



# TrustSec How-To Guide: On-boarding and Provisioning

---

For Comments, please email: [howtoguides@external.cisco.com](mailto:howtoguides@external.cisco.com)

Current Document Version: 3.0

August 27, 2012

# Table of Contents

---

Table of Contents .....	2
Introduction .....	3
What Is the Cisco TrustSec System? .....	3
About the TrustSec How-To Guides .....	3
<i>What does it mean to be 'TrustSec Certified'?</i> .....	4
Overview .....	5
<b>Scenario Overview</b> .....	6
<i>Architecture/ Diagram</i> .....	7
<i>Components</i> .....	7
Cisco ISE Configuration .....	8
<i>Identify Users for BYOD Flow</i> .....	8
<i>Create an Identity Source Sequence</i> .....	11
<i>Configuring My Devices Portal</i> .....	12
<i>Configuring Guest Portal Sequence</i> .....	15
<i>Create a Client Provisioning Policy</i> .....	17
<i>Policy Configuration</i> .....	20
<i>Configure an Authentication Policy</i> .....	22
Appendix A: Android and Play.Google.Com .....	34
Why Android is Different .....	34
Appendix B: BYOD flows .....	35
Appendix C: References .....	37
Cisco TrustSec System: .....	37
Device Configuration Guides: .....	37

# Introduction

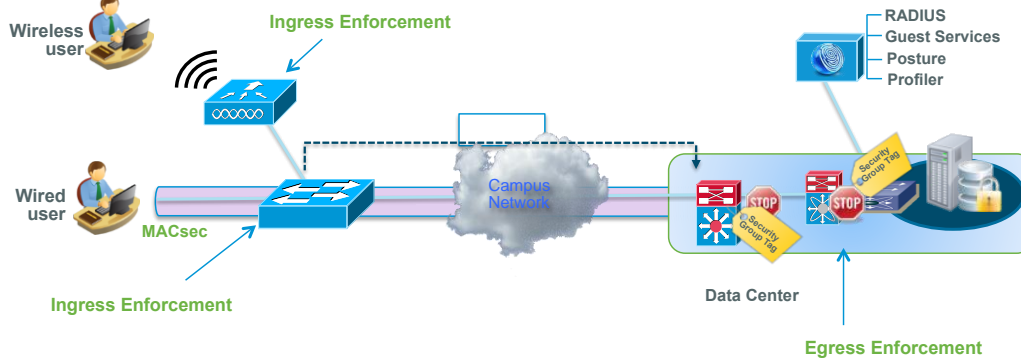
## What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

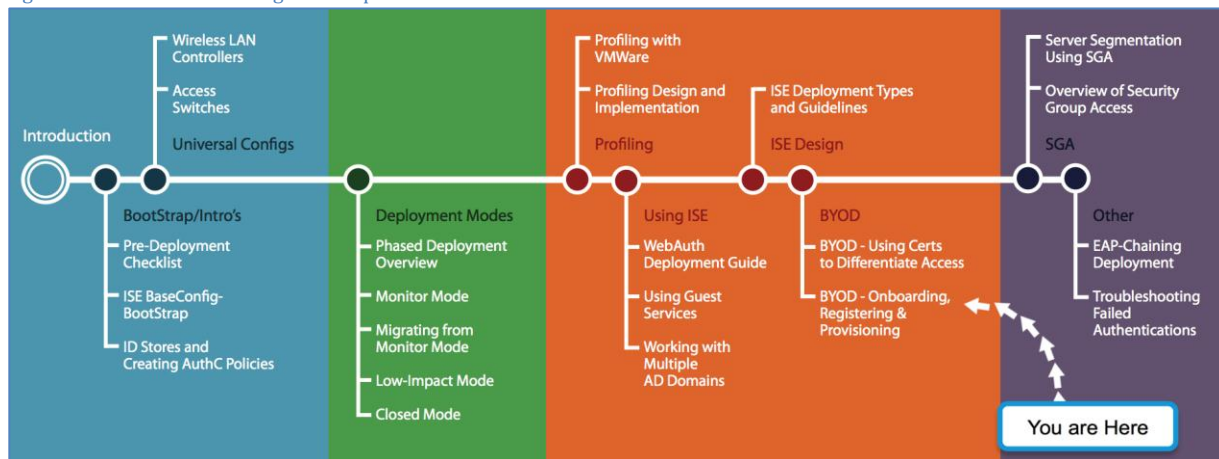


## About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide in this series comes with a subway-style “You Are Here” map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



## What does it mean to be ‘TrustSec Certified’?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked “TrustSec certified,” all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as “TrustSec certified”. The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

---

**Note:** Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

---

# Overview

---

The explosion of mobile devices and the pressure on corporations to support the Bring Your Own Device (BYOD) phenomena has created new security requirements that must be met to safeguard network services, protect data and provide a balance between enterprise needs and user demands. This application note covers some of the security features built into the Identity Services Engine such as Device Registration and Native Supplicant provisioning which customers can use to address some of the requirements around BYOD.

This how-to guide covers how the system is setup for on-boarding which includes native supplicant provisioning, the type of supplicant profile being pushed and how to write policy to differentiate access.

Table 1 lists the supported platforms, supplicant profile location after download and corresponding place to view or clear a profile.

Table 1: Supported Platforms

Device	Certificate Store	Certificate Info	Version
iPhone/iPad/iPod	Device Certificate Store (configuration profiles)	Can be viewed through: Settings → General → Profile	5.0 and above
Android	Device Encrypted Certificate Store	Cannot be viewed. But it may be cleared from: Settings → Location & Security → Clear Storage (Clear all device certificates and passwords)	3.2 & above
Windows	User Certificate Store	Can be viewed by launching the Certificate Snap-In for MMC.	WindowsXP – SP3 Windows Vista – SP? Windows7 – all versions
MacOS-X	Keychains	Can be viewed by launching application → Utilities → Keychain Access	MacOS-X 10.6 and 10.7

---

**Note:** MacOS-X 10.8 has the following Caveats

1. SPW (Supplicant MAC and is not getting installed when we select the option "MAC App Store and identified developers" in security & Privacy Preference Pane
  2. Pop up is presented multiple times when installing SPW Profile/Certificate
- 

---

**Note:** Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for Cisco TrustSec deployment as prescribed by best practices to ensure a successful project deployment.

If interested in provisioning Certificates along with the supplicant profile, please refer to the following how-to-guide "BYOD-Using\_Certificates\_for\_Differentiated\_Access"

**Warning:** The document has been designed to be followed from beginning to end – bypassing sections may have undesirable results.

---

## Scenario Overview

This document will discuss the self-service on-boarding of personal devices, where an employee will register a new device, and the native supplicant is automatically provisioned for that user & device and installed using a supplicant profile that is pre-configured to connect the device to the corporate network. The Cisco ISE policy could also be configured to provide differentiated access to the user/device based on user, device type, location and time.

Device on-boarding for wireless could be setup to use Single SSID and or Dual SSID, registration and on-boarding flow for each user case is as follows

To explain the scenario used in this document, let's follow an example of Native Supplicant Provisioning and Authorization of an iPad:

### Dual SSID Wireless BYOD Self Registration

1. Customer Network is setup with 2 SSIDs, one that is OPEN for Guest/BYOD (BYOD-Open) and other is for secure corporate access (BYOD-Dot1x).
2. Employee associates to Guest SSID (BYOD-Open).
3. Opens a browser and is redirected to the Cisco ISE CWA (Central Web Auth) Guest portal
4. Employee enters their corporate username and password in the standard Guest portal
5. Cisco ISE authenticates the user against the corporate Active Directory or other corporate Identity Store, provides and authorization policy of accept with redirect to the Employee Device Registration Portal
6. Device MAC address is pre-populated in the Device Registration Portal for DeviceID and employee could enter optional description and then accept the Acceptable User Policy (if required)
7. Employee selects accept and begins downloading and installing the supplicant provisioning wizard
8. Using OTA, the Cisco ISE Policy Services Node sends a new profile to the iPad including the issued certificate (if configured) embedded with the iPad's MAC address and employee's AD username as well as a Wi-Fi supplicant profile that enforces the use of MSCHAPv2 or EAP-TLS for 802.1X authentication.
9. Now the iPad is configured to associate to the corporate wireless network using MSCHAPv2 or EAP-TLS for authentication, and the Cisco ISE authorization policy will use the attributes in the certificate to enforce network access (for example, provide limited access, since this is not a corporate asset).
10. Cisco ISE initiates a Change Of Authorization (CoA), employee re-associates (incase if dual-SSID Employee would have to manually connect to the corporate SSID where as for single-SSID iPad would automatically reconnect using EAP-TLS) to the Corporate SSID(BYOD-Dot1x) and Authenticates via MSCHAPv2 or EAP-TLS (authentication method configured for that supplicant)

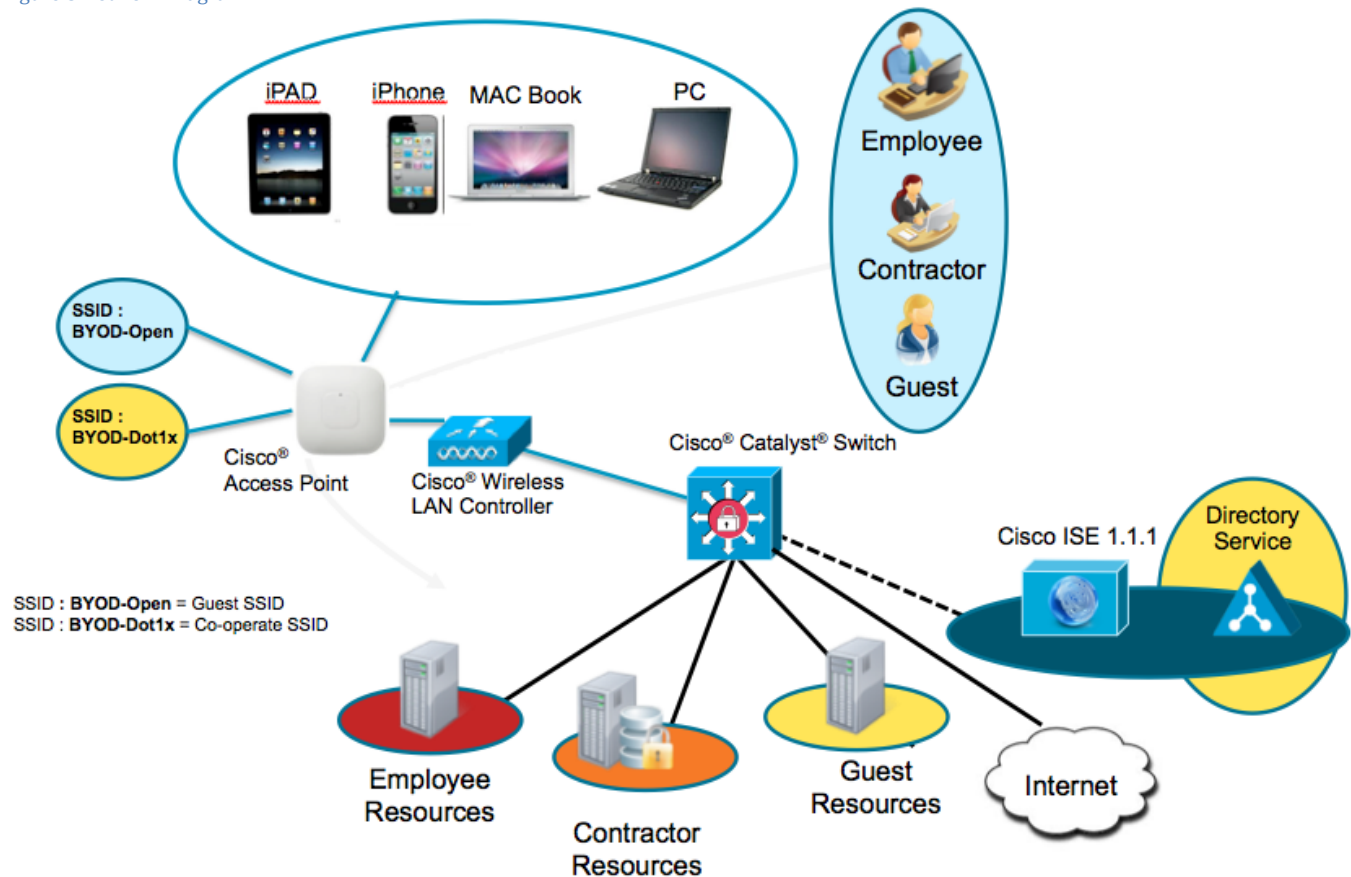
### Single SSID Wireless BYOD Self Registration

1. Customer Network is setup with a single SSID (BYOD-Dot1x) for secure corporate access that could support both PEAP and EAP- TLS (when using Certificates).
2. Employee associates to Corporate SSID (BYOD-Dot1x).
3. Enters into the supplicant their EMPLOYEE username and password for the PEAP authentication
4. Cisco ISE authenticates the user against the corporate Active Directory or other corporate Identity Store, provides and authorization policy of accept with redirect to the Employee Device Registration Portal
5. Employee opens a browser and is redirected to the Employee Device Registration Portal.
6. Device MAC address is pre-populated in the Device Registration Portal for DeviceID and employee could enter optional description and then accept the Acceptable User Policy (if required)
7. Employee selects accept and begins downloading and installing the supplicant provisioning wizard

8. Using OTA, the Cisco ISE Policy Services Node sends a new profile to the iPad including the issued certificate (if configured) embedded with the iPad's MAC address and employee's AD username as well as a Wi-Fi supplicant profile that enforces the use of MSCHAPv2 or EAP-TLS for 802.1X authentication.
9. Now the iPad is configured to associate to the corporate wireless network using MSCHAPv2 or EAP-TLS for authentication (in case if dual-SSID Employee would have to manually connect to the corporate SSID where as for single-SSID iPad would automatically reconnect using EAP-TLS), and the Cisco ISE authorization policy will use the attributes in the certificate to enforce network access (for example, provide limited access, since this is not a corporate asset).
10. Cisco ISE initiates a Change Of Authorization (CoA), employee re-associates to the Corporate SSID (BYOD-Dot1x) and Authenticates via MSCHAPv2 or EAP-TLS (authentication method configured for that supplicant)

## Architecture/ Diagram

Figure 3 Network Diagram



## Components

Table 2: Components Used in this Document

Component	Hardware	Features Tested	Cisco IOS® Software Release
The Cisco Identity Services Engine (ISE)	Any: 1121/3315, 3355, 3395, VMware	Integrated AAA, policy server, and services (guest, profiler, and posture)	ISE 1.1.1
Wireless LAN Controller (WLC)	5500-series 2500-series WLSM-2	Profiling and Change of Authorization (CoA)	Unified Wireless 7.2.???
Apple iOS and Google Android	Apple & Google	N/A	Apple iOS 5.0 Google Android 2.3

**Note:** Wireless was tested with Central Switching mode only.

# Cisco ISE Configuration

In this section we will go through steps that will be needed to implement the use case described in the How-To-Guide. This will include basic configuration like creating a user group to advance configurations like creating a supplicant profile for PEAP-MSCHAPv2, an Authentication and Authorization policy accordingly.

## Identify Users for BYOD Flow.

As part of user on-boarding (On-Boarding is a term that references the process of registering an asset and provisioning that assets supplicant to be able to access the corporate network), we can select identity stores to define resources to be forwarded to on-boarding (BYOD) flow. The following example illustrates users defined in local store in the Cisco Identity Services Engine as well as in Active Directory, which are part of the identity source sequence.

As part of the best-practice on-boarding procedure, we will use Active Directory as the identity-source to determine what group(s) of users are permitted to on-board their device(s). The following procedure illustrates users defined in the Cisco ISE local user-database as well as in Active Directory, which are part of the identity source sequence.

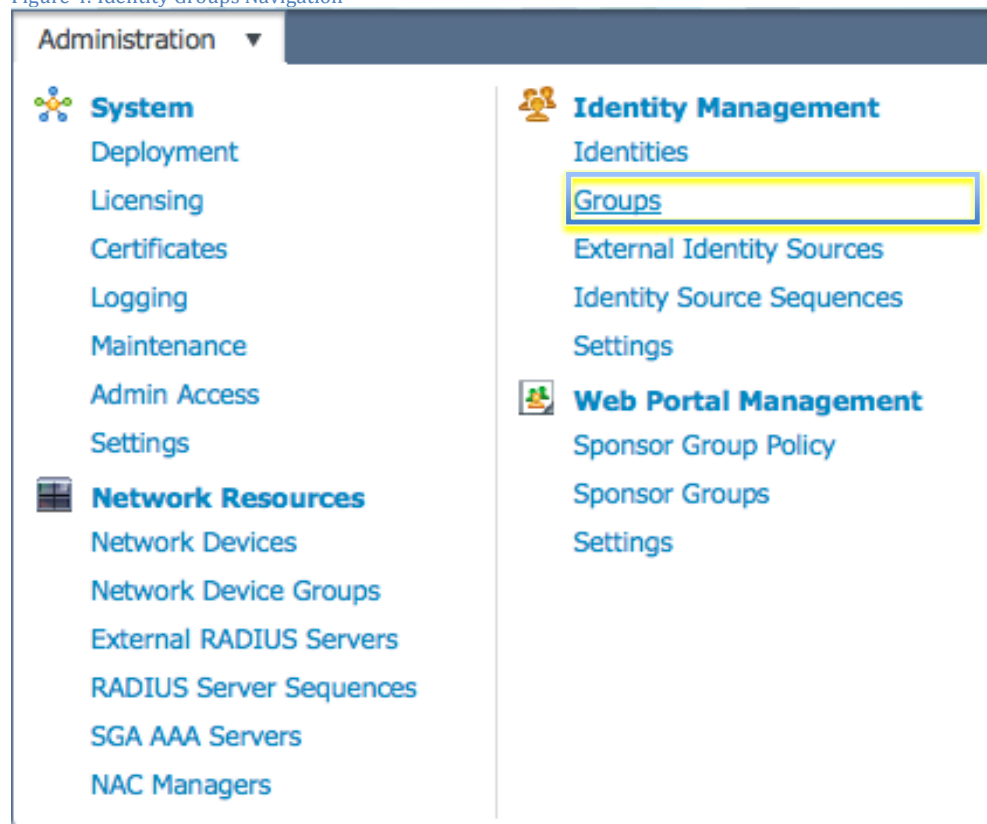
User Groups are a collection of individual users or endpoints that share a common set of privileges that allow them to access a specific set of Cisco ISE services and functionality. For example, if you belong to the Change User Password admin group, you can change administrative passwords for other users.

## Procedure 1 Configure a user group

**Step 1** Navigate to Administration → Identity Management → Groups

**Step 2** Click on ADD.

Figure 4: Identity Groups Navigation



**Step 3** Create an Identity Group.



In this example we are naming our Identity Group: “Employee”

Figure 5: User Identity Groups

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The left sidebar shows 'Identities' > 'Groups'. The main content area is titled 'User Identity Groups > Employee'. It displays the 'Employee' Identity Group configuration with the following details:

- Name:** Employee
- Description:** Default Employee User Group
- Member Users:** A table showing two users: 'test' and 'test1', both with a status of 'Enabled'.

Status	Email	Username	First Name	Last Name
<input checked="" type="checkbox"/> Enabled		test		
<input checked="" type="checkbox"/> Enabled		test1		

## Procedure 2 Create a user in the Employee Group

Step 1 Navigate to Administration → Identity Management → Identities → Users

Step 2 Click on ADD

Figure 6: User Account

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface for creating a new user. The top navigation bar includes 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The left sidebar shows 'Identities' > 'Users'. The main content area is titled 'Network Access Users > test'. It displays the 'test' user account configuration with the following details:

- Name:** test
- Status:** Enabled
- Password:** (masked with asterisks)
- Re-Enter Password:** (masked with asterisks)
- User Information:** First Name and Last Name fields.
- Account Options:** Description (Cisco123 - engineering by avi - don't delete) and Password Change (Change password on next login).
- User Groups:** Employee



## Create an Identity Source Sequence.

Identity source sequences define the order in which the Cisco ISE will look for user credentials in the different databases. Cisco ISE supports the following databases: Internal Users, Internal Endpoints, Active Directory, LDAP, RSA, RADIUS Token Servers and Certificate Authentication Profiles.

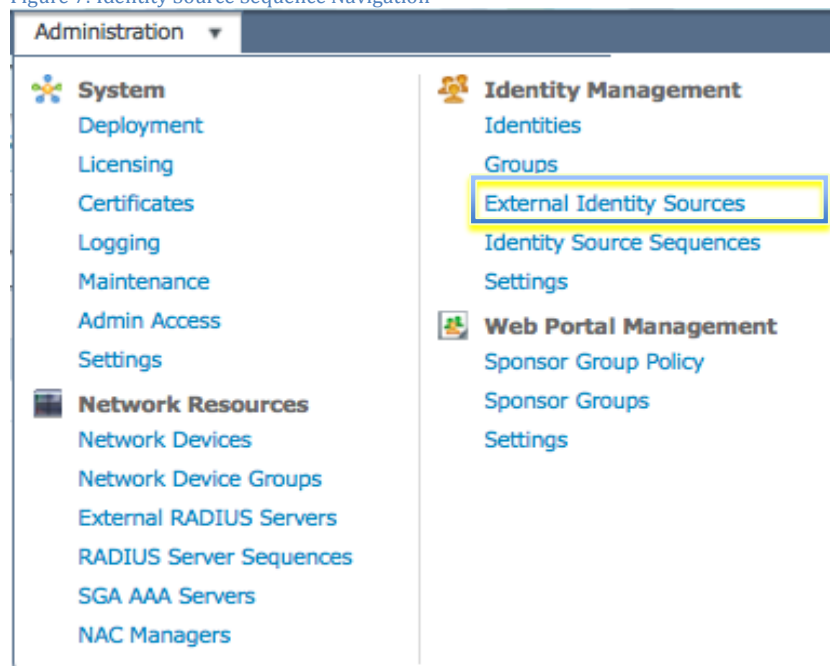
If your organization stores credentials in more than one of these identity stores, you can define an identity source sequence, which states the order in which you want the Cisco ISE to look for user information in these databases. Once a match is found, the Cisco ISE does not look any further, but evaluates the credentials and returns the authorization result to the Network Access Device. This policy is the first match policy.

### Procedure 1 Create an Identity source sequence.

Step 1 Administration → Identity Source Sequence

Step 2 Click on ADD

Figure 7: Identity Source Sequence Navigation



Step 3 Name the sequence

In this example we are naming the sequence “**Dot1x**”.

Step 4 Select your Active Directory Server (AD1), Internal Endpoints and Internal Users in the **Authentication Search List**.

Figure 8: Identity Source Sequence

The screenshot shows a web interface for configuring an Identity Source Sequence. The navigation bar includes Home, Operations, Policy, and Administration. The main menu has System, Identity Management, Network Resources, and Web Portal Management. The sub-menu includes Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The page title is 'Identity Source Sequence List > Dot1x'. The main heading is 'Identity Source Sequence'. Below this, there are several sections: 'Identity Source Sequence' with a 'Name' field containing 'Dot1x' and a 'Description' text area; 'Certificate Based Authentication' with a checkbox 'Select Certificate Authentication Profile' and an empty text field; 'Authentication Search List' with a description 'A set of identity sources that will be accessed in sequence until first authentication succeeds' and two list boxes: 'Available' containing 'Internal Endpoints' and 'Selected' containing 'AD1' and 'Internal Users'; and 'Advanced Search List Settings' with two radio buttons: 'Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"' (selected) and 'Treat as if the user was not found and proceed to the next store in the sequence'. At the bottom are 'Save' and 'Reset' buttons.

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences List > Dot1x

### Identity Source Sequence

▼ Identity Source Sequence

\* Name

Description

▼ Certificate Based Authentication

☐ Select Certificate Authentication Profile

▼ Authentication Search List

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

Available Selected

Internal Endpoints AD1 Internal Users

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

☒ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

☐ Treat as if the user was not found and proceed to the next store in the sequence

Save Reset

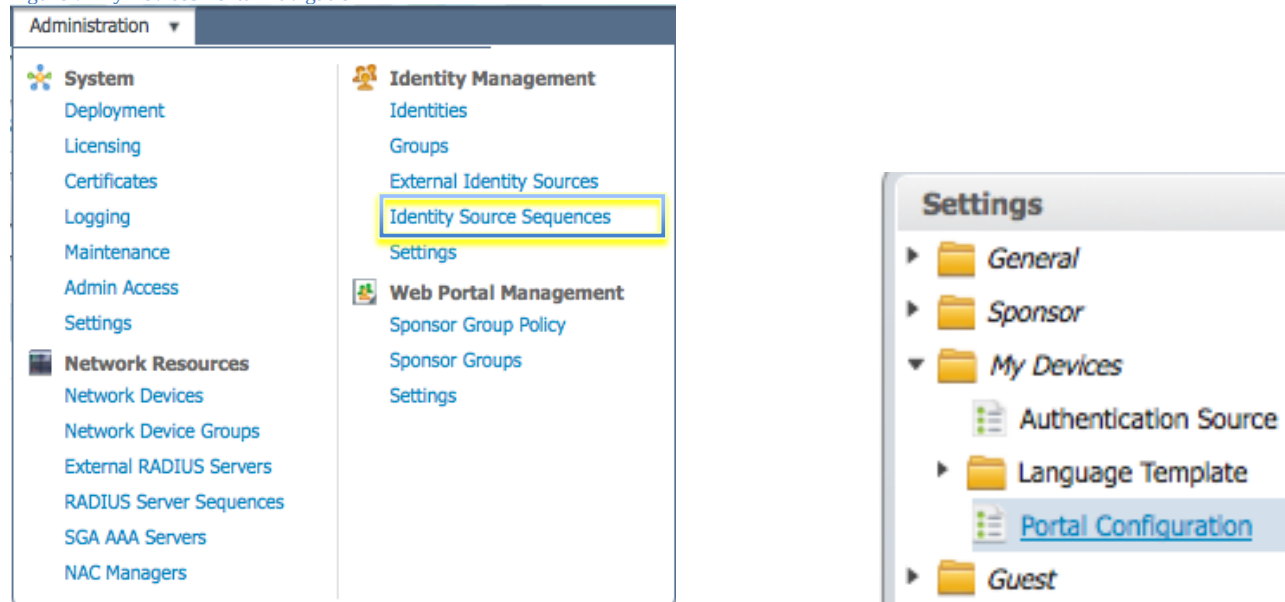
## Configuring My Devices Portal

The primary purpose of My Devices Portal is for end users to self serve bringing devices onto the network. While this portal can be used to enter any device into the ISE Endpoints Database and therefore allow it onto the network, it is intended for devices that don't have users or browsers and therefore can't go through the self-provisioning flow. These devices might include IV pumps, printers, game consoles, etc.

## Procedure 1 My Devices Portal settings

**Step 3 To Enable My Devices Portal, Administration → Web Portal Management → Settings → My Devices → Portal Configuration**

Figure 9: My Devices Portal Navigation



**Step 4** By default, the My Devices portal is enabled, however navigate to the portal management page for My Devices and verify that it is enabled

**Step 5** Click **ADD**

Figure 10: My Devices Portal Settings

The image shows the 'My Devices Portal Settings' page in the Cisco ISE administration interface. The page is divided into several sections: 'General', 'Acceptable Use Policy', 'Device Management', and 'Help Desk'. In the 'General' section, the 'Enable My Devices Portal' checkbox is checked. In the 'Acceptable Use Policy' section, the 'Enable the Acceptable Use Policy link' checkbox is checked, and there is a reminder text: 'Reminder: If the AUP link is enabled, please set the AUP text on all the appropriate My Devices Portal language templates.' In the 'Device Management' section, there is a text box for 'The maximum number of devices to register' with the value '5' entered, and a note '(Valid Range 1 to 20)'. In the 'Help Desk' section, there are two text boxes: 'Email Address' with the value 'imbashir@cisco.com' and 'Phone Number' with the value '4085264000'. At the bottom of the page, there are 'Save' and 'Reset' buttons.

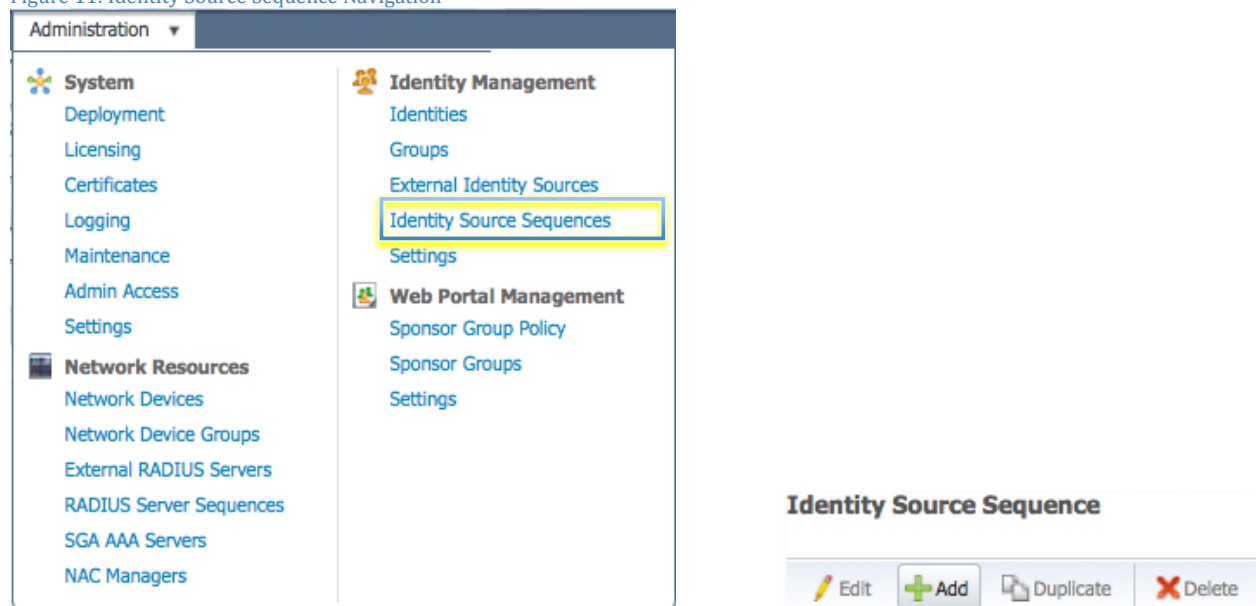
## Procedure 2 Create and ID Source Sequence for MyDevices Portal

Configure Identity Source Sequence, which defines the authentication sequence for login to the My Devices Portal.

**Step 1** Go to Administration → Identity Management → Identity Source Sequence.

**Step 2** Click **ADD**.

Figure 11: Identity Source Sequence Navigation



Step 3 Define the Identity Source Sequence for MyDevices Portal

Figure 12: Identity Source Sequence Settings

Identities
Groups
External Identity Sources
Identity Source Sequences
Settings

Identity Source Sequences List > [MyDevices\\_Portal\\_Sequence](#)

### Identity Source Sequence

▼ Identity Source Sequence

\* Name
MyDevices\_Portal\_Sequence

Description
A Built-in Identity Sequence For The My Devices Portal

▼ Certificate Based Authentication

☐ Select Certificate Authentication Profile

▼ Authentication Search List

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

Available		Selected	
Internal Endpoints	>	AD1	⬆
	<	Internal Users	⬆
	>>		⬇
	<<		⬇

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

☐ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

☒ Treat as if the user was not found and proceed to the next store in the sequence

Save
Reset

## Configuring Guest Portal Sequence

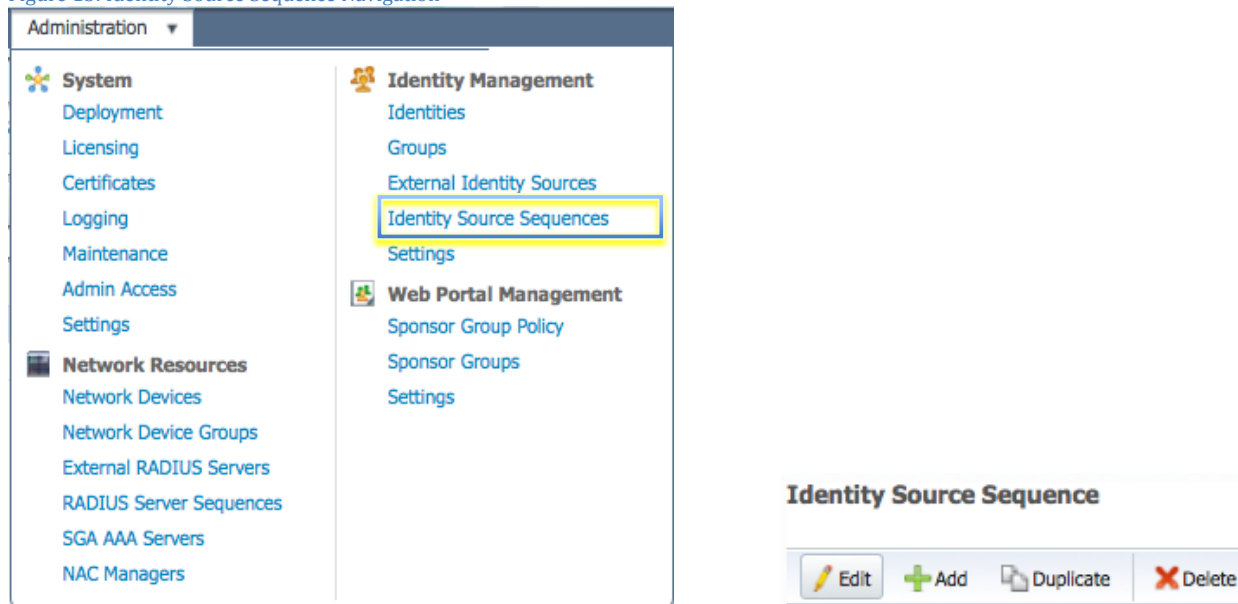
Guest portal will also be used to authenticate corporate users therefore its important to add Active Directory in to default Guest Portal Sequence

### Procedure 1 Configuring the Guest Portal Sequence

Step 1 Go to **Administration → Identity Management → Identity Source Sequence**.

Step 2 Edit “**Guest\_Portal\_Sequence**”.

Figure 13: Identity Source Sequence Navigation



Step 3 Add Active Directory to “Guest\_Portal\_Sequence”.

Figure 14: Identity Source Sequence Settings - Guest Portal

Identity Source Sequences List > [Guest\\_Portal\\_Sequence](#)

### Identity Source Sequence

**Identity Source Sequence**

\* Name:

Description:

**Certificate Based Authentication**

☐ Select Certificate Authentication Profile

**Authentication Search List**

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

Available		Selected
Internal Endpoints	>	Internal Users
	<	AD1
	>>	
	<<	

**Advanced Search List Settings**

Select the action to be performed if a selected identity store cannot be accessed for authentication

☐ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

☒ Treat as if the user was not found and proceed to the next store in the sequence



## Create a Client Provisioning Policy.

The Cisco Identity Services Engine looks at various elements when classifying the type of login session through which users access the internal network. We can leverage Client Provisioning Policy to create supplicant profiles to configure end points (e.g iPhones, iPad's, Windows, MAC OSx ..)

With Native Supplicant Provisioning (NSP), the Cisco ISE will have different provisioning policies per operating system. Each policy will contain a "Native Supplicant Profile" which dictates whether to use PEAP or EAP-TLS, what wireless SSID to connect to, and more. Additionally the Client Provisioning Policy will reference which provisioning wizard to use. Naturally, the supplicant one provision for an iPad will differ from that of an Android device. To determine which package to provision to an endpoint, we leverage the Client Provisioning Policies in the Cisco ISE to bind the supplicant profile to the provisioning wizard, per operating system.

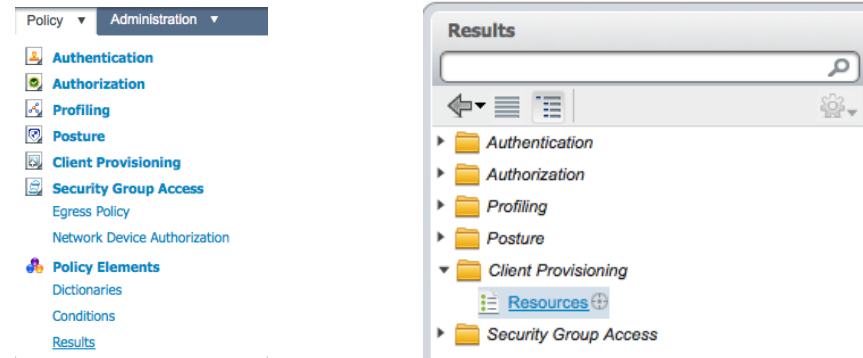
### Procedure 2 Create a Client Provisioning Policy

**Step 1** Create a Native Supplicant Profile. Go to **Policy** → **Policy Elements** → **Results**.

**Step 2** Click on **Client Provisioning** → **Resources**

**Step 3** Click **ADD**

Figure 15: Client Provisioning Resources Navigation



### Procedure 3 Name the Native Supplicant Profile

**Step 1** Select the Operating System

---

**Note:** We are able to configure one Supplicant Profile for all Operating Systems. However, we will be specifying different provisioning methods per operating-system later in this document.

---

**Step 2** Select Connection Type, **Wired** and/or **Wireless**.

**Step 3** Type your Corporate Wireless SSID, as configured on the Wireless LAN Controller.

**Step 4** Select the Allowed Protocols, in this case **“PEAP”**.

Figure 16: Native Supplicant Profile

Native Supplicant Profile > **PEAP-MSCHAPv2**

### Native Supplicant Profile

* Name	<input type="text" value="PEAP-MSCHAPv2"/>
Description	<input type="text" value="PEAP-MSCHAPv2"/>
* Operating System	<input type="text" value="ALL"/>
* Connection Type	<input type="checkbox"/> Wired <input checked="" type="checkbox"/> Wireless
* SSID	<input type="text" value="BYOD-Dot1x"/>
Security	<input type="text" value="WPA2 Enterprise"/>
* Allowed Protocol	<input type="text" value="PEAP"/>
<b>Optional Settings</b>	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

#### Procedure 4 Create Client Provisioning Policy (CPP)

In this, procedure we are creating the Client Provisioning Policy to configure the native supplicant for iOS and Android devices. Additionally CPP could be created for Windows and Mac OSx supplicants as well.

**Step 1** Download supplicant wizards for Windows and MAC OSx.

**Step 2** Go to Policy → Policy Elements → Results → Client Provisioning → Resources

**Step 3** On the right hand side, Click on ADD

**Step 4** Choose “Agent resources from Cisco site”

In this example we have selected WinSPWizard 1.0.0.15 and MacOSXSPWizard 1.0.0.999

Figure 17: Native Supplicant Wizard A

Download Remote Resources...


<input type="checkbox"/>	Name	Type	Version
<input type="checkbox"/>	MacOsXAgent 4.9.0.652	MacOsXAgent	4.9.0.652
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.3	MacOsXSPWizard	1.0.0.3
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.6	MacOsXSPWizard	1.0.0.6
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.7	MacOsXSPWizard	1.0.0.7
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.998	MacOsXSPWizard	1.0.0.998
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.999	MacOsXSPWizard	1.0.0.999
<input type="checkbox"/>	NACAgent 4.9.0.27	NACAgent	4.9.0.27
<input type="checkbox"/>	NACAgent 4.9.0.28	NACAgent	4.9.0.28
<input type="checkbox"/>	NACAgent 4.9.0.40	NACAgent	4.9.0.40
<input type="checkbox"/>	NativeSPPProfile 1.0.0.0	NativeSPPProfile	1.0.0.0
<input type="checkbox"/>	NativeSPPProfile 1.0.0.1	NativeSPPProfile	1.0.0.1
<input type="checkbox"/>	NativeSPPProfile 1.0.0.2	NativeSPPProfile	1.0.0.2
<input type="checkbox"/>	WebAgent 4.9.0.13	WebAgent	4.9.0.13
<input type="checkbox"/>	WebAgent 4.9.0.14	WebAgent	4.9.0.14
<input type="checkbox"/>	WebAgent 4.9.0.22	WebAgent	4.9.0.22
<input type="checkbox"/>	WinSPWizard 1.0.0.12	WinSPWizard	1.0.0.12


Step 5 Select the latest supplicant wizards.


Figure 18: Native Supplicant Wizards B


Figure 10: Native Supplicant Wizard

## Resources

 Edit

 Add

 Duplicate

 Delete

<input type="checkbox"/>	Name	Type	Version	Last Update
<input type="checkbox"/>	NACAgent 4.9.0.37	NACAgent	4.9.0.37	2012/04/14 06:38:31
<input type="checkbox"/>	MacOsXAgent 4.9.0.650	MacOsXAgent	4.9.0.650	2012/04/14 06:38:37
<input type="checkbox"/>	ComplianceModule 3.5.526.2	ComplianceModule	3.5.526.2	2012/04/14 06:38:41
<input type="checkbox"/>	WebAgent 4.9.0.20	WebAgent	4.9.0.20	2012/04/14 06:38:49
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.999	MacOsXSPWizard	1.0.0.999	2012/04/13 01:15:21
<input type="checkbox"/>	PEAP	Native Supplicant Profile	Not Applicable	2012/04/12 23:21:35
<input type="checkbox"/>	WinSPWizard 1.0.0.15	WinSPWizard	1.0.0.15	2012/04/18 00:58:10
<input type="checkbox"/>	EAP_TLS	Native Supplicant Profile	Not Applicable	2012/04/18 01:49:07

## Procedure 5 Create a Client Provisioning Policy for Apple iOS

Step 1 Go to Policy → Client Provisioning

Step 2 On the right hand side, Click on Actions → Insert new Policy above

Step 3 Create an Apple iOS CPP policy.

Figure 19: Apple iOS Client Provisioning Policy

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> ios	If Any and	Mac iOS All and	Condition(s) then	PEAP-MSCHAPv2 Actions

Step 4 Create an Android CPP policy.

Figure 20: Android Client Provisioning Policy

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> android	If Any and	Android and	Condition(s) then	PEAP-MSCHAPv2 Actions

Step 5 (Optional): Create a MAC OSx CPP policy.

Figure 21: OSx Client Provisioning Policy

Step 6 (Optional): Create a Windows CPP policy.

Figure 22: Windows Client Provisioning Policy

Note: Windows and OSx have additional supplicant provisioning profiles, which are Java-based wizards to do the supplicant and certificate provision and are downloadable from cisco.com as part of updates.

## Policy Configuration.

In this configuration section, we will create multiple ACL's within the Wireless LAN Controller, which would be used in the policy later to redirect clients selected for BYOD supplicant and certificate provisioning, to deny traffic when the device has been blacklisted, and more.

**The Cisco Identity Services Engine IP address = 10.35.50.165**

**Internal Corporate Networks = 192.168.0.0, 172.16.0.0 (to redirect)**

### Procedure 1 Configure the Supplicant Provisioning ACL

In this configuration section, we will create an ACL within the Wireless LAN Controller, which would be used in the policy later to redirect clients selected for BYOD supplicant and certificate provisioning.

Step 1 Navigate to: Security → Access Control Lists.

Step 2 Add a new ACL, named “NSP-ACL”

Figure 23: Access Control List for re-directing client to BYOD flow

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0	<input checked="" type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0	<input checked="" type="checkbox"/>
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	<input checked="" type="checkbox"/>
6	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
7	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
8	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
9	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>

Explanation of the **NSP-ACL** in Figure 17 is as follows

1. Allow all traffic “outbound” from Server to Client
2. Allow ICMP traffic “inbound” from Client to Server for trouble shooting, it is optional

3. Allow all traffic “inbound” from Client to Server to ISE for Web Portal and supplicant and Certificate provisioning flows
4. Allow DNS traffic “inbound” from Client to Server for name resolution.
5. Allow DHCP traffic “inbound” from Client to Server for IP addresses.
6. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
7. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
8. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
9. Permit all the rest of traffic (Optional)

## Procedure 2 Create the Blacklist ACL

Create an ACL named “**BLACKLIST-ACL**” in the Wireless LAN Controller, which would be used in the policy later to restrict access to devices that have been blacklisted.

Figure 24: Blacklist ACL

Access Control Lists > Edit [< Back](#) [Add New Rule](#)

**General**

Access List Name: BLACKLIST-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
<a href="#">1</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0	<input checked="" type="checkbox"/>
<a href="#">2</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
<a href="#">3</a>	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
<a href="#">4</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0	<input checked="" type="checkbox"/>
<a href="#">5</a>	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>

Explanation of the **BLACKLIST-ACL** in Figure 18 is as follows

1. Allow all traffic “outbound” from Server to Client
2. Allow ICMP traffic “inbound” from Client to Server for trouble shooting, it is optional
3. Allow all traffic “inbound” from Client to Server to ISE for Blacklist Web Portal page
4. Allow DNS traffic “inbound” from Client to Server for name resolution.
5. Deny all the rest of traffic.

**Step 3** Create an ACL named “**NSP-ACL-Google**” in the Wireless LAN Controller, which would be used in the policy later for provisioning Android devices.

Figure 25: Google Access ACL  
Access Control Lists > Edit

### General

Access List Name NSP-ACL-Google

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
<a href="#">1</a>	Permit	0.0.0.0 /	10.35.50.165 /	Any	Any	Any	Any	Inbound	110	▼
		0.0.0.0	255.255.255.255							
<a href="#">2</a>	Permit	10.35.50.165 /	0.0.0.0 /	Any	Any	Any	Any	Outbound	114	▼
		255.255.255.255	0.0.0.0							
<a href="#">3</a>	Deny	0.0.0.0 /	10.0.0.0 /	Any	Any	Any	Any	Inbound	5	▼
		0.0.0.0	255.0.0.0							
<a href="#">4</a>	Deny	0.0.0.0 /	192.168.0.0 /	Any	Any	Any	Any	Inbound	0	▼
		0.0.0.0	255.255.0.0							
<a href="#">5</a>	Deny	0.0.0.0 /	172.16.0.0 /	Any	Any	Any	Any	Inbound	0	▼
		0.0.0.0	255.240.0.0							
<a href="#">6</a>	Deny	0.0.0.0 /	171.71.181.0 /	Any	Any	Any	Any	Inbound	0	▼
		0.0.0.0	255.255.255.0							
<a href="#">7</a>	Permit	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	3449	▼
		0.0.0.0	0.0.0.0							

Explanation of the **NSP-ACL-Google** in above Figure as follows

1. Allow all traffic "Inbound" to ISE (this step is optional).
2. Allow all traffic "Outbound" from ISE (this step is optional).
3. Deny all traffic "inbound" to corporate internal subnet (can be configured per company policy)
4. Deny all traffic "inbound" to corporate internal subnet (can be configured per company policy)
5. Deny all traffic "inbound" to corporate internal subnet (can be configured per company policy)
6. Permit all the rest of traffic (This could be limited to Google Play subnet only but please note that Google Play subnets could be different per location).

**Note:** If required additional lines could be added for troubleshooting e.g. ICMP.

**Note:** Please review Appendix B for more information on how to allow play.google.com ONLY. If required, additional lines could be added for troubleshooting e.g. ICMP.

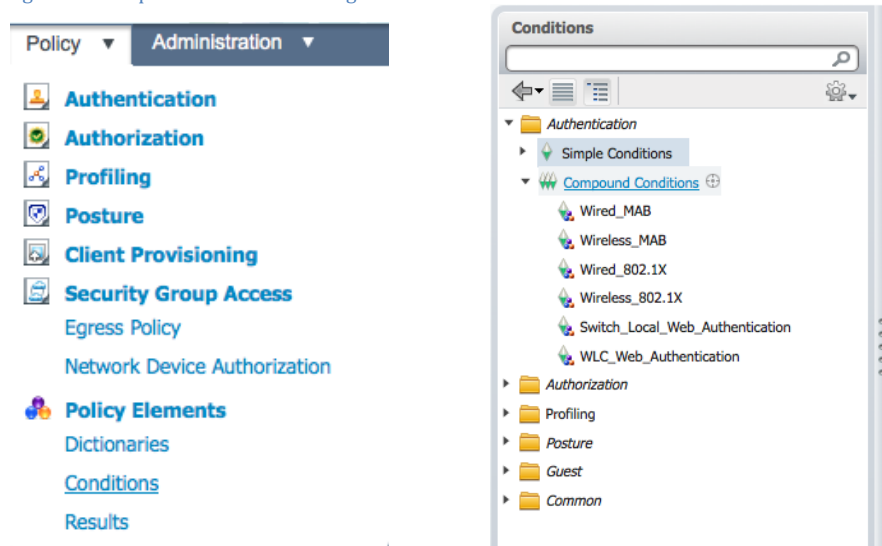
## Configure an Authentication Policy

### Procedure 1 Compound **Authentication** policy configuration.

Review Compound Authentication Conditions, which would be later, used in the policy configurations. We are reviewing these built-in policies to ensure they exist and have not been modified, as they will be referenced in our new policies.

**Step 4** Click Policy → Conditions → Authentication → Compound Conditions

Figure 26 Compound Conditions Navigation



#### Step 5 Review a compound condition named “Wireless\_MAB”

**“Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Wireless - IEEE 802.11”**

Figure 27 Wireless MAB

Authentication Compound Condition List > **Wireless\_MAB**

### Authentication Compound Conditions

\* Name:

Description:

Condition Name	Expression	AND
<input type="text"/>	Radius:Service-Type <input type="text" value="Equals"/> Call Check	AND
<input type="text"/>	Radius:NAS-Port-Type <input type="text" value="Equals"/> Wireless - I	

#### Step 6 Review a compound condition named “Wired\_MAB”

**“Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Ethernet”**

Figure 28 Wired MAB

Authentication Compound Condition List > **Wired\_MAB**

### Authentication Compound Conditions

\* Name:

Description:

Condition Name	Expression	AND
<input type="text"/>	Radius:Service-Type <input type="text" value="Equals"/> Call Check	AND
<input type="text"/>	Radius:NAS-Port-Type <input type="text" value="Equals"/> Ethernet	

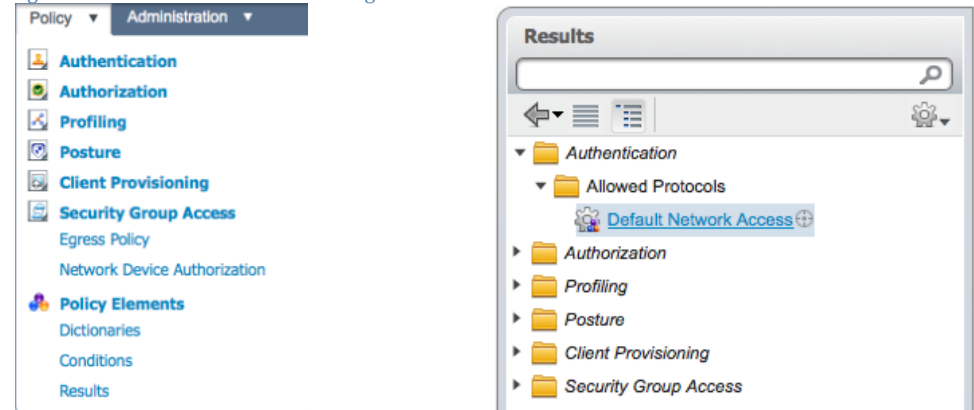
## Procedure 2      Verify Default Network Access Result

This procedure describes the current protocol settings under “**Default Network Access**”.

Step 7 Click Policy → Policy Elements → Results

Step 8 Click Authentication → Allowed Protocols → Default Network Access

Figure 29 Default Network Access Navigation



---

**Note:** Please verify protocol settings as per the following screen shot since we will be using the pre-built Default Network Access object for allowed protocols... Please ensure your default object has not been changed and configuration matches the following screenshot

---



Figure 30 Default Network Access Policy  
Allowed Protocols Services List > [Default Network Access](#)

**Allowed Protocols**

Name: Default Network Access

Description: Default Allowed Protocol Service

▼ Allowed Protocols

☒ Process Host Lookup

**Authentication Protocols**

▼ ☒ Allow PAP/ASCII

☐ Detect PAP as Host Lookup

☐ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

▼ ☒ Allow EAP-MD5

☐ Detect EAP-MD5 as Host Lookup

☒ Allow EAP-TLS

☐ Allow LEAP

▼ ☒ Allow PEAP

**PEAP Inner Methods**

☒ Allow EAP-MS-CHAPv2

☒ Allow Password Change Retries: 1 (Valid Range 0 to 3)

☒ Allow EAP-GTC

☒ Allow Password Change Retries: 1 (Valid Range 0 to 3)

☒ Allow EAP-TLS

▼ ☒ Allow EAP-FAST

▼ ☒ Allow EAP-FAST

**EAP-FAST Inner Methods**

☒ Allow EAP-MS-CHAPv2

☒ Allow Password Change Retries: 3 (Valid Range 1 to 3)

☒ Allow EAP-GTC

☒ Allow Password Change Retries: 3 (Valid Range 1 to 3)

☒ Allow EAP-TLS

☒ Use PACs ☐ Don't Use PACs

Tunnel PAC Time To Live: 90 Days

Proactive PAC update will occur after 90 % of PAC Time To Live has expired

☒ Allow Anonymous In-Band PAC Provisioning

☒ Allow Authenticated In-Band PAC Provisioning

☒ Server Returns Access Accept After Authenticated Provisioning

☐ Accept Client Certificate For Provisioning

☒ Allow Machine Authentication

Machine PAC Time To Live: 1 Weeks

☒ Enable Stateless Session Resume

Authorization PAC Time To Live: 1 Hours

☐ Enable EAP Chaining

☐ Preferred EAP Protocol: LEAP

**Step 9 Review Authentication Policy Configuration**, following screenshot is full policy view for reference, individual policies will be configured in subsequent steps

Figure 31 Authentication Policy Configuration

**Authentication Policy**

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

Policy Type: ☐ Simple ☒ Rule-Based

1. ☒ MAB : If Wired\_MAB... allow protocols Allowed Protocol : Default Network and...

2. ☒ Default : use Dot1x

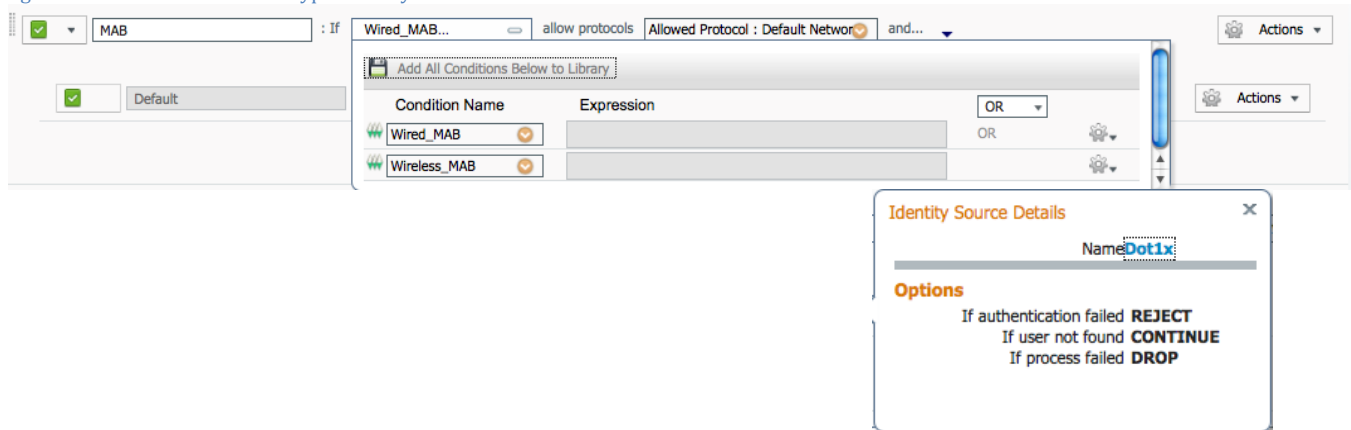
3. ☒ Dot1X : If Wired\_802.1X... allow protocols Allowed Protocol : Default Network and...

4. ☒ Default : use Dot1x

5. ☒ Default Rule (If no match) : allow protocols Allowed Protocol : Default Network and use identity source : Internal Users

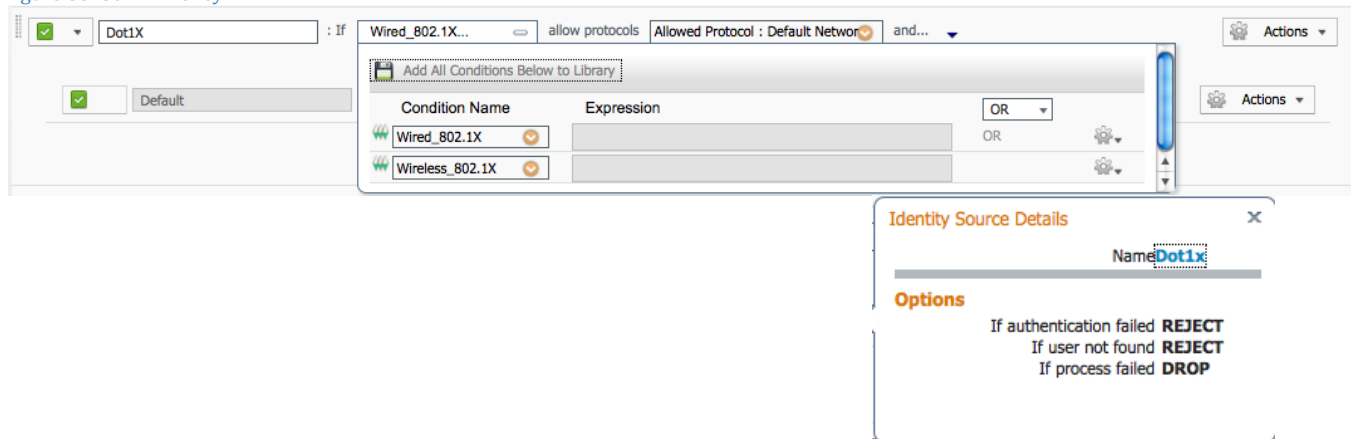
**Step 10 Authentication policy for MAB**, please add conditions (**Wired\_MAB OR Wireless\_MAB**)

Figure 32 MAC Authentication Bypass Policy



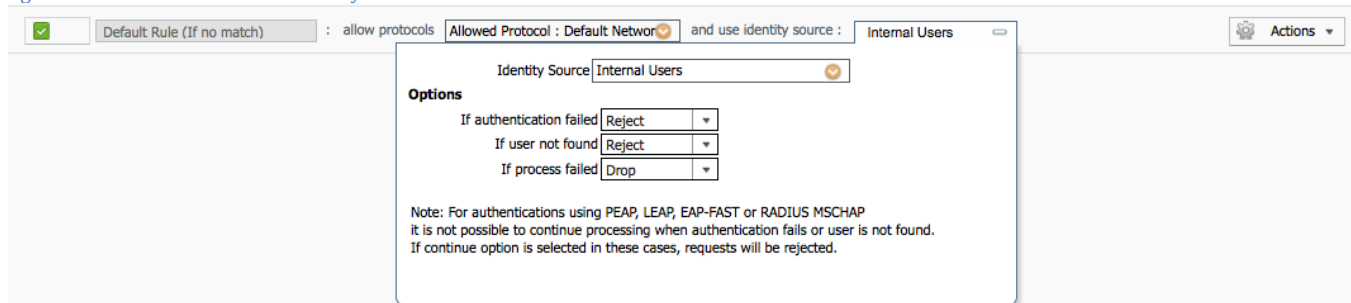
Step 11 Authentication policy for **Dot1x**, please add conditions (**Wired\_802.1X** OR **Wireless\_802.1X**)

Figure 33 802.1X Policy



Step 12 Default Authentication policy.

Figure 34 Default Authentication Policy



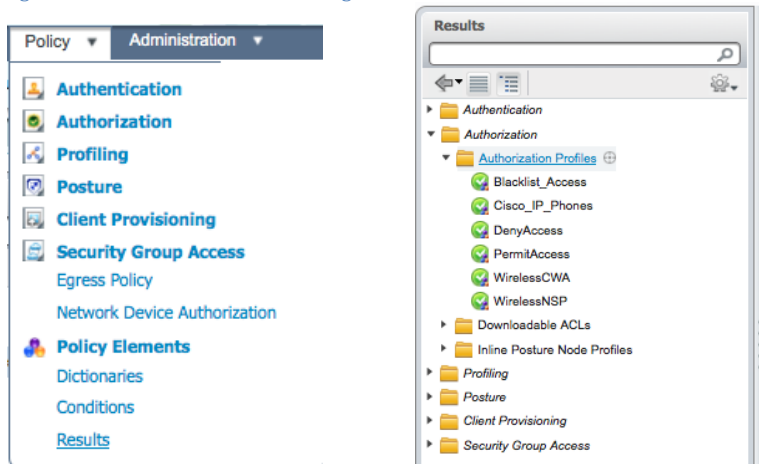
### Procedure 3 Configure an Authorization policy named “CWA”

Step 13 Click Policy → Policy Elements → Results.

Step 14 Choose Authorization → Authorization Profiles

Step 15 Click “ADD”

Figure 35 Authorization Profiles Navigation

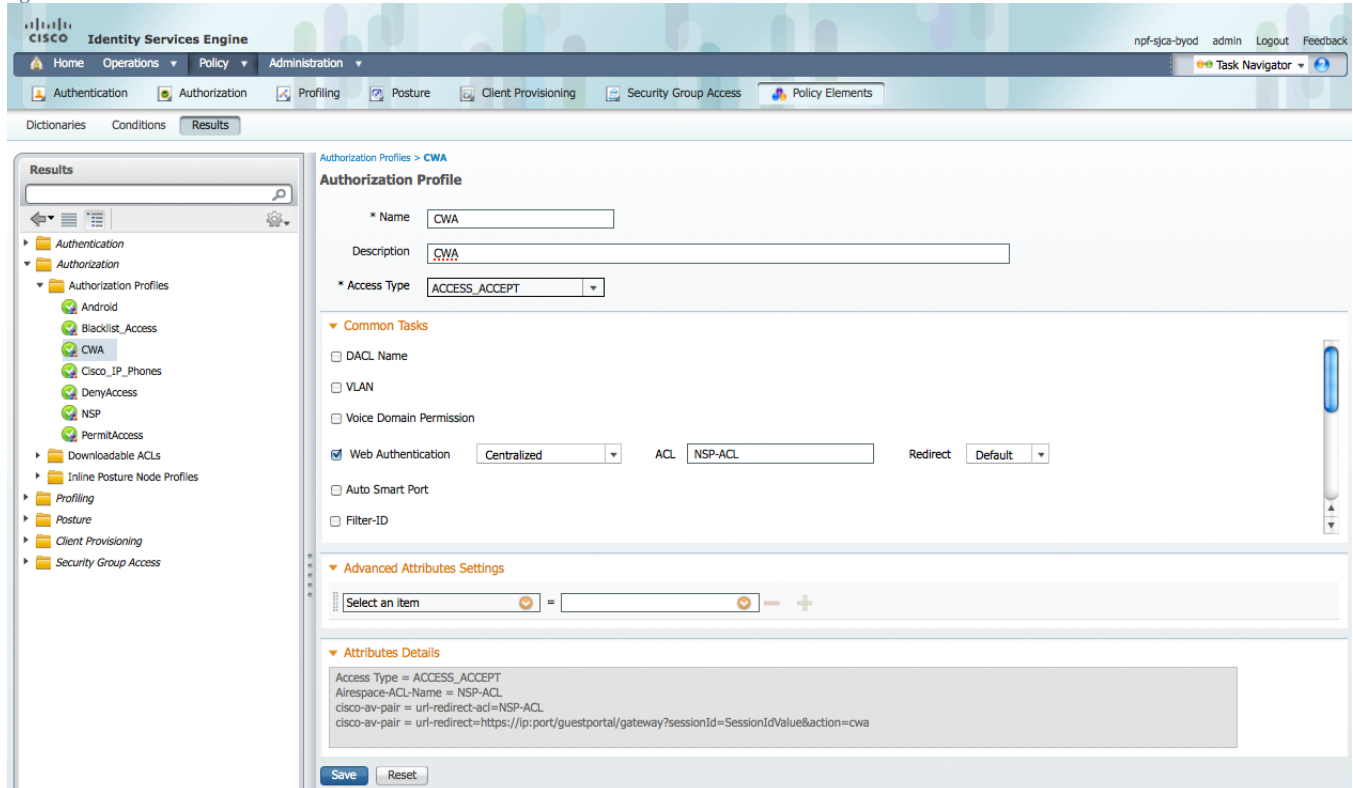


#### Step 16 Add an Authorization Profile named “CWA”.

Central web authentication (CWA) offers the possibility to have a central device acting as web portal (here, the Cisco Identity Services Engine). In Central web-authentication client is shifted to layer 2 along with mac/dot1x authentication, the Cisco Identity Services Engine then returns a special attributes indicating to the switch that a web redirection has to happen. Globally, if the MAC address of the client station is not known by the radius server (but other criteria can also be used), the server returns redirection attributes and the switch authorizes the station (via MAB) but places an access-list to redirect the web traffic to the portal.

Once the user logs in on the guest portal, it is possible via Change of Authorization (CoA) to bounce the switchport so that a new layer 2 MAB authentication occurs. The ISE can then remember it was a webauth user and apply layer 2 attributes (like dynamic VLAN assignment) to the user. An activeX component can also force the client PC to refresh its IP address.

Figure 36 CWA Authorization Profile



#### Step 17 Add an Authorization Profile named “CWA\_GooglePlay”.

This profile will be used by Android devices to allow access to Google Play for downloading “Cisco Network Setup Assistant”.

Figure 37 CWA Authorization Profile for Android to Access Google

**Authorization Profile**

\* Name

Description

\* Access Type

▼ **Common Tasks**

☐ DACL Name

☐ VLAN

☐ Voice Domain Permission

☒ Web Authentication  ACL  Redirect

☐ Auto Smart Port

☐ Filter-ID

▼ **Advanced Attributes Settings**

=  - +

▼ **Attributes Details**

Access Type = ACCESS\_ACCEPT  
Airespace-ACL-Name = NSP-ACL-Google  
cisco-av-pair = url-redirect-acl=NSP-ACL-Google  
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

#### Procedure 4 Review Policy conditions under Authorization Profiles

Step 18 Click Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 19 Review Profile named “**Blacklist\_Access**”

Figure 38 Blacklist Authorization Profile

Authorization Profiles > **Blacklist\_Access**

### Authorization Profile

\* Name

Description

\* Access Type

---

▼ Common Tasks

- ☐ DACL Name
- ☐ VLAN
- ☐ Voice Domain Permission
- ☐ Web Authentication
- ☐ Auto Smart Port
- ☐ Filter-ID

---

▼ Advanced Attributes Settings

Cisco:cisco-av-pair	=	url-redirect=https://ip:port/mydev
Cisco:cisco-av-pair	=	url-redirect-acl=BLACKLIST-ACL

---

▼ Attributes Details

Access Type = ACCESS\_ACCEPT

cisco-av-pair = url-redirect=https://ip:port/mydevices/blackhole.jsp

cisco-av-pair = url-redirect-acl=BLACKLIST-ACL

#### Advanced Attribute Settings

Cisco:cisco-av-pair = url-redirect=https://ip:port/mydevices/blackhole.jsp

Cisco:cisco-av-pair = url-redirect-acl=BLACKLIST-ACL

Step 20 Create an Authorization Profile named “NSP”

Figure 39 Native Supplicant Provisioning Authorization Profile

Authorization Profiles > **NSP**

### Authorization Profile

\* Name

Description

\* Access Type

▼ Common Tasks

☐ DACL Name

☐ VLAN

☐ Voice Domain Permission

☒ Web Authentication  ACL

☐ Auto Smart Port

☐ Filter-ID

▼ Advanced Attributes Settings

Select an item  =

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
Airespace-ACL-Name = NSP-ACL  
cisco-av-pair = url-redirect-acl=NSP-ACL  
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp

---

**Note:** Please also click ☒ Airespace ACL Name

Step 21 Create an Authorization Profile named “**NSP\_Google**”

Figure 40 NSP\_Google Authorization Profile

**Authorization Profile**

\* Name

Description

\* Access Type

**Common Tasks**

☒ Web Authentication  ACL

☐ Auto Smart Port

☐ Filter-ID

☐ Reauthentication

☐ MACSec Policy

☐ NEAT

**Advanced Attributes Settings**

Select an item =  - +

**Attributes Details**

Access Type = ACCESS\_ACCEPT  
Airespace-ACL-Name = NSP-ACL-Google  
cisco-av-pair = url-redirect-acd=NSP-ACL-Google  
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp

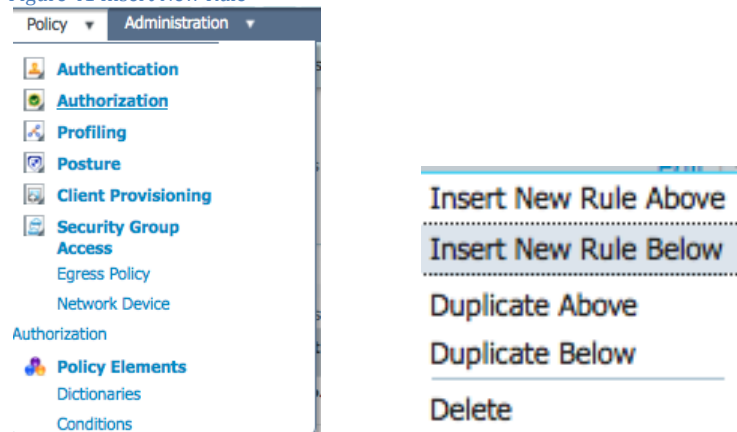
**Note:** Please also click ☒ Airespace ACL Name

## Procedure 5 Add the Authorization Policies

Step 22 Click Policy → Authorization

Step 23 Click “Insert New Rule Below”

Figure 41 Insert New Rule



Please add the following Authorization Policy

**Black List Default** = This is the Default Authorization rule for blacklisting the devices, it could be customized as per company policy where devices could either be redirected to a restricted web page or even not allowed to be on the network once blacklisted.

**Profiled Cisco IP Phones** = Default Authorization rule for Cisco IP Phones.

**Corp\_Owned** = This Authorization Rule is added for devices which would by-pass BYOD supplicant and certificate provisioning flows when they are classified as corporate assets "**Corp\_Assets**" and coming over Corporate Wireless SSID using 802.1x using protocol MSCHAPV2.

**Android\_SingleSSID** = This Authorization Rule is added for Android devices since they require to download the Cisco Network Setup Assistant to complete the provisioning. The rule is specific to Single SSID setup. Once the Android device hits the "Register" button during device registration, ISE sends a Re-Auth COA to the controller. When the Android connects back to the network the session ID remains same since COA issued from ISE was Ra-Auth and NOT Session Terminate. ISE then applies the NSP\_Google permission to continue with the provisioning process

**Android\_DualSSID** = This Authorization Rule is added for Android devices since they require to download the Cisco Network Setup Assistant to complete the provisioning. The rule is specific to Dual SSID setup. Once the Android device hits the "Register" button during device registration, ISE sends a Re-Auth COA to the controller. When the Android connects back to the network the session ID remains same since COA issued from ISE was Ra-Auth and NOT Session Terminate. ISE then applies the NSP\_Google permission to continue with the provisioning process

**CWA** = Authorization rule added for Central Web Authentication.

**NSP** = This Authorization Rule is added for devices which will go through the BYOD supplicant and certificate provisioning flows when coming over Corporate Wireless SSID using 802.1x using protocol MSCHAPV2.

**PERMIT** = Devices which have completed BYOD Supplicant and Certificate provisioning, with a certificate using EAP-TLS for authentication and coming over Corporate Wireless SSID will fall under this Authorization Policy.

**Default** = Default Authorization Policy set as Deny Access.



Figure 42 Authorization Policy

	Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
⋮	✓	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_802.1X	then Blacklist_Access <a href="#">Edit</a>   ▼
⋮	✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones <a href="#">Edit</a>   ▼
⋮	✓	Corp_Owned	if <b>Corp_Assets</b> AND (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 )	then PermitAccess <a href="#">Edit</a>   ▼
⋮	✓	Android_SingleSSID	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android )	then NSP_Google <a href="#">Edit</a>   ▼
⋮	✓	Android_DualSSID	if (Wireless_MAB AND Session:Device-OS EQUALS Android )	then CWA_GooglePlay <a href="#">Edit</a>   ▼
⋮	✓	CWA	if Wireless_MAB	then CWA <a href="#">Edit</a>   ▼
⋮	✓	NSP	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 )	then NSP <a href="#">Edit</a>   ▼
⋮	✓	PERMIT	if Wireless_802.1X	then PermitAccess <a href="#">Edit</a>   ▼
	✓	Default	if no matches, then	DenyAccess <a href="#">Edit</a>   ▼



You are done!

Please see the how-to-guide “[BYOD-Using\\_Certificates\\_for\\_Differentiated\\_Access](#)” If interested in provisioning Certificates along with the supplicant profile.

# Appendix A: Android and Play.Google.Com

---

## Why Android is Different

Android devices need to be treated differently than iOS Devices and/or Windows. This is partially because no two Android devices are exactly the same, but also because of the requirement to use a supplicant provisioning App to configure the Supplicant and Certificate for Android.

By default, the Android devices will not accept the App from just any source; it must come from a trusted App Store, such as “play.google.com”. While it is possible to configure the Cisco ISE to host the Supplicant Provisioning Wizard (SPW) App, the end-users’ Android devices will not be configured trust the Cisco ISE as an App Store. Therefore, unlike: Windows, MAC, and iOS; Android devices must have access to the internet to participate in BYOD and Native Supplicant Provisioning.

During the TrustSec testing, it was discovered that in many cases Google Play uses TCP and UDP ports 5228. However, this was not enough for all tested Android devices to work. Internet searches (see Appendix C: References) yielded that port 8880 may need to be opened as well. Depending on the Android’s configuration the end-user may be prompted for either “Internet” or “Play Store” options.

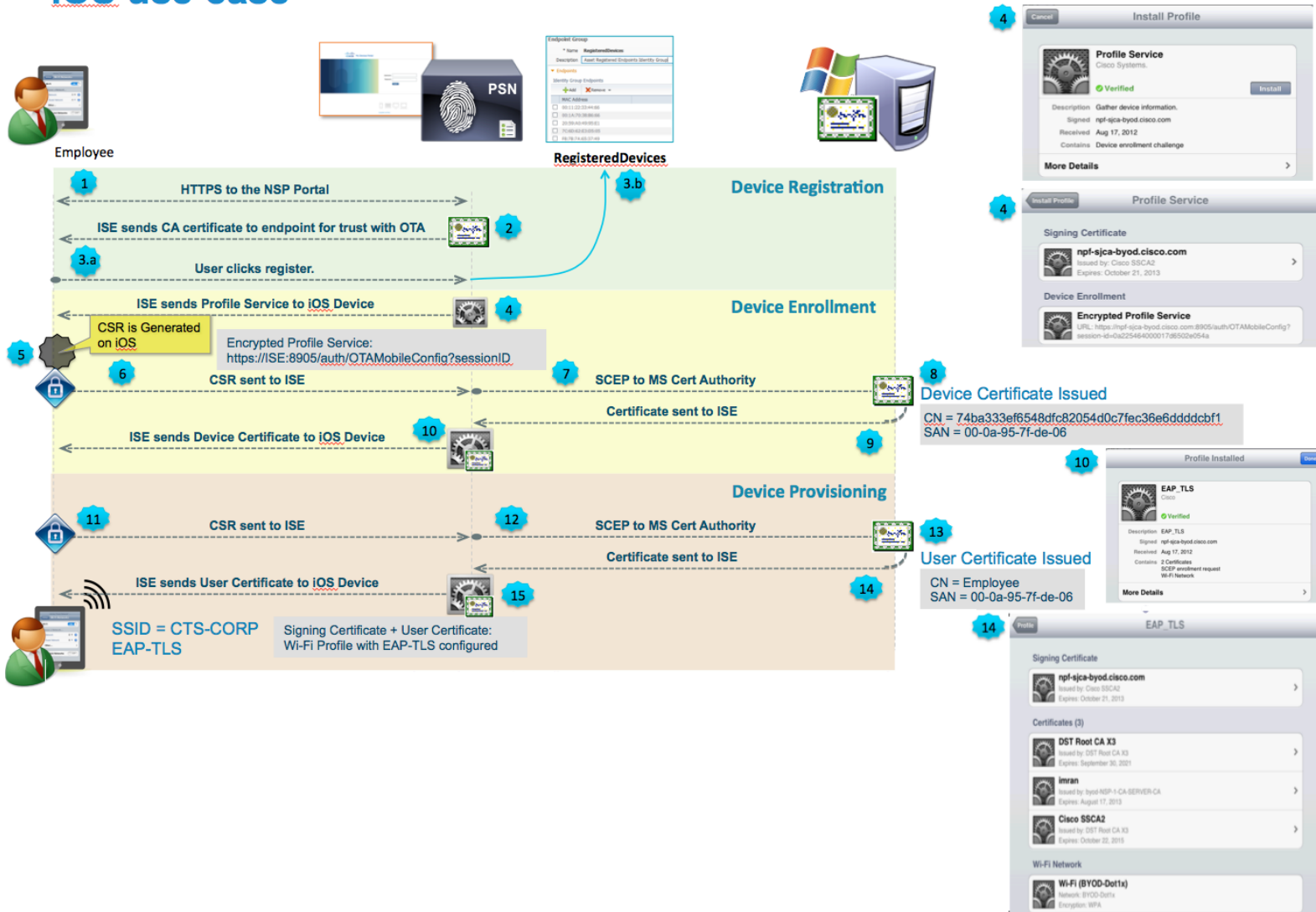
What worked in the testing lab:

Android Option	Network Range to Open	TCP & UDP Ports
Google Play option	74.125.00/16 173.194.0.0/16	TCP/UDP:5228 TCP/UDP:8889
Internet Option	74.125.00/16 173.194.0.0/16	UDP: 5228 TCP: All Ports

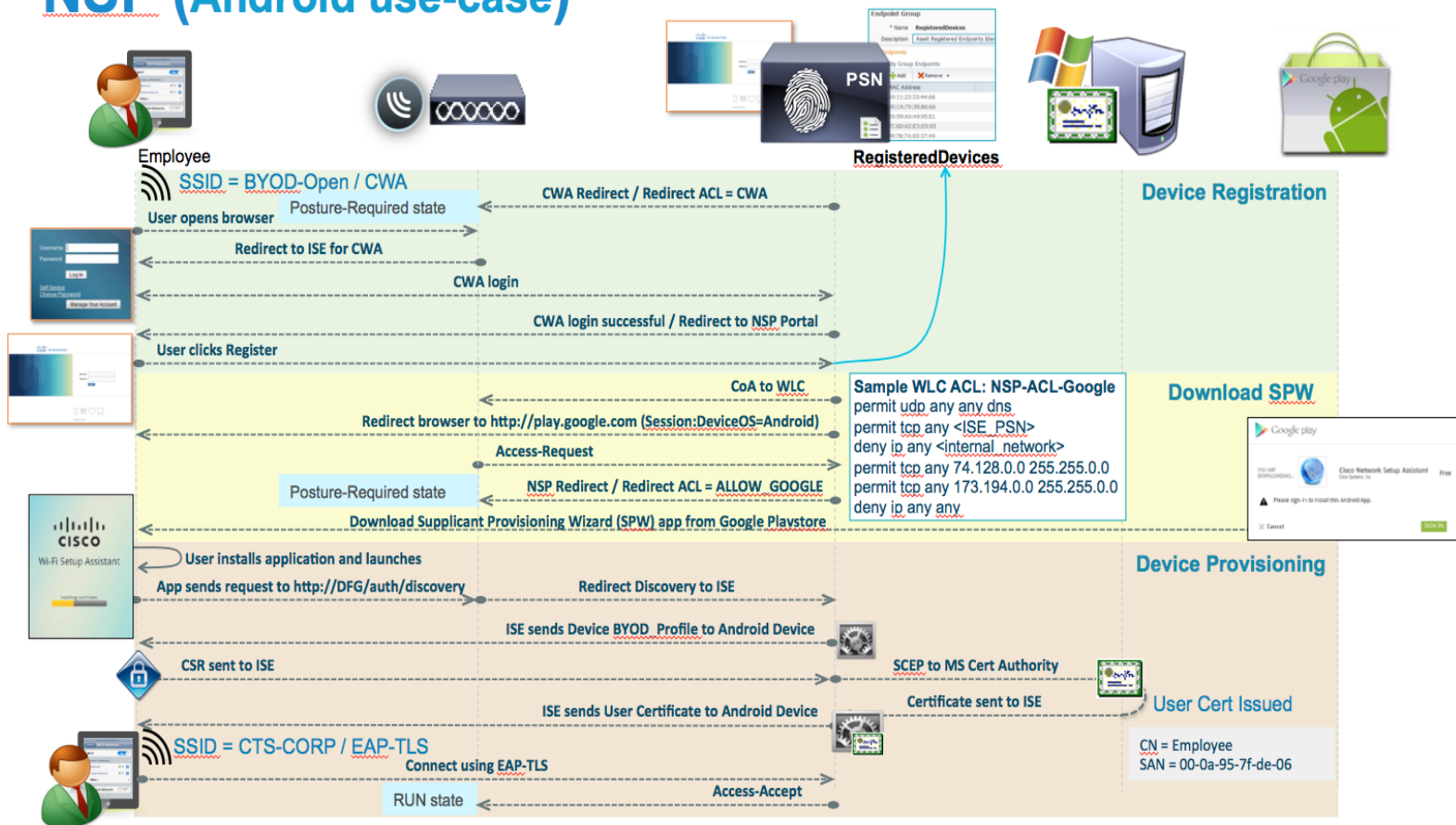
# Appendix B: BYOD flows

This section goes through BYOD flows for iOS and Android Devices

## iOS use-case



## NSP (Android use-case)



# Appendix C: References

---

## Cisco TrustSec System:

- <http://www.cisco.com/go/trustsec>
- [http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing\\_DesignZone\\_TrustSec.html](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html)

## Device Configuration Guides:

### Cisco Identity Services Engine User Guides:

[http://www.cisco.com/en/US/products/ps11640/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html)

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:  
[http://www.cisco.com/en/US/products/ps6406/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html)
- For Cisco Catalyst 3000 series switches:  
[http://www.cisco.com/en/US/products/ps7077/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html)
- For Cisco Catalyst 3000-X series switches:  
[http://www.cisco.com/en/US/products/ps10745/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html)
- For Cisco Catalyst 4500 series switches:  
[http://www.cisco.com/en/US/products/hw/switches/ps4324/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html)
- For Cisco Catalyst 6500 series switches:  
[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)
- For Cisco ASR 1000 series routers:  
[http://www.cisco.com/en/US/products/ps9343/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html)
- For Cisco Wireless LAN Controllers:  
[http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc\\_cg70MR1.html](http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html)