On-boarding and Provisioning with Cisco Identity Services Engine

Secure Access How-To Guide Series

Date: April 2012
Author: Imran Bashir
# Table of Contents

Overview ........................................................................................................................................... 3

Scenario Overview ............................................................................................................................ 4
  Dual SSID Wireless BYOD Self Registration .................................................................................... 4
  Single SSID Wireless BYOD Self Registration ................................................................................ 4
  Architecture/ Diagram ..................................................................................................................... 5
  Components ................................................................................................................................. 6

Cisco ISE Configuration ..................................................................................................................... 6
  Identify Users for BYOD Flow ......................................................................................................... 6
  Create an Identity Source Sequence ............................................................................................ 9
  Configuring My Devices Portal ..................................................................................................... 11
  Configuring Guest Portal Sequence ............................................................................................ 13
  Create a Client Provisioning Policy .............................................................................................. 15
  Policy Configuration ................................................................................................................... 18
  Configure an Authentication Policy ............................................................................................ 20

Appendix A: Android and Play.Google.Com .................................................................................... 33
  Why Android is Different? ............................................................................................................ 33

Appendix B: BYOD flows ................................................................................................................ 34

Appendix C: References .................................................................................................................. 36
  Cisco TrustSec System .................................................................................................................. 36
  Device Configuration Guides: ....................................................................................................... 36
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

<table>
<thead>
<tr>
<th>Device</th>
<th>Certificate Store</th>
<th>Certificate Info</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone/iPad/iPod</td>
<td>Device Certificate Store (configuration profiles)</td>
<td>Can be viewed through: Settings → General → Profile</td>
<td>5.0 and above</td>
</tr>
<tr>
<td>Android</td>
<td>Device Encrypted Certificate Store</td>
<td>Cannot be viewed. But it may be cleared from: Settings → Location &amp; Security → Clear Storage (Clear all device certificates and passwords)</td>
<td>3.2 &amp; above</td>
</tr>
</tbody>
</table>
| 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
SPW (Supplicant MAC and is not getting installed when we select the option "MAC App Store and identified developers" in security & Privacy Preference Pane
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 is designed for users to follow 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

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).

Employee associates to Guest SSID (BYOD-Open).

Opens a browser and is redirected to the Cisco ISE CWA (Central Web Auth) Guest portal

Employee enters their corporate username and password in the standard Guest portal

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

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)

Employee selects accept and begins downloading and installing the supplicant provisioning wizard

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.

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).

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 1. Network Diagram
Components

Table 2: Components Used in this Document

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

**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.

**Configure a user group**

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

**Step 2** Click on ADD.
Step 3 Create an Identity Group.

In this example we are naming our Identity Group: “Employee”
Create a user in the Employee Group

Step 1  Navigate to Administration → Identity Management → Identities → Users
Step 2  Click on ADD
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.

Create an Identity source sequence.

**Step 1**  Administration → Identity Source Sequence

**Step 2**  Click on ADD
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.
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.

**My Devices Portal settings**

**Step 1** To Enable My Devices Portal, Administration → Web Portal Management → Settings → My Devices → Portal Configuration.

![My Devices Portal Navigation]

**Figure 7.** My Devices Portal Navigation

**Step 2** 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 3** Click ADD.

![My Devices Portal Settings]

**Figure 8.** My Devices Portal Settings

**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 9. Identity Source Sequence Navigation

Step 3  Define the Identity Source Sequence for MyDevices Portal
Configuring Guest Portal Sequence

Guest portal will also be used to authenticate corporate users therefore it’s important to add Active Directory into default Guest Portal Sequence

**Configuring the Guest Portal Sequence**

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

**Step 2**  Edit “Guest_Portal_Sequence”.

Figure 10. Identity Source Sequence Settings
Step 3  Add Active Directory to "Guest_Portal_Sequence".

Figure 11. Identity Source Sequence Navigation

Figure 12. Identity Source Sequence Settings - Guest Portal
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.

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 13. Client Provisioning Resources Navigation](image)

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”.
**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 14. Client Provisioning Resources Navigation**

**Figure 15. Native Supplicant Wizard A**
Step 5  Select the latest supplicant wizards.

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.

Step 4  Create an Android CPP policy.

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

Step 6  (Optional): Create a Windows CPP 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.

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 1:** Access Control List for re-directing client to BYOD flow

**Figure 21.**

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)

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 2: Blacklist ACL

<table>
<thead>
<tr>
<th>Access Control Lists &gt; Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td>Access List Name</td>
</tr>
<tr>
<td>Deny Counters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Seq</th>
<th>Action</th>
<th>Source IP/Mask</th>
<th>Destination IP/Mask</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>DSCP</th>
<th>Direction</th>
<th>Number of Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Permit</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Outbound</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Permit</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0</td>
<td>ICMP</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Permit</td>
<td>0.0.0.0/0</td>
<td>10.35.50.155</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Permit</td>
<td>0.0.0.0/0</td>
<td>255.255.255.255</td>
<td>UDP</td>
<td>Any</td>
<td>DNS</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Deny</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 22.

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-Googl” in the Wireless LAN Controller, which would be used in the policy later for provisioning Android devices.
**Access Control Lists > Edit**

**General**

- **Access List Name**: NSP-ACL-Google
- **Deny Counters**: 0

<table>
<thead>
<tr>
<th>Seq</th>
<th>Action</th>
<th>Source IP/Mask</th>
<th>Destination IP/Mask</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Dest Port</th>
<th>DSCP</th>
<th>Direction</th>
<th>Number of Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Permit</td>
<td>0.0.0.0</td>
<td>10.35.50.165</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/</td>
<td>255.255.255.255</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Permit</td>
<td>10.35.50.165</td>
<td>0.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Outbound</td>
<td>114</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/</td>
<td>255.255.255.255</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Deny</td>
<td>0.0.0.0</td>
<td>10.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/</td>
<td>255.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Deny</td>
<td>0.0.0.0</td>
<td>192.168.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/</td>
<td>255.255.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Deny</td>
<td>0.0.0.0</td>
<td>172.16.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/</td>
<td>255.240.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Deny</td>
<td>0.0.0.0</td>
<td>171.71.181.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Permit</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>3449</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3: Google Access ACL**

**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**

**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 1**  Click Policy → Conditions → Authentication → Compound Conditions
Step 2  Review a compound condition named “Wireless_MAB”

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

Figure 4 Wireless MAB

Step 3  Review a compound condition named “Wired_MAB”

“Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Ethernet”
Verify Default Network Access Result
This procedure describes the current protocol settings under “Default Network Access”.

**Step 1**  Click Policy → Policy Elements → Results
**Step 2**  Click Authentication → Allowed Protocols → Default Network Access
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 7 Default Network Access Policy

Figure 26.

Step 3 Review Authentication Policy Configuration, following screenshot is full policy view for reference, individual policies will be configured in subsequent steps.
Step 4 Authentication policy for MAB, please add conditions (Wired_MAB OR Wireless_MAB)

Step 5 Authentication policy for Dot1x, please add conditions (Wired_802.1X OR Wireless_802.1X)
Step 6 Default Authentication policy.

Figure 11 Default Authentication Policy

Configure an Authorization policy named “CWA”

Step 1 Click Policy → Policy Elements → Results.
Step 2 Choose Authorization → Authorization Profiles
Step 3 Click “ADD”
Step 4  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.
Step 5  Add an Authorization Profile named “CWA_GooglePlay”.

Android devices will use this profile to allow access to Google Play for downloading “Cisco Network Setup Assistant”.

![Authorization Profile](image)

Figure 31. CWA Authorization Profile for Android to Access Google

Review Policy conditions under Authorization Profiles

Step 1  Click Policy → Policy Elements → Results → Authorization → Authorization Profiles.
Step 2  Review Profile named “Blacklist_Access”
Figure 32. Blacklist Authorization Profile

Advanced Attribute Settings

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

Step 3  Create an Authorization Profile named “NSP.”
Note: Please also click **Step 4** Create an Authorization Profile named “NSP_Google”
Add the Authorization Policies

Step 1  Click Policy → Authorization
Step 2  Click “Insert New Rule Below”

Figure 12 Insert New Rules

Step 3  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
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.

STOP

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.

Figure 36. Authorization Policies
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.

Lab Testing:

<table>
<thead>
<tr>
<th>Android Option</th>
<th>Network Range to Open</th>
<th>TCP &amp; UDP Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Play option</td>
<td>74.125.00/16 173.194.0.0/16</td>
<td>TCP/UDP:5228 TCP/UDP:8889</td>
</tr>
<tr>
<td>Internet Option</td>
<td>74.125.00/16 173.194.0.0/16</td>
<td>UDP: 5228 TCP: All Ports</td>
</tr>
</tbody>
</table>
Appendix B: BYOD flows

This section covers BYOD flows for iOS and Android Devices.

Figure 37. BYOD flows for iOS and Android Devices
Figure 38. Android Use Cases
Appendix C: References

Cisco TrustSec System

http://www.cisco.com/go/trustsec

Device Configuration Guides:

Cisco Identity Services Engine User Guides:

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:

For Cisco Catalyst 3000 series switches:

For Cisco Catalyst 3000-X series switches:

For Cisco Catalyst 4500 series switches:

For Cisco Catalyst 6500 series switches:

For Cisco ASR 1000 series routers:

For Cisco Wireless LAN Controllers: