Using Certificates for Differentiate Access with Cisco Identity Services Engine

Secure Access How-To Guides Series

Author: Imran Bashir
Date: September 2013
Table of Contents

Overview .................................................. 3
  Digital Certificates ........................................... 3
  Certificate Provisioning ...................................... 3
  Scenario Overview .......................................... 5
    Architecture/ Diagram .................................... 6
    Components ................................................ 6

The Cisco Identity Services Engine Configuration ........................................... 8
  Identify Users for BYOD Flow ................................ 8
  Create a Certificate Authentication Profile ..................... 11
  Create an Identity Source Sequence .......................... 12
  Create a Client Provisioning Policy .......................... 14
  Prepare the WLC for BYOD Onboarding ....................... 19
  Configure an Authentication Policy ........................ 21
  Simple Certificate Enrollment Protocol (SCEP) Setup ........ 34

Appendix A: Configuring SCEP Server ........................................... 35
  Setup SCEP Server .......................................... 35
  Configuring SCEP Enrollment ................................ 36
  Assign the new Template for Issuance ....................... 45

Appendix B: Android and Play.Google.Com ........................................... 50
  Why Android is Different ................................. 50

Appendix C: BYOD flows ........................................... 51

Appendix D: References ........................................... 53
  Cisco TrustSec System: .................................... 53
  Device Configuration Guides: .................
Overview

This how-to guide addresses the use of certificates to identify corporate vs. non-corporate devices and how to apply different authorization policies based on this classification. This How-To Guide also covers how the system is setup for on-boarding which includes native supplicant provisioning, the type of certificates being pushed and what fields within the certificates can be used to write policy to differentiate access.

Digital Certificates

Although profiling can be used as a method of identifying and classifying endpoints, digital certificates may also be used to provide similar functionality. The use of Digital Certificates along with profiling can additively provide a more accurate mechanism for finger-printing endpoints.

Digital signatures, enabled by public key cryptography, provide a way 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.

In simple terms, a signature is formed when data is encrypted with a private key. The signature is attached to the data and sent to the receiver. The receiver applies the public key of the sender to the data. 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.

Certificate Provisioning

The Cisco Identity Services Engine supplicant provisioning supports the deployment of supplicant profiles. The provisioning of EAP-TLS profiles also includes the provisioning of digital certificates. In that case the Cisco Identity Services Engine Policy Services Node (PSN) acts as a Registration Authority for endpoints initiating SCEP requests.

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

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>
<tr>
<td>Windows</td>
<td>User Certificate</td>
<td>Can be viewed by launching the Certificate Snap-In for</td>
<td>WindowsXP – SP3</td>
</tr>
<tr>
<td>Device</td>
<td>Certificate Store</td>
<td>Certificate Info</td>
<td>Version</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td></td>
<td>Store</td>
<td>MMC.</td>
<td>Windows Vista – SP?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Windows7 – all versions</td>
</tr>
<tr>
<td>MacOS-X</td>
<td>Keychains</td>
<td>Can be viewed by launching application → Utilities → Keychain Access</td>
<td>MacOS-X 10.6 and 10.7</td>
</tr>
</tbody>
</table>

**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
The provisioned certificate will have the following attributes:

- **Common Name (CN) of the Subject:** User identity used for authentication
- **Subject Alternative Name:** MAC address(es) of the endpoint.

**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. **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 a certificate is automatically provisioned for that user & device and installed along with a supplicant profile that is pre-configured to use that certificate & connect the device to the corporate network. The Cisco ISE policy will also be configured to provide differentiated access to the user/device based on the certificate.

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

1. An employee connects to the corporate wireless SSID using their new iPad.
2. The iPad web browser will be redirected to a self-registration portal hosted on the Cisco ISE Policy Services Node (PSN).
3. The employee will enter their credentials into the web portal.
4. The employee's credentials are authenticated against the corporate Active Directory or other corporate Identity Store.
5. The PSN will send down an Apple Over-the-Air (OTA) provisioning profile that will generate the Certificate Signing Request (CSR).
6. The iPad sends the CSR to the Policy Services Node which, acting as a Registration Authority, will proxy the request to the Active Directory Certificate Authority (CA).
7. The Active Directory Certificate Authority will issue the certificate and send it back to the Cisco ISE Policy Services Node.
8. Using OTA, the Cisco ISE PSN sends a new profile to the iPad including the issued certificate 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 EAP-TLS for 802.1X authentication.
9. Now the iPad is configured to associate to the corporate wireless network using EAP-TLS for authentication (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), 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).
Architecture/ Diagram

![Architecture Diagram](image)

**Figure 1.** Architecture 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>Certificate Authority Server</td>
<td>Any per specification of Microsoft (Windows 2008 R2 Enterprise SP2)</td>
<td>SCEP, Certificate Authority Server</td>
<td>N/A</td>
</tr>
<tr>
<td>Wireless LAN Controller</td>
<td>5500-series</td>
<td>Profiling and Change of Authorization (CoA)</td>
<td>Unified Wireless</td>
</tr>
</tbody>
</table>
## SECURE ACCESS HOW-TO GUIDES

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware</th>
<th>Features Tested</th>
<th>Cisco IOS® Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>(WLC)</td>
<td>2500-series</td>
<td></td>
<td>7.2.???</td>
</tr>
<tr>
<td></td>
<td>WLSM-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple iOS and</td>
<td>Apple &amp; Google</td>
<td>N/A</td>
<td>Apple iOS 5.0</td>
</tr>
<tr>
<td>Google Android</td>
<td></td>
<td></td>
<td>Google Android 2.3</td>
</tr>
</tbody>
</table>

**Note:** Wireless was tested with Central Switching mode only.
The Cisco Identity Services Engine 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 EAP-TLS and an Auth policy to check for Certificates.

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.

Create an Identity Group.

Figure 2. Identity Groups Navigation
In this example we are naming our Identity Group: “Employee.”

Create a user in the Employee Group

Step 4  Navigate to Administration → Identity Management → Identities → Users.
Step 5  Click on ADD.
Figure 4. User Account
Create a Certificate Authentication Profile

Certificate authentication profiles (CAPs) are used in authentication policies for certificate-based authentications. The CAP defines certain attributes in the certificate to view & use as an additional identity source. For example, if the username is in the CN= field of the certificate, you will create a CAP that examines the CN= field. That data may then be used and checked against other identity sources, such as Active Directory. The certificate authentication profile allow you to specify the following items:

- The certificate field that should be used as the principal username
- Whether a binary comparison of the certificate should be performed

Note: The Certificate Authentication Profiles page lists the profiles that you have added.

Create a Certificate Authorization Profile

Step 1 Navigate to Administration → External Identity Sources → Certificate Authorization Profile.

Figure 5. Navigation

Step 2 Click ADD and Name the profile, in this case its named as “Cisco_CAP.”
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 the Certificate Authentication Profile created previously in the section named “Cisco_CAP”.

Step 5 Select your Active Directory Server (AD1), Internal Endpoints and Internal Users in the Authentication Search List.
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’s 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 Native Supplicant Profile

Step 1  Go to Policy → Policy Elements → Results.
SECURE ACCESS HOW-TO GUIDES

Step 2  Click on Client Provisioning → Resources.
Step 3  Click ADD..

![Client Provisioning Resources Navigation](image)

Figure 9. Client Provisioning Resources Navigation

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 “**TLS**” since it’s using certificates.
Step 5  Select Key Size. **1024**.
Download supplicant wizards for Windows and MAC OSx

Step 6  Go to Policy → Policy Elements → Results → Client Provisioning → Resources
Step 7  On the right hand side, Click on ADD
Step 8  Choose “Agent resources from Cisco site”

In this example we have selected WinSPWizard 1.0.0.15 and MacOsXSPWizard 1.0.0.999
Step 9  Select the latest supplicant wizards.
Create a Client Provisioning Policy for Apple iOS

Step 10  Go to Policy → Client Provisioning
Step 11  On the right hand, Click on Actions → Insert new Policy above
Step 12
Step 13

Step 14  Create an Apple iOS CPP policy.

Step 15  Create an Android CPP policy.

Step 16  (Optional): Create a MAC OSx CPP policy.

Step 17  (Optional): Create a Windows CPP policy.
Note: Please note that 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.

Prepare the WLC for BYOD Onboarding

Configure an Access Control List for Wireless LAN Controller

In this procedure, we will create multiple ACLs in the Wireless LAN Controller, which would be used later in the policy to redirect clients selected for BYOD supplicant and certificate provisioning.

The Cisco Identity Services Engine IP address = 10.35.50.165
Internal Corporate Networks = 192.168.0.0, 172.16.0.0 (to redirect)

Step 18 Create an ACL named “NSP-ACL” similar to the one depicted below.

![Figure 9 ACL for re-directing client to BYOD Flow](image)

<table>
<thead>
<tr>
<th>Seq</th>
<th>Action</th>
<th>Source IP/Host</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>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</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>10.35.50.165</td>
<td></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>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>Permit</td>
<td>0.0.0.0</td>
<td>UDP</td>
<td>Any</td>
<td>DHCP Server</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Deny</td>
<td>192.168.0.0</td>
<td></td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Deny</td>
<td>172.16.0.0</td>
<td></td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Deny</td>
<td>10.0.0.0</td>
<td></td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Permit</td>
<td>0.0.0.0</td>
<td></td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
</tbody>
</table>

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)

**Step 19** Create an ACL named “BLACKLIST-ACL” in the Wireless LAN Controller, which would be used in the policy later to restrict access to blacklisted devices.

![Figure 10 Blacklist ACL](image)

**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 20** Create an ACL named “NSP-ACL-Google” in the Wireless LAN Controller, which would be used in the policy later for provisioning Android devices.
Access Control Lists > Edit

**General**

<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 / 0.0.0.0</td>
<td>10.35.50.165 / 255.255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>110</td>
</tr>
<tr>
<td>2</td>
<td>Permit</td>
<td>10.35.50.165 / 255.255.255.255</td>
<td>0.0.0.0 / 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>3</td>
<td>Deny</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>10.0.0.0 / 255.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Deny</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>192.168.0.0 / 255.255.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Deny</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>172.16.0.0 / 255.240.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Deny</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>171.171.181.0 / 255.255.255.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Inbound</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Permit</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>0.0.0.0 / 0.0.0.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>3449</td>
</tr>
</tbody>
</table>

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:** 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”

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.
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.
Configure an Authorization policy named “CWA”

Step 1  Click Policy → Policy Elements → Results.
Step 2  Choose Authorization → Authorization Profiles
Step 3  Click “ADD.”

![Figure 19. Authorization Profiles Navigation](image)

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 authentications 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 use this profile. This profile allows access to Google Play for downloading “Cisco Network Setup Assistant”.

Figure 20. CWA Authorization Profile
Review Policy conditions under Authorization Profiles

Step 1   Click Policy → Policy Elements → Results → Authorization → Authorization Profiles.
Step 2   Review Profile named “Blacklist_Access.”
Advanced Attribute Settings

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

**Step 1**  Create an Authorization Profile named “NSP.”
**Figure 23.** Native Supplicant Provisioning Authorization Profile

**Step 2**  
Click Airespace ACL Name.

**Step 3**  
Create an Authorization Profile named “NSP_Google.”
Step 4  Note: Please also click Airespace ACL Name.

Add the Authorization Policies
Step 1  Click Policy → Authorization.
Step 2  Click “Insert New Rule Below”
**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 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.


---

**Figure 26. Authorization Policy**
Simple Certificate Enrollment Protocol (SCEP) Setup

In this procedure we will configure SCEP profile that is used for certificate provisioning on the clients. The process of enrollment requires a certificate authority (CA) to issue the certificates using the Simple Certificate Enrollment Protocol (SCEP). ISE acts as a Registration Authority (RA) and communicates with the CA to provision certificates on the clients.

Add a SCEP CA Profile

**Step 1**  
Click Administration ➔ Certificates ➔ SCEP CA Profiles.

**Step 2**  
Click Add.

**Step 3**  
Add SCEP CA profile/.

CA Server IP = 172.21.77.24.

**Figure 27.** Navigation to SCEP CA Profiles

**Figure 28.** SCEP CA Profile

You are done!
Appendix A: Configuring SCEP Server

This section walks through step-by-step process for configuring Microsoft 2008 R2 Enterprise SP2 as a SCEP server, the following tasks are required for SCEP setup.

Setup SCEP Server

**Microsoft 2008 R2 Enterprise SP2 setup for SCEP Server.**

**Step 1**  Install Windows Server 2008 R2 Enterprise server.
**Step 2**  After the installation completes, run Microsoft updates to get all the necessary updates.
**Step 3**  Activate windows license.
**Step 4**  Run dpromo in command prompt window. This will install Active Directory Domain Services to the server.
**Step 5**  Go through the installation of the Active Directory Domain Services.
   a. Select ‘advanced’ mode checkbox.
   b. Create a new domain in a forest
   c. Insert name for the forest root domain.
   d. Install DNS server
   e. Wait for Active Domain Services to complete installing.
   f. Server will reboot.
**Step 6**  Add Administrator or SCEP_User to IIS_IUSRS group

Install a Role: Active Directory Certificate Services

**Step 1**  AD CS: Click Next
   a. Role Services:
      i. Certification Authority.
      ii. Certification Authority Web Enrollment.
   b. Setup Type: Select “Enterprise.”
   c. CA Type: Root CA.
   d. Private Key: Create a new private key.
      i. Cryptography: Default value, but select SHA256 for the hash algorithm
      ii. CA Name: leave it as default.
      iii. Validity Period: leave it as default.
   e. Certificate Database: leave it as default.

**Step 2**  Web Server (IIS): Click Next.
   a. Role Services: leave it as default, click Next.

**Step 3**  Confirmation: Click Install.

Add Role Services

**Step 1**  From Server Manager → Roles → Active Directory Certificate Services:
**Step 2**  Select “Network Device Enrollment Service.”
**Step 3**  Select “Certificate Enrollment Web Service.”
User Account
Specify user account (Select User). This may be the administrator account or a SCEP service account (the one added to IIS_USERS group)

Step 4 RA Information – leave it as default.
Step 5 Cryptography – leave as default.
Step 6 CA for CES – leave as default.
Step 7 Authentication Type – leave as default.
Step 8 Service Account – leave as default and choose the administrator account.
Step 9 Server Authentication Certificate.
Step 10 Choose an existing certificate for SSL encryption – select the certificate with ‘Client Authentication’ as Intended Purpose.
Step 11 Web Server (IIS) – Click Next.
Step 12 Role Servers – leave as default.
Step 13 Confirmation: Click Install.

Modify the Registry
Step 1 Type regedit from the ‘Start’ menu.
Step 2 In the registry editor, go to: HKEY_LOCAL_MACHINE → Software → Microsoft → Cryptography → MSCEP .
Step 3 Click the key labeled: Enforce Password.
Step 4 Modify EnforcePassword from value 1 to 0.
Step 5 Restart the server.

Configuring SCEP Enrollment.

Create a SCEP Service Account
Once CA server and services are installed, configure the server to do SCEP enrollment.

Step 1 Create a new account.
Create and save an MMC for working with Certificates

Step 1  Start → Run → mmc.
Step 2  Add Snap-in for Certificate Templates, Certificates (Local Computer), Certification Authority (Local) and Enterprise PKI.
Step 3  When done click ‘Ok’. (Snapshot shown below).

Step 4  Save the mmc console. So it can be accessed easily at a later time.

Create a New Certificate Template

Step 1  Select Certificate Templates and duplicate ‘User’ template.
Step 2  Select “Windows Server 2008 Enterprise” (in this document example, could also use Windows Server 2003 Enterprise).

Step 3  Click OK.

Step 4  Give it a template name (in this example its called “byod”).

General Tab

Step 1  Publish the cert in Active Directory, which will sync it to all Domain Controllers.
Request Handling Tab
This tab states that certificate will be used for signing & encrypting.

**Step 1** Please **uncheck** “allow private key to be exported” to mark it as “non-exportable” if required.
**Step 2** Certificates will be requested through the BYOD provisioning flow that would be automated processes therefore please ensure “enroll subject without requiring any user input”.

![Image of Request Handling Tab](image-url)
Subject Name Tab

Step 1 Select “Supply in Request”.

This is necessary since the certificate is not being created by an Active Directory member, but through SCEP instead.
Cryptography Tab

Step 1  Select “Requests can use any provider available on the subject’s computer.”
Extensions Tab

Step 1  Applications Policies:

If the descriptions of the Application Policies do not show what is in the snapshot, you can click “Edit” and “Add” the Application Policies.
Step 2  Basic Constraints.

This sets the certificate to belong to an endpoint, and not a subsequent signer.
Step 3  Issuance Policies.

Issuance Policies must be configured, to allow the CA to actually issue the certificate. Please select “All issuance policies”
Security Tab

In this section we will add the “Service Account User” to have Full Control the Certificate Template. The account was created in previous step that the SCEP service is running-as.

**Step 1**  
Click Add.

**Step 2**  
SCEP_USER.

![Security Tab](image)

Assign the new Template for Issuance

At this point we have completed the duplicate template process, next we have to choose it as one to be issued.

**Assign the new Template for Issuance**

**Step 1**  
Server Manager → Roles → AD Certificate Authority → <your CA--> → Certificate Templates.

**Step 2**  
Right-Click.

**Step 3**  
New → Certificate Template to Issue.

**Step 4**  
Choose your new Certificate Template.
Step 5  Choose the template you created from previous steps.

You should be able to see template shown on the right hand side pane after this step is completed.

Modify the Default Certificate

The default Certificate Template for SCEP to issue, is an IPSEC template. This must be changed to use the new User-Template:

Step 1  Run Regedit.
Step 2  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP.
Step 3  Modify the EncryptionTemplate, GeneralPurposeTemplate, and SignatureTemplate to the name of the template you created above. Make sure the name is spelt the same way you have created.
Set the EnforcePassword to zero and disable the “UseSinglePassword” setting:

Step 1 Run Regedit.
Step 2 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword`.
Step 3 Change the value to 0 UseSinglePassword is set to zero ‘0’.
Step 4 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword`.
Step 5 Change the value to 0 EnforcePassword is set to zero ‘0’.
UseSinglePassword:
Step 6  Save the mmc console that you created from above if you have not done so yet.
Step 7  Restart the entire server.

You are done!
Appendix B: 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 to 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:

Table 3. Android and Play.Google.Com

<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</td>
<td>TCP/UDP:5228</td>
</tr>
<tr>
<td></td>
<td>173.194.0.0/16</td>
<td>TCP/UDP:8889</td>
</tr>
<tr>
<td>Internet Option</td>
<td>74.125.00/16</td>
<td>UDP: 5228</td>
</tr>
<tr>
<td></td>
<td>173.194.0.0/16</td>
<td>TCP: All Ports</td>
</tr>
</tbody>
</table>
Appendix C: BYOD flows

This section shows BYOD flows for iOS and Android Devices.
**NSP (Android use-case)**

- **Employee**
  - SSID = BYOD-Open / CWA
  - User opens browser
  - Redirect to ISE for CWA
  - CWA login
  - Redirect to ISE for CWA
  - CWA login success / Redirect to NSP Portal
  - User click Register
  - CoA to WLC
  - Access Request
  - Posture-Required state
  - Download SPW: NSP Redirect / Redirect ACL = ALLOW GOOGLE
  - User installs application and launches
  - App sends request to http://ASE/auth/discovery
  - ISE sends Device BYOD Profile to Android Device
  - CMR sent to ISE
  - ISE sends User Certificate to Android Device
  - SSID = CTS-CORP / EAP-TLS
  - Connect using EAP-TLS
  - GUI state

**Device Registration**

- Sample WLC ACL: NSP=ACL-NSP
  - Permit UDP anytime any any <device_Internal_DNS> any any
  - Permit TCP any Host 14.128.0.0 255.255.0.0 any any
  - Permit TCP any Host 19.16.0.0 255.255.0.0 any any

**Device Provisioning**

- User Cert issued
  - CN = Employee
Appendix D: 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: