

Table of Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Bootstrapping ISE](#)

[Download and Install ISE](#)

[Provision CA and Server Certificates](#)

[CA Certificate](#)

[ISE Local Server Certificates](#)

[Registering Nodes and Setting up a distributed deployment](#)

[Setting up the primary node](#)

[Joining secondary / PSN nodes](#)

[Adding a Network Device to ISE](#)

[Setting up the Wireless LAN Controller](#)

[Add ISE as a RADIUS Authentication/Accounting Server](#)

[Create the redirect ACL](#)

[Proxy Considerations](#)

[Create the WLANs / SSIDs](#)

[Open SSID \(For Dual SSID BYOD\)](#)

[Secure SSID \(For Dual and Single SSID BYOD\)](#)

[Setting up Identity Sources](#)

[Joining Nodes to Active Directory](#)

[Adding Active Directory Groups](#)

[Certificate Authentication Profile](#)

[Identity Source Sequence](#)

[Guest Portal Setup](#)

[Client Provisioning Setup](#)

[Enable Client Provisioning](#)

[Download Provisioning Resources](#)

[Create Provisioning Profile](#)

[Client Provisioning Rules / Policies](#)

[Simple Certificate Enrolment Protocol \(SCEP\)](#)

[Windows Server Setup](#)

[Configure ISE as a SCEP Proxy](#)

[Authentication and Authorization](#)

[Authentication Rules](#)

[Authorization Profiles](#)

[Authorization Rules](#)

[User Experience](#)

[Dual SSID Employee](#)

[Single SSID Employee](#)

Single and Dual SSID Contractor

Introduction

This document describes how to configure Bring Your Own Device (BYOD) Supplicant Provisioning with Cisco Identity Services Engine (ISE) and a Cisco Wireless Lan Controller (WLC).

This document attempts to include all the necessary steps from Installing ISE to User Experience.

The goal of this configuration is to provide differentiated access between hypothetical Employees and Contractors.

- Employees will authenticate via Central Web Authentication (Dual SSID) or PEAP (Single SSID) and be provisioned with an identity certificate via Simple Certificate Enrollment Protocol (SCEP) for EAP-TLS.
- Contractors will receive immediate network access regardless of their network access method.

We are going to implement a mix of Single SSID BYOD and Dual SSID BYOD.

Dual SSID BYOD	Client enters network via open SSID, authenticates via MAC Address Bypass (MAB) and CWA Guest portal redirects Employees to supplicant provisioning and Guests/Contractors to Internet Access.
Single SSID BYOD	Employee enters network via PEAP on secured SSID and is provisioned for EAP-TLS access on the same SSID. Contractors receive immediate network access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE)
- Wireless Lan Controllers
- Windows Server

Components Used

- ISE 1.1.3 Patch 1
- WLC 7.2+
- Windows Server 2008 SR2

Configure

Bootstrapping ISE

Download and Install ISE

1. Download ISE's installer .iso file.

Download Link:

<http://software.cisco.com/download/release.html?mdfid=283801620&softwareid=283802505>

1. Install ISE on your favourite physical or virtual infrastructure and perform post installation tasks

Relevant Guide:

http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_install_guide.html

Note: ISE installation requires: Network connectivity, DNS server, NTP. Without these installation will break.

1. For our example deployment we will be using ISE 113-1.sec.lab and ISE113-2.sec.lab.

The domain will be sec.lab.

ISE113-1 will be our PAP/PAN (Primary Administration Point / Administration Node) and MNT (Monitoring) Node.

ISE113-2 will be our PSN (Policy Service Node).

10.66.83.1 will be our gateway

10.66.83.88 will be our NTP, DNS, DC/GC (Active Directory)

ISE113-1 (PAP/PAN + MNT)	ISE113-2 (PSN)
hostname ise113-1	hostname ise113-2
!	!
ip domain-name sec.lab	ip domain-name sec.lab
!	!

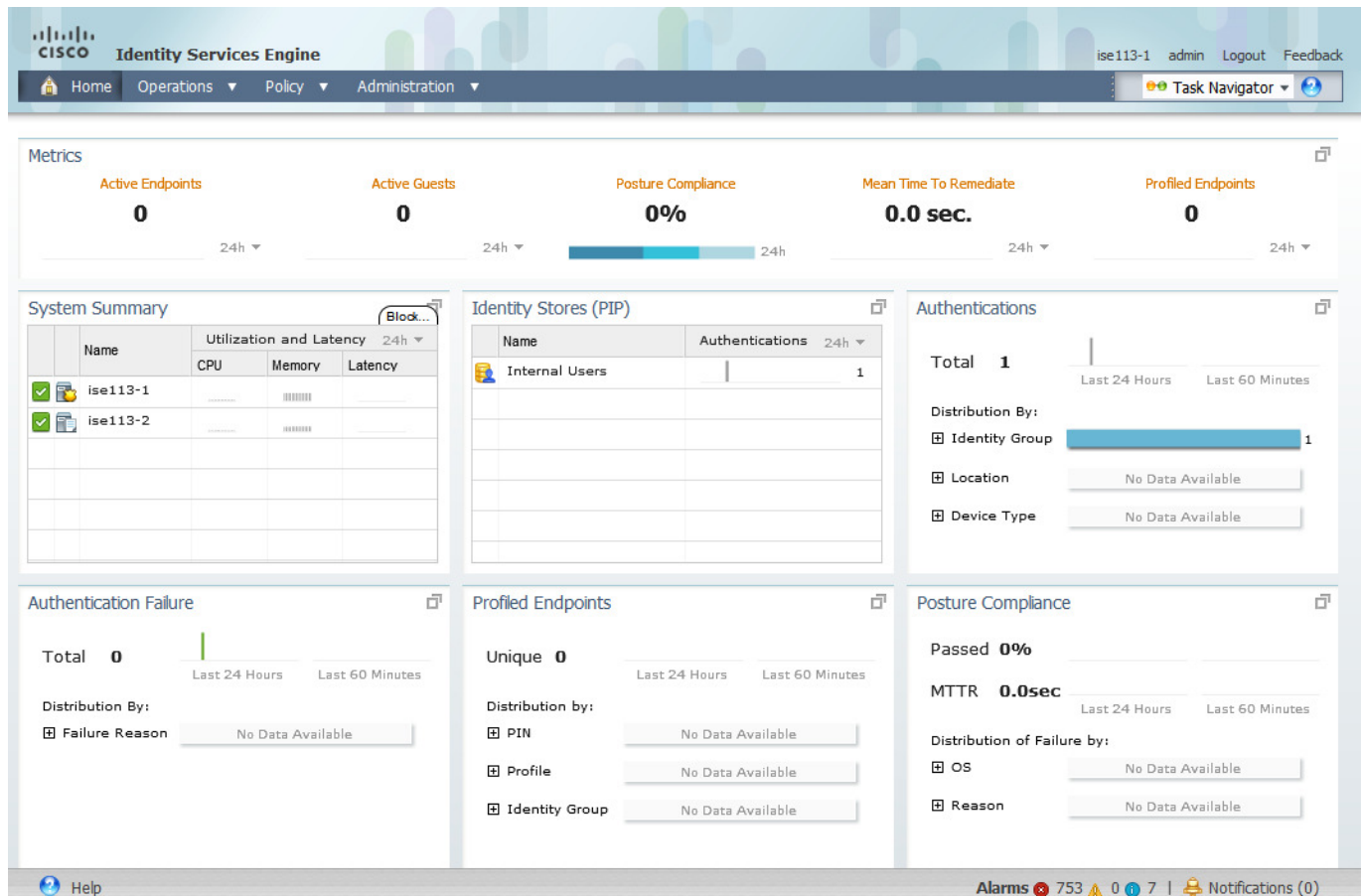
<pre> interface GigabitEthernet 0 ip address 10.66.83.155 255.255.255.0 ipv6 address autoconfig ! ip name-server 10.66.83.88 ! ip default-gateway 10.66.83.1 ! ip route 192.168.0.0 255.255.0.0 gateway 10.66.83.254 ! clock timezone Australia/Sydney ! ntp server 10.66.83.88 ! username admin password hash \$1\$E3/BSI7F\$FPF1Ad18dumzG2pStzjwd. role admin ! service sshd ! repository FTP url ftp://10.137.8.64 user administrator password hash </pre>	<pre> interface GigabitEthernet 0 ip address 10.66.83.156 255.255.255.0 ipv6 address autoconfig ! ip name-server 10.66.83.88 ! ip default-gateway 10.66.83.1 ! ip route 192.168.0.0 255.255.0.0 gateway 10.66.83.254 ! clock timezone Australia/Sydney ! ntp server 10.66.83.88 ! username admin password hash \$1\$t72wHUqd\$cmVOlbBGQr/qAgcxfceu. role admin ! service sshd ! repository FTP url ftp://10.137.8.64 user administrator password hash </pre>
---	--

cc14bc179d2708cc31cbc21ee6a679cd22c095ae	cc14bc179d2708cc31cbc21ee6a679cd22c095ae
!	!
password-policy	password-policy
lower-case-required	lower-case-required
upper-case-required	upper-case-required
digit-required	digit-required
no-username	no-username
disable-cisco-passwords	disable-cisco-passwords
min-password-length 6	min-password-length 6
password-lock-enabled	password-lock-enabled
password-lock-retry-count 5	password-lock-retry-count 5
!	!
logging localhost	logging localhost
logging loglevel 6	logging loglevel 6
!	!
cdp timer 60	cdp timer 60
cdp holdtime 180	cdp holdtime 180
cdp run GigabitEthernet 0	cdp run GigabitEthernet 0
!	!
icmp echo on	icmp echo on
!	!

1. Let's login with the credentials we defined during the post-installation setup.



1. We are greeted by the ISE dashboard.



Provisioning CA and Server Certificates

Provision both ISE nodes with the CA root certificate and their own individual server certificates (generated by certificate signing requests).

Relevant documentation:

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_man_cert.html

CA Certificate

1. First, download the Root CA Certificate from your Certificate Authority

http://<ca>/certsrv/

Click “Download a CA certificate, certificate chain, or CRL”

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

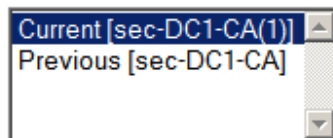
1. Click “Download CA Certificate”

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and en

CA certificate:



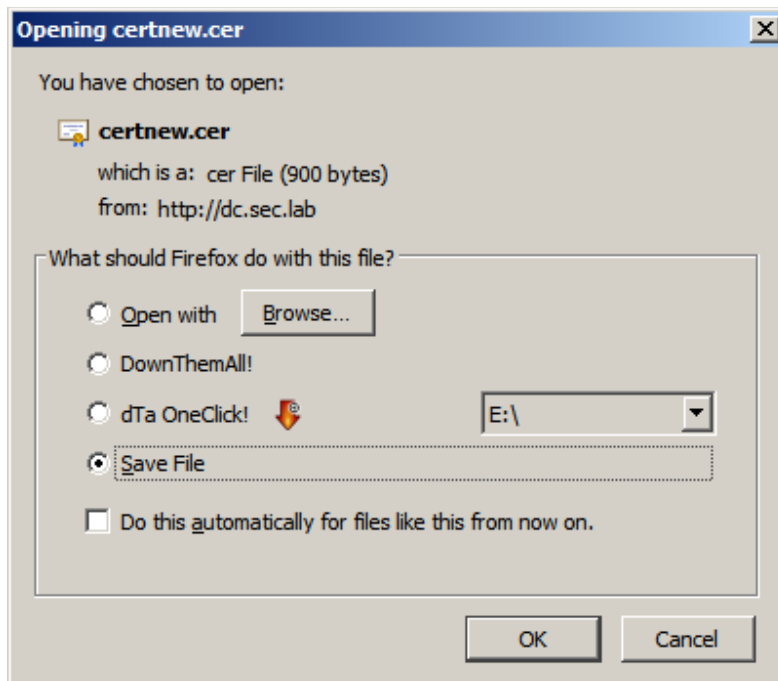
Encoding method:

- DER
- Base 64

[Install CA certificate](#)

[Download CA certificate](#)

1. Save it to a location on your file system.



1. On ISE go to Administration > System > Certificates > Certificate Store. Click "Import"

2. Click Browse and locate the root CA Certificate.
3. Tick "Trust for Client Authentication". If you don't you may see failures with "12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain" when using EAP-TLS
4. Click "Submit".

Certificate Store > Import

Import a new Certificate into the Certificate Store

* Certificate File

Friendly Name

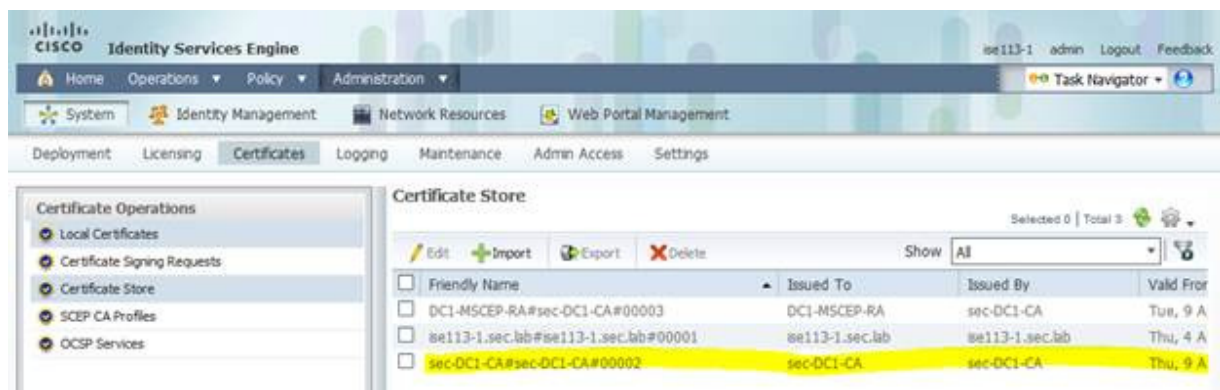
All Trust Certificates are available for selection as the Root CA for secure LDAP connection enabled for EAP-TLS and administrative authentication below:

Trust for client authentication

Enable Validation of Certificate Extensions (accept only valid certificate)

Description

1. The CA Certificate will appear alongside the original self-signed certificate generated by ISE.



1. Repeat these steps on all nodes that will be in the deployment.

ISE Local Server Certificates

1. On each node go to Administration > System > Certificates > Local Certificates
2. Click Add > Generate Certificate Signing Request

3. Fill in the CN with the ISE nodes FQDN and any other relevant fields. Click "Submit"

Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

Certificate

* Certificate Subject

* Key Length ▼

* Digest to Sign With ▼

1. Go to Administration > System > Certificates > Certificate Signing Requests >
2. Tick the request and click export.

Certificate Operations

- Local Certificates
- Certificate Signing Requests**
- Certificate Store
- SCEP CA Profiles
- OCSP Services

Certificate Signing Requests

Show

<input type="checkbox"/>	Friendly Name	Certificate Subject
<input checked="" type="checkbox"/>	ise113-1	CN=ise113-1

Opening ise1131.pem

You have chosen to open:

ise1131.pem
which is a: Compressed (zipped) Folder
from: https://ise113-1.sec.lab

What should Firefox do with this file?

Open with

DownThemAll!

dTa OneClick! ▼

Save File

Do this automatically for files like this from now on.

1. Save the request onto your computer and open it in notepad.
2. On your Microsoft CA Server (<http://dc.sec.lab/certsrv/>) go to Request Certificate > advanced certificate request >
3. Paste the contents of the CSR into the request field and select “Web Server” as the template.

Microsoft Active Directory Certificate Services -- sec-DC1-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or generated by an external source (such as a Web server) in the Saved R

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
3aZtVWXiLsvXasBGj3m7p2a2kxUy2dmKmc0is081l
9Q6sqM0ge6CqNJVLbB1AFmZI8bkMfg7ZvPx8ELss:
BCtPWeNhpA51DkGIVyAPtZRn9sOswSIUFquHAZPL
hkZBdcvKX4wn8rpgETywfohw3dDqn3EwdNA51UEx!
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

1. Click Submit
2. Download the DER encoded certificate. Click “Download Certificate”
3. On ISE go to go to Administration > System > Certificates > Local Certificates
4. Click “Add” > “Bind CA Certificate”
5. Select the certificate from your computer. Tick “EAP” and “Management Interface” and click “Submit”

Local Certificates > Bind CA Signed Certificate

Bind CA Signed Certificate

Certificate

* Certificate File

Friendly Name

Enable Validation of Certificate Extensions (accept only valid certificate)

Protocol

EAP: Use certificate for EAP protocols that use SSL/TLS tunneling

Management Interface: Use certificate to authenticate the web server (GUI)

Override Policy

Replace Certificate A certificate being imported may be determined to already exist in the system with the same Subject or Issuer and serial number as an existing certificate. In such a case, the "Replace Certificate" option will allow the certificate contents to be replaced while maintaining existing protocol selections for the certificate.

1. ISE will need to reload to complete the certificate installation.
2. Perform this task on all nodes in the deployment before joining them together.

Registering Nodes and Setting up a Distributed Deployment

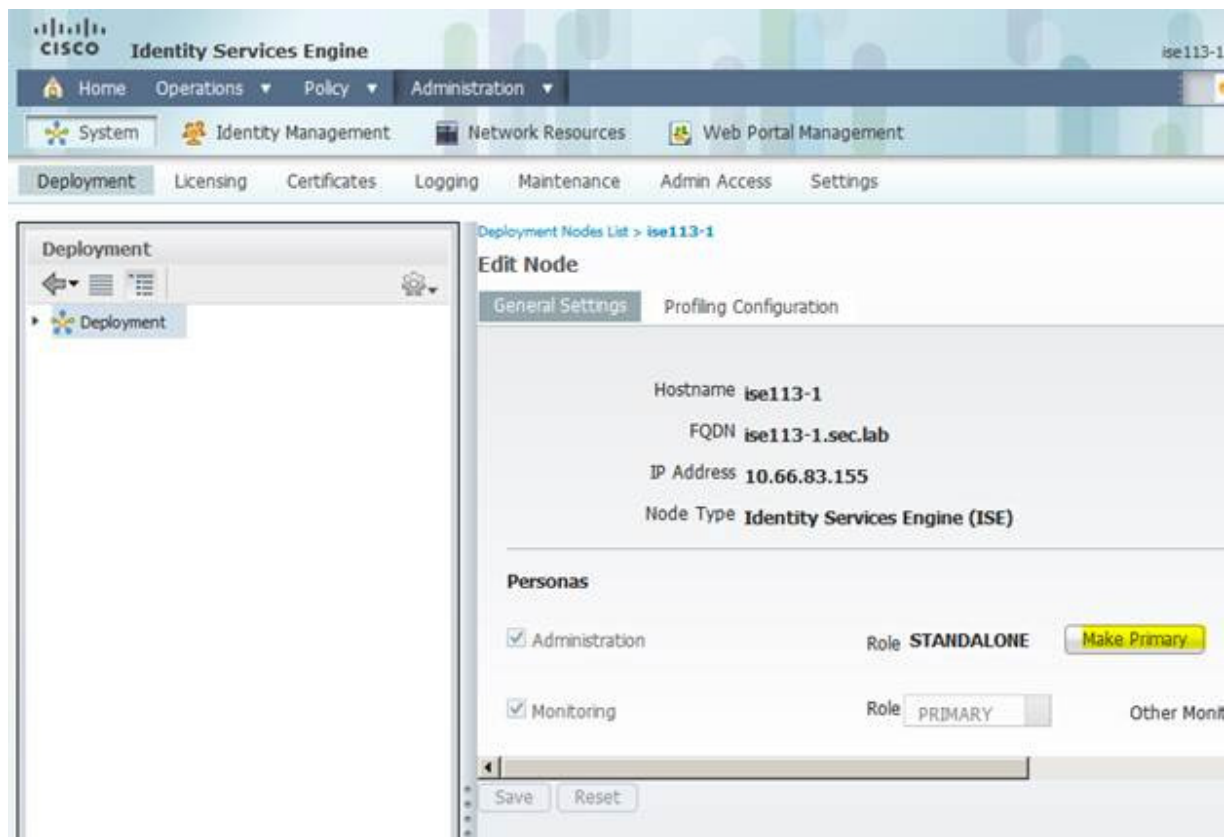
Now we will register our policy node (PSN) to our primary administration/monitoring (PAP/PAN/MNT) node.

Relevant documentation:

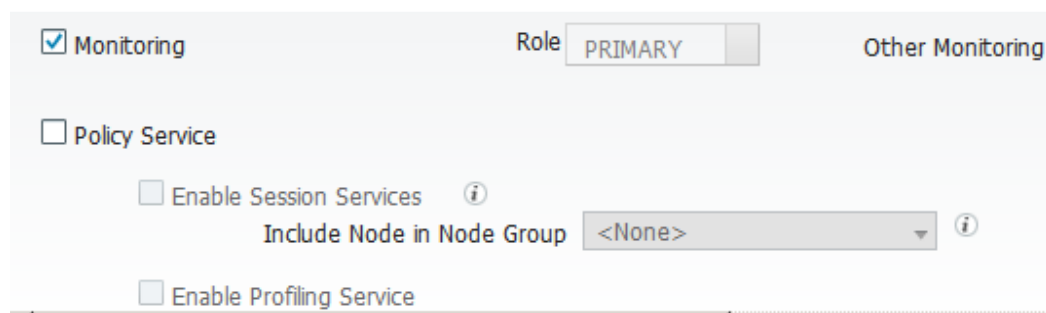
http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_dis_deploy.html

Setting up the primary node

1. Go to Administration > System > Deployment and click on the current node to edit it.
2. Click the "Make Primary" button.



1. Since this will be our Administration and Monitoring node, we should untick Policy Service.



1. Click "Save". The node will be restarted.

Joining secondary / PSN nodes

1. On the PAP go to Administration > System > Deployment and click "Register > An ISE node"

2. Enter the FQDN/IP and credentials of the new node.

Deployment Nodes List > Specify Hostname

Register Inline Posture Node - Step 1: Specify Node Hostname or IP Address and Credentials

* Hostname or IP Address

* User Name

* Password

1. Since this will be a Policy Service Node (PSN) we will untick Administration and Monitoring and leave Policy Service Ticked.

Node Type **Identity Services Engine (ISE)**

Personas

Administration Role

Monitoring Role Other Monitor

Policy Service

Enable Session Services ⓘ
Include Node in Node Group ⓘ

Enable Profiling Service

1. Click "Submit".
2. Synchronisation will occur and the PSN node will be restarted. When finished the Replication Status will be COMPLETE and the Sync Status will be SYNC COMPLETED.

Deployment Nodes

Edit Register Export Import Show All

<input type="checkbox"/>	Hostname	Node Type	Personas
<input type="checkbox"/>	ise113-1	ISE	Administration, Monitoring
<input type="checkbox"/>	ise113-2	ISE	Policy Service

Adding a Network Device to ISE

We will need to add our Wireless Lan Controller (WLC) or switch as a Network Device in ISE so that ISE trusts RADIUS traffic coming from it.

1. Go to Administration > Network Resources > Network Devices
2. Click the 'Add' button.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The navigation menu includes Home, Operations, Policy, and Administration. Under Administration, the 'Network Resources' tab is selected, showing 'Network Devices', 'Network Device Groups', 'External RADIUS Servers', and 'RADIUS Server Sequences'. The 'Network Devices' page is displayed, featuring a search bar, a left sidebar with a tree view containing 'Network Devices' and 'Default Device', and a main content area. The main content area has a toolbar with 'Edit', 'Add' (highlighted in yellow), 'Duplicate', 'Import', and 'Export' buttons. Below the toolbar is a table with columns for Name, IP/Mask, and Location. One device is listed: 'WLC' with IP/Mask '192.168.63.1...' and Location 'Security Area'.

1. Fill out the Network Devices page with the required information. Select authentication and define a RADIUS shared secret.

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Location

Device Type



Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL



SNMP Settings



Advanced TrustSec Settings

1. Click save and you're done.

Configuring the Wireless LAN Controller

We need to add the PSN as a RADIUS Authentication and Accounting Server, Create an unsecure SSID (for Central Web Authentication) and a Secure SSID (for EAP-TLS and PEAP) and define a redirection ACL.

Relevant Guides:

Central Web Authentication on the WLC and ISE Configuration Example

http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080bead09.shtml

Central Web Authentication with a Switch and Identity Services Engine Configuration Example

http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080ba6514.shtml

Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions

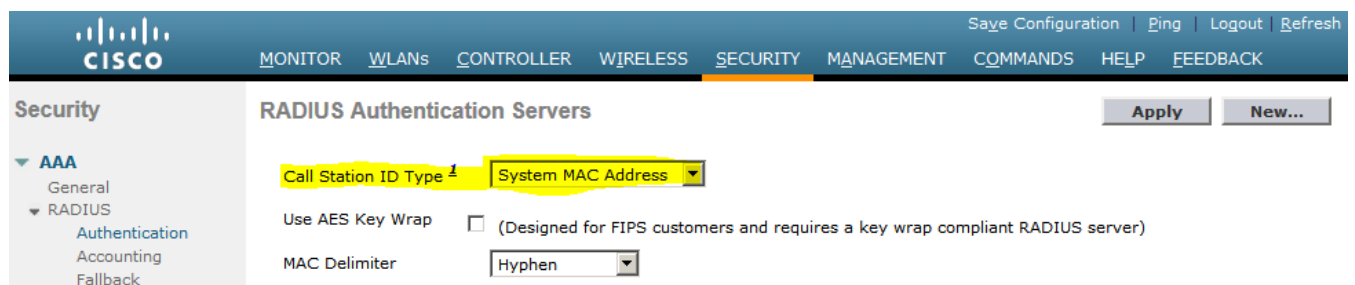
http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_sw_cnfg.html

Cisco TrustSec How -To Guide: Central Web Authentication

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_40webauthenticat...

Add ISE as a RADIUS Authentication/Accounting Server

1. Go to Security > AAA > RADIUS > Authentication
2. Set the Calling Station ID Type as "System MAC Address"



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the right of the navigation bar are links for Save Configuration, Ping, Logout, and Refresh. The left sidebar shows the Security menu with AAA expanded to RADIUS, and Authentication selected. The main content area is titled "RADIUS Authentication Servers" and contains the following configuration options:

- Call Station ID Type: System MAC Address (highlighted in yellow)
- Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- MAC Delimiter: Hyphen

Buttons for "Apply" and "New..." are visible in the top right corner of the configuration area.

1. Click the 'New' button.
2. Enter the IP address of the PSN node, RADIUS shared secret (configured on ISE) and leave the other options as default.

RADIUS Authentication Servers > New

< Back

Apply

Server Index (Priority)

Server IP Address

Shared Secret Format

Shared Secret

Confirm Shared Secret

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number

Server Status

Support for RFC 3576

Server Timeout seconds

Network User Enable

Management Enable

IPSec Enable

Note: Support for RFC 3576 enables CoA, which is required to send redirect URLs and new Authz profiles.

1. Click Apply. The RADIUS Authentication Server will appear in the list:

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input type="checkbox"/>	<input type="checkbox"/>	1	10.66.83.85	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.66.83.183	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	3	10.66.83.53	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	4	10.66.83.182	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	5	10.66.83.57	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	6	10.66.83.54	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	7	10.66.83.93	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8	10.66.83.156	1812	Disabled	Enabled

1. Perform the same steps to add ISE as an accounting server under Security > AAA > RADIUS > Accounting.

RADIUS Accounting Servers

App

MAC Delimiter

Network User	Server Index	Server Address	Port	IPSec	Admin Status	
<input type="checkbox"/>	1	10.66.83.85	1813	Disabled	Enabled	<input type="checkbox"/>
<input type="checkbox"/>	2	10.66.83.183	1813	Disabled	Enabled	<input type="checkbox"/>
<input type="checkbox"/>	3	10.66.83.53	1813	Disabled	Enabled	<input type="checkbox"/>
<input type="checkbox"/>	4	10.66.83.182	1813	Disabled	Enabled	<input type="checkbox"/>
<input type="checkbox"/>	5	10.66.83.54	1813	Disabled	Enabled	<input type="checkbox"/>
<input type="checkbox"/>	6	10.66.83.93	1813	Disabled	Enabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	7	10.66.83.156	1813	Disabled	Enabled	<input type="checkbox"/>

Creating the redirect ACL

When we perform URL redirection on a WLC we need to define a redirection ACL. This ACL will identify traffic which should NOT be processed for redirection by PERMITTING it. Traffic which should be redirected will be identified via an explicit or implicit DENY.

When we perform a redirection on a switch a similar ACL will be used, however, the syntax is the opposite. On a switch we identify traffic we DO wish to redirect using a PERMIT and traffic we do NOT want to redirect using a DENY.

1. On the WLC go to Security > Access Control Lists > Access Control Lists
2. Click 'New' and give the ACL a name. For example, ACL-NSP-REDIRECT. Select IPv4.

Access Control Lists > New

Access Control List
Name

ACL Type

IPv4 IPv6

1. Click 'Add New Rule'.

This ACL is referenced in the access-accept from the ISE and defines what traffic should be redirected (denied by the ACL) and what traffic should not be redirected (permitted by the ACL). Basically, DNS and traffic to/from the ISE needs to be permitted.

General

Access List Name ACL-NSP-REDIRECT

Deny Counters 3912

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.66.83.156 / 255.255.255.255	Any	Any	Any	Any
2	Permit	10.66.83.156 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	10.66.83.88 / 255.255.255.255	UDP	Any	DNS	Any
4	Permit	10.66.83.88 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0/ 0.0.0.0	10.66.83.156/255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.66.83.156/255.255.255.255	0.0.0.0/ 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0/ 0.0.0.0	10.66.83.88/255.255.255.255	UDP	Any	DNS	Any	Any
4	Permit	10.66.83.88/255.255.255.255	0.0.0.0/ 0.0.0.0	UDP	DNS	Any	Any	Any

Note: An explicit deny any any exists at the end. All traffic not permitted will be marked for redirection.

As an example of Switch redirect ACL:

```
ip access-list extended ACL-NSP-REDIRECT
remark explicitly deny DNS from being redirected
Deny udp any host <dns ip> eq 53
remark explicitly deny traffic to ISE from being redirected
deny ip any host <ise PSN IP>
remark define which traffic should trigger a redirect
permit tcp any any eq www
permit tcp any any eq 443
permit tcp any any eq 8443
remark implicit deny will stop all other traffic from being redirected on.
```

See the following for more information:

Switch Configuration Required To Support ISE Functions

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_sw_cnfg.html

Central Web Authentication with a Switch and Identity Services Engine Configuration Example

http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080ba6514.shtml

Proxy Considerations

NOTE: By default Cisco switches and WLCs only process packets marked for redirection which have a destination port of 80 or 443. If we are going to use a proxy on our Web Browser then

we need to explicitly allow traffic to ISE without proxying. All modern browsers support this function.

If the proxy uses a non-standard port, then we will need to configure our WLC and Switch to support this:

On Wireless Lan Controllers:

(Cisco Controller) >config network web-auth port ?

<port> Configures additional ports for web-auth redirection.

On Cisco Switches:

ip http port 8080

ip port-map http port 8080

Where '8080' is any port the customer is using for their proxy.

Create the WLANs / SSIDs

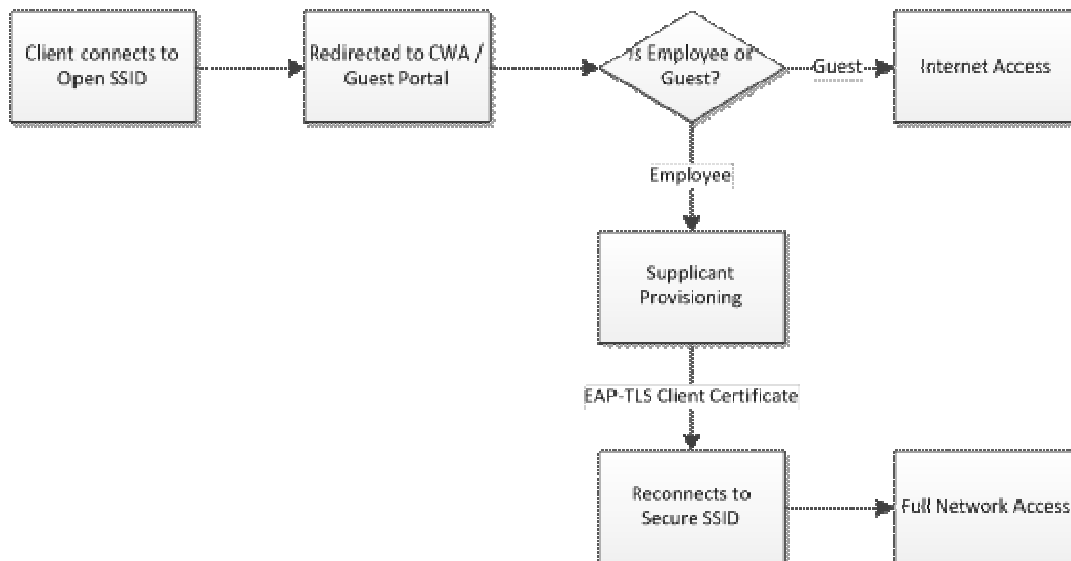
We will need two SSIDs since we are going to perform a combination of Single and Dual SSID BYOD.

Dual SSID BYOD	Client enters network via open SSID and is redirected to CWA. Guest portal redirects Employees to supplicant provisioning and Guests to Internet Access.
Single SSID BYOD	Employee enters network via PEAP-MSCHAPv2 on secured SSID and is provisioned for EAP-TLS access on the same SSID. Guest cannot access this SSID.

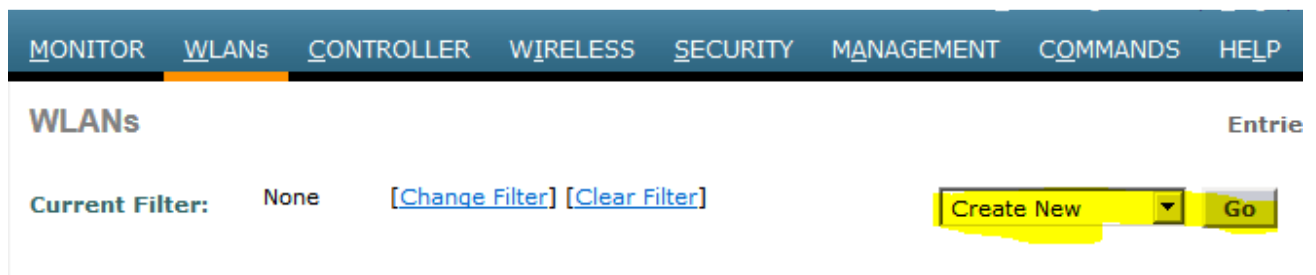
The open SSID, called Onboarding, will redirect employees to supplicant provisioning and guests to internet access.

The closed SSID, called Corporate, will redirect employees to supplication provisioning if they authenticate via PEAP and allow full access if they authenticate via EAP-TLS.

Open SSID (For Dual SSID BYOD)



1. On the WLC go to WLANs. Select 'Create New' and click 'Go'.



1. Fill in the Profile name and SSID with an appropriate name and click 'Apply'. E.g. Guest, Onboarding, CWA.

WLANs > New

[< Back](#) [Apply](#)

Type	<input type="text" value="WLAN"/>
Profile Name	<input type="text" value="Onboarding"/>
SSID	<input type="text" value="Onboarding"/>
ID	<input type="text" value="11"/>

1. On the General Page tick 'Status Enabled' and 'Broadcast SSID Enabled'. Configure an Interface Group.

The screenshot shows the 'Security' tab of a WLAN configuration page. The 'General' tab is also visible. The configuration includes:

Profile Name	Onboarding
Type	WLAN
SSID	Onboarding
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	MAC Filtering (Modifications done under security tab)
Radio Policy	All
Interface/Interface Group(G)	364
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

1. Under Security > Layer 2 select:

Layer 2 Security None

MAC Filtering Ticked – This will enable MAB/Call-Check based authentication.

WLANs > Edit 'Onboarding'

The screenshot shows the 'Layer 2' sub-tab of the 'Security' tab. The configuration includes:

Layer 2 Security	None
MAC Filtering	<input checked="" type="checkbox"/>
Fast Transition	<input type="checkbox"/>

1. Under Security > AAA Servers

Configure the ISE PSN as the radius and accounting server.

Tick 'Interim Update'

Set RADIUS as the first authentication source used.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.1.100.5, Port:1812	<input checked="" type="checkbox"/> Enabled IP:10.1.100.5, Port:1813
Server 2	None	None
Server 3	None	None

Radius Server Accounting

Interim Update Interim Interval 600

Authentication priority order for web-auth user

Not Used

Order Used For Authentication

RADIUS LOCAL

Up

1. Under Advanced

Enable 'AAA Override'

Set the NAC State as 'Radius NAC'

Enable 'DHCP Profiling'

General **Security** **QoS** **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

P2P Blocking Action

Client Exclusion Enabled 60
Timeout Value (secs)

Maximum

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

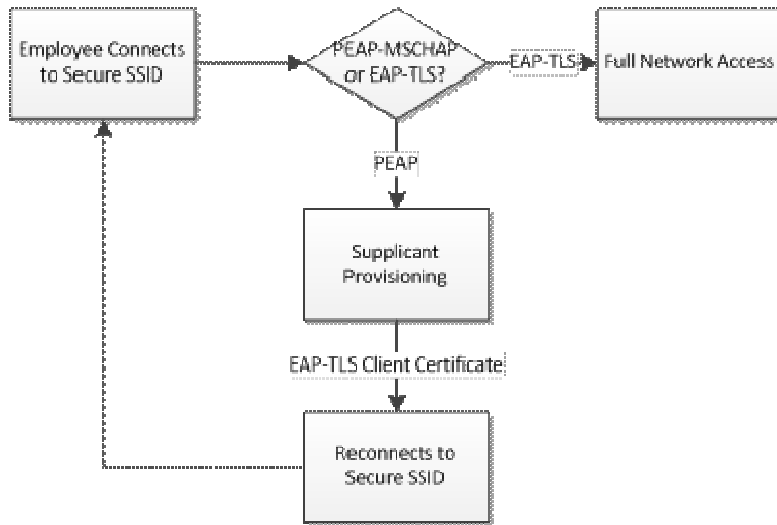
NAC State

Client Profiling

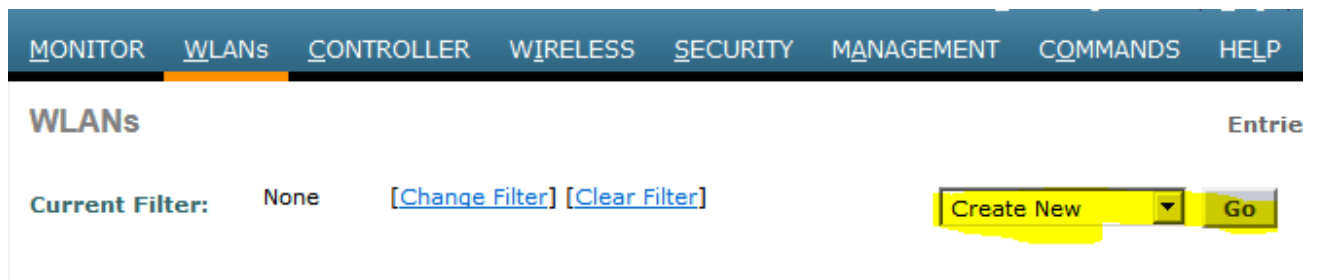
DHCP Profiling Enabled

1. Click the 'Apply' button.

Secure SSID (For Dual and Single SSID BYOD)



1. On the WLC go to WLANs. Select 'Create New' and click 'Go'.



1. Fill in the Profile name and SSID with an appropriate name and click 'Apply'. E.g. Corporate, Secure.

WLANs > New [< Back](#) [Apply](#)

Type	<input type="text" value="WLAN"/>
Profile Name	<input type="text" value="Onboarding"/>
SSID	<input type="text" value="Onboarding"/>
ID	<input type="text" value="11"/>

1. On the General Page tick 'Status Enabled' and 'Broadcast SSID Enabled'. Configure an Interface Group.

General	Security	QoS	Advanced
Profile Name	Corporate		
Type	WLAN		
SSID	Corporate		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under secur		
Radio Policy	All		
Interface/Interface Group(G)	364		
Multicast Vlan Feature	<input type="checkbox"/> Enabled		
Broadcast SSID	<input checked="" type="checkbox"/> Enabled		

1. Under Security > Layer 2 select:

Layer 2 Security WPA+WPA2

WPA2 Policy Ticked

WPA2 Encryption AES

Key Management > 802.1X Enable

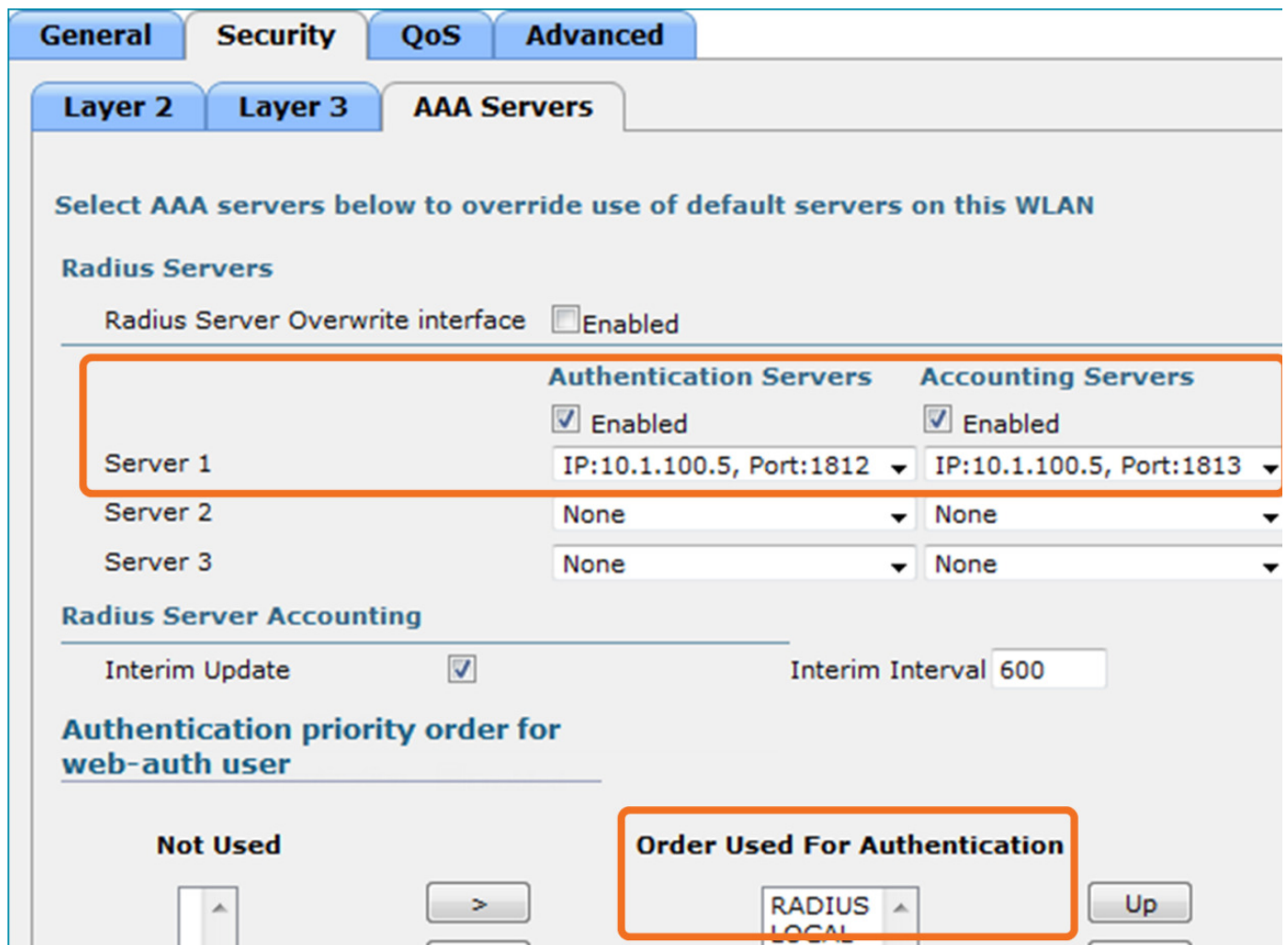
The screenshot shows the configuration page for AAA Servers, specifically the Layer 2 Security section. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'MAC Filtering' checkbox is unchecked. Under the 'Fast Transition' section, the 'Fast Transition' checkbox is unchecked. In the 'WPA+WPA2 Parameters' section, 'WPA Policy' is unchecked, 'WPA2 Policy' is checked, 'WPA2 Encryption' is checked with 'AES' selected, and 'TKIP' is unchecked. In the 'Authentication Key Management' section, '802.1X' is checked with 'Enable' selected.

1. Under Security > AAA Servers

Configure the ISE PSN as the radius and accounting server.

Tick 'Interim Update'

Set RADIUS as the first authentication source used.



1. Under Advanced

Enable 'AAA Override'

Set the NAC State as 'Radius NAC'

Enable 'DHCP Profiling'

General Security QoS **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

P2P Blocking Action

Client Exclusion Enabled 60
Timeout Value (secs)

Maximum

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Client Profiling

DHCP Profiling Enabled

As far as the WLC is concerned, we're done. Users authenticating on the Open SSID 'Onboarding' will generate a MAB based authentication to ISE. Users authenticating on the Secure SSID 'Corporate' will generate a 802.1x RADIUS PEAP/EAP-TLS authentication to ISE.

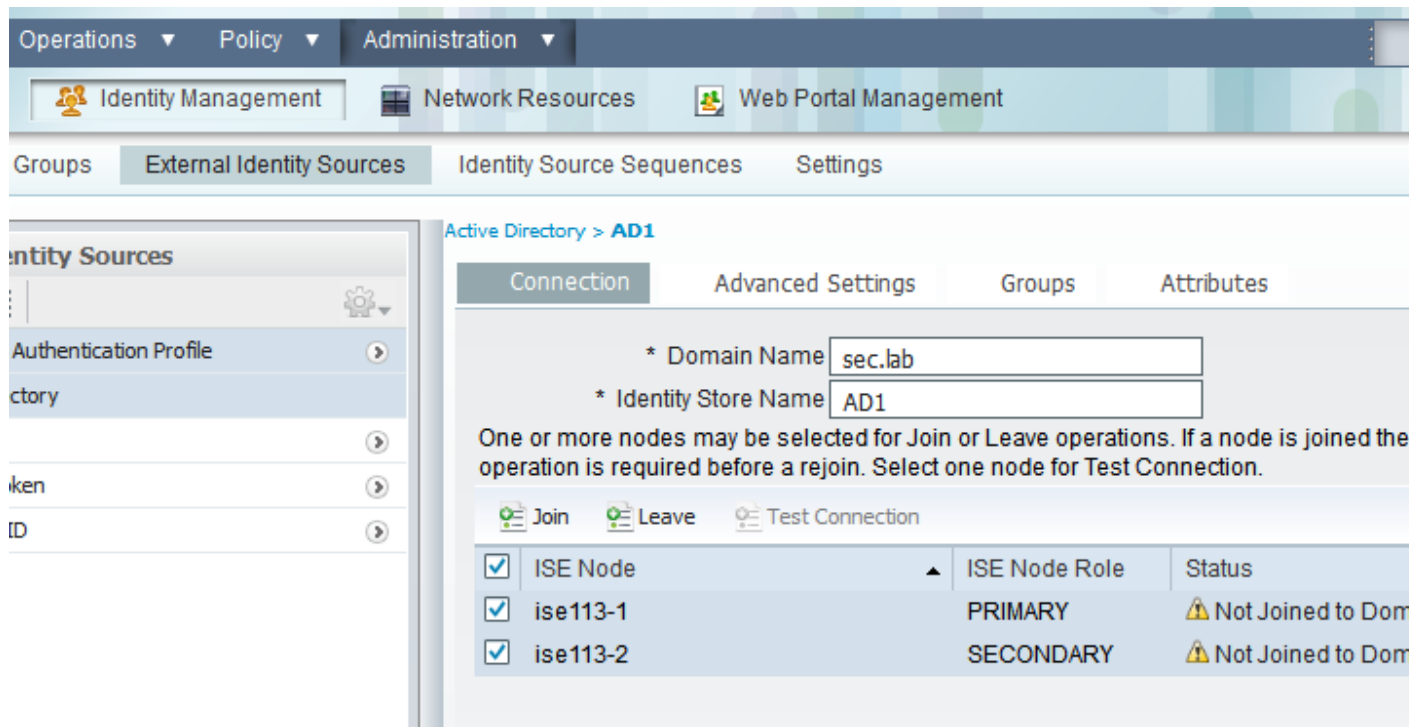
Configuring Identity Sources

Joining Nodes to Active Directory

Managing External Identity Stores

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_man_id_stores.html

1. Go to Administration > Identity Management > External Identity Sources > Active Directory
2. Tick all the relevant nodes.

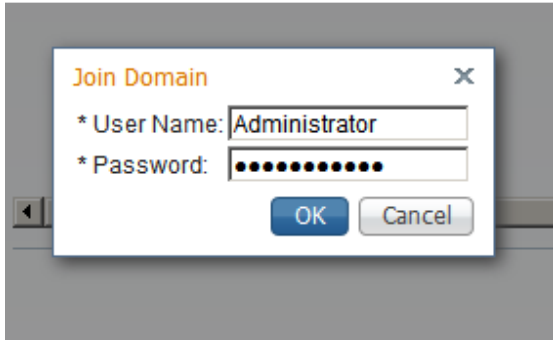


1. Click the Join button and type in the credentials to join the domain.

Note: The Active Directory account required for domain access in ISE should have either of these:

- 'Add workstations to domain' user right in corresponding domain.
- 'Create Computer Objects' or 'Delete Computer Objects' permission on corresponding computers container where ISEs machine's account is created before joining ACS machine to the domain.

By Default AD Domain Admins, Administrators and Account Operators can add/delete computers to the domain



1. The join should complete successfully.

Join Operation Status



The list below shows the status of the requested operation for each node.

Status: Successful

ISE Node	Status
ise113-1	✓ Completed.
ise113-2	✓ Completed.

1. The nodes will display which domain controller they have joined to.

Active Directory > AD1

Connection Advanced Settings Groups Attributes

* Domain Name

* Identity Store Name

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

Join
 Leave
 Test Connection

<input checked="" type="checkbox"/>	ISE Node	ISE Node Role	Status
<input checked="" type="checkbox"/>	ise113-1	PRIMARY	✓ Connected to: dc1.sec.lab
<input checked="" type="checkbox"/>	ise113-2	SECONDARY	✓ Connected to: dc1.sec.lab

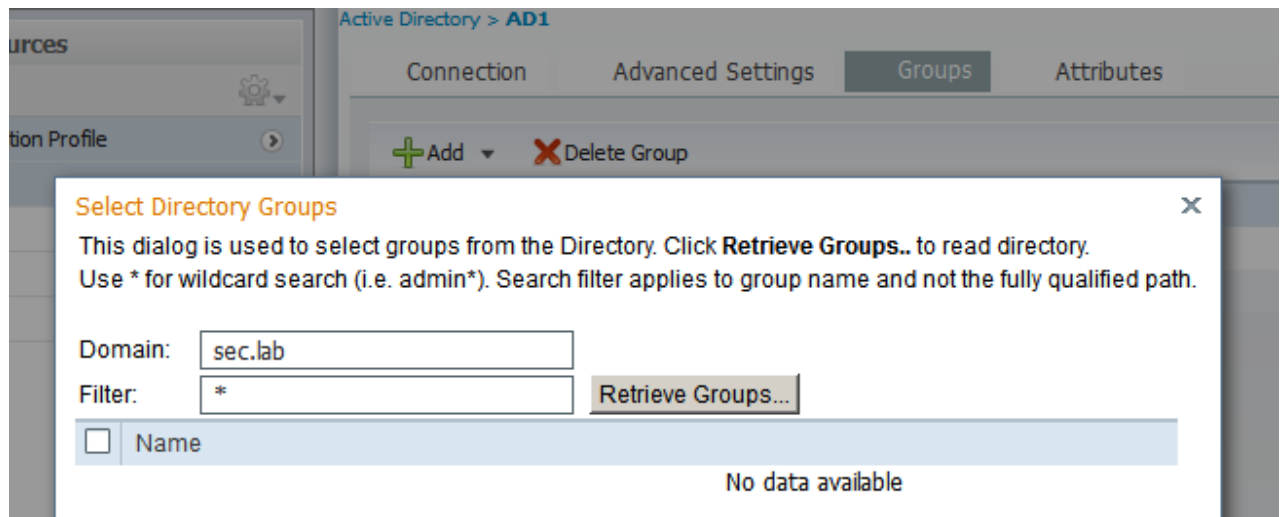
Adding Active Directory Groups

We are going to use two Active Directory groups for our example configuration.

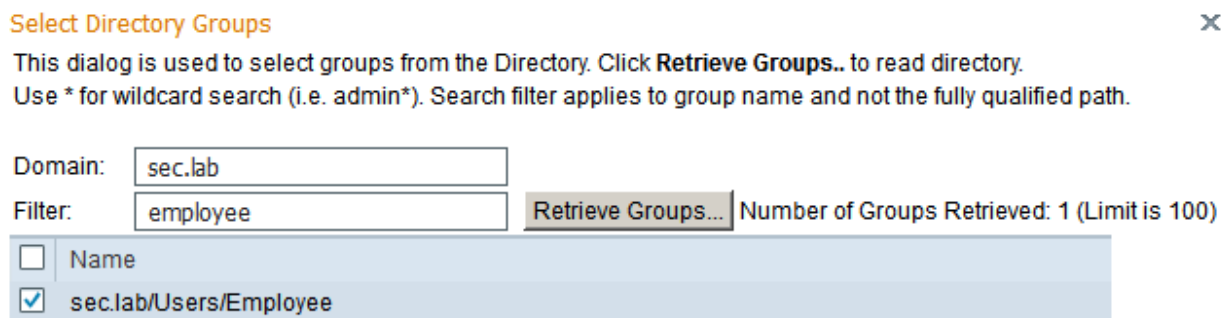
Contractors will not undergo provisioning and will be provided network access.

Employees will undergo provisioning before being provided with network access.

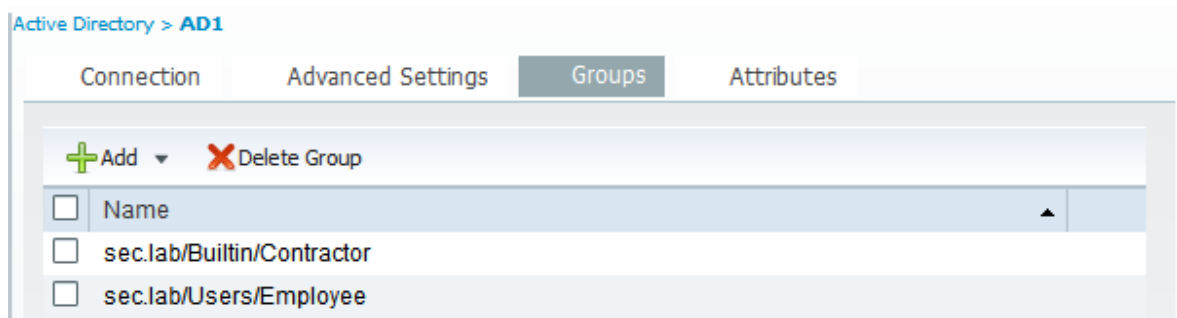
1. Go to Administration > Identity Management > External Identity Sources > Active Directory
2. Click the 'Groups' tab.
3. Click the 'Add' button and choose 'Select Groups from Directory'.



1. Click the 'Retrieve Groups' button to retrieve the groups. Optionally: Specify a group name.
2. Tick the desired groups and click 'Ok' to add them.



1. You will see the groups appear in the Groups list on ISE.



Certificate Authentication Profile

This will be the 'identity source' which authenticates client certificates as in the case of EAP-TLS.

The principle username x509 attribute will be the field from the client certificate that ISE uses to perform a lookup in Active Directory. This means we can perform certificate authentication, but still match groups and attributes of certain users and computers.

1. Go to Administration > Identity Management > External Identity Sources > Certificate Authentication Profile
2. Click Add
3. Give the profile a name and selected the principle username attribute.

The principle username x509 attribute will be the field from the client certificate that ISE uses to perform a lookup in Active Directory.

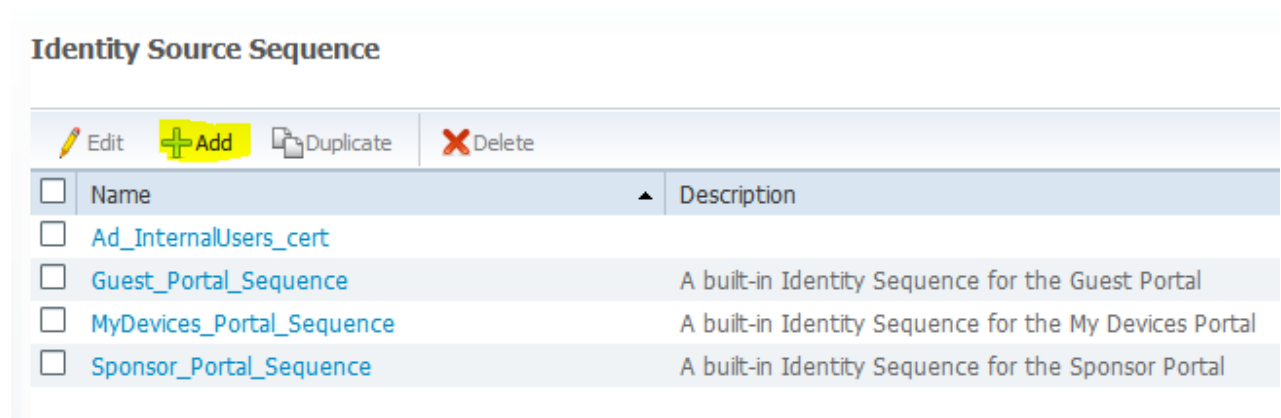
A screenshot of the 'Certificate Authentication Profile' configuration form. The breadcrumb is 'Certificate Authentication Profiles List > Ad_Cert_Profile'. The title is 'Certificate Authentication Profile'. There are several fields: '* Name' with the value 'Ad Cert Profile'; 'Description' which is empty; 'Principal Username X509 Attribute' with a dropdown menu showing 'Common Name'; a checkbox for 'Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active D' which is unchecked; and 'LDAP/AD Instance Name' with an empty text box. At the bottom, there are 'Save' and 'Reset' buttons.

1. Click 'Save' and the Certificate Authentication Profile will appear in the list.

Identity Source Sequence

We're going to use an Identity Source Sequence for our Guest Portal and Secure SSID 'Corporate' authentication rules. This is essentially a catch-all Identity Source Sequence that will authenticate users from Active Directory, Certificate based authentications and Internal Users.

1. Go to Administration > Identity Management > Identity Source Sequences
2. Click the Add button



<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Ad_InternalUsers_cert	
<input type="checkbox"/>	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal
<input type="checkbox"/>	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal
<input type="checkbox"/>	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal

1. Name: AD_InternalUsers_Cert

Tick 'Certificate Authentication Profile' and select our previously created cert profile from the list.

Select 'AD1' and 'Internal Users' as possible Identity Sources.

Under 'Advanced' select 'Treat as if the user was not found and proceed to the next store in the sequence'. This will allow us to continue authentications even in the case of Active Directory connectivity issues.

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

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

Available



Selected







▼ 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

1. Click Save and the Identity Source Sequence will appear in the list.

Identity Source Sequence




 Edit	 Add	 Duplicate	 Delete
<input type="checkbox"/> Name	Description		
<input type="checkbox"/> Ad_InternalUsers_cert			
<input type="checkbox"/> Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal		
<input type="checkbox"/> MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal		
<input type="checkbox"/> Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal		

Guest Portal Setup

We need to create a guest portal which we can send to users performing Web Authentication. We must assign an authentication sequence as well such that Internal Users and Active Directory Users can authenticate via the portal.

1. Go to Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration
2. Click the “Add” button

Multi-Portal Configurations

 Edit	 Add	 Delete
<input type="checkbox"/> Multi-Portal Name	Portal Type	
<input type="checkbox"/> AccessDeniedPortal	CustomDefault	
<input type="checkbox"/> DefaultGuestPortal	Default	

1. On the General tab, name the portal and choose either “Default Portal” or “Custom Default Portal” if you want to upload custom HTML pages.

Multi-Portal

General	Operations	Customization	Authentication
---------	------------	---------------	----------------

* Name

Description

Please select a portal type

- Default Portal (Choose customization template and theme)
- Device Web Authorization Portal (Choose customization template and theme)
- Custom Default Portal (Upload files)
- Custom Device Web Authorization Portal (Upload files)

1. On the operations tab make the following configuration:

Untick “Enable Self-Provisioning Flow” – Ticking this option forces Non-Guest users through provisioning. However, if we don’t have any provisioning rules you may see the error “Your device configuration is not supported by the setup wizard”. We also want to be more granular with which users will undergo provisioning so we will leave this option unticked.

General	Operations	Customization	Authentication
---------	------------	---------------	----------------

Guest Portal Policy Configuration
Guest users should agree to an acceptable use policy

- Not Used
- First Login
- Every Login

Enable Self-Provisioning Flow

Allow guest users to change password

1. On the Authentication tab make the following configuration:

Authentication Type – Choose “Both”

Identity Store Sequence – Choose the one we setup earlier “AD_Internal_Cert”

Note: Guest allows only Internal Guest users to authenticate. Central Web Auth allows only Internal and External Users to Authenticate.

General Operations Customization **Authentication**

Authentication Type

Guest




Central Web Auth

Both

* Identity Store Sequence

1. Click "Save" and the portal will be stored.

Multi-Portal Configurations Select

 Edit  Add  Delete Show

<input type="checkbox"/>	Multi-Portal Name	Portal Type	Description
<input type="checkbox"/>	AccessDeniedPortal	CustomDefault	
<input type="checkbox"/>	DefaultGuestPortal	Default	default portal

Client Provisioning Setup

Enable Client Provisioning

1. Go to Administration > System > Settings > Client Provisioning
2. Check that Client Provisioning is set to "Enabled".

Client Provisioning

* Enable Provisioning:

* Enable Automatic Download: ⓘ

* Update Feed URL:





* Native Supplciant Provisioning Policy Unavailable:

1. Enable Feeds if desired. This will allow ISE to pull the latest supplicant provisioning wizard from Cisco.com.
2. Set “Native Supplicant Provisioning Policy Unavailable” to “Apply Defined Authorization Policy”. This means that devices without client provisioning policies will proceed to the next most relevant Authorization rule.

Download Provisioning Resources

1. Go to Policy > Policy Elements > Results > Client Provisioning > Resources
2. Click the “Add” Button and select “Agent Resourced from Cisco Site”

Resources

		SI
	Edit	
	Add	
	Duplicate	
	Delete	
<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	WinSPWizard 1.0.0.28	WinSPWizard
<input type="checkbox"/>	BYOD	Native Supplicant Profile
<input type="checkbox"/>	WinSPWizard 1.0.0.31	WinSPWizard

1. We are interested in the agent resourced ending with SPWizard (Supplicant Provisioning Wizard). We will be using WinSPWizard 1.0.0.28 so we will tick this then click “Save”

Download Remote Resources... X

<input type="checkbox"/>	Name	Type	Version	Description
<input type="checkbox"/>	MacOsXAgent 4.9.0.654	MacOsXAgent	4.9.0.654	Posture Agent for Mac OSX (ISE ...)
<input type="checkbox"/>	MacOsXAgent 4.9.0.655	MacOsXAgent	4.9.0.655	Posture Agent for Mac OSX (ISE ...)
<input type="checkbox"/>	MacOsXAgent 4.9.0.659	MacOsXAgent	4.9.0.659	Posture Agent for Mac OS X v4.9...
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.11	MacOsXSPWizard	1.0.0.11	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	MacOsXSPWizard	1.0.0.18	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	NACAgent 4.9.0.37	NACAgent	4.9.0.37	Windows Agent (ISE 1.0MR only)
<input type="checkbox"/>	NACAgent 4.9.0.37	NACAgent	4.9.0.37	Windows Agent (ISE 1.1 release...
<input type="checkbox"/>	NACAgent 4.9.0.42	NACAgent	4.9.0.42	Windows Agent (ISE 1.1.1 or later)
<input type="checkbox"/>	NACAgent 4.9.0.47	NACAgent	4.9.0.47	Windows Agent with Win8 OS s...
<input type="checkbox"/>	NACAgent 4.9.0.51	NACAgent	4.9.0.51	Windows Agent (ISE 1.1.3 Rele...
<input type="checkbox"/>	WebAgent 4.9.0.20	WebAgent	4.9.0.20	Web Agent (ISE 1.0MR only)
<input type="checkbox"/>	WebAgent 4.9.0.24	WebAgent	4.9.0.24	Web Agent (ISE 1.1.1 or later)
<input type="checkbox"/>	WebAgent 4.9.0.27	WebAgent	4.9.0.27	Web Agent with Win8 OS suppo...
<input type="checkbox"/>	WebAgent 4.9.0.28	WebAgent	4.9.0.28	Web Agent (ISE 1.1.3 release)
<input type="checkbox"/>	WinSPWizard 1.0.0.22	WinSPWizard	1.0.0.22	Supplicant Provisioning Wizard f...
<input type="checkbox"/>	WinSPWizard 1.0.0.23	WinSPWizard	1.0.0.23	SP Wizard for Windows with Win...
<input checked="" type="checkbox"/>	WinSPWizard 1.0.0.28	WinSPWizard	1.0.0.28	Supplicant Provisioning Wizard f...

1. After the download finishes the wizard will appear in the list of Resources.

Resources

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	WinSPWizard 1.0.0.28	WinSPWizard
<input type="checkbox"/>	BYOD	Native Supplicant Profile
<input type="checkbox"/>	WinSPWizard 1.0.0.31	WinSPWizard

Create Provisioning Profile

The provisioning profile or Native Supplicant Profile is pushed to devices using the supplicant provisioning wizard. It contains settings concerning the protocol we are expect to use after provisioning, and which SSID we will connect to (as in the case of Dual SSID BYOD).

1. Go to Policy > Policy Elements > Results > Client Provisioning > Resources
2. Click "Add" and select "Native Supplicant Profile".

3. Configure the following:


- Name – Can be anything. We'll use BYOD.
- Operating System – All
- Connection Type – Wired and Wireless. This allows the profile to be used to provision devices on wired and wireless connections
- Security – WPA2 Enterprise
- Allowed Protocol – TLS. Since we intend to provision endpoints with certificates we will choose TLS. PEAP is used for Username / Passwords.
- Key Size – 2048

Native Supplicant Profile > BYOD

Native Supplicant Profile

* Name

Description


* Operating System 

* Connection Type Wired
 Wireless

*SSID





Security

* Allowed Protocol

* Key Size 

1. Click "Save" and the profile will appear in the list of resources.

Resources

 Edit	 Add	 Duplicate	 Delete	Show
<input type="checkbox"/>	Name		Type	
<input type="checkbox"/>	WinSPWizard 1.0.0.28		WinSPWizard	
<input type="checkbox"/>	BYOD		Native Supplicant Profile	
<input type="checkbox"/>	WinSPWizard 1.0.0.31		WinSPWizard	






Client Provisioning Rules / Policies

These policies / rules are used to decide which Identity Group, Operating System or Other Conditions receive which Supplicant Provisioning Wizard and Provisioning Profile.

We are going to push WinSPWizard 1.0.0.28 and the “BYOD” profile for AD group “Employees” who are on Windows.

Enabled	Rule Name	Identity Group	Operating System	Other Conditions	Results
Yes	Windows	Any	Windows All	AD1:ExternalGroups EQUALS sec.lab/Users/Employees	WinSPWizard 1.0.0.28 AND BYOD

1. Go to Policy > Client Provisioning Policy
2. Per the table above, enter in each of the required conditions. The basic requirement here is that we specify and Operating System and User Group and select which BYOD profile and provisioning wizard they will receive.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> 	Windows	If Any  and Window... 	and AD1:ExternalGroups EQUALS se... 	then
	WinSPWizard 1.0.0.28 And BYOD 			

Simple Certificate Enrolment Protocol (SCEP)

Relevant Guides:

TrustSec How-to BYOD Using Certificates for Differentiated Access

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certifica...

TrustSec BYOD Smart Solution Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html

Configure SCEP Support for BYOD

http://www.cisco.com/en/US/products/ps11640/products_tech_note09186a0080bff108.shtml

Windows Server Setup

1. Install Windows Server 2008 R2 Enterprise Server
2. After installation completes activate the Windows License and download all Microsoft Updates.

Before you configure SCEP support for BYOD, ensure that the Windows 2008 R2 NDES server has these Microsoft hotfixes installed:

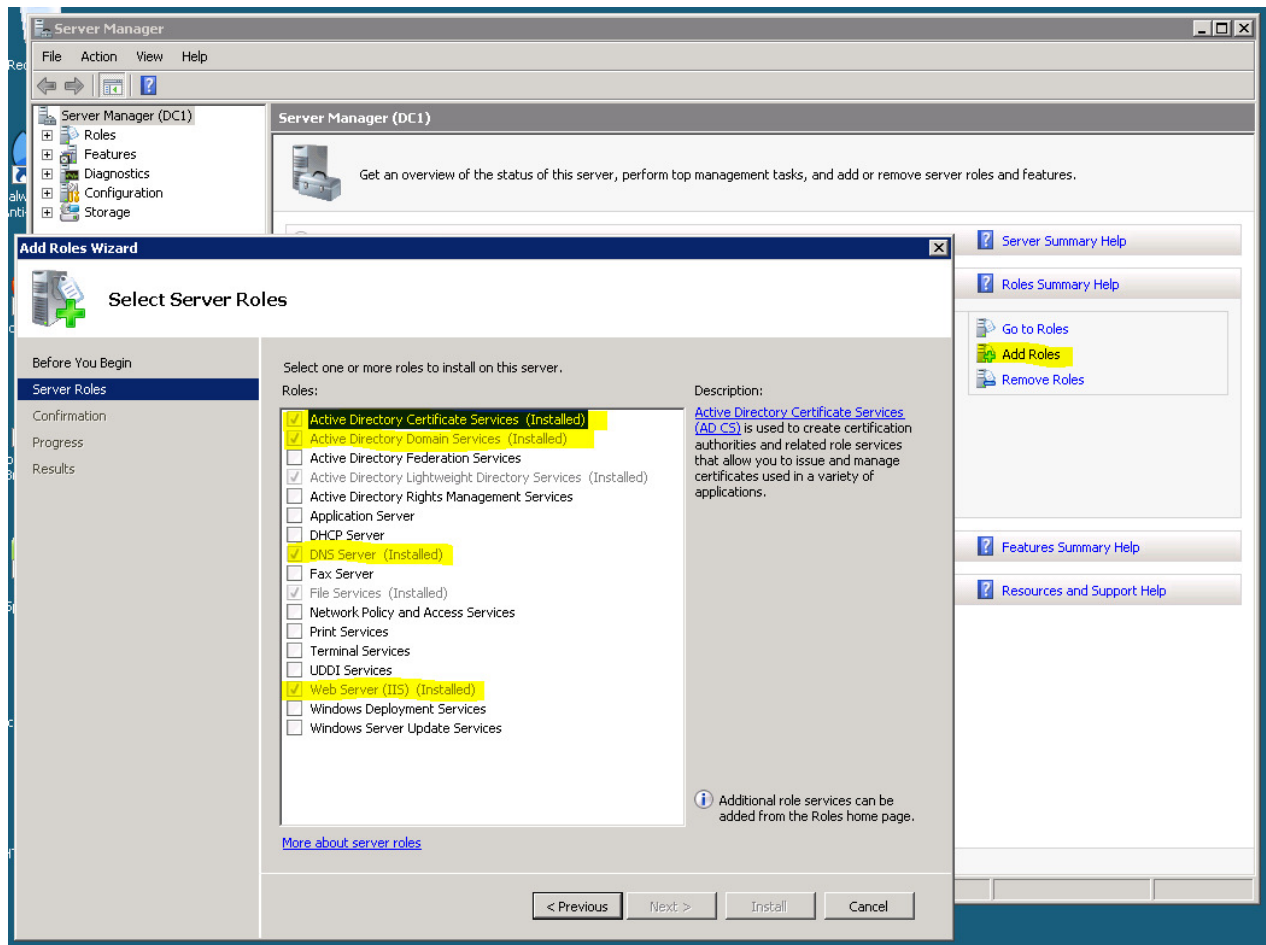
Renewal request for a SCEP certificate fails in Windows Server 2008 R2 if the certificate is managed... - This issue occurs because NDES does not support the GetCACaps operation.

<http://support.microsoft.com/kb/2483564>

NDES does not submit certificate requests after the enterprise CA is restarted in Windows Server 200... - This message appears in the Event Viewer: "The Network Device Enrolment Service cannot submit the certificate request (0x800706ba). The RPC server is unavailable."

<http://support.microsoft.com/kb/2633200>

1. Install and configure Active Directory Domain Services
 1. Select the "advanced" mode checkbox.
 2. Create a new domain in a forest.
 3. Insert the name for the forest root domain.
 4. Install DNS Server.
 5. Wait for Active Directory Services to finish installing and reboot.



1. Install and configure Active Directory Certificate Services.

1. Role Services:

- Certificate Authority
- Certificate Authority Web Enrolment

1. Setup Type: Select "Enterprise"
2. CA Type: Root CA
3. Private Key: Create New Private Key

- Cryptography: Default Value, select SHA256 for hash algorithm.
- CA Name: leave as default
- Validity Period: Default

1. Certificate Database: Default

Server Manager (DC1)

- Roles
 - Active Directory Certificate
 - Active Directory Domain Se
 - Active Directory Lightweigh
 - DNS Server
 - File Services
 - Web Server (IIS)
- Features
- Diagnostics
- Configuration
- Storage

Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary [Roles Summary Help](#)

Active Directory Certificate Services [AD CS Help](#)

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Role Status [Go to Active Directory Certificate Services](#)

Messages: None
 System Services: All Running
 Events: 4 errors, 6 warnings, 2 informational in the last 24 hours

Role Services: 3 installed [Add Role Services](#) [Remove Role Services](#)

Role Service	Status
Certification Authority	Installed
Certification Authority Web Enrollment	Installed
Online Responder	Not installed
Network Device Enrollment Service	Installed

Description:
[Network Device Enrollment Service](#) makes it possible to issue and manage certificates for routers and other network devices that do not have network accounts.

Add Role Services

Select Role Services

Select the role services to install for Active Directory Certificate Services:

Role services:

- Certification Authority (Installed)
- Certification Authority Web Enrollment (Installed)
- Online Responder
- Network Device Enrollment Service (Installed)

Description:
[Certification Authority \(CA\)](#) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

[More about role services](#)

< Previous Next > Install Cancel

1. Web Server (IIS): Click Next

- Role Services: Default

1. Click Install

2. Go to Server Manager > Roles > Active Directory Certificate Services

- Select “Network Device Enrolment Service” and “Certificate Authority Web Enrollment”
- For the Web Enrollement user account, this may be a local Administrator or a SCEP service account (one added to the IIS_USERS Group).

RA Information – Default

Cryptography – Default

CA for CES – Default

Authentication Type – Default

Service Account – Default / Choose an administrator account.

Server Authentication Certificate

Choose an existing certificate for SSL encryption - Select the certificate with ‘Client Authentication’ as the Intended Purpose.

Web Server (IIS) – Click Next

Role Servers – Default

Confirmation: Install

1. Disable SCEP Enrollement Challenge Password Requirement

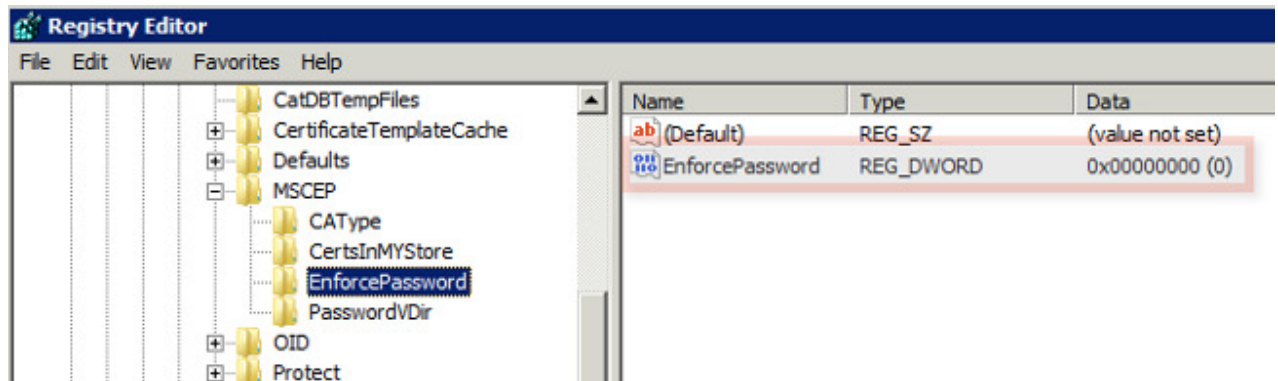
By default, Microsoft's SCEP (MSCEP) implementation uses a dynamic challenge password to authenticate clients and endpoints throughout the certificate enrollment process. With this configuration requirement in place, users must browse to the MSCEP admin web GUI on the NDES server to generate a password on-demand. As part of the registration request, the user must include this password.

In a BYOD deployment, the requirement of a challenge password defeats the purpose of a user self-service solution. In order to remove this requirement, this registry key must be modified on the NDES server:

- Click Start and enter regedit in the search bar.
- Navigate to: Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword.

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

- Ensure that the EnforcePassword value is set to "0" (default is "1").

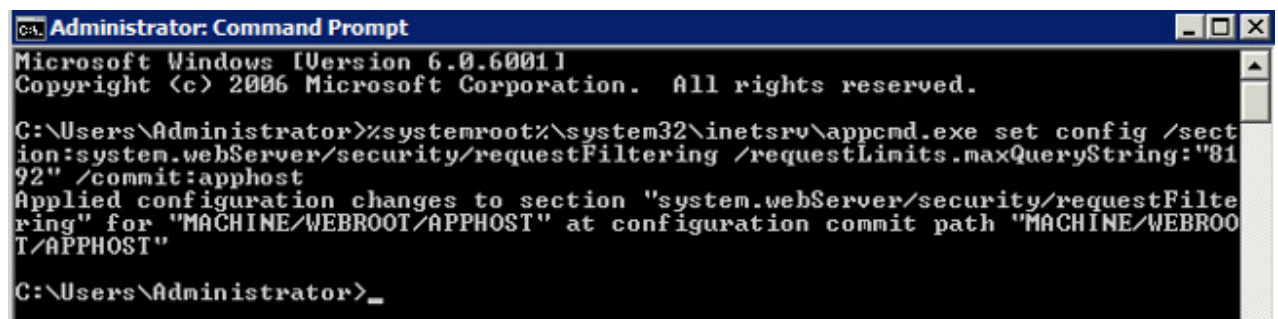


1. Extend URL Length in IIS

It is possible for ISE to generate URLs, which are too long for the IIS web server. To avoid this problem, the default IIS configuration can be modified to allow longer URLs.

Enter the following command in a CLI cmd.exe:

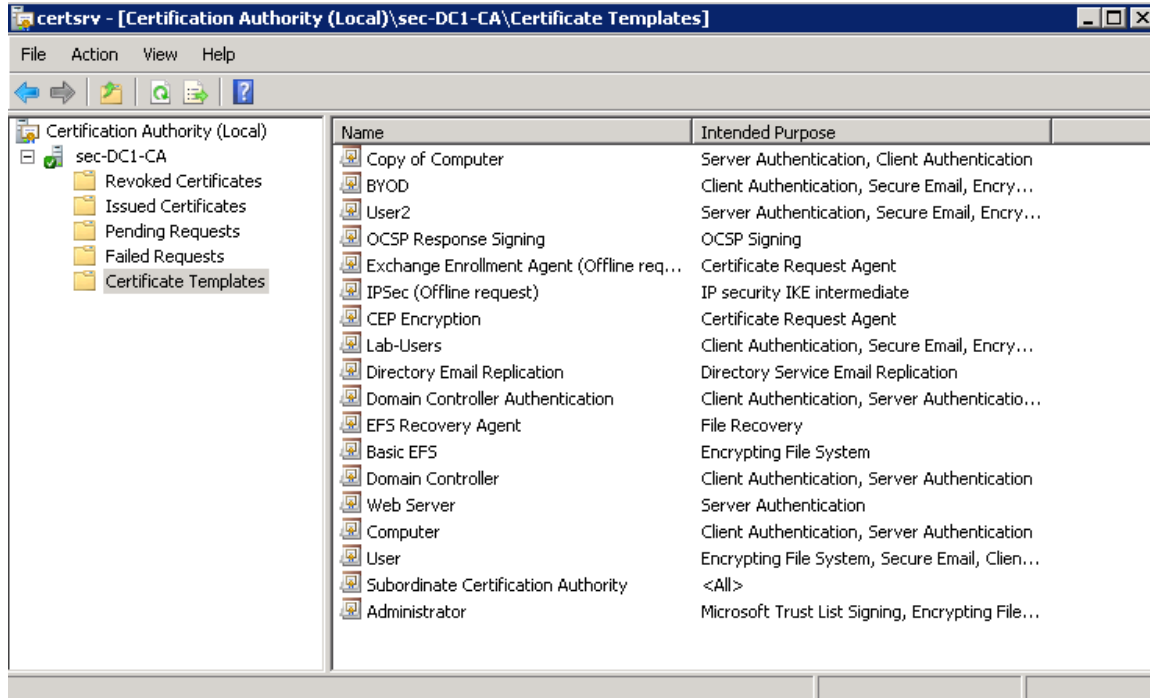
```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
```



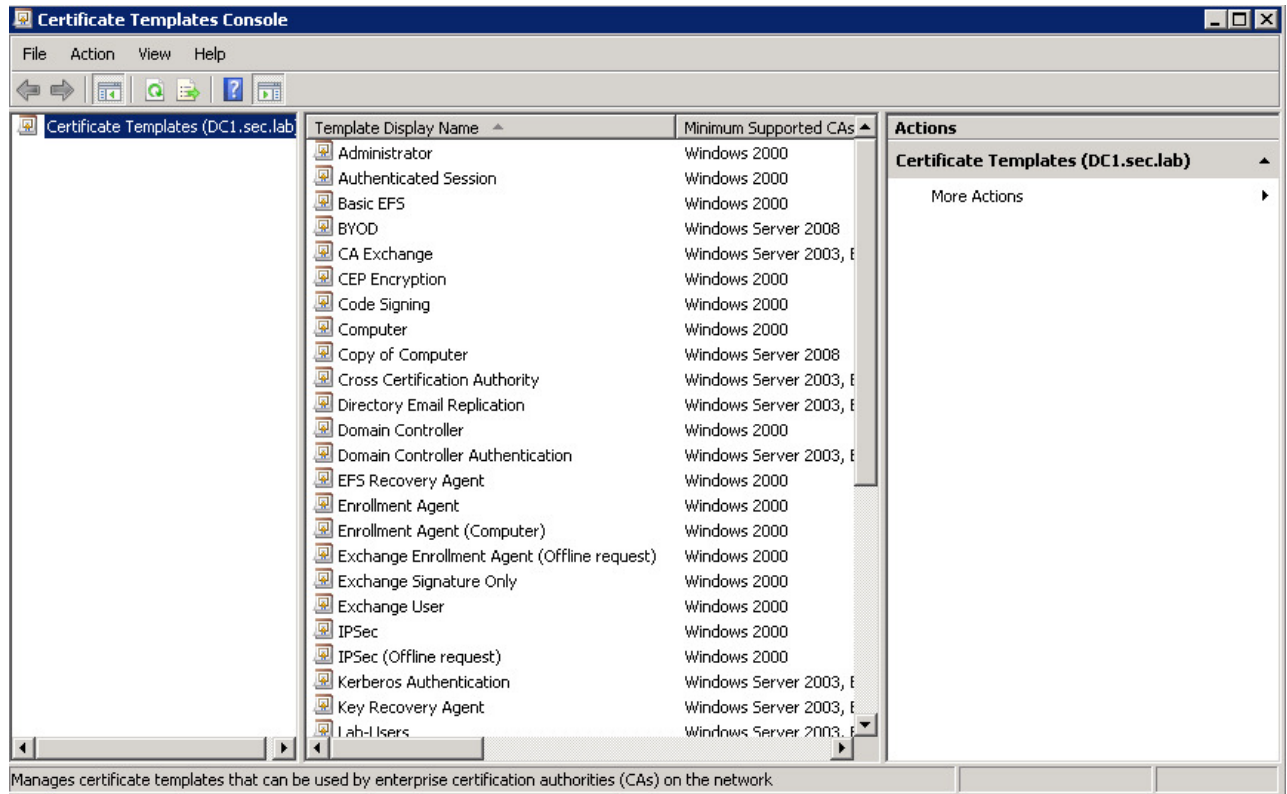
1. Certificate Template Configuration

1. On your CA Server go to Administrative Tools > Certification Authority

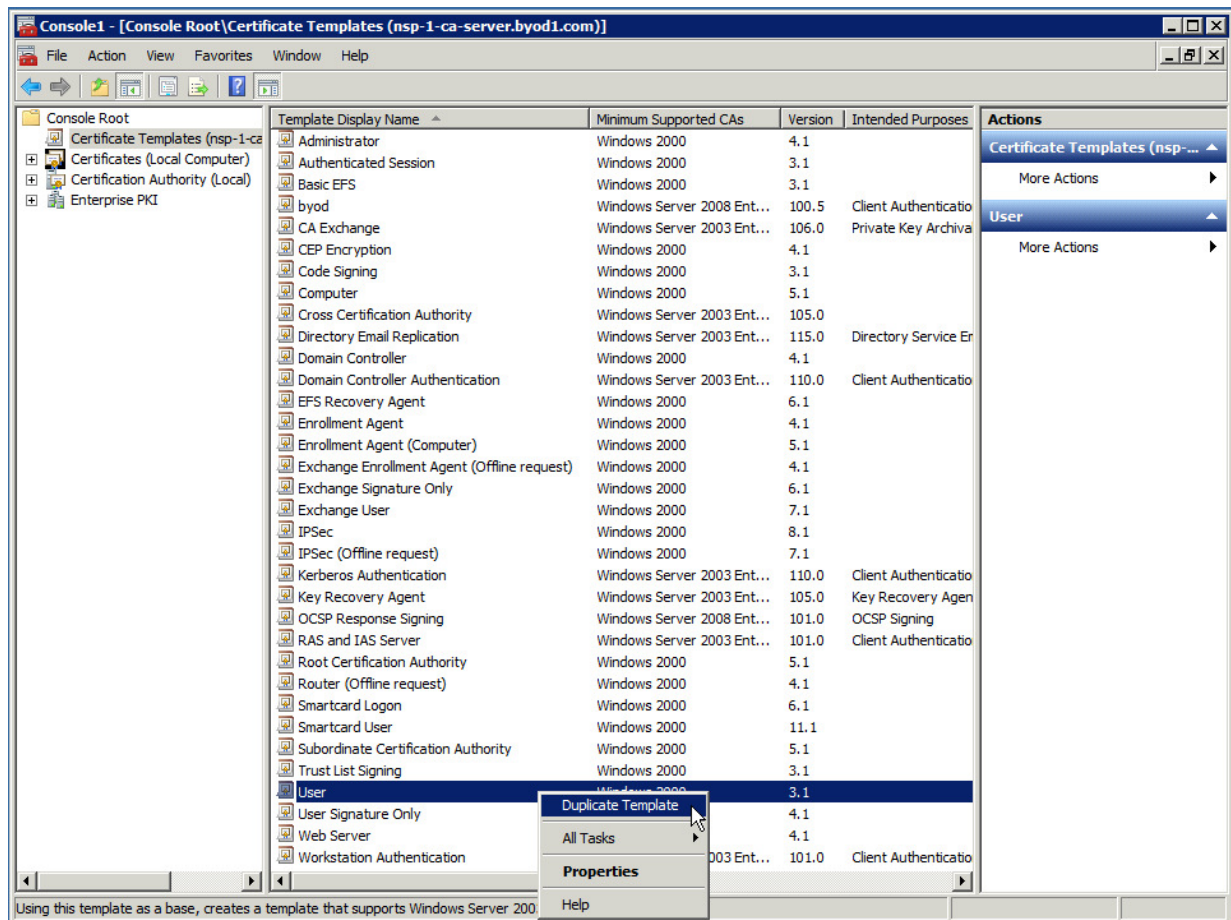
- Open the Certificate Templates folder. These are the currently enabled Certificate Templates.



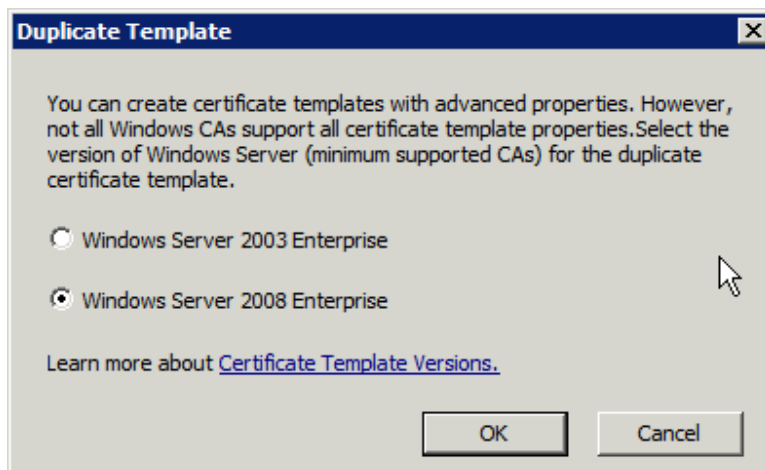
- Right Click on the Certificate Templates Folder and choose Manage. This will open the Certificates Templates Console.



1. Right Click on the 'User' template and duplicate it.



1. Then choose Windows 2003 or Windows 2008, dependent upon the minimum CA operating system (OS) in the environment.



1. On the General tab add a display name, such as BYOD.

Check 'Publish Certificate in Active Directory'

The screenshot shows the 'Properties of New Template' dialog box with the 'General' tab selected. The 'Template display name' and 'Template name' fields both contain 'BYOD'. The 'Validity period' is set to 1 year and the 'Renewal period' is set to 6 weeks. The checkbox 'Publish certificate in Active Directory' is checked, with the sub-option 'Do not automatically reenroll if a duplicate certificate exists in Active Directory' unchecked. The checkbox 'For automatic renewal of smart card certificates, use the existing key if a new key cannot be created' is also unchecked. The dialog box has buttons for 'OK', 'Cancel', 'Apply', and 'Help' at the bottom.

Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Cryptography | Subject Name

Template display name:
BYOD

Minimum Supported CAs: Windows Server 2008

After you apply changes to this tab, you can no longer change the template name.

Template name:
BYOD

Validity period: 1 years Renewal period: 6 weeks

Publish certificate in Active Directory

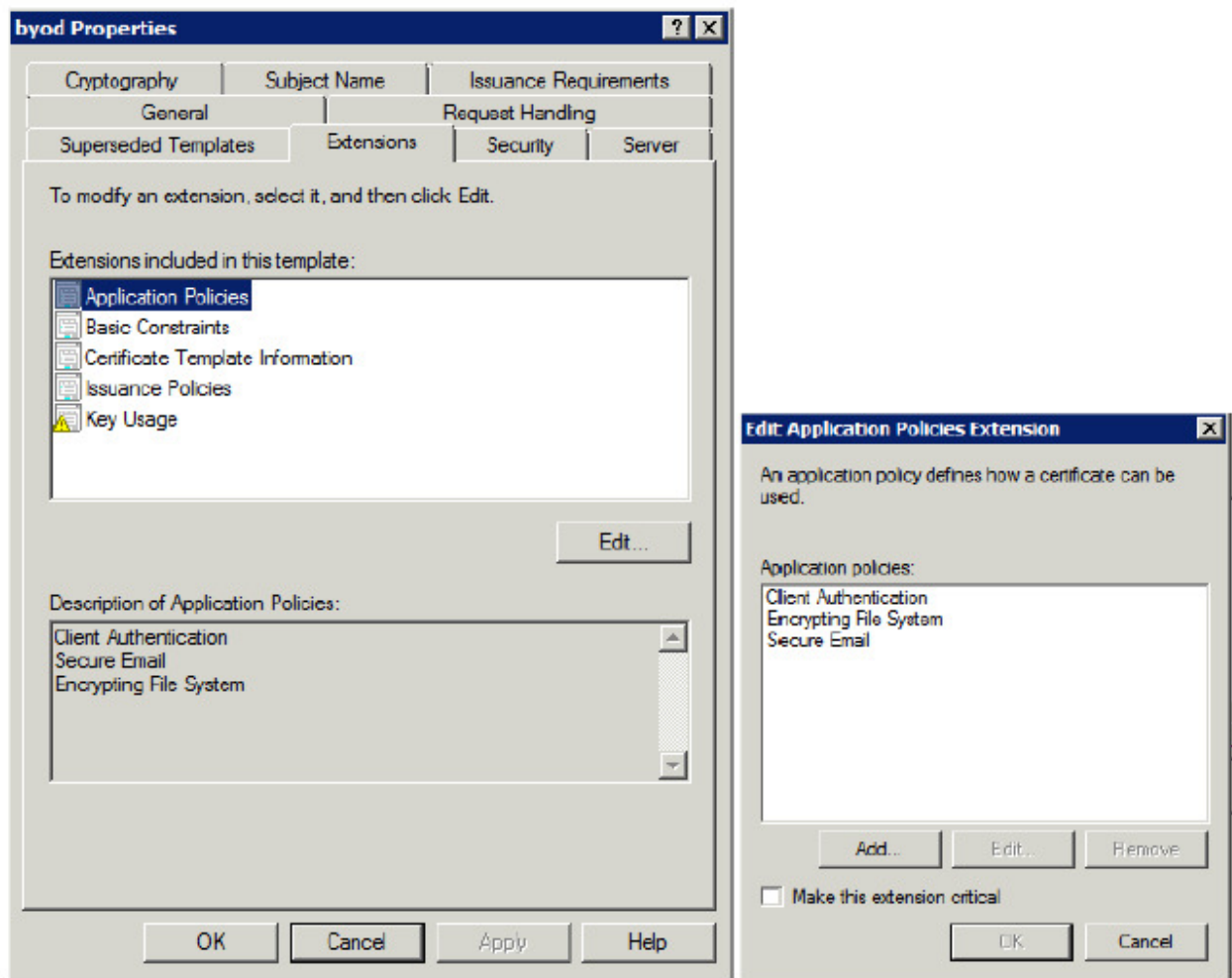
Do not automatically reenroll if a duplicate certificate exists in Active Directory

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

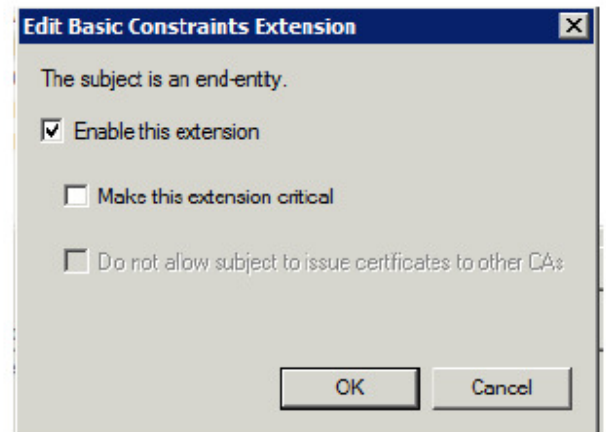
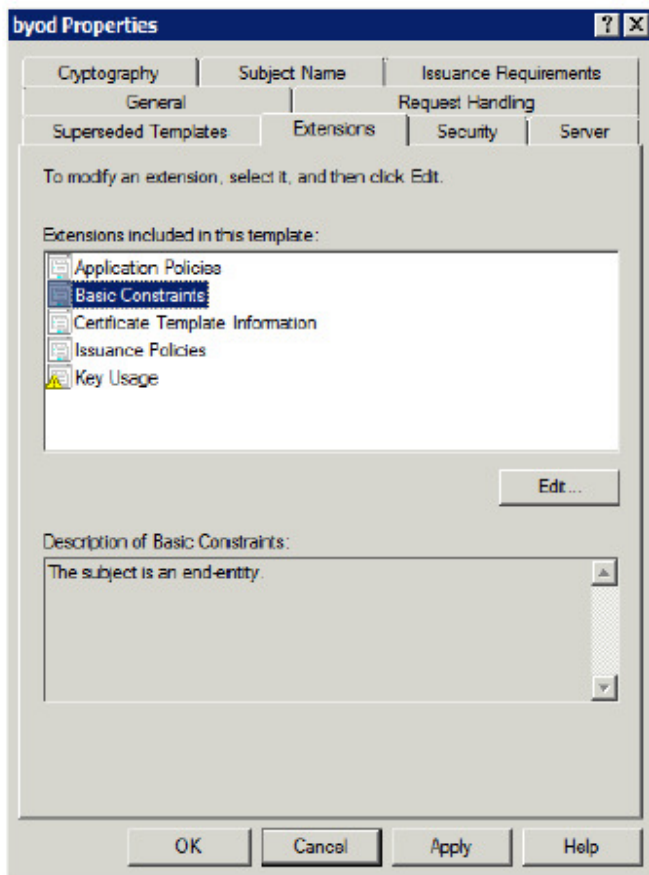
OK Cancel Apply Help

1. On the Extensions tab:

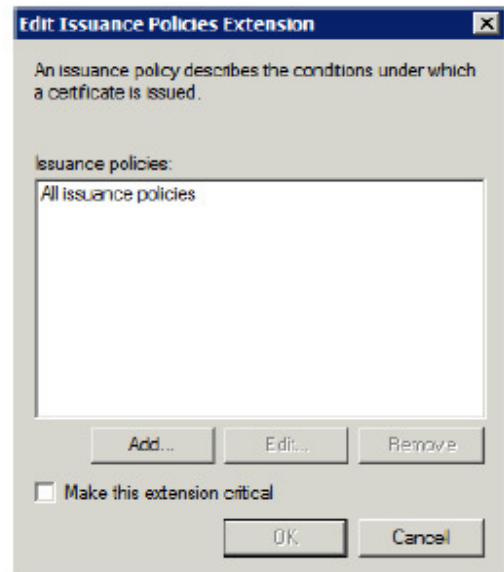
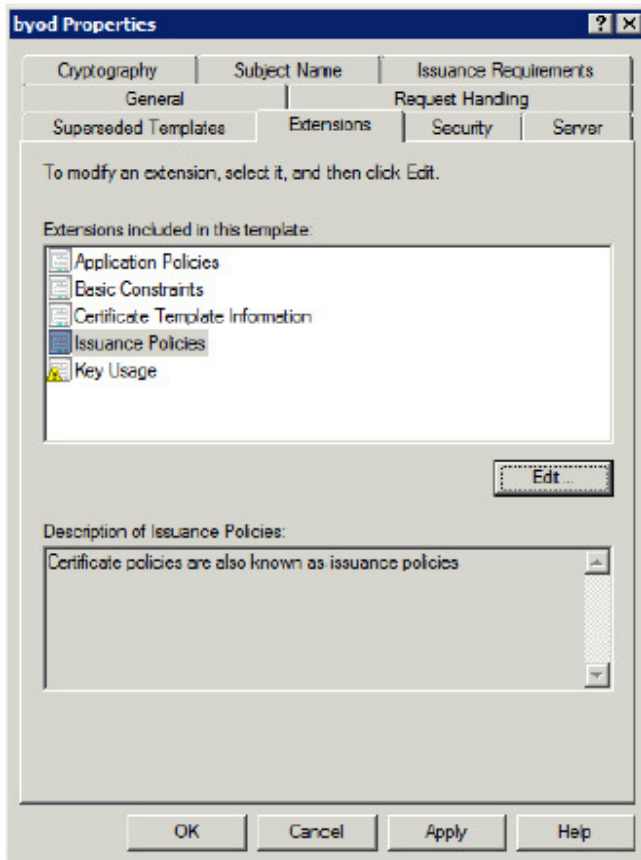
- Click Application Policies > Edit
- Ensure 'Client Authentication' is added as an application policy.
- Click Ok



- If possible, configure 'Basic Constraints' to 'Enable this Extension'. This sets the certificate to belong to an endpoint, and not a subsequent signer. (optional)

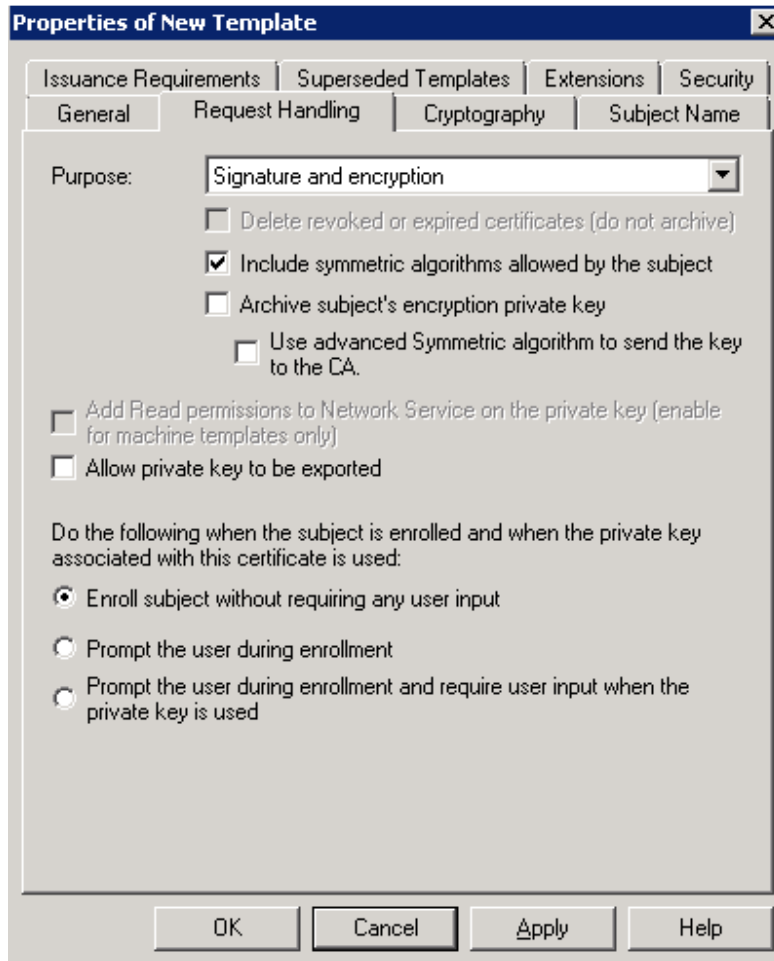


- Edit 'Issuance Policies' and add 'All Issuance Policies'. Issuance Policies must be configured, to allow the CA to actually issue the certificate.



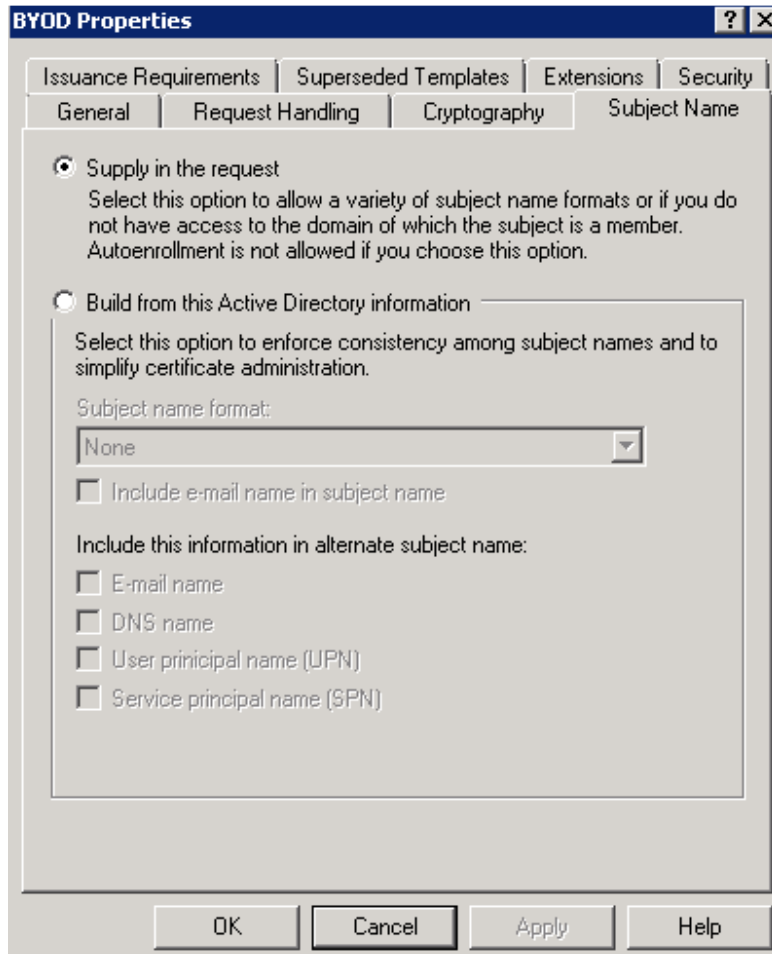
1. On the Request Handling Tab:

- Uncheck Allow Private Key to be Exported.
- Select 'Enroll Subject without Requiring any user input'



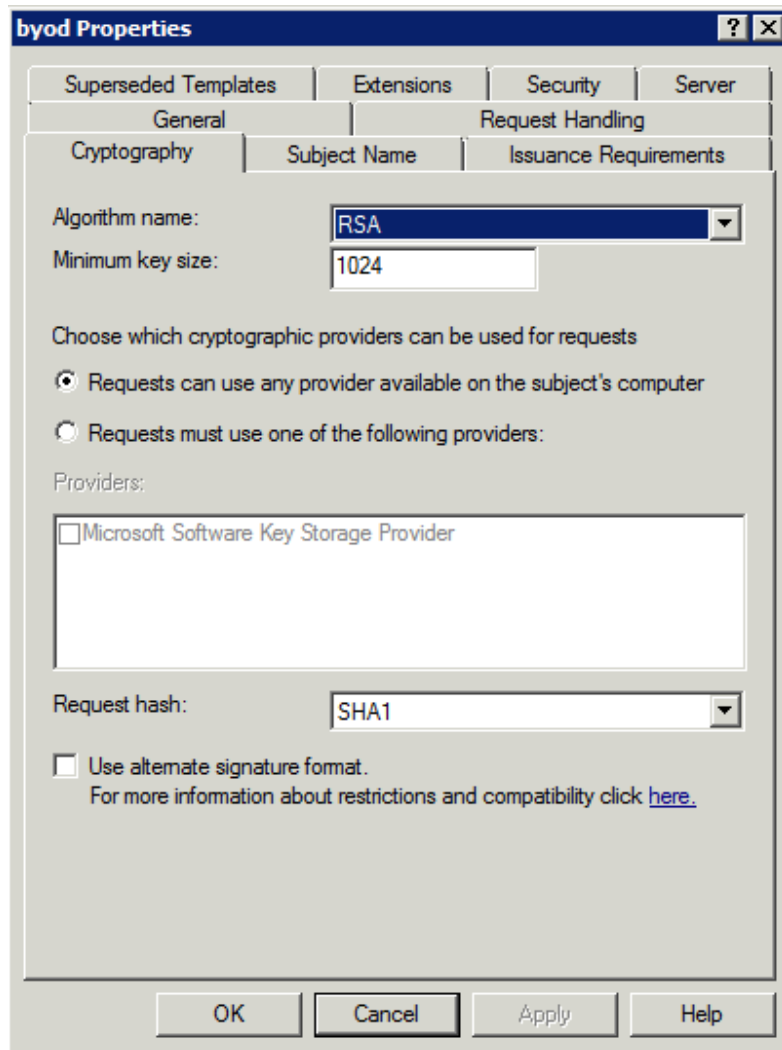
1. On the Subject Name Tab

- Select "Supply In Request", ignore any security warnings. This is necessary since the certificate is not being created by an Active Directory member, but through SCEP instead.



1. On the Cryptography Tab

- Select 'Requests can use any provider available on the subject's computer'.

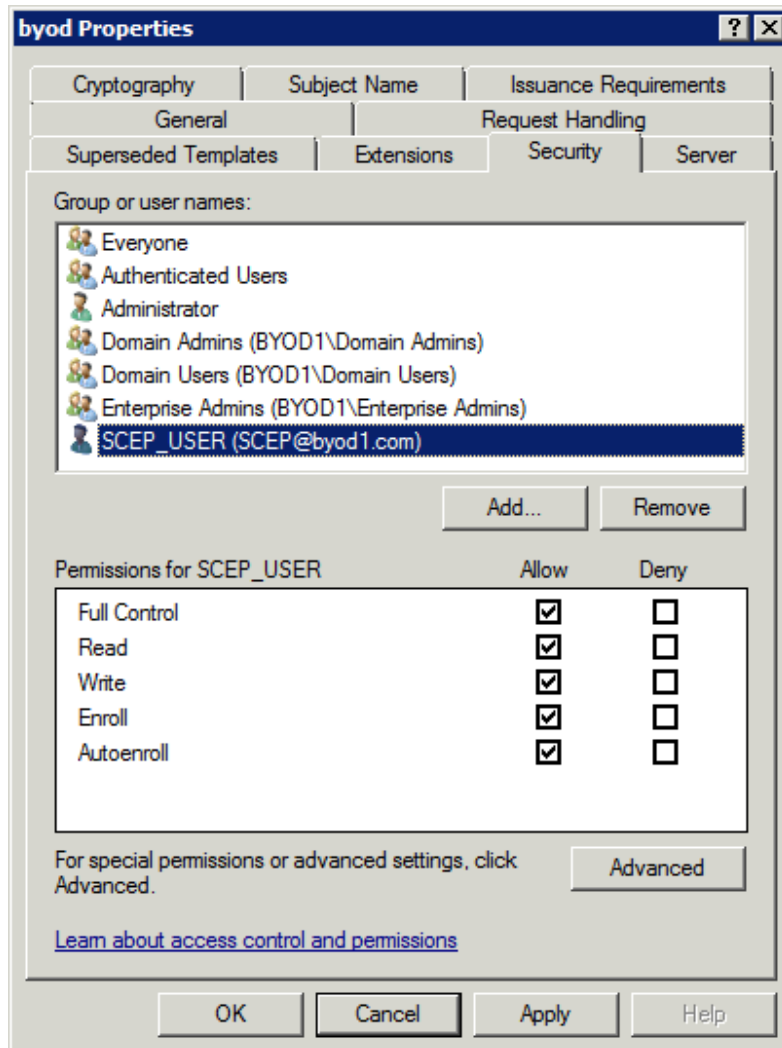


1. If you are using a SCEP service account add this user in the Security Tab.

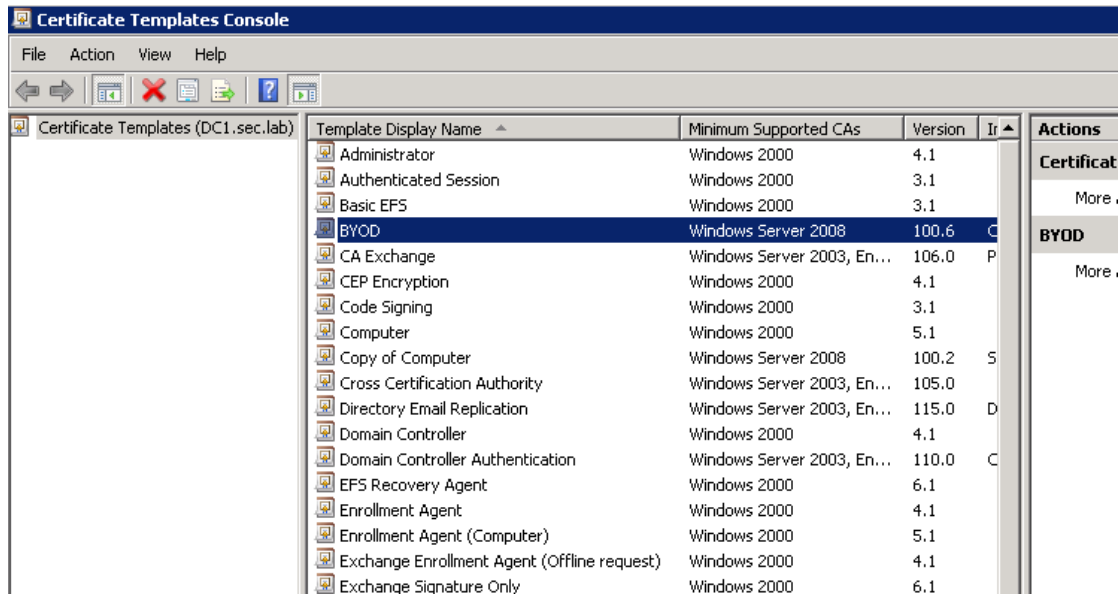
See the following for more details:

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certifica...

For our test we are just using 'Administrator'.



1. Click 'OK' and the finished template should appear in the list of Certificate Templates:

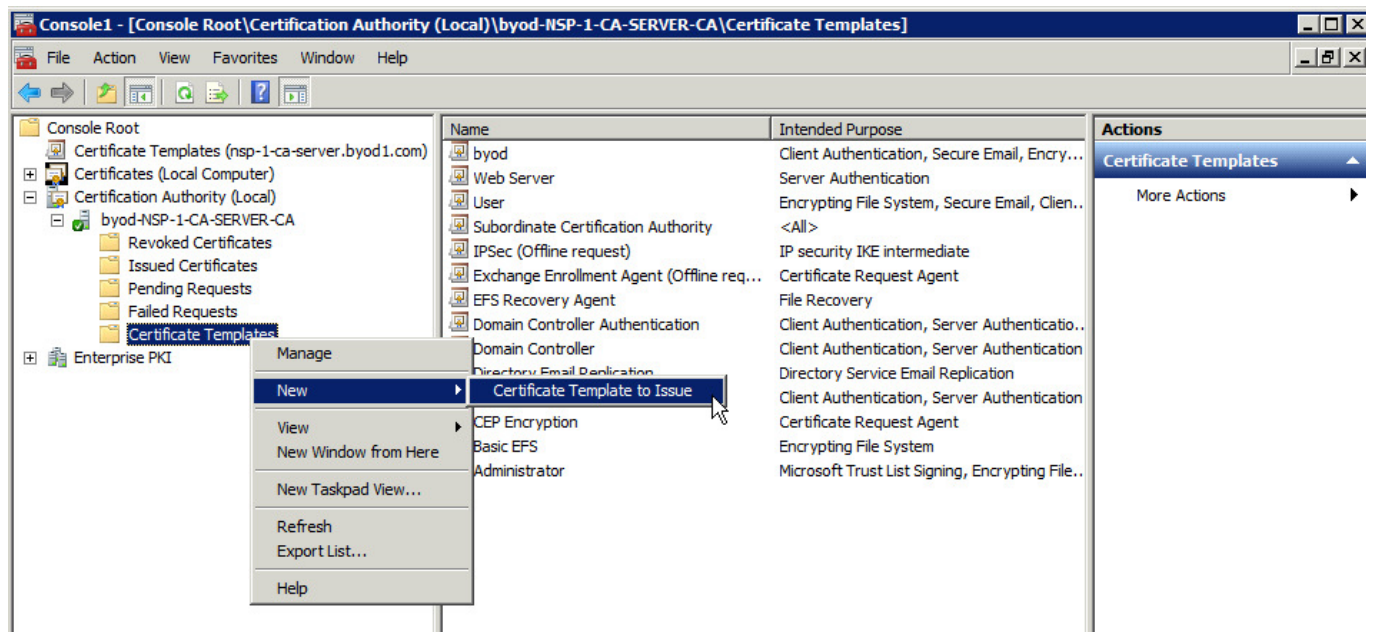


1. Assign the Template for Issuance

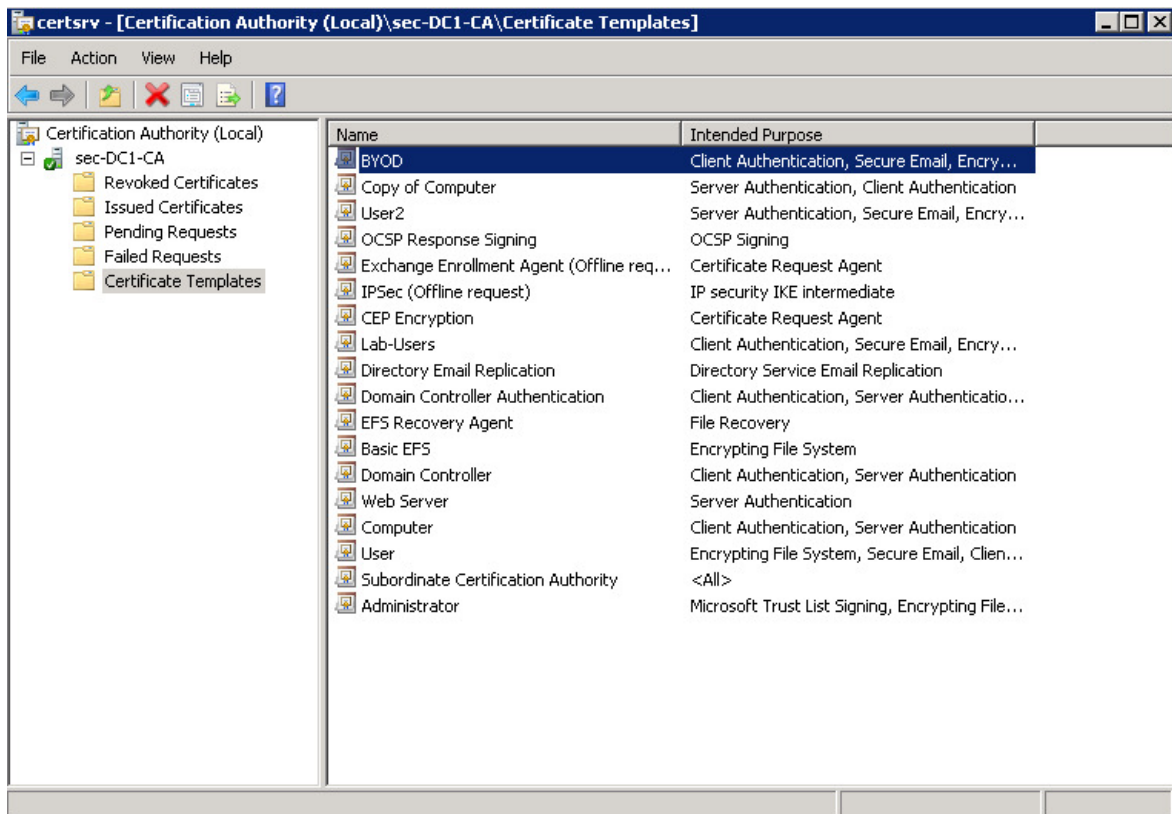
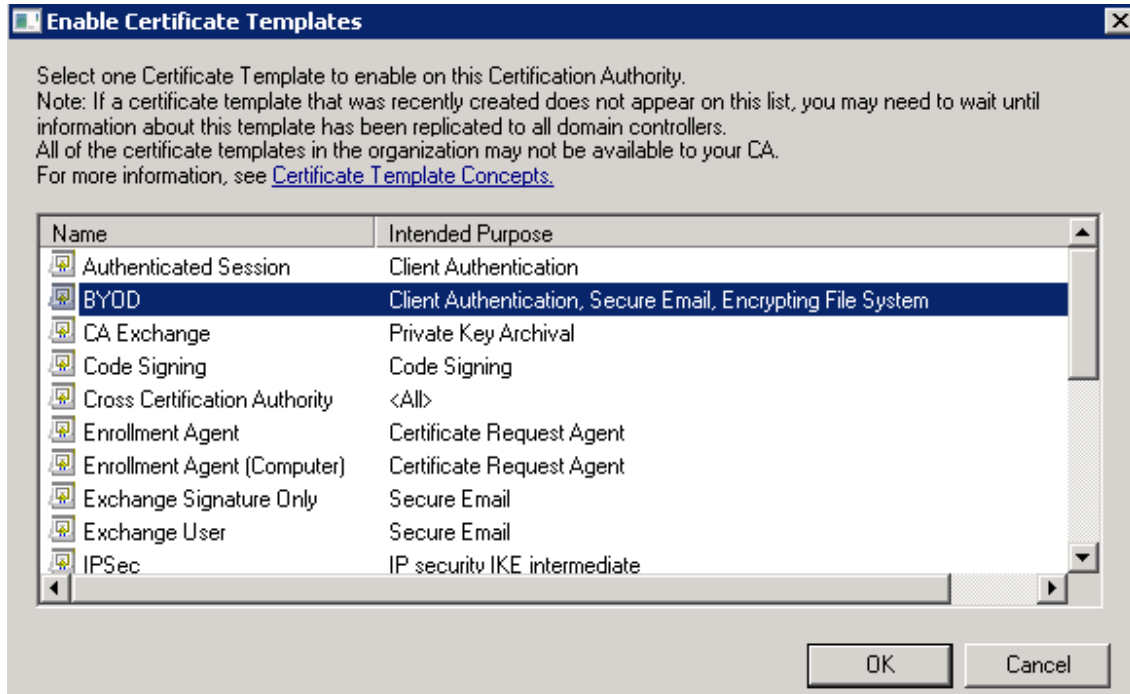
- Return to the Certificate Authority management console (Administrative Tools > Certification Authority). Right Click 'Certificate Templates' and click 'New > Certificate Template to Issue'

Alternatively, this step can be performed from the command line CLI:

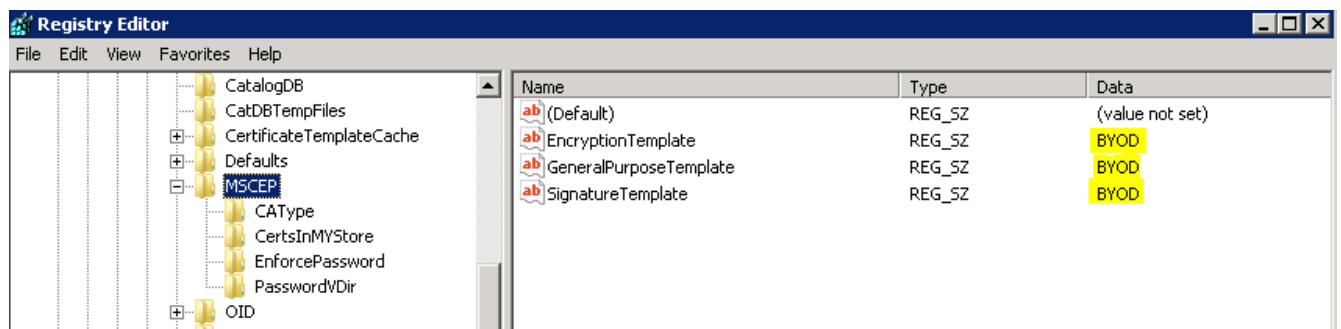
certutil -SetCAtemplates +BYOD



1. Select the 'BYOD' Certificate Template we made earlier and click 'OK'. It should then appear in the list of CA Certificate Templates.



1. Modify the Default Certificate that is Issued (Certificate Template Registry Configuration)
 1. Go to Start > Run > Regedit
 2. Navigate to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP
 3. Change the EncryptionTemplate, GeneralPurposeTemplate, and SignatureTemplate keys from IPsec (Offline Request) to the BYOD template previously created.



1. Restart the Server to apply these settings.
2. Test the SCEP URL in your browser, usually <http://domain-controller-fqdn/certsrv/mscep>

Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

This URL is used by network devices to submit certificate requests.

To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is http://DC1/CertSrv/mscep_admin

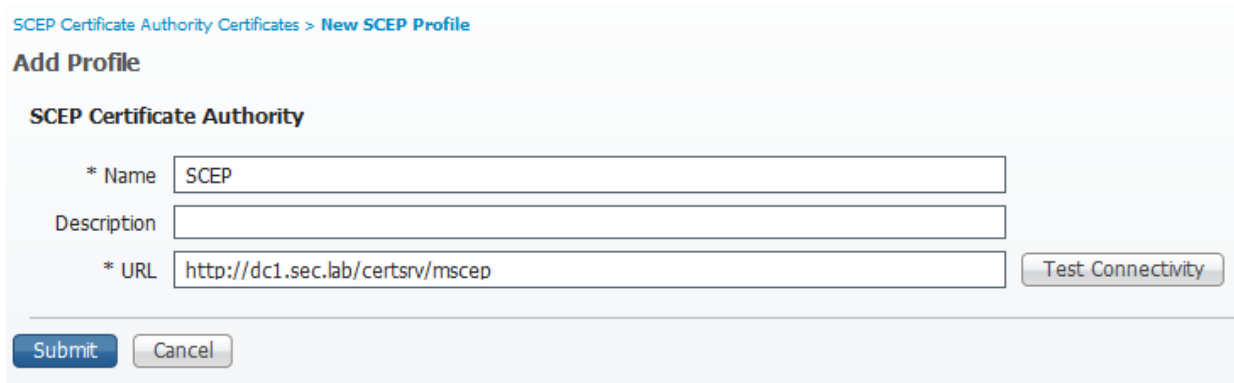
For more information see [Using Network Device Enrollment Service](#).

Configure ISE as a SCEP Proxy

In a BYOD deployment, the endpoint does not communicate directly with the backend NDES server. Instead, the ISE policy node is configured as a SCEP proxy and communicates with the NDES server on behalf of the endpoints. The endpoints communicate directly with ISE. The IIS

instance on the NDES server can be configured to support HTTP and/or HTTPS bindings for the SCEP virtual directories.

1. In ISE, go to Administration > Certificates > SCEP CA Profiles.
2. Click 'Add'.
3. Enter a Server Name and Description



SCEP Certificate Authority Certificates > New SCEP Profile

Add Profile

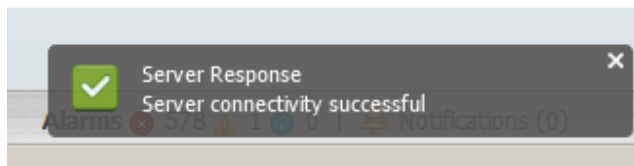
SCEP Certificate Authority

* Name

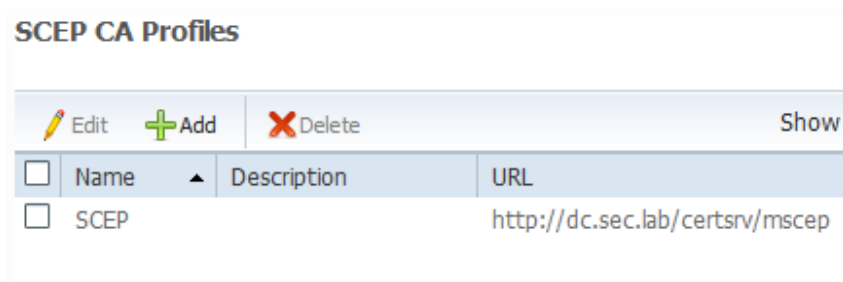
Description

* URL

1. Click the 'Test Connectivity' button to ensure ISE can load the URL.



1. Click 'Submit', the SCEP profile should appear in the list of profiles.



SCEP CA Profiles

<input type="checkbox"/>	Name	Description	URL
<input type="checkbox"/>	SCEP		http://dc.sec.lab/certsrv/mscep

Authentication and Authorization

Authentication Rules

We need four authentication rules to cover Wireless MAC Address Bypass (Wireless MAB), Wireless dot1x (such as PEAP and EAP-TLS), Wired MAB and Wired Dot1x.

The MAB rules should use the Internal Endpoints Identity Store. The other special requirement here is that the MAB rules be set to 'Continue' in the case of 'User Not Found'. This is because ISE has no prior knowledge of the endpoint and we need it to proceed through to authorization so we can redirect it to CWA.

The dot1x rules should use the 'AD_InternalUsers_Cert' Identity Sequence we configured earlier. This will allow 802.1x clients to authenticate with their choice of PEAP and EAP-TLS and hit Active Directory, Internal Users or a Certificate Profile.

Name	Conditions	Allowed Protocol	Identity Source	Options
Wireless MAB	Wireless_MAB	Default Network Access	Internal Endpoints	Authentication Failed = Reject User Not Found = Continue Process Failed = Drop
Wireless Dot1X	Wireless_802.1X	Default Network Access	AD_InternalUsers_Cert	Authentication Failed = Reject User Not Found = Reject Process Failed = Drop
MAB	Wired_MAB	Default Network Access	Internal Endpoints	Authentication Failed = Reject User Not Found = Continue Process Failed = Drop
Dot1X	Wired_802.1X	Default Network Access	AD_InternalUsers_Cert	Authentication Failed = Reject User Not Found = Reject Process Failed = Drop

Relevant Documents:

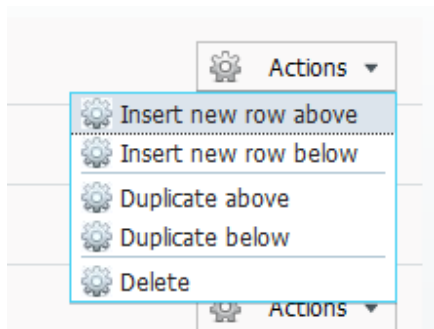
Central Web Authentication on the WLC and ISE Configuration Example

http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080bead09.shtml

Central Web Authentication with a Switch and Identity Services Engine Configuration Example

http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080ba6514.shtml

1. Go to Policy > Authentication
2. Click Actions > Insert New Row Above for each of the needed rules.



1. Fill out each rule per the table above.
2. For the Condition choose Compound Condition then the appropriate condition for the rule as outlined in the above table.

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the Policy Type Simple Rule-Based

The screenshot shows the 'Authentication Policy' configuration page. It features a list of rules on the left and a configuration area on the right. The rules are:

- Wireless MAB : If
- Wireless Dot1X : If
- MAB : If
- Dot1X : If
- Default Rule (If no match) : allow protocols Allowed Prot

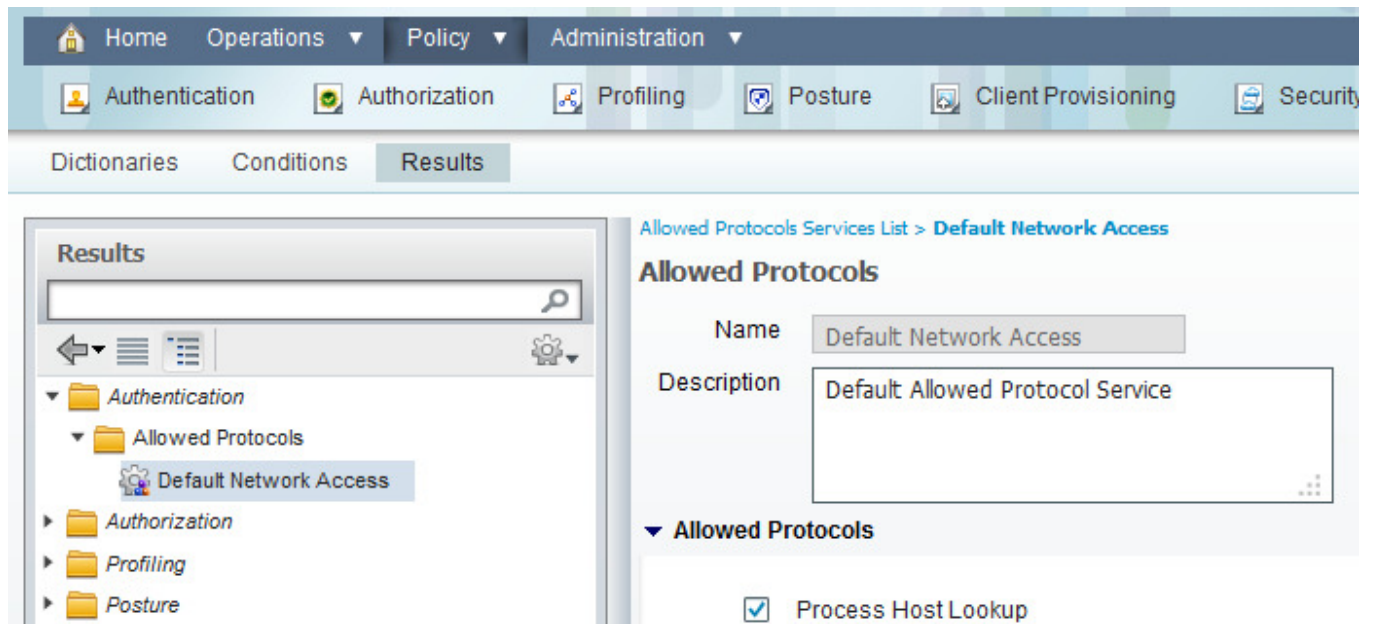
The configuration area on the right shows a table with columns for 'Condition Name' and 'Expression'. A 'Wireless_MAB' condition is selected. A 'Compound Condition' dialog is open, showing a list of protocols:

- Wired_MAB
- Wireless_MAB
- Wired_802.1X
- Wireless_802.1X
- Switch_Local_Web_Authentication
- WLC_Web_Authentication

1. For the Allowed Protocol choose 'Default Network Access'.

The screenshot shows the 'Allowed Protocols' configuration dialog. It features a search bar and a list of protocols. The 'Default Network Access' protocol is selected.

More rules may be created or edited, if desired, in Policy > Results > Authentication. This is where you may choose which authentication methods (Host Lookup, EAP, PEAP etc) are allowed for a specific Authentication Rule.



1. Click the drop down arrow and for the Identity Store choose the relevant Identity Source and Reject/Drop/Continue options for each scenario as outlined in the table above.

Authentication Policy

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

Policy Type Simple Rule-Based

Wireless MAB : If allow protocols and...

Default : use

Wireless dot1x : If

MAB : If

Dot1X : If

Default Rule (If no match) : allow proto

Internal Endpoints

Identity Source

Options

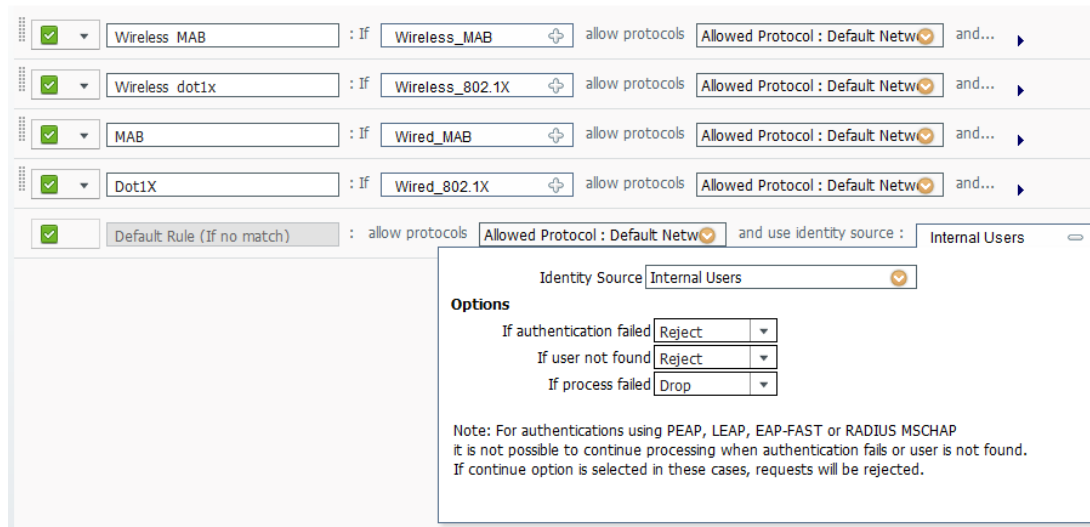
If authentication failed

If user not found

If process failed

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.

1. Once all the rules have been recreated they should look like this:



Authorization Profiles

The Authorization Profiles define what kind of access we push back to a user that succeeds Authentication. Authorization Profiles can contain many things such as: Web Authentication Redirection, Client Provisioning, Posture Assessment and Provisioning, VLANs, DACLS, etc.

For our implementation we will need to create two Authorization Profiles:

CWA – To push a Centralised Web Authentication (CWA) Redirect to users who have authenticated via MAB.

NSP – To push the Supplicant Provisioning Wizard and EAP-TLS Client Provisioning Profile to users who authenticate via PEAP.

1. Go to Policy > Results > Authorization Profiles.
2. Click the 'Add' button.
3. For the 'CWA' profile configure as follows:

- Name: CWA
- Access Type: Access_Accept
- Common Tasks:
- Web Authentication – Centralized – ACL: ACL-NSP-REDIRECT – Redirect: Default

Note: ACL-NSP-REDIRECT is the redirect ACL defined on the WLC or Switch for redirect traffic. We configured this earlier.

Note: 'Redirect:' may be set to 'Manual' and we can manually specify 'DefaultGuestPortal' or our own Custom Portal.

Redirect Value

Authorization Profiles > CWA

Authorization Profile

* Name

Description

* Access Type

Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication ACL Redirect

Auto Smart Port

Advanced Attributes Settings

= - +

Attributes Details

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

1. For the 'NSP' profile, configure as follows:

- Name: NSP

- Access Type: Access_Accept
- Common Tasks:
- Web Authentication – Supplicant Provisioning – ACL: ACL-NSP-REDIRECT

Authorization Profiles > NSP

Authorization Profile

* Name

Description

* Access Type

▼ Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication ACL

Auto Smart Port

▼ Advanced Attributes Settings

= - +

▼ Attributes Details

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

1. We should now have our CWA, NSP, PermitAccess and DenyAccess authorization profiles:

Standard Authorization Profiles	
<input type="checkbox"/> Edit <input type="checkbox"/> Add <input type="checkbox"/> Duplicate <input type="checkbox"/> Delete	
<input type="checkbox"/> Name	Description
<input type="checkbox"/> AccessDenyPage	
<input type="checkbox"/> Blackhole_Wireless_Access	Profile for Wireless
<input type="checkbox"/> CWA	
<input type="checkbox"/> Cisco_IP_Phones	Profile For Cisco P
<input type="checkbox"/> DenyAccess	Default Network.
<input type="checkbox"/> NSP	
<input type="checkbox"/> OnlyISEandDNS	
<input type="checkbox"/> PermitAccess	Default Network.
<input type="checkbox"/> Post_Unknown	

Authorization Rules

We are going to implement the rules necessary for both Single SSID and Dual SSID Mode.

- In **Single SSID** mode we are going to check which group the user belongs to and whether they authenticate via PEAP or EAP-TLS.

- If the user access is PEAP and a Contractor: we permit them access.
- If the user access is PEAP and an Employee: we send them through supplicant provisioning and they reconnect to the Corporate SSID with EAP-TLS.
- If the user access is EAP-TLS and an Employee: we permit them access.

- In **Dual SSID** mode users will authenticate via MAB and login via the CWA Guest Portal before we allow access or provision them.

- If the user access is Guest Flow and a Contractor: we permit them access.
- If the user access is Guest Flow and an Employee: we send them through supplicant provisioning and they reconnect with EAP-TLS.

The way this looks in terms of actual rules is as such:

	Name	Conditions	Permissions
1	Contractor	AD1:ExternalGroups EQUALS sec.lab/Builtin/Contractor	PermitAccess

2	Employee_PostCWA	(AD1:ExternalGroups EQUALS sec.lab/Users/Employee AND Network Access:UseCase EQUALS Guest Flow)	NSP
3	Employee_PEAP	(AD1:ExternalGroups EQUALS sec.lab/Users/Employee AND Network Access:EapTunnel EQUALS PEAP)	NSP
4	Employee	(AD1:ExternalGroups EQUALS sec.lab/Users/Employee AND Network Access:EapAuthentication EQUALS EAP-TLS)	PermitAccess
5	Guest	Guest	PermitAccess
6	CWA	Wireless_MAB	CWA
7	Default	--	DenyAccess

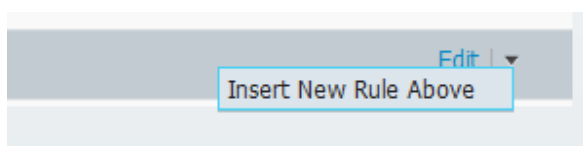
Note: ISE evaluates each rule sequentially. It will choose the first rule that satisfies all the criteria conditions. In this sense, we 'fail' each rule until we hit one that matches.

For example, unknown endpoints authenticating via Wireless_MAB will fail all previous rules because ISE will not know their Group Membership or Username. They will match the CWA rule and receive the CWA authorization profile, which redirects them to the Guest Portal.

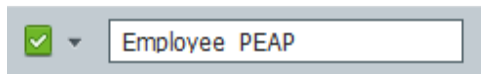
Note: The condition 'Network Access:UseCase EQUALS Guest Flow' refers to a session flag which is set if the client authenticates via the Guest Portal. With this condition, when referenced in an authorization rule, we are checking to see if the user came in through the Guest Portal or not.

As part of this configuration example we will configure the Employee_PEAP rule. The Employee_PEAP rule will match employees authenticating on the Corporate SSID with their Active Directory credentials (PEAP). It will then push an authorization profile that will redirect employees through supplicant provisioning.

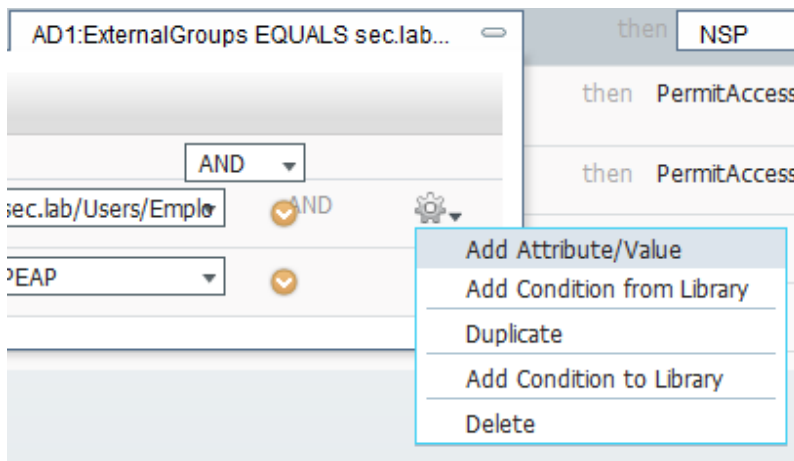
1. Go to Policy > Authorization
2. Click the Down Arrow and click "Insert New Rule Above"



1. Name the rule Employee_PEAP



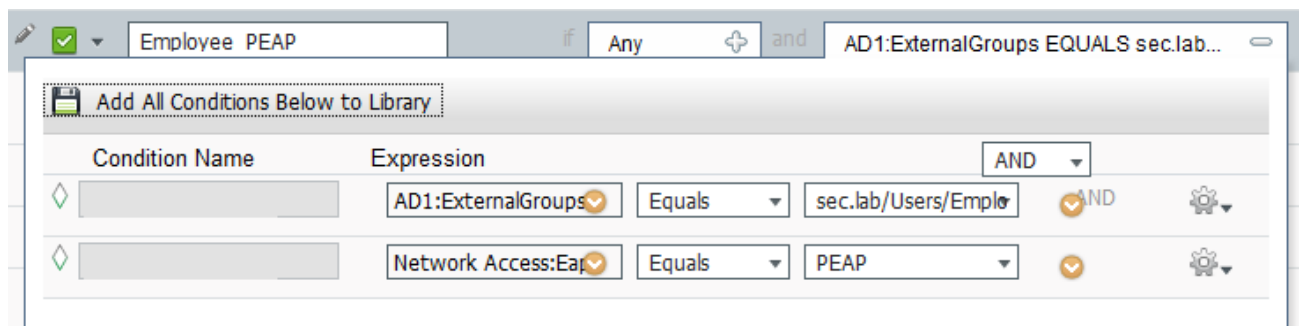
1. For the Identity Group choose 'Any'. These Identity Groups refer to Internal groups in ISE. We will be referencing the Active Directory group in our Conditions.
2. Expand the conditions box, click the cog and select 'Add Attribute/Value'.



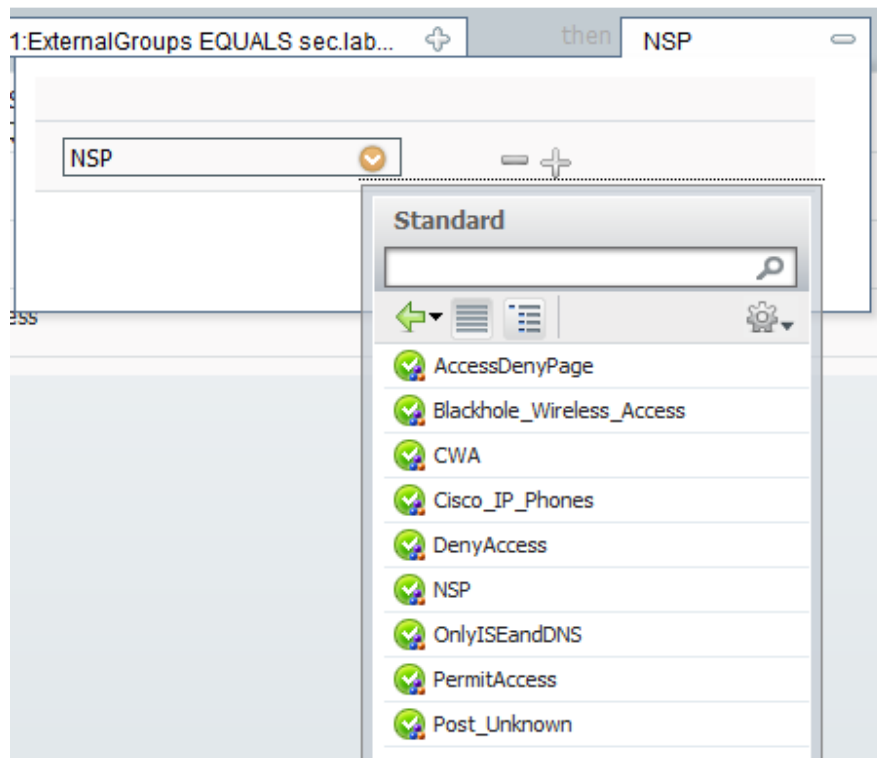
1. Add the following attributes/values to build our conditions:

AD1:ExternalGroups EQUALS sec.lab/Users/Employee

Network Access:EapTunnel EQUALS PEAP



1. Close the Conditions box and expand the Permissions box. Select Standard then 'NSP'.

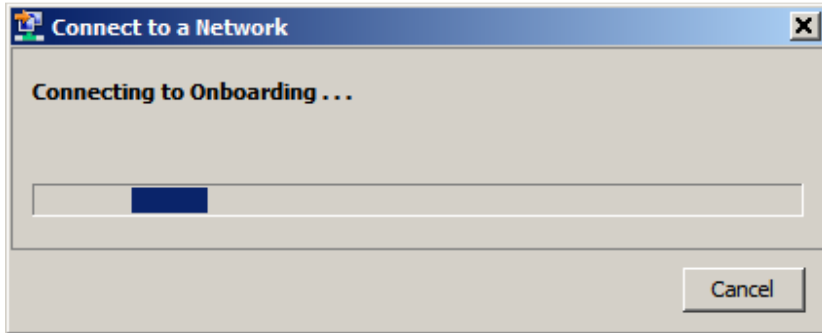


1. Repeat the above steps for each of the needed authorization rules

User Experience

Dual SSID Employee

1. The employee connects to WLAN SSID 'Onboarding' and authentication takes place in the background via MAB.

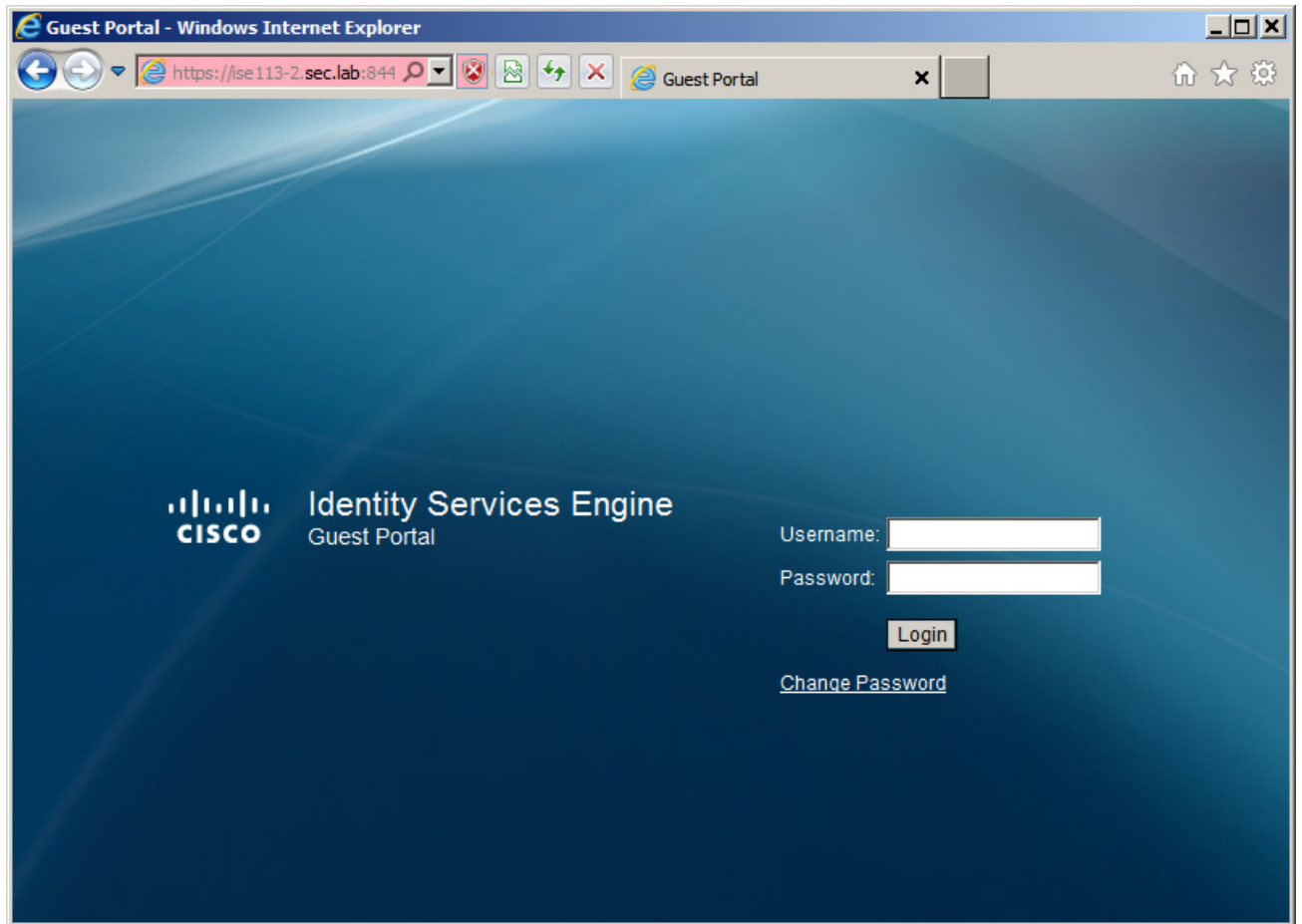


1. This is what the MAB authentication and CWA authorization looks like on the ISE

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Jun 20,13 04:51:04.596 PM	✓		00:19:D2:AD:40:61	00:19:D2:AD:40:61		WLC2		CWA

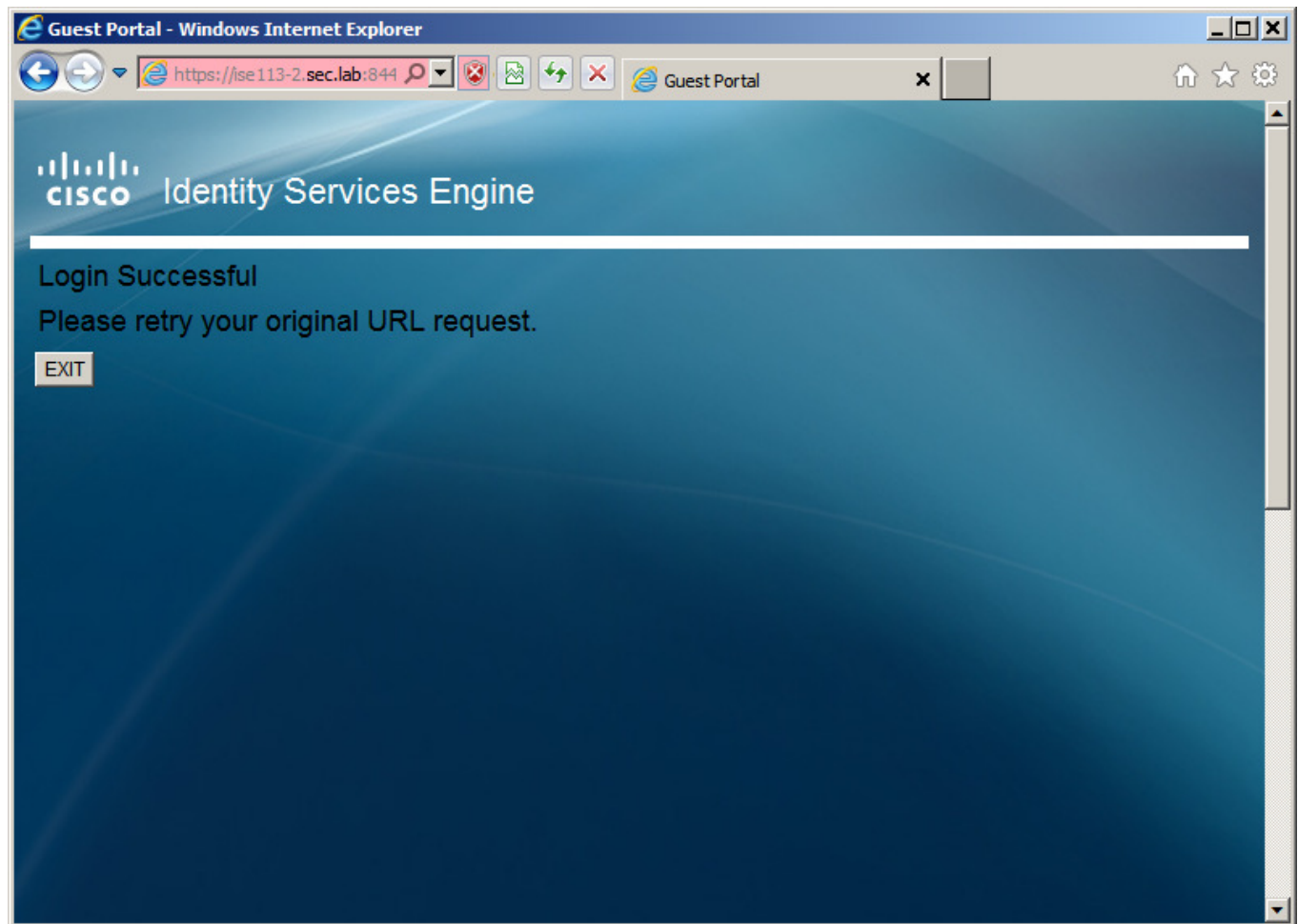
1. When the user attempts to access a website, for example <http://www.cisco.com/>, they are redirected by the WLC to the ISE Guest Portal.

The default web address for the ISE Guest Portal is <https://ise113-2.sec.lab:8443/guestportal/Login.action> with a session ID on the end.



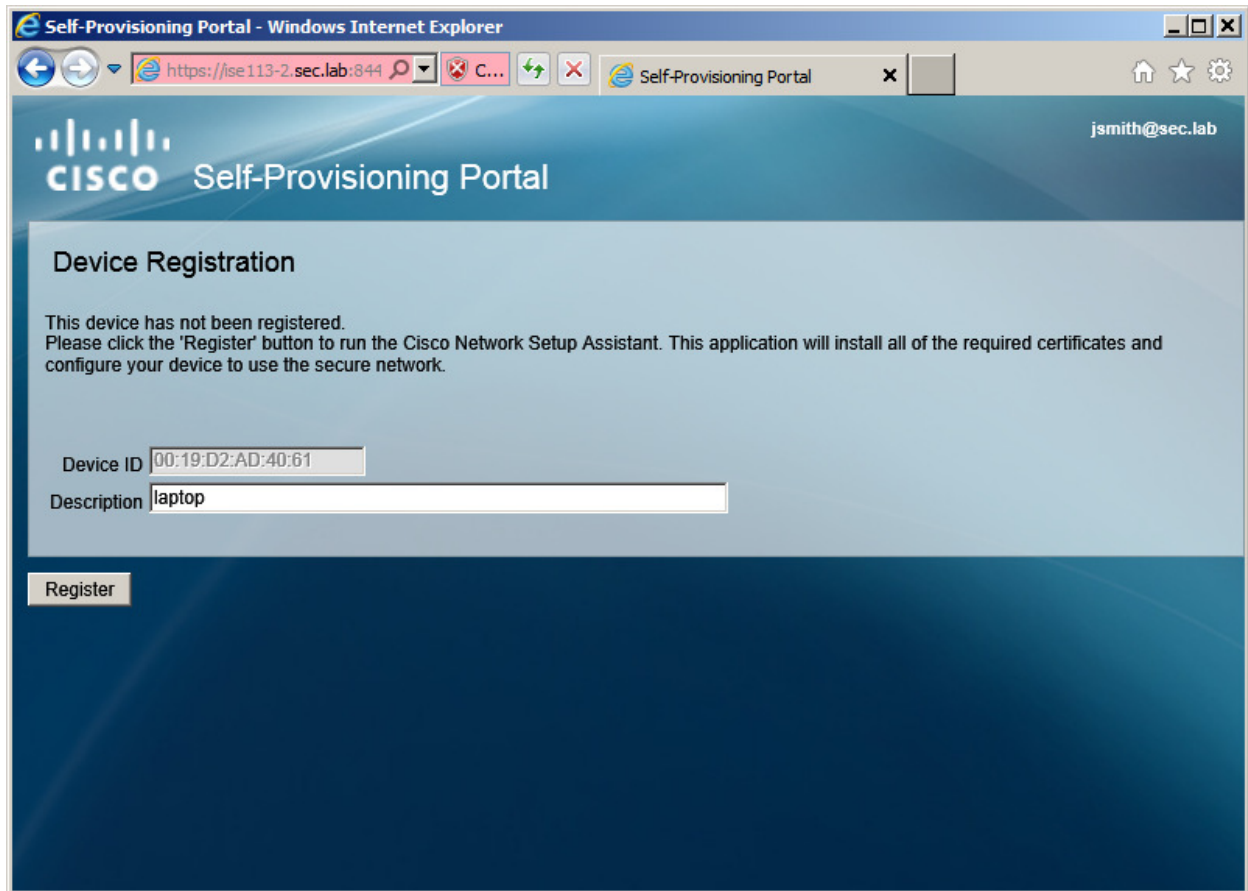
1. The user passes authentication and is asked to retry their original URL.

Although there is no way for ISE to automatically redirect users to their originally requested page, if we use a custom portal then we can include a HTML or Javascript redirect in our success html page to force their browsers to a page of our choice.

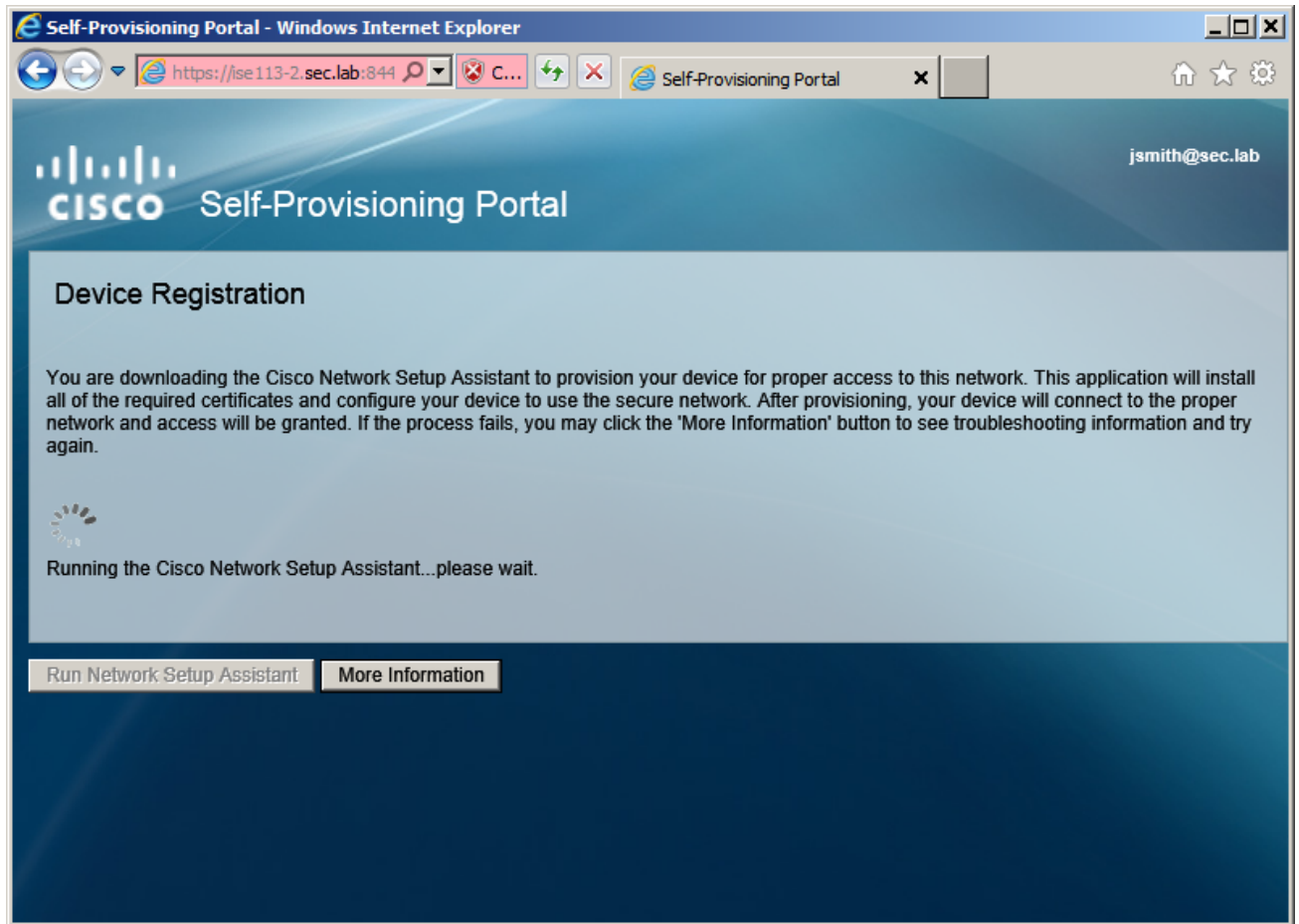


1. The makes another request for <http://www.cisco.com/> and is redirected once more to the Self-Provisioning Portal.

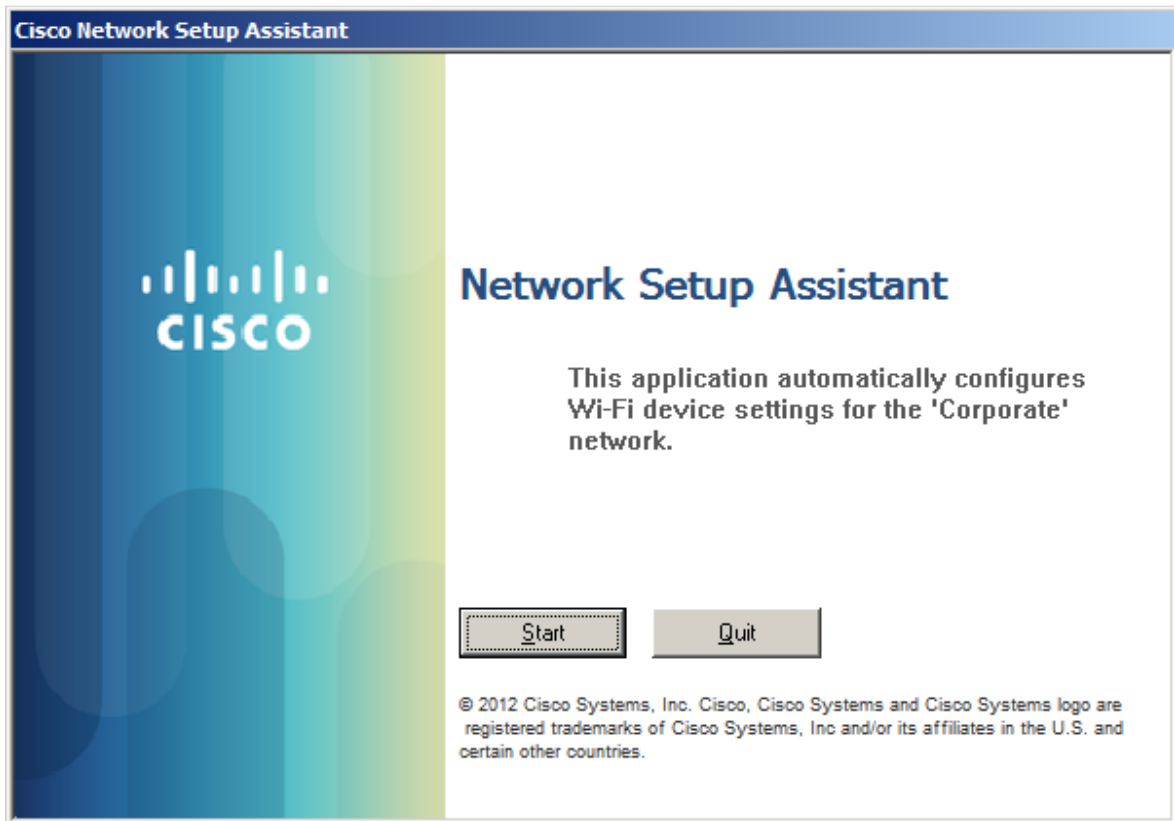
Note: We can avoid needing to make a second website request by forcing users directly into provisioning. This achieved by ticking 'Enable Self-Provisioning Flow' for the specific portal setup in ISE. This is covered in the section 'Guest Portal Setup' above.



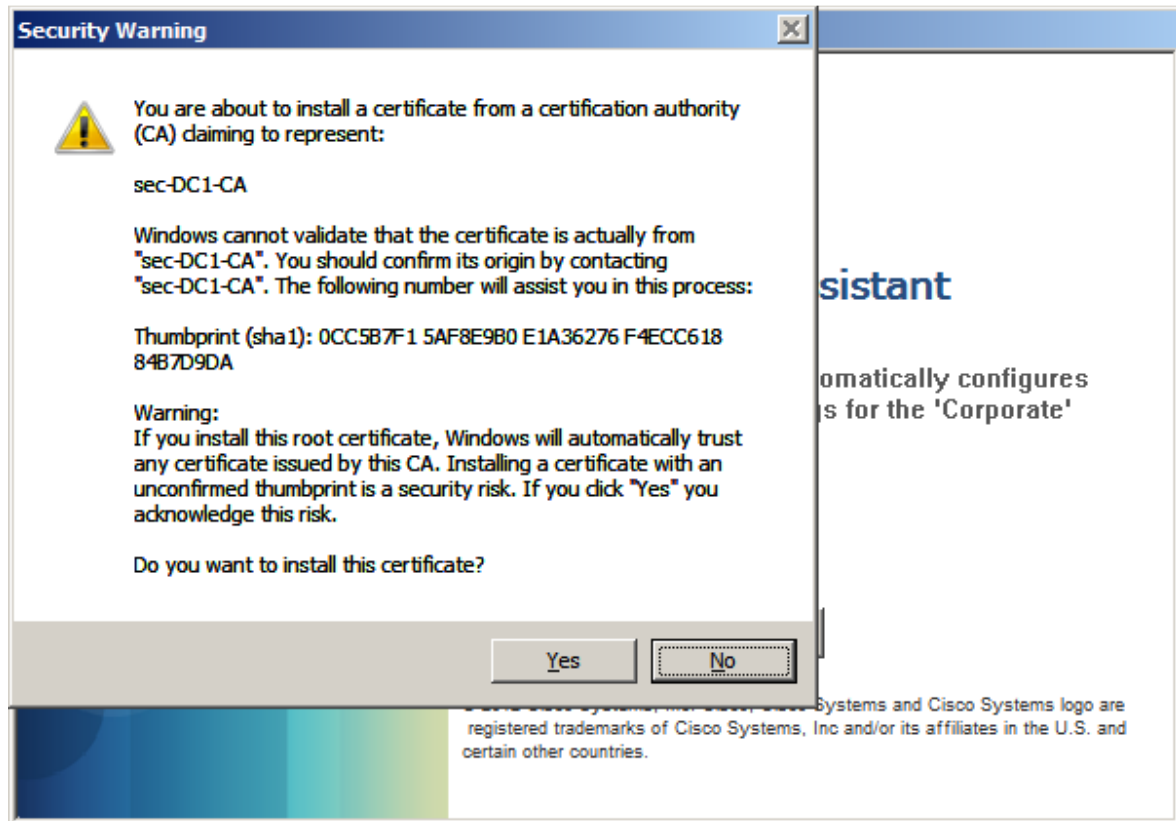
1. After the user clicks 'Register' they are prompted to download and run the Network Setup Assistant, also known as the Native Supplicant Provisioning Wizard (NSP or SPW).



1. The Network Setup Assistant appears. The user may be prompted by browser security warnings.



1. The wizard prompts the user for permission to install the CA certificate chain.

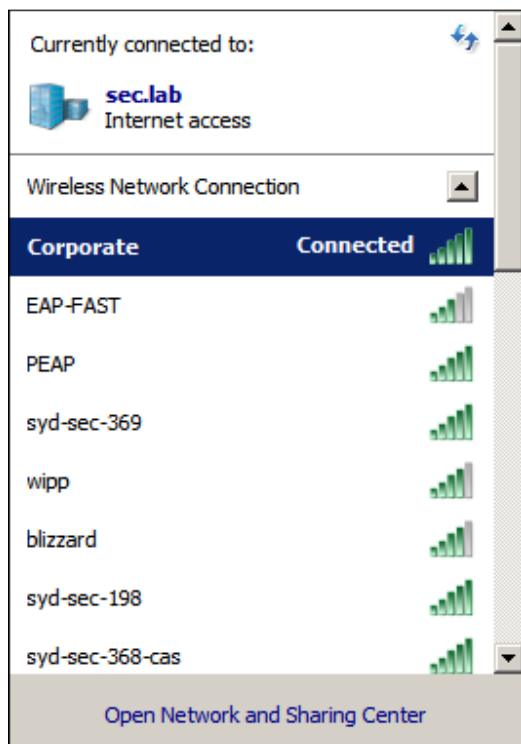


1. The wizard should successfully install the CA certificate chain and provision an identity certificate for the device via SCEP.

If an error occurs, check the spwProfileLog.txt file located in C:\Users\[your username]\AppData\Local\Temp.



1. The wizard will automatically connect the user to the network defined in the Provisioning profile. In our case it is 'Corporate'. The user now has full network access.



1. This is what the final set of authentications/authorizations look like on the ISE dashboard:

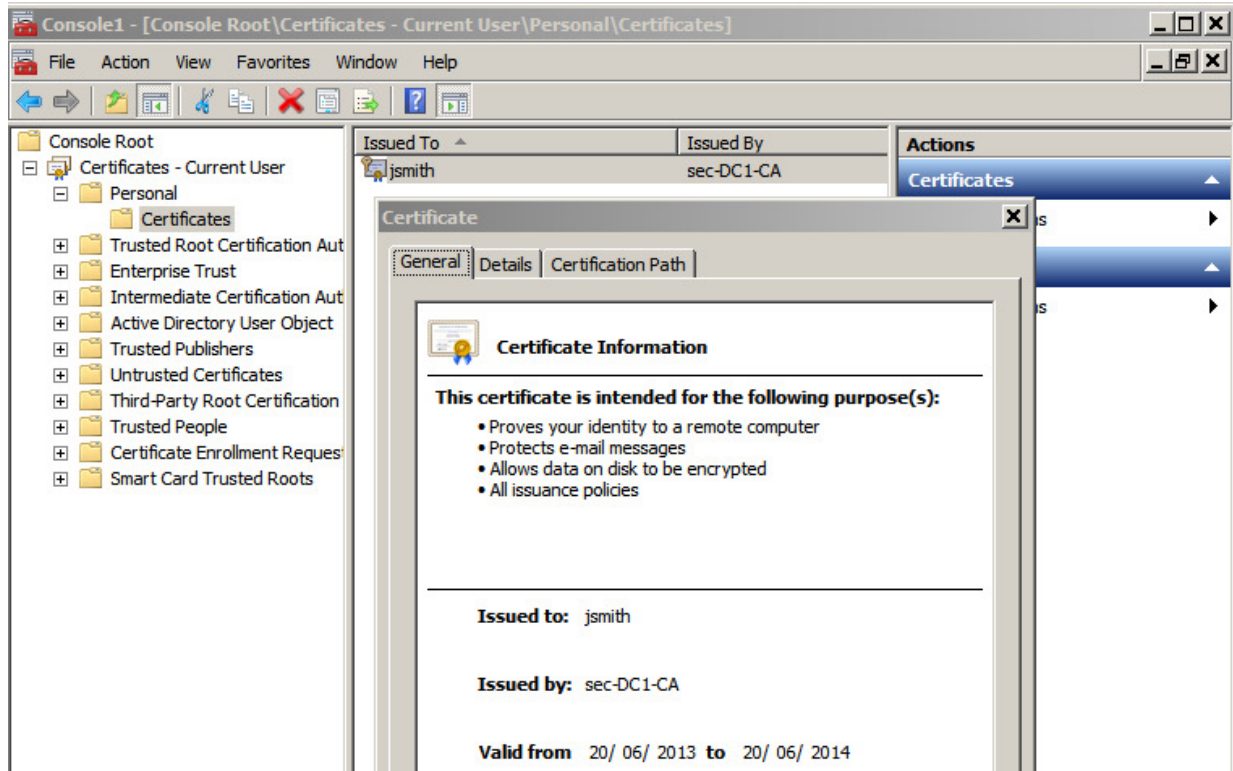
Live Authentications

Add or Remove Columns Refresh Refresh Every

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Jun 20,13 05:23:36.825 PM	✓		jsmith	40:61		WLC2		PermitAccess
Jun 20,13 05:21:02.140 PM	✓		jsmith	00:19:D2:AD:40:61		WLC2		NSP
Jun 20,13 05:20:52.180 PM	✓		jsmith	00:19:D2:AD:40:61		WLC2		NSP
Jun 20,13 05:20:52.130 PM	✓		jsmith	00:19:D2:AD:40:61		WLC2		NSP
Jun 20,13 04:51:04.596 PM	✓		00:19:D2:AD:40:61	00:19:D2:AD:40:61		WLC2		CWA

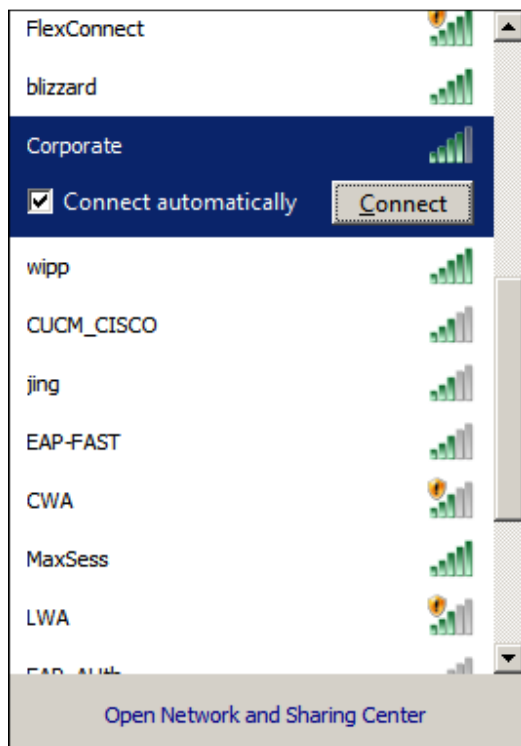
Note how the user proceeds through CWA, NSP and finally PermitAccess.

1. If we open the Windows Management Console (Start > Run > mmc) and then the Certificates snap-in (File > Add/Remove Snap-in) we can see the Identity certificate provisioned by ISE via SCEP:

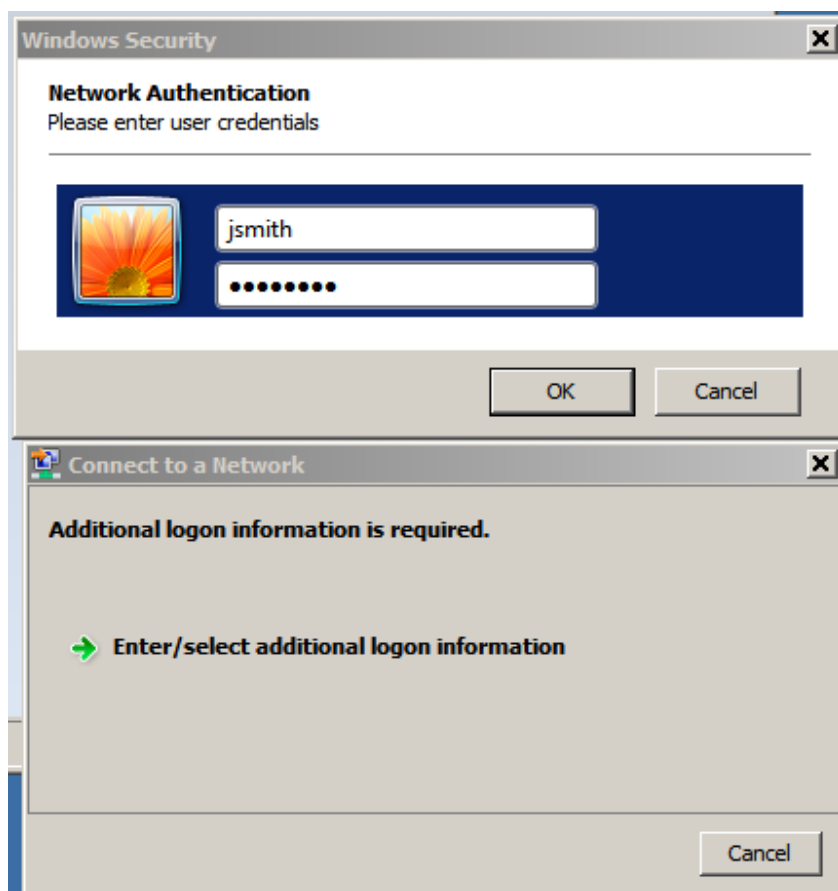


Single SSID Employee

1. The employee connects to WLAN SSID 'Corporate' and is prompted for their Active Directory credentials.



For this example the employee is jsmith.



1. The user goes through the same steps as 5-10 in the section 'Dual SSID Employee' above.
2. This is what the final set of authentications/authorizations look like on the ISE dashboard:

Jun 20,13 05:31:53.619 PM	✓	🔒	jsmith	00:19:D2:AD:40:61	WLC2	PermitAccess
Jun 20,13 05:31:22.350 PM	✓	🔒	jsmith	00:19:D2:AD:40:61	WLC2	NSP




Note how the user proceeds through NSP and PermitAccess.

Single and Dual SSID Contractor

Since our authorization rule permits access to contractors regardless of their Network Access type (Guest Portal, PEAP, etc) they will never go through supplicant provisioning.

Contractors connecting via the open 'Onboarding' or secure 'Corporate' network will immediately proceed to full network access.

Here is how a contractor authentication appears on the ISE dashboard. In this case the contractor has connected to SSID 'Onboarding' and authenticated via the guest portal.

Jun 20,13 05:41:07.854 PM	✓	 jdoe	00:19:D2:AD:40:61	WLC2	PermitAccess	Any,RegisteredDevi...
Jun 20,13 05:40:28.082 PM	✓	 jdoe	00:19:D2:AD:40:61			Any
Jun 20,13 05:39:53.292 PM	✓	 00:19:D2:AD:40:61	00:19:D2:AD:40:61	WLC2	CWA	RegisteredDevices
