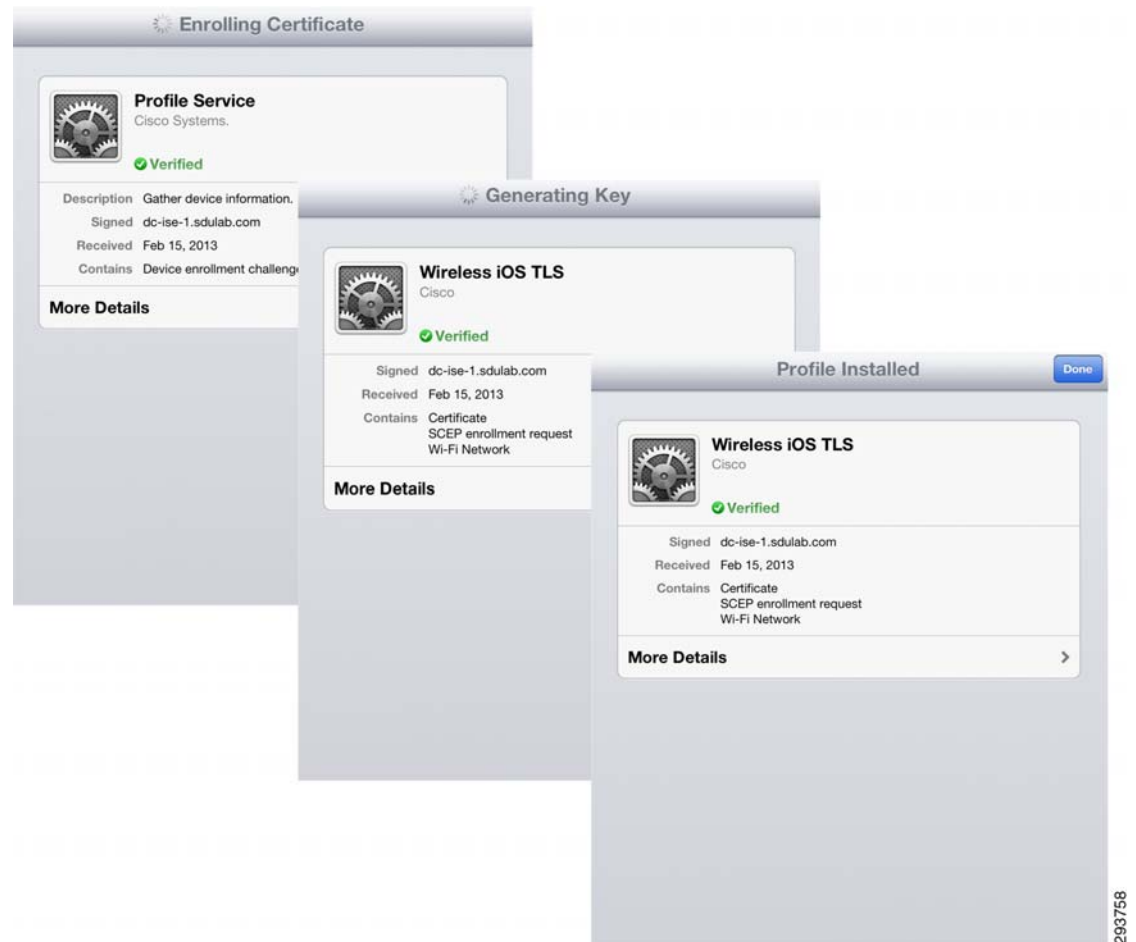
Cisco has been made aware of potential incompatibilities introduced by Apple iOS 7. We are working to understand the limitations and design updates will be made to this publication.

---

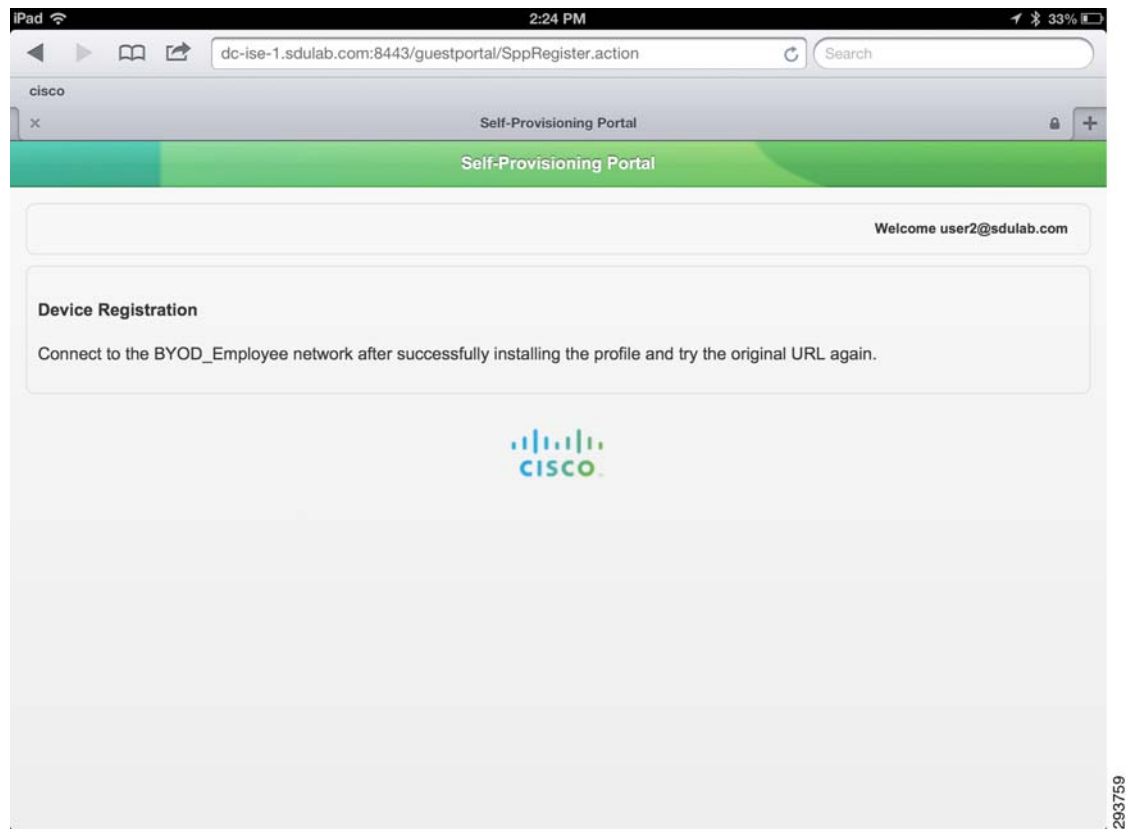
**Figure 19-1** Guest Portal and Self-Registration Portal

- The supplicant profile is downloaded and installed on the endpoint.
- Keys are generated and the certificate is enrolled.
- The Wi-Fi profile required to connect to the BYOD\_Employee is installed.



**Figure 19-2** Enrollment and Profile Installation

The employee is notified that registration is complete and is reminded to manually connect to the BYOD\_Employee SSID.

**Figure 19-3** *Device Registration Complete***Note**

For iOS devices, the employee is required to connect manually to the BYOD\_Employee SSID.

The certificates and profile can be viewed by clicking **Settings > General > Profiles** and selecting **Mobile Profile**. [Figure 19-4](#) highlights the Wi-Fi profile to connect to the BYOD\_Employee SSID.

**Figure 19-4** Mobile Profile Details

As shown in [Figure 19-5](#), the ISE maintains a detailed log of the authentications as they take place:

- The first log shows how the first time the device connects, the MAC address is used for authentication, and the Wireless CWA profile is used for authorization, enabling the redirection to the Guest Registration portal.
- Once the enrollment and provisioning take place, the user connects to the secure BYOD\_Employee SSID. ISE grants Partial Access to the device.

**Figure 19-5** ISE Authentications Log

Cisco Identity Services Engine									
<a href="#">Home</a>   <a href="#">Operations</a>   <a href="#">Policy</a>   <a href="#">Administration</a>   <a href="#">Troubleshoot</a>									
<a href="#">Authentications</a>   <a href="#">Reports</a>   <a href="#">Endpoint Protection Service</a>   <a href="#">Troubleshoot</a>									
<a href="#">Show Live Sessions</a>   <a href="#">Add or Remove Columns</a>   <a href="#">Refresh</a>									
Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group
Feb 15, 13 04:22:38.055 PM	✓		user2	1C:AB:A7:B4:85:12				Campus WiFi Partial Access	RegisteredDevices
Feb 15, 13 04:21:03.764 PM	✓		user2	1C:AB:A7:B4:85:12					Any
Feb 15, 13 04:11:22.362 PM	✓		user2	1C:AB:A7:B4:85:12					Any
Feb 15, 13 04:10:48.938 PM	✓		1C:AB:A7:B4:85:12	1C:AB:A7:B4:85:12				Wireless CWA	RegisteredDevices

[Figure 19-6](#) shows in more detail the steps that took place and how the rule was evaluated to grant Partial Access.

- Authentication is dot1x and EAP-TLS.
- Username is user2. The Active Directory (AD1) identity store was used.

- MAC Address is discovered.
- The Wireless\_Dot1X\_AuthC authentication rule was used.
- The Campus WiFi Partial Access authorization rule matched. This rule enforces the access list ACL\_Partial\_Access in the Wireless LAN Controller.

Figure 19-6 ISE Authentication Details

Authentication Details	
Source Timestamp	2013-02-15 16:22:38.055
Received Timestamp	2013-02-15 16:22:38.055
Policy Server	dc-ise-1
Event	5200 Authentication succeeded
Username	user2
User Type	
Endpoint Id	1C:AB:A7:B4:85:12
IP Address	
Identity Store	
Identity Group	RegisteredDevices
Audit Session Id	27101f0a000001a533981e51
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	
Device Type	Network#WLC
Location	Campus_Controllers
NAS IP Address	10.31.16.39
NAS Port Id	
Authorization Profile	Campus WiFi Partial Access
Posture Status	NotApplicable
Security Group	
Failure Reason	
Response Time	381

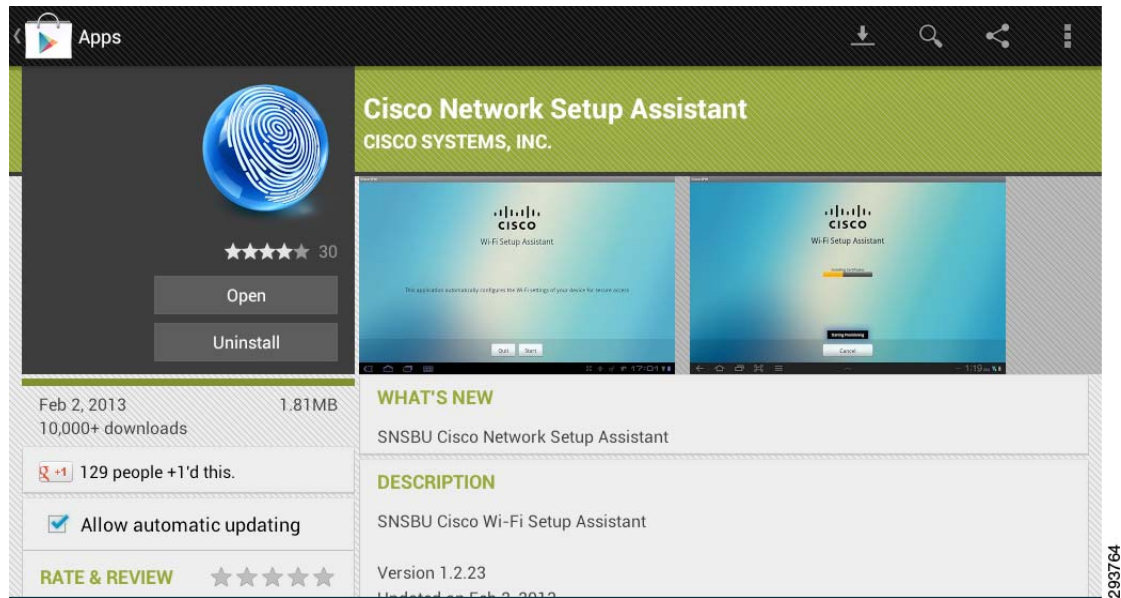
# Android Devices

The user experience is very similar when provisioning Android devices. The employee is redirected to the Guest Registration portal and is allowed to enter a description for the new device.

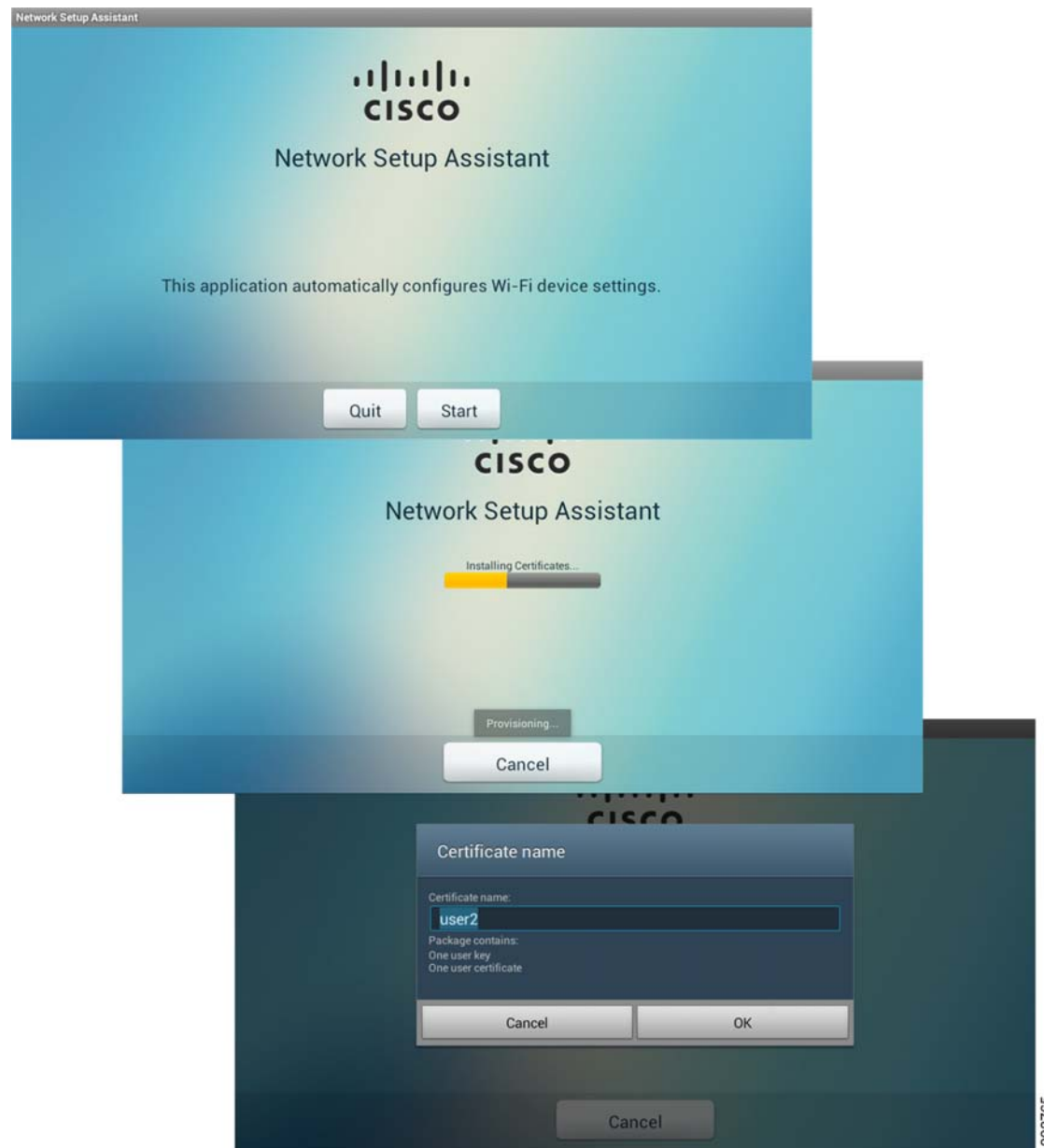
**Figure 19-7** Guest Portal and Self-Registration Portal

The figure consists of two overlapping browser window screenshots. The top window shows the 'Guest Portal' login page with a green header bar. It contains a login form with 'Username:' and 'Password:' labels, corresponding text input fields, a blue 'Sign On' button, and a 'Change Password' link with a right-pointing arrow. Below the form is the Cisco logo. The bottom window shows the 'Device Registration' page, also with a green header bar. It features a 'Welcome user2@sdulab.com' message in the top right. The main content area states 'This device has not been registered.' and provides instructions: 'Click the "Register" button to be redirected to the Android Market, where you can download the Cisco Network Setup Assistant application.' Below this text is a registration form with 'Device ID' and 'Description' labels, input fields containing '18:E2:C2:82:43:AF' and 'Galaxy Tab' respectively, and a blue 'Register' button. A vertical text label '293763' is positioned to the right of the bottom screenshot.

The employee is then redirected to Google Play where the Cisco SPW for Android may be downloaded.

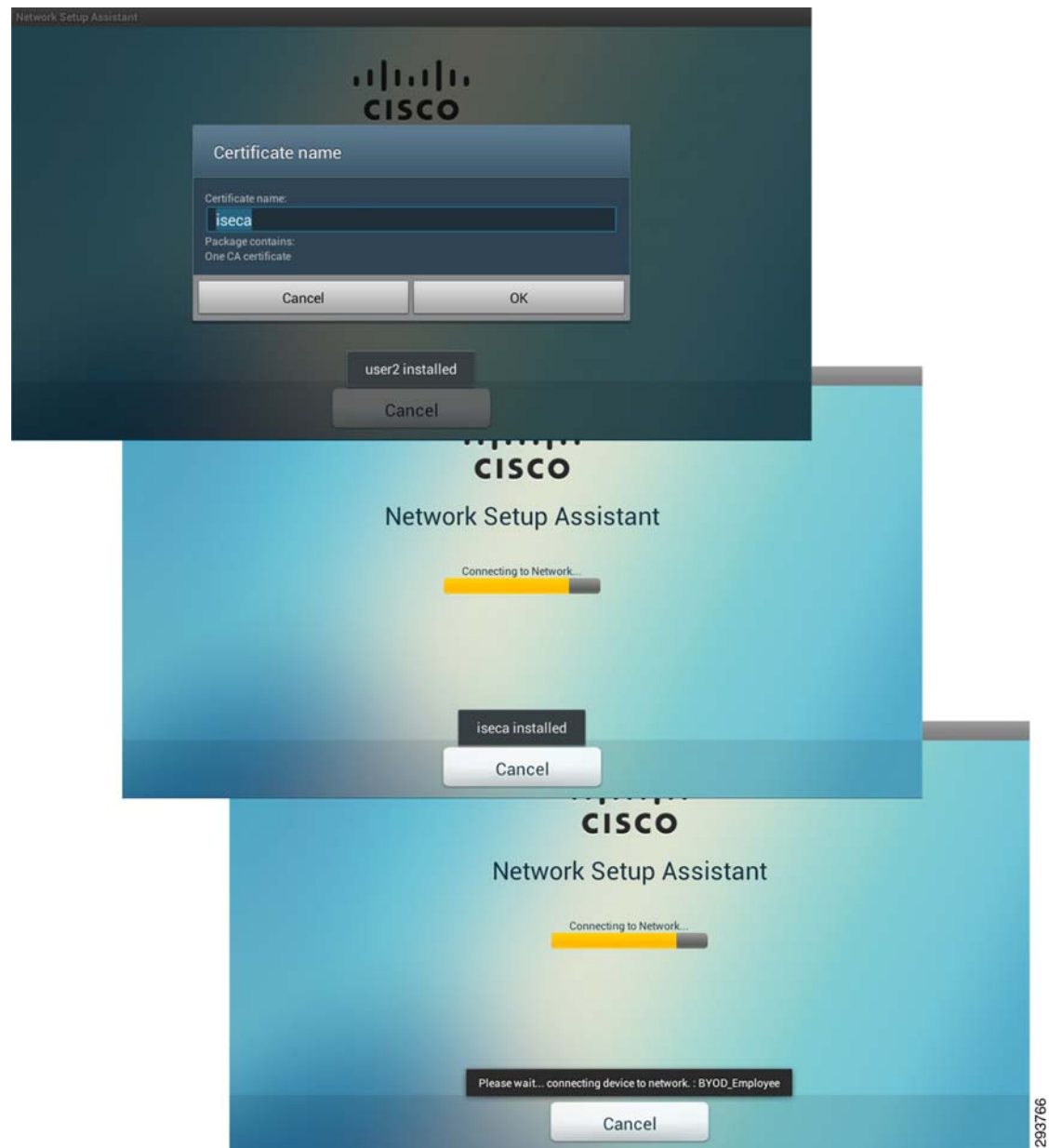
**Figure 19-8** Supplicant Provisioning Wizard from Google Play

The SPW is launched and the provisioning process begins. The SPW discovers the ISE and begins downloading the profile and installing the certificates.

**Figure 19-9**     **Provisioning Process**

The employee is allowed to name the certificate and provides a password for the certificate storage for their device. The Wi-Fi profile to connect to BYOD\_Employee is applied.

**Figure 19-10** Certificate and Profile



Without employee intervention, the provisioning process automatically connects the Android device to the BYOD\_Employee SSID, as shown in [Figure 19-11](#).



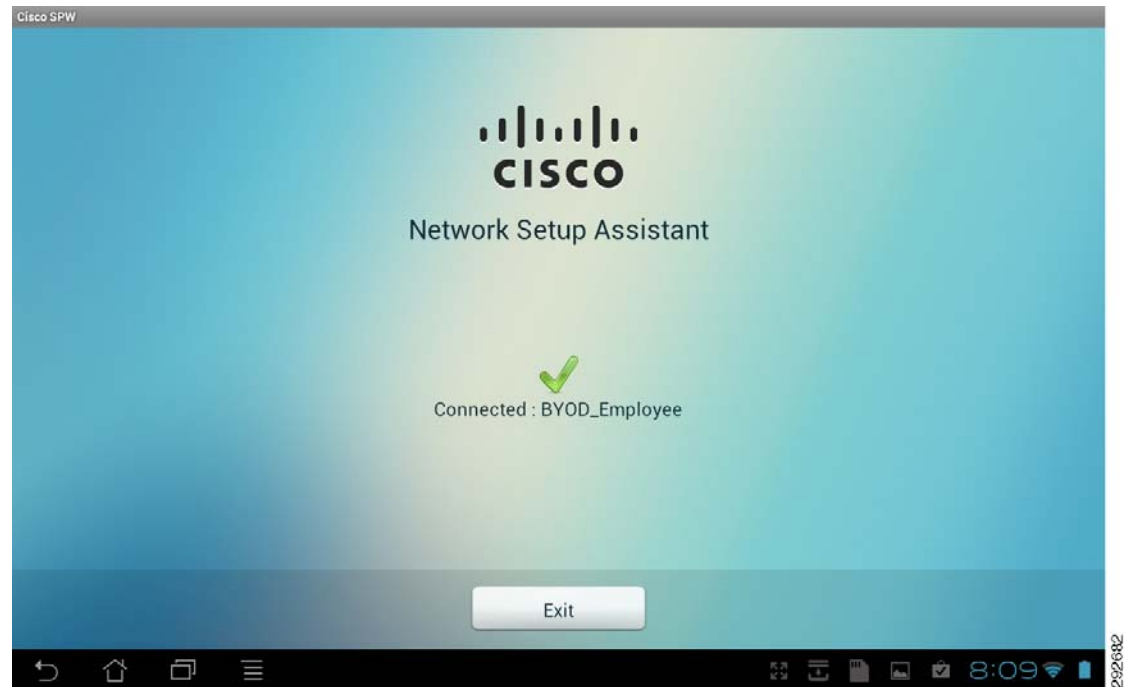
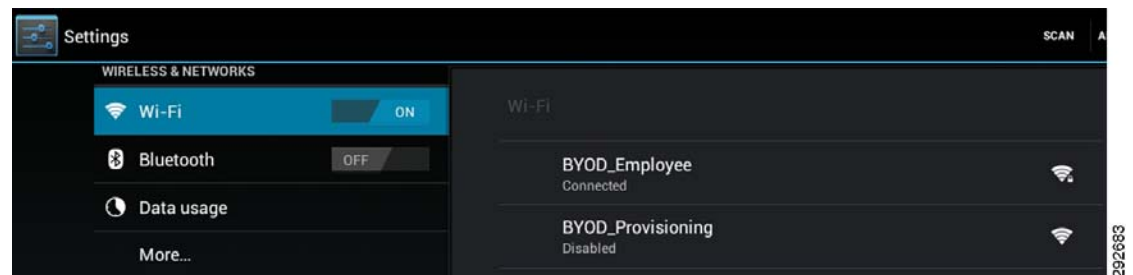
**Figure 19-11** Automatic Connection to BYOD\_Employee

Figure 19-12 shows how the device is automatically connected to the secure BYOD\_Employee SSID.

**Figure 19-12** BYOD\_Employee Secure SSID

## Windows Devices

The user experience while provisioning a Windows device is very similar, redirecting the session to the Guest Registration portal and asking the employee for authentication.

Some Windows devices have multiple network adapters, for example, a laptop with both wired and wireless adapter. The network security policy checks that the device mac-address (sent using calling-station-id attribute) matches the SAN field of the device digital certificate before allowing access. This is done to prevent spoofing. Since each adapter has a unique mac-address, the anti-spoofing policy check can cause difficulties for devices with multiple adapters. If a device registers with a wired adapter, it will obtain a digital certificate with the mac-address of the wired adapter. If the same device attempts to later authenticate to the secure wireless network, most operating systems will attempt to the

use the wired adapter certificate for authentication and will fail because the mac-address of the wireless adapter will not match the SAN field of the digital certificate. To avoid this problem, a device with multiple adapters must register both the wired and wireless adapter.

There are two methods for provisioning wireless devices:

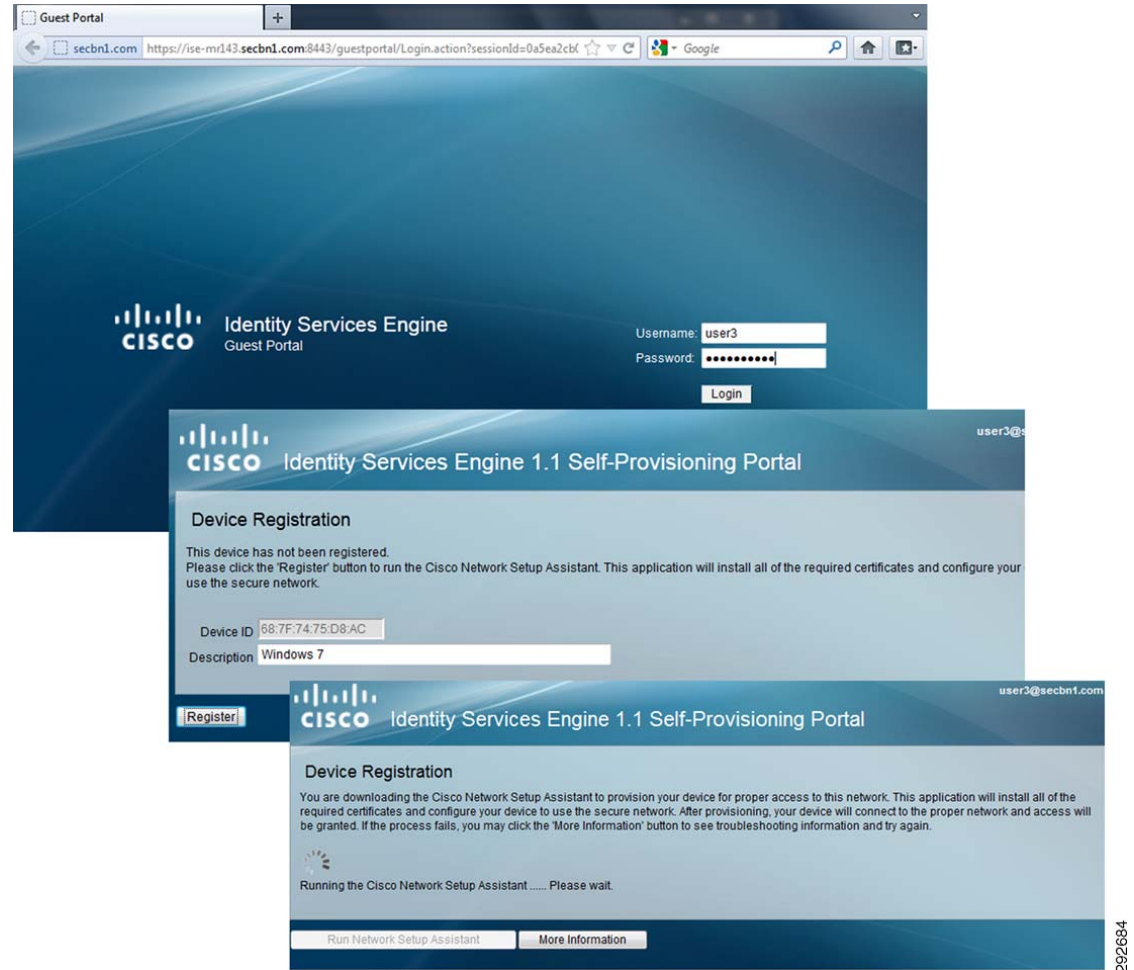
- Dual SSID model, which supports MAB on the provisioning SSID and dot1X on the employee SSID.
- Single SSID model, which supports only the dot1X protocol.

For the Dual SSID method, the wired and wireless adapters may be provisioned in any order. For example, if the device associates with the provisioning SSID (which supports MAB) and is successfully provisioned, then subsequently connects with the wired adapter, 802.1X will fail because of the anti-spoofing check in the policy and the user will be re-directed to complete the provisioning process. Thereafter, the device can access the network with either adapter.

For the Single SSID method, the order in which the wired and wireless adapters are provisioned matters. For example, if the device connects using the wired adapter first and is successfully provisioned, then subsequently connects using the wireless adapter, some operating systems attempt to establish a EAP-TLS connection using the wired digital certificate instead of undergoing the provisioning process. This connection attempt will fail because of the anti-spoofing check in the policy. To prevent this from happening, the user must provision the wireless adapter before connecting with the wired adapter for the single SSID method.

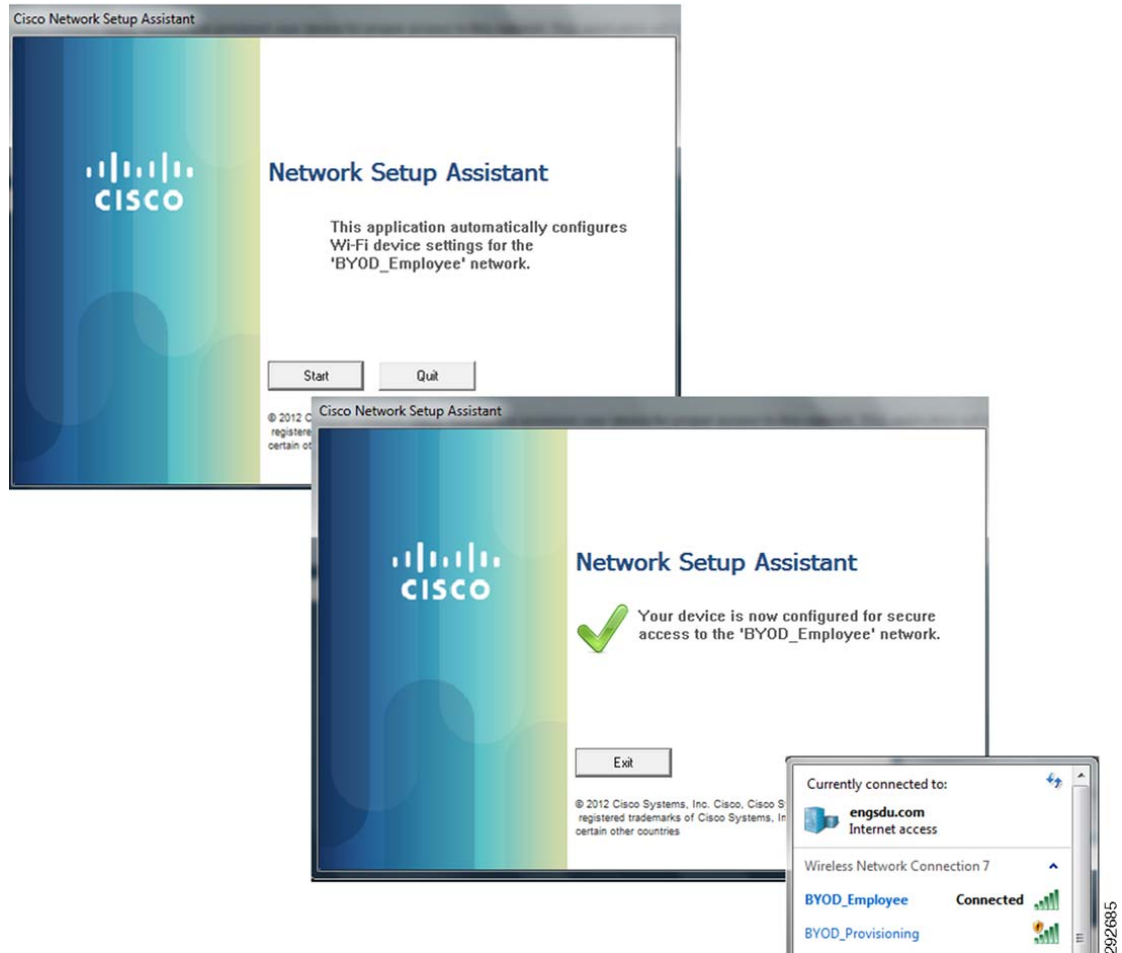
## Windows Wireless Devices

After authenticating at the portal and entering a description for the new Windows device, the SPW is downloaded.

**Figure 19-13** Guest Registration Portal

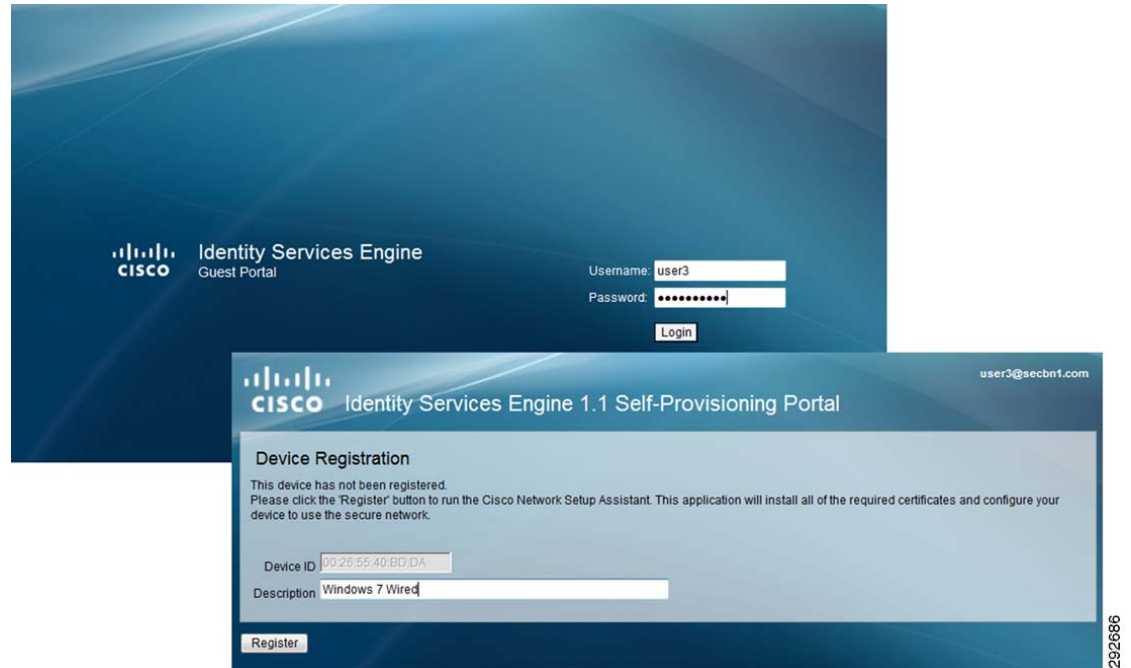
The SPW is launched to install the profile, the keys are generated, and the certificate enrollment takes place.

The SPW installs the BYOD\_Employee configuration to connect to the secure SSID. The connection is switched automatically to the BYOD\_Employee SSID.

**Figure 19-14** SPW and Connection to Secure SSID

## Windows Wired Devices

The user experience is very similar, but instead of configuring access to a secure SSID, the SPW configures the devices to connect via a wired connection.

**Figure 19-15** Guest Registration Portal

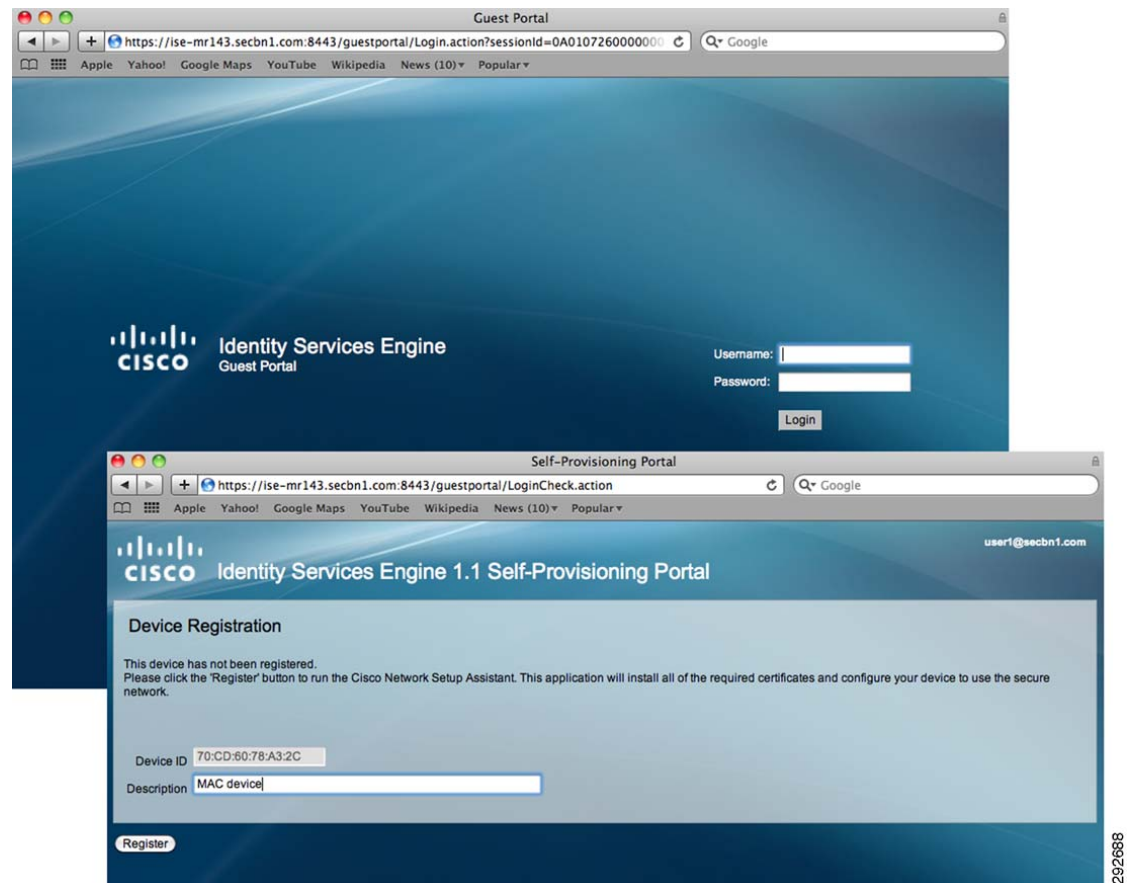
The SPW is downloaded and the proper configurations are applied to the device.

**Figure 19-16** *SPW and Secure Access*

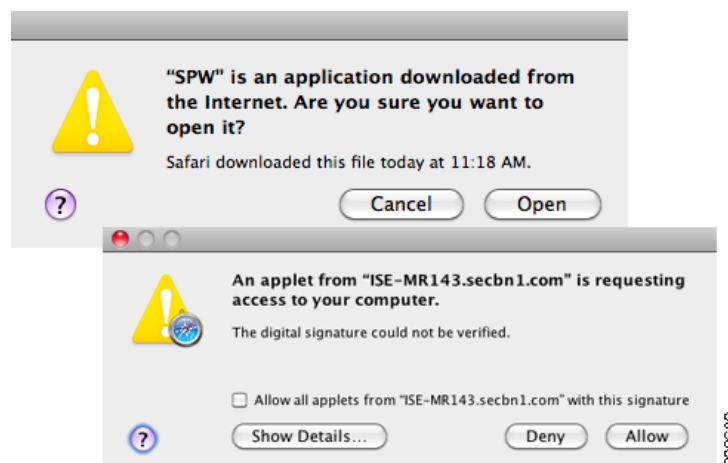
292687

## Mac OS/X Devices

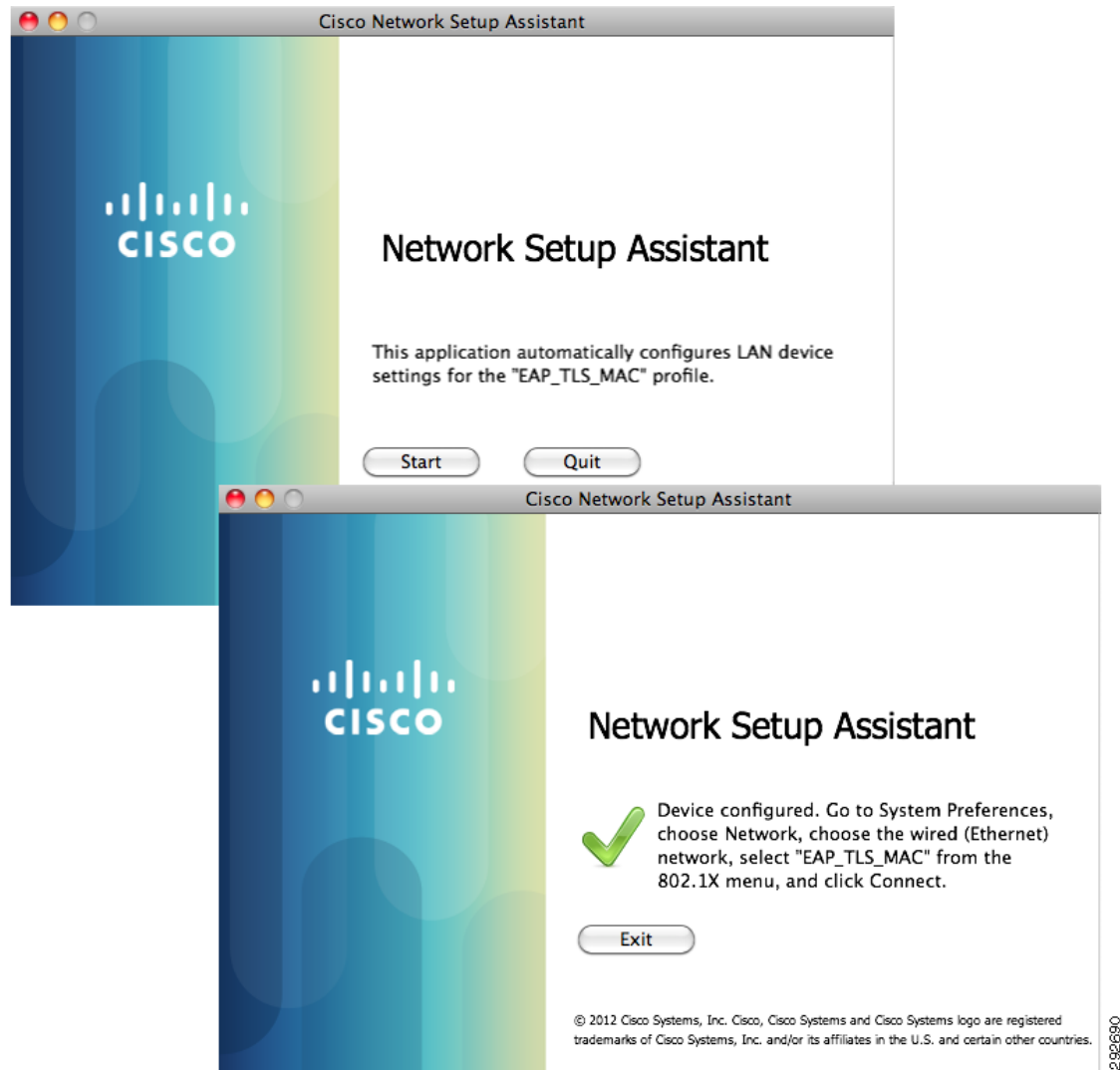
The user experience while provisioning a Mac OS X wired device is also very similar, redirecting the session to the Guest Registration portal and asking the employee for authentication.

**Figure 19-17** Guest Registration and Self-Registration Portals

The SPW is downloaded and installed.

**Figure 19-18** SPW and Secure Access

The Network Setup Assistant configures the EAP-TLS\_MAC profile for secure access.

**Figure 19-19** *Network Setup Assistant*

The network settings in [Figure 19-20](#) show the new EAP\_TLS\_MAC configuration.



Figure 19-20 Network Settings

