TrustSec How-To Guide:
Using Certificates for Differentiate Access

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Introduction

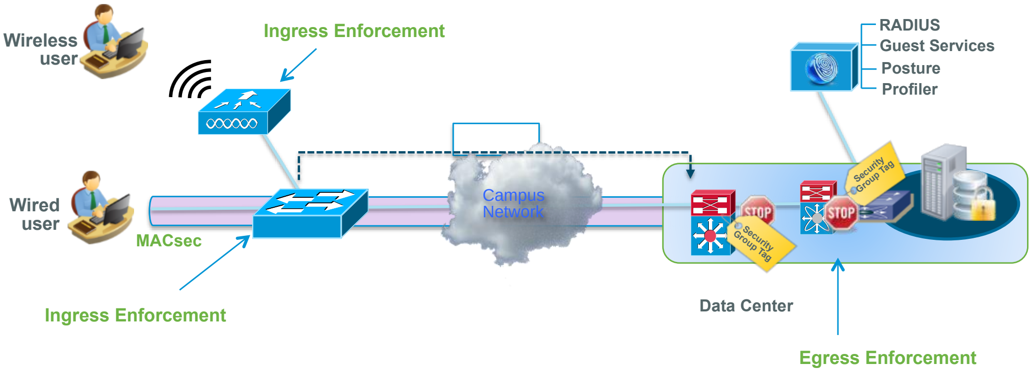
What Is the Cisco TrustSec System?

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

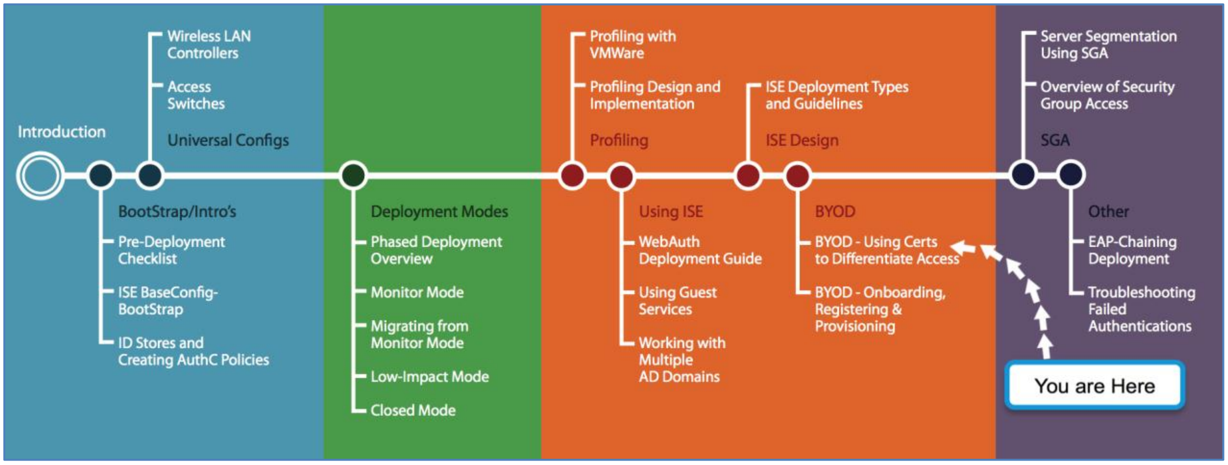


About the TrustSec How-To Guides

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 is 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


Introduction
Wireless LAN Controllers
Access Switches
Universal Configs
BootStrap/Intro's
Pre-Deployment Checklist
ISE BaseConfig-BootStrap
ID Stores and Creating AuthC Policies
Deployment Modes
Phased Deployment Overview
Monitor Mode
Migrating from Monitor Mode
Low-Impact Mode
Closed Mode
Profiling with VMWare
Profiling Design and Implementation
Profiling
ISE Deployment Types and Guidelines
ISE Design
Using ISE
WebAuth Deployment Guide
Using Guest Services
Working with Multiple AD Domains
BYOD
BYOD - Using Certs to Differentiate Access
BYOD - Onboarding, Registering & Provisioning
Server Segmentation Using SGA
Overview of Security Group Access
SGA
Other
EAP-Chaining Deployment
Troubleshooting Failed Authentications
You are Here

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

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

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

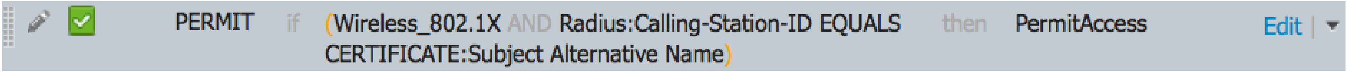
Note: MACOS-X 10.8 has the following Caveats

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

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.
```



✓ PERMIT if (Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name) then PermitAccess

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).

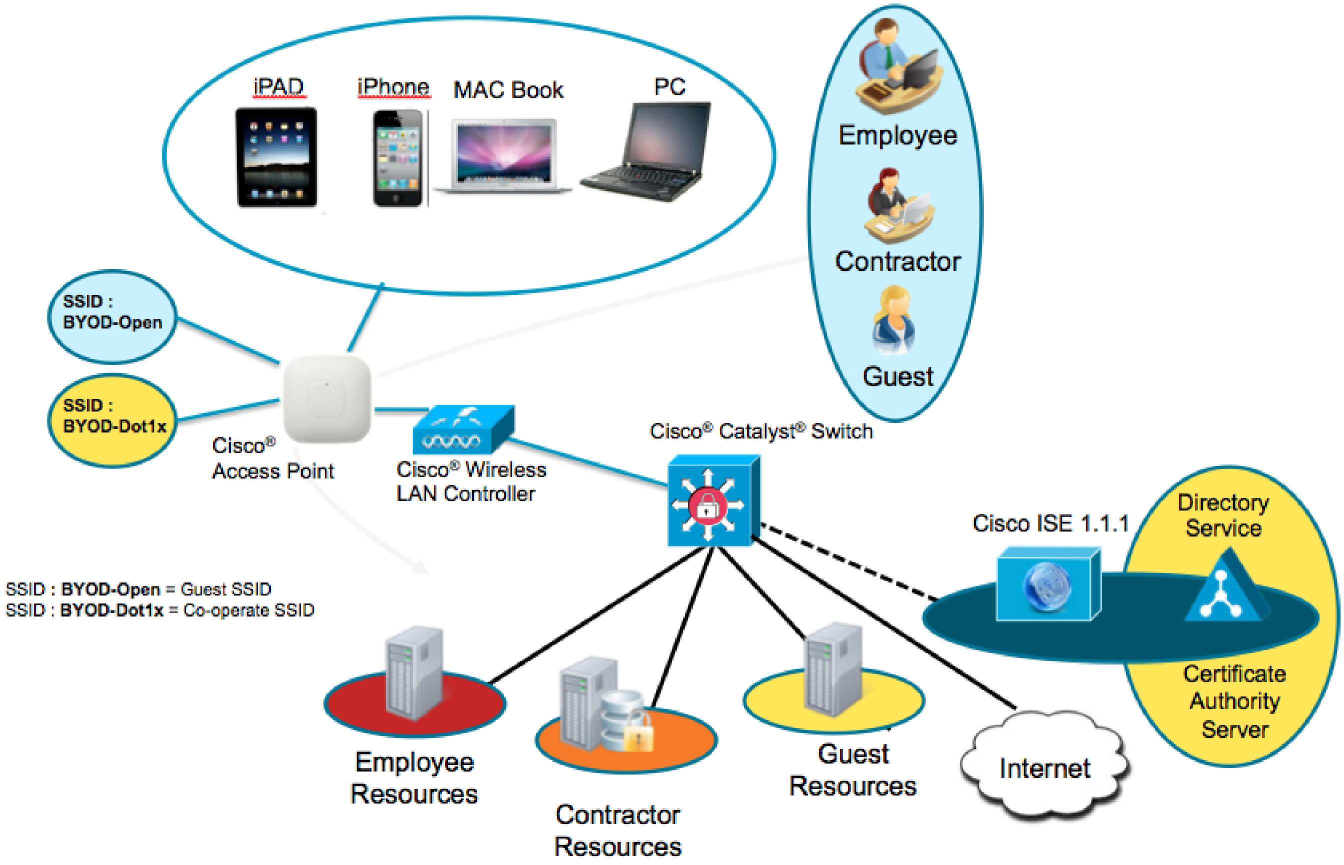
7. The Active Directory Certificate Authority will issue the certificate and send it back to the Cisco ISE Policy Services Node.

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

Figure 3 Architecture 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
Certificate Authority Server	Any per specification of Microsoft (Windows 2008 R2 Enterprise SP2)	SCEP, Certificate Authority Server	N/A
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.

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.

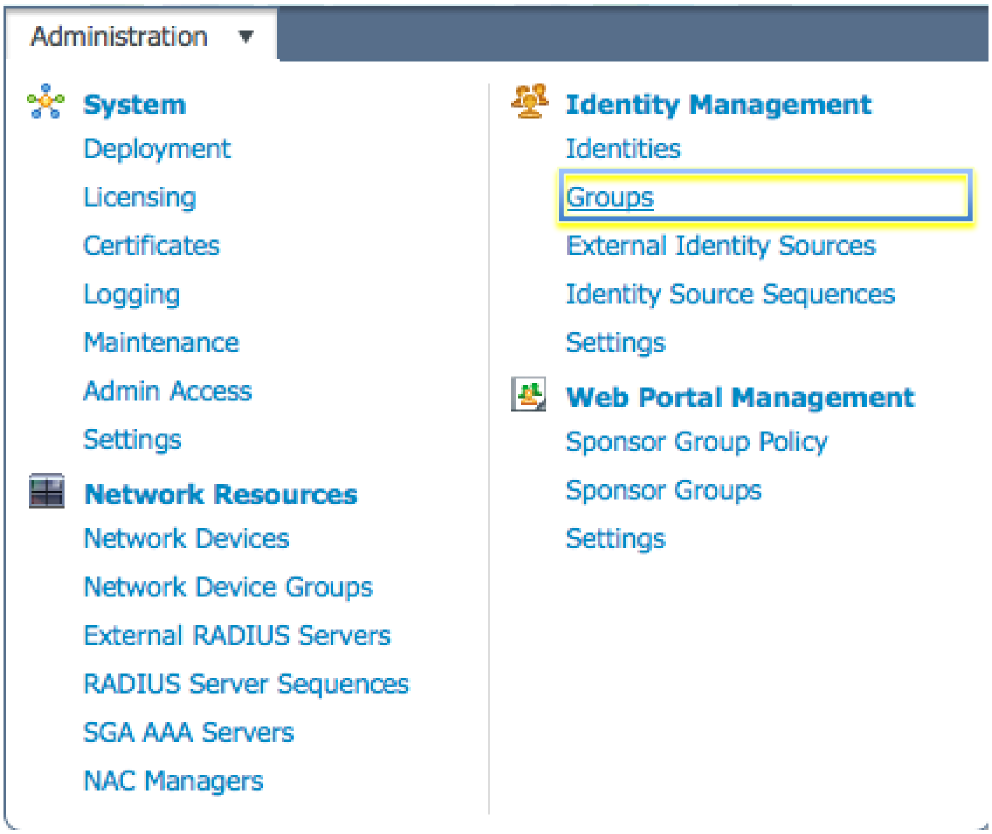
User Groups are a collection of individual users or endpoints that share a common set of privileges that allow them to access a specific set of Cisco ISE services and functionality. For example, if you belong to the Change User Password admin group, you can change administrative passwords for other users.

Procedure 1 Configure a user group

Step 1 Navigate to Administration → Identity Management → Groups

Step 2 Click on ADD.

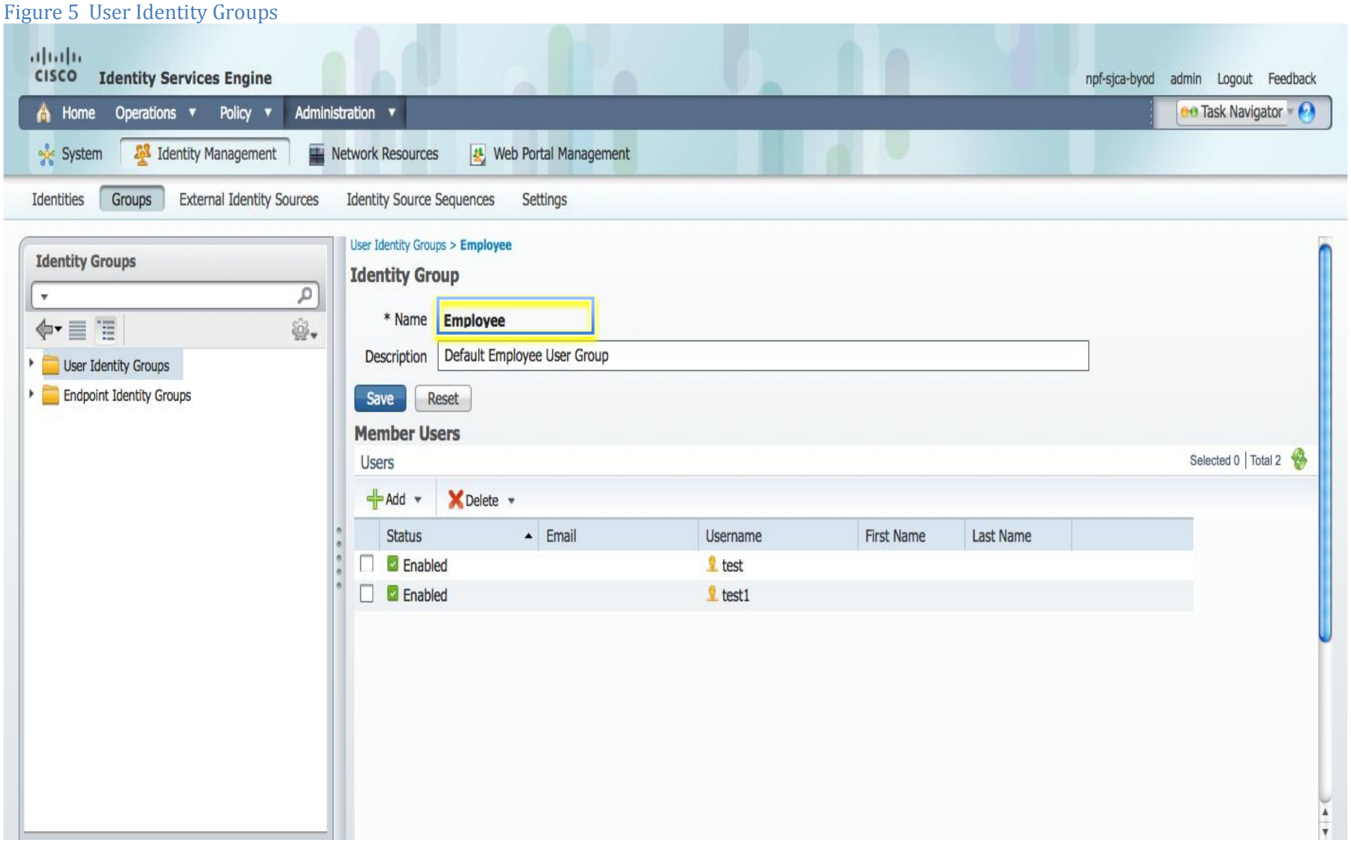
Figure 4 Identity Groups Navigation



Step 3 Create an Identity Group.

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

Figure 5 User Identity Groups



Identity Group

* Name: Employee

Description: Default Employee User Group

Member Users

Users

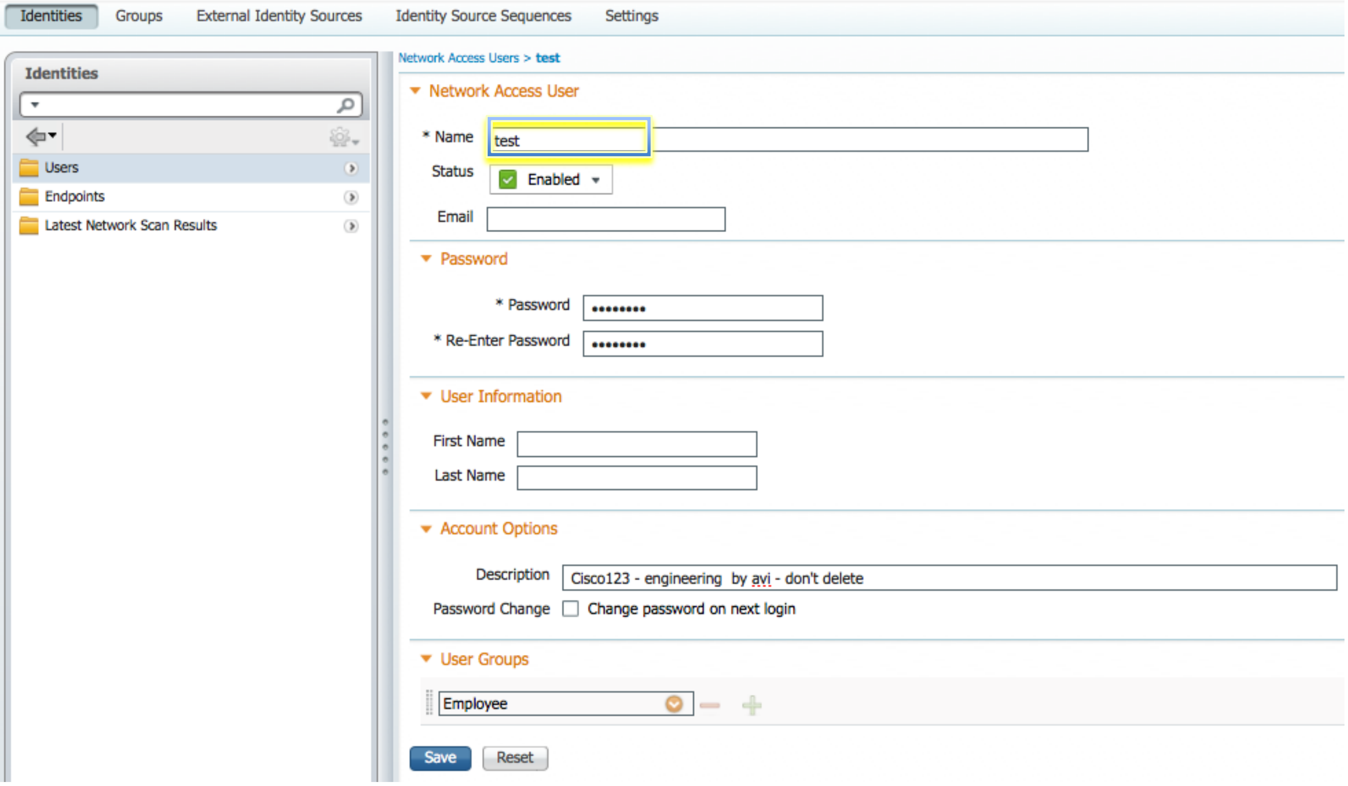
	Status	Email	Username	First Name	Last Name
□	Enabled		test		
□	Enabled		test1		

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



Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identities
Users
Endpoints
Latest Network Scan Results
Network Access Users > test

Network Access User

* Name: test

Status: ☑ Enabled

Email:

Password

* Password: ••••••••

* Re-Enter Password: ••••••••

User Information

First Name:

Last Name:

Account Options

Description: Cisco123 - engineering by avi - don't delete

Password Change: □ Change password on next login

User Groups

Employee

Create a Certificate Authentication Profile.

Certificate authentication profiles (CAP)s 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:

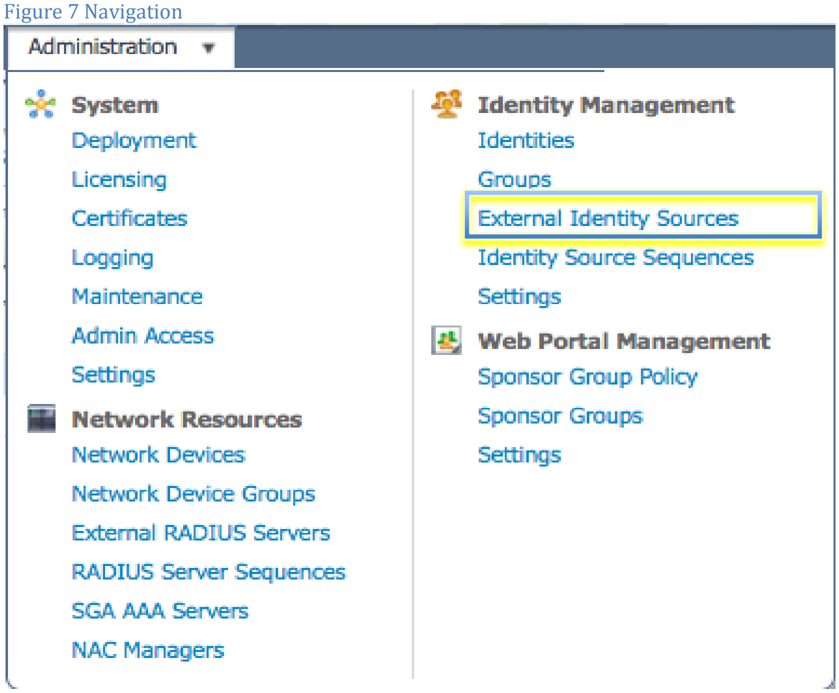
```
    The certificate field that should be used as the principal username
    Whether a binary comparison of the certificate should be performed
```

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

Procedure 1 Create a Certificate Authorization Profile

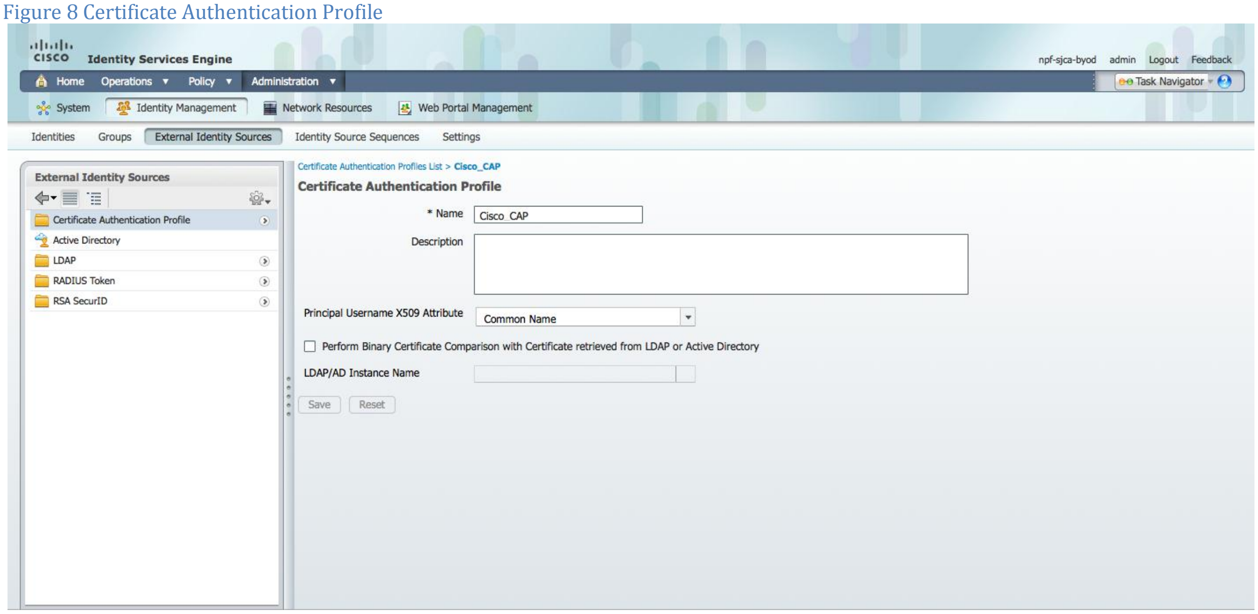
Step 1 Navigate to Administration → External Identity Sources → Certificate Authorization Profile

Figure 7 Navigation



Step 2 Click ADD and Name the profile, in this case its named as **"Cisco_CAP"**

Figure 8 Certificate Authentication Profile


cisco Identity Services Engine
npf-sjca-byod admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Web Portal Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Certificate Authentication Profiles List > Cisco_CAP
Save
Reset

Certificate Authentication Profile

* Name: Cisco_CAP

Description:

Principal Username X509 Attribute: Common Name

□ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name:

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.

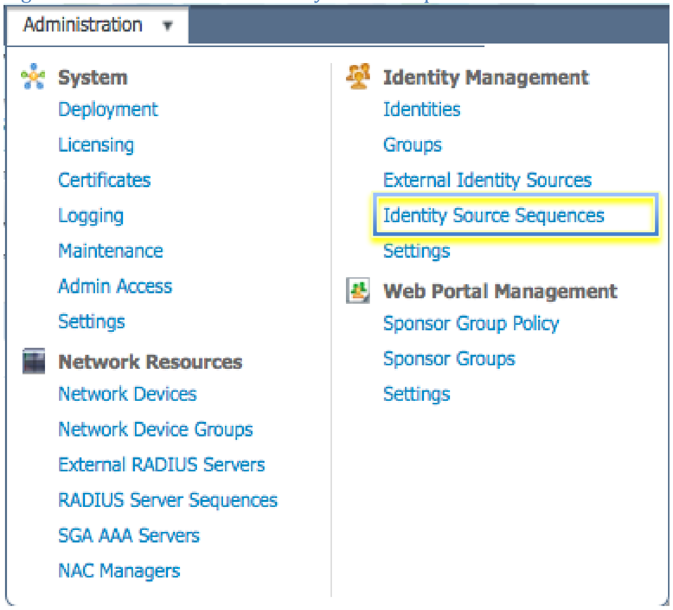
If your organization stores credentials in more than one of these identity stores, you can define an identity source sequence, which states the order in which you want the Cisco ISE to look for user information in these databases. Once a match is found, the Cisco ISE does not look any further, but evaluates 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 9 Administration → Identity Source Sequences



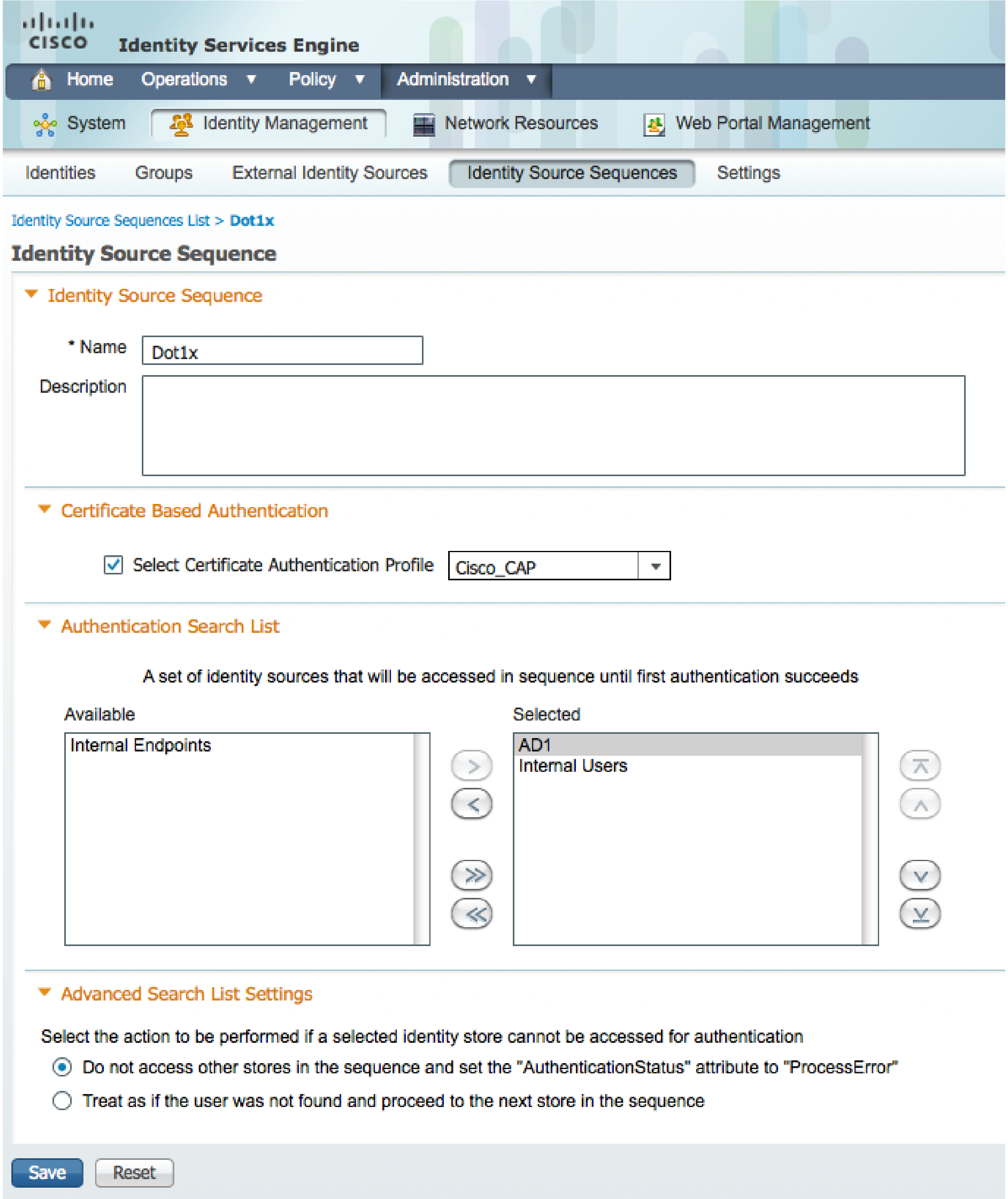
Step 3 Name the sequence

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**.

Figure 10 Identity Source Sequence



Identity Source Sequence

Identity Source Sequence

* Name: Dot1x

Description:

Certificate Based Authentication

☑ Select Certificate Authentication Profile: Cisco_CAP

Authentication Search List

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

Available: Internal Endpoints

Selected: 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

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.

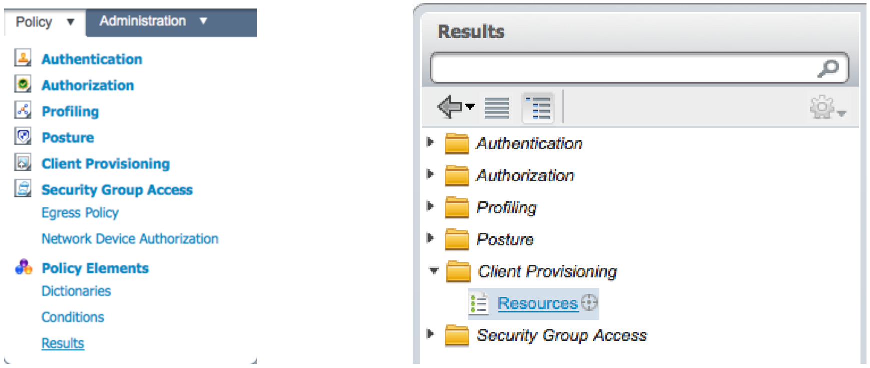
Procedure 1 Create a Native Supplicant Profile

Step 1 Go to **Policy → Policy Elements → Results**.

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

Step 3 Click **ADD**

Figure 9: Client Provisioning Resources Navigation



Procedure 2 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.

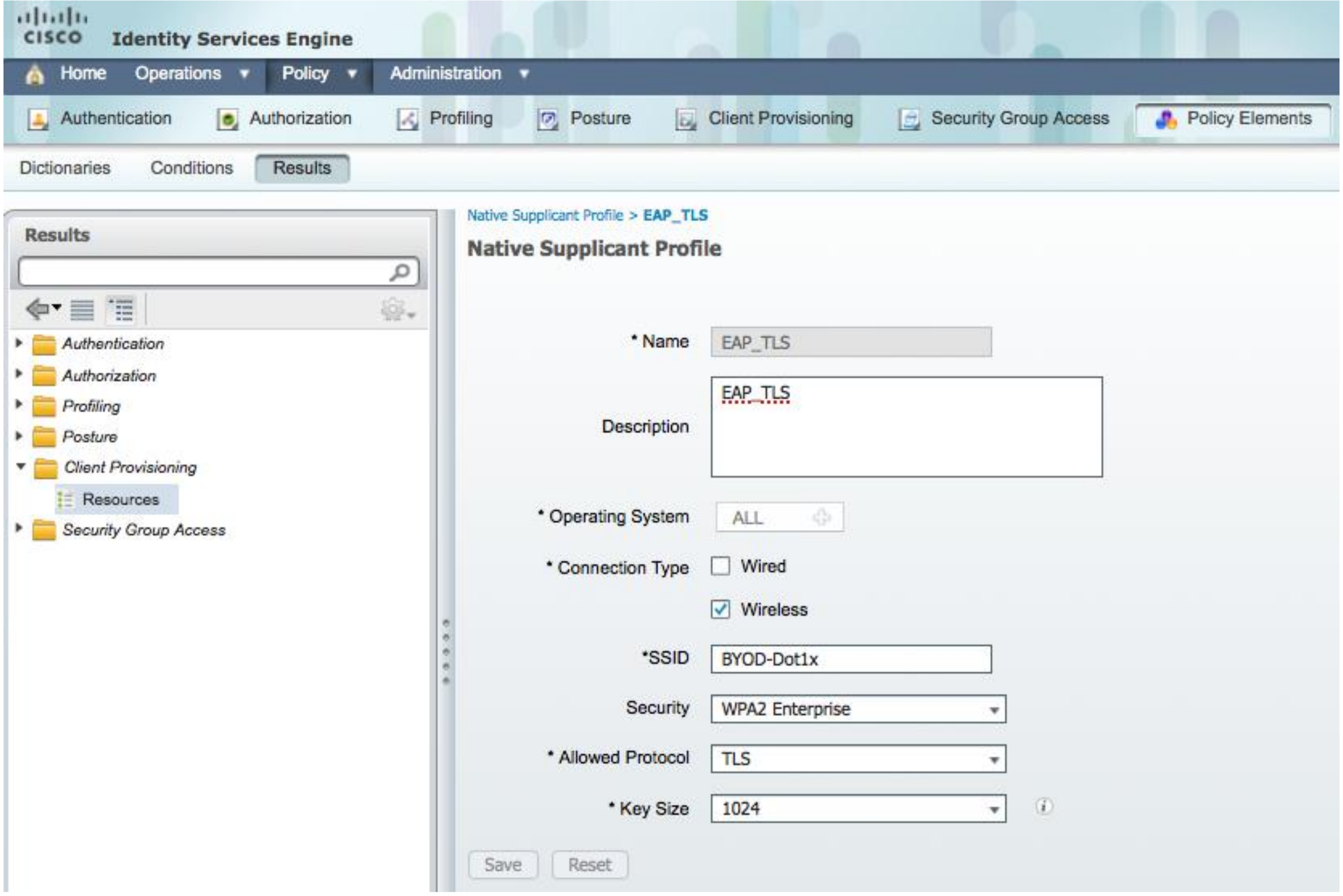
Step 2 Select Connection Type, **Wired** and/or **Wireless**.

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**.

Figure 11 Native Supplicant Profile



Native Supplicant Profile

* Name	EAP_TLS
Description	EAP_TLS
* Operating System	ALL
* Connection Type	□ Wired ☑ Wireless
*SSID	BYOD-Dot1x
Security	WPA2 Enterprise
* Allowed Protocol	TLS
* Key Size	1024

Procedure 3 Download supplicant wizards for Windows and MAC OSx

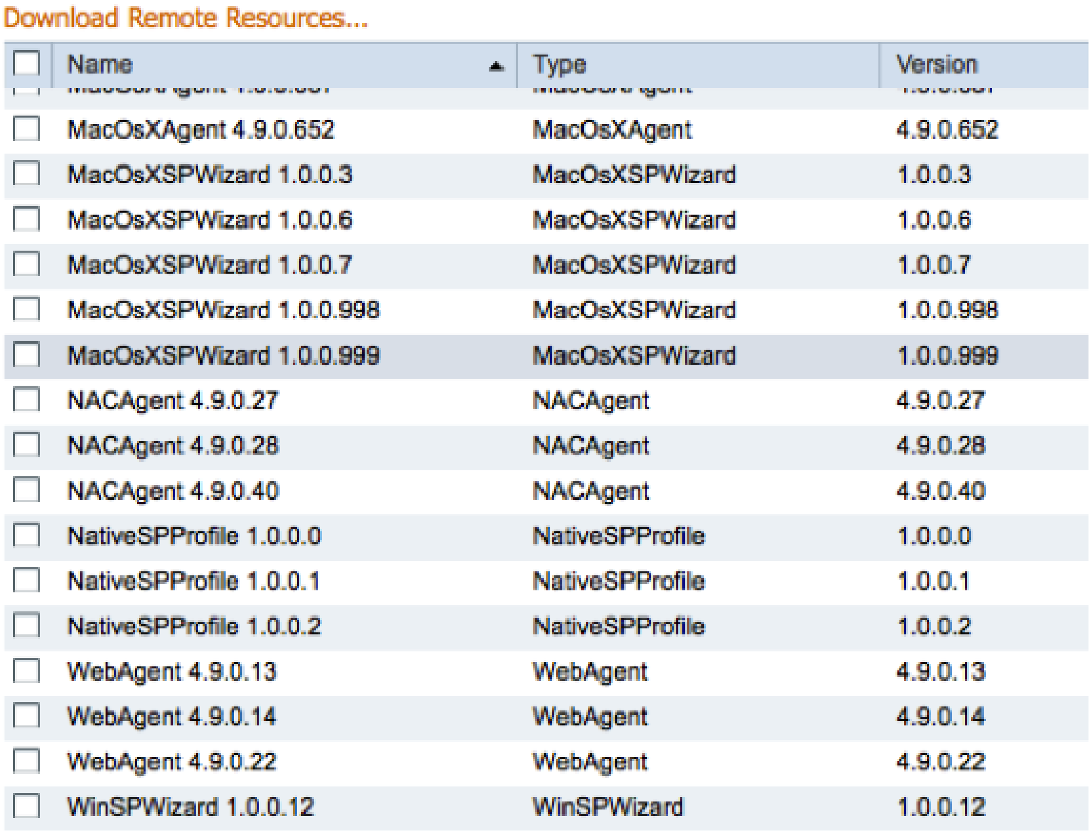
Step 1 Go to Policy → Policy Elements → Results → Client Provisioning → Resources

Step 2 On the right hand side, Click on ADD

Step 3 Choose "Agent resources from Cisco site"

In this example we have selected WinSPWizard 1.0.0.15 and MacOsXSPWizard 1.0.0.999

Figure 12 Native Supplicant Wizards A

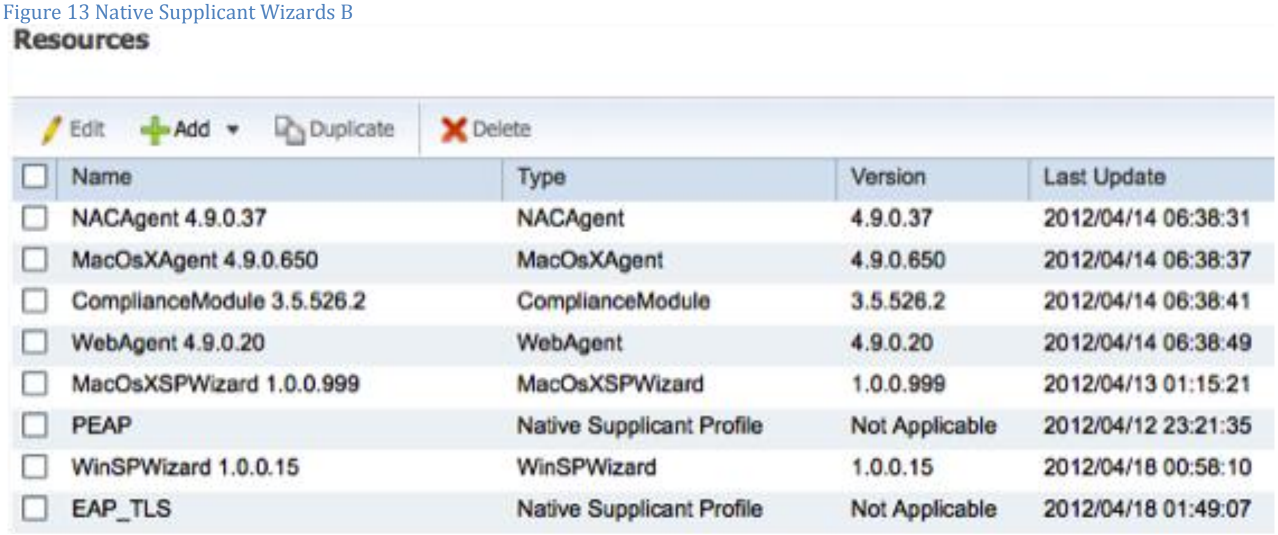


Download Remote Resources...

□	Name	Type	Version
□	MacOsXAgent 4.9.0.652	MacOsXAgent	4.9.0.652
□	MacOsXSPWizard 1.0.0.3	MacOsXSPWizard	1.0.0.3
□	MacOsXSPWizard 1.0.0.6	MacOsXSPWizard	1.0.0.6
□	MacOsXSPWizard 1.0.0.7	MacOsXSPWizard	1.0.0.7
□	MacOsXSPWizard 1.0.0.998	MacOsXSPWizard	1.0.0.998
□	MacOsXSPWizard 1.0.0.999	MacOsXSPWizard	1.0.0.999
□	NACAgent 4.9.0.27	NACAgent	4.9.0.27
□	NACAgent 4.9.0.28	NACAgent	4.9.0.28
□	NACAgent 4.9.0.40	NACAgent	4.9.0.40
□	NativeSPProfile 1.0.0.0	NativeSPProfile	1.0.0.0
□	NativeSPProfile 1.0.0.1	NativeSPProfile	1.0.0.1
□	NativeSPProfile 1.0.0.2	NativeSPProfile	1.0.0.2
□	WebAgent 4.9.0.13	WebAgent	4.9.0.13
□	WebAgent 4.9.0.14	WebAgent	4.9.0.14
□	WebAgent 4.9.0.22	WebAgent	4.9.0.22
□	WinSPWizard 1.0.0.12	WinSPWizard	1.0.0.12

Step 4 Select the latest supplicant wizards.

Figure 13 Native Supplicant Wizards B



Resources

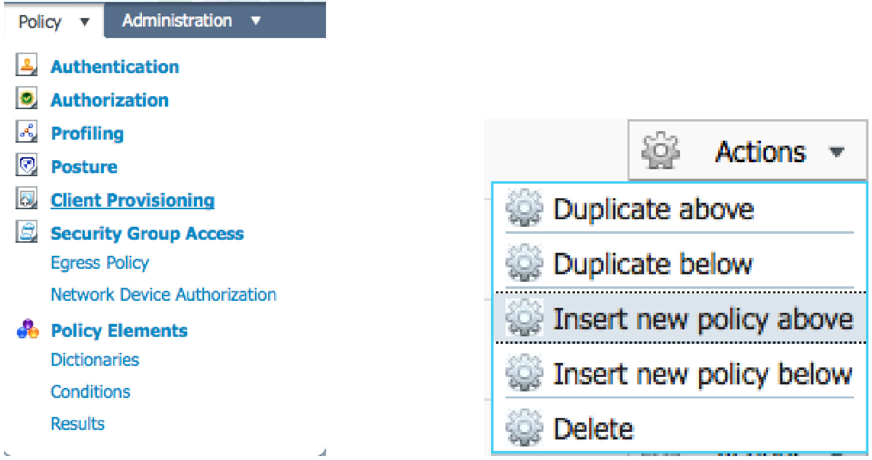
□	Name	Type	Version	Last Update
□	NACAgent 4.9.0.37	NACAgent	4.9.0.37	2012/04/14 06:38:31
□	MacOsXAgent 4.9.0.650	MacOsXAgent	4.9.0.650	2012/04/14 06:38:37
□	ComplianceModule 3.5.526.2	ComplianceModule	3.5.526.2	2012/04/14 06:38:41
□	WebAgent 4.9.0.20	WebAgent	4.9.0.20	2012/04/14 06:38:49
□	MacOsXSPWizard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

Procedure 4 Create a Client Provisioning Policy for Apple iOS

Step 1 Go to Policy → Client Provisioning

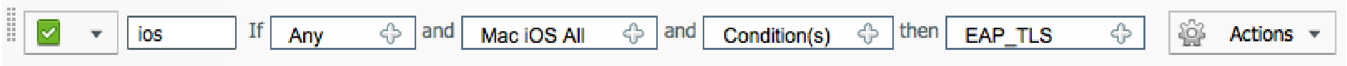
Step 2 On the right hand, Click on Actions → Insert new Policy above

Figure 14 Client Provisioning Policy



Step 3 Create an Apple iOS CPP policy.

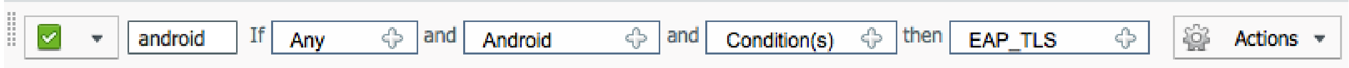
Figure 15 Apple iOS Client Provisioning Policy



ios If Any and Mac iOS All and Condition(s) then EAP_TLS

Step 4 Create an Android CPP policy.

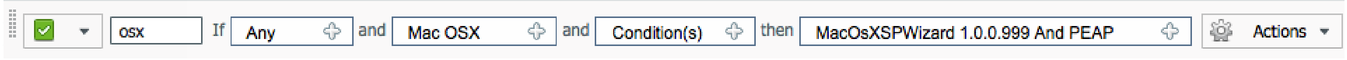
Figure 16 Android Provisioning Policy



android If Any and Android and Condition(s) then EAP_TLS

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

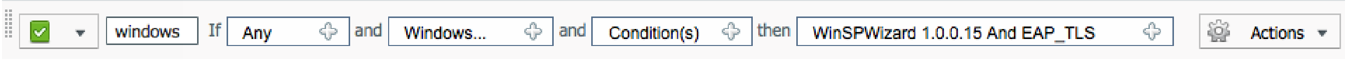
Figure 17 MacOS-X Provisioning Policy



osx If Any and Mac OSX and Condition(s) then MacOsXSPWizard 1.0.0.999 And PEAP

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

Figure 18 Windows Client Provisioning Policy



windows If Any and Windows... and Condition(s) then WinSPWizard 1.0.0.15 And EAP_TLS

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

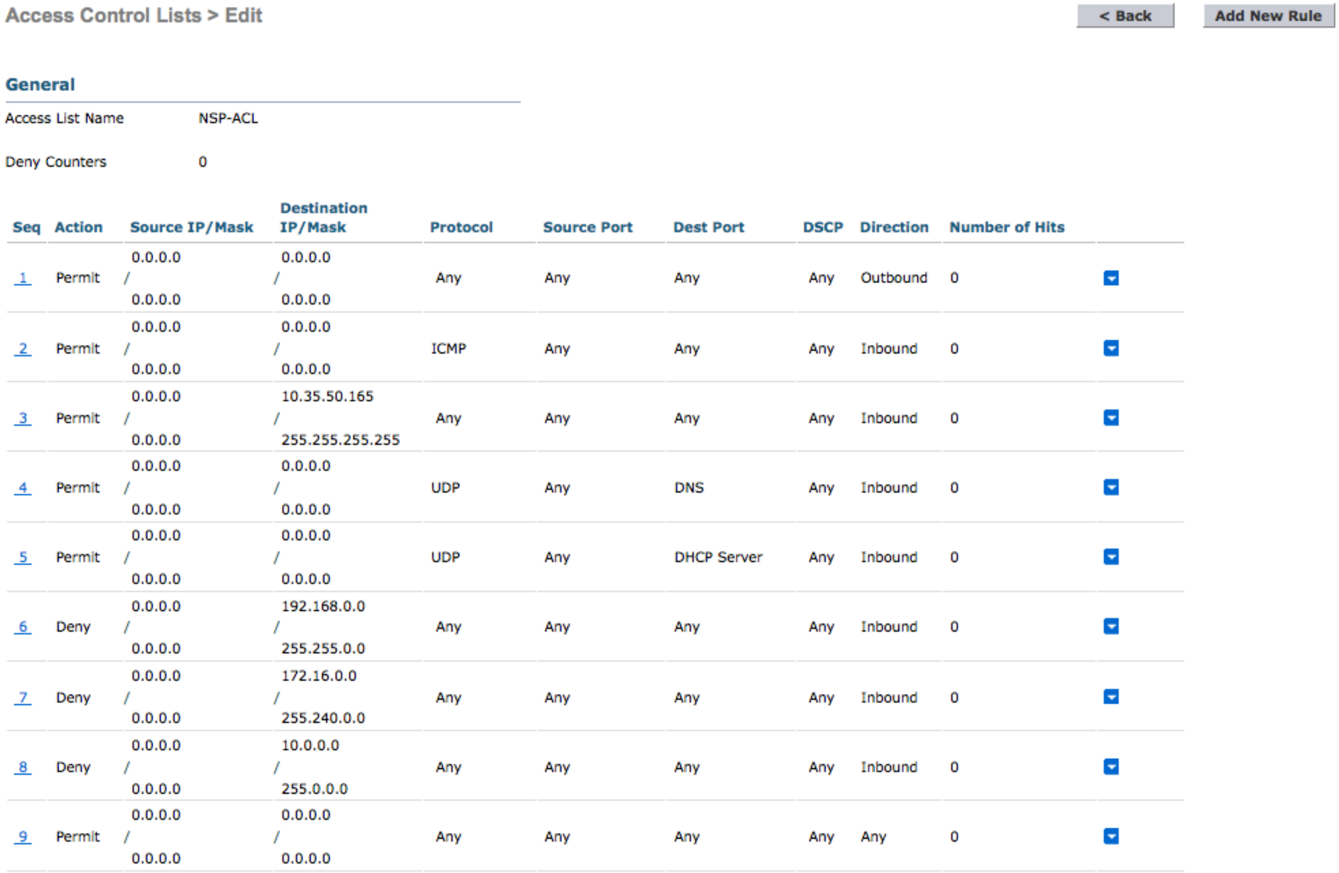
Procedure 1 Configure an Access Control List for Wireless LAN Controller

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 1 Create an ACL named “**NSP-ACL**” similar to the one depicted below.

Figure 19 ACL for re-directing client to BYOD Flow



Access Control Lists > Edit

General

Access List Name NSP-ACL

Deny Counters 0

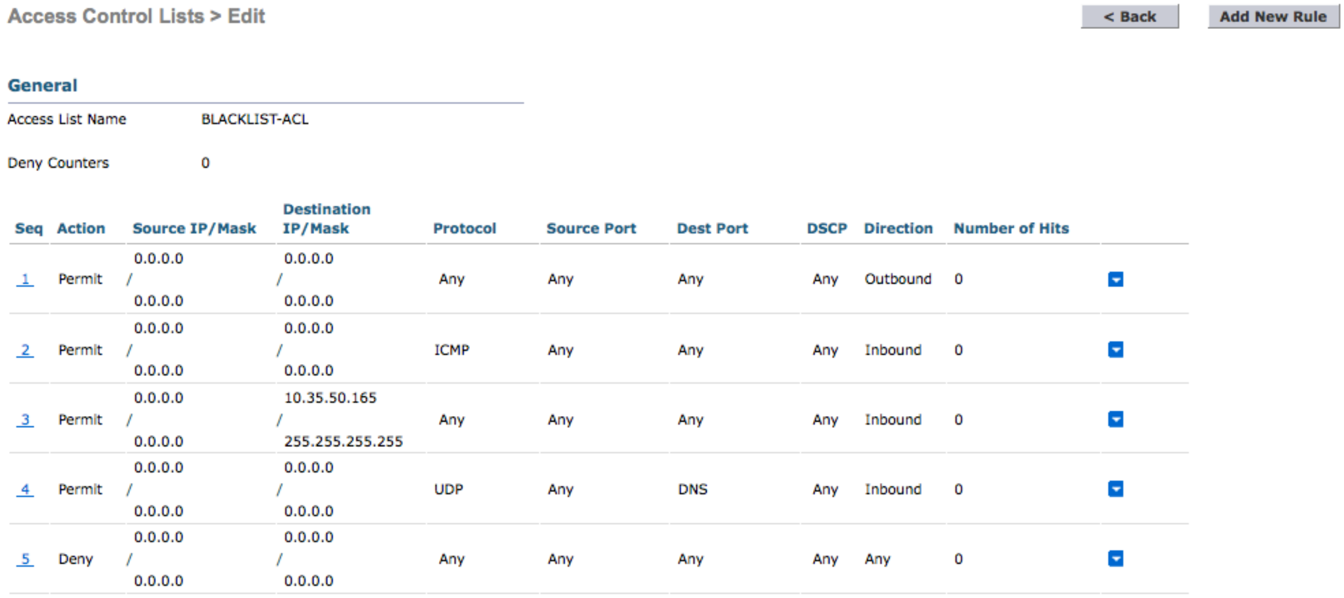
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	0
3	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0
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
6	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	0
9	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

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 2 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 20 Blacklist ACL



Access Control Lists > Edit

General

Access List Name   BLACKLIST-ACL

Deny Counters   0

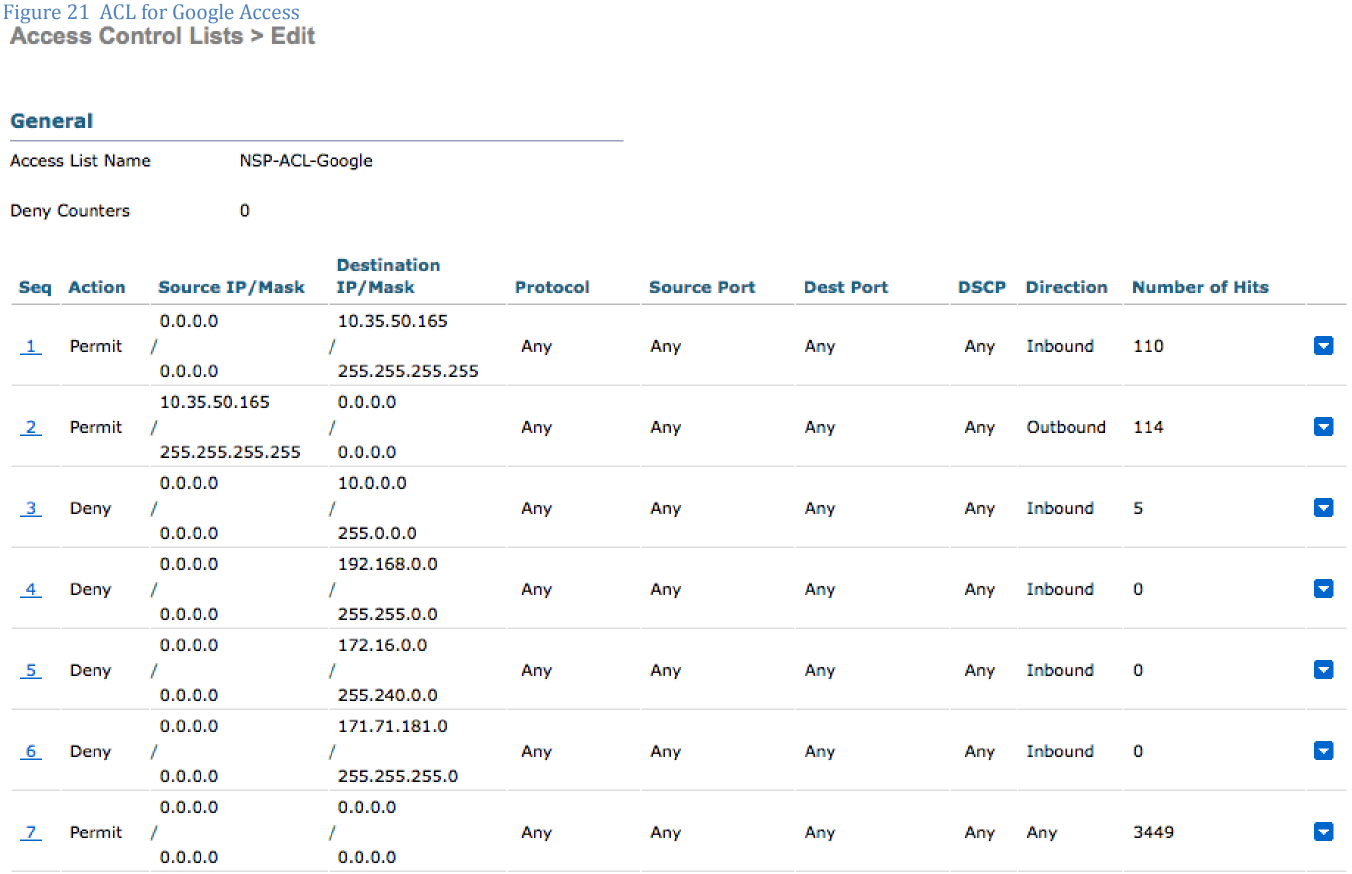
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0	▾
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	0	▾
3	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	0	▾
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0	▾
5	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	▾

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 21 ACL for Google Access



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	
1	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	110	▾
2	Permit	10.35.50.165 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	114	▾
3	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	5	▾
4	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	▾
5	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	0	▾
6	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0	▾
7	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	3449	▾

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.

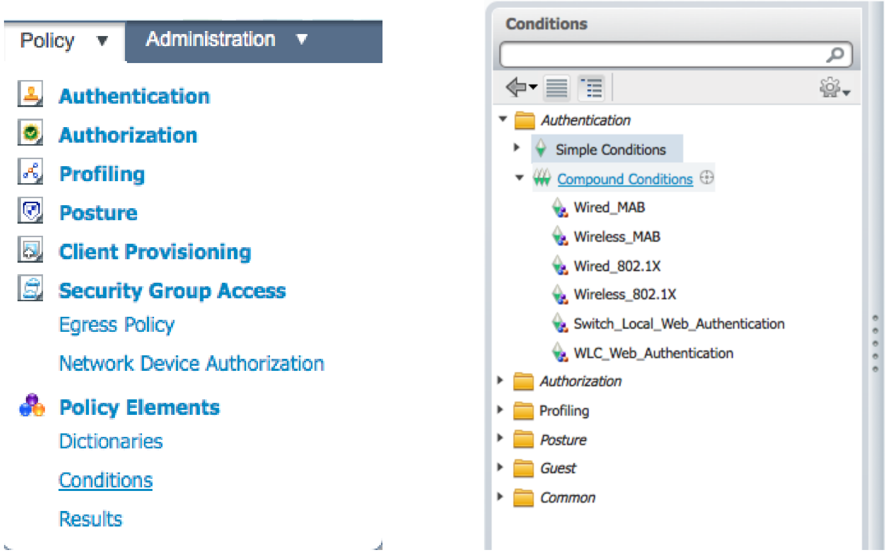
Configure an Authentication Policy

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 1 Click Policy → Conditions → Authentication → Compound Conditions

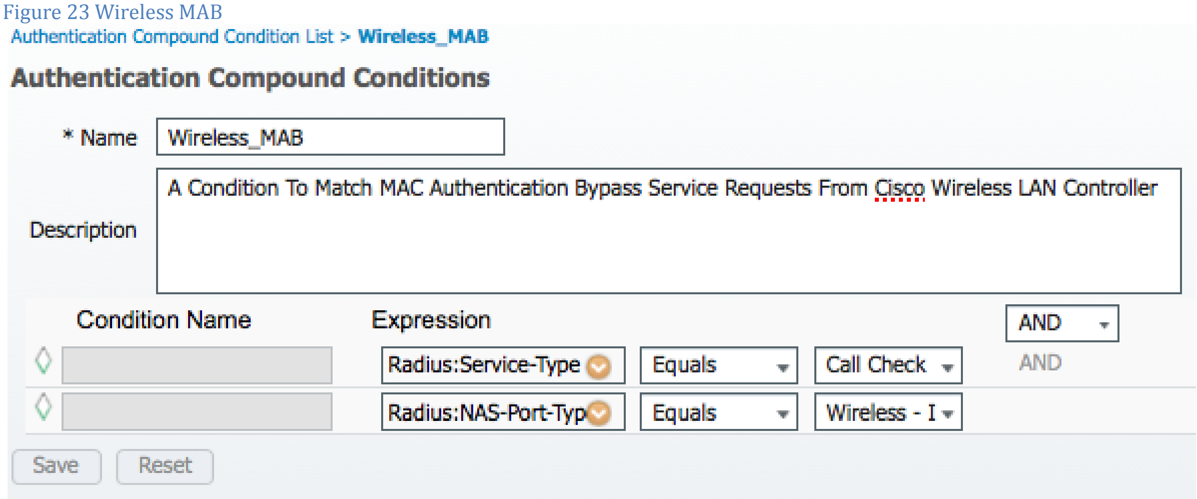
Figure 22 Compound Conditions Navigation



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 23 Wireless MAB



Authentication Compound Condition List > **Wireless_MAB**

Authentication Compound Conditions

* Name: Wireless_MAB

Description: A Condition To Match MAC Authentication Bypass Service Requests From Cisco Wireless LAN Controller

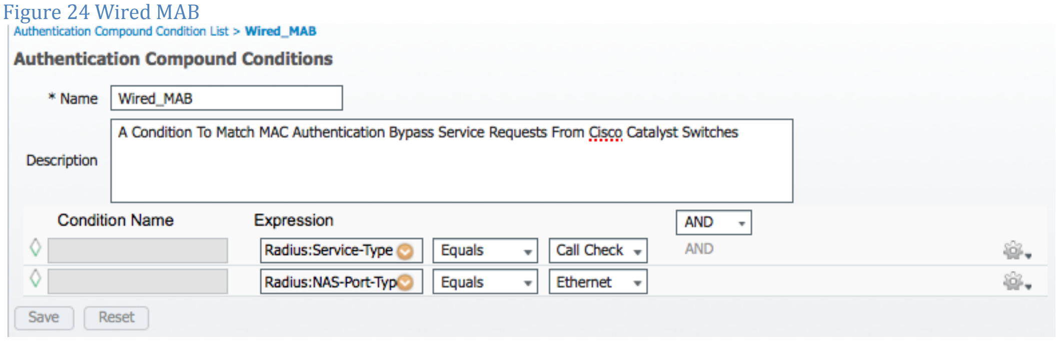
Condition Name	Expression			AND
	Radius:Service-Type	Equals	Call Check	AND
	Radius:NAS-Port-Typ	Equals	Wireless - I	

Save Reset

Step 3 Review a compound condition named "**Wired_MAB**"

"Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Ethernet"

Figure 24 Wired MAB



Authentication Compound Condition List > **Wired_MAB**

Authentication Compound Conditions

* Name: Wired_MAB

Description: A Condition To Match MAC Authentication Bypass Service Requests From Cisco Catalyst Switches

Condition Name	Expression			AND
	Radius:Service-Type	Equals	Call Check	AND
	Radius:NAS-Port-Typ	Equals	Ethernet	

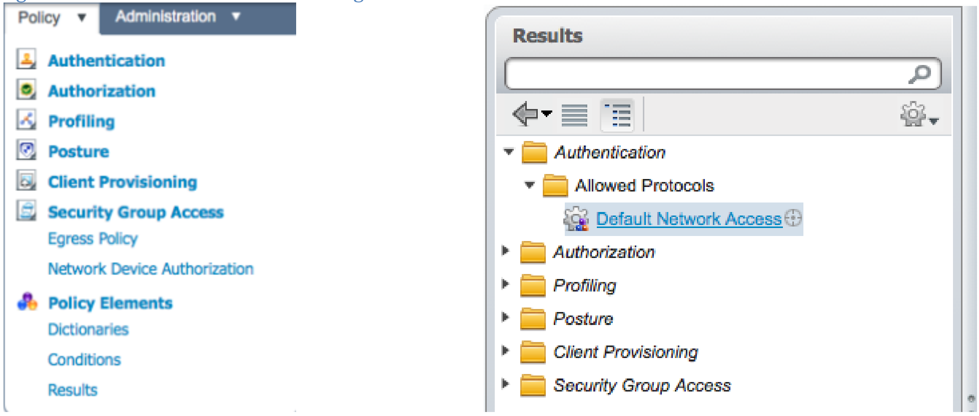
Procedure 2 Verify Default Network Access Result

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

Step 1 Click Policy → Policy Elements → Results

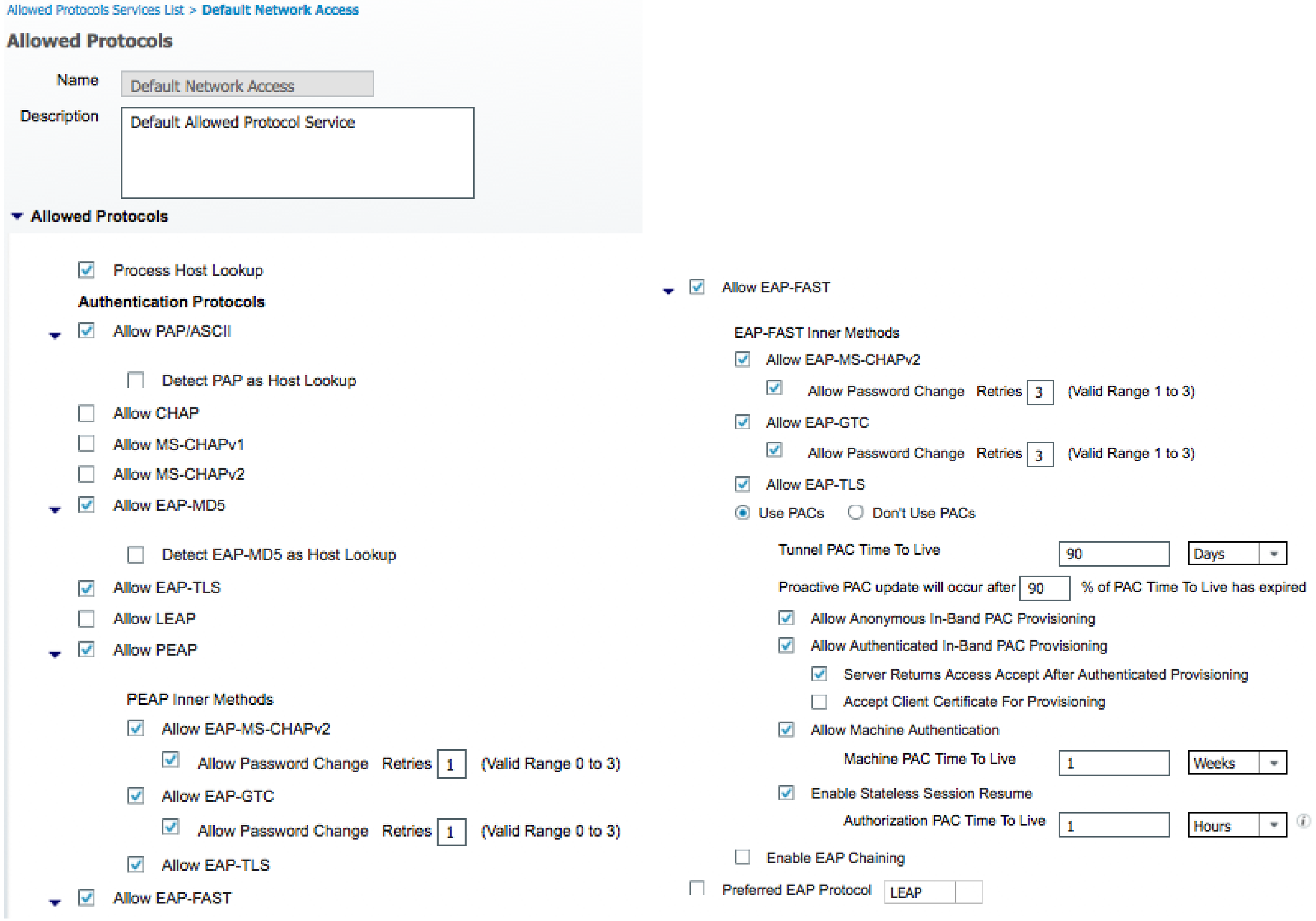
Step 2 Click Authentication → Allowed Protocols → Default Network Access

Figure 25 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 26 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

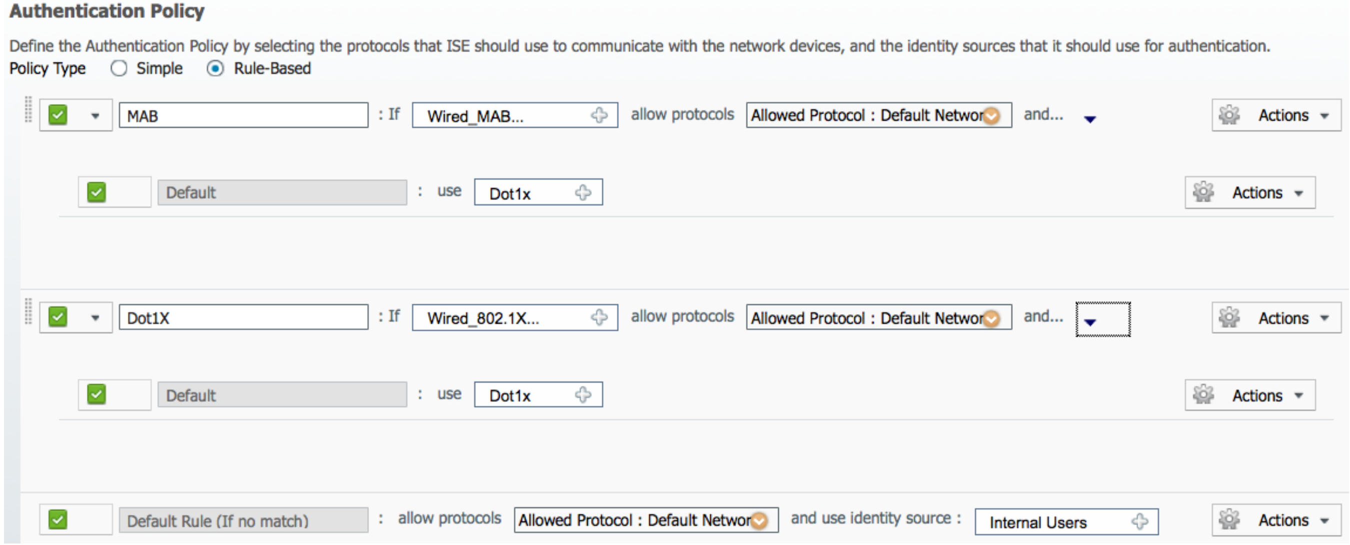
      Authorization PAC Time To Live 1 Hours

  □ Enable EAP Chaining

□ Preferred EAP Protocol LEAP

Step 3 Review Authentication Policy Configuration, following screenshot is full policy view for reference, individual policies will be configured in subsequent steps

Figure 27 Authentication Policy Configuration



Authentication Policy

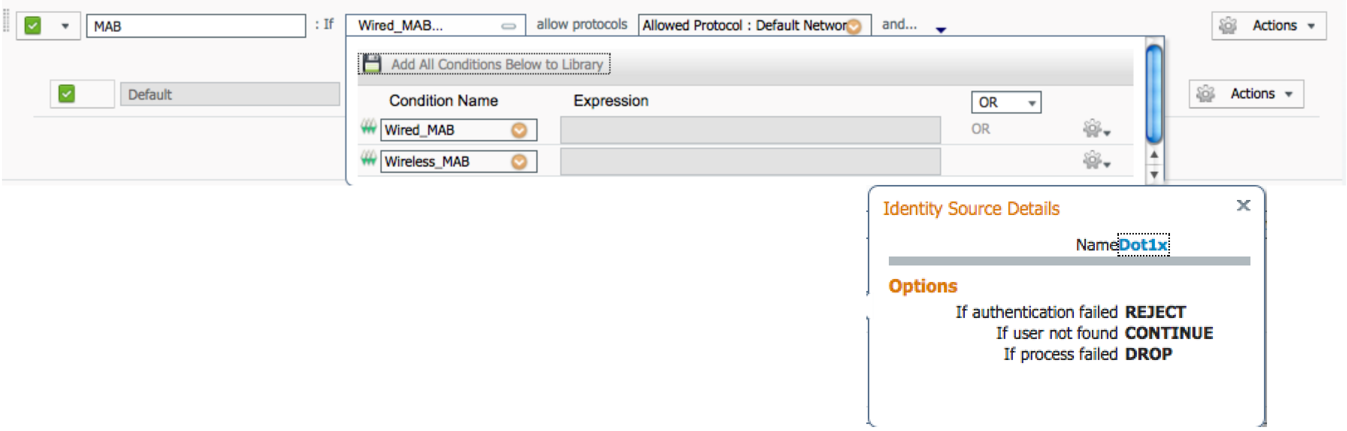
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑	MAB	: If	Wired_MAB...	allow protocols	Allowed Protocol : Default Networ	and...
☑	Default	: use	Dot1x			
☑	Dot1X	: If	Wired_802.1X...	allow protocols	Allowed Protocol : Default Networ	and...
☑	Default	: use	Dot1x			
☑	Default Rule (If no match)	:	allow protocols	Allowed Protocol : Default Networ	and use identity source :	Internal Users

Step 4 Authentication policy for MAB, please add conditions (**Wired_MAB** OR **Wireless_MAB**)

Figure 28 MAC Authentication Bypass Policy



☑ MAB : If Wired_MAB... allow protocols Allowed Protocol : Default Networ and... Actions

☑ Default Actions

Add All Conditions Below to Library

Condition Name	Expression	OR
Wired_MAB		OR
Wireless_MAB		

Identity Source Details

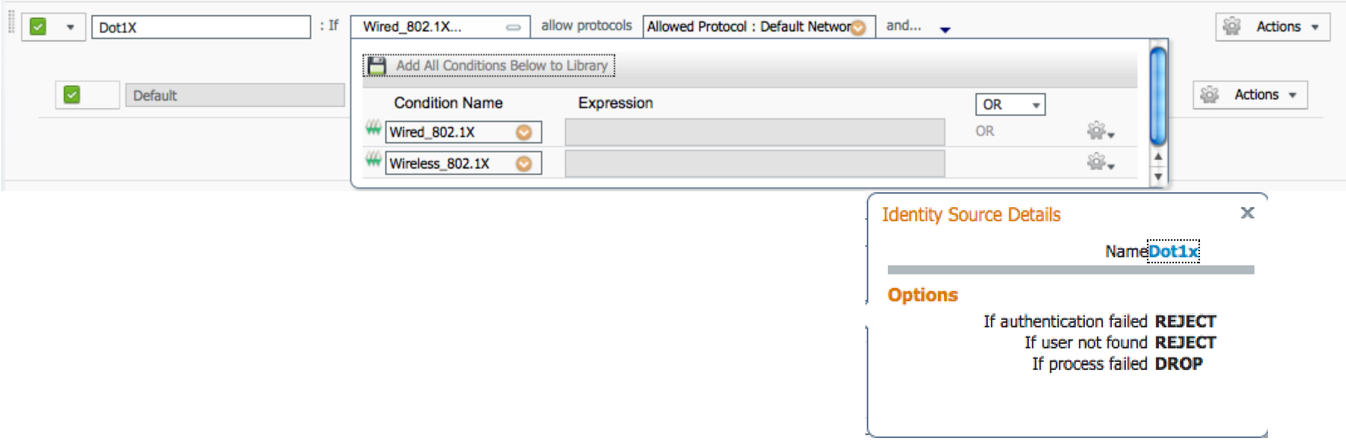
Name Dot1x

Options

If authentication failed **REJECT**
If user not found **CONTINUE**
If process failed **DROP**

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

Figure 29 802.1X Policy



☑ Dot1X : If Wired_802.1X... allow protocols Allowed Protocol : Default Networ and... Actions

☑ Default Actions

Add All Conditions Below to Library

Condition Name	Expression	OR
Wired_802.1X		OR
Wireless_802.1X		

Identity Source Details

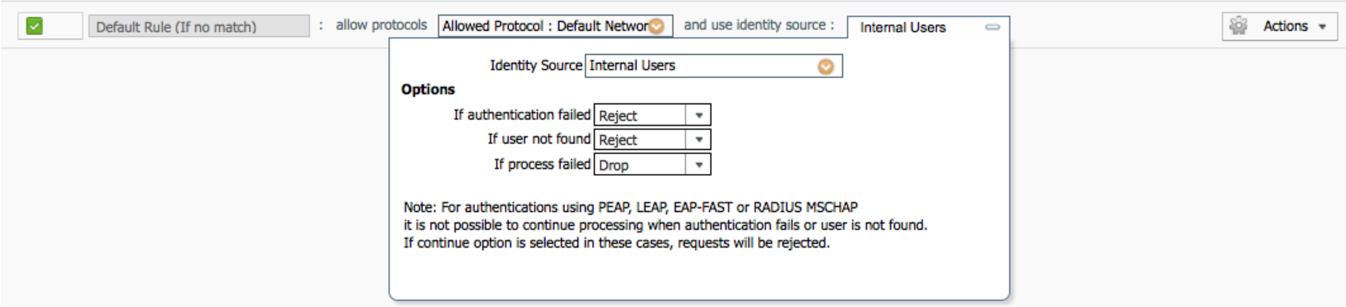
Name Dot1x

Options

If authentication failed **REJECT**
If user not found **REJECT**
If process failed **DROP**

Step 6 Default Authentication policy.

Figure 30 Default Authentication Policy



☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Networ and use identity source : Internal Users Actions

Identity Source Internal Users

Options

If authentication failed Reject
If user not found Reject
If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP
it is not possible to continue processing when authentication fails or user is not found.
If continue option is selected in these cases, requests will be rejected.

Procedure 3 Configure an Authorization policy named "CWA"

Step 1 Click Policy → Policy Elements → Results.

Step 2 Choose Authorization → Authorization Profiles

Step 3 Click "ADD"

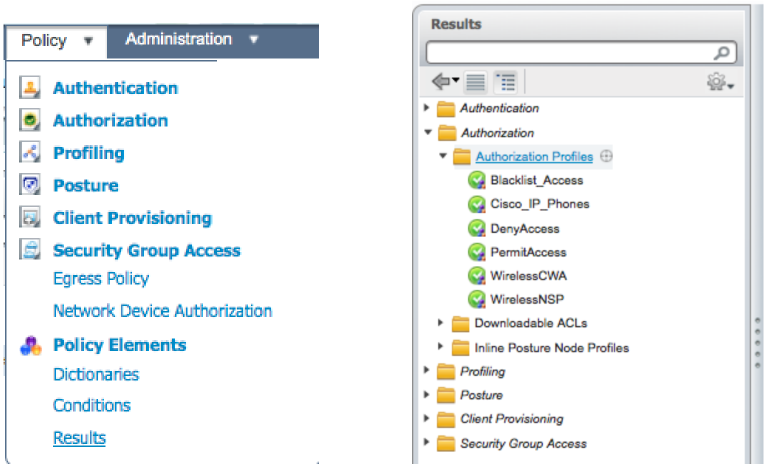


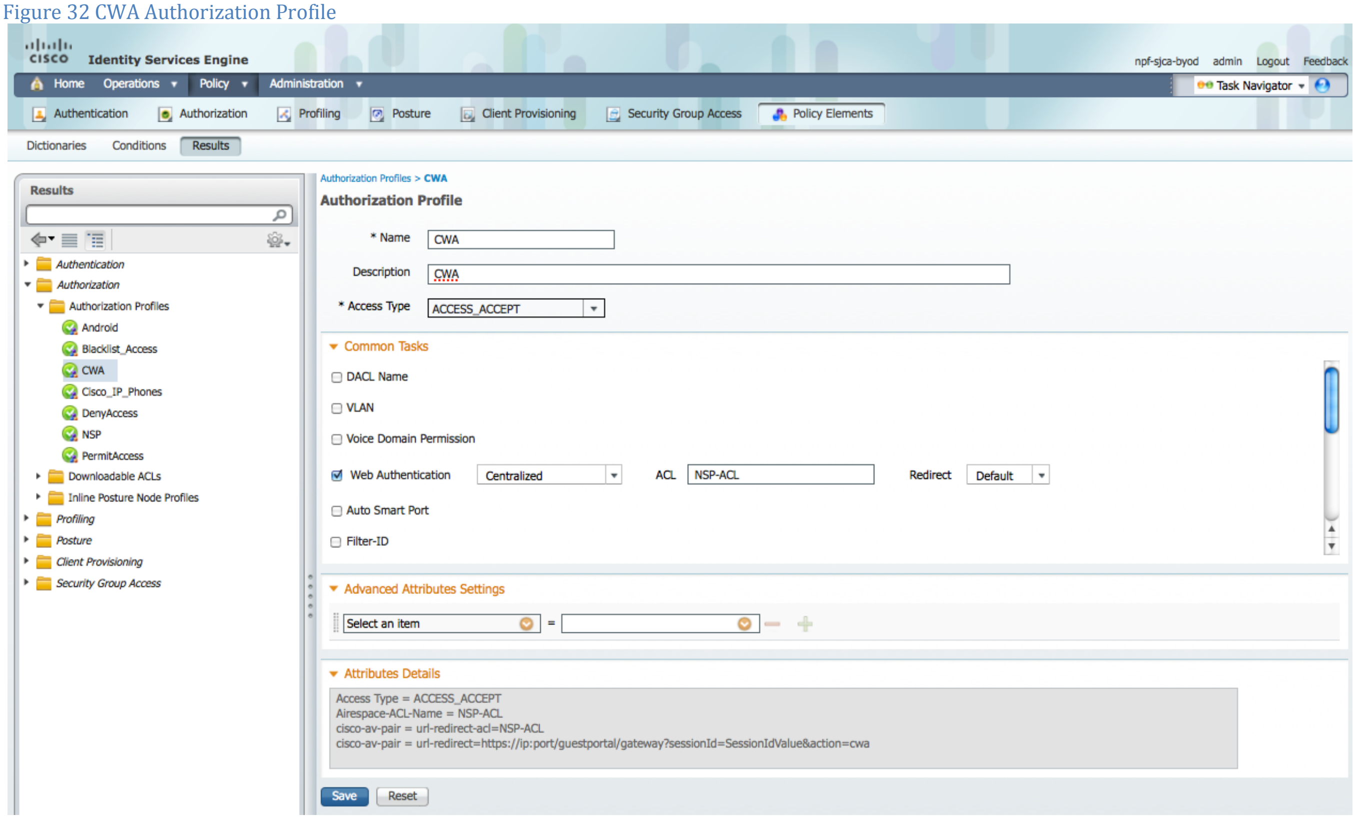
Figure 31 Authorization Profiles Navigation

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.

Figure 32 CWA Authorization Profile



Authorization Profiles > CWA

Authorization Profile

* Name: CWA

Description: CWA

* Access Type: ACCESS_ACCEPT

Common Tasks

☐ DACL Name

☐ VLAN

☐ Voice Domain Permission

☑ Web Authentication: Centralized ACL: NSP-ACL Redirect: Default

☐ Auto Smart Port

☐ Filter-ID

Advanced Attributes Settings

Select an item =

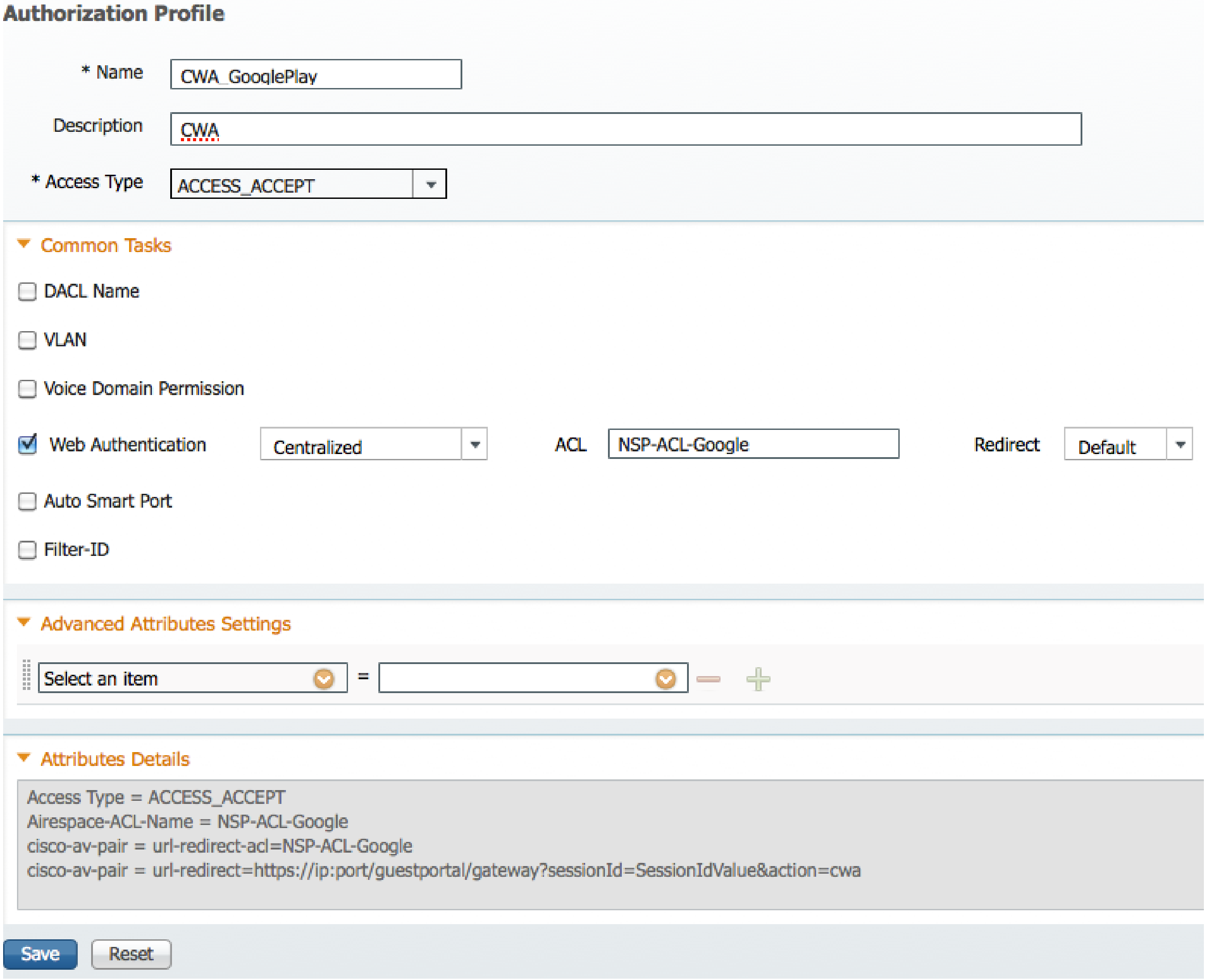
Attributes Details

```
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=cwa
```

Step 5 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 33 CWA Authorization Profile for Android to Access Google



Authorization Profile

* Name	CWA_GooglePlay
Description	CWA
* Access Type	ACCESS_ACCEPT

▼ Common Tasks

☐ DACL Name

☐ VLAN

☐ Voice Domain Permission

☑ Web Authentication Centralized ACL NSP-ACL-Google Redirect Default

☐ Auto Smart Port

☐ Filter-ID

▼ Advanced Attributes Settings

▼ Attributes Details

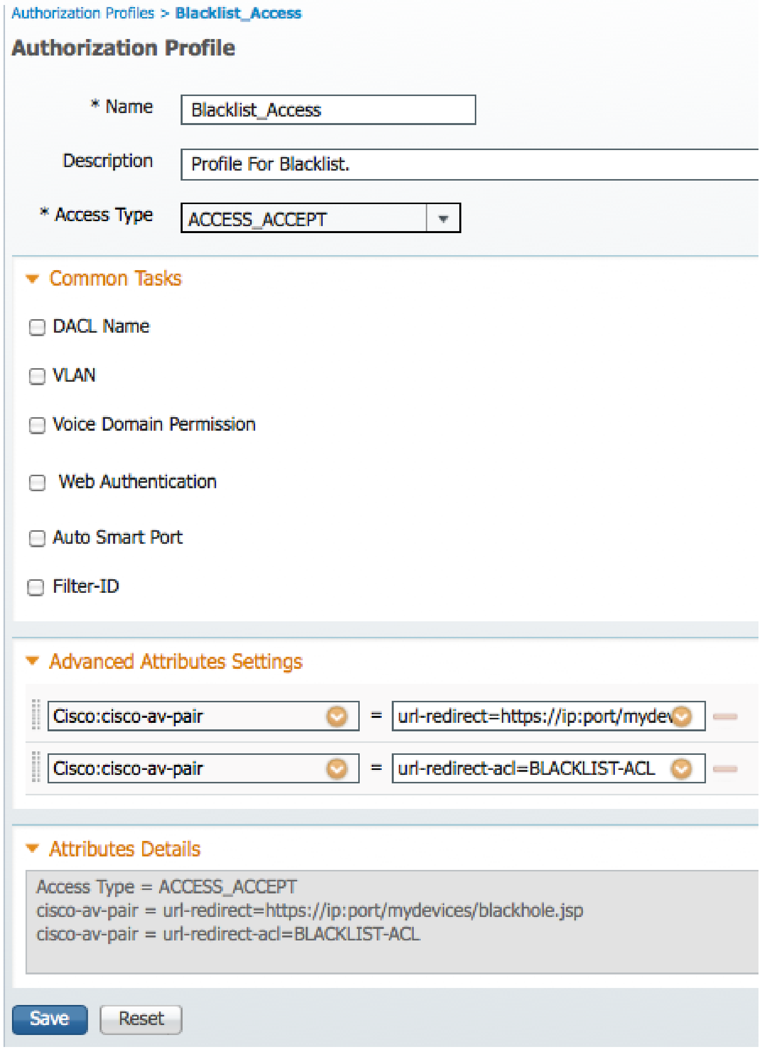
```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = NSP-ACL-Google
cisco-av-pair = url-redirect-acl=NSP-ACL-Google
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

Procedure 4 Review Policy conditions under Authorization Profiles

Step 1 Click Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Review Profile named "**Blacklist_Access**"

Figure 34 Blacklist Authorization Profile



Authorization Profiles > Blacklist_Access

Authorization Profile

* Name: Blacklist_Access

Description: Profile For Blacklist.

* Access Type: ACCESS_ACCEPT

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

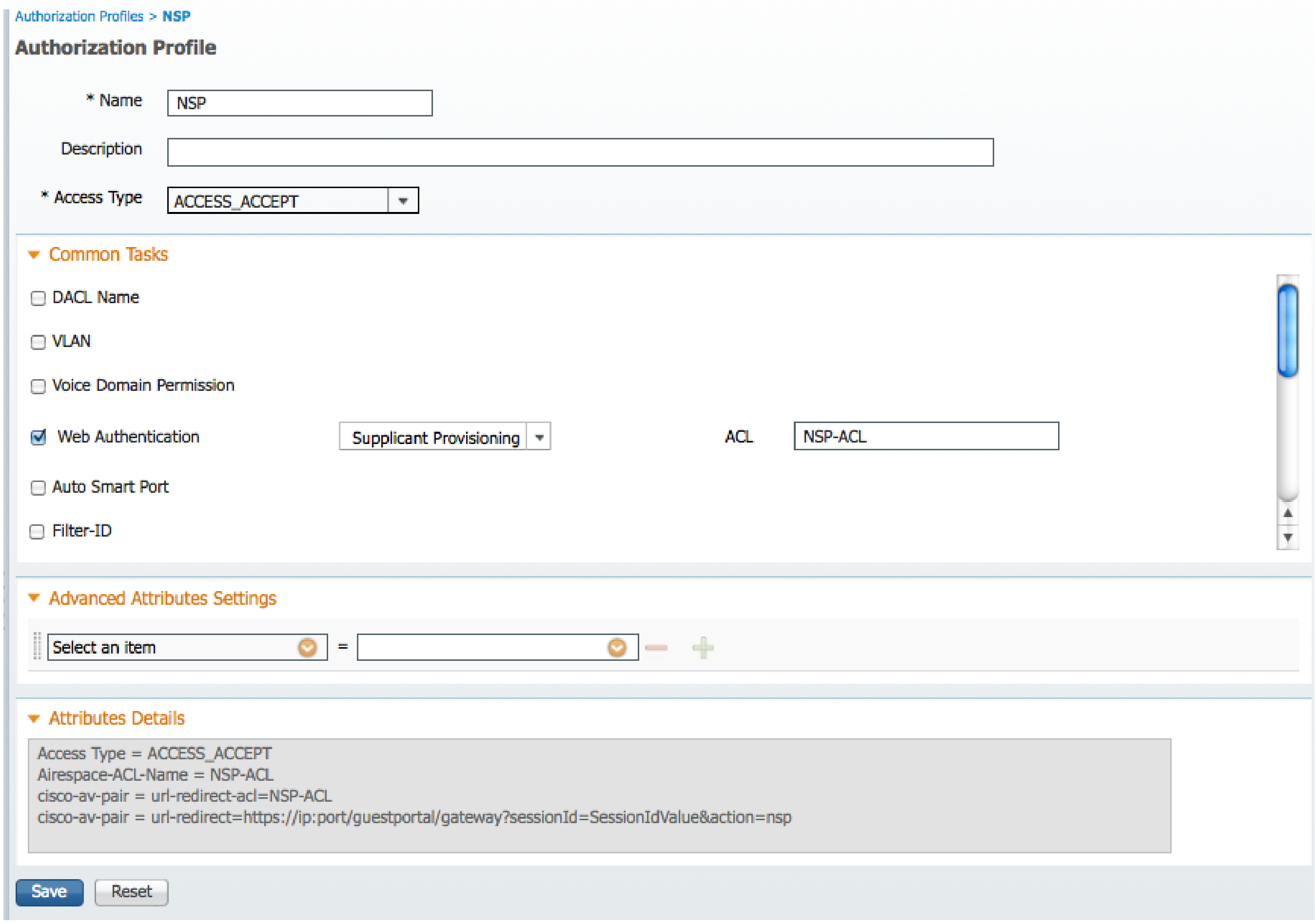
```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect=https://ip:port/mydevices/blackhole.jsp
cisco-av-pair = url-redirect-acl=BLACKLIST-ACL
```

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 3 Create an Authorization Profile named “**NSP**”

Figure 35 Native Supplicant Provisioning Authorization Profile



Authorization Profiles > NSP

Authorization Profile

* Name: NSP

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☐ DACL Name

☐ VLAN

☐ Voice Domain Permission

☑ Web Authentication — Supplicant Provisioning — ACL: NSP-ACL

☐ Auto Smart Port

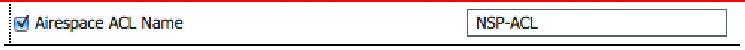
☐ Filter-ID

Advanced Attributes Settings

Select an item =

Attributes Details

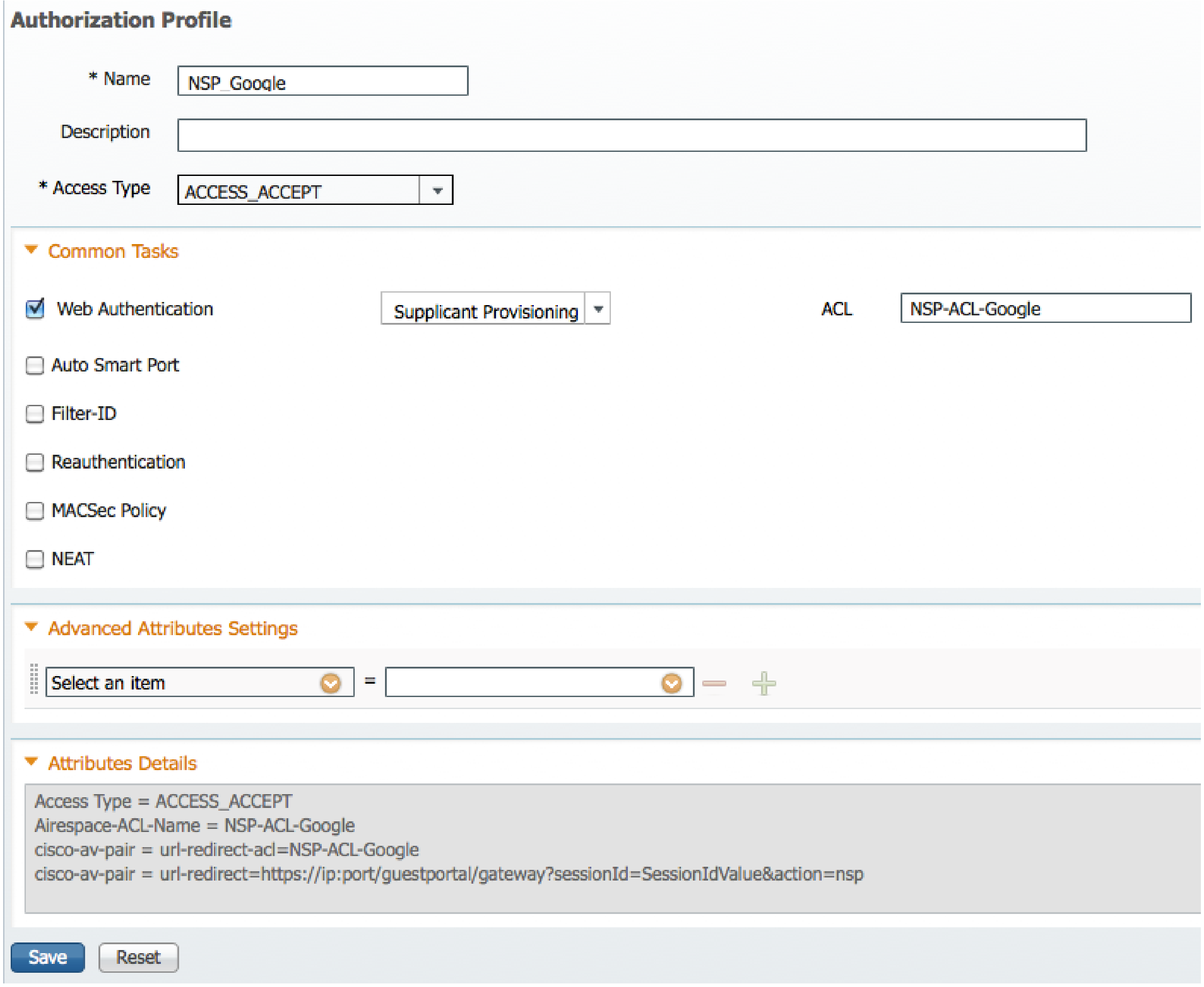
```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = NSP-ACL
cisco-av-pair = url-redirect-acl=NSP-ACL
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp
```

Note: Please also click 

☑ Airespace ACL Name: NSP-ACL

Step 4 Create an Authorization Profile named “**NSP_Google**”

Figure 36 NSP_Google Authorization Profile



Authorization Profile

* Name: NSP_Google

Description:

* Access Type: ACCESS_ACCEPT

▼ Common Tasks

☑ Web Authentication — Supplicant Provisioning — ACL: NSP-ACL-Google

□ Auto Smart Port

□ Filter-ID

□ Reauthentication

□ MACSec Policy

□ NEAT

▼ 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=nsp
```

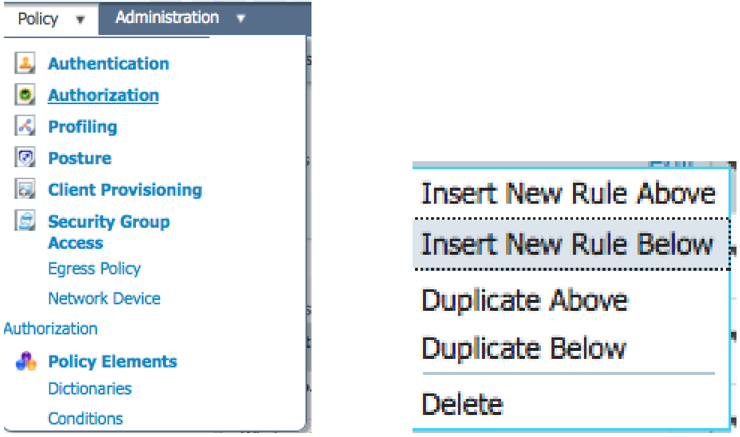
Note: Please also click ☑ Airespace ACL Name NSP-ACL-Google

Procedure 5 Add the Authorization Policies

Step 1 Click Policy → Authorization

Step 2 Click "Insert New Rule Below"

Figure 37 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

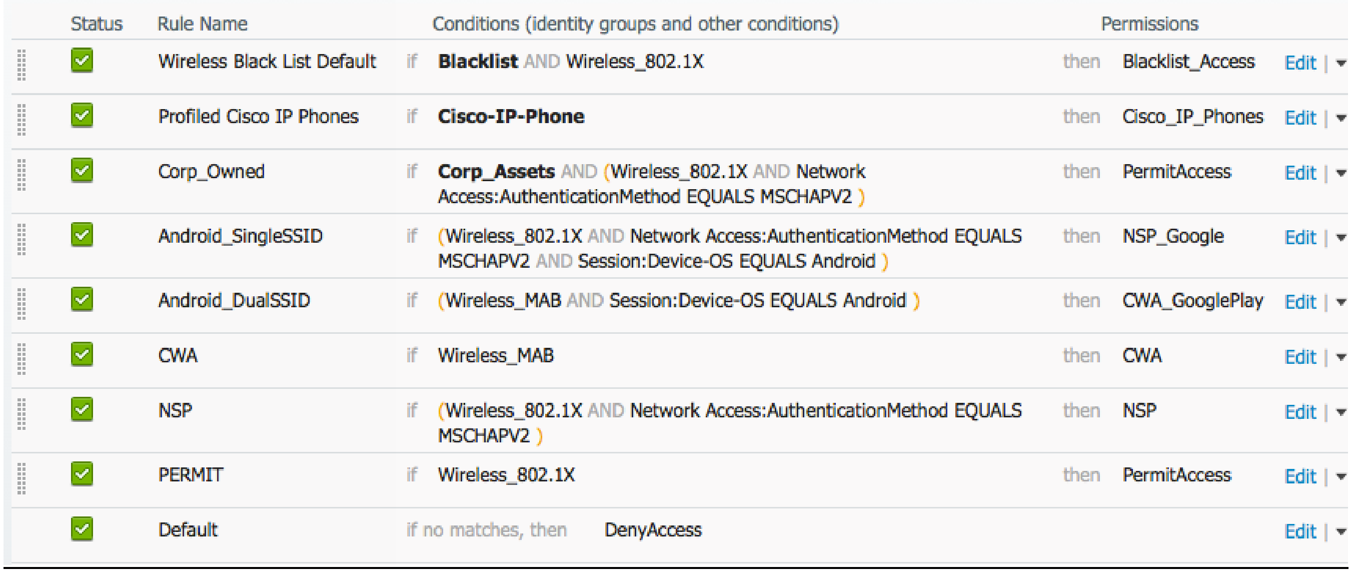
CWA = Authorization rule added for Central Web Authentication.

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 38 Authorization Policy



Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
☑	Wireless Black List Default	if **Blacklist** AND Wireless_802.1X	then Blacklist_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if **Cisco-IP-Phone**	then Cisco_IP_Phones	Edit | ▾
☑	Corp_Owned	if **Corp_Assets** AND (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then PermitAccess	Edit | ▾
☑	Android_SingleSSID	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	then NSP_Google	Edit | ▾
☑	Android_DualSSID	if (Wireless_MAB AND Session:Device-OS EQUALS Android)	then CWA_GooglePlay	Edit | ▾
☑	CWA	if Wireless_MAB	then CWA	Edit | ▾
☑	NSP	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then NSP	Edit | ▾
☑	PERMIT	if Wireless_802.1X	then PermitAccess	Edit | ▾
☑	Default	if no matches, then DenyAccess		Edit | ▾

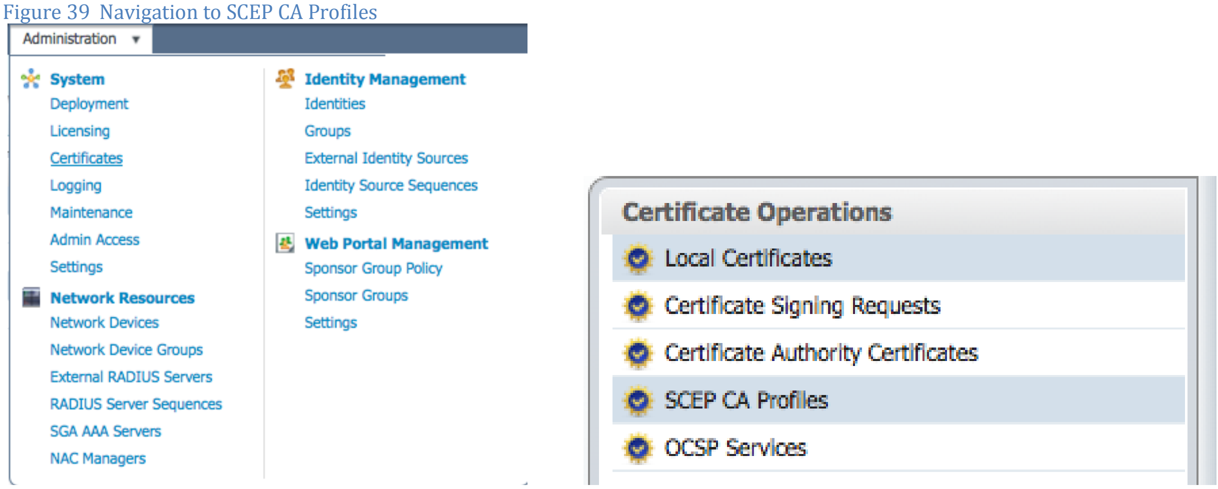
Simple Certificate Enrollment Protocol (SCEP) Setup

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.

Procedure 1 Add a SCEP CA Profile

Step 1 Click Administration → Certificates → SCEP CA Profiles

Figure 39 Navigation to SCEP CA Profiles

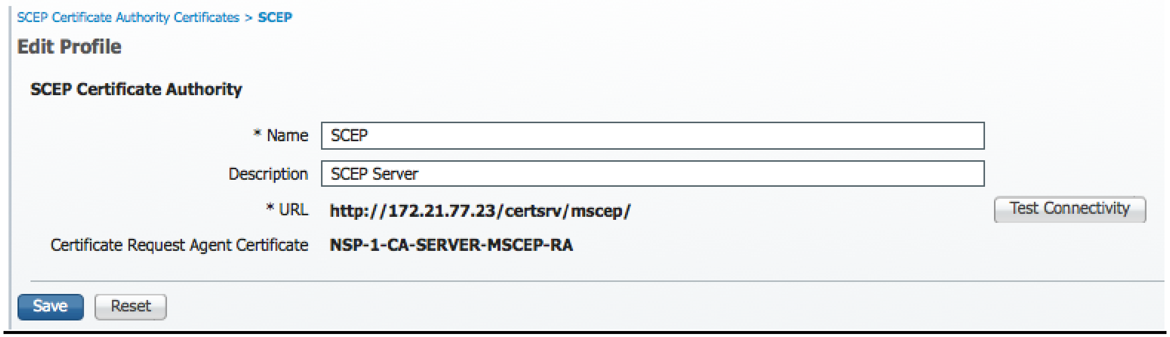


Step 2 Click Add

Step 3 Add SCEP CA profile

```
    CA Server IP = 172.21.77.24.
```

Figure 40 SCEP CA Profile



Edit Profile

SCEP Certificate Authority

* Name	SCEP
Description	SCEP Server
* URL	http://172.21.77.23/certsrv/mscep/
Certificate Request Agent Certificate	NSP-1-CA-SERVER-MSCEP-RA

STOP You are done!
Please see the TrustSec How-To Guide titled "On-boarding" for more information.

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

Procedure 1 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 dcpromo 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

Procedure 2 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

Procedure 3 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

Procedure 4 Modify the Registry

Step 1 Type regedit from the ‘Start’ menu

Step 2 In the registry editor, go to: HKEY_LOCAL_MACHINE → Software → Microsoft → Crytography → MSCEP

Step 3 Click the key labeled: Enforce Password

Step 4 Modify EnforcePassword from value 1 to 0.

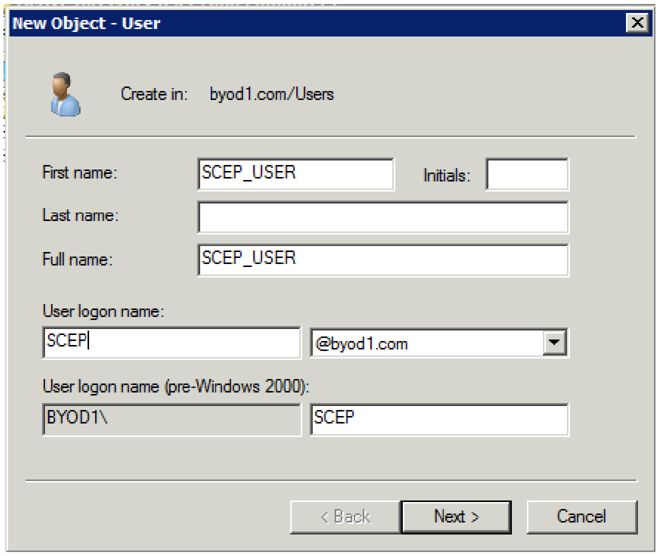
Step 5 Restart the server.

Configuring SCEP Enrollment.

Procedure 1 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.



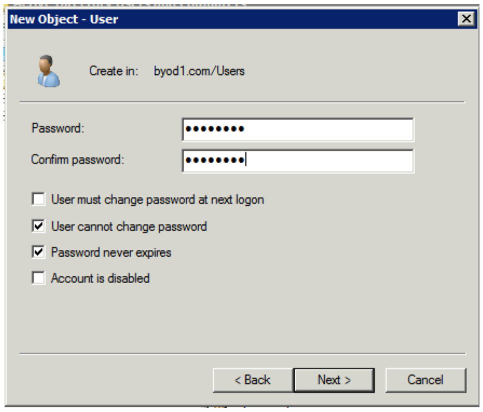
New Object - User

Create in: byod1.com/Users

First name: SCEP_USER
Initials:
Last name:
Full name: SCEP_USER

User logon name:
SCEP @byod1.com

User logon name (pre-Windows 2000):
BYOD1\ SCEP

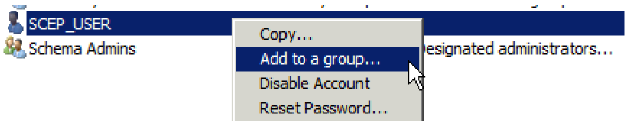


New Object - User

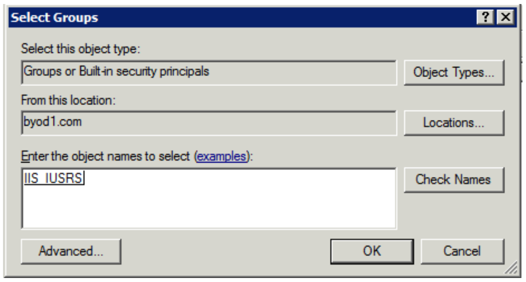
Create in: byod1.com/Users

Password: ••••••••
Confirm password: ••••••••

☐ User must change password at next logon
☑ User cannot change password
☑ Password never expires
☐ Account is disabled



SCEP_USER
Schema Admins ...esignated administrators...



Select Groups

Select this object type:
Groups or Built-in security principals

From this location:
byod1.com

Enter the object names to select (examples):
IIS_IUSRS

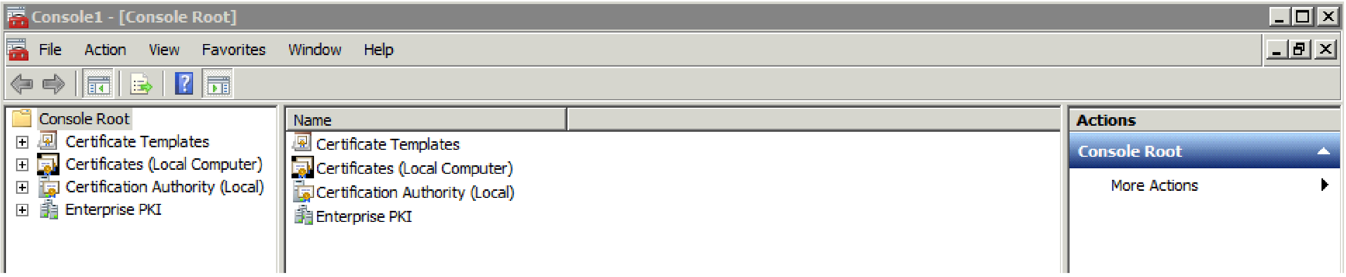
Reference: http://technet.microsoft.com/en-us/library/ff955646%28v=ws.10%29.aspx

Procedure 2 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).



Console1 - [Console Root]

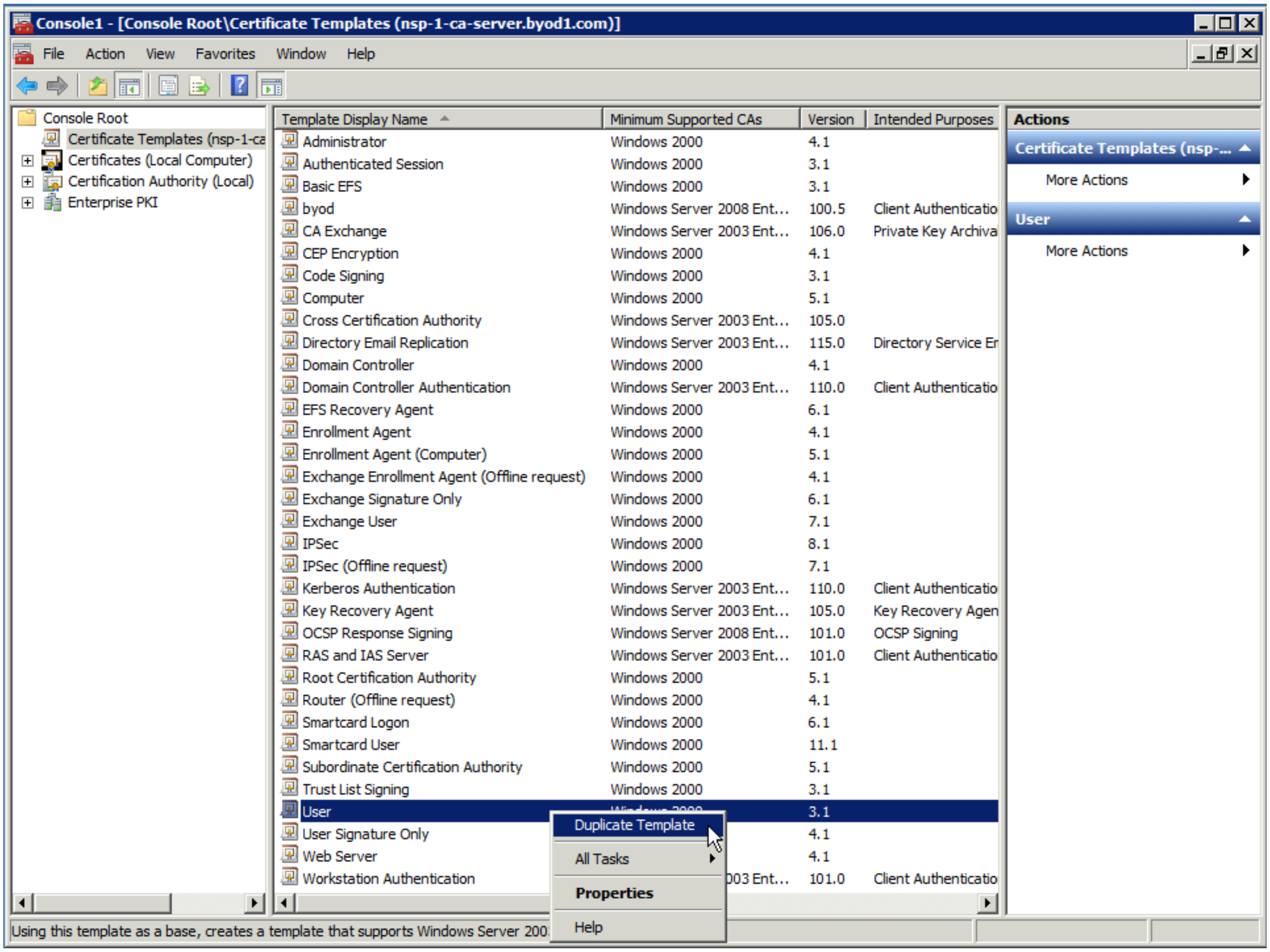
Console Root
- Certificate Templates
- Certificates (Local Computer)
- Certification Authority (Local)
- Enterprise PKI

Name
- Certificate Templates
- Certificates (Local Computer)
- Certification Authority (Local)
- Enterprise PKI

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

Procedure 3 Create a New Certificate Template

Step 1 Select Certificate Templates and duplicate 'User' template.

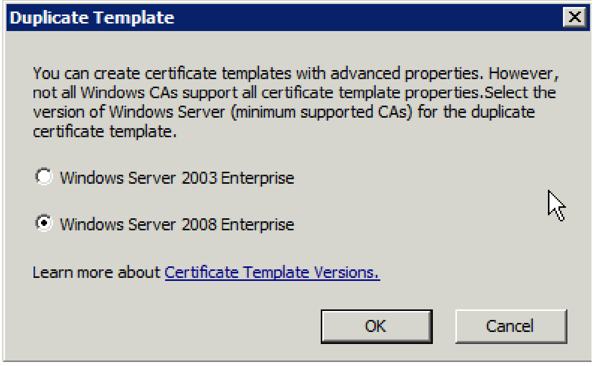

Console1 - [Console Root\Certificate Templates (nsp-1-ca-server.byod1.com)]
File
Action
View
Favorites
Window
Help
Console Root
Certificate Templates (nsp-1-ca
Certificates (Local Computer)
Certification Authority (Local)
Enterprise PKI
Actions
Certificate Templates (nsp-...
More Actions
User
More Actions
Duplicate Template
All Tasks
Properties
Help

Template Display Name	Minimum Supported CAs	Version	Intended Purposes
Administrator	Windows 2000	4.1	
Authenticated Session	Windows 2000	3.1	
Basic EFS	Windows 2000	3.1	
byod	Windows Server 2008 Ent...	100.5	Client Authenticatio
CA Exchange	Windows Server 2003 Ent...	106.0	Private Key Archiva
CEP Encryption	Windows 2000	4.1	
Code Signing	Windows 2000	3.1	
Computer	Windows 2000	5.1	
Cross Certification Authority	Windows Server 2003 Ent...	105.0	
Directory Email Replication	Windows Server 2003 Ent...	115.0	Directory Service Er
Domain Controller	Windows 2000	4.1	
Domain Controller Authentication	Windows Server 2003 Ent...	110.0	Client Authenticatio
EFS Recovery Agent	Windows 2000	6.1	
Enrollment Agent	Windows 2000	4.1	
Enrollment Agent (Computer)	Windows 2000	5.1	
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	
Exchange Signature Only	Windows 2000	6.1	
Exchange User	Windows 2000	7.1	
IPSec	Windows 2000	8.1	
IPSec (Offline request)	Windows 2000	7.1	
Kerberos Authentication	Windows Server 2003 Ent...	110.0	Client Authenticatio
Key Recovery Agent	Windows Server 2003 Ent...	105.0	Key Recovery Agen
OCSP Response Signing	Windows Server 2008 Ent...	101.0	OCSP Signing
RAS and IAS Server	Windows Server 2003 Ent...	101.0	Client Authenticatio
Root Certification Authority	Windows 2000	5.1	
Router (Offline request)	Windows 2000	4.1	
Smartcard Logon	Windows 2000	6.1	
Smartcard User	Windows 2000	11.1	
Subordinate Certification Authority	Windows 2000	5.1	
Trust List Signing	Windows 2000	3.1	
User	Windows 2000	3.1	
User Signature Only		4.1	
Web Server		4.1	
Workstation Authentication	003 Ent...	101.0	Client Authenticatio

Using this template as a base, creates a template that supports Windows Server 200

Step 2 Select "Windows Server 2008 Enterprise" (in this document example, could also use Windows Server 2003 Enterprise).

Step 3 Click OK.



You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

○ Windows Server 2003 Enterprise

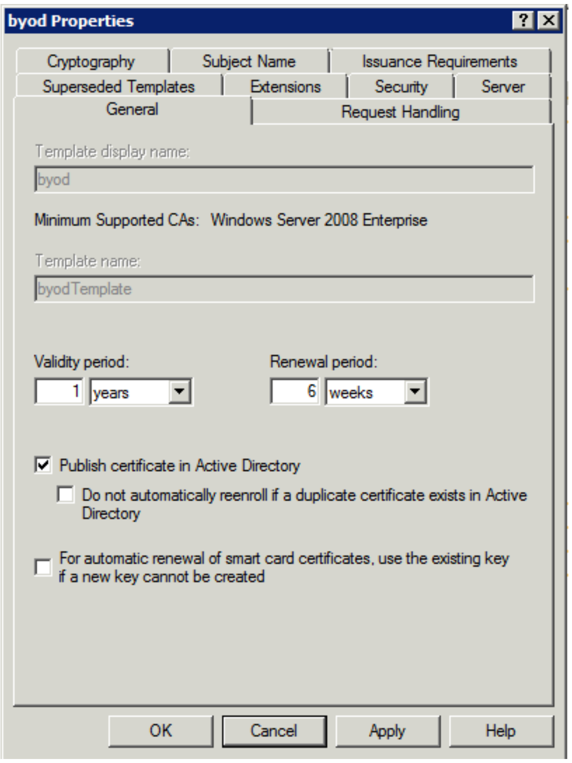
● Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

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

Procedure 4 General Tab

Step 1 Publish the cert in Active Directory, which will sync it to all Domain Controllers.



Template display name: byod

Minimum Supported CAs: Windows Server 2008 Enterprise

Template name: byodTemplate

Validity period: 1 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

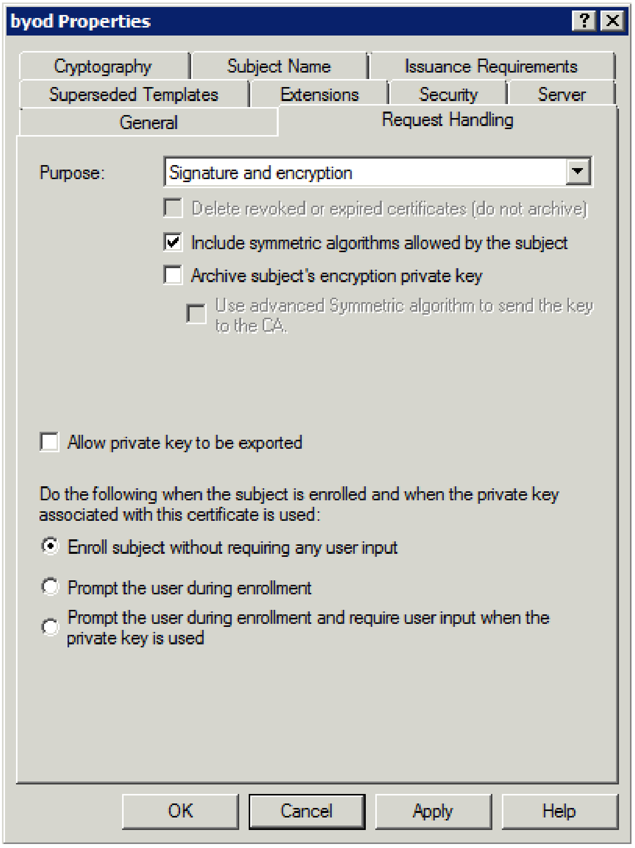
□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Procedure 5 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**".



Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

☑ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Use advanced Symmetric algorithm to send the key to the CA.

□ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

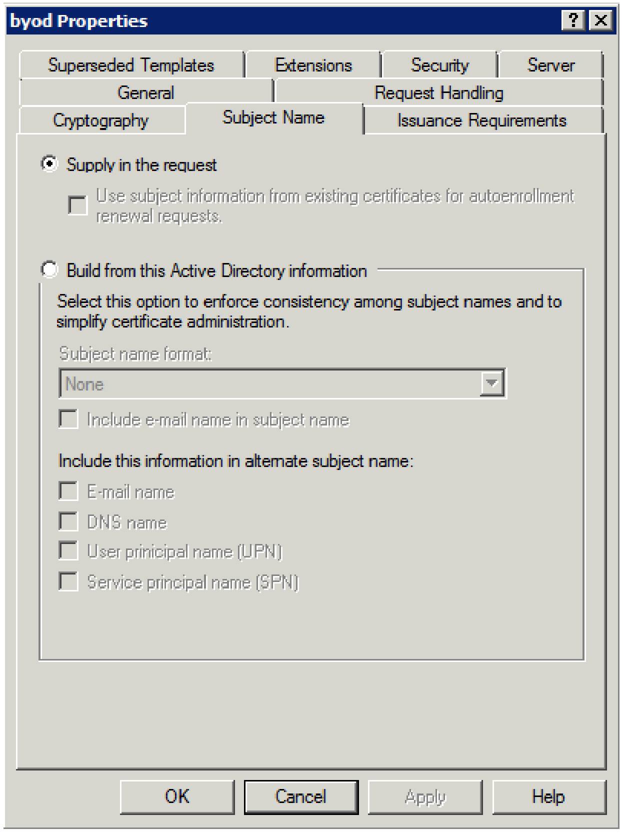
○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

Procedure 6 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.



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

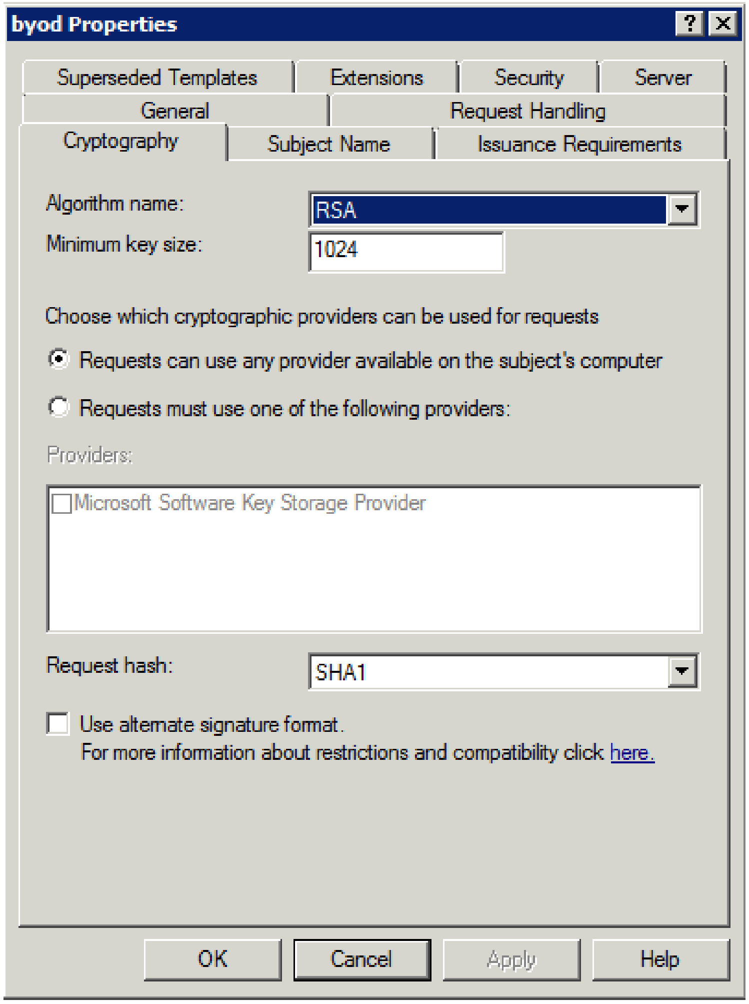
□ DNS name

□ User prinicipal name (UPN)

□ Service principal name (SPN)

Procedure 7 Cryptography Tab

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



byod Properties

Algorithm name: RSA

Minimum key size: 1024

Choose which cryptographic providers can be used for requests

● Requests can use any provider available on the subject's computer

○ Requests must use one of the following providers:

Providers:

□ Microsoft Software Key Storage Provider

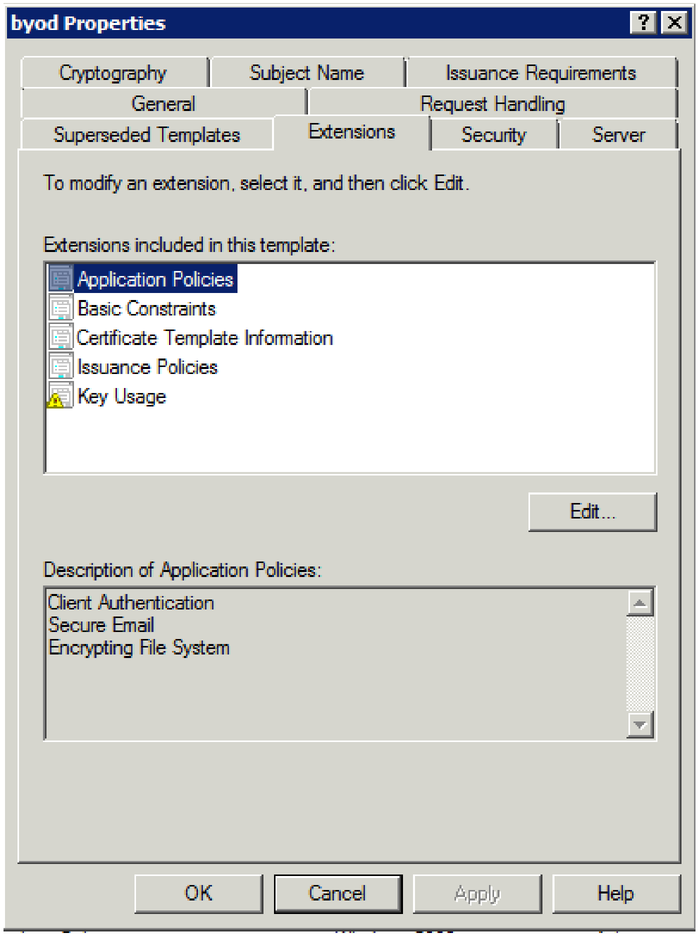
Request hash: SHA1

□ Use alternate signature format.
For more information about restrictions and compatibility click here.

Procedure 8 Extensions Tab

Step 1 Applications Policies:

If the description of the Application Policies do not show what is in the snapshot, you can click "Edit" and "Add" the Application Policies.



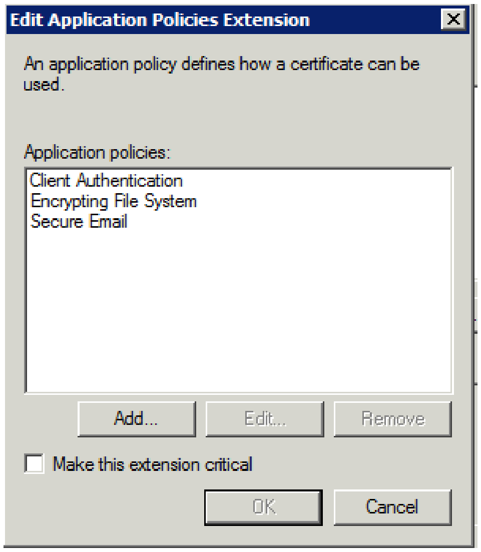
To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Client Authentication
Secure Email
Encrypting File System



An application policy defines how a certificate can be used.

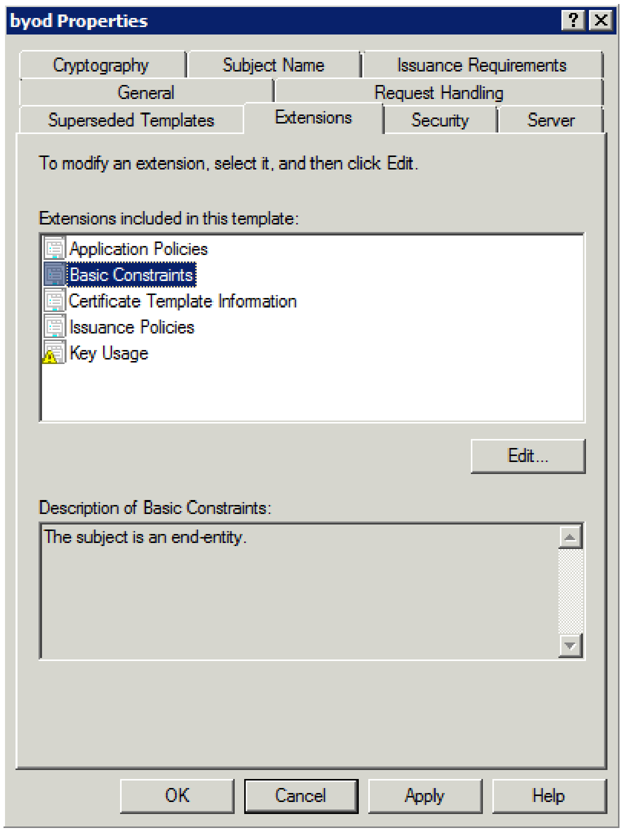
Application policies:

Client Authentication
Encrypting File System
Secure Email

□ Make this extension critical

Step 2 Basic Constraints

This Sets the certificate to belong to an endpoint, and not a subsequent signer



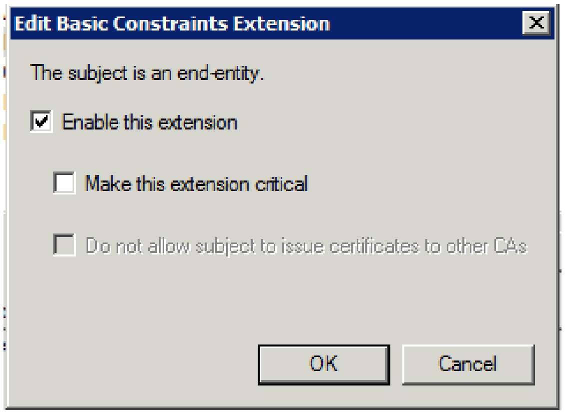
To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Basic Constraints:

The subject is an end-entity.



The subject is an end-entity.

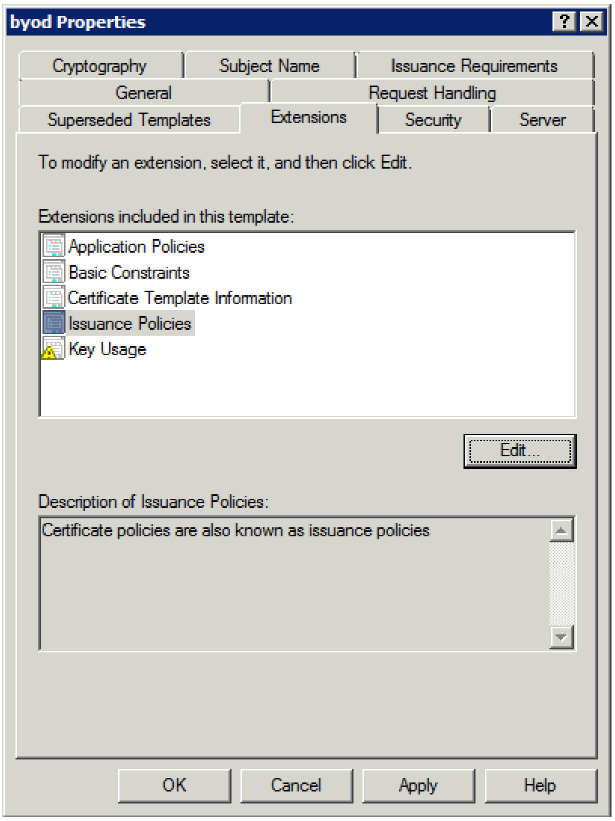
☑ Enable this extension

□ Make this extension critical

□ Do not allow subject to issue certificates to other CAs

Step 3 Issuance Policies

Issuance Policies must be configured, to allow the CA to actually issue the certificate. Please select "All issuance policies"



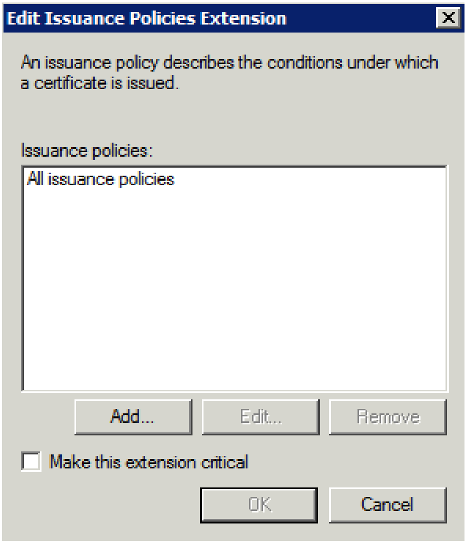
To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Issuance Policies:

Certificate policies are also known as issuance policies



An issuance policy describes the conditions under which a certificate is issued.

Issuance policies:

All issuance policies

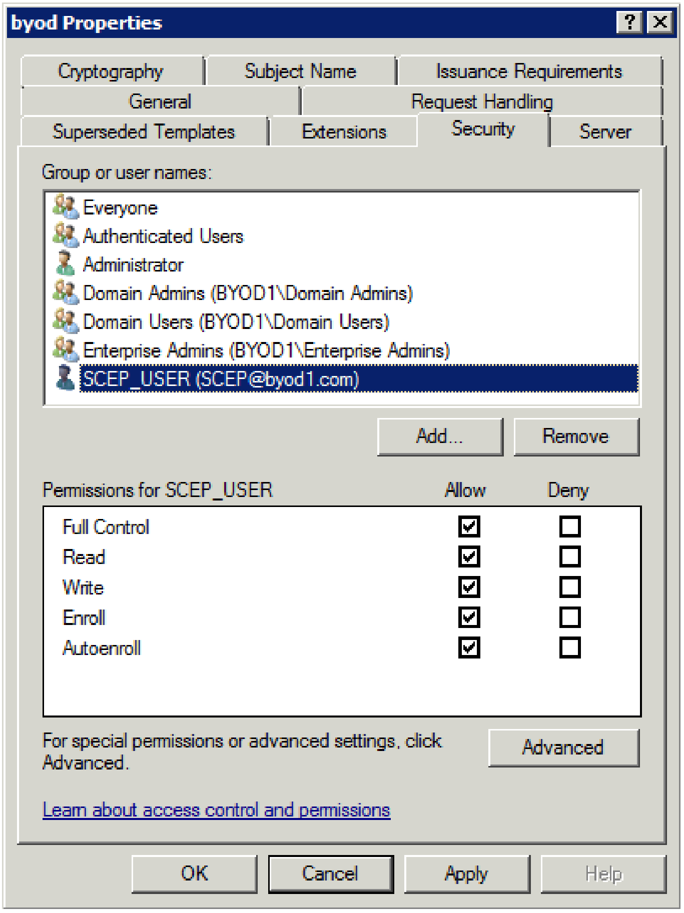
□ Make this extension critical

Procedure 9 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



byod Properties

Group or user names:

- Everyone
- Authenticated Users
- Administrator
- Domain Admins (BYOD1\Domain Admins)
- Domain Users (BYOD1\Domain Users)
- Enterprise Admins (BYOD1\Enterprise Admins)
- SCEP_USER (SCEP@byod1.com)

Permissions for SCEP_USER	Allow	Deny
Full Control	☑	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.

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.

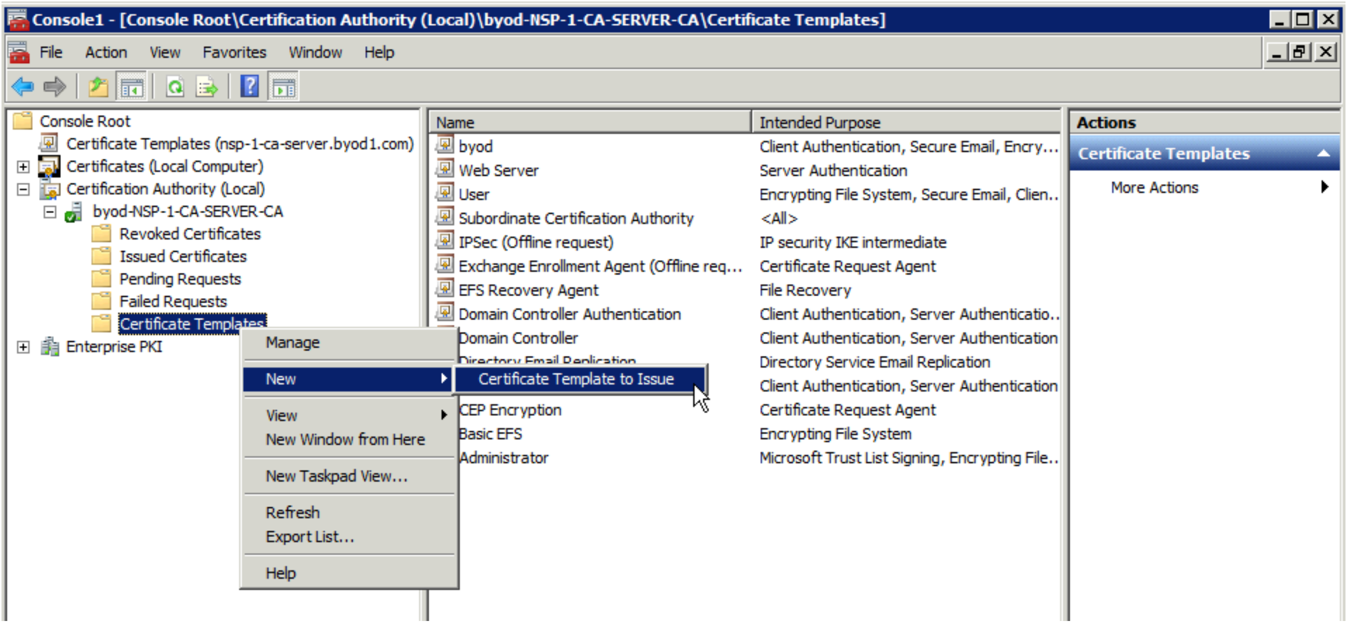
Procedure 1 Assign the new Template for Issuance

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



Name	Intended Purpose
byod	Client Authentication, Secure Email, Encry...
Web Server	Server Authentication
User	Encrypting File System, Secure Email, Clien..
Subordinate Certification Authority	<All>
IPSec (Offline request)	IP security IKE intermediate
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
EFS Recovery Agent	File Recovery
Domain Controller Authentication	Client Authentication, Server Authenticatio..
Domain Controller	Client Authentication, Server Authentication
Directory Email Replication	Directory Service Email Replication
	Client Authentication, Server Authentication
CEP Encryption	Certificate Request Agent
Basic EFS	Encrypting File System
Administrator	Microsoft Trust List Signing, Encrypting File..

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.
```

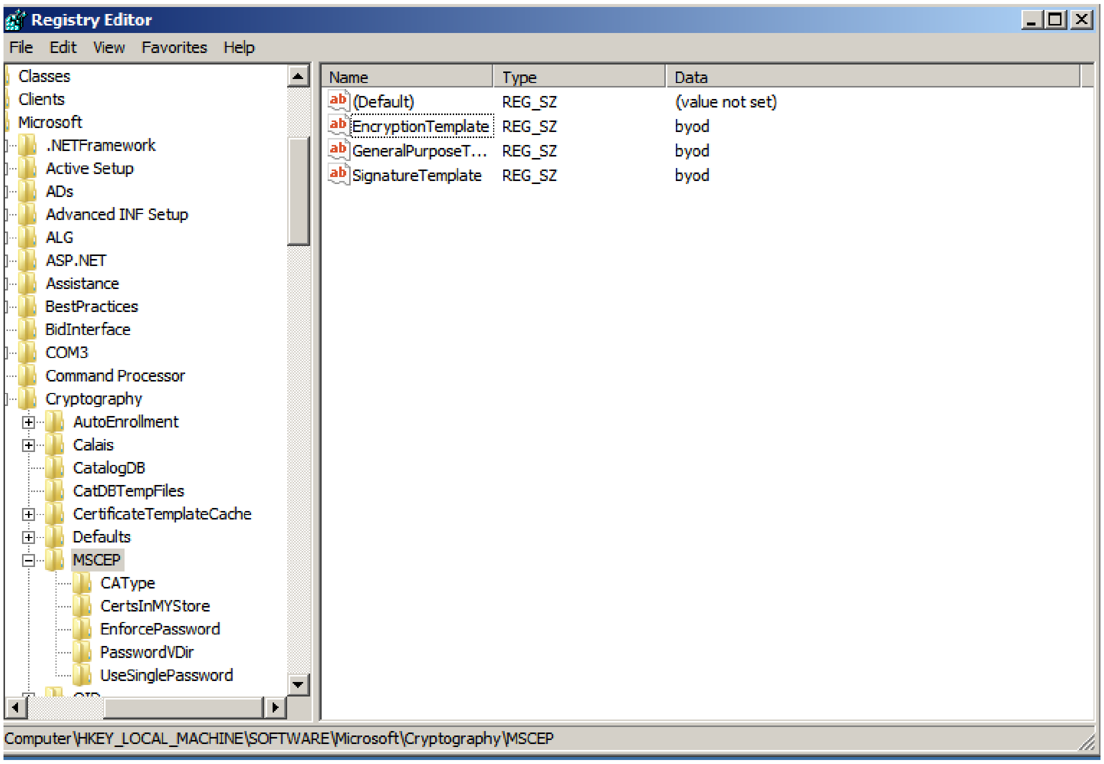
Procedure 2 Modify the Default Certificate that is Issued

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\Cryptrography\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.



Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	byod
GeneralPurposeT…	REG_SZ	byod
SignatureTemplate	REG_SZ	byod

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

Procedure 3 Set the EnforcePassword to zero and disable the “UseSinglePassword” setting:

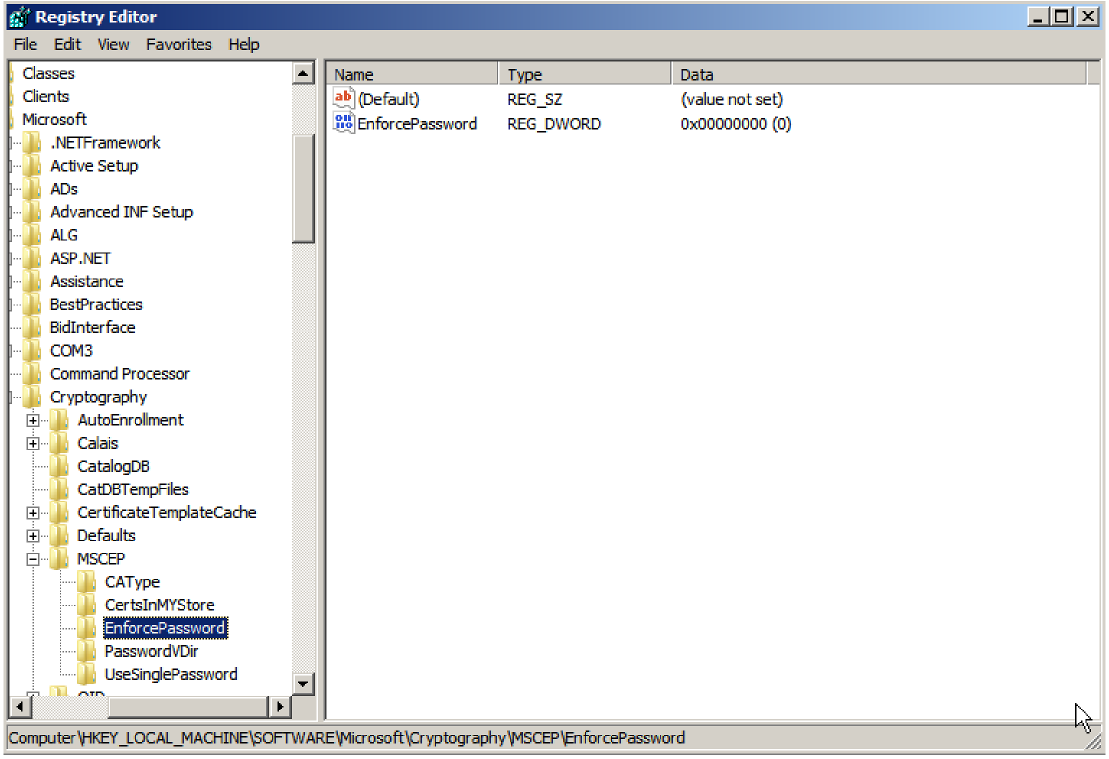
Step 1 Run Regedit

Step 2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptrography\MSCEP\UseSinglePassword.

Step 3 Change the value to 0 UseSinglePassword is set to zero ‘0’.

Step 4 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptrography\MSCEP\ EnforcePassword.

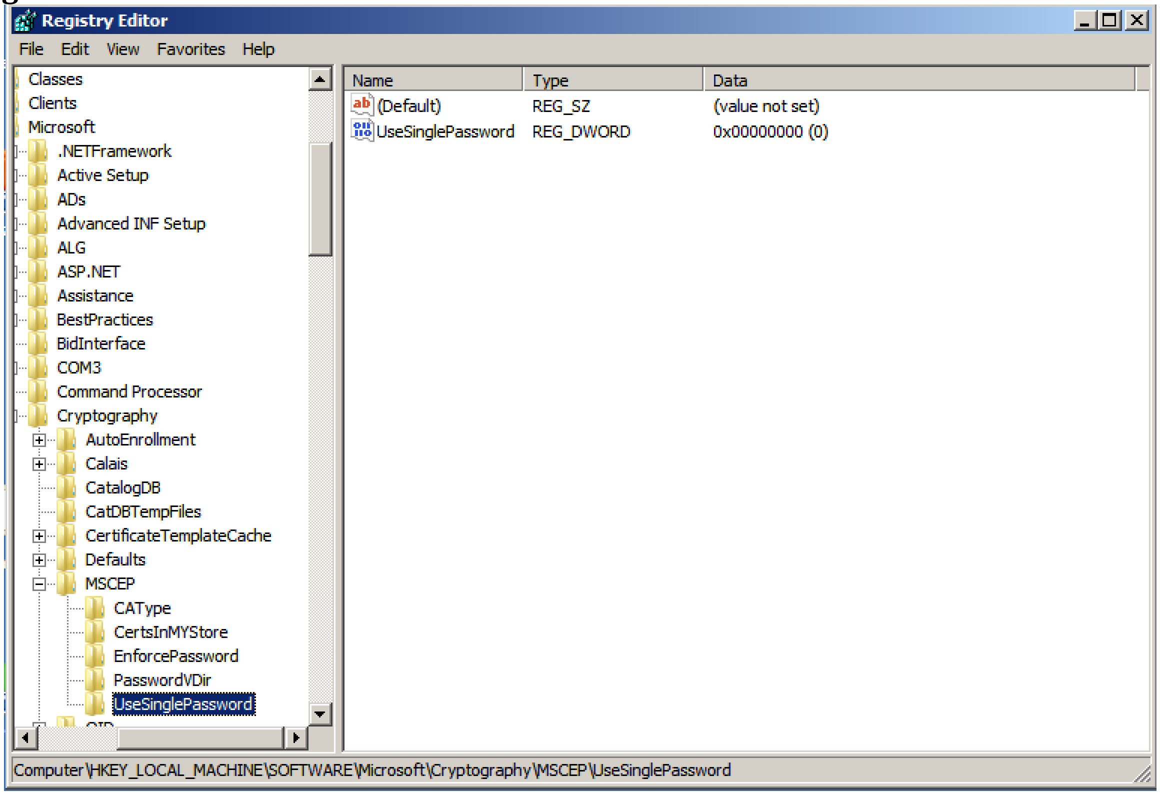
Step 5 Change the value to 0 EnforcePassword is set to zero ‘0’.



Name	Type	Data
(Default)	REG_SZ	(value not set)
EnforcePassword	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

UseSinglePassword:



Name	Type	Data
(Default)	REG_SZ	(value not set)
UseSinglePassword	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\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 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.

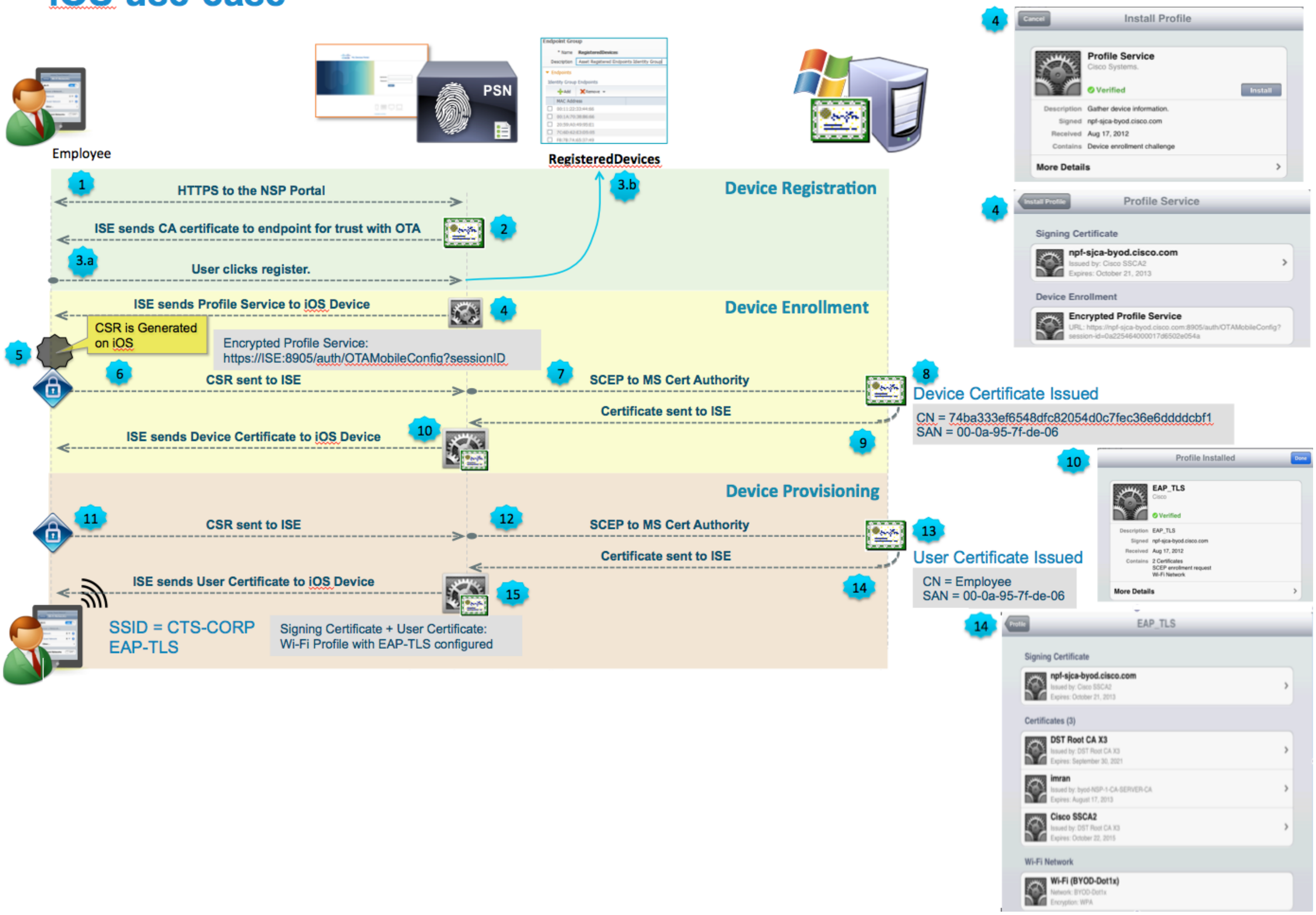
What worked in the testing lab:

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 C: BYOD flows

This section goes through BYOD flows for iOS and Android Devices

iOS use-case



Encrypted Profile Service:
https://ISE:8905/auth/OTAMobileConfig?sessionID

CN = 74ba333ef6548dfc82054d0c7fec36e6ddddcbf1
SAN = 00-0a-95-7f-de-06

CN = Employee
SAN = 00-0a-95-7f-de-06

Signing Certificate + User Certificate:
Wi-Fi Profile with EAP-TLS configured

4 — Install Profile

Profile Service
Cisco Systems.
Verified

Description	Gather device information.
Signed	npf-sjca-byod.cisco.com
Received	Aug 17, 2012
Contains	Device enrollment challenge

More Details

4 — Profile Service

Signing Certificate
npf-sjca-byod.cisco.com
Issued by: Cisco SSCA2
Expires: October 21, 2013

Device Enrollment
Encrypted Profile Service
URL: https://npf-sjca-byod.cisco.com:8905/auth/OTAMobileConfig?session-id=0a225464000017d6502e054a

10 — Profile Installed

EAP_TLS
Cisco
Verified

Description	EAP_TLS
Signed	npf-sjca-byod.cisco.com
Received	Aug 17, 2012
Contains	2 Certificates SCEP enrollment request Wi-Fi Network

More Details

14 — EAP_TLS

Signing Certificate
npf-sjca-byod.cisco.com
Issued by: Cisco SSCA2
Expires: October 21, 2013

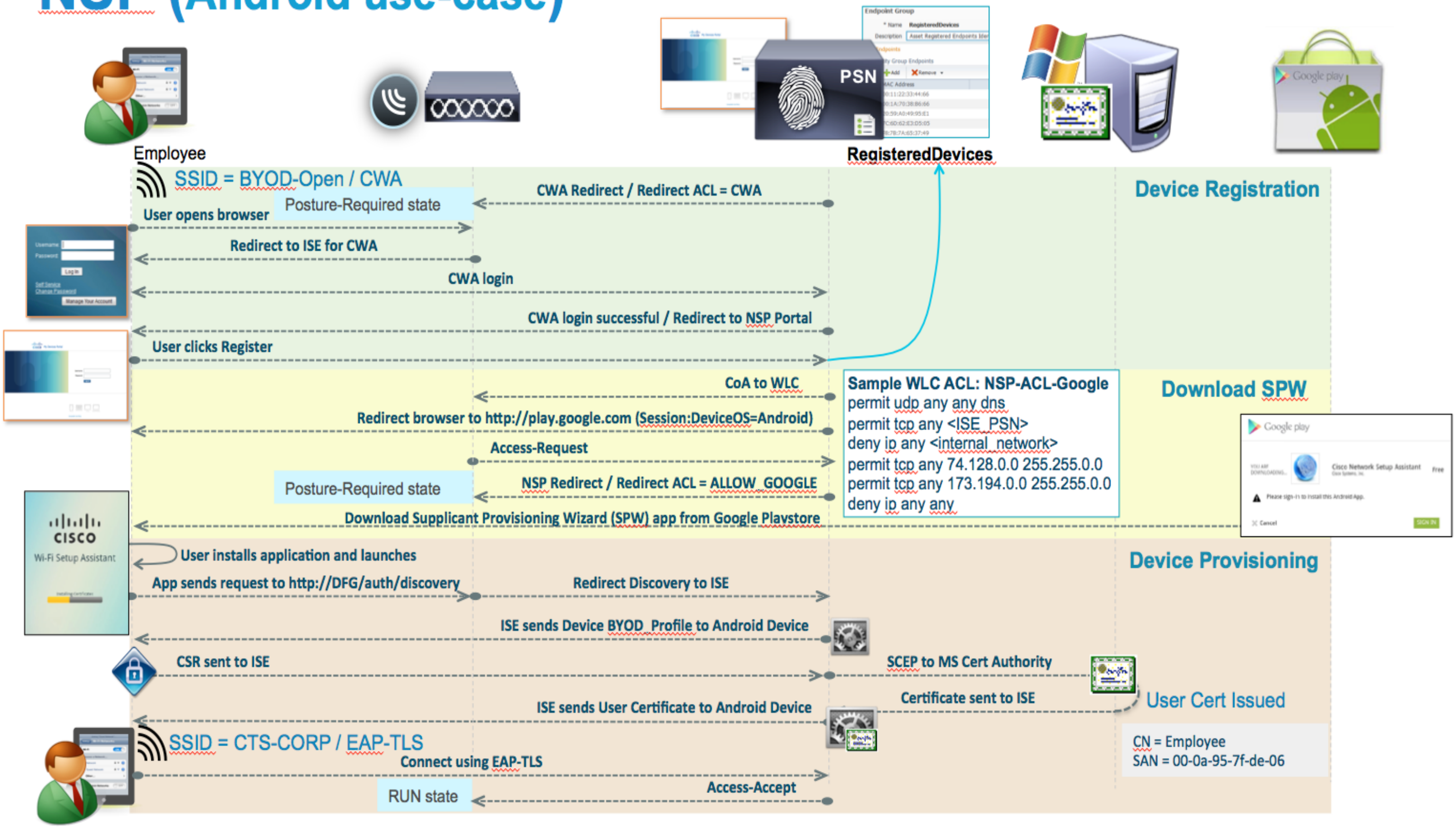
Certificates (3)
DST Root CA X3
Issued by: DST Root CA X3
Expires: September 30, 2021

imran
Issued by: byod-NSP-1-CA-SERVER-CA
Expires: August 17, 2013

Cisco SSCA2
Issued by: DST Root CA X3
Expires: October 22, 2015

Wi-Fi Network
Wi-Fi (BYOD-Dot1x)
Network: BYOD-Dot1x
Encryption: WPA

NSP (Android use-case)



Employee

RegisteredDevices

SSID = BYOD-Open / CWA

Device Registration

User opens browser

Posture-Required state

CWA Redirect / Redirect ACL = CWA

Redirect to ISE for CWA

CWA login

CWA login successful / Redirect to NSP Portal

User clicks Register

Download SPW

CoA to WLC

Redirect browser to http://play.google.com (Session:DeviceOS=Android)

Access-Request

Posture-Required state

NSP Redirect / Redirect ACL = ALLOW_GOOGLE

Download Supplicant Provisioning Wizard (SPW) app from Google Playstore

Sample WLC ACL: NSP-ACL-Google

```
permit udp any any dns
permit tcp any <ISE_PSN>
deny ip any <internal_network>
permit tcp any 74.128.0.0 255.255.0.0
permit tcp any 173.194.0.0 255.255.0.0
deny ip any any
```

Device Provisioning

User installs application and launches

App sends request to http://DFG/auth/discovery

Redirect Discovery to ISE

ISE sends Device BYOD_Profile to Android Device

CSR sent to ISE

SCEP to MS Cert Authority

Certificate sent to ISE

User Cert Issued

ISE sends User Certificate to Android Device

CN = Employee
SAN = 00-0a-95-7f-de-06

SSID = CTS-CORP / EAP-TLS

Connect using EAP-TLS

Access-Accept

RUN state

Appendix D: 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

Device Configuration Guides:

Cisco Identity Services Engine User Guides:
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
- For Cisco Catalyst 3000 series switches: 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
- For Cisco Catalyst 4500 series switches: 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
- For Cisco ASR 1000 series routers: 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