Cisco Support Community Presents

Tech-Talk

Deploying Cisco Secure BYOD

With,

Dhiresh Yadav , Brahadesh Srinivasaraghavan & Gautam Bhagwandas

Engineer-Customer Support, GTC- HTTS

July ‘2014

Agenda

- BYOD Introduction
- BYOD Flow: Single SSID and Two SSID
- Device Profiling
- WLC Configuration
- ISE Configuration: Authentication , Authorization and AD Integration
- Deploying Certificate Services
  - Root CA Setup
  - Sub CA Setup
  - ISE SCEP CA Profile and certificate Installation
  - Caveat
- Supplicant Provisioning
- Troubleshooting BYOD

BYOD Introduction

- BYOD or Bring Your Own Device is a concept which allows users to connect, register, and provision their own personal devices onto the corporate network. Devices are evolving so rapidly that it is impractical to pre-approve each and every device by the IT department. It is also somewhat impractical to expect IT organizations to have the same level of support for each and every device that employees may bring to the workplace.

- On-boarding of new devices—should be simple and, ideally, self-service with minimal IT intervention, especially for employee bought devices. This on-boarding does not require any pre-installed software. So this can be used to provide access to guests as well

Devices Involved

- ISE & Backend Servers (directory / CA)
- WLC & Access Points
- Endpoints
    - iOS devices (iPhone/iPad)
    - Android devices
    - Windows laptops
    - Mac OS/X laptops

BYOD Onboarding

With this support for Client devices for secure connection and Mobility, We have two broad subfamilies which exist in this solution:

- One SSID, where EAP-TLS and a weaker authentication mechanisms are allowed, users bring their BYOD, connect with the weaker mechanism and their credentials, register their BYOD then switch to TLS on the same WLAN.

  Use case is large enterprise authorizing BYODs
- 2 SSIDs, where one SSID is open, the other TLS-based. Users bring their BYOD, use webauth to register their device into ISE, then switch to the TLS-based SSID.

  User case is guest in a corporate/secure guest network

Single SSID Wireless BYOD Self Registration

1. User associates to CORPORATE SSID using PEAP.
2. User enters into the supplicant their EMPLOYEE username and password for PEAP authentication.
3. ISE authenticates the user and based on the PEAP method, provides Redirect ACL having Restricted access and the Redirect URL for Device Registration guest page.
4. User opens a browser and is redirected to the Device Registration guest page.
5. MAC address is pre-populated in the Device Registration guest page for DeviceID and the user enters in a description and accepts the AUP = Acceptable User Policy.
6. The Device is identified as IPAD/Android/Windows and Provision Profile.
7. User selects accept and begins downloading and installing the supplicant provisioning wizard (SPW).
8. Device's supplicant is provisioned and sends CSR to the ISE which in turn forwards it to the CA Server using SCEP and all the Certificates are Provisioned.
9. CoA session terminate triggers and device re-associates to the CORP SSID and authenticates via EAP-TLS.

Dual SSID Wireless BYOD Self Registration

There are 2 SSIDs, one that is OPEN for Guest/BYOD and one that is authenticating for CORPORATE access.

1. User associates to Guest SSID configured.
2. User opens a browser and is redirected to the ISE CWA Guest portal.
3. User enters their username and password in the Guest portal.
4. ISE authenticates the user and they are directed to the Device Registration guest page.
5. MAC address is pre-populated in the Device Registration guest page for DeviceID and the user enters in a description.
6. User selects ‘Accept Registration”.
7. Device is identified (IPAD/Windows) and begins downloading and installing the supplicant provisioning wizard (SPW).
8. User’s device supplicant is provisioned , CSR is generated on the Client and forwarded to the ISE which in turn is forwarded to the CA server and any certificates are provisioned.
9. COA session terminate happens.
10. User associates to the CORPORATE SSID and authenticates via EAP-TLS.

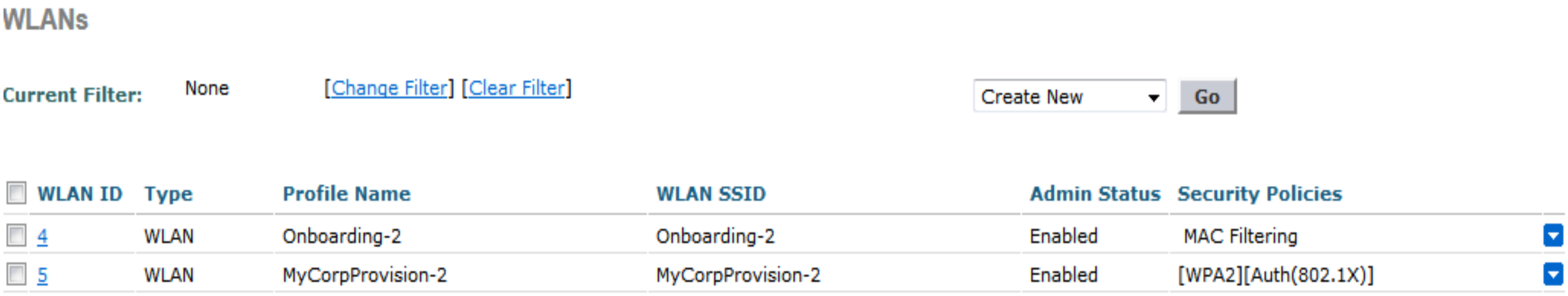
Device Profiling Introduction

- Profiling means determining a device’s type from the information received from the device during its connection to the network..
- A new task (NAC Device Profiler task) has been defined on the WLC which enables it to act as a collector for device profiling and interact with the DHCP thread along with the RADIUS accounting task running on the WLC. WLC acts as a Collector and ISE as an Analyzer.
- The WLC receives a copy of the DHCP_REQUEST packet sent from the DHCP thread and parses the DHCP packet for two DHCP Options:
    1. Option 12 - HostName of the client
    2. Option 60 - The Vendor Class Identifier
- Once this information is obtained from the DHCP_REQUEST, a message is formed by the WLC with these Option fields and is sent to the RADIUS accounting thread. This is then transmitted to the ISE in the form of an interim accounting message.

Packet Flow

1. Client sends a DHCP_REQUEST packet.
2. Packet is intercepted by WLC, and a copy is made & sent to the NAC Device Profiler task in the WLC.
3. The WLC acting as the Collector, parses the packets and obtains the following fields from the DHCP packet:
   - HostName of the client (option 12)
   - Vendor Class Identifier (option 60)
4. This information is stored on a local database – AVL Tree.
5. Once the client enters the RUN state on the WLC, the information is sent to the ISE in the form of a RADIUS Accounting message.
6. The ISE (Analyzer) uses the RADIUS Accounting message to ‘profile’ the device.

WLAN Configuration for OPEN SSID - Dual SSID Setup

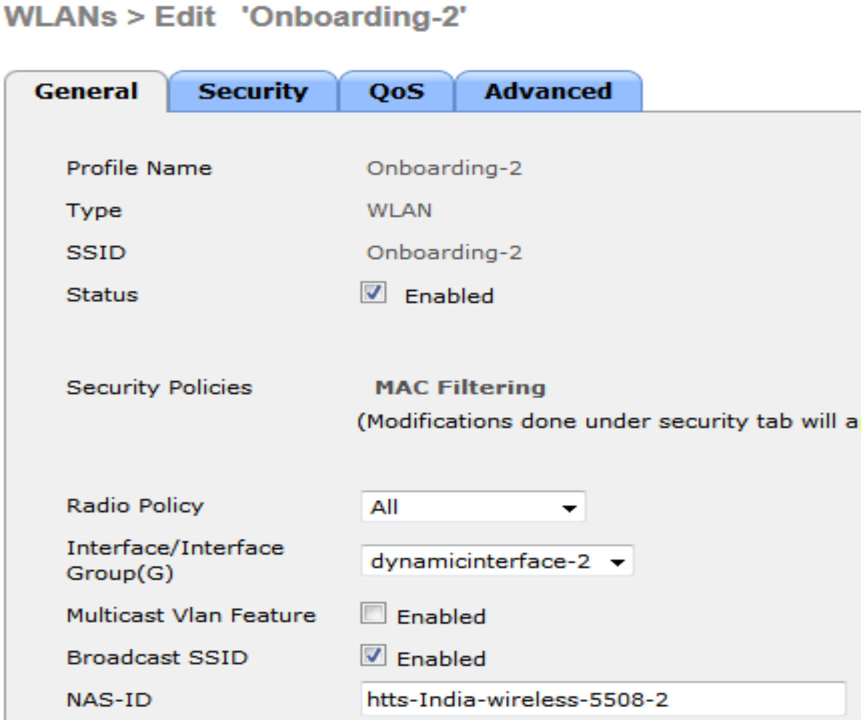


WLANs

Current Filter: None [Change Filter] [Clear Filter]

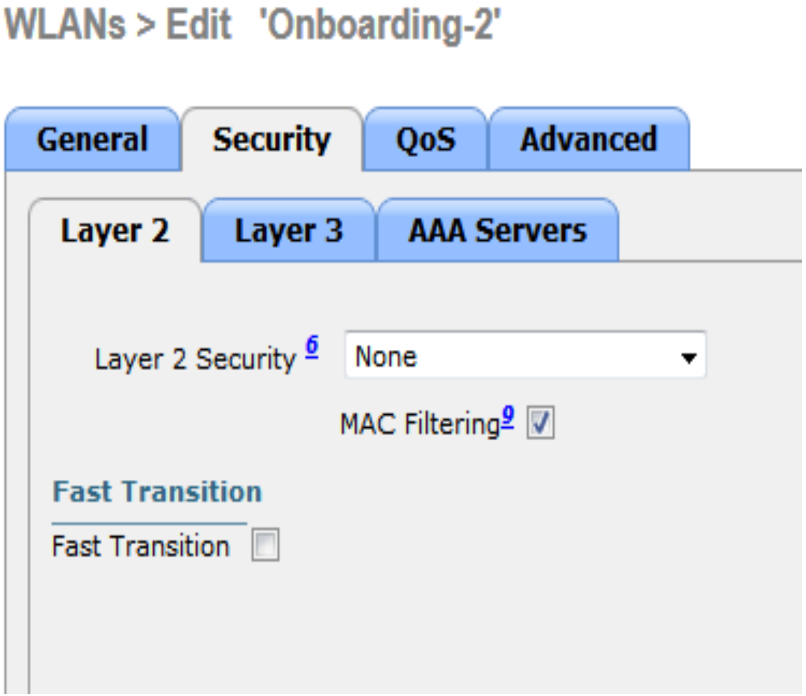
□	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
□	4	WLAN	Onboarding-2	Onboarding-2	Enabled	MAC Filtering	▾
□	5	WLAN	MyCorpProvision-2	MyCorpProvision-2	Enabled	[WPA2][Auth(802.1X)]	▾

WLAN Configuration-Open SSID



WLANs > Edit 'Onboarding-2'

Profile Name	Onboarding-2
Type	WLAN
SSID	Onboarding-2
Status	☑ Enabled
Security Policies	**MAC Filtering** (Modifications done under security tab will a
Radio Policy	All
Interface/Interface Group(G)	dynamicinterface-2
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	htts-India-wireless-5508-2



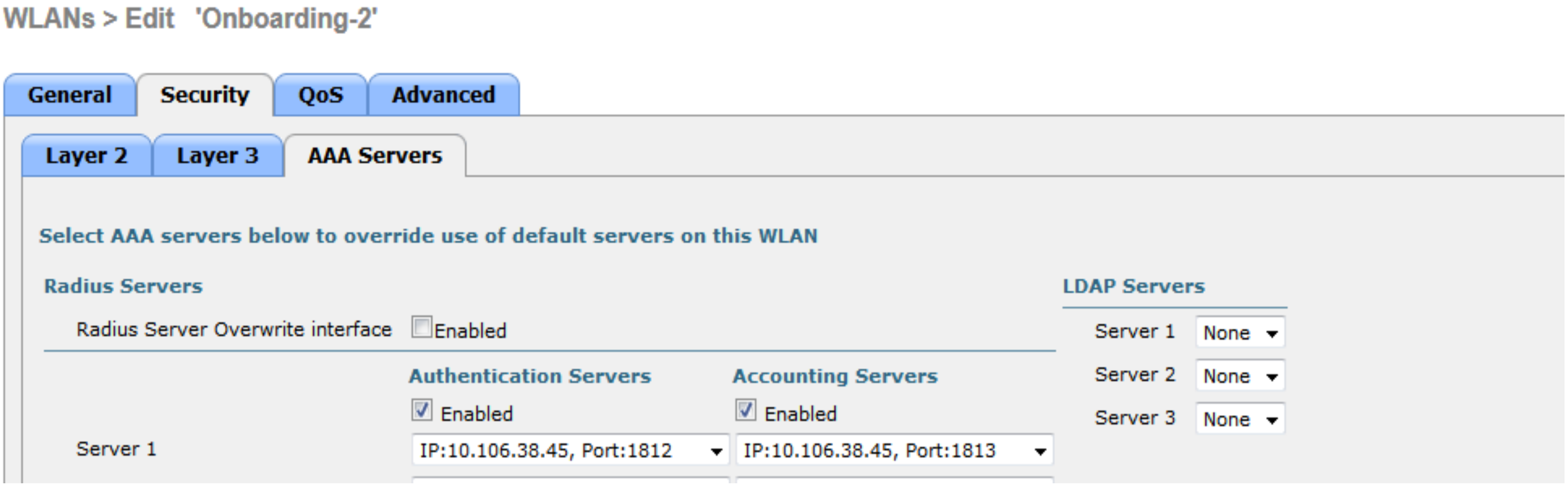
WLANs > Edit 'Onboarding-2'

Layer 2 Security [6]	None
MAC Filtering[9]	☑

Fast Transition

Fast Transition	□

WLAN Configuration –AAA



WLANs > Edit 'Onboarding-2'

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

Radius Servers

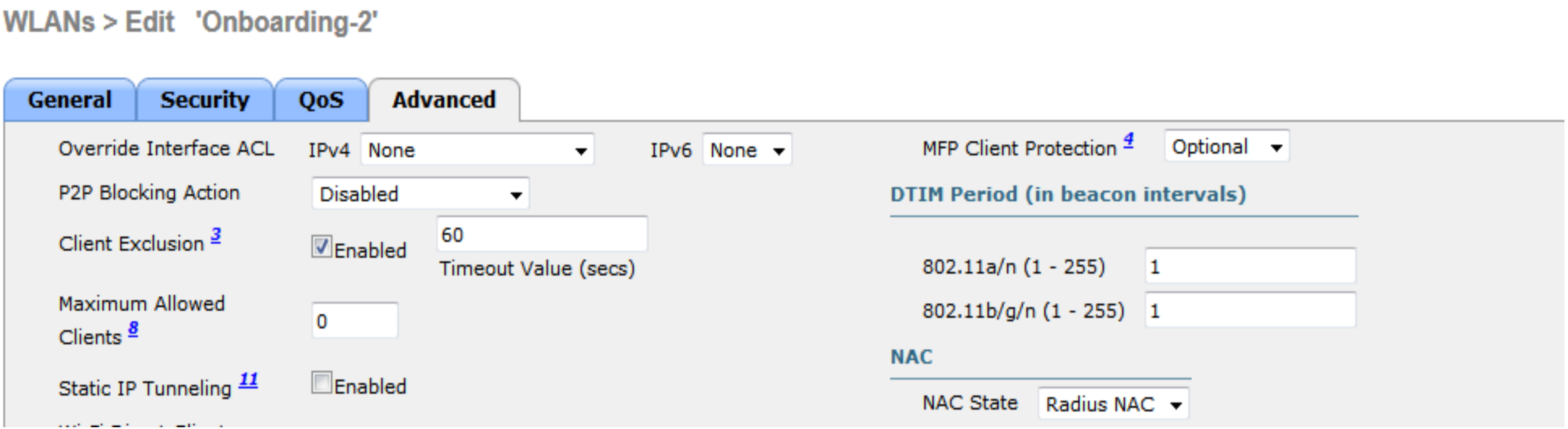
Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.106.38.45, Port:1812	IP:10.106.38.45, Port:1813

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

WLAN Configuration-Radius NAC



WLANs > Edit 'Onboarding-2'

Override Interface ACL IPv4 None IPv6 None

P2P Blocking Action Disabled

Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients [8] 0

Static IP Tunneling [11] □ Enabled

MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)

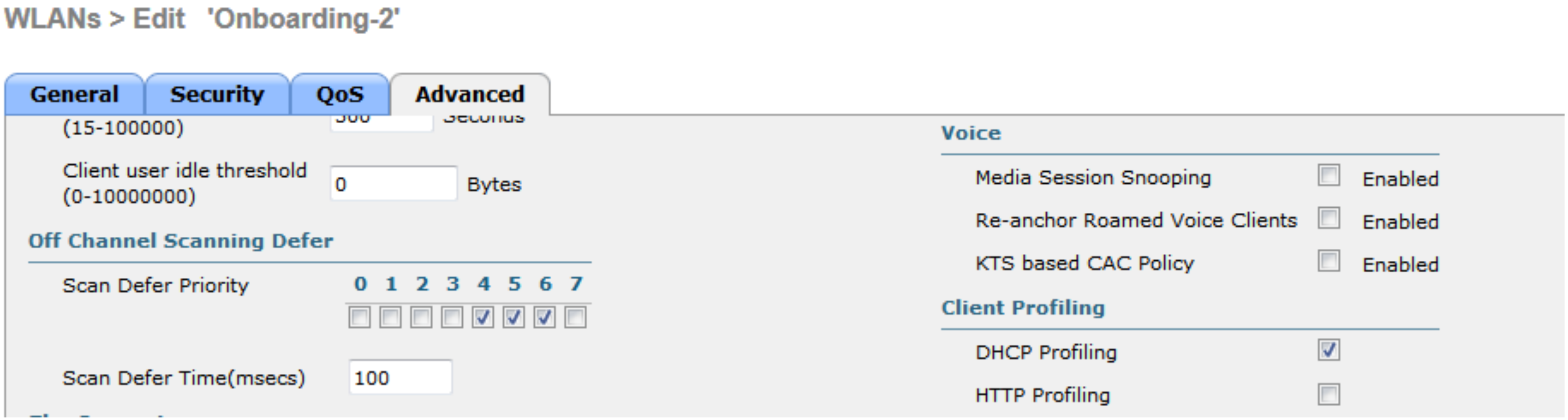
802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State Radius NAC

WLAN Configuration - Profiling



WLANs > Edit 'Onboarding-2'

(15-100000) 300 Seconds

Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority

0	1	2	3	4	5	6	7
□	□	□	□	☑	☑	☑	□

Scan Defer Time(msecs) 100

Voice

Media Session Snooping □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

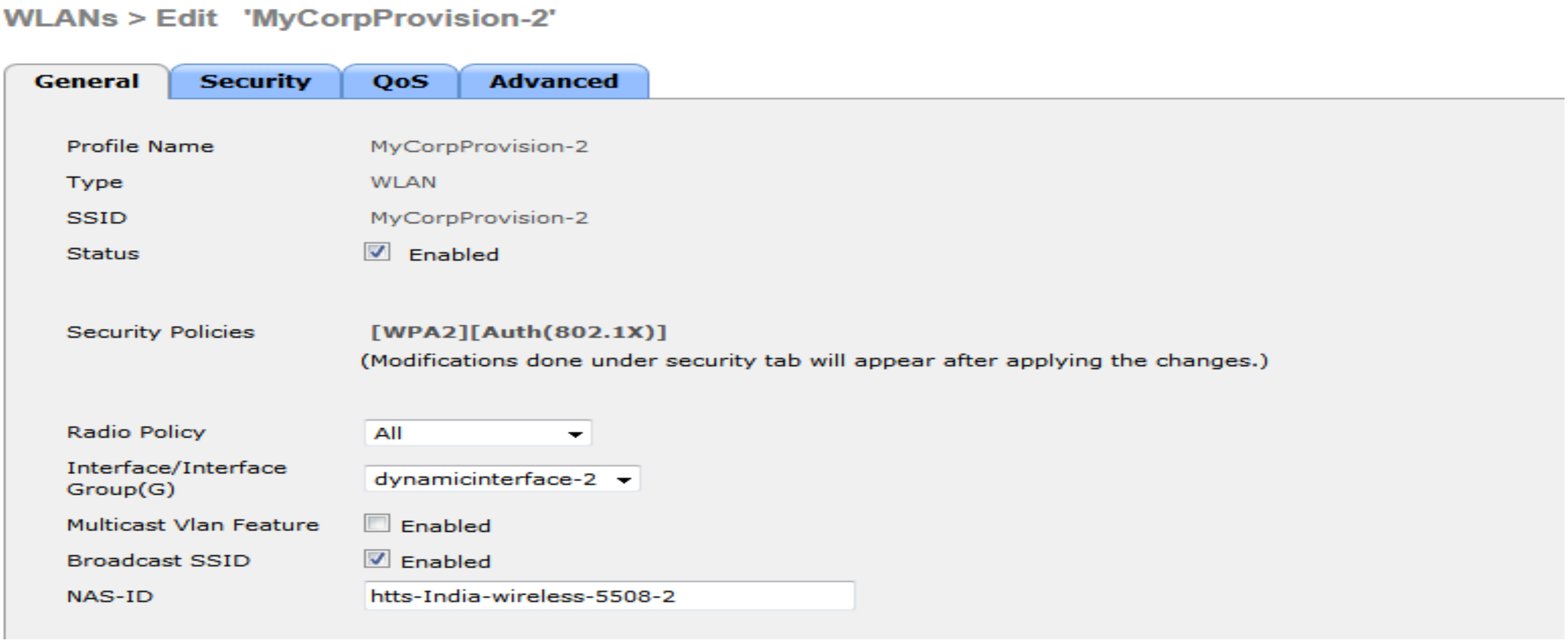
KTS based CAC Policy □ Enabled

Client Profiling

DHCP Profiling ☑

HTTP Profiling □

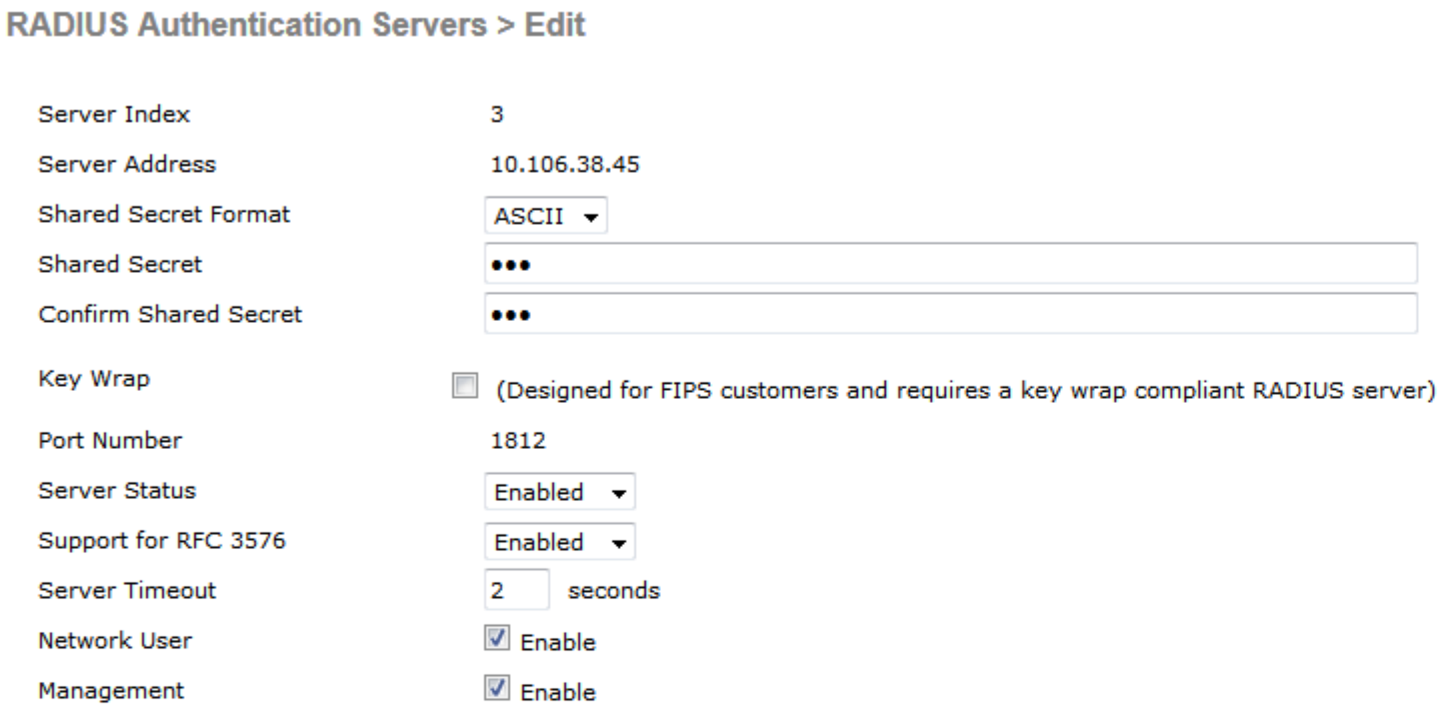
WLAN Configuration- 802.1x SSID



WLANs > Edit 'MyCorpProvision-2'

Profile Name	MyCorpProvision-2
Type	WLAN
SSID	MyCorpProvision-2
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	dynamicinterface-2
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	htts-India-wireless-5508-2

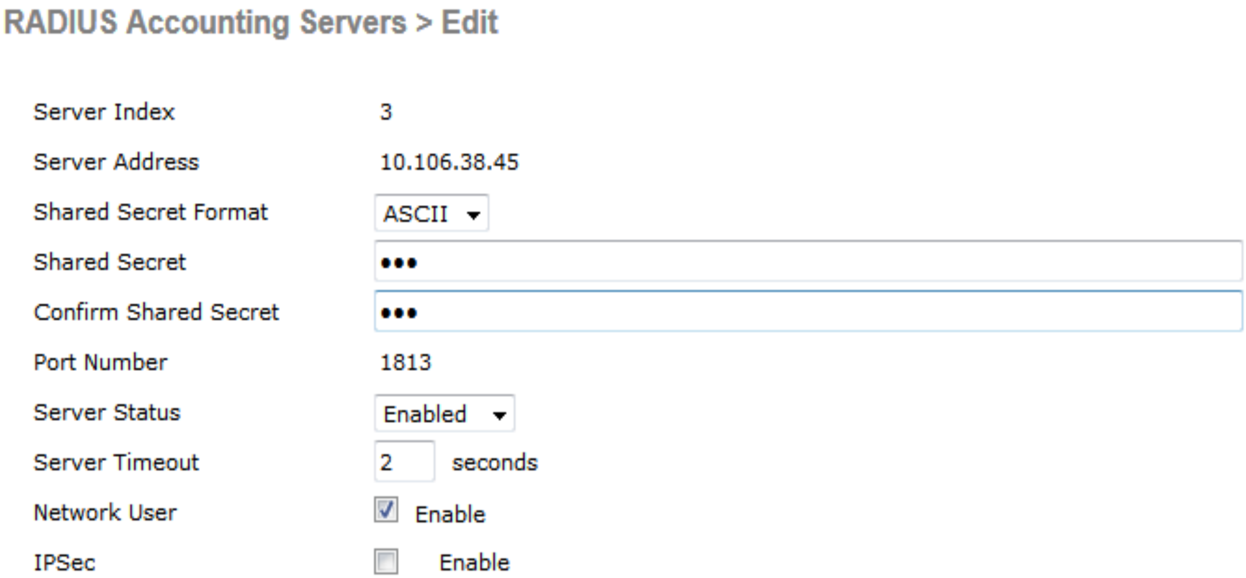
Radius Authentication Server



RADIUS Authentication Servers > Edit

Server Index	3
Server Address	10.106.38.45
Shared Secret Format	ASCII ▾
Shared Secret	●●●
Confirm Shared Secret	●●●
Key Wrap	☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled ▾
Support for RFC 3576	Enabled ▾
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable

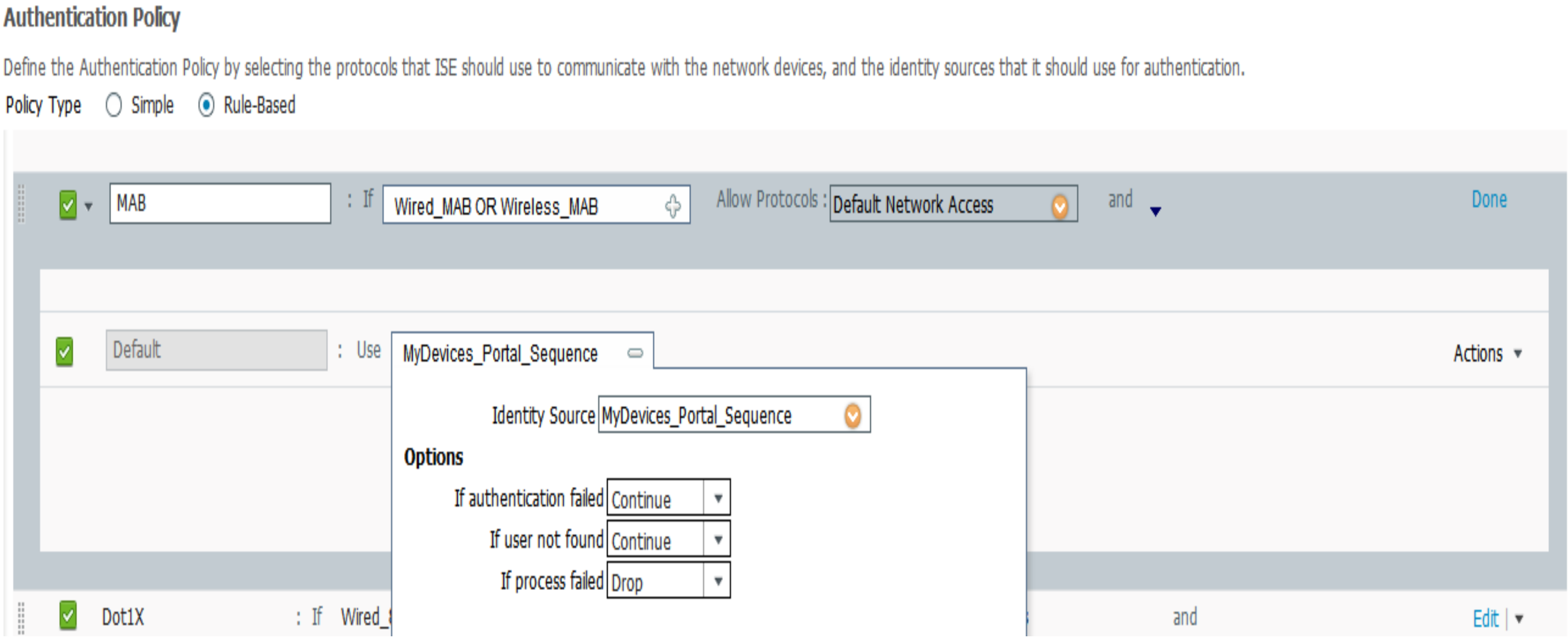
Radius Accounting Server



RADIUS Accounting Servers > Edit

Server Index	3
Server Address	10.106.38.45
Shared Secret Format	ASCII ▾
Shared Secret	•••
Confirm Shared Secret	•••
Port Number	1813
Server Status	Enabled ▾
Server Timeout	2 seconds
Network User	☑ Enable
IPSec	□ Enable

Two SSID MAB Policy



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 OR Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : Use MyDevices_Portal_Sequence

Identity Source MyDevices_Portal_Sequence

Options

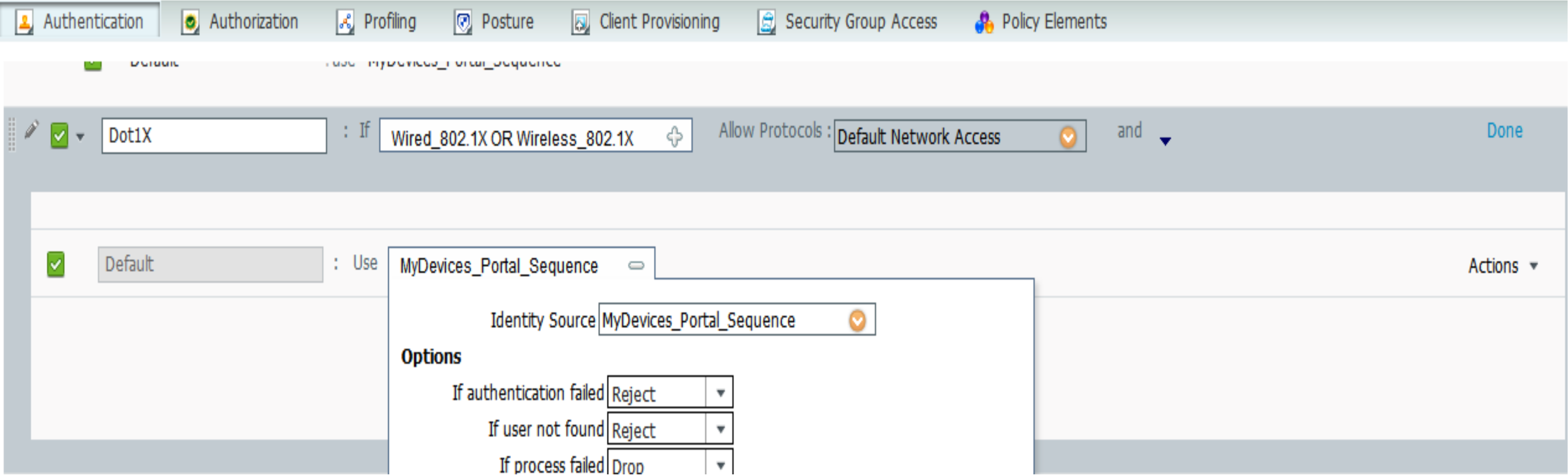
If authentication failed Continue

If user not found Continue

If process failed Drop

☑ Dot1X : If Wired_ and

Single SSID DOT1X Policy



Default : use MyDevices_Portal_Sequence

☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

☑ Default : Use MyDevices_Portal_Sequence

Identity Source MyDevices_Portal_Sequence

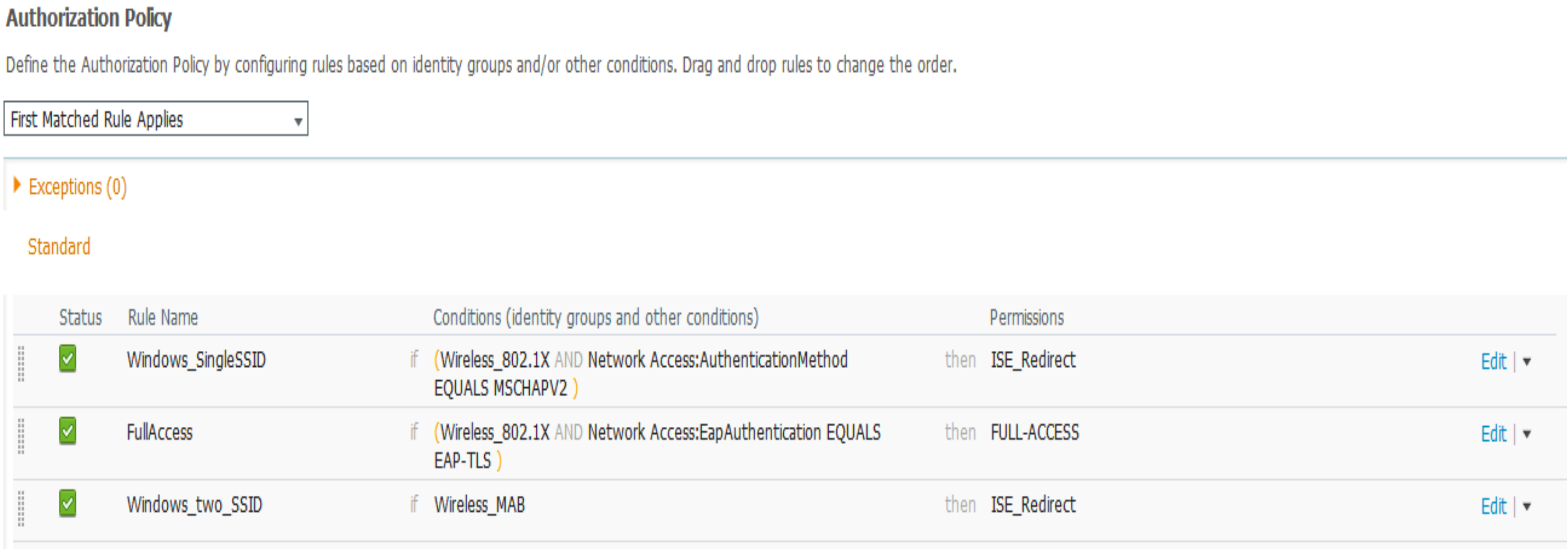
Options

If authentication failed Reject

If user not found Reject

If process failed Drop

Authorization Policy



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

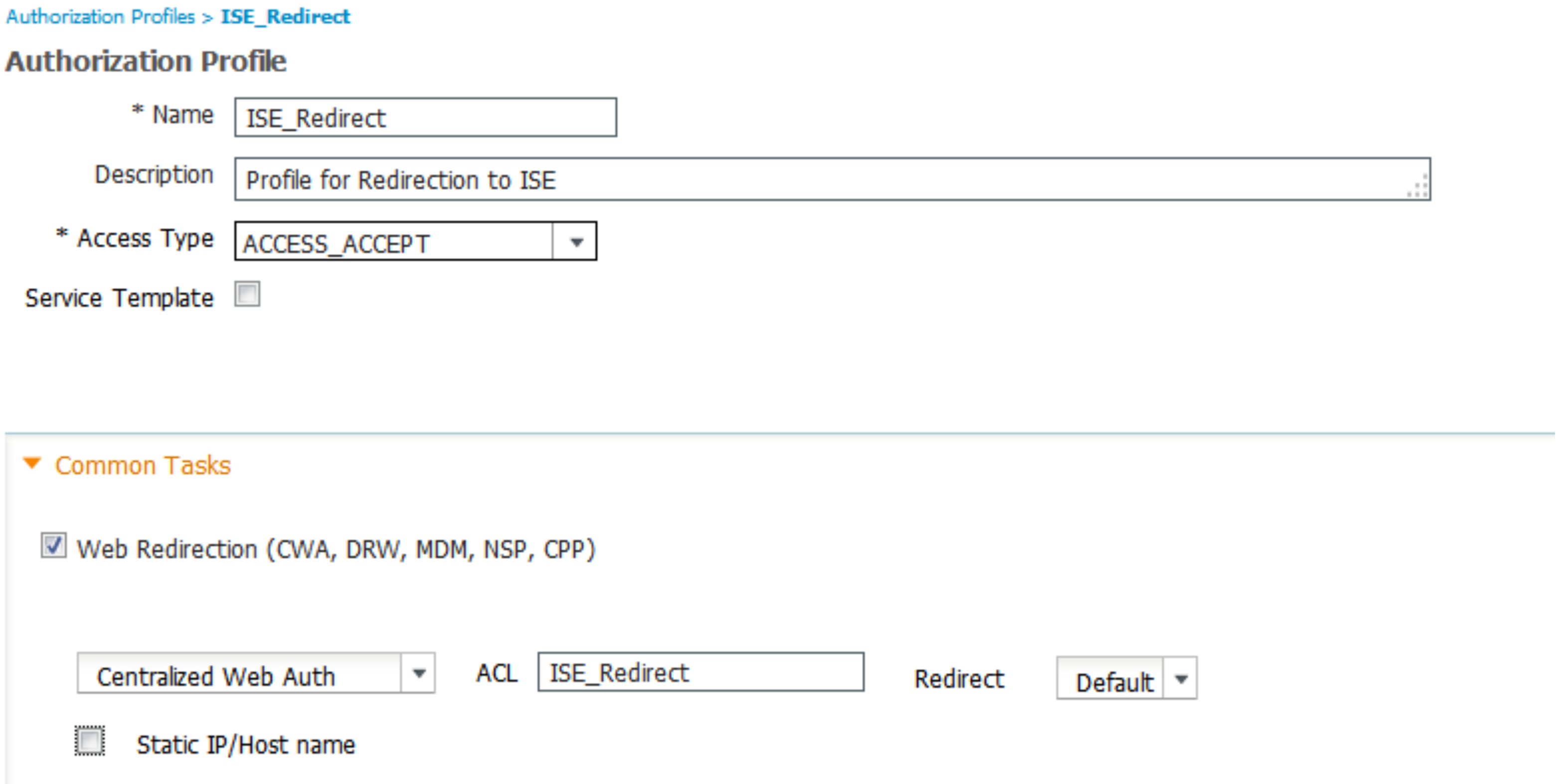
First Matched Rule Applies ▾

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Windows_SingleSSID	if	(Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then	ISE_Redirect	Edit | ▾
✓	FullAccess	if	(Wireless_802.1X AND Network Access:EapAuthentication EQUALS EAP-TLS)	then	FULL-ACCESS	Edit | ▾
✓	Windows_two_SSID	if	Wireless_MAB	then	ISE_Redirect	Edit | ▾

Authorization Profile for ISE Redirect



Authorization Profiles > **ISE_Redirect**

Authorization Profile

* Name: ISE_Redirect

Description: Profile for Redirection to ISE

* Access Type: ACCESS_ACCEPT ▾

Service Template: □

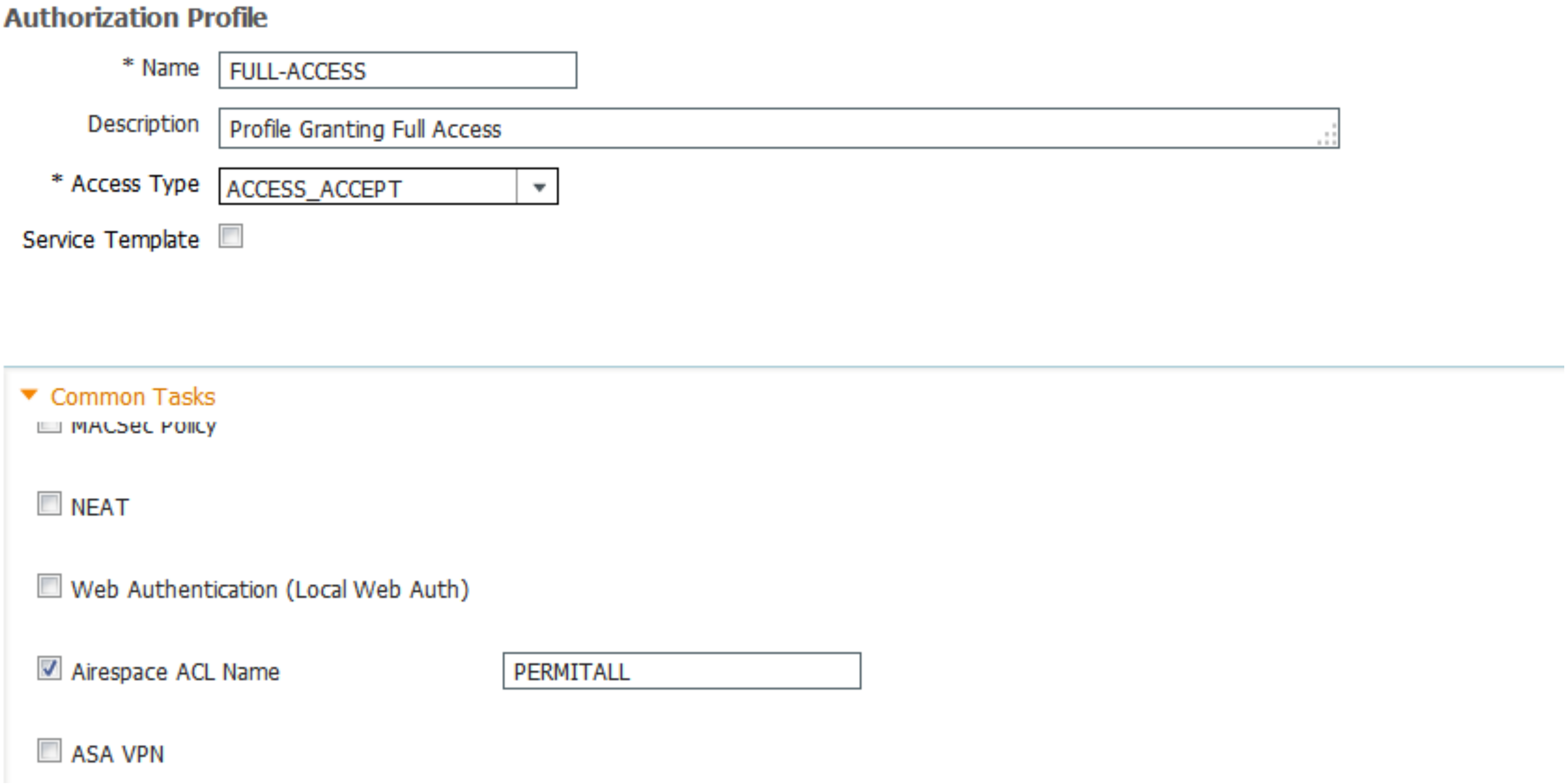
▾ Common Tasks

☑ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Centralized Web Auth ▾ ACL: ISE_Redirect Redirect: Default ▾

□ Static IP/Host name

Authorization Profile for full access



Authorization Profile

* Name	FULL-ACCESS
Description	Profile Granting Full Access
* Access Type	ACCESS_ACCEPT
Service Template	□

▼ Common Tasks

□ MACsec Policy

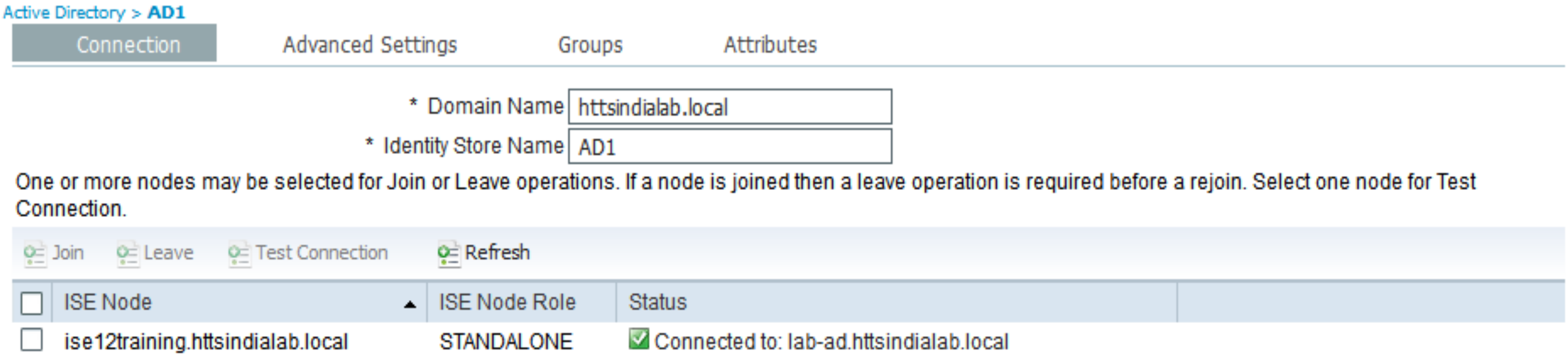
□ NEAT

□ Web Authentication (Local Web Auth)

☑ Airspace ACL Name PERMITALL

□ ASA VPN

AD Integration



* Domain Name: httsindialab.local

* Identity Store Name: AD1

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.

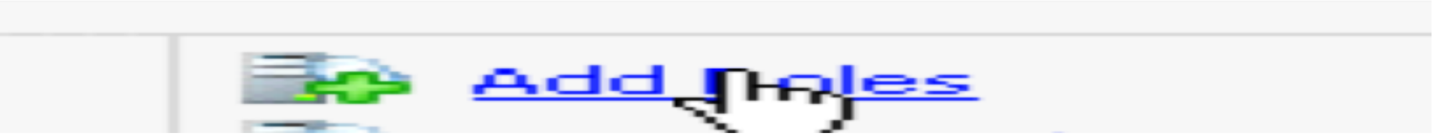
□	ISE Node	ISE Node Role	Status
□	ise12training.httsindialab.local	STANDALONE	✓ Connected to: lab-ad.httsindialab.local

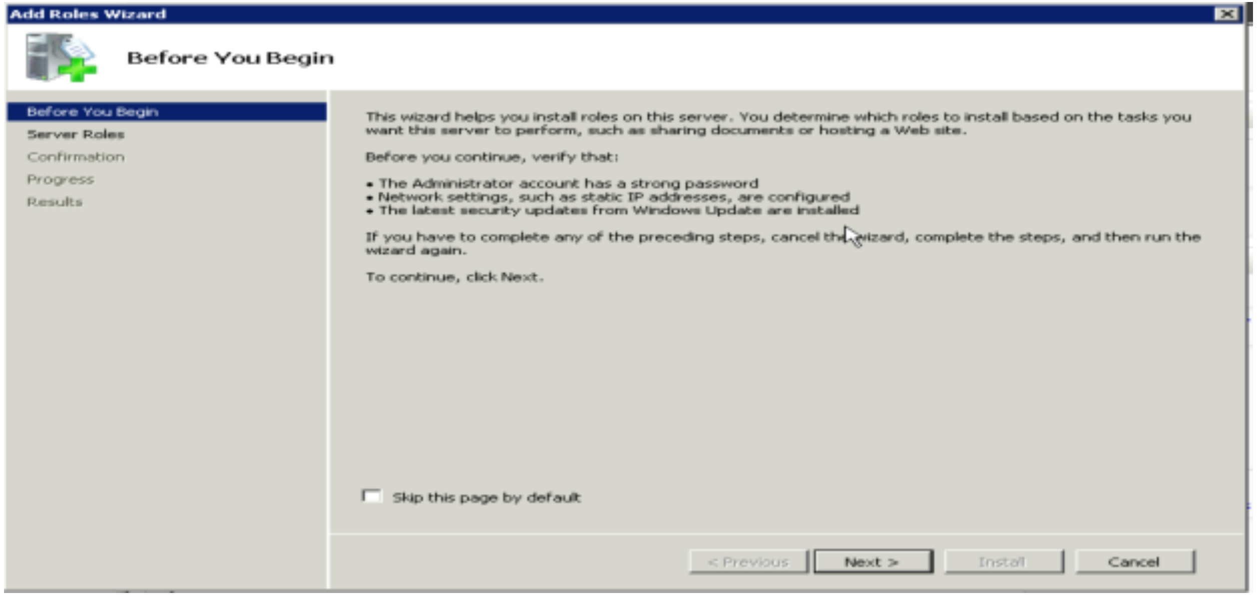
Deploying Certificate Services

Root CA Setup

Root CA - Installation

Go to Server Manager→Add Roles Wizard





This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

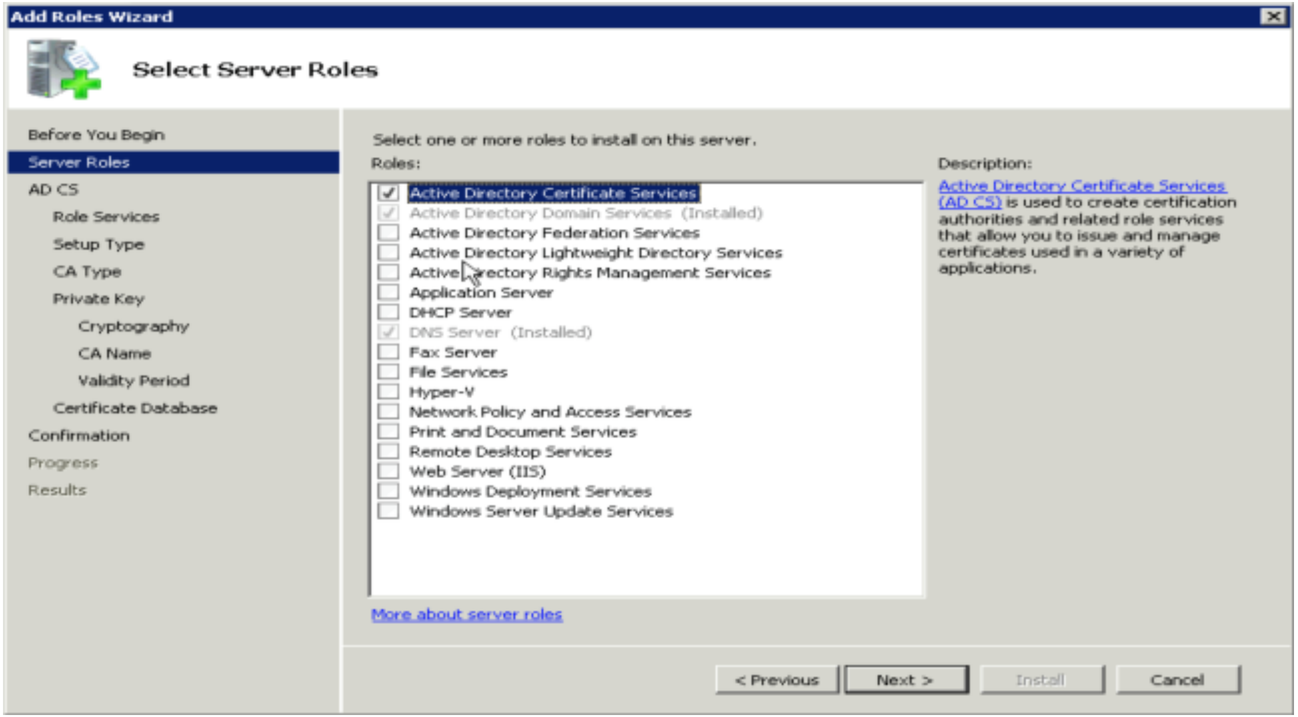
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Root CA – Installation Contd

Choose Active Directory Certificate services



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

Roles:

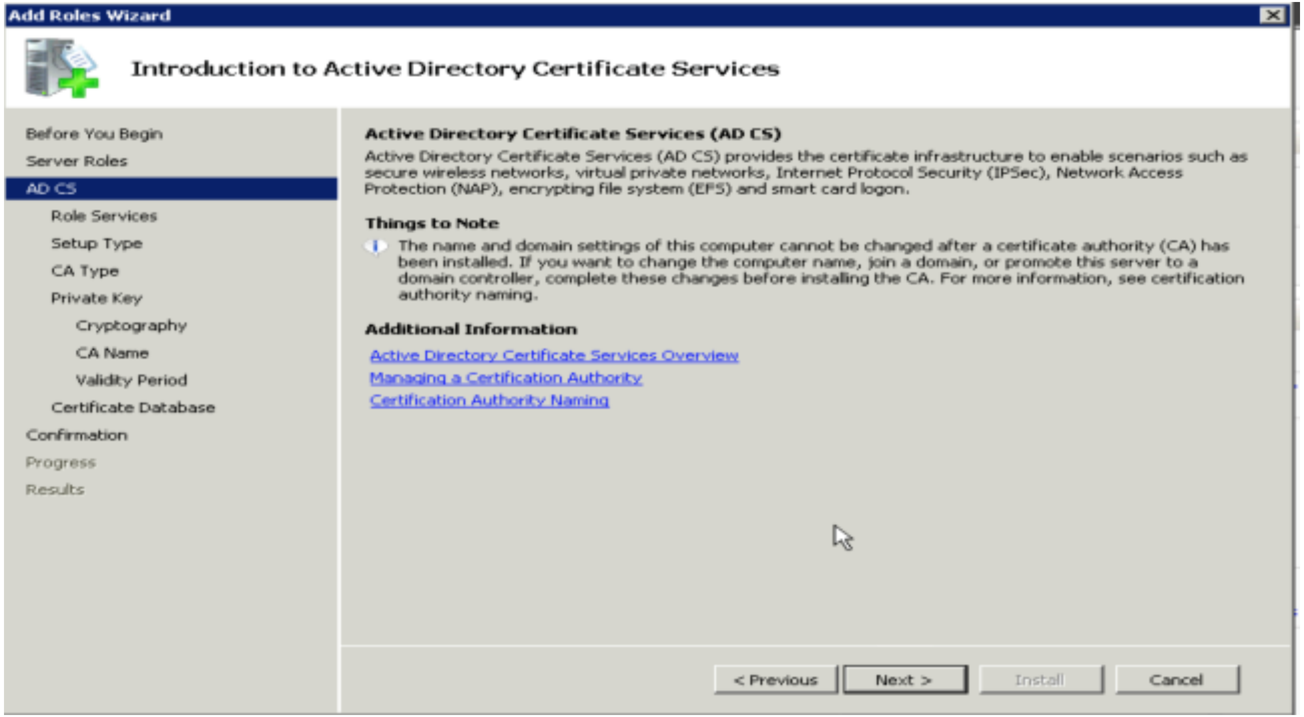
- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

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.

More about server roles

Root CA - Installation



Introduction to Active Directory Certificate Services

Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card logon.

Things to Note

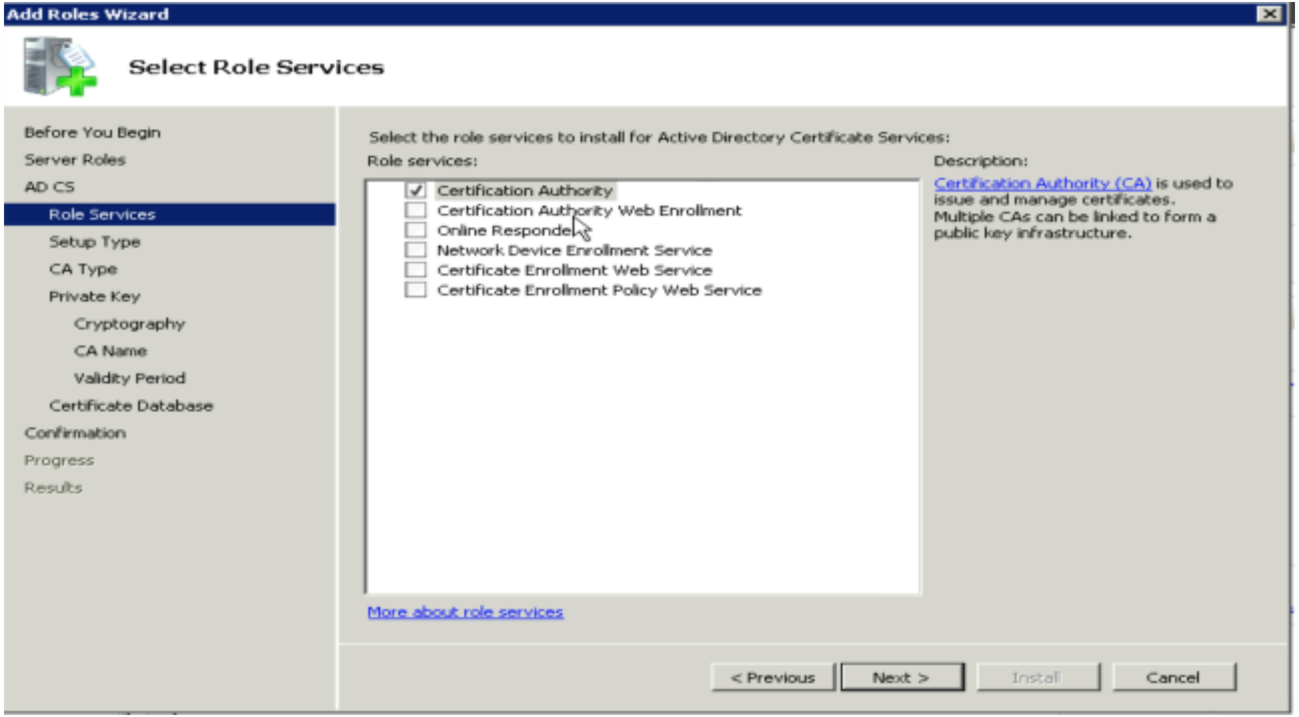
The name and domain settings of this computer cannot be changed after a certificate authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Additional Information

Active Directory Certificate Services Overview
Managing a Certification Authority
Certification Authority Naming

Root CA - Installation

Select the first component – Certificate Authority



Select Role Services

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

Role services:

- ☑ Certification Authority
- □ Certification Authority Web Enrollment
- □ Online Responder
- □ Network Device Enrollment Service
- □ Certificate Enrollment Web Service
- □ Certificate Enrollment Policy Web Service

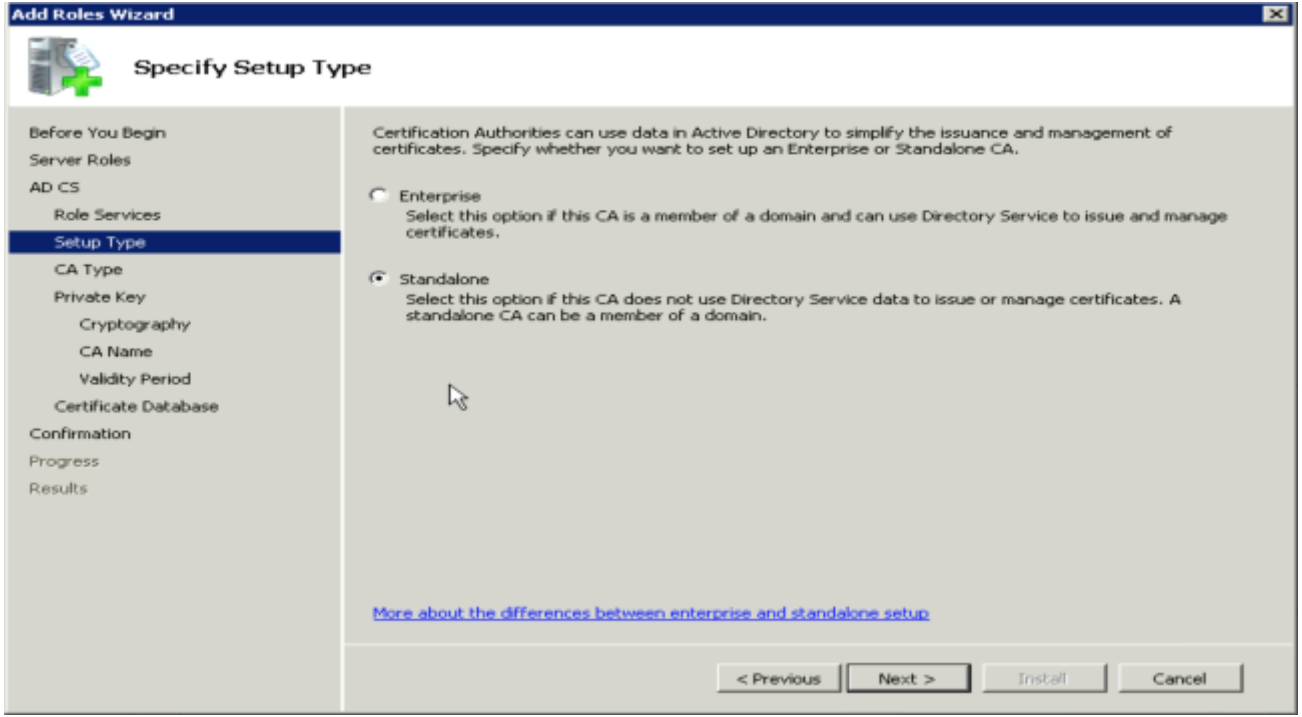
Description:

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

Root CA – Installation Contd

Choose standalone



Add Roles Wizard

Specify Setup Type

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

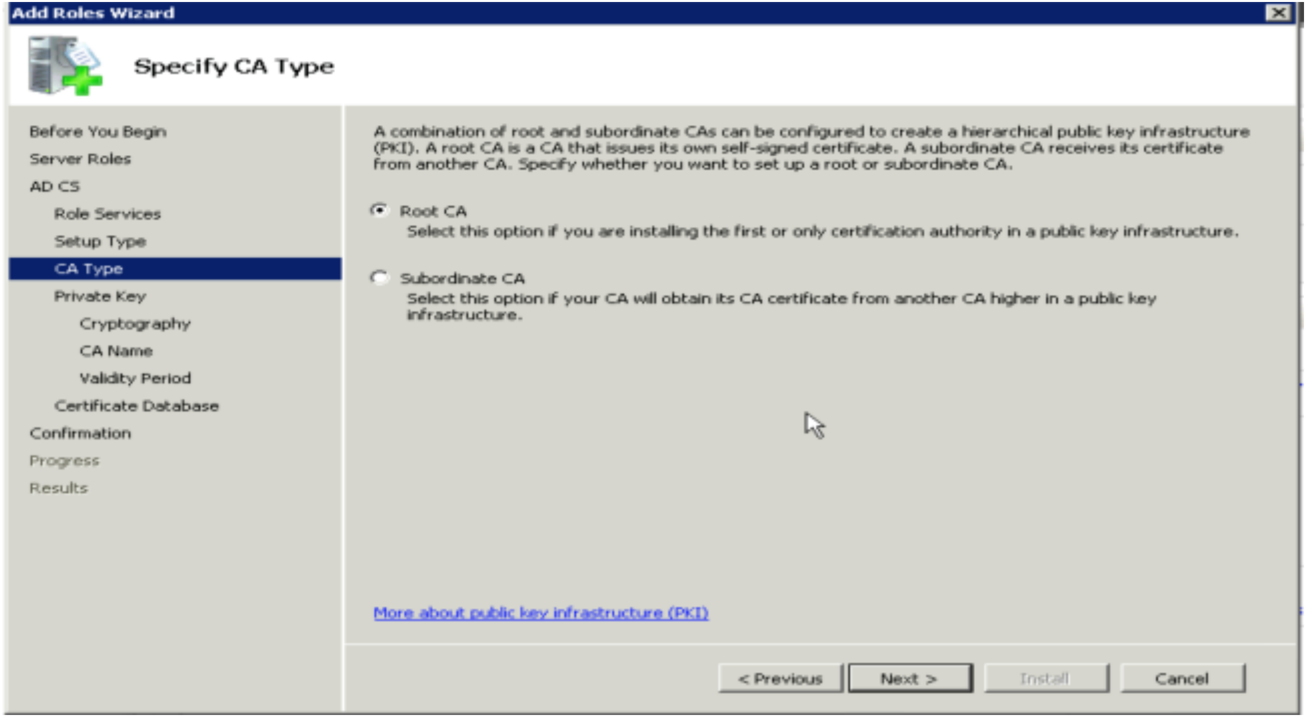
○ Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

● Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

More about the differences between enterprise and standalone setup

Root CA – Installation Contd

Choose Root CA



Add Roles Wizard

Specify CA Type

- Before You Begin
- Server Roles
- AD CS
  - Role Services
  - Setup Type
  - CA Type
  - Private Key
    - Cryptography
    - CA Name
    - Validity Period
  - Certificate Database
- Confirmation
- Progress
- Results

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

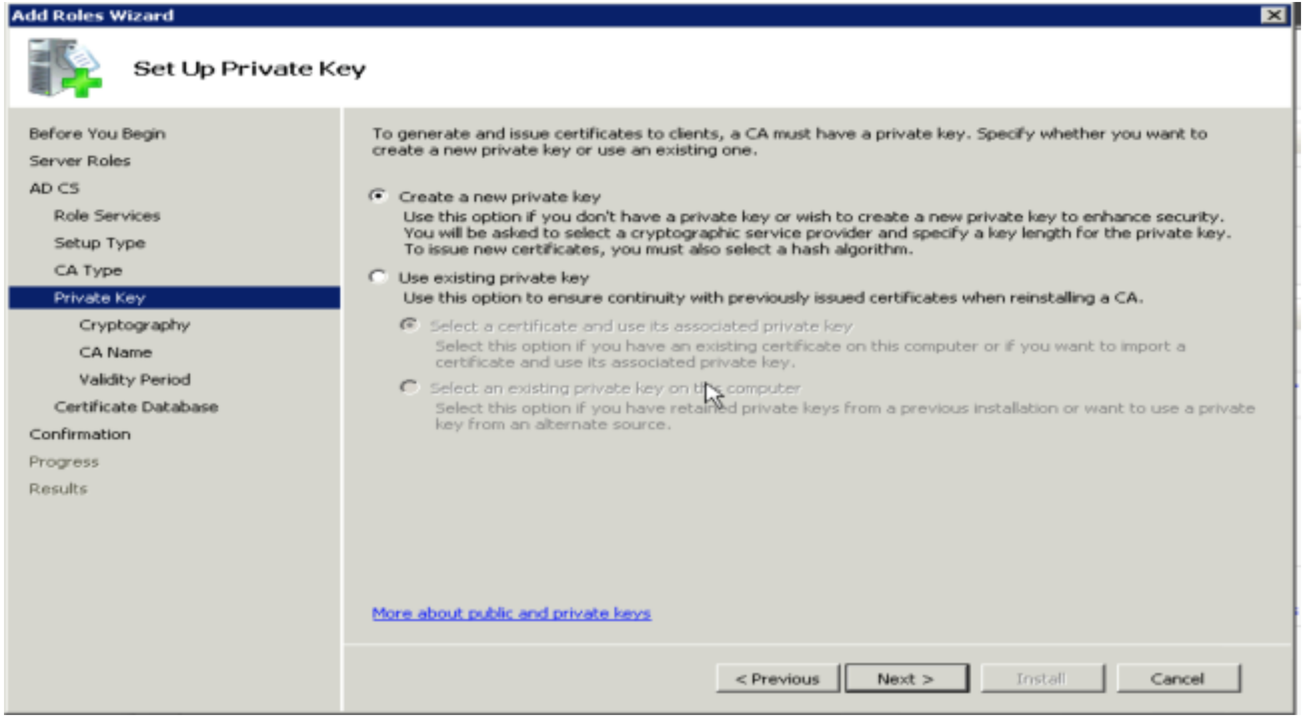
● Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

○ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

More about public key infrastructure (PKI)

Root CA – Installation Contd

Choose Create a new private key



To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key

Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key

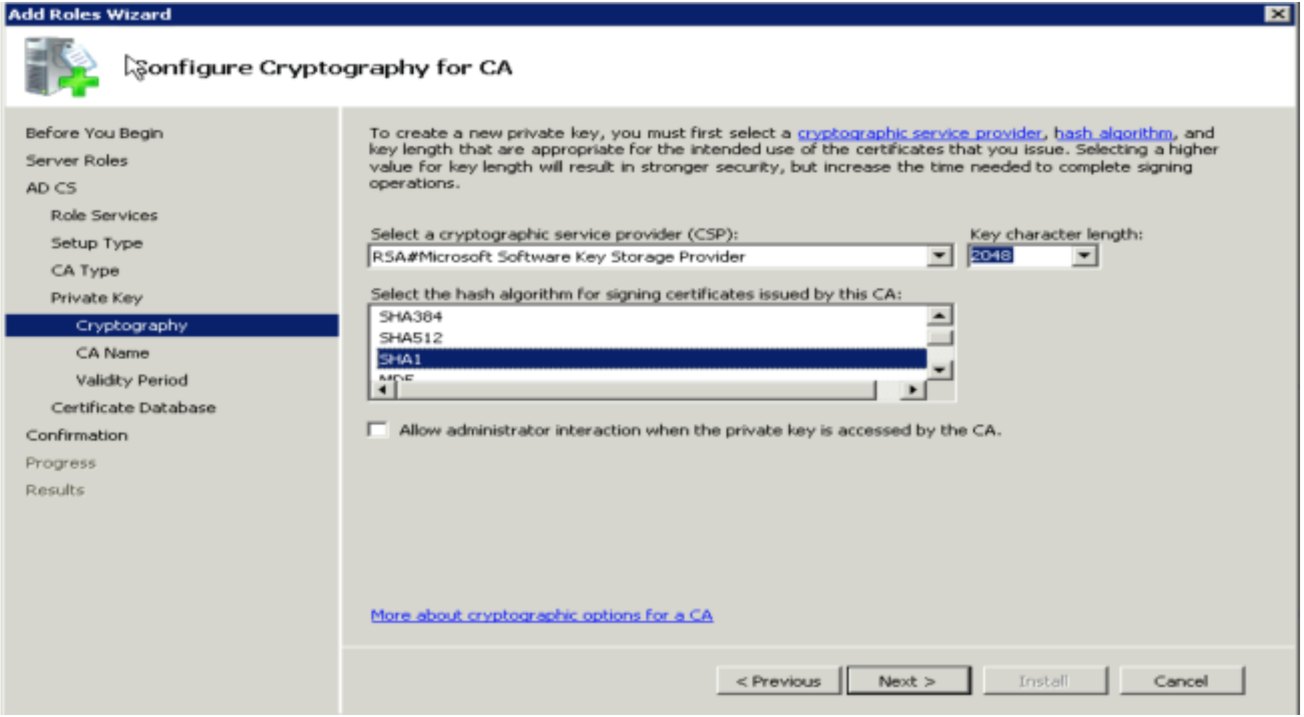
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about public and private keys

Root CA – Installation Contd



Configure Cryptography for CA

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

Key character length: 2048

Select the hash algorithm for signing certificates issued by this CA:

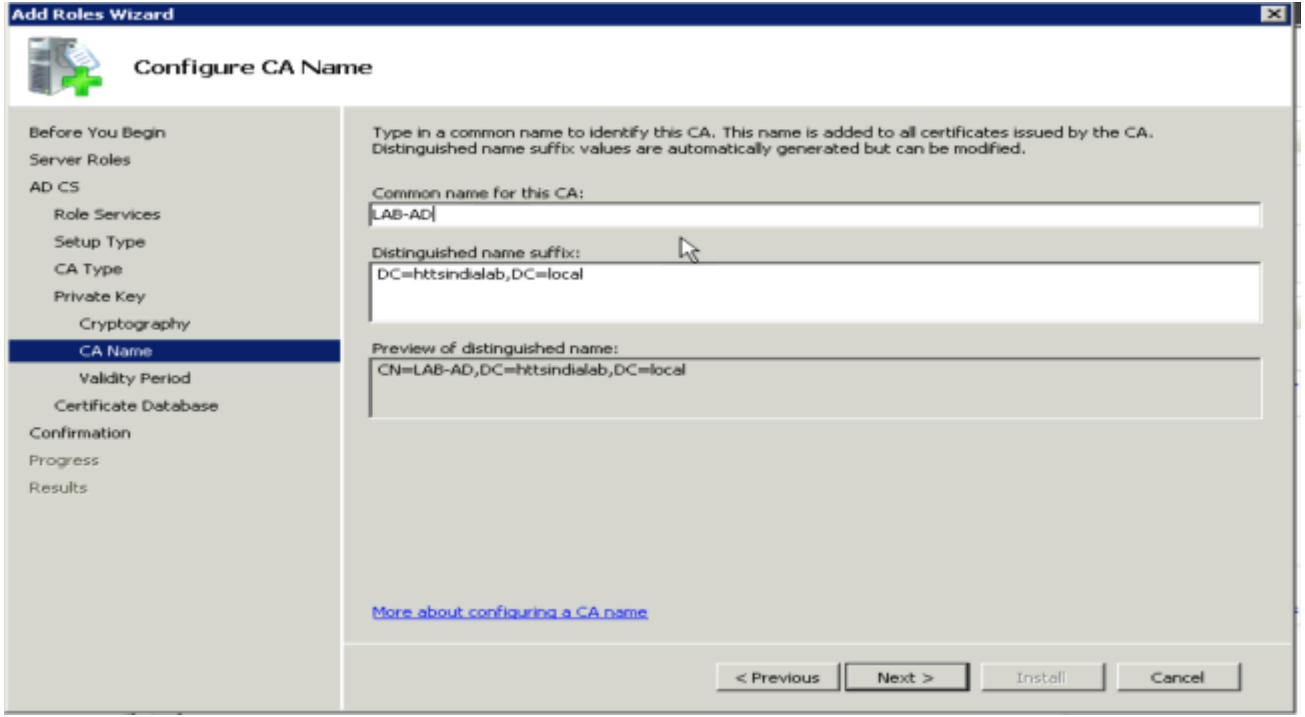
SHA384
SHA512
SHA1
MDE

□ Allow administrator interaction when the private key is accessed by the CA.

More about cryptographic options for a CA

Root CA – Installation Contd

Common Name can be NETBIOS name



Configure CA Name

Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
LAB-AD

Distinguished name suffix:
DC=httsindialab,DC=local

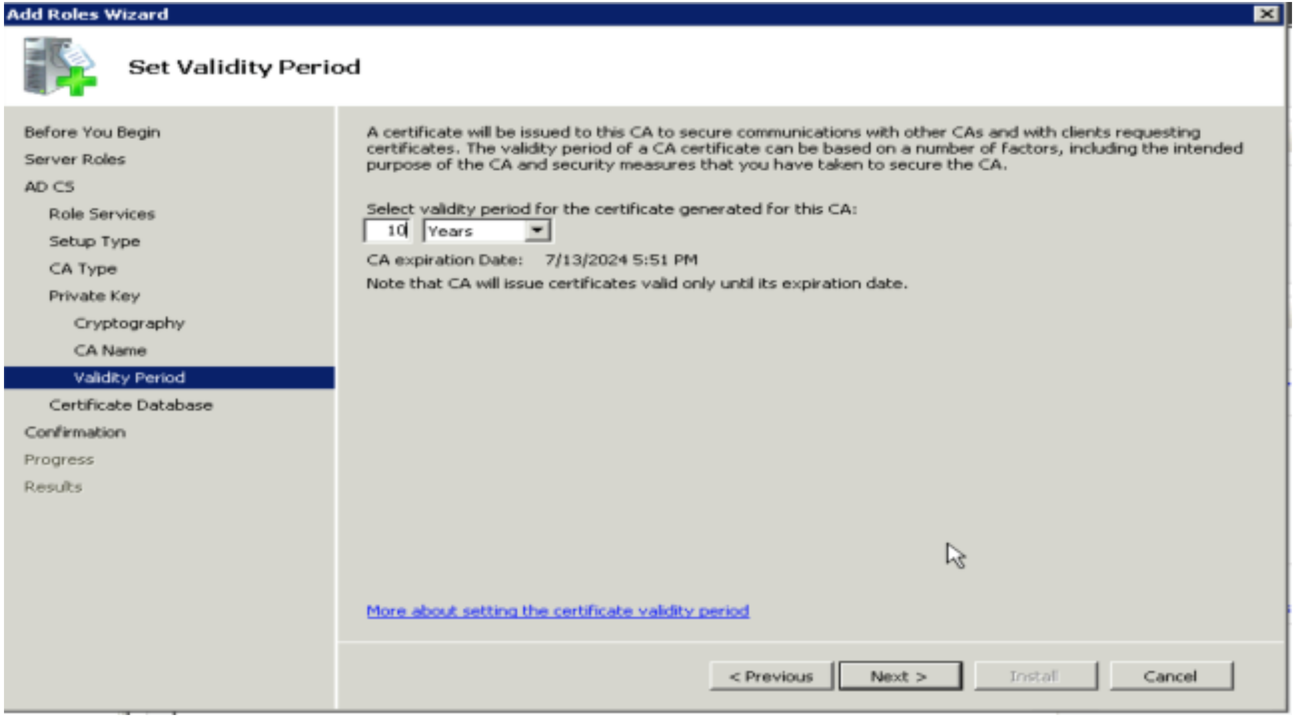
Preview of distinguished name:
CN=LAB-AD,DC=httsindialab,DC=local

More about configuring a CA name

Root CA – Installation Contd

CA Lifetime=10 years

Ideally CA Lifetime>Sub CA Lifetime>Endpoint certificate lifetime



A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

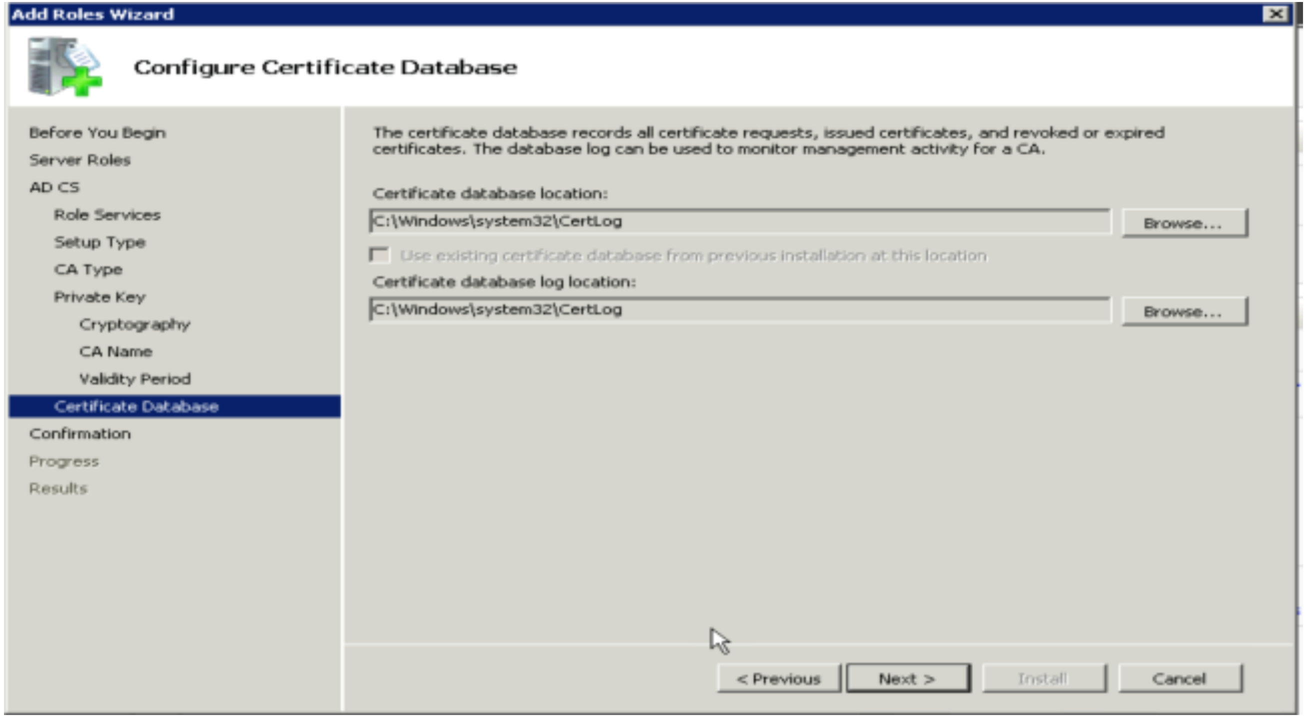
Select validity period for the certificate generated for this CA:

10 Years

CA expiration Date: 7/13/2024 5:51 PM

Note that CA will issue certificates valid only until its expiration date.

Root CA – Installation Contd



Configure Certificate Database

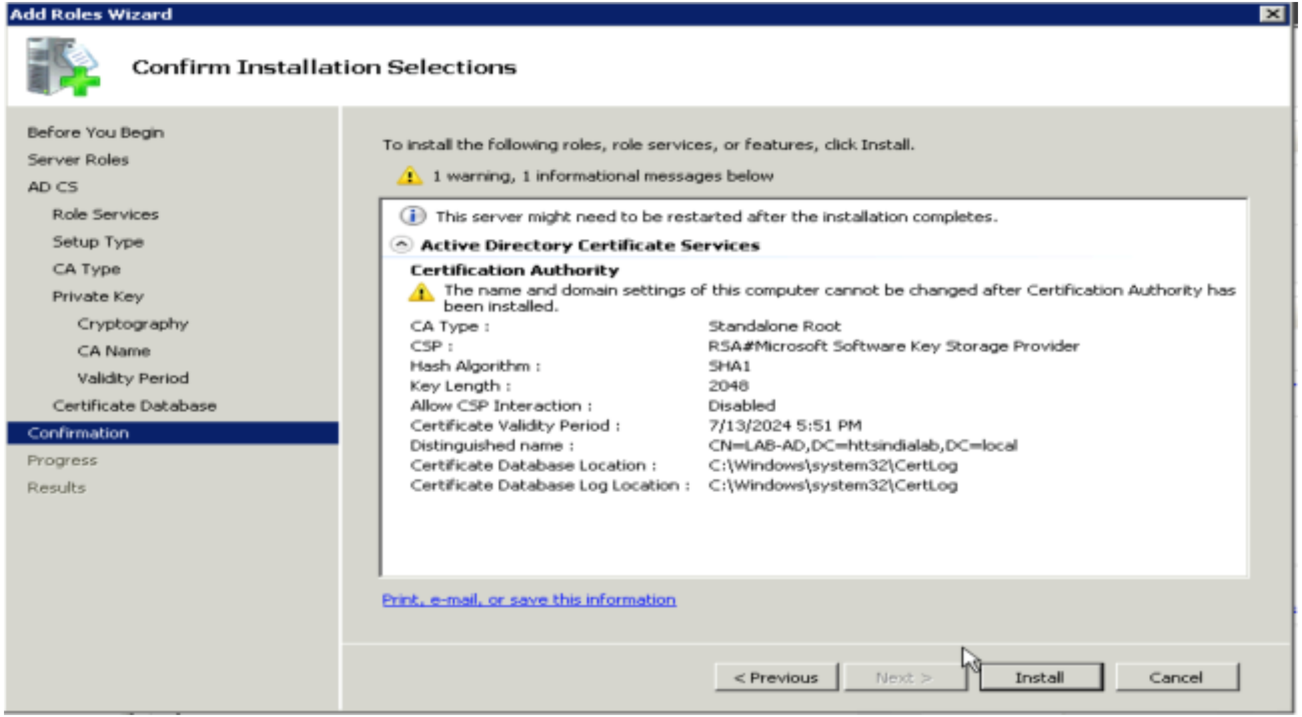
The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

Certificate database location: C:\Windows\system32\CertLog

☐ Use existing certificate database from previous installation at this location

Certificate database log location: C:\Windows\system32\CertLog

Root CA – Installation Contd



To install the following roles, role services, or features, click Install.

⚠ 1 warning, 1 informational messages below

ⓘ This server might need to restart after the installation completes.

Active Directory Certificate Services

Certification Authority

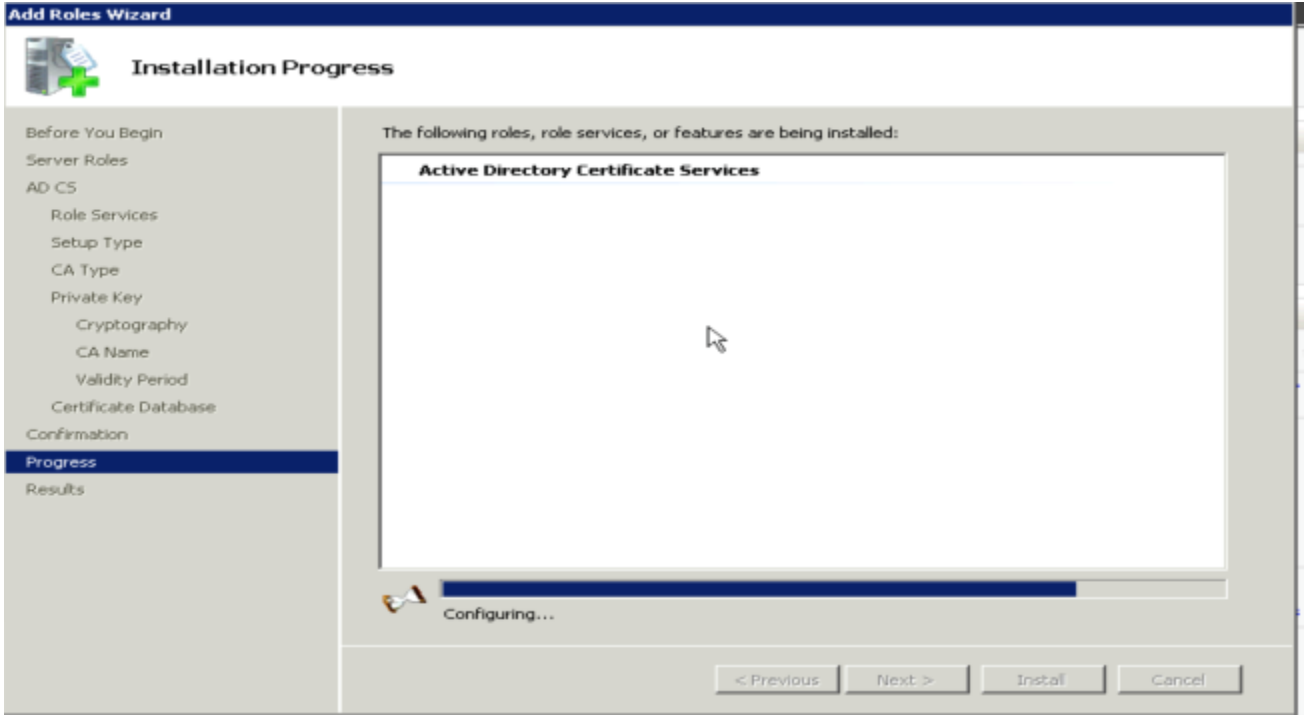
⚠ The name and domain settings of this computer cannot be changed after Certification Authority has been installed.

```
CA Type :                            Standalone Root
CSP :                                RSA#Microsoft Software Key Storage Provider
Hash Algorithm :                     SHA1
Key Length :                         2048
Allow CSP Interaction :              Disabled
Certificate Validity Period :        7/13/2024 5:51 PM
Distinguished name :                 CN=LAB-AD,DC=httsindialab,DC=local
Certificate Database Location :      C:\Windows\system32\CertLog
Certificate Database Log Location :  C:\Windows\system32\CertLog
```

Print, e-mail, or save this information

Root CA – Installation Contd

Last step in setting up Root CA

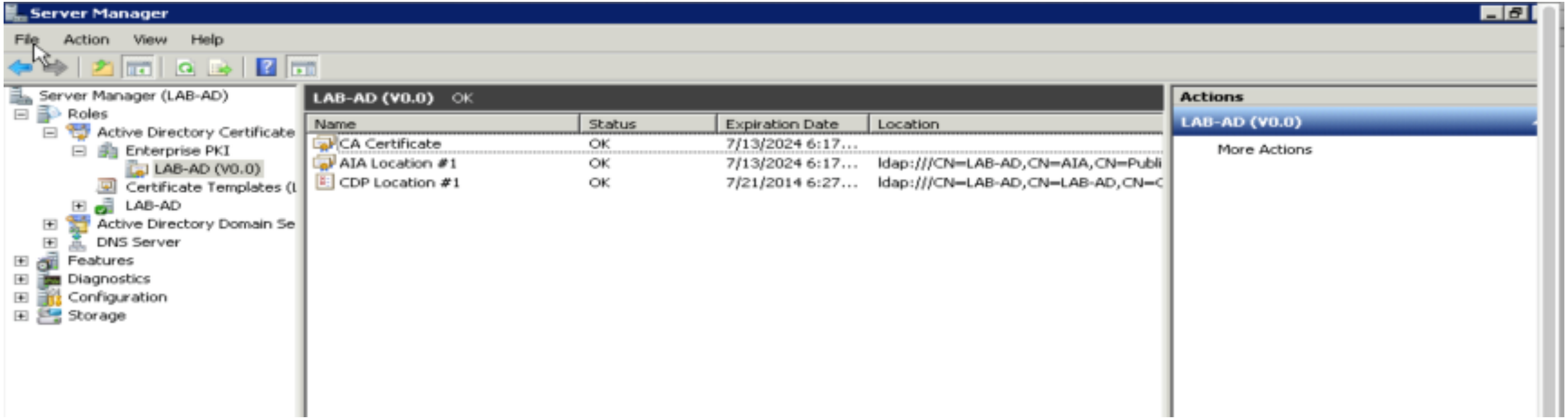


The following roles, role services, or features are being installed:

Active Directory Certificate Services

Configuring...

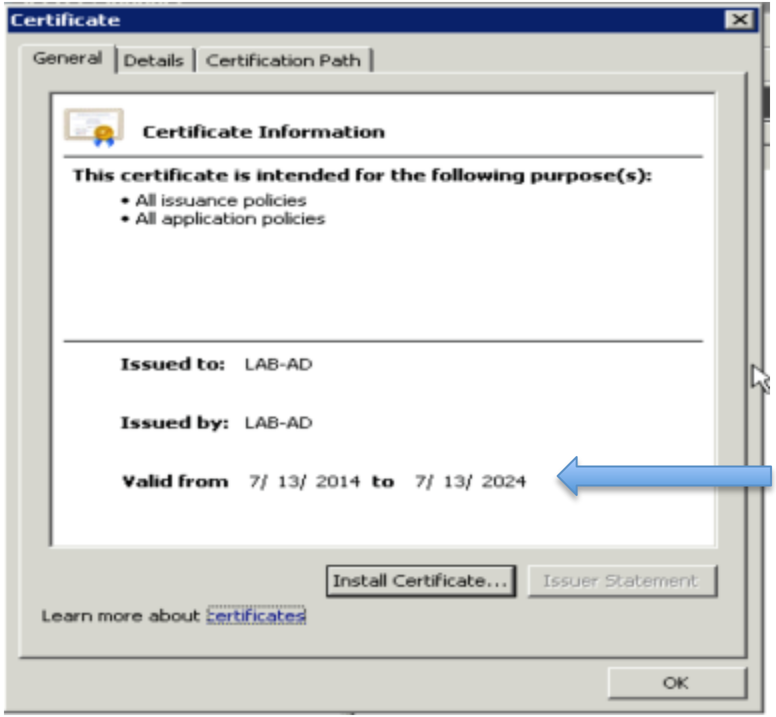
Server Manager – AD CS



LAB-AD (V0.0) OK

Name	Status	Expiration Date	Location
CA Certificate	OK	7/13/2024 6:17...	
AIA Location #1	OK	7/13/2024 6:17...	ldap:///CN=LAB-AD,CN=AIA,CN=Publi
CDP Location #1	OK	7/21/2014 6:27...	ldap:///CN=LAB-AD,CN=LAB-AD,CN=C

Root CA Self-signed Certificate



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: LAB-AD

Issued by: LAB-AD

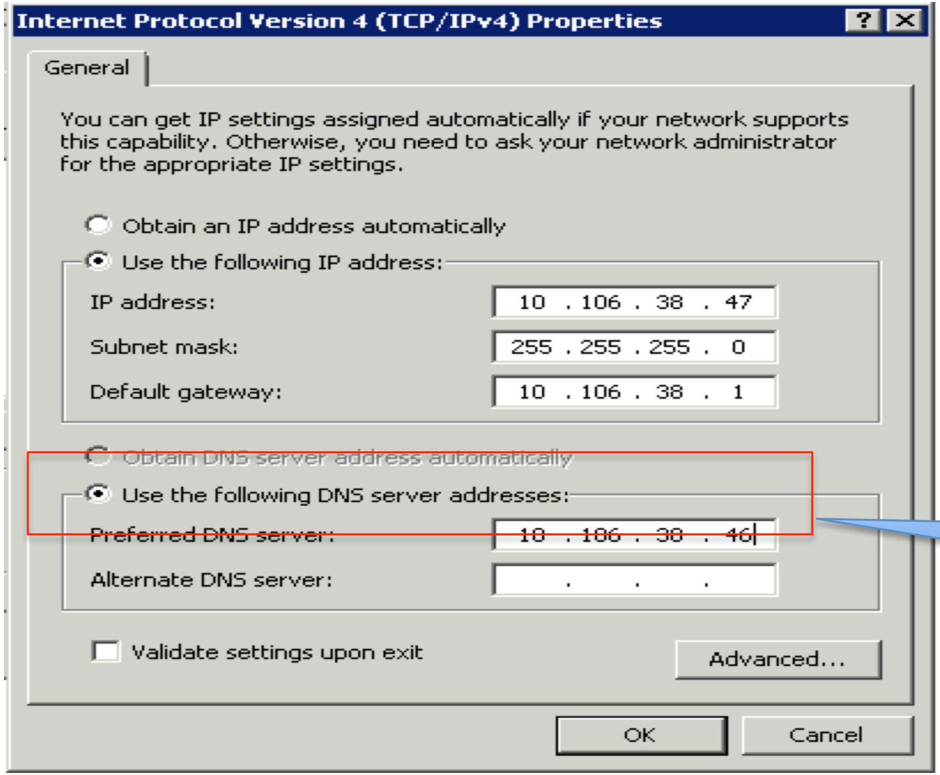
Valid from 7/ 13/ 2014 to 7/ 13/ 2024

The lifetime for Root CA shows up here

Certificate Services

Sub CA Setup – Pre-requisites

Prerequisite #1 – Add DNS server to the Network settings



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 106 . 38 . 47

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 106 . 38 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 106 . 38 . 46

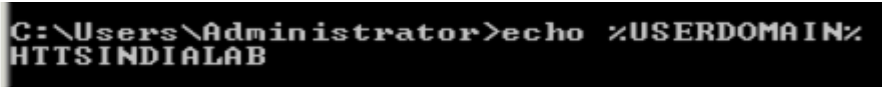
Alternate DNS server: . . .

□ Validate settings upon exit

Lab AD IP address

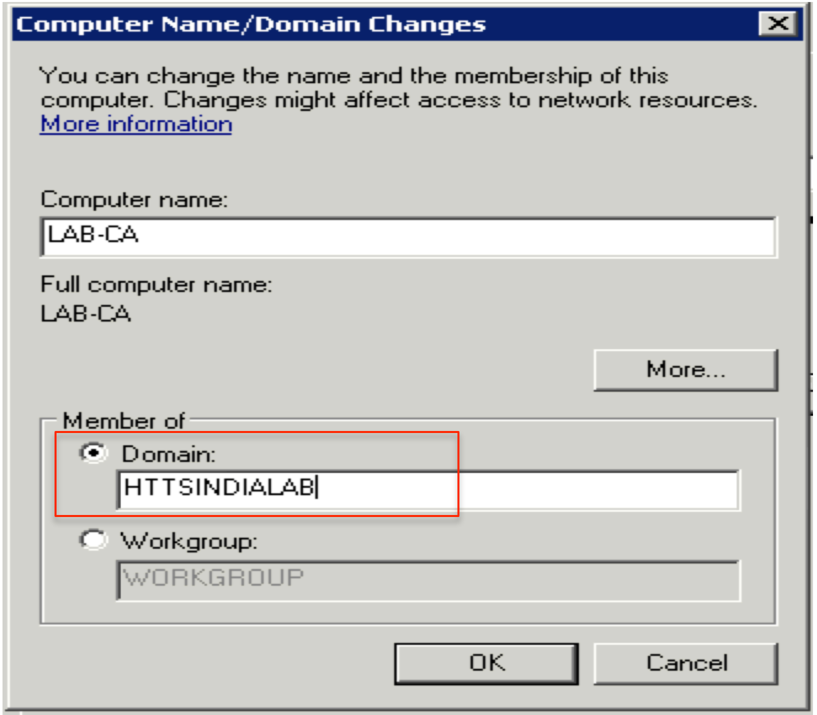
Prerequisite #2 – Join the intended sub CA to domain as member server

Before Joining to domain, you need to know the domain name that you are joining. The command is **echo %USERDOMAIN%** from the AD server



```
C:\Users\Administrator>echo %USERDOMAIN%
HTTSINDIALAB
```

Prerequisite #2 – Join the intended sub CA to domain as member server Continued



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

More information

Computer name:

LAB-CA

Full computer name:

LAB-CA

Member of

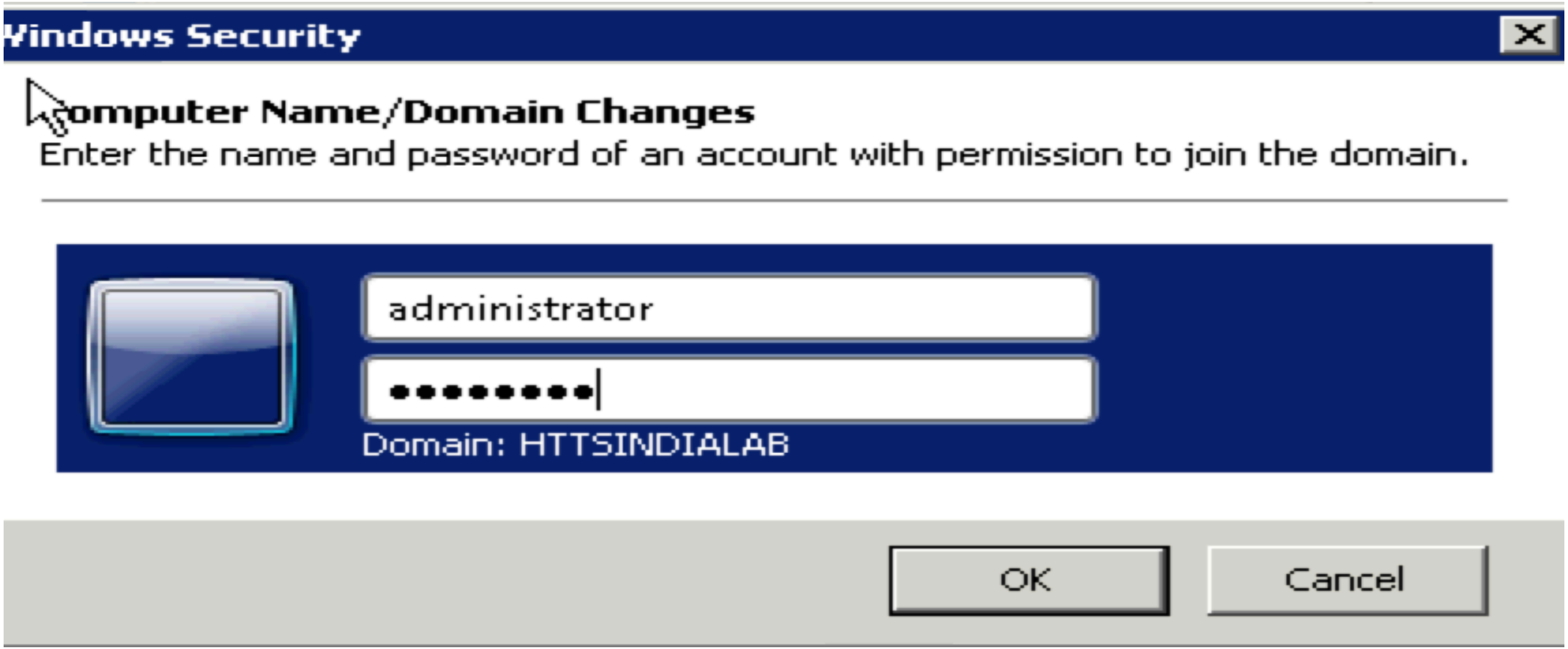
● Domain:

HTTSINDIALAB

○ Workgroup:

WORKGROUP

Prerequisite #2 – Join the intended sub CA to domain as member server Continued



Vindows Security

Computer Name/Domain Changes

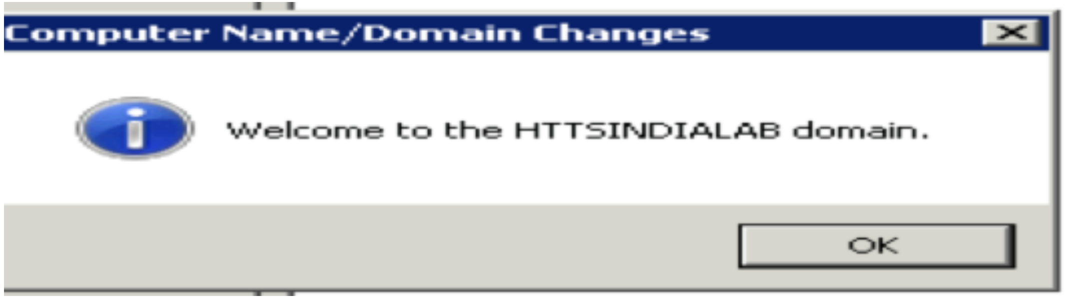
Enter the name and password of an account with permission to join the domain.

administrator

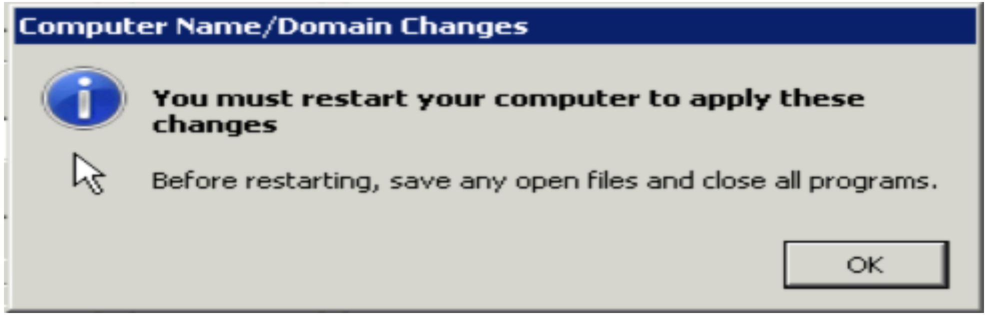
●●●●●●●●●

Domain: HTTSINDIALAB

Prerequisite #2 – Join the intended sub CA to domain as member server Continued



Welcome to the HTTSINDIALAB domain.



You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

Pre-requisite #3: Configure NTP

We configure our Windows server to sync with NTP

```
C:\Users\Administrator>w32tm /config /manualpeerlist:10.76.72.3,0x8 /syncfromflags:MANUAL
The command completed successfully.
```

W32 Time service Manual Sync

We restart the W32 time services

```
C:\Users\Administrator>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.


C:\Users\Administrator>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.
```

Stop and Start services

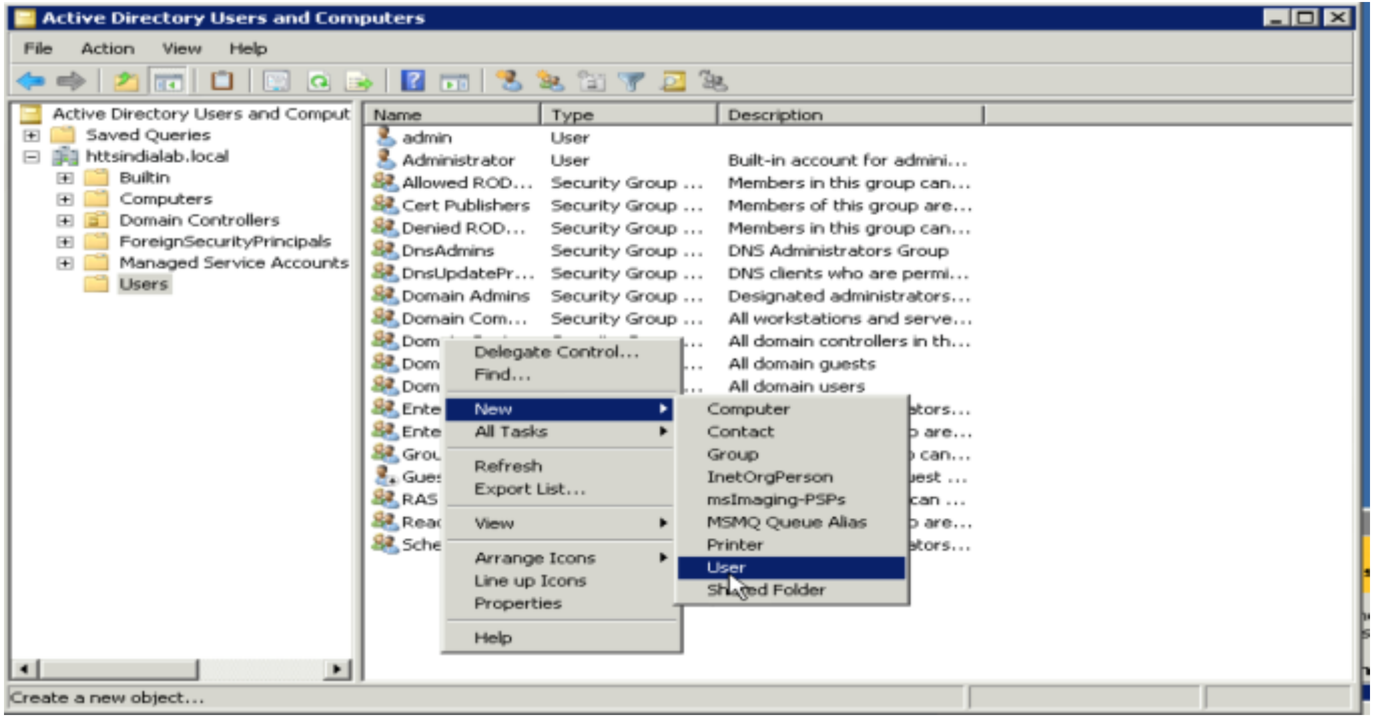
We query and check the clock status confirming if NTP sync was successful

```
C:\Users\Administrator>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0319366s
Root Dispersion: 7.7861956s
ReferenceId: 0x0A4C4803 (source IP:  10.76.72.3)
Last Successful Sync Time: 7/16/2014 8:27:34 AM
Source: 10.76.72.3,0x8
Poll Interval: 6 (64s)
```

Verify NTP is in sync

Pre-requisite#4: Add SCEP user

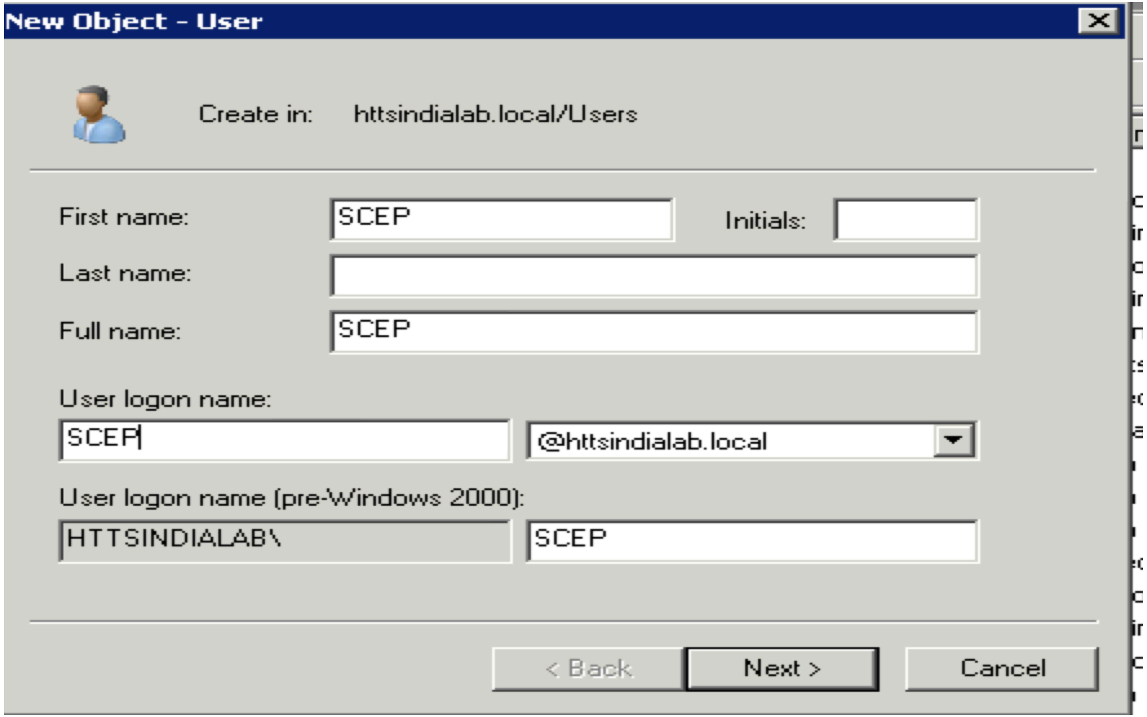
On LAB AD server: Create SCEP service account for NDES



Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Allowed ROD...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied ROD...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Com...	Security Group ...	All workstations and serve...
Dom	...	All domain controllers in th...
Dom	...	All domain guests
Dom	...	All domain users
Ente		tors...
Ente		are...
Grou		can...
Gues		uest ...
RAS		can ...
Reac		are...
Sche		tors...

Create a new object...

Pre-requisite#4: Add SCEP user (Contd)



Create in: httsindialab.local/Users

First name: SCEP

Initials:

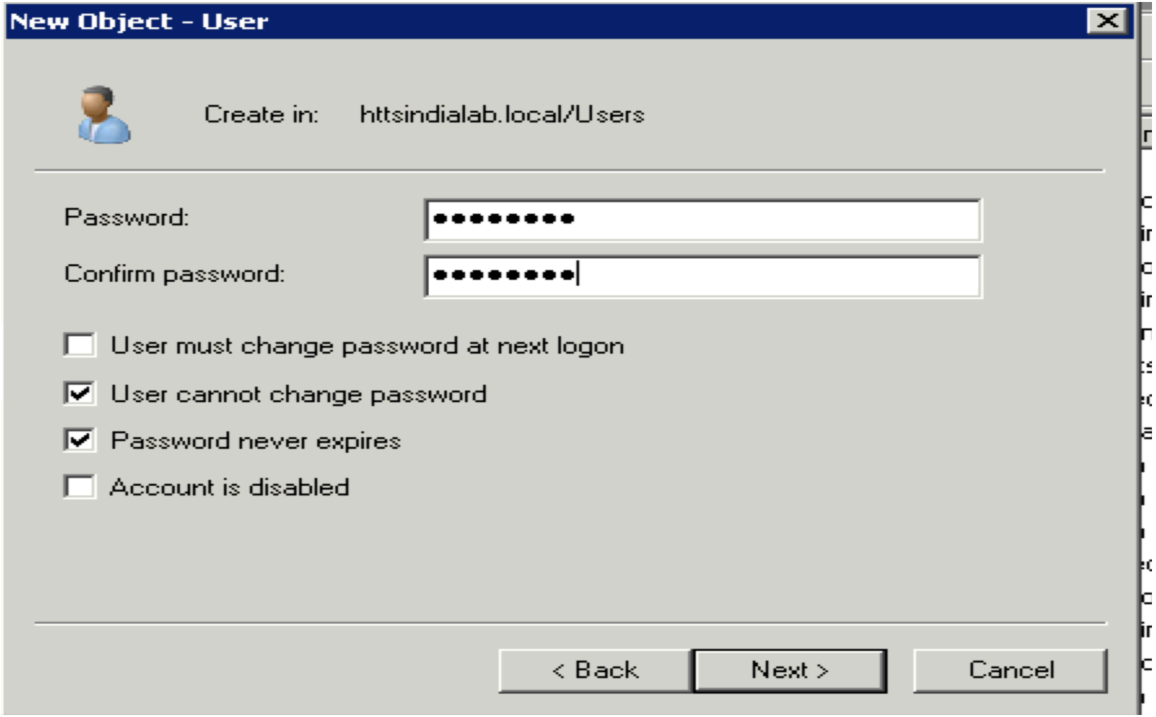
Last name:

Full name: SCEP

User logon name: SCEP @httsindialab.local

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

Pre-requisite#4: Add SCEP user (Contd)



Create in: httsindialab.local/Users

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ User must change password at next logon

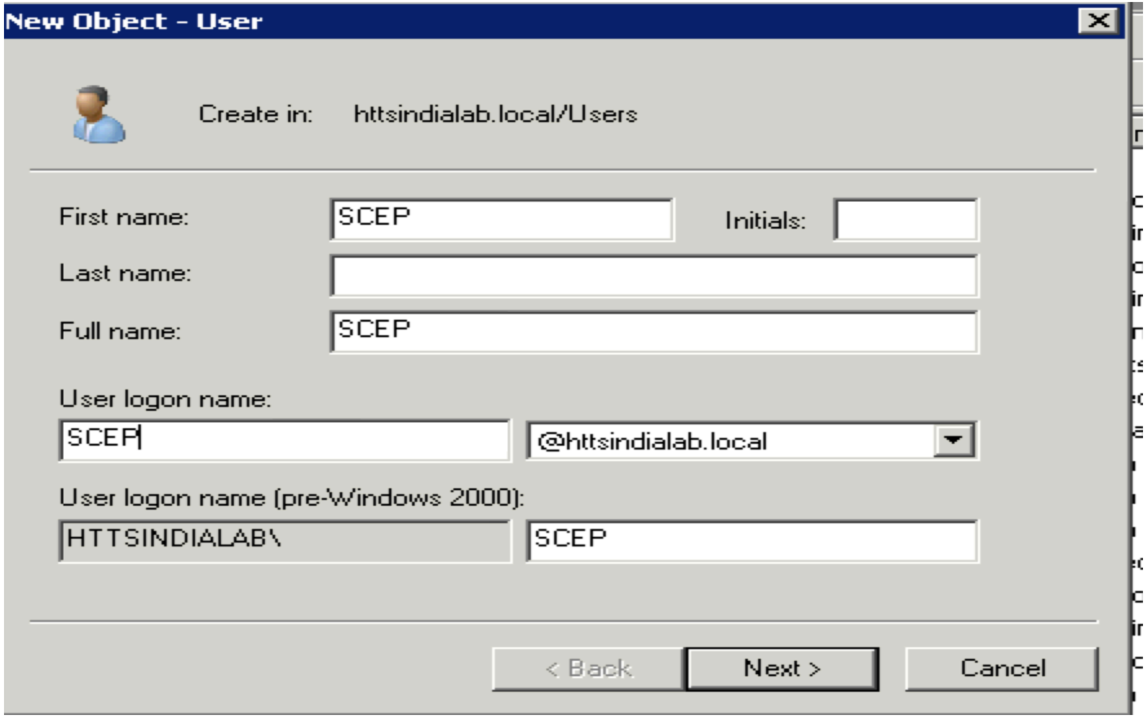
☑ User cannot change password

☑ Password never expires

□ Account is disabled

Ensure to select these check boxes

Pre-requisite#4: Add SCEP user (Contd)



New Object - User

Create in: httsindialab.local/Users

First name: SCEP

Initials:

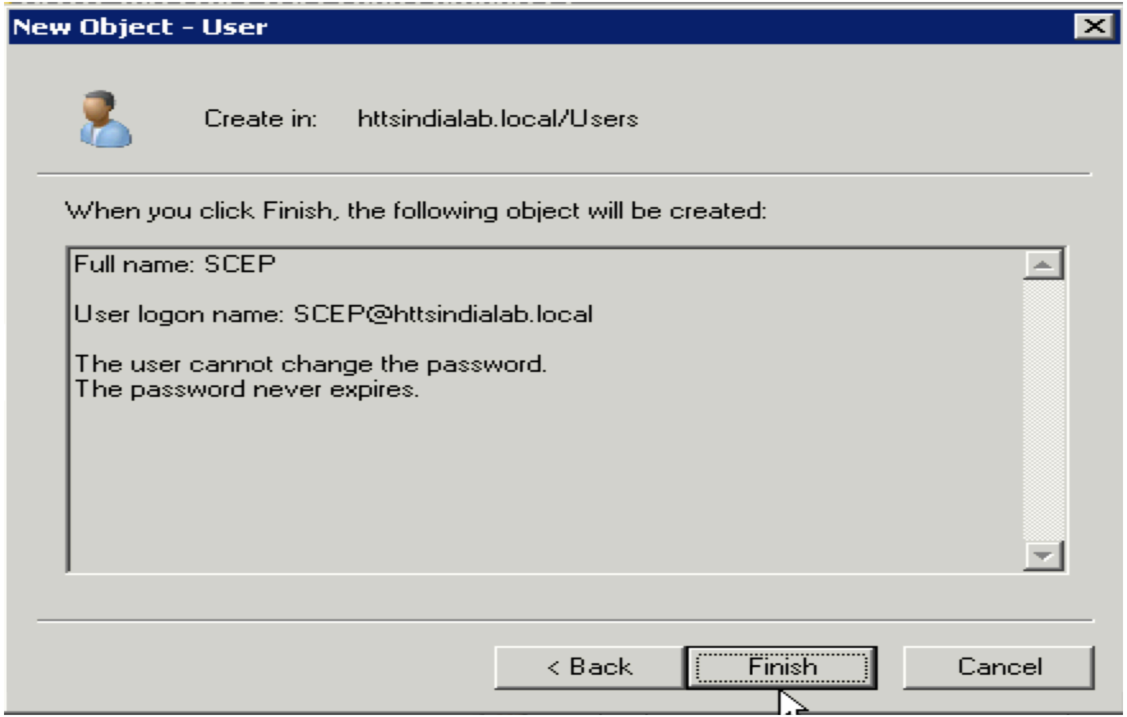
Last name:

Full name: SCEP

User logon name: SCEP @httsindialab.local

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

Pre-requisite#4: Add SCEP user (Contd)



Create in: httsindialab.local/Users

When you click Finish, the following object will be created:

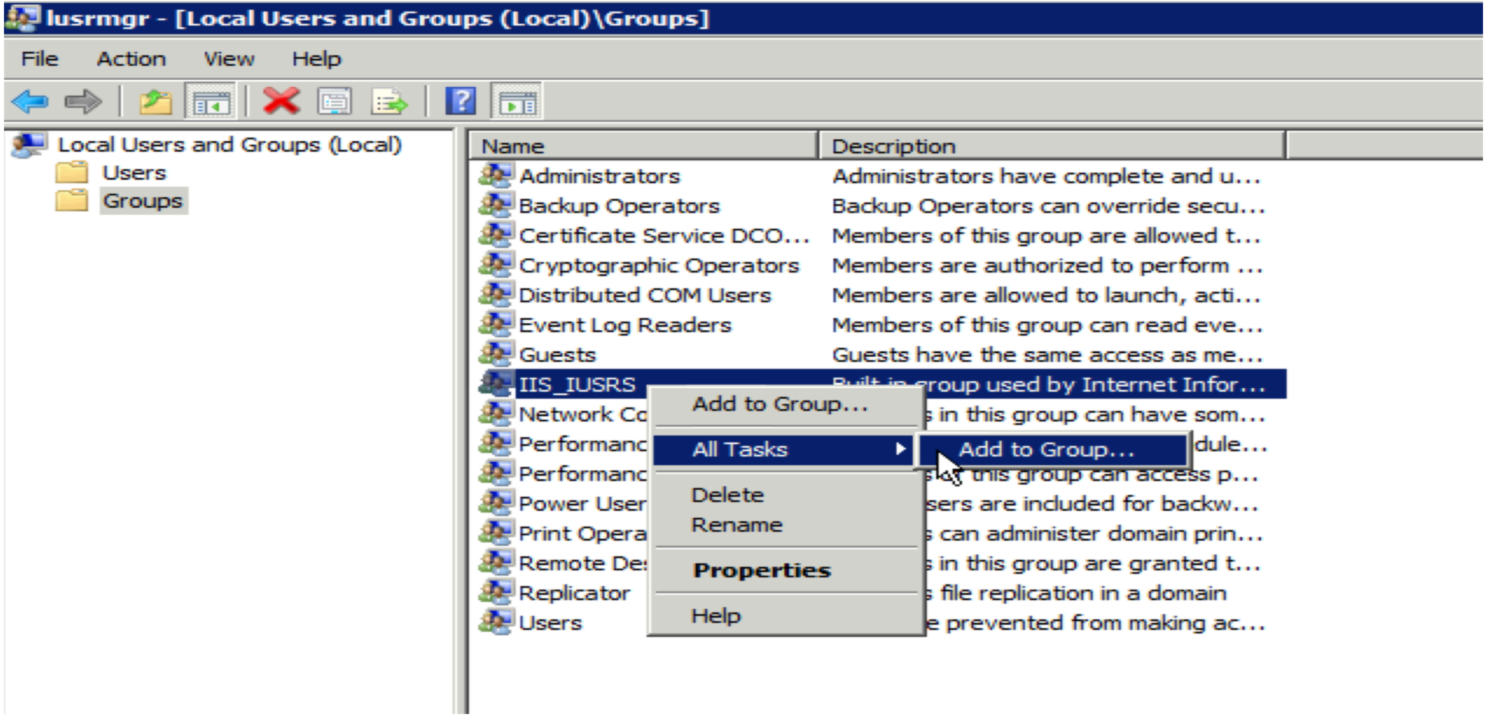
Full name: SCEP

User logon name: SCEP@httsindialab.local

The user cannot change the password.
The password never expires.

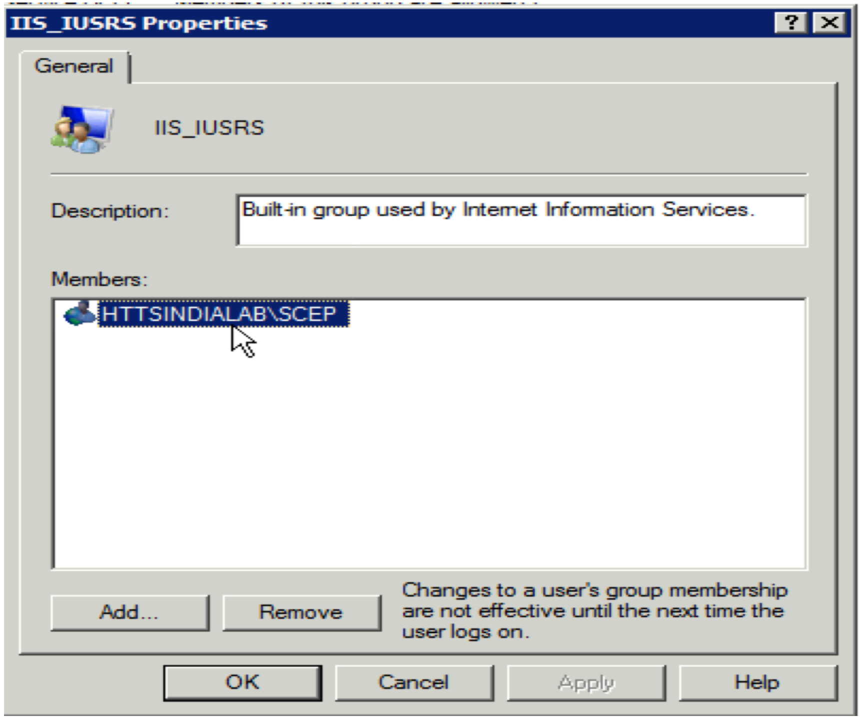
Pre-requisite#4: Add SCEP user (Contd)

Local Users and Groups (lusrmgr.msc) → Add SCEP to IIS_IUSRS groups



Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Certificate Service DCO...	Members of this group are allowed t...
Cryptographic Operators	Members are authorized to perform ...
Distributed COM Users	Members are allowed to launch, acti...
Event Log Readers	Members of this group can read eve...
Guests	Guests have the same access as me...
IIS_IUSRS	Built-in group used by Internet Infor...
Network Co	s in this group can have som...
Performanc	dule...
Performanc	s this group can access p...
Power User	sers are included for backw...
Print Opera	s can administer domain prin...
Remote De:	s in this group are granted t...
Replicator	s file replication in a domain
Users	e prevented from making ac...

Pre-requisite#4: Add SCEP user (Contd)



IIS_IUSRS Properties

IIS_IUSRS

Description: Built-in group used by Internet Information Services.

Members:

HTTSINDIALAB\SCEP

Changes to a user's group membership are not effective until the next time the user logs on.

Pre-requisite 5: Getting Hotfixes

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

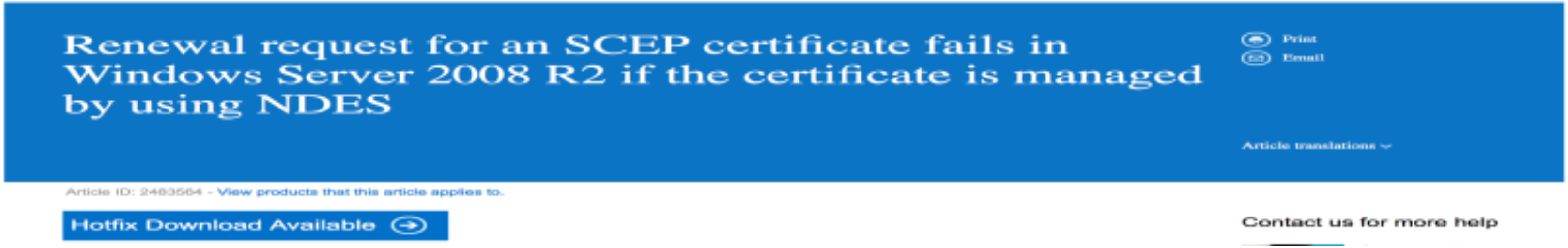
***http://support.microsoft.com/kb/2483564* - Renewal request for an SCEP certificate fails in Windows Server 2008 R2 if the certificate is managed by using NDES**

Download Hotfix from here

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.

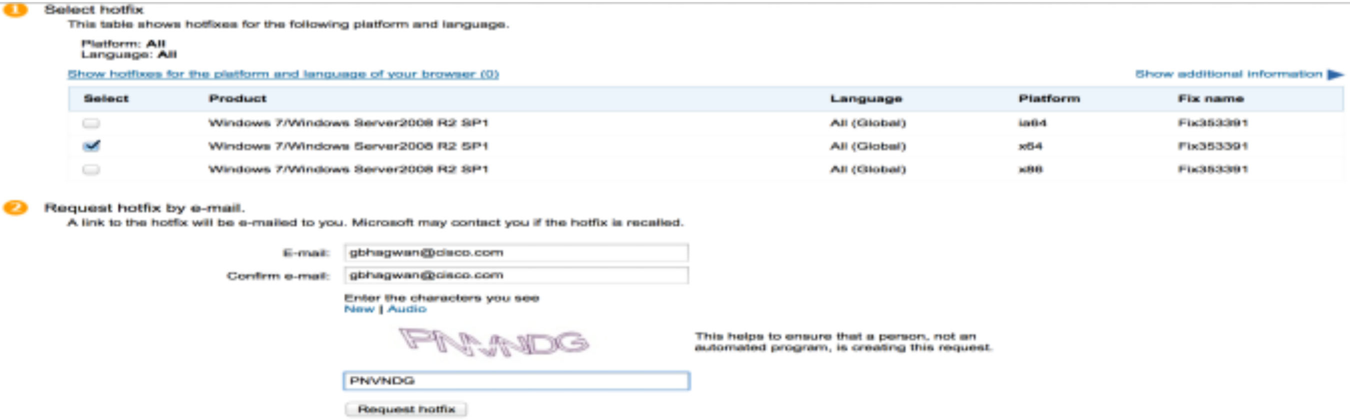
Download Hotfix from MS KB

Pre-requisite 5: Getting Hotfixes (Contd)



Renewal request for an SCEP certificate fails in Windows Server 2008 R2 if the certificate is managed by using NDES

Article ID: 2483564 - View products that this article applies to.



1 Select hotfix

This table shows hotfixes for the following platform and language.

Platform: **All**
Language: **All**

Show hotfixes for the platform and language of your browser (0)

Select	Product	Language	Platform	Fix name
☐	Windows 7/Windows Server2008 R2 SP1	All (Global)	ia64	Fix353391
☑	Windows 7/Windows Server2008 R2 SP1	All (Global)	x64	Fix353391
☐	Windows 7/Windows Server2008 R2 SP1	All (Global)	x86	Fix353391

2 Request hotfix by e-mail.

A link to the hotfix will be e-mailed to you. Microsoft may contact you if the hotfix is recalled.

E-mail: gbhagwan@cisco.com

Confirm e-mail: gbhagwan@cisco.com

Enter the characters you see
New | Audio

This helps to ensure that a person, not an automated program, is creating this request.

PNVNDG

Pre-requisite 5: Getting Hotfixes

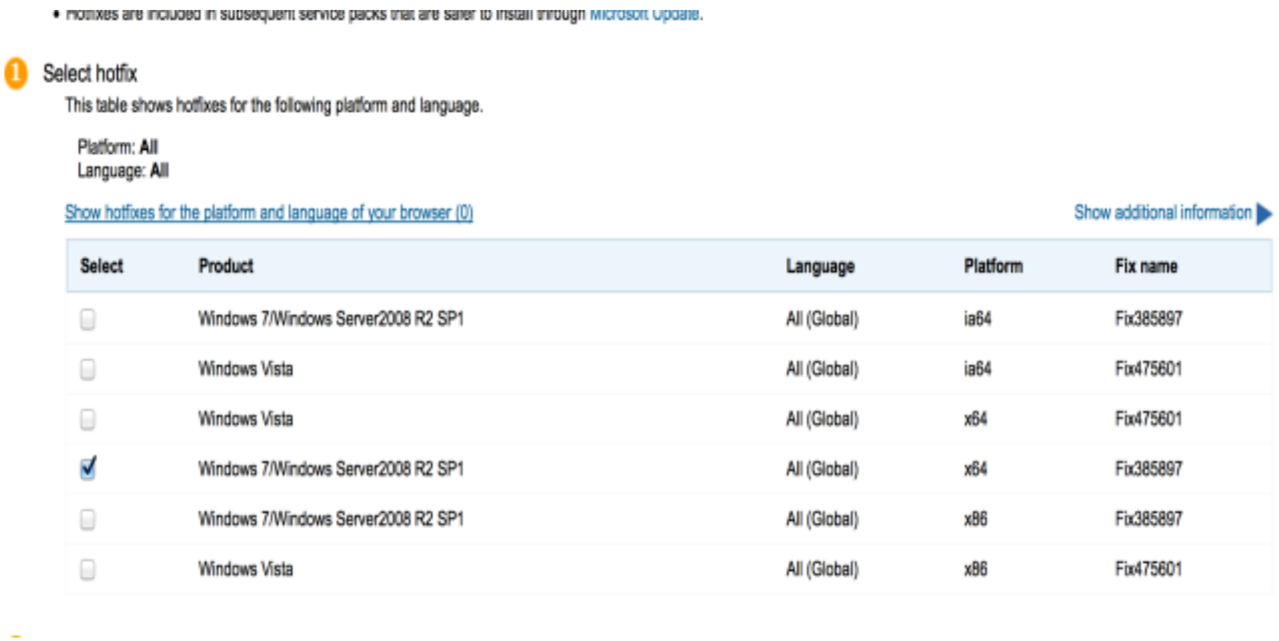
CSR Submit failure after Win 2008 R2 server is restarted

http://support.microsoft.com/kb/2633200 - 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 Enrollment Service cannot submit the certificate request (0x800706ba). The RPC server is unavailable."

NDES does not submit certificate requests after the enterprise CA is restarted in Windows Server 2008 R2 SP1 or Windows Server 2008 SP2

Article ID: 2633200 - View products that this article applies to.

Pre-requisite 5: Getting Hotfixes (Contd)



- Hotfixes are included in subsequent service packs that are safer to install through Microsoft Update.

1 Select hotfix

This table shows hotfixes for the following platform and language.

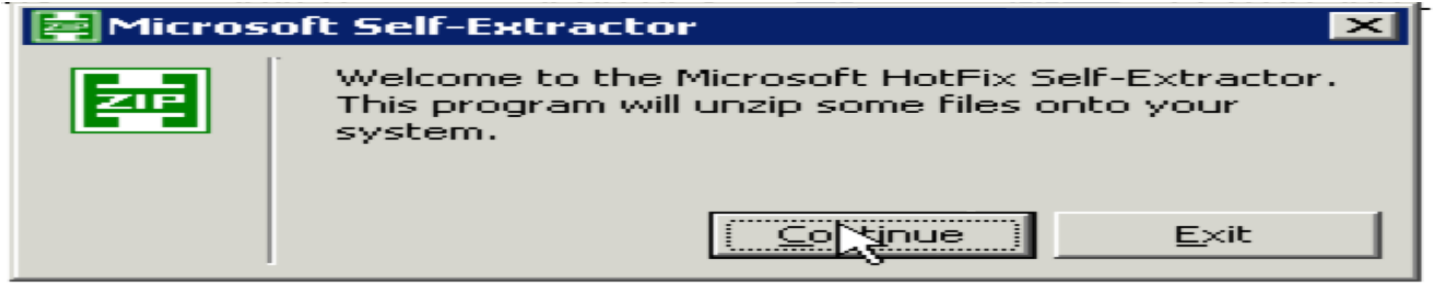
Platform: **All**
Language: **All**

Show hotfixes for the platform and language of your browser (0)

Show additional information ▶

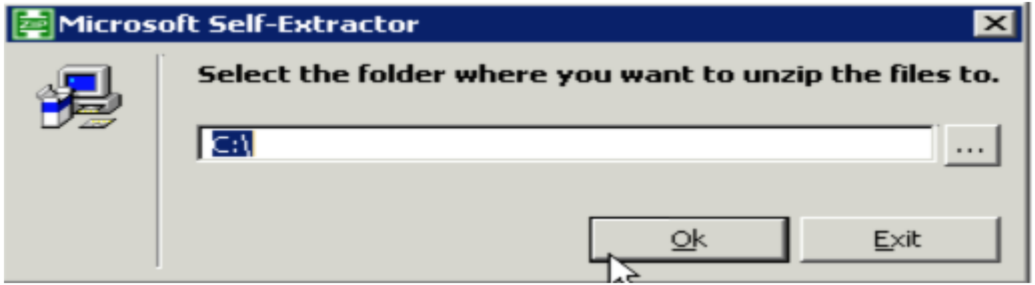
Select	Product	Language	Platform	Fix name
☐	Windows 7/Windows Server2008 R2 SP1	All (Global)	ia64	Fix385897
☐	Windows Vista	All (Global)	ia64	Fix475601
☐	Windows Vista	All (Global)	x64	Fix475601
☑	Windows 7/Windows Server2008 R2 SP1	All (Global)	x64	Fix385897
☐	Windows 7/Windows Server2008 R2 SP1	All (Global)	x86	Fix385897
☐	Windows Vista	All (Global)	x86	Fix475601

Pre-requisite 5: Getting Hotfixes (Contd)



Microsoft Self-Extractor

Welcome to the Microsoft HotFix Self-Extractor. This program will unzip some files onto your system.

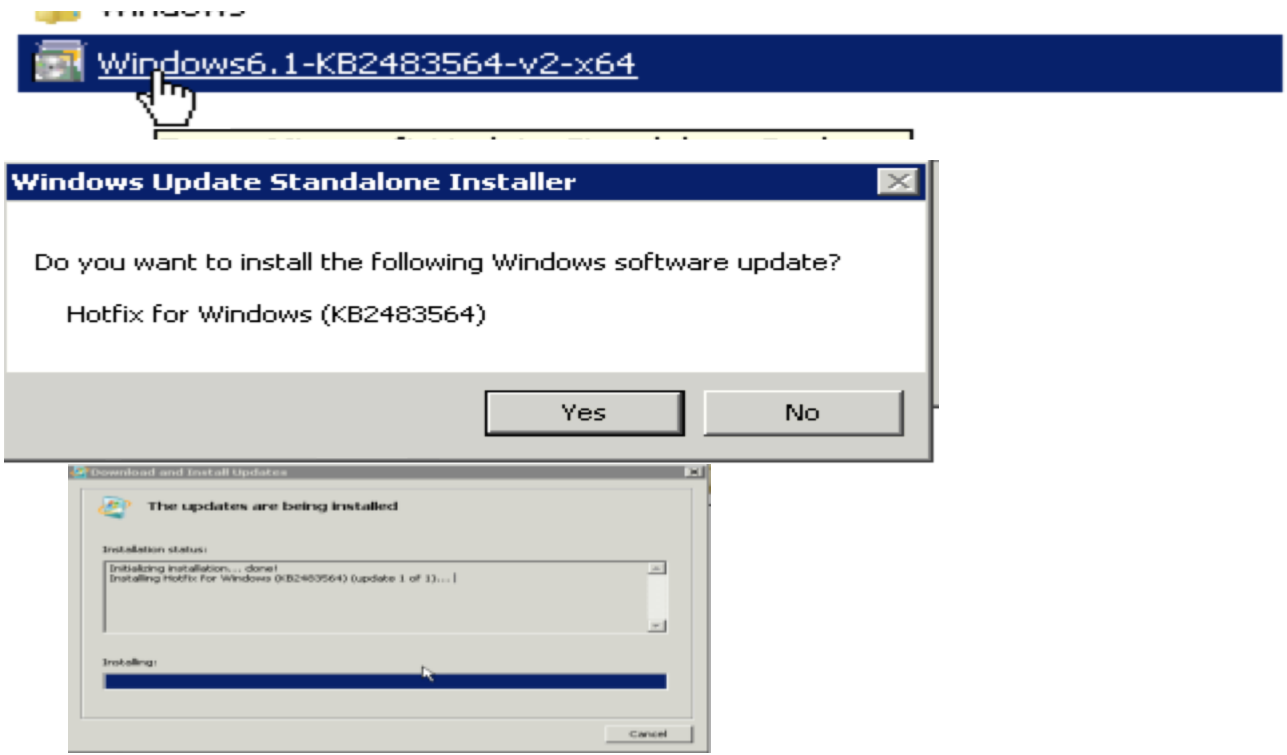


Microsoft Self-Extractor

Select the folder where you want to unzip the files to.

C:\

Pre-requisite 5: Getting Hotfixes (Contd)



Windows6.1-KB2483564-v2-x64

Windows Update Standalone Installer

Do you want to install the following Windows software update?

Hotfix for Windows (KB2483564)

Download and Install Updates

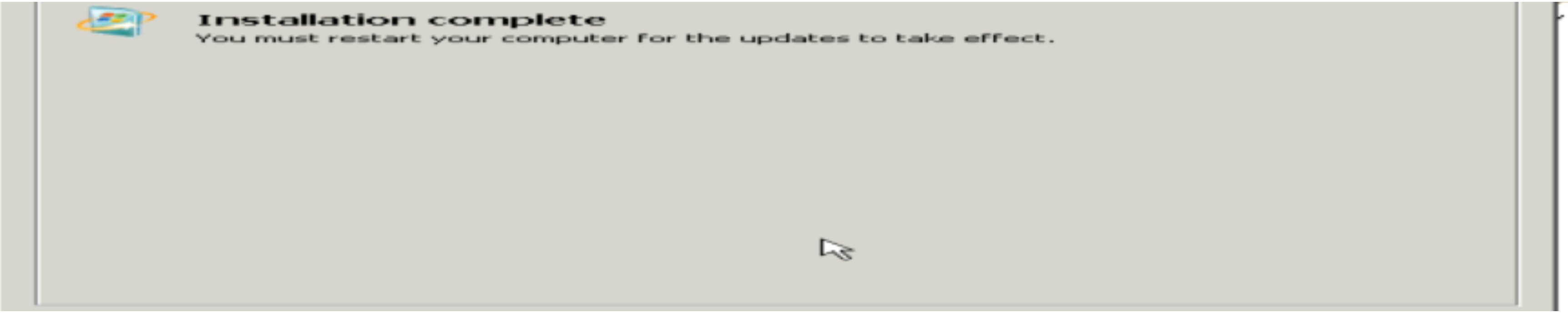
The updates are being installed

Installation status:

```
Initializing installation... done!
Installing Hotfix for Windows (KB2483564) (update 1 of 1)...
```

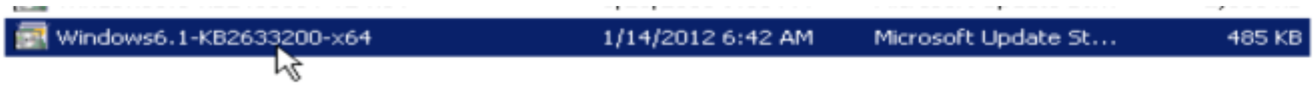
Installing:

Pre-requisite 5: Getting Hotfixes (Contd)



Installation complete

You must restart your computer for the updates to take effect.



```
Windows6.1-KB2633200-x64        1/14/2012 6:42 AM    Microsoft Update St...    485 KB
```

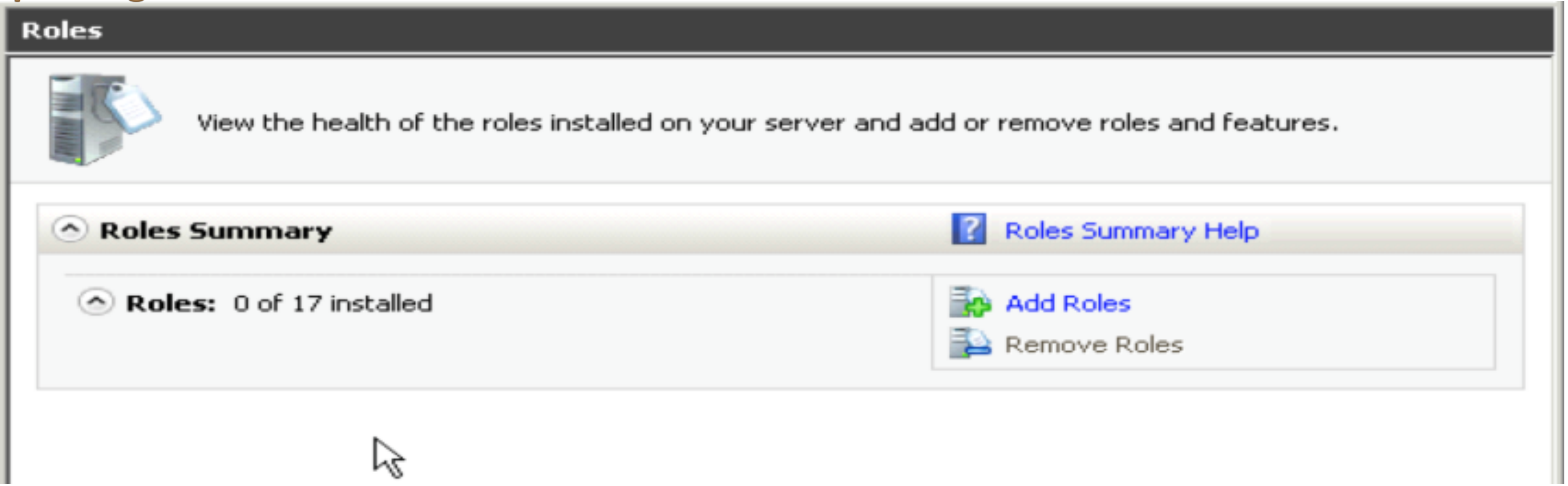
Certificate Services

Sub CA Setup – Installation

Install Subordinate CA

Similar steps for installing Sub CA like for Root CA – Go to Add Roles Wizard again

Prerequisite before starting install: Login as admin with Domain or Enterprise admin privileges

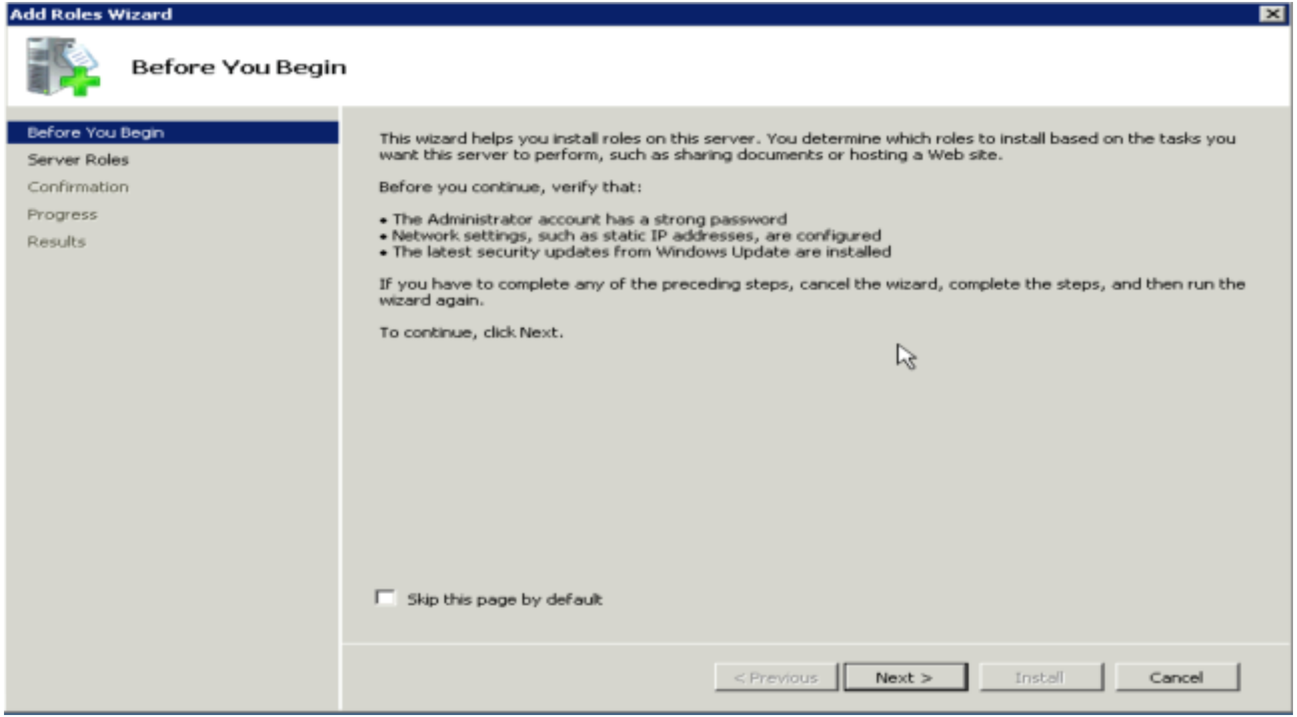


Roles

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

Roles: 0 of 17 installed

Install Subordinate CA - Contd



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

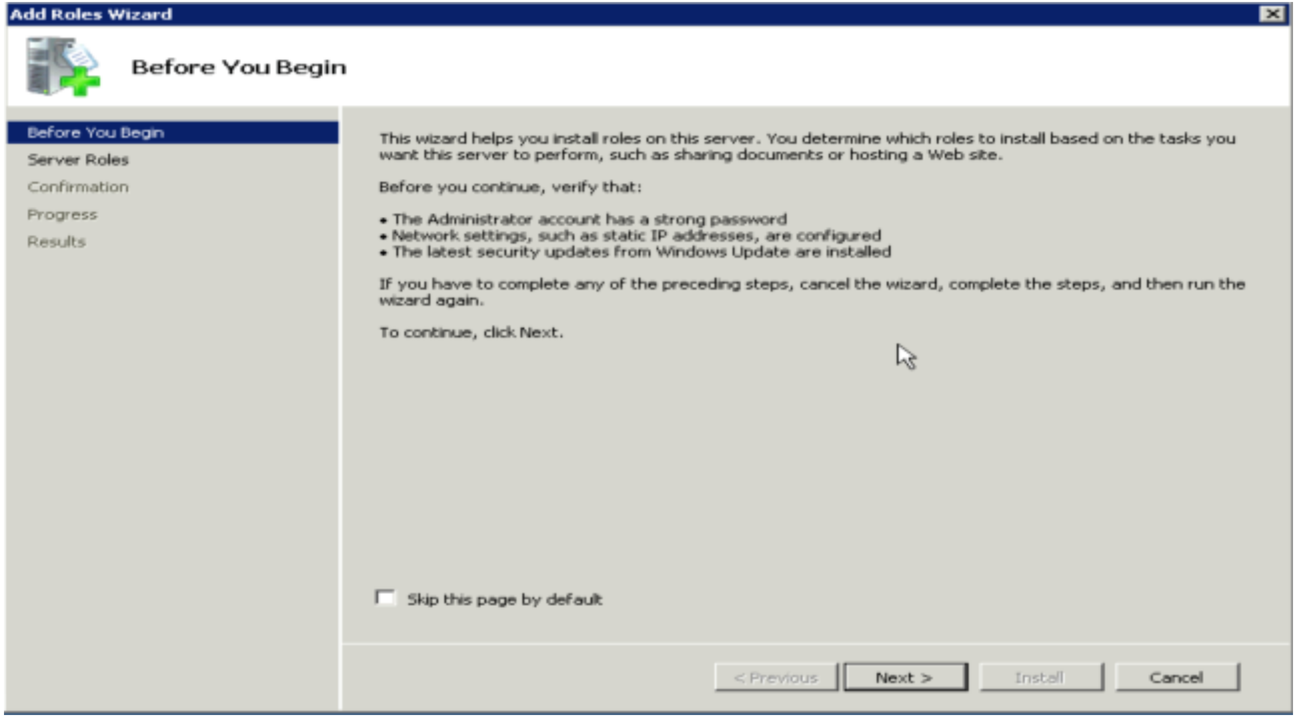
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Install Subordinate CA - Contd



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

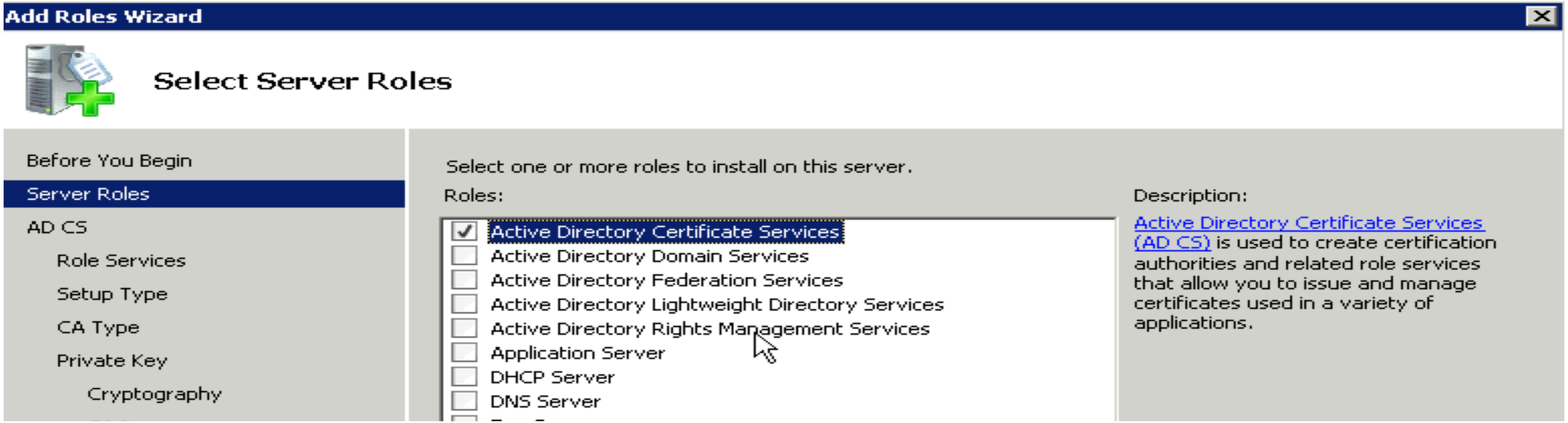
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Install Subordinate CA - Contd



Select Server Roles

Select one or more roles to install on this server.

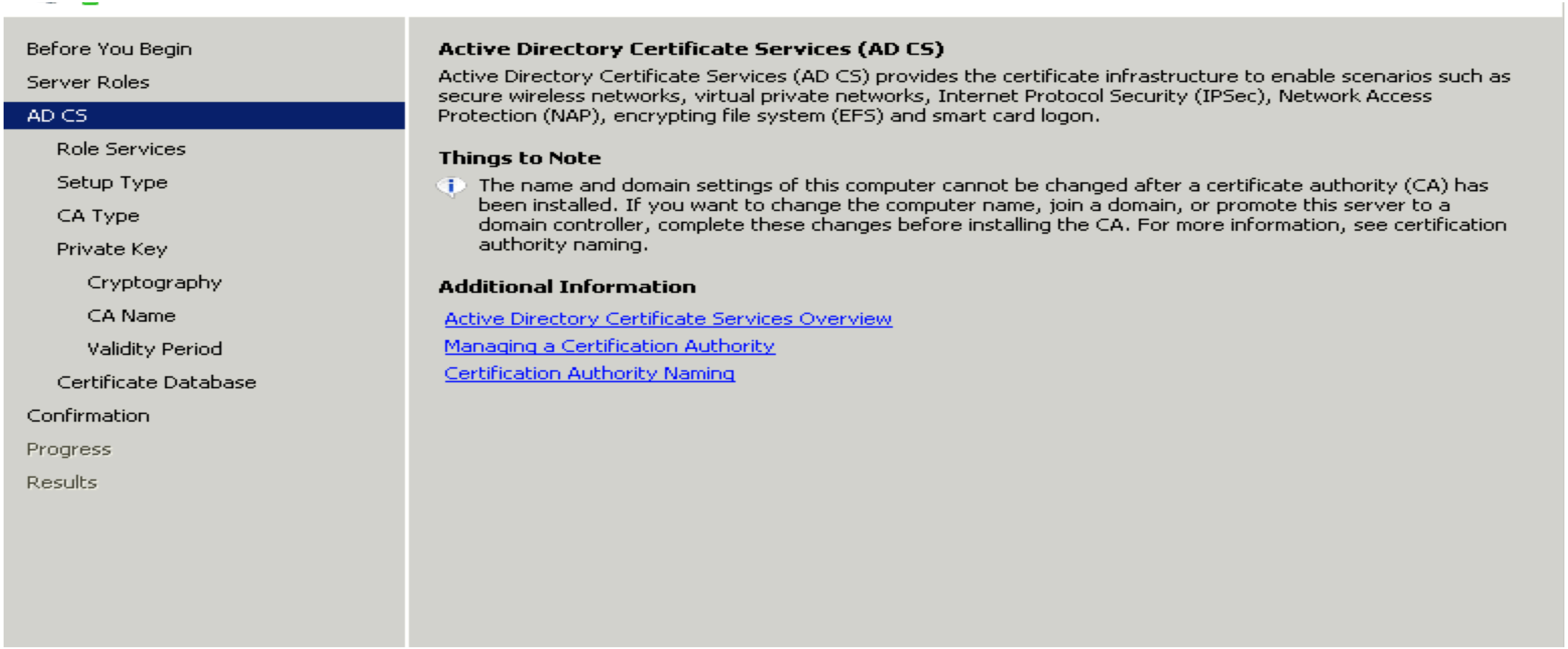
Roles:

- ☑ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server

Description:

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.

Install Subordinate CA - Contd



Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card logon.

Things to Note

The name and domain settings of this computer cannot be changed after a certificate authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Additional Information

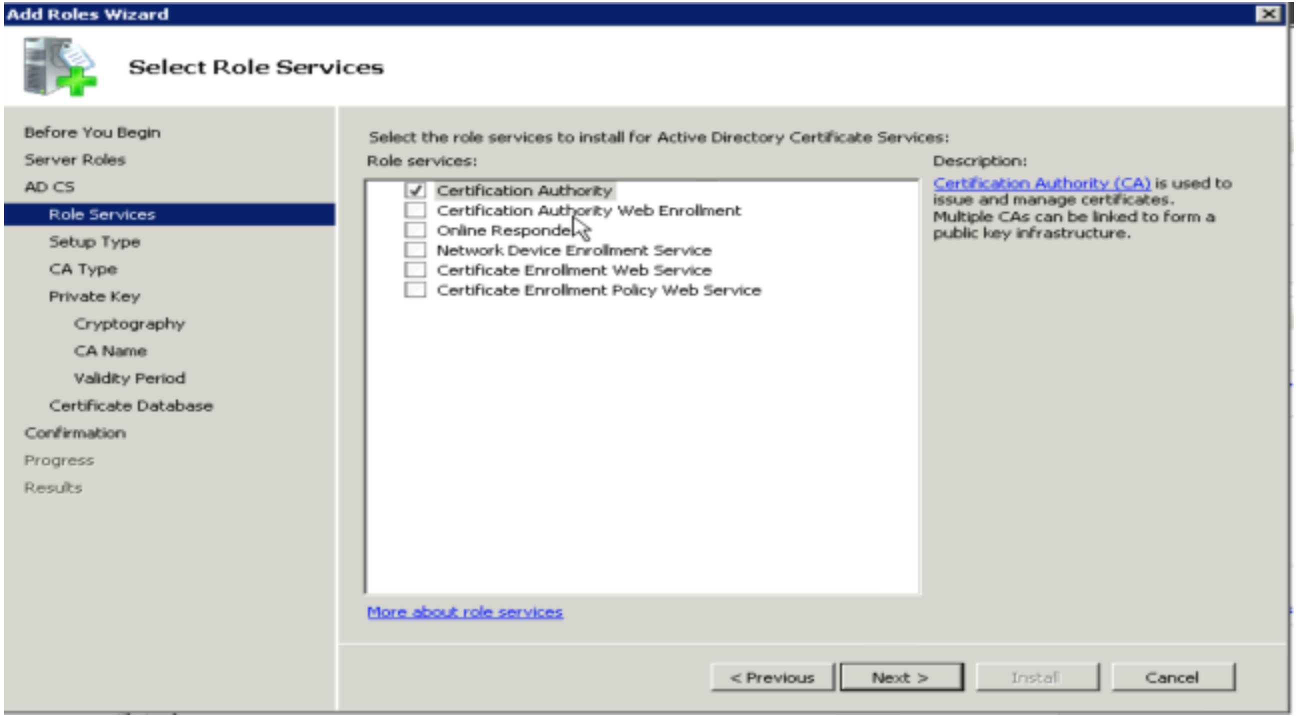
Active Directory Certificate Services Overview

Managing a Certification Authority

Certification Authority Naming

Install Subordinate CA - Contd

Choose Components 1,2,3 and 6 – Certification Authority, Certificate Authority Web enrollment, Online Responder and Certificate enrollment Policy Web service



Add Roles Wizard

Select Role Services

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

Role services:

- ☑ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

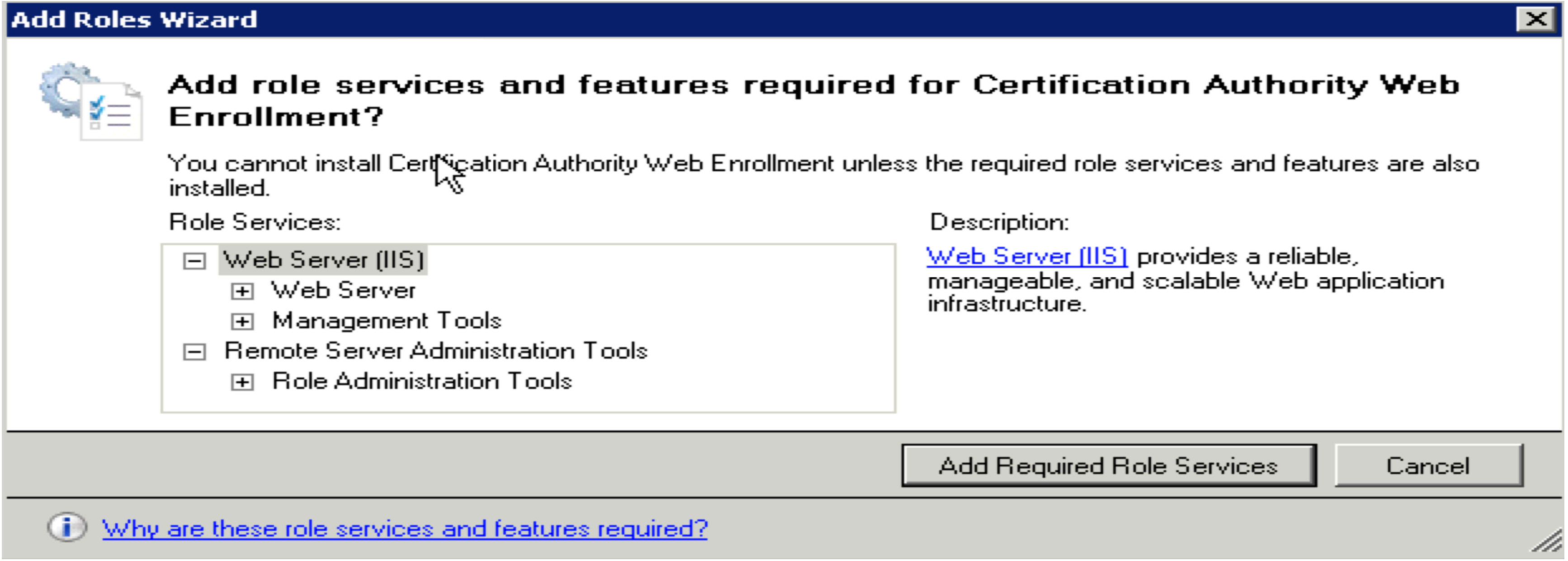
Description:

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

Install Subordinate CA - Contd

Install IIS – prerequisite for CA web enrollment



Add Roles Wizard

Add role services and features required for Certification Authority Web Enrollment?

You cannot install Certification Authority Web Enrollment unless the required role services and features are also installed.

Role Services:

- ⊟ Web Server (IIS)
  - ⊞ Web Server
  - ⊞ Management Tools
- ⊟ Remote Server Administration Tools
  - ⊞ Role Administration Tools

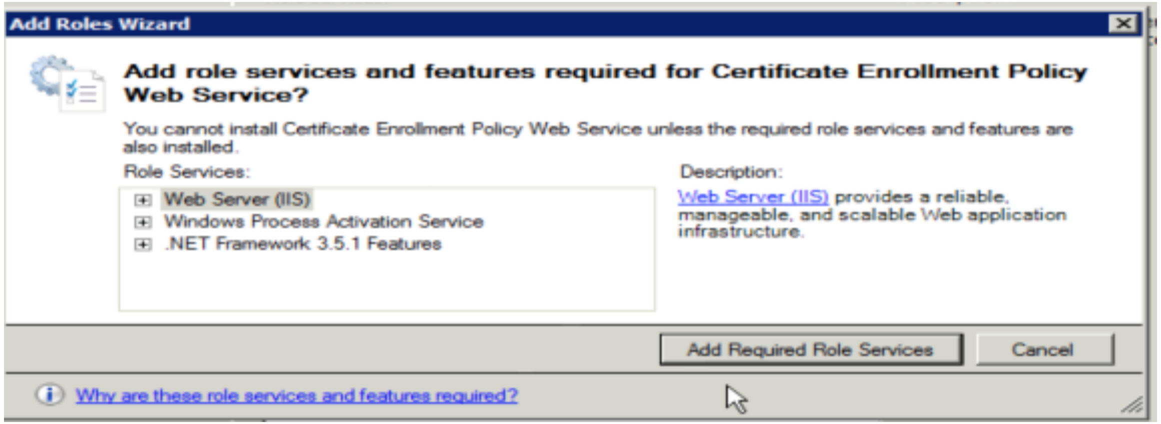
Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Why are these role services and features required?

Install Subordinate CA - Contd

Similar prompt for Certificate Enrollment Policy web service



Add Roles Wizard

Add role services and features required for Certificate Enrollment Policy Web Service?

You cannot install Certificate Enrollment Policy Web Service unless the required role services and features are also installed.

Role Services:

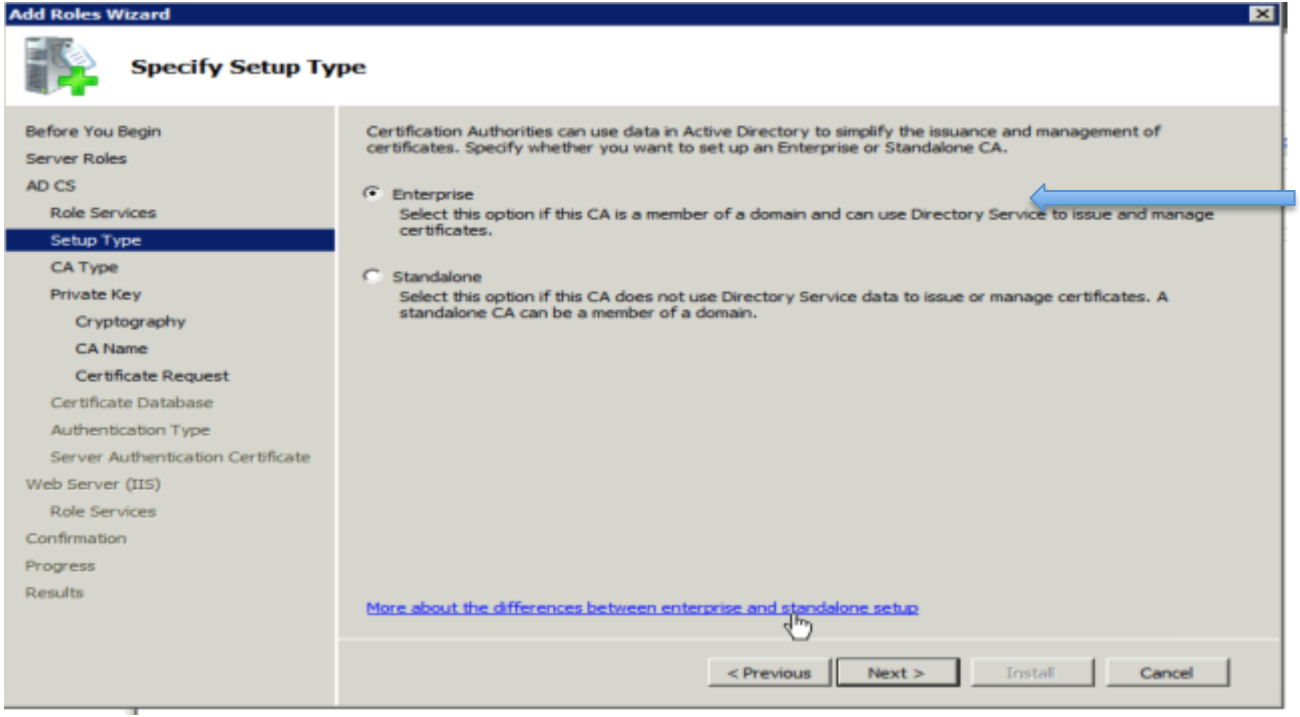
- ⊞ Web Server (IIS)
- ⊞ Windows Process Activation Service
- ⊞ .NET Framework 3.5.1 Features

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Add Required Role Services
Cancel
Why are these role services and features required?

Install Subordinate CA - Contd



Specify Setup Type

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

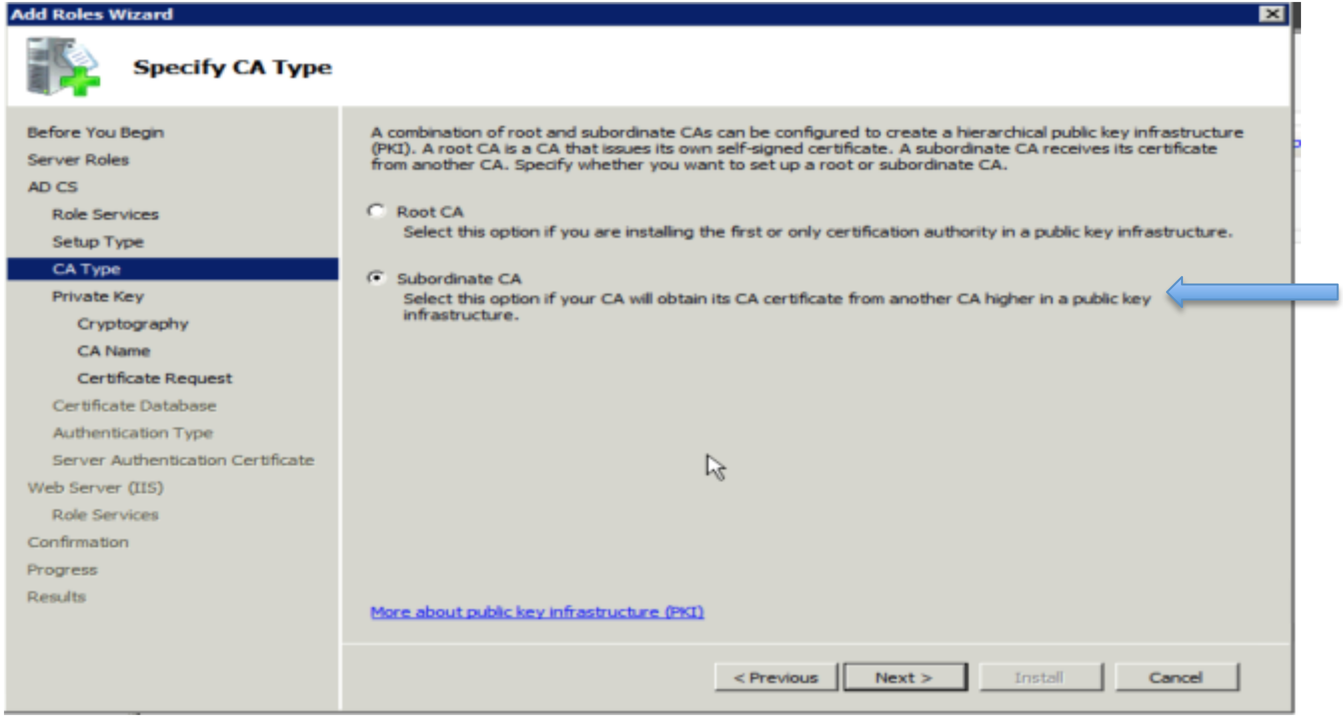
● Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

○ Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

More about the differences between enterprise and standalone setup

Enterprise CA

Install Subordinate CA - Contd



Add Roles Wizard

Specify CA Type

- Before You Begin
- Server Roles
- AD CS
  - Role Services
  - Setup Type
  - CA Type
  - Private Key
    - Cryptography
    - CA Name
    - Certificate Request
  - Certificate Database
  - Authentication Type
  - Server Authentication Certificate
- Web Server (IIS)
  - Role Services
- Confirmation
- Progress
- Results

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

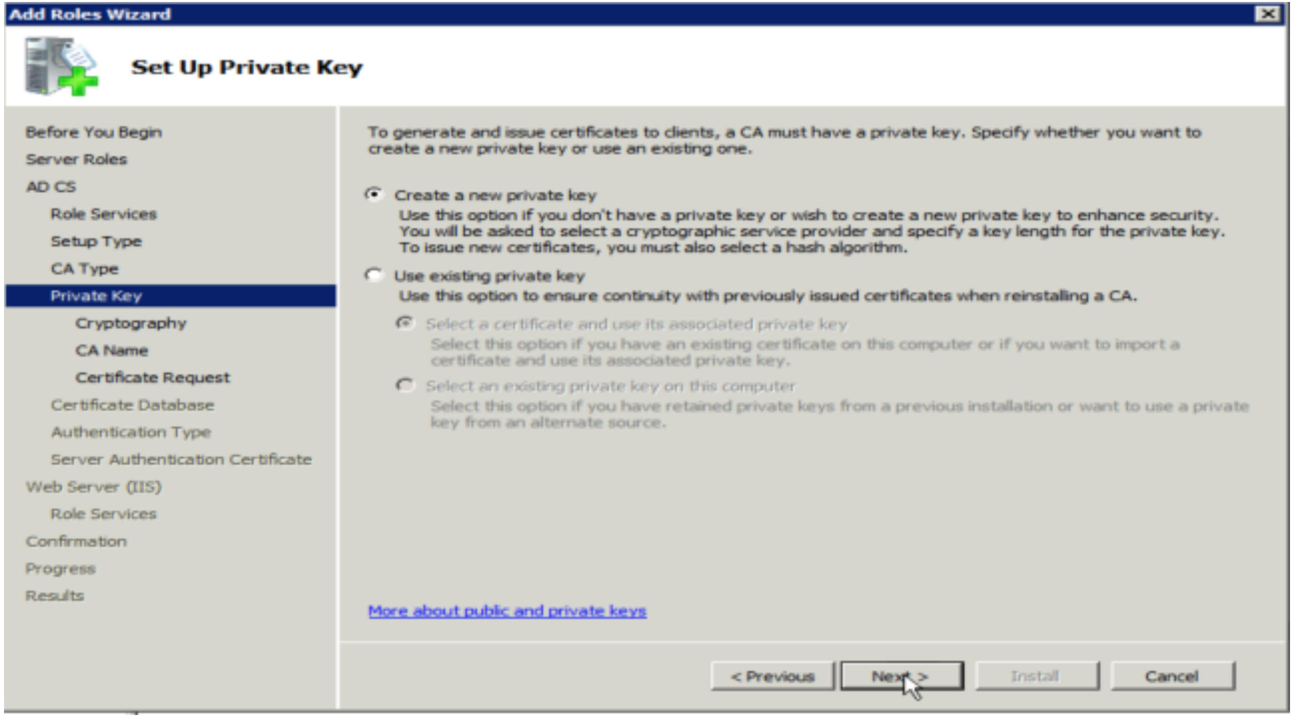
○ Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

● Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

More about public key infrastructure (PKI)

Sub CA

Install Subordinate CA - Contd



To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key

Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key

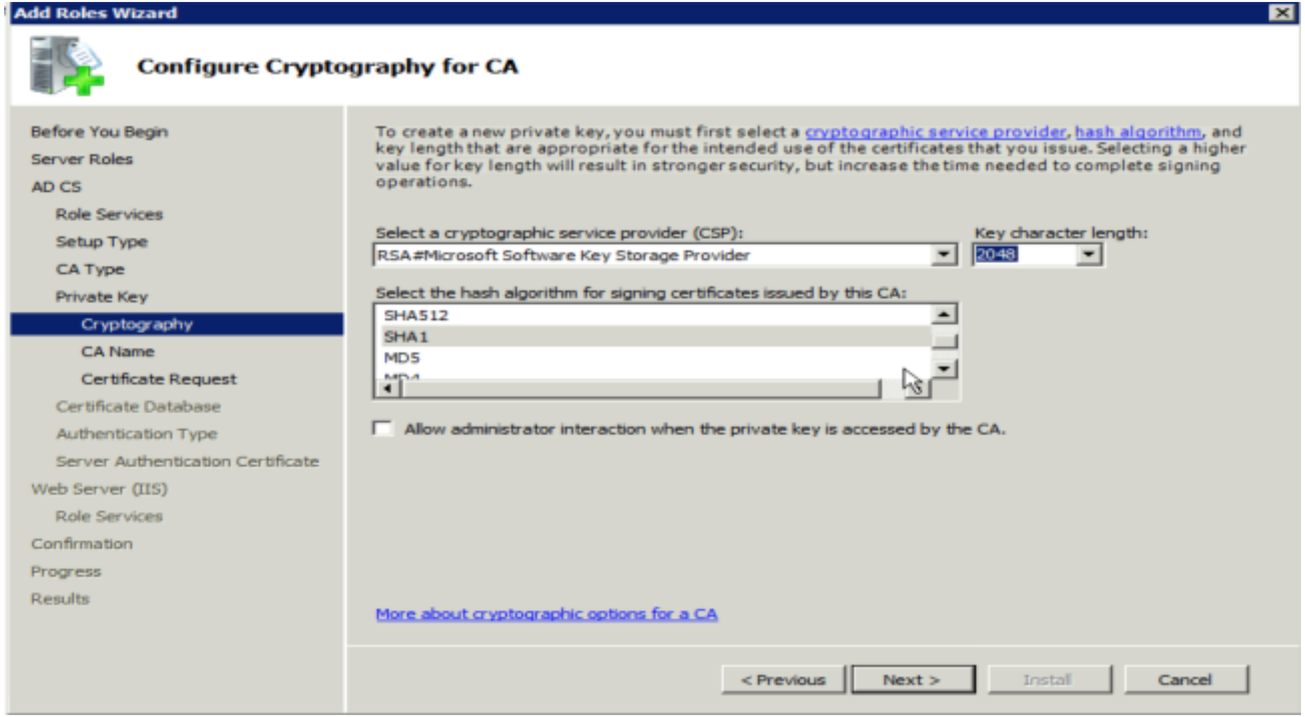
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about public and private keys

Install Subordinate CA - Contd



Configure Cryptography for CA

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

Key character length: 2048

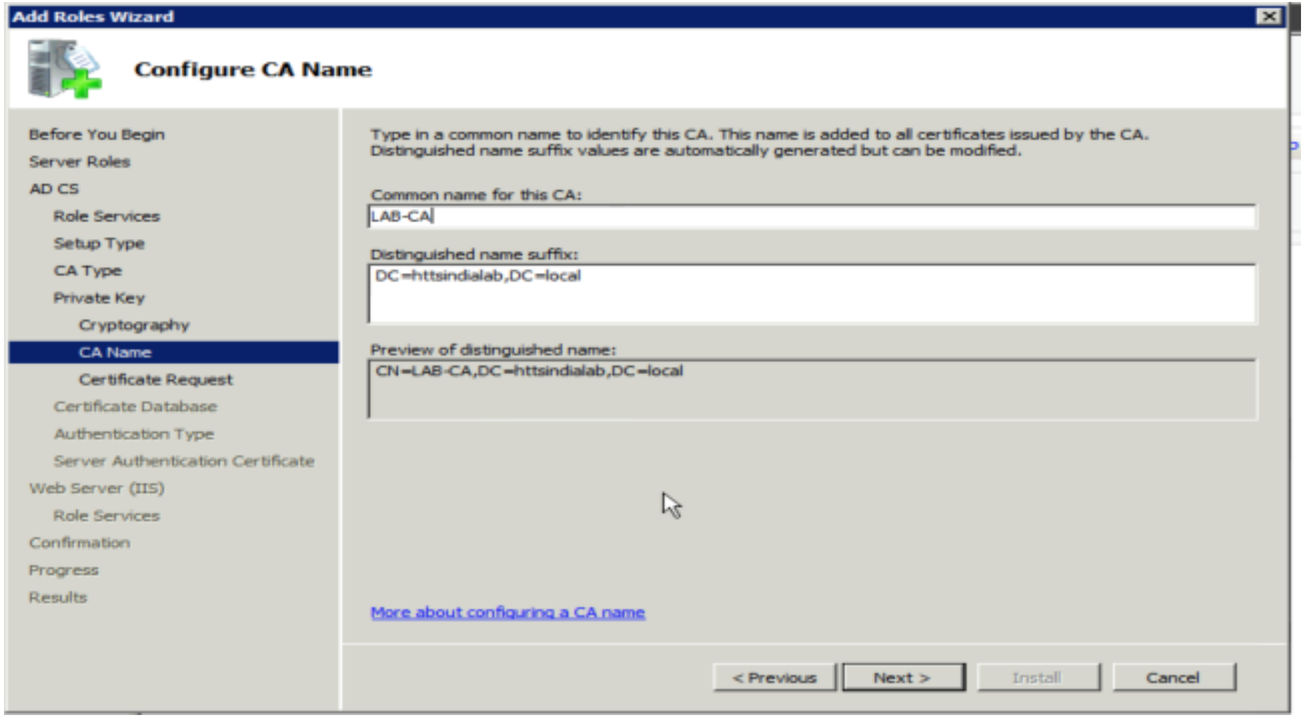
Select the hash algorithm for signing certificates issued by this CA:

SHA512
SHA1
MD5
MD4

□ Allow administrator interaction when the private key is accessed by the CA.

More about cryptographic options for a CA

Install Subordinate CA - Contd



Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

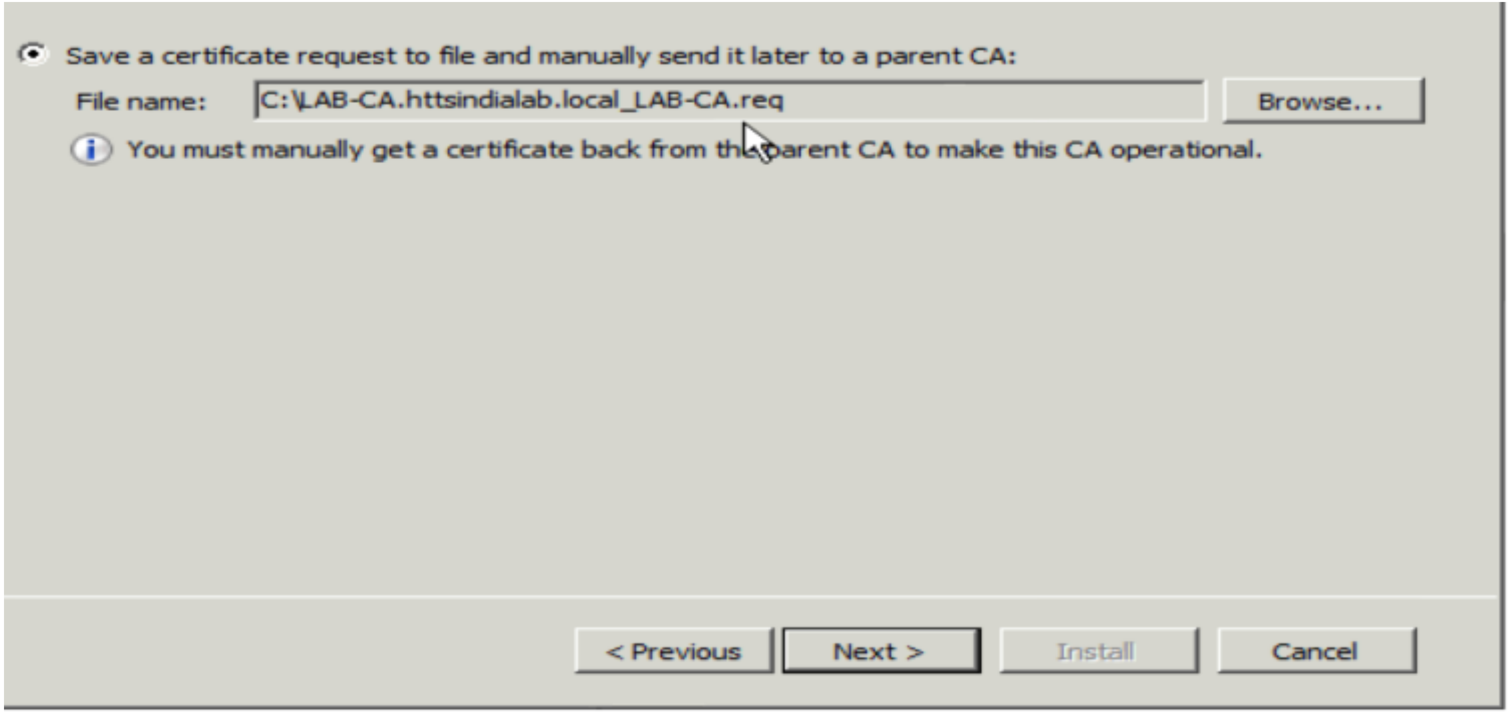
Common name for this CA: LAB-CA

Distinguished name suffix: DC=httsindialab,DC=local

Preview of distinguished name: CN=LAB-CA,DC=httsindialab,DC=local

Install Subordinate CA - Contd

Let the wizard create a CSR for Sub CA

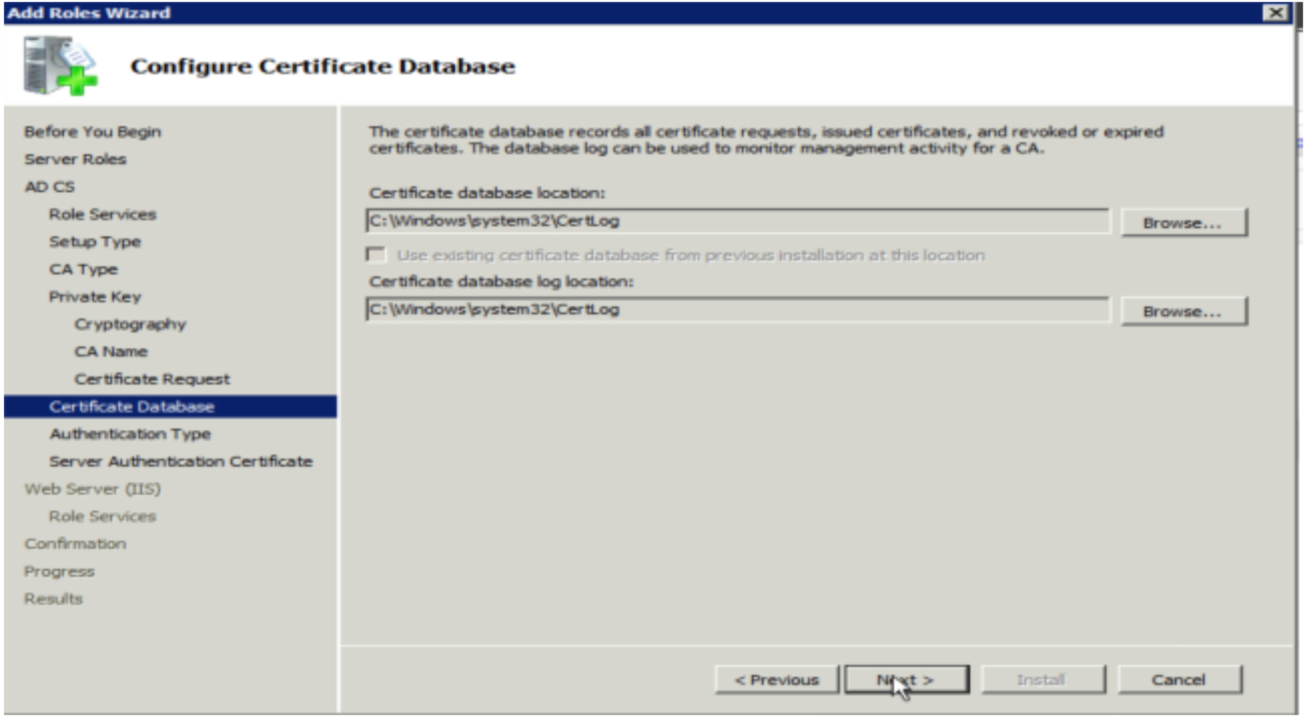


● Save a certificate request to file and manually send it later to a parent CA:

File name: C:\LAB-CA.httsindialab.local_LAB-CA.req

You must manually get a certificate back from the parent CA to make this CA operational.

Install Subordinate CA - Contd



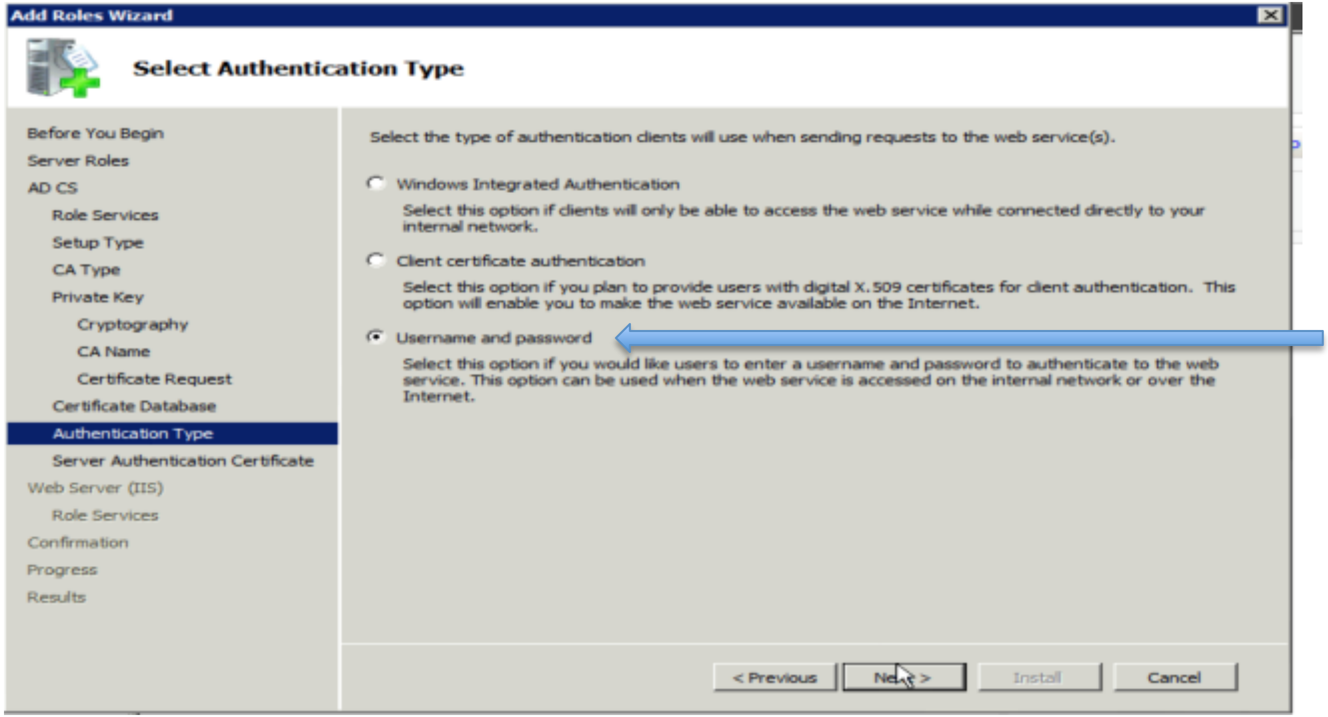
The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

Certificate database location: C:\Windows\system32\CertLog

☐ Use existing certificate database from previous installation at this location

Certificate database log location: C:\Windows\system32\CertLog

Install Subordinate CA - Contd



Select Authentication Type

Select the type of authentication clients will use when sending requests to the web service(s).

○ Windows Integrated Authentication

Select this option if clients will only be able to access the web service while connected directly to your internal network.

○ Client certificate authentication

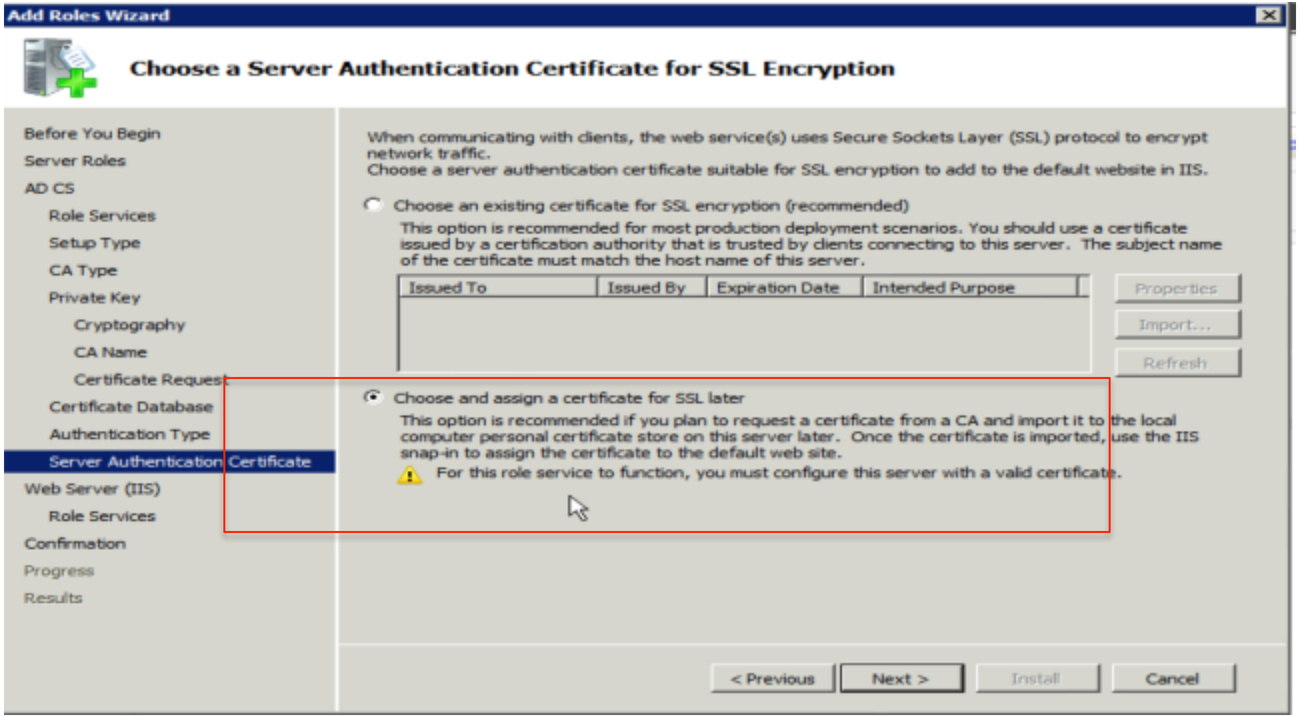
Select this option if you plan to provide users with digital X.509 certificates for client authentication. This option will enable you to make the web service available on the Internet.

● Username and password

Select this option if you would like users to enter a username and password to authenticate to the web service. This option can be used when the web service is accessed on the internal network or over the Internet.

Choose username and password

Install Subordinate CA - Contd



Add Roles Wizard

Choose a Server Authentication Certificate for SSL Encryption

When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.
Choose a server authentication certificate suitable for SSL encryption to add to the default website in IIS.

○ Choose an existing certificate for SSL encryption (recommended)

This option is recommended for most production deployment scenarios. You should use a certificate issued by a certification authority that is trusted by clients connecting to this server. The subject name of the certificate must match the host name of this server.

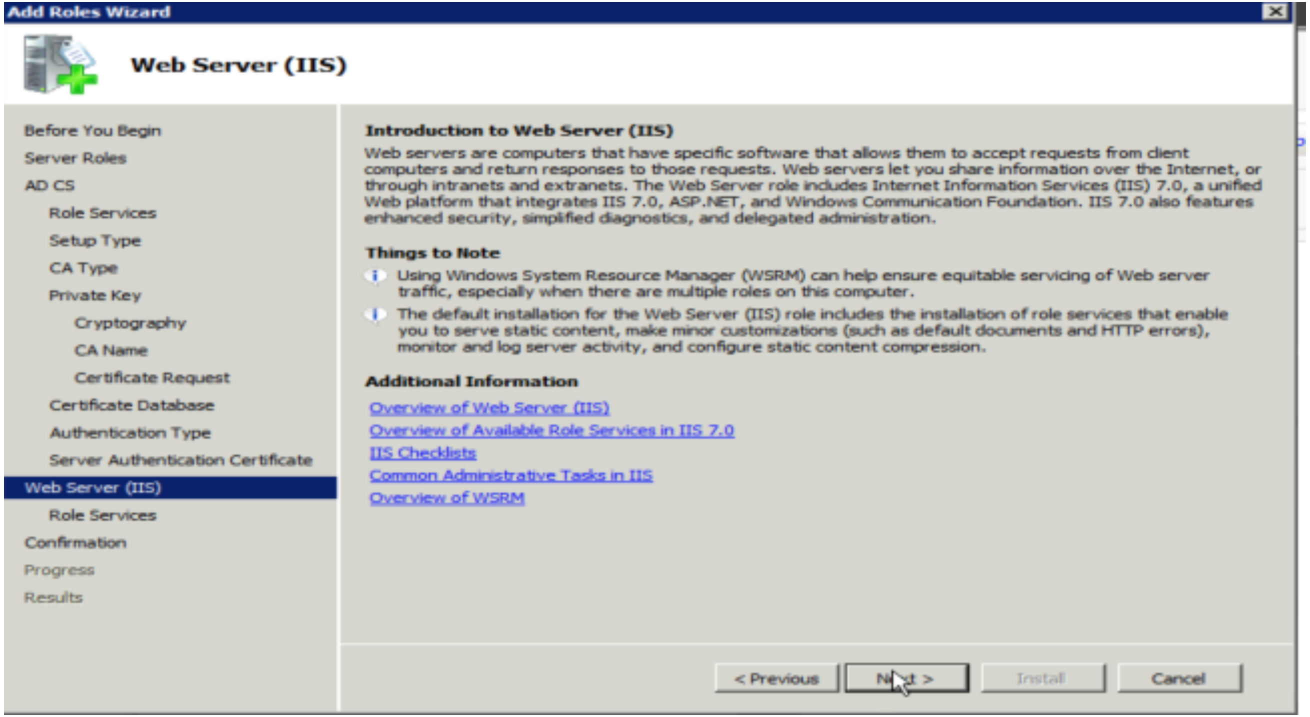
Issued To	Issued By	Expiration Date	Intended Purpose

● Choose and assign a certificate for SSL later

This option is recommended if you plan to request a certificate from a CA and import it to the local computer personal certificate store on this server later. Once the certificate is imported, use the IIS snap-in to assign the certificate to the default web site.

⚠ For this role service to function, you must configure this server with a valid certificate.

Install Subordinate CA - Contd



Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

Things to Note

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Additional Information

Overview of Web Server (IIS)

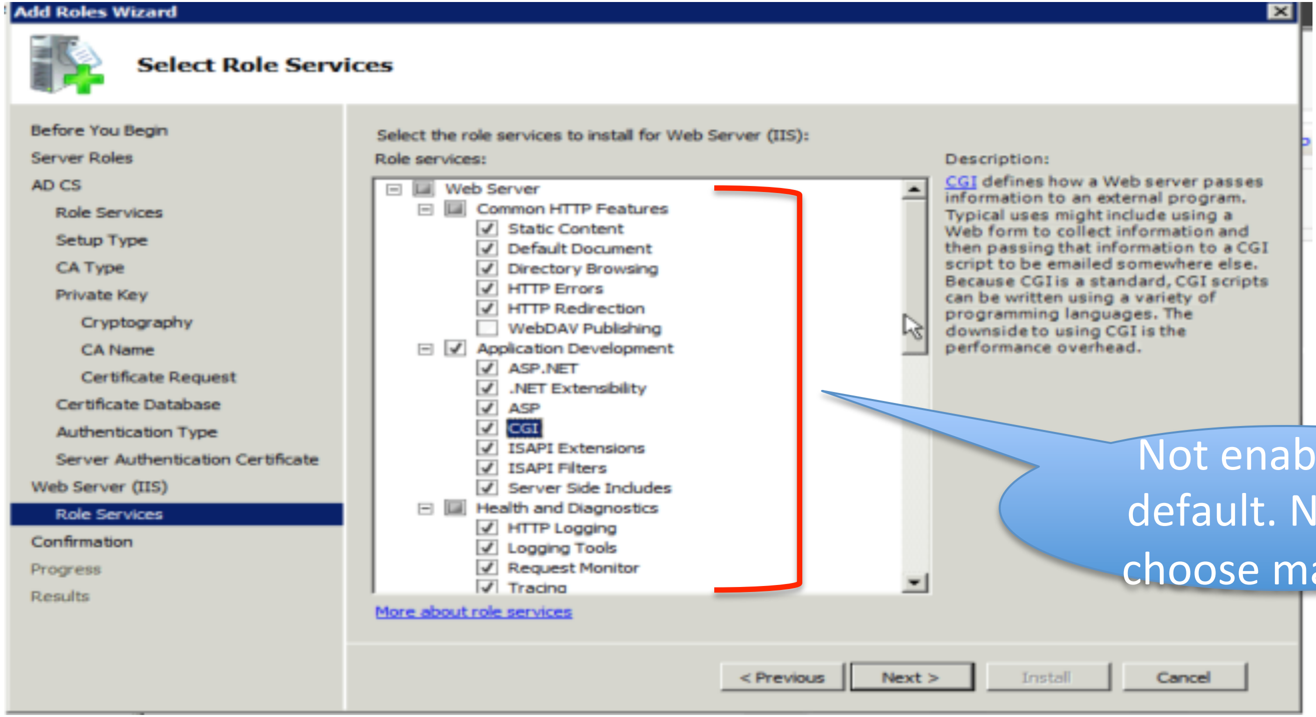
Overview of Available Role Services in IIS 7.0

IIS Checklists

Common Administrative Tasks in IIS

Overview of WSRM

Install Subordinate CA - Contd



Add Roles Wizard

Select Role Services

- Before You Begin
- Server Roles
- AD CS
  - Role Services
  - Setup Type
  - CA Type
  - Private Key
    - Cryptography
    - CA Name
    - Certificate Request
  - Certificate Database
  - Authentication Type
  - Server Authentication Certificate
- Web Server (IIS)
  - **Role Services**
- Confirmation
- Progress
- Results

Select the role services to install for Web Server (IIS):

Role services:

```
⊟ ▣ Web Server
   ⊟ ▣ Common HTTP Features
        ☑ Static Content
        ☑ Default Document
        ☑ Directory Browsing
        ☑ HTTP Errors
        ☑ HTTP Redirection
        □ WebDAV Publishing
   ⊟ ☑ Application Development
        ☑ ASP.NET
        ☑ .NET Extensibility
        ☑ ASP
        ☑ CGI
        ☑ ISAPI Extensions
        ☑ ISAPI Filters
        ☑ Server Side Includes
   ⊟ ▣ Health and Diagnostics
        ☑ HTTP Logging
        ☑ Logging Tools
        ☑ Request Monitor
        ☑ Tracing
```

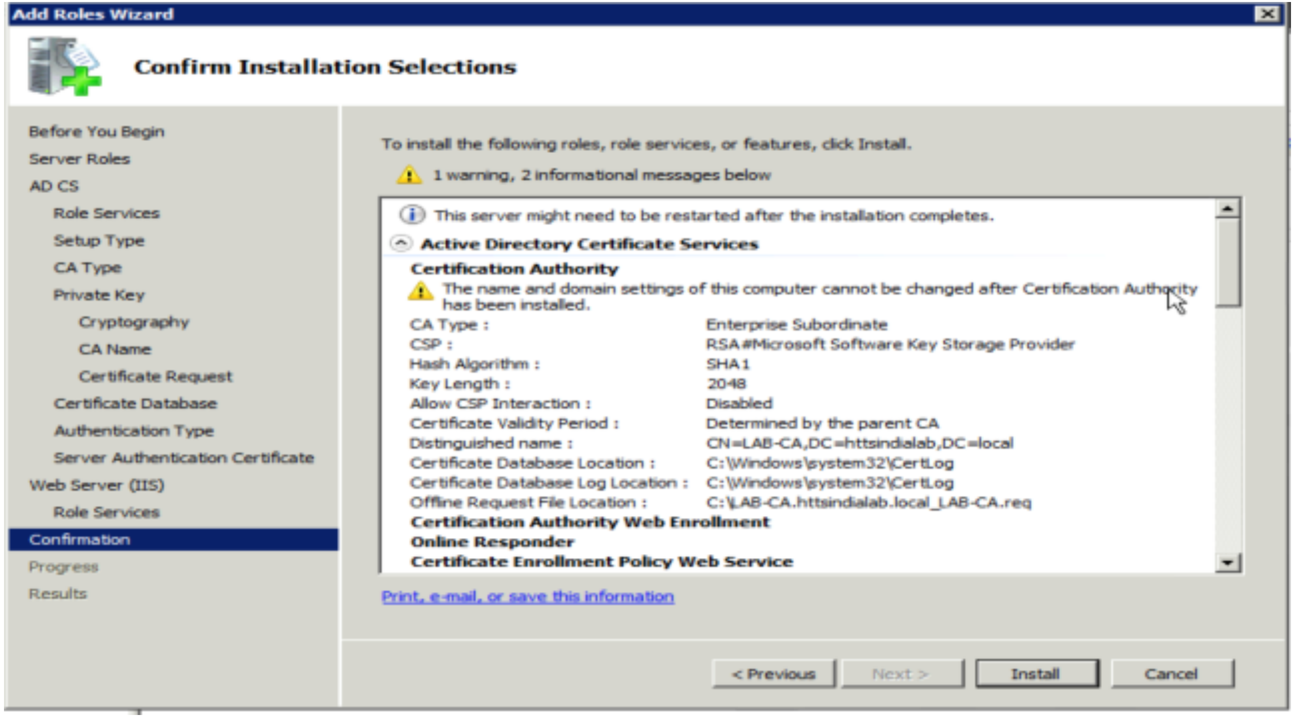
Description:

CGI defines how a Web server passes information to an external program. Typical uses might include using a Web form to collect information and then passing that information to a CGI script to be emailed somewhere else. Because CGI is a standard, CGI scripts can be written using a variety of programming languages. The downside to using CGI is the performance overhead.

More about role services

Not enabled by default. Need to choose manually

Install Subordinate CA - Contd



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

⚠ 1 warning, 2 informational messages below

ⓘ This server might need to be restarted after the installation completes.

Active Directory Certificate Services

Certification Authority

⚠ The name and domain settings of this computer cannot be changed after Certification Authority has been installed.

CA Type :	Enterprise Subordinate
CSP :	RSA#Microsoft Software Key Storage Provider
Hash Algorithm :	SHA1
Key Length :	2048
Allow CSP Interaction :	Disabled
Certificate Validity Period :	Determined by the parent CA
Distinguished name :	CN=LAB-CA,DC=httsindialab,DC=local
Certificate Database Location :	C:\Windows\system32\CertLog
Certificate Database Log Location :	C:\Windows\system32\CertLog
Offline Request File Location :	C:\LAB-CA.httsindialab.local_LAB-CA.req

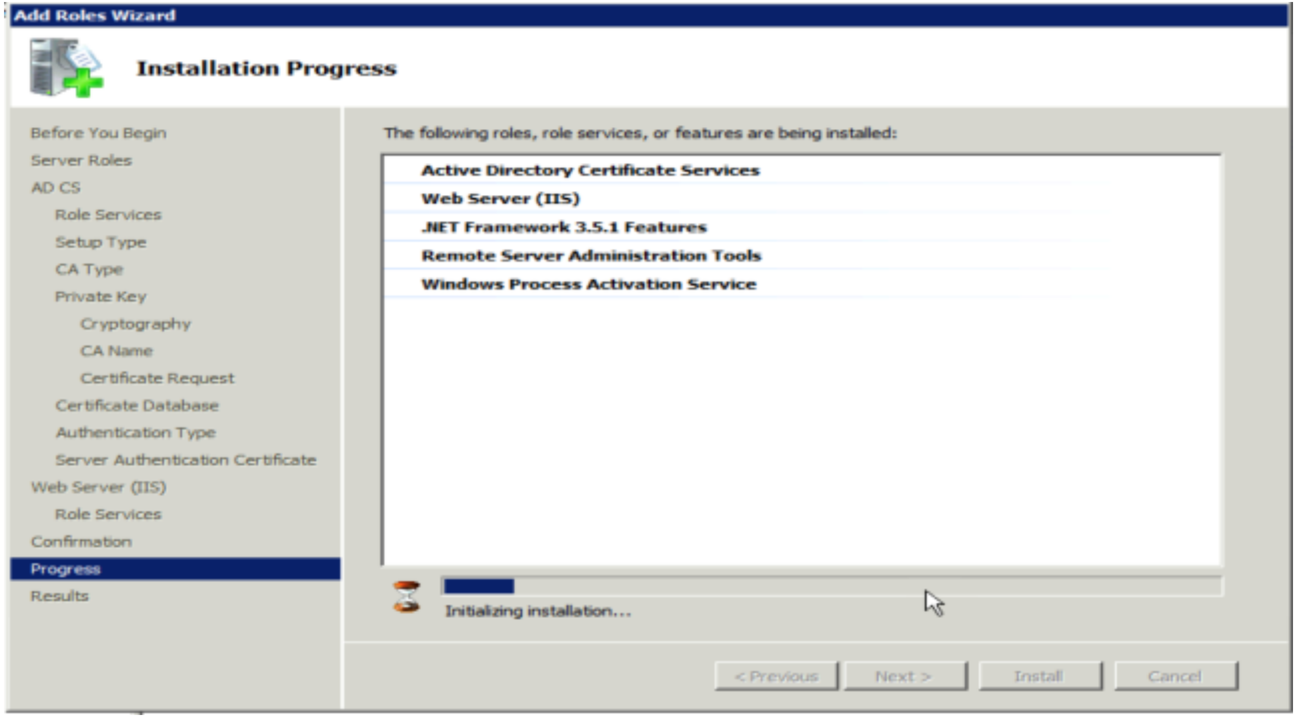
Certification Authority Web Enrollment

Online Responder

Certificate Enrollment Policy Web Service

Print, e-mail, or save this information

Install Subordinate CA - Contd



Installation Progress

The following roles, role services, or features are being installed:

- Active Directory Certificate Services
- Web Server (IIS)
- .NET Framework 3.5.1 Features
- Remote Server Administration Tools
- Windows Process Activation Service

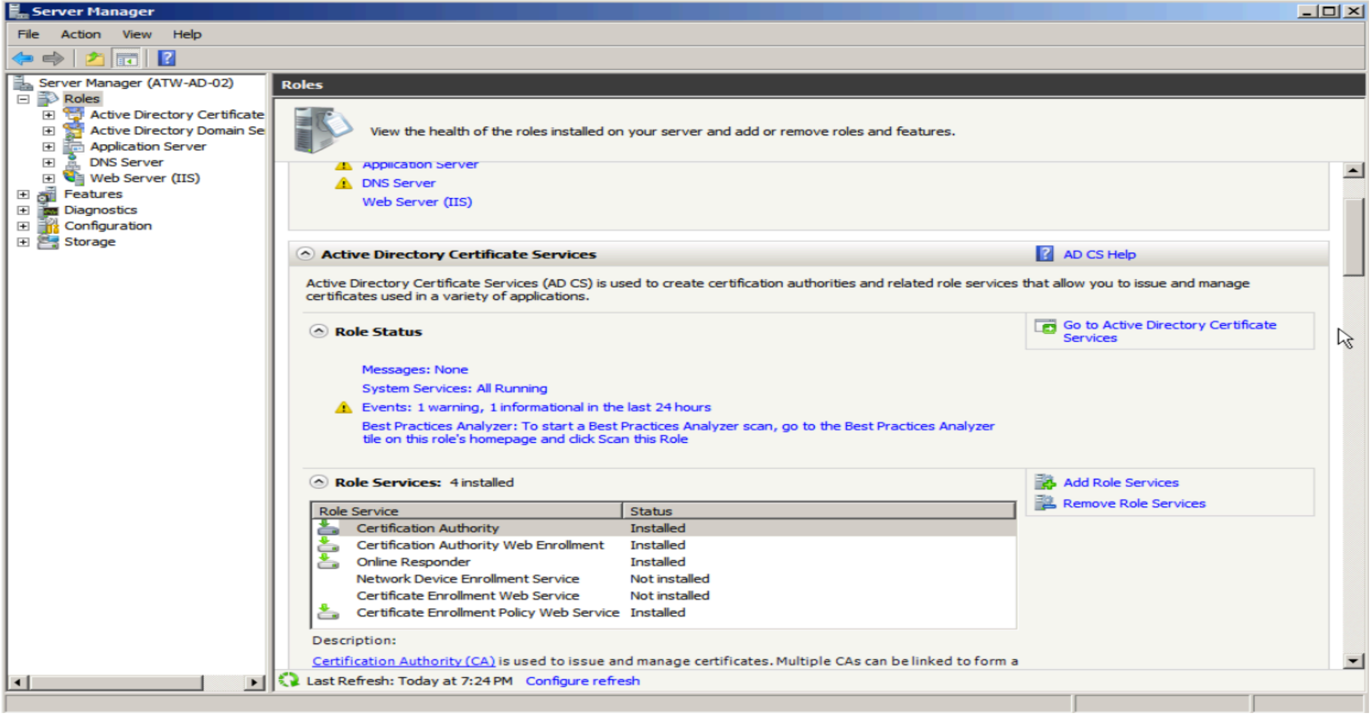
Initializing installation...

Install Subordinate CA - Contd

- Sub CA services would not start until you get the certificate from Root CA.
- In the Certificate Services MMC (certsrv.msc) on the Root CA, select the root node (CA Name), right click, then select **All Tasks**, then **Submit new request (choose the .req file generated at the time of install of Sub CA).**
- The request will now be pending. Navigate to the **Pending Request** Folder and locate the request. Right click on the request, select **All Tasks**, and then **Issue**.
- Export the issued certificate and install it on certificate on Sub CA using Certificate Authority→**Action** menu, point to **All Tasks**, and then click **Install CA Certificate**.

Installation of NDES

NDES installation separately, cannot be with Sub CA



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

Application Server
DNS Server
Web Server (IIS)

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: 1 warning, 1 informational in the last 24 hours

Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

Role Services: 4 installed

Add Role Services

Remove Role Services

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

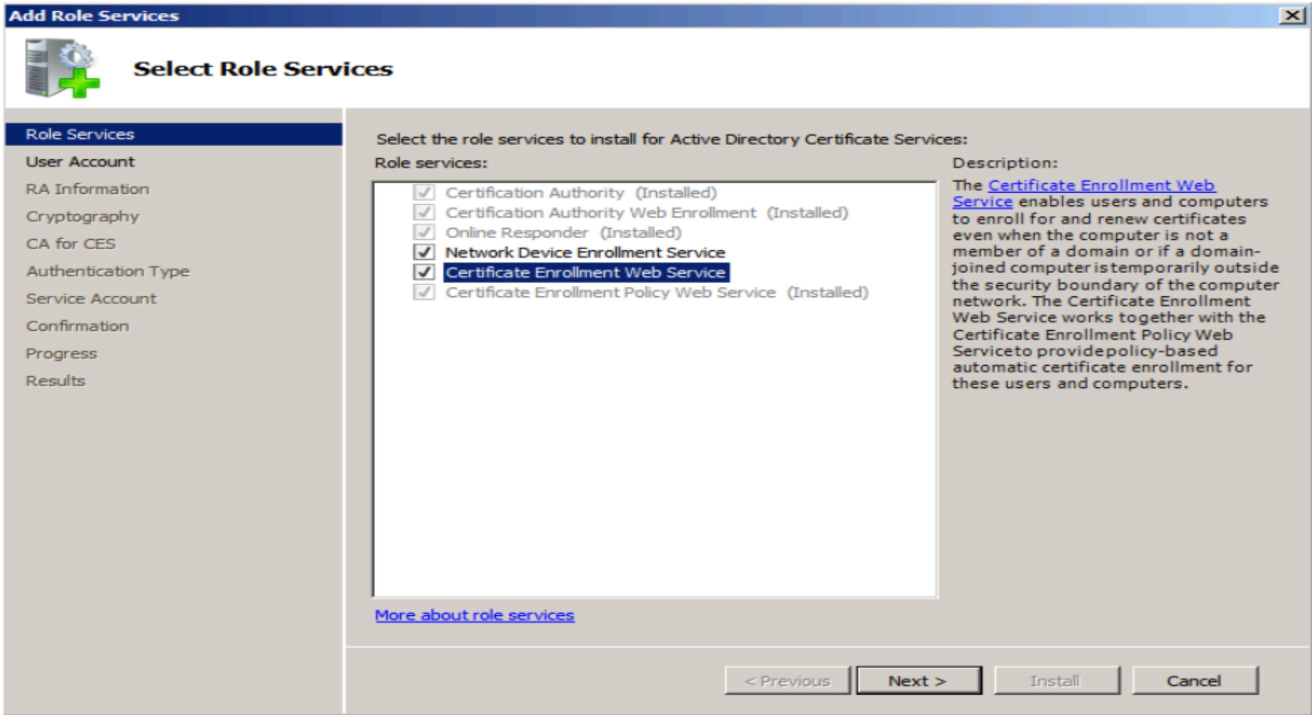
Description:

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a

Last Refresh: Today at 7:24 PM Configure refresh

Installation of NDES Contd

Choose Option 4 and 5 – Network Device Enrollment service and Certificate enrollment web service



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 (Installed)
- ☑ Network Device Enrollment Service
- ☑ Certificate Enrollment Web Service
- ☑ Certificate Enrollment Policy Web Service (Installed)

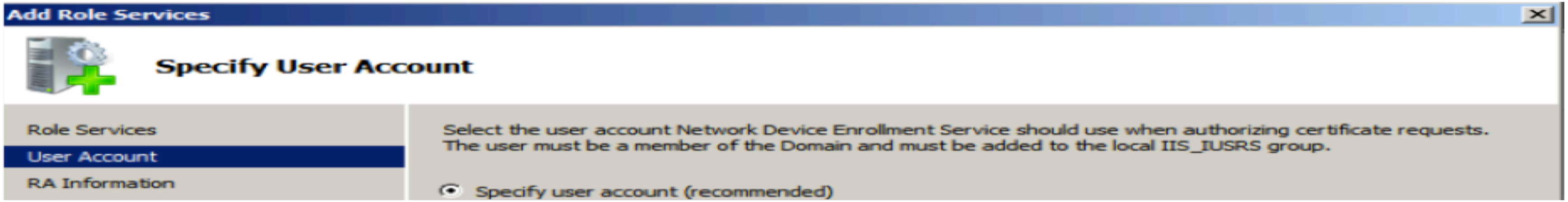
Description:

The Certificate Enrollment Web Service enables users and computers to enroll for and renew certificates even when the computer is not a member of a domain or if a domain-joined computer istemporarily outside the security boundary of the computer network. The Certificate Enrollment Web Service works together with the Certificate Enrollment Policy Web Serviceto providepolicy-based automatic certificate enrollment for these users and computers.

More about role services

Installation of NDES (Contd)

Mention the user account as HTTSINDIALAB\SCEP



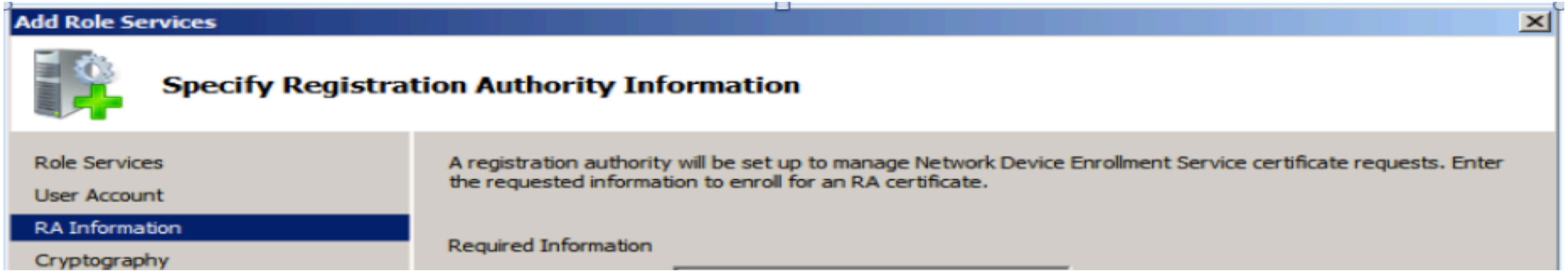
Add Role Services

Specify User Account

Select the user account Network Device Enrollment Service should use when authorizing certificate requests. The user must be a member of the Domain and must be added to the local IIS_IUSRS group.

● Specify user account (recommended)

Installation of NDES (Contd)



Add Role Services

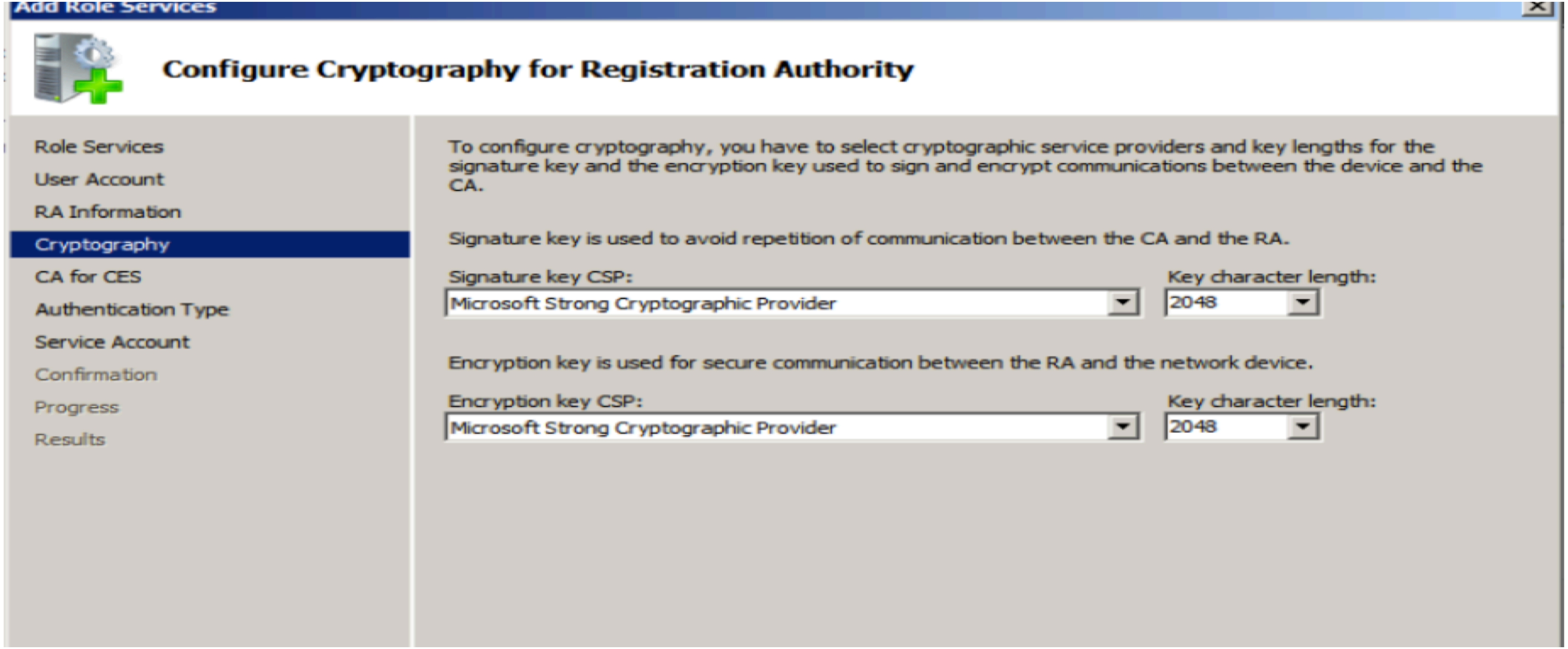
Specify Registration Authority Information

A registration authority will be set up to manage Network Device Enrollment Service certificate requests. Enter the requested information to enroll for an RA certificate.

Required Information

Mention the RA Name as LAB-CA and specify the country

Installation of NDES (Contd)



Configure Cryptography for Registration Authority

To configure cryptography, you have to select cryptographic service providers and key lengths for the signature key and the encryption key used to sign and encrypt communications between the device and the CA.

Signature key is used to avoid repetition of communication between the CA and the RA.

Signature key CSP: Microsoft Strong Cryptographic Provider

Key character length: 2048

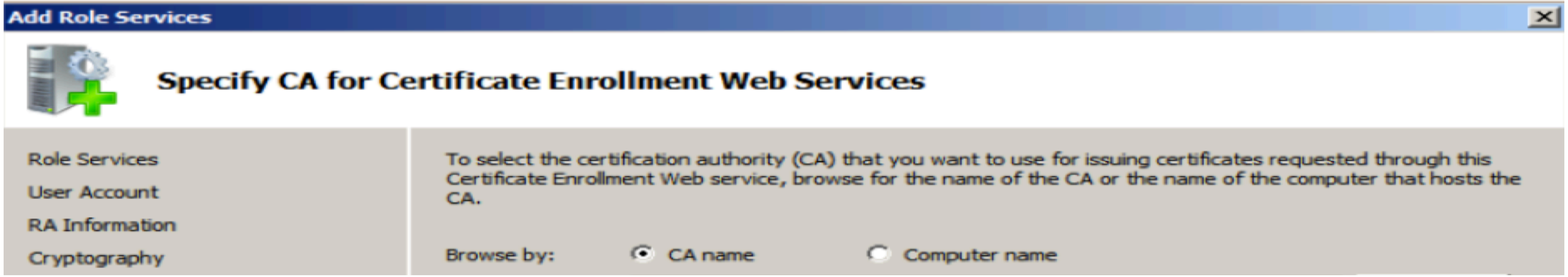
Encryption key is used for secure communication between the RA and the network device.

Encryption key CSP: Microsoft Strong Cryptographic Provider

Key character length: 2048

Installation of NDES (Contd)

In the Specify CA, specify the CA created viz. LAB-CA



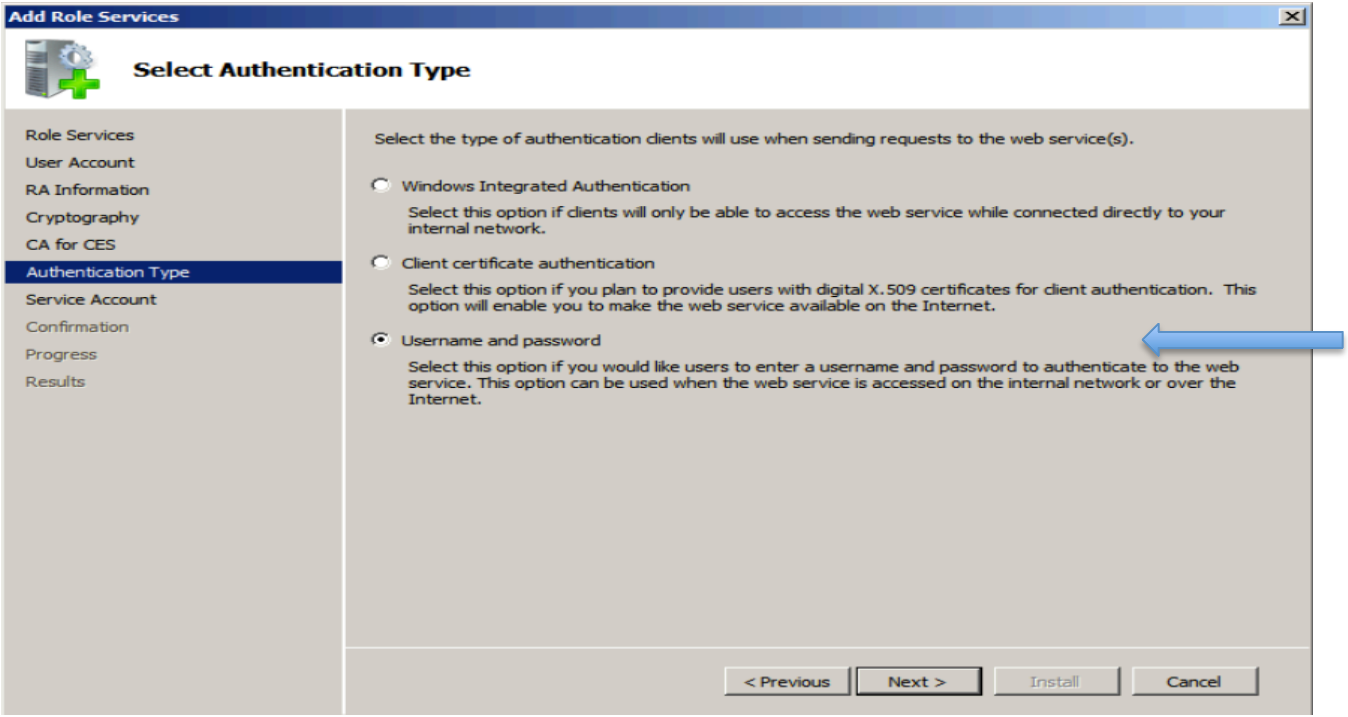
Add Role Services

Specify CA for Certificate Enrollment Web Services

To select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web service, browse for the name of the CA or the name of the computer that hosts the CA.

Browse by: ● CA name ○ Computer name

Installation of NDES (Contd)



Select Authentication Type

Select the type of authentication clients will use when sending requests to the web service(s).

○ Windows Integrated Authentication

Select this option if clients will only be able to access the web service while connected directly to your internal network.

○ Client certificate authentication

Select this option if you plan to provide users with digital X.509 certificates for client authentication. This option will enable you to make the web service available on the Internet.

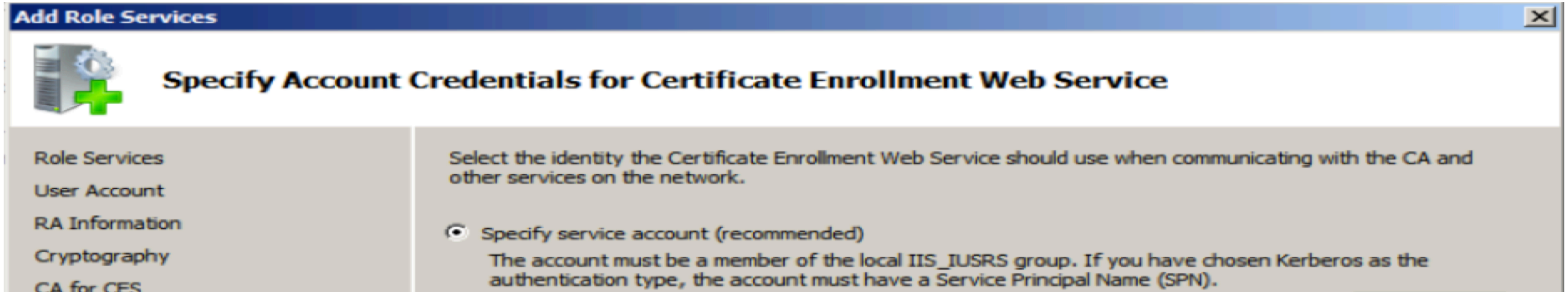
● Username and password

Select this option if you would like users to enter a username and password to authenticate to the web service. This option can be used when the web service is accessed on the internal network or over the Internet.

Username and password

Installation of NDES (Contd)

Specify the SCEP user account that was created



Specify Account Credentials for Certificate Enrollment Web Service

Select the identity the Certificate Enrollment Web Service should use when communicating with the CA and other services on the network.

● Specify service account (recommended)

The account must be a member of the local IIS_IUSRS group. If you have chosen Kerberos as the authentication type, the account must have a Service Principal Name (SPN).

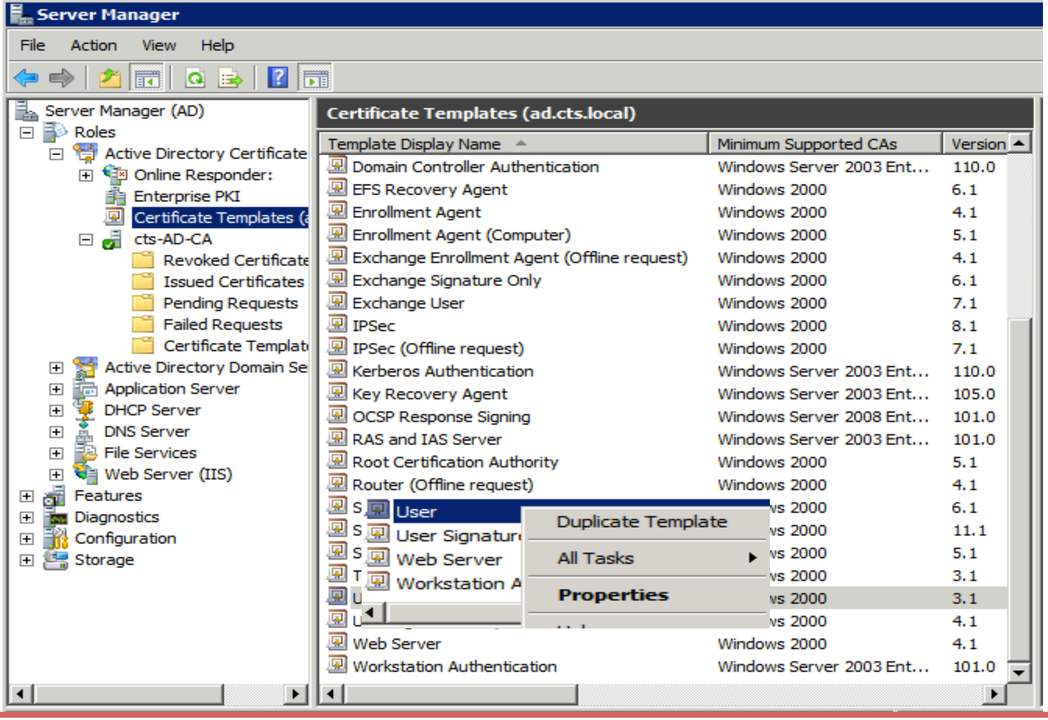
Post installation tasks

In the post installation tasks, we will cover:

- Certificate template configuration
- Registry changes

Certificate template configuration

Clone user template on Root CA for user certificate

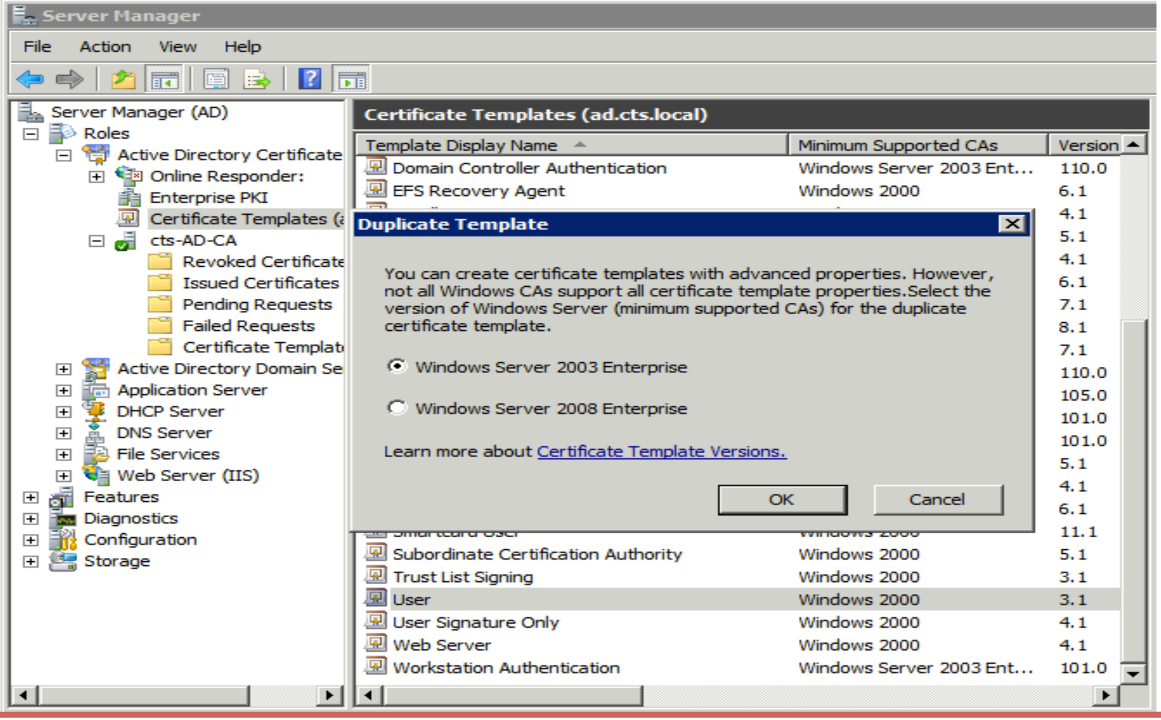


Server Manager (AD)
- Roles
  - Active Directory Certificate
    - Online Responder:
    - Enterprise PKI
    - Certificate Templates (
    - cts-AD-CA
      - Revoked Certificate
      - Issued Certificates
      - Pending Requests
      - Failed Requests
      - Certificate Templat
  - Active Directory Domain Se
  - Application Server
  - DHCP Server
  - DNS Server
  - File Services
  - Web Server (IIS)
- Features
- Diagnostics
- Configuration
- Storage

Certificate Templates (ad.cts.local)

Template Display Name	Minimum Supported CAs	Version
Domain Controller Authentication	Windows Server 2003 Ent...	110.0
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
Key Recovery Agent	Windows Server 2003 Ent...	105.0
OCSP Response Signing	Windows Server 2008 Ent...	101.0
RAS and IAS Server	Windows Server 2003 Ent...	101.0
Root Certification Authority	Windows 2000	5.1
Router (Offline request)	Windows 2000	4.1
S	ws 2000	6.1
S	ws 2000	11.1
S	ws 2000	5.1
T	ws 2000	3.1
U	ws 2000	3.1
U	ws 2000	4.1
Web Server	Windows 2000	4.1
Workstation Authentication	Windows Server 2003 Ent...	101.0

Certificate template configuration (Contd)



Certificate Templates (ad.cts.local)

Template Display Name	Minimum Supported CAs	Version
Domain Controller Authentication	Windows Server 2003 Ent...	110.0
EFS Recovery Agent	Windows 2000	6.1
		4.1
		5.1
		4.1
		6.1
		7.1
		8.1
		7.1
		110.0
		105.0
		101.0
		101.0
		5.1
		4.1
		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	Windows 2000	4.1
Web Server	Windows 2000	4.1
Workstation Authentication	Windows Server 2003 Ent...	101.0

Duplicate Template

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.

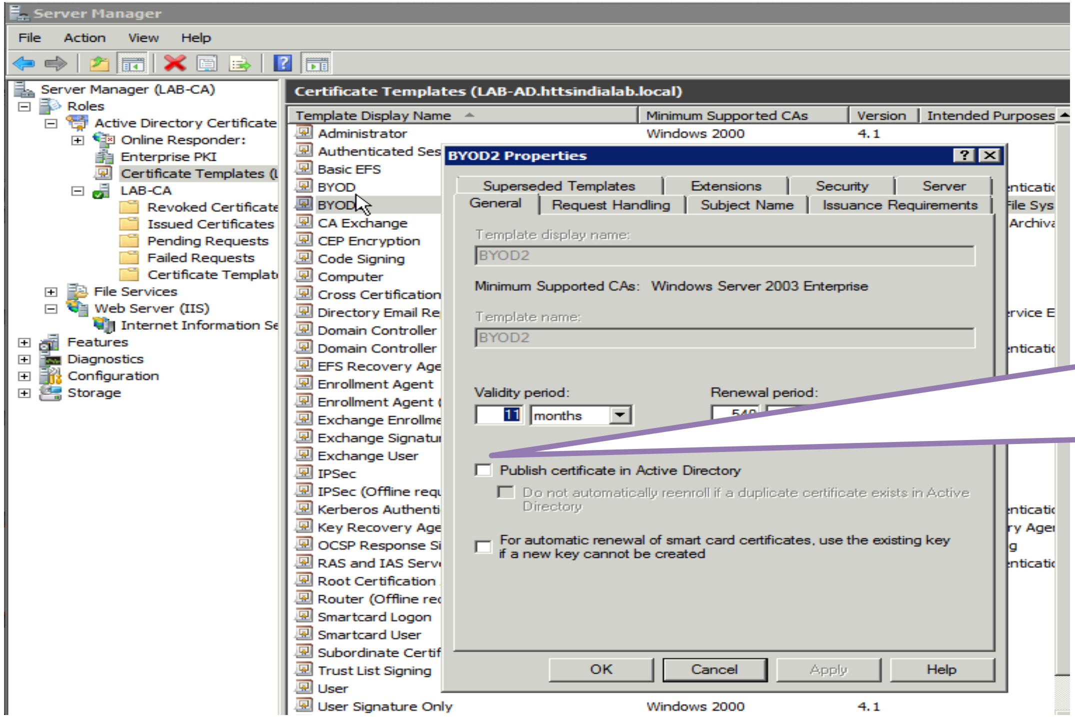
● Windows Server 2003 Enterprise

○ Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

OK Cancel

Certificate template configuration (Contd)



Certificate Templates (LAB-AD.httsindialab.local)

Template Display Name	Minimum Supported CAs	Version	Intended Purposes
Administrator	Windows 2000	4.1	
Authenticated Ses			
Basic EFS			
BYOD			nticatic
BYOD2			File Sys
CA Exchange			Archiva
CEP Encryption			
Code Signing			
Computer			
Cross Certification			
Directory Email Re			rvice E
Domain Controller			
Domain Controller			nticatic
EFS Recovery Age			
Enrollment Agent			
Enrollment Agent (			
Exchange Enrollme			
Exchange Signatu			
Exchange User			
IPSec			
IPSec (Offline requ			
Kerberos Authenti			nticatic
Key Recovery Age			ry Agei
OCSP Response Si			g
RAS and IAS Serv			nticatic
Root Certification			
Router (Offline rec			
Smartcard Logon			
Smartcard User			
Subordinate Certif			
Trust List Signing			
User			
User Signature Only	Windows 2000	4.1	

BYOD2 Properties

Template display name: BYOD2

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name: BYOD2

Validity period: 11 months

Renewal period: 540

□ Publish certificate in Active Directory

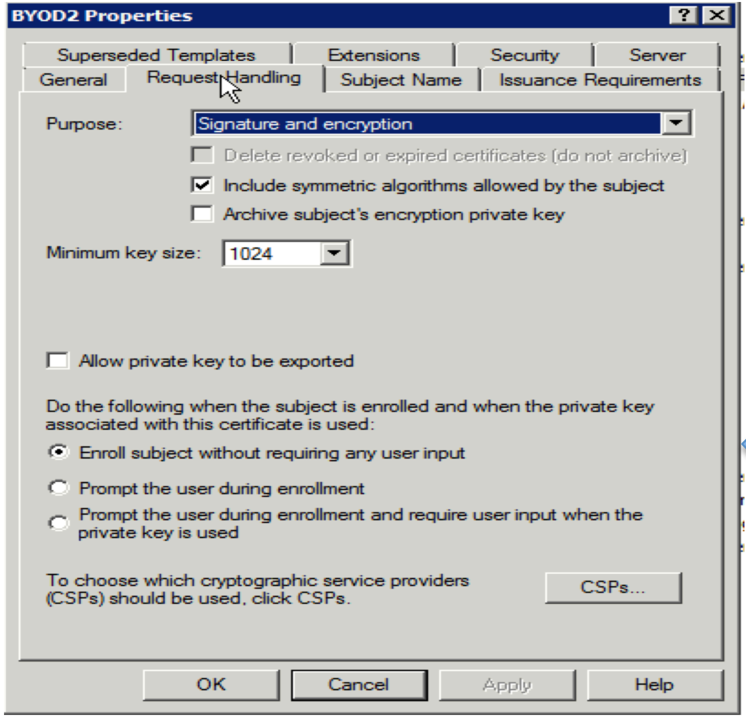
□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

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

Uncheck this!!

This option publishes all generated certificates to the user object used as the NDES service account and may eventually exceed the limits of numbers of published certificates for an AD user.

Certificate template configuration (Contd)



BYOD2 Properties

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

Minimum key size: 1024

□ 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

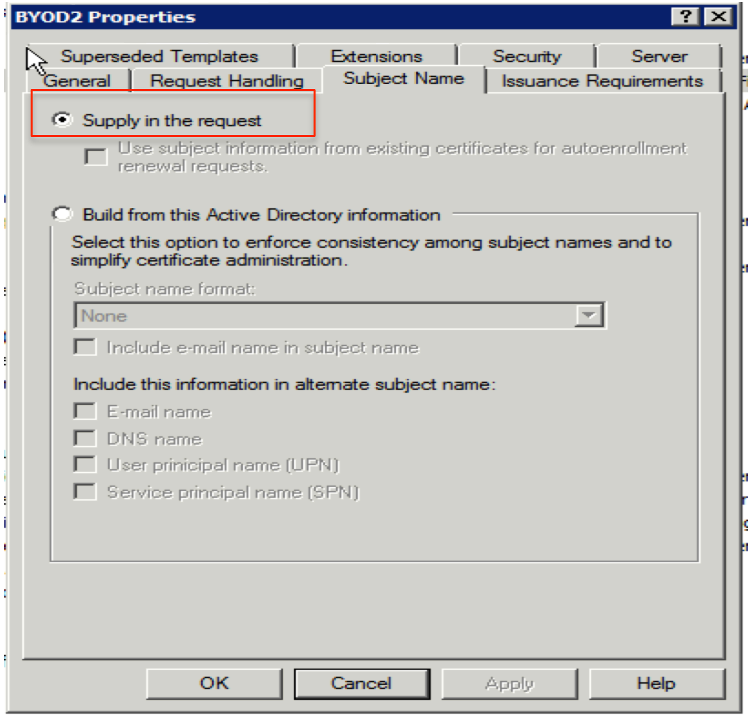
○ Prompt the user during enrollment

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

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

Enroll without user input to make it fully automated

Certificate template configuration (Contd)



● 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:

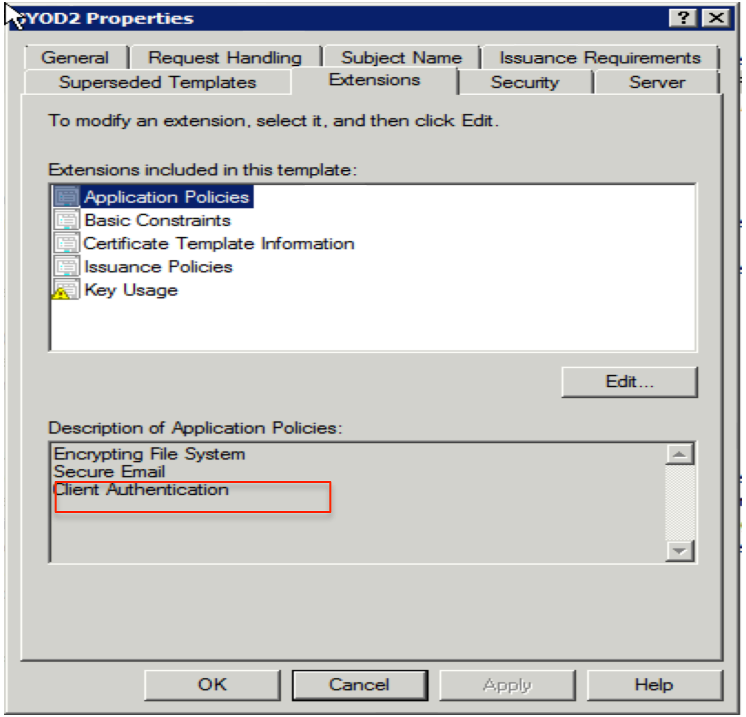
□ E-mail name

□ DNS name

□ User prinicipal name (UPN)

□ Service principal name (SPN)

Certificate template configuration (Contd)



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

Extensions included in this template:

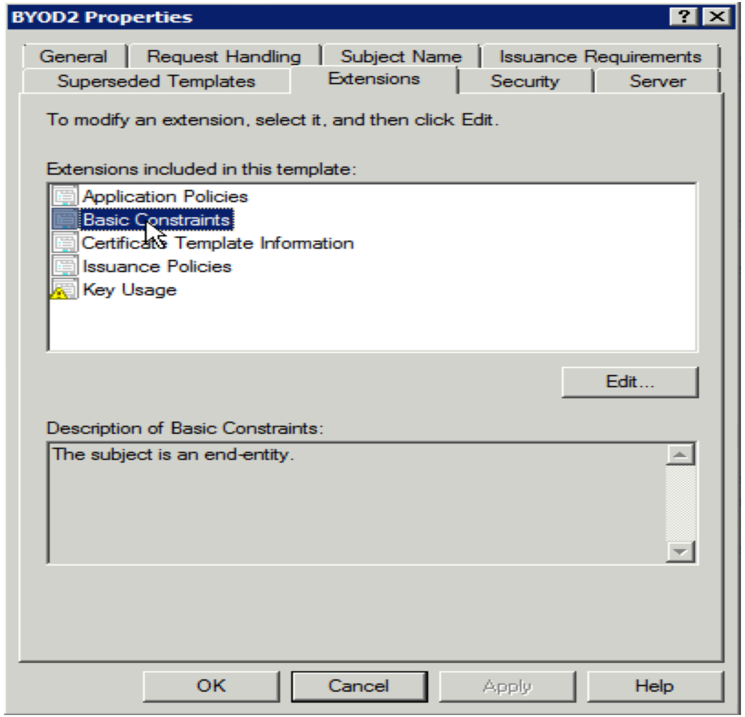
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Encrypting File System
Secure Email
Client Authentication

Client Authentication

Certificate template configuration (Contd)



BYOD2 Properties

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

Extensions included in this template:

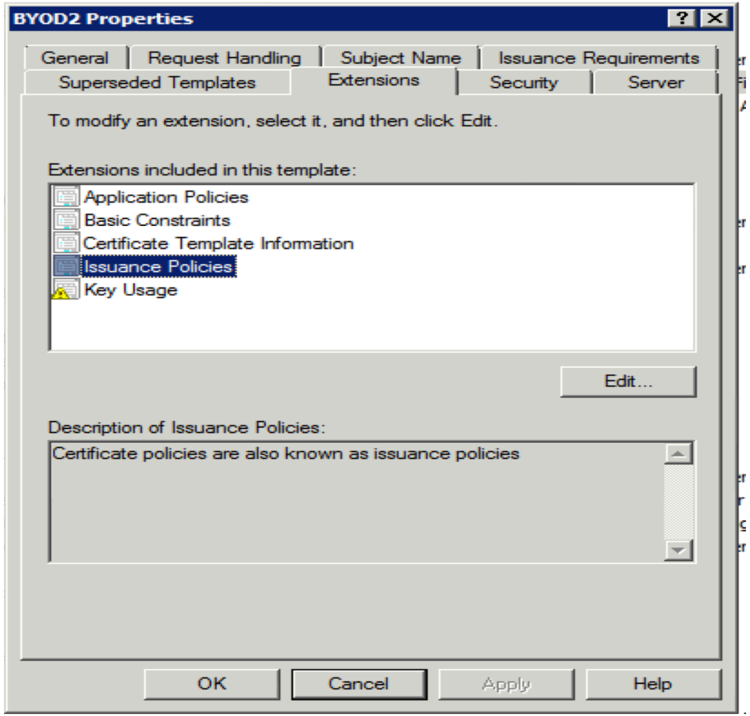
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Basic Constraints:

The subject is an end-entity.

Certificate template configuration (Contd)

Issuance Policies left at default. If choosing "All Issuance policies", ensure that SubCA is given adequate privileges by Root CA



BYOD2 Properties

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

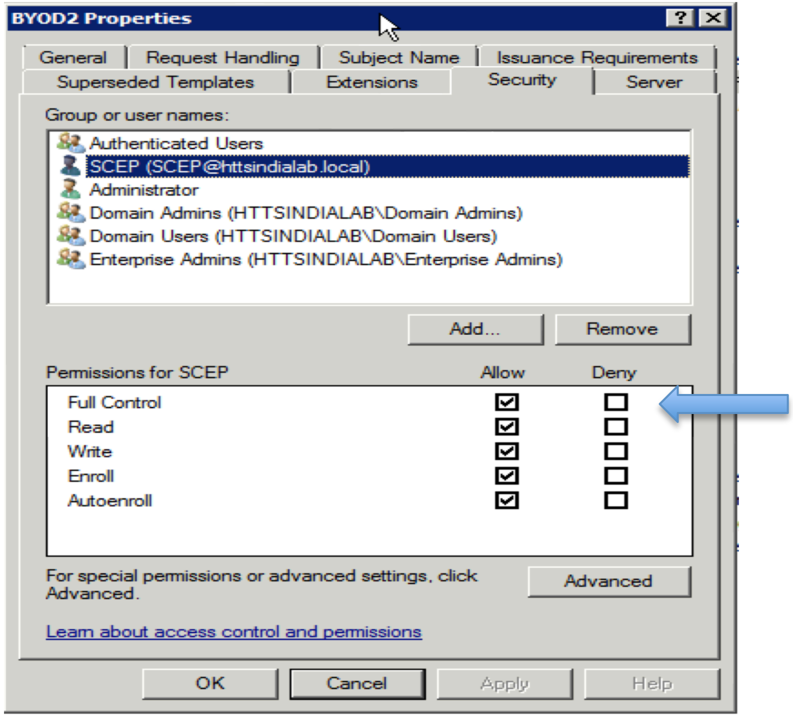
Extensions included in this template:

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

Description of Issuance Policies:

Certificate policies are also known as issuance policies

Certificate template configuration (Contd)



Group or user names:

- Authenticated Users
- SCEP (SCEP@httsindialab.local)
- Administrator
- Domain Admins (HTTSINDIALAB\Domain Admins)
- Domain Users (HTTSINDIALAB\Domain Users)
- Enterprise Admins (HTTSINDIALAB\Enterprise Admins)

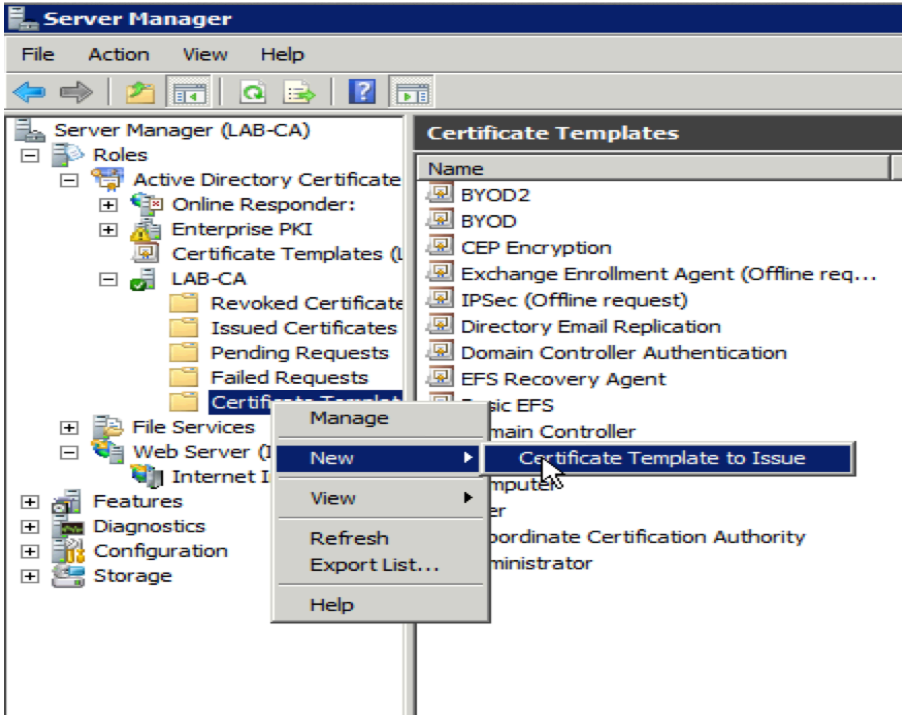
Permissions for SCEP	Allow	Deny
Full Control	☑	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.

Full control for SCEP User on Certificate Template

Certificate template configuration (Contd)

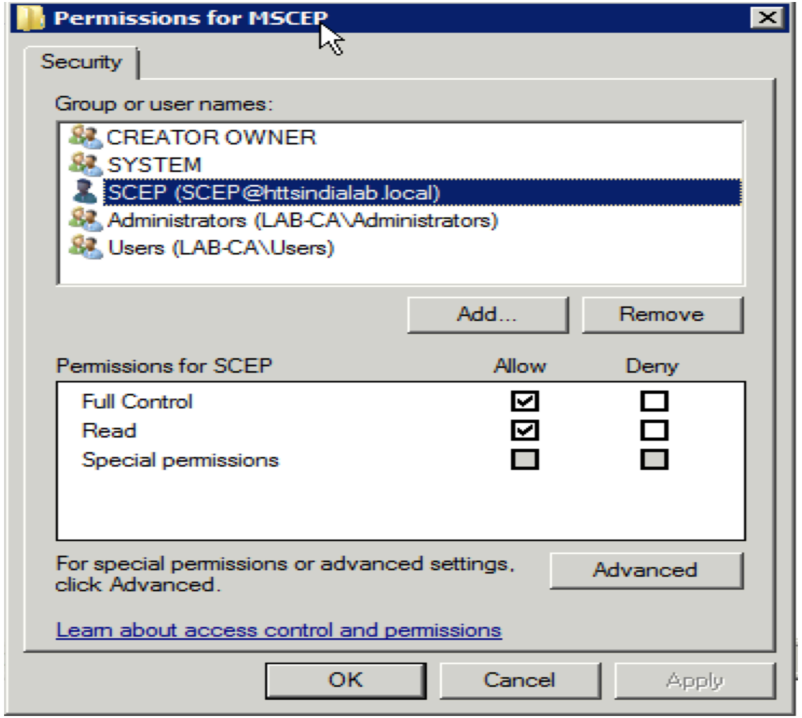
Lab CA→Choose the certificate template cloned earlier (BYOD2)



Registry changes

Note: Better to backup the registry before making any changes first

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP→Right click permissions



Permissions for MSCEP

Group or user names:

- CREATOR OWNER
- SYSTEM
- SCEP (SCEP@httsindialab.local)
- Administrators (LAB-CA\Administrators)
- Users (LAB-CA\Users)

Permissions for SCEP	Allow	Deny
Full Control	☑	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Full control for SCEP user

Registry changes (Contd)

Modify two more registry values for password to ensure a complete automated cert enrollment

- Set EnforcePassword to 0 under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

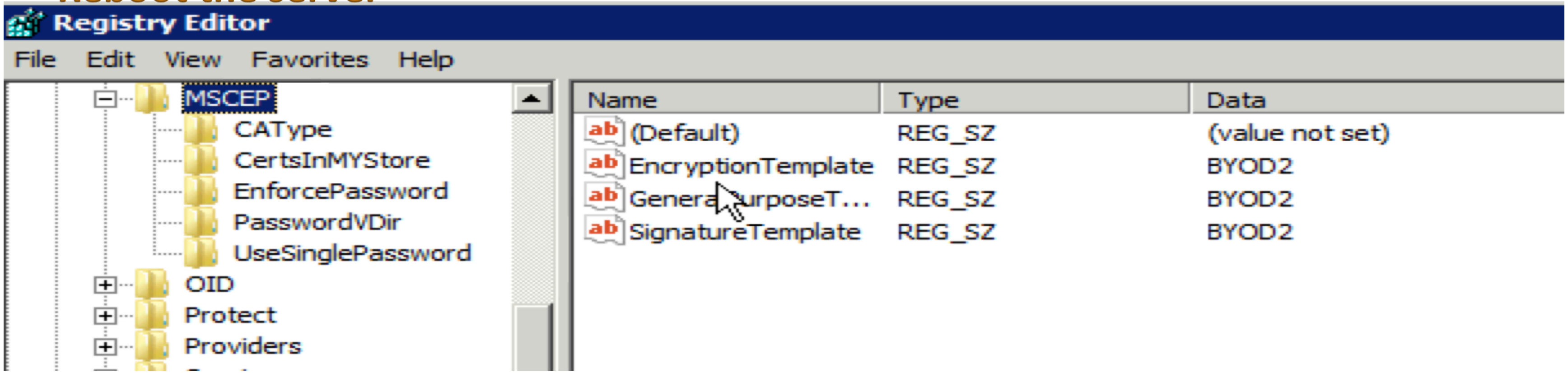
- Set UseSinglePassword to 0 under the same key.

MSCEP Certificate template changes in Registry

HKLM → Software → Microsoft → Cryptography → MSCEP

Set 3 Registry Values (Encryption template, General Purpose and Signature template) to name of your newly created template (BYOD2)

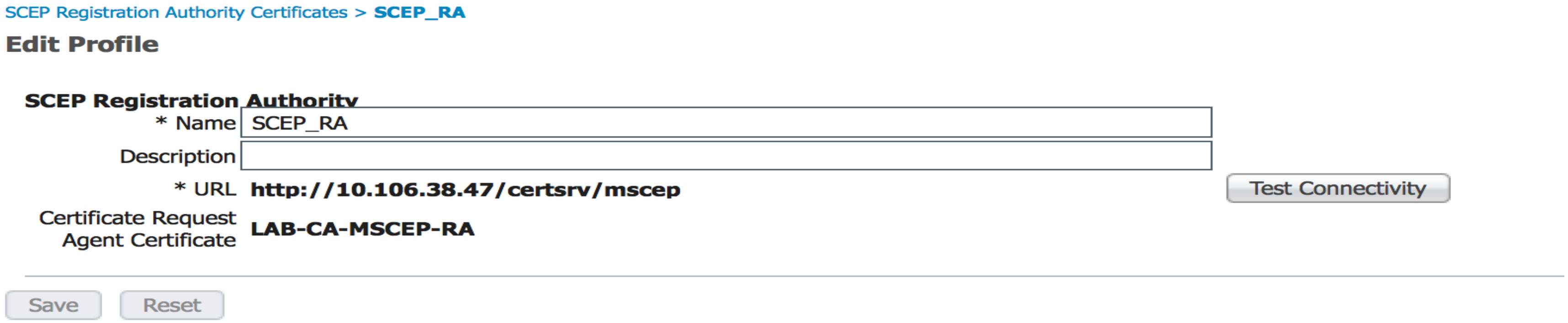
Reboot the server



Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	BYOD2
GeneralPurposeT...	REG_SZ	BYOD2
SignatureTemplate	REG_SZ	BYOD2

ISE SCEP CA Profile

Enable ISE to act as SCEP proxy
Administration→System-→Certificates→SCEP RA Profile



SCEP Registration Authority Certificates > **SCEP_RA**

Edit Profile

SCEP Registration Authority

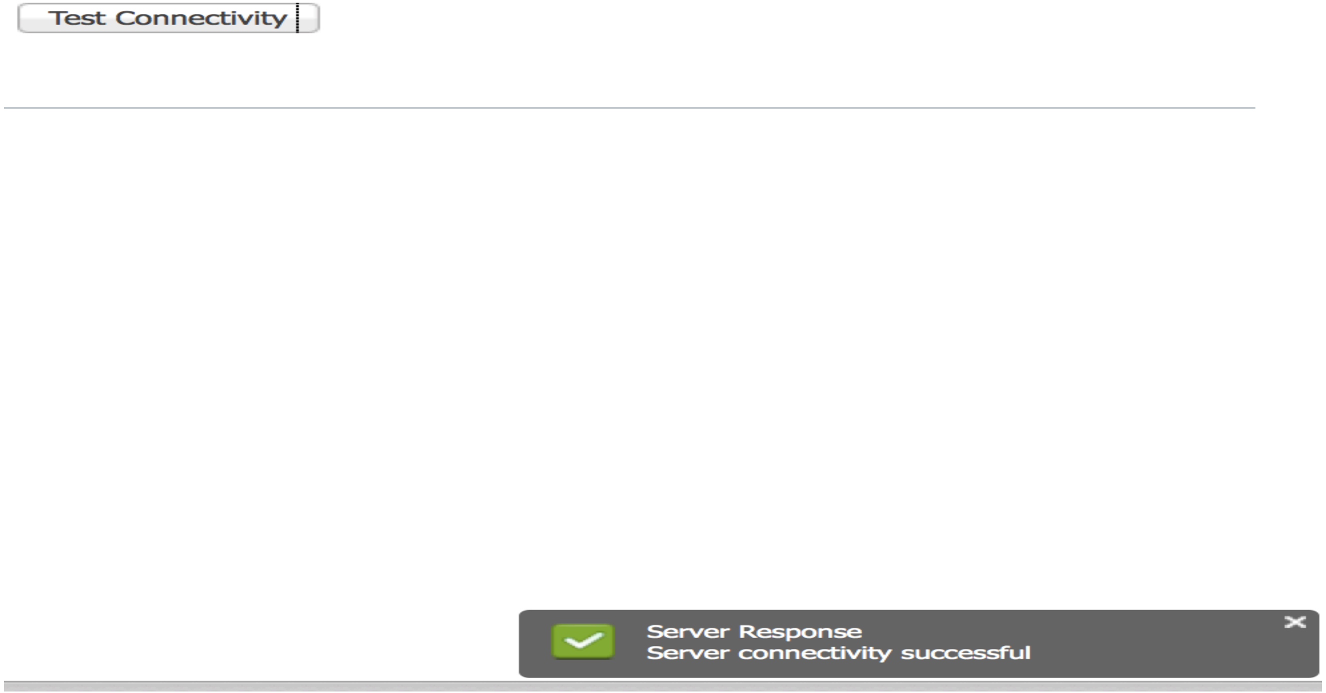
* Name SCEP_RA

Description

* URL **http://10.106.38.47/certsrv/mscep**

Certificate Request Agent Certificate **LAB-CA-MSCEP-RA**

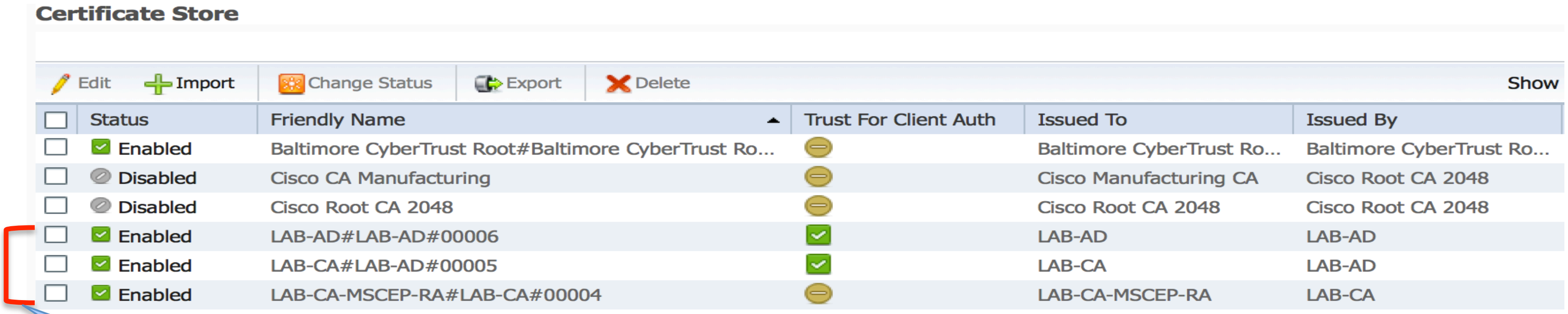
ISE SCEP CA Profile (Contd)



Server Response
Server connectivity successful

ISE SCEP CA Profile (Contd)

Administration→System→Certificates→Certificate Store



Certificate Store

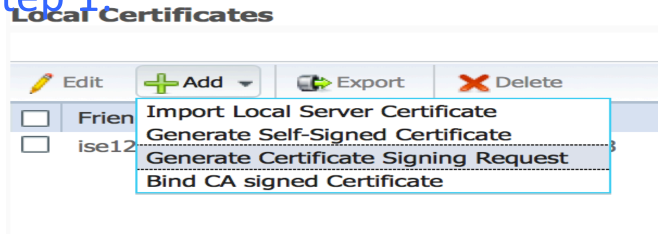
□	Status	Friendly Name	Trust For Client Auth	Issued To	Issued By
□	Enabled	Baltimore CyberTrust Root#Baltimore CyberTrust Ro...	⊖	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...
□	Disabled	Cisco CA Manufacturing	⊖	Cisco Manufacturing CA	Cisco Root CA 2048
□	Disabled	Cisco Root CA 2048	⊖	Cisco Root CA 2048	Cisco Root CA 2048
□	Enabled	LAB-AD#LAB-AD#00006	✓	LAB-AD	LAB-AD
□	Enabled	LAB-CA#LAB-AD#00005	✓	LAB-CA	LAB-AD
□	Enabled	LAB-CA-MSCEP-RA#LAB-CA#00004	⊖	LAB-CA-MSCEP-RA	LAB-CA

Two certs (Root CA+Sub CA) + SCEP RA cert issue by Sub CA

ISE – CSR Generation

Administration→System→Certificates

Step 1:



Local Certificates

Edit | Add | Export | Delete

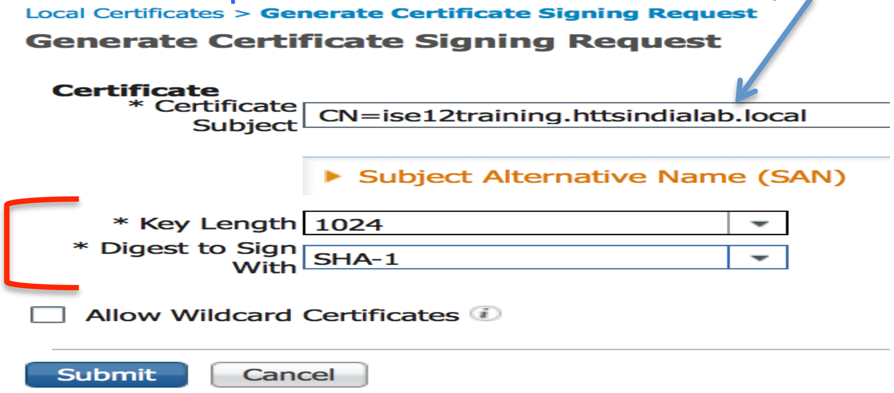
□	Frien
□	ise12

- Import Local Server Certificate
- Generate Self-Signed Certificate
- Generate Certificate Signing Request
- Bind CA signed Certificate

SHA-1 more widely compatible

Step 2:

FQDN of ISE



Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

Certificate

* Certificate Subject: CN=ise12training.httsindialab.local

▶ Subject Alternative Name (SAN)

* Key Length: 1024

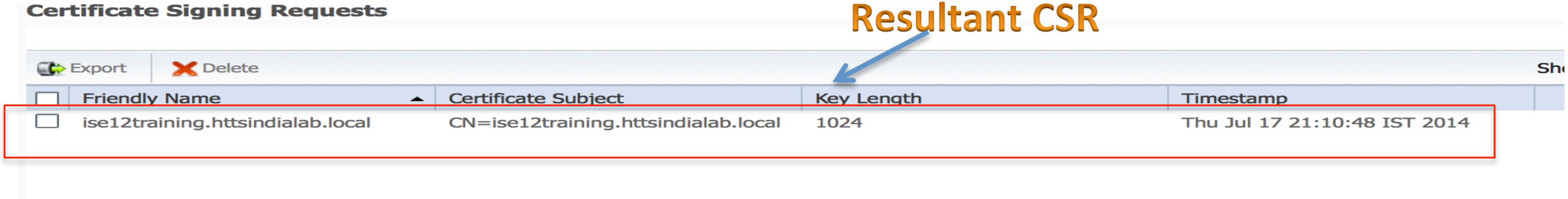
* Digest to Sign With: SHA-1

□ Allow Wildcard Certificates

Submit | Cancel

Step 3:

Resultant CSR

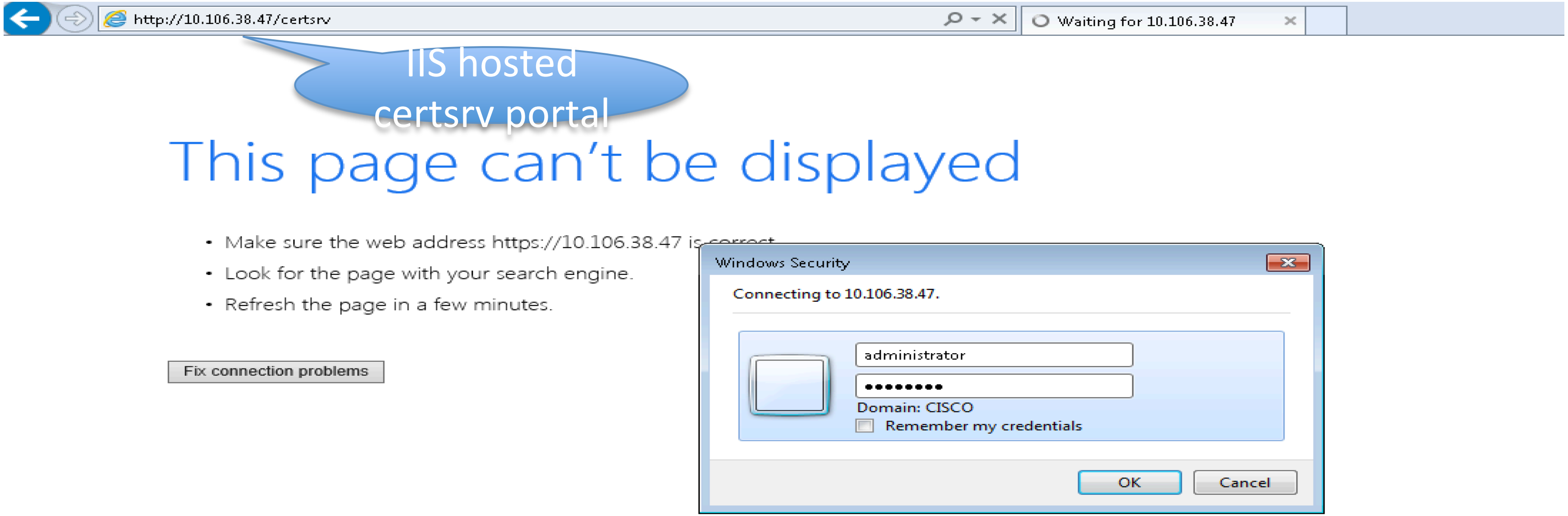


Certificate Signing Requests

Export | Delete | Sh

□	Friendly Name	Certificate Subject	Key Length	Timestamp
□	ise12training.httsindialab.local	CN=ise12training.httsindialab.local	1024	Thu Jul 17 21:10:48 IST 2014

Submit CSR



http://10.106.38.47/certsrv

Waiting for 10.106.38.47

IIS hosted certsrv portal

This page can’t be displayed

- Make sure the web address https://10.106.38.47 is correct
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Fix connection problems

Windows Security

Connecting to 10.106.38.47.

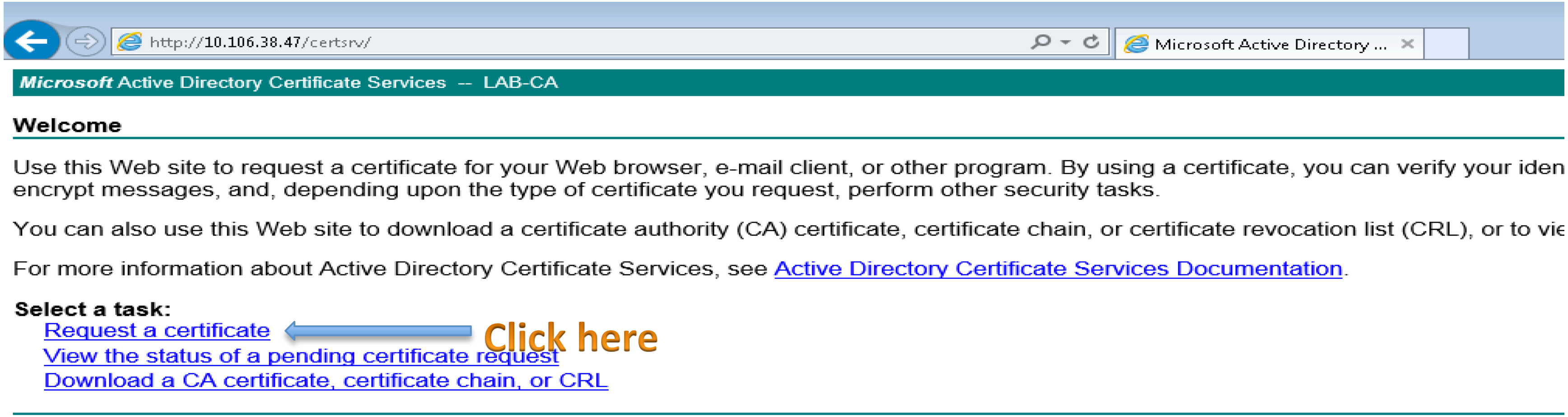
administrator

●●●●●●●●●

Domain: CISCO

□ Remember my credentials

Submit CSR (Contd)



Microsoft Active Directory Certificate Services -- LAB-CA

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 iden 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 vie

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

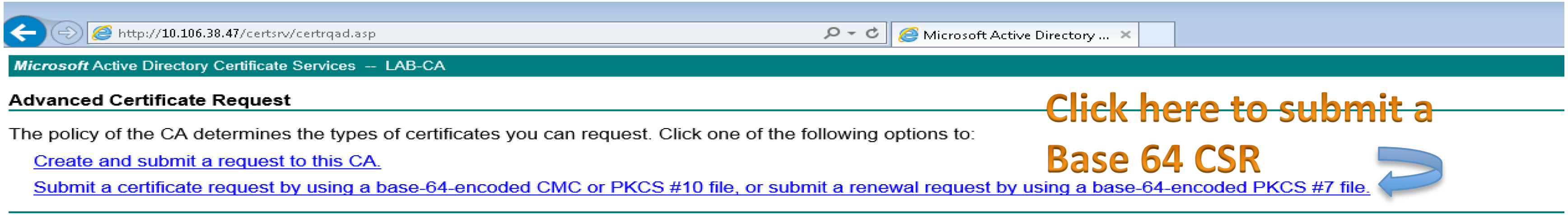
Request a certificate

View the status of a pending certificate request

Download a CA certificate, certificate chain, or CRL

Click here

Submit CSR (Contd)



http://10.106.38.47/certsrv/certrqad.asp
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- LAB-CA

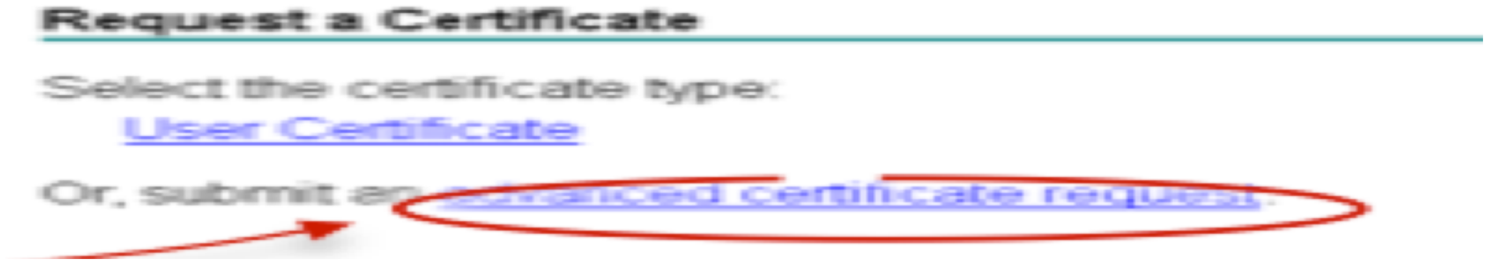
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- Create and submit a request to this CA.
- Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Click here to submit a Base 64 CSR

Submit CSR (Contd)

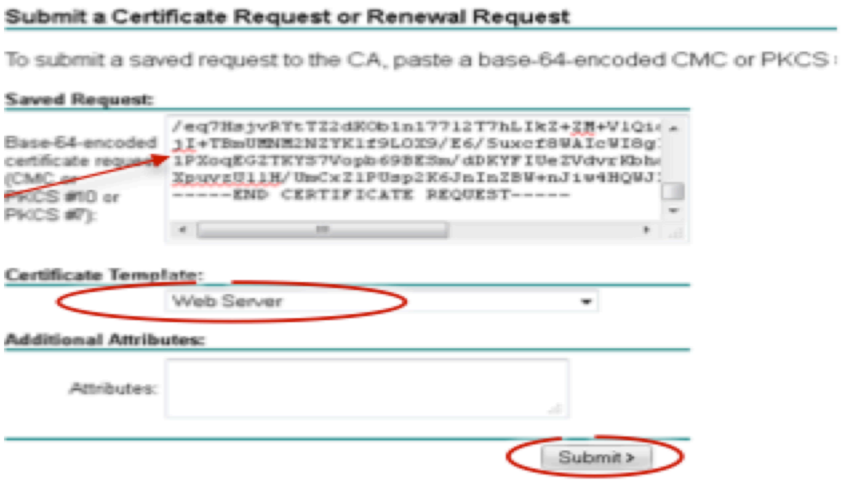


Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request.



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS

Saved Request:

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

/eq7HsjvRYtTZ2dKOb1n17712T7hLIkZ+ZM+V1Qi
jI+TBmUMNM2NZYK1f9LOX9/E6/Suxcf8WAIcWI8g
1PXoqEGZTKYS7Vopb69BESm/dDKYFIUeZVdvrKbh
XpuvzU11H/UmCxZ1PUsp2K6JnInZBW+nJ1w4HQWJ
-----END CERTIFICATE REQUEST-----

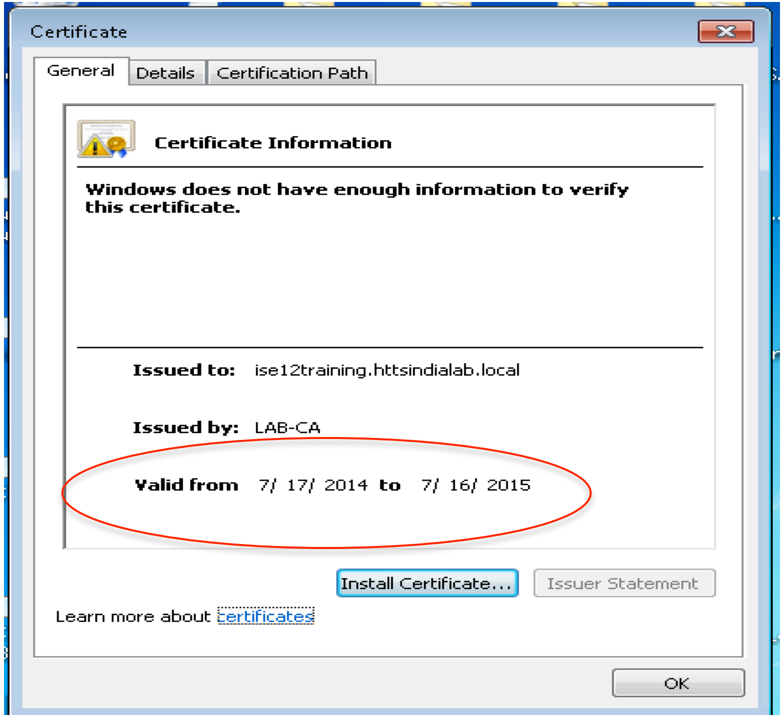
Certificate Template:

Web Server

Additional Attributes:

Attributes:

ISE Certificate



Certificate

General | Details | Certification Path

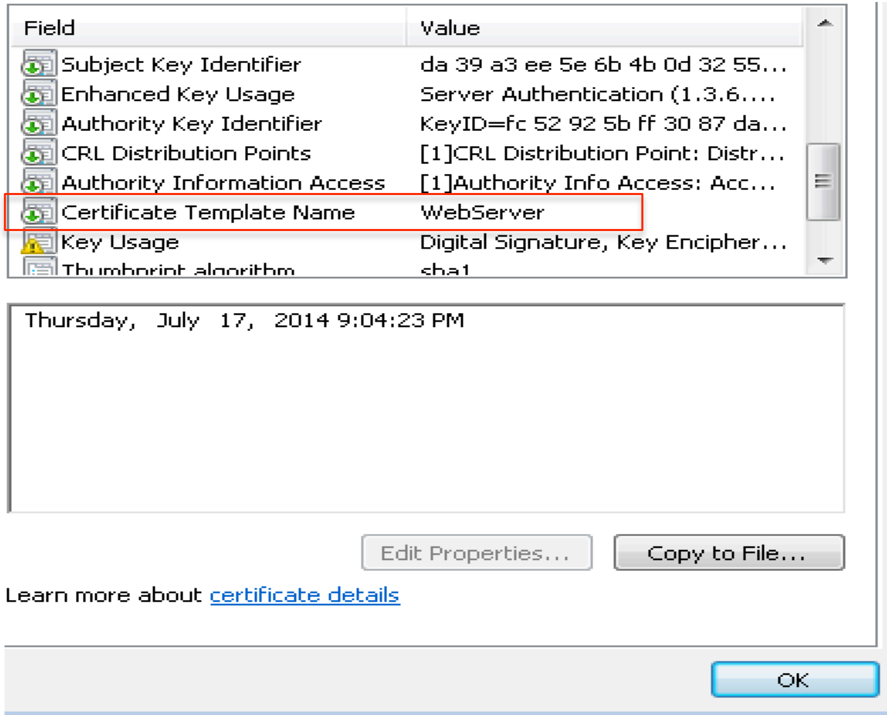
Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: ise12training.httsindialab.local

Issued by: LAB-CA

Valid from 7/ 17/ 2014 **to** 7/ 16/ 2015

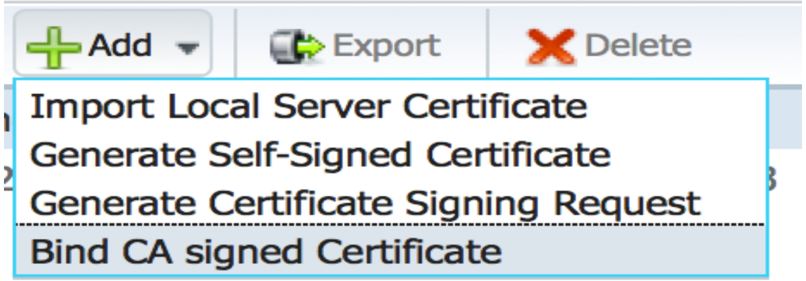


Field	Value
Subject Key Identifier	da 39 a3 ee 5e 6b 4b 0d 32 55...
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Key Identifier	KeyID=fc 52 92 5b ff 30 87 da...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Template Name	WebServer
Key Usage	Digital Signature, Key Encipher...
Thumbprint algorithm	sha1

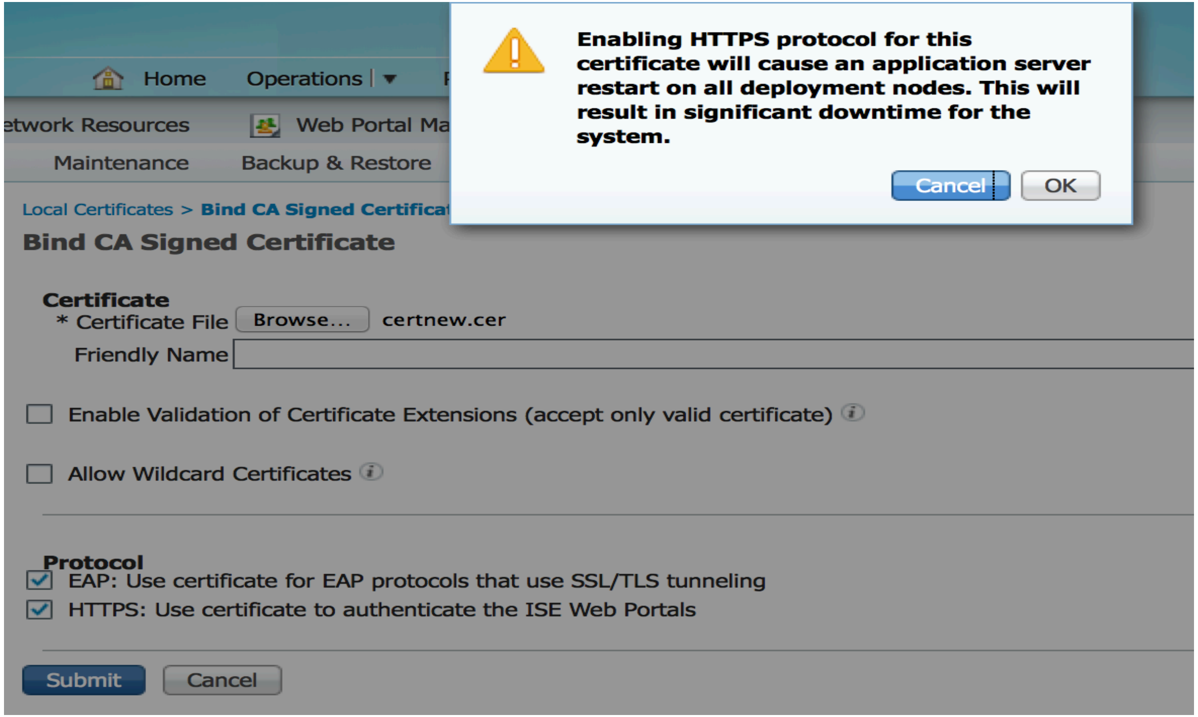
Thursday, July 17, 2014 9:04:23 PM

Certificate installation

Administration→System→Certificates→Local Certificates


Add
Export
Delete
Import Local Server Certificate
Generate Self-Signed Certificate
Generate Certificate Signing Request
Bind CA signed Certificate

Certificate installation (Contd)



Enabling HTTPS protocol for this certificate will cause an application server restart on all deployment nodes. This will result in significant downtime for the system.

Local Certificates > Bind CA Signed Certificat

Bind CA Signed Certificate

Certificate

* Certificate File Browse... certnew.cer

Friendly Name

□ Enable Validation of Certificate Extensions (accept only valid certificate)

□ Allow Wildcard Certificates

Protocol

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

☑ HTTPS: Use certificate to authenticate the ISE Web Portals

Same cert used for HTTPS+EAP

Caveats

1. Use certutil to extend SubCA cert lifetimes

Default Certificate Template lifetime for SubCA: 5 years

Actual Sub CA certificate lifetime: 1 year

Endpoint certificate lifetime: 1 year

Endpoint cert lifetime<Sub CA cert lifetime<Root Cert lifetime

Caveats (Contd)

2. Issuance Policies

Default: No “All Issuance policies” permission granted to SubCA. Ensure to keep it disabled for user / cloned user templates.

Note: If enabling “All issuance policies” extension, please ensure that Root CA grants this to Sub CA first

Caveats (Contd)

3. Ensure that CN on ISE certificate=FQDN of redirect URL

Failing to follow this will lead to:

```
[Sat Jul 19 11:34:44 2014] Warning - [HTTPConnection] InternetOpen() failed with code: [12038]
[Sat Jul 19 11:34:44 2014] Warning - [HTTPConnection] Abort the HTTP connection due to invalid certificate CN
```

Error seen in: Windows 7, %TEMP%\spwprofile.log

References: BRKSEC-3045.pdf (Page 20)

Note: Don’t use IP address in redirect URL- if using, please ensure to use it in the SAN field of Certificate too

References

- SCEP configuration for BYOD

http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-product-00.html

- CCO guides on BYOD

BYOD: Using Certificates for Differentiated Access

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

BYOD: On-Boarding and Provisioning

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_61_byod_provisioning.pdf

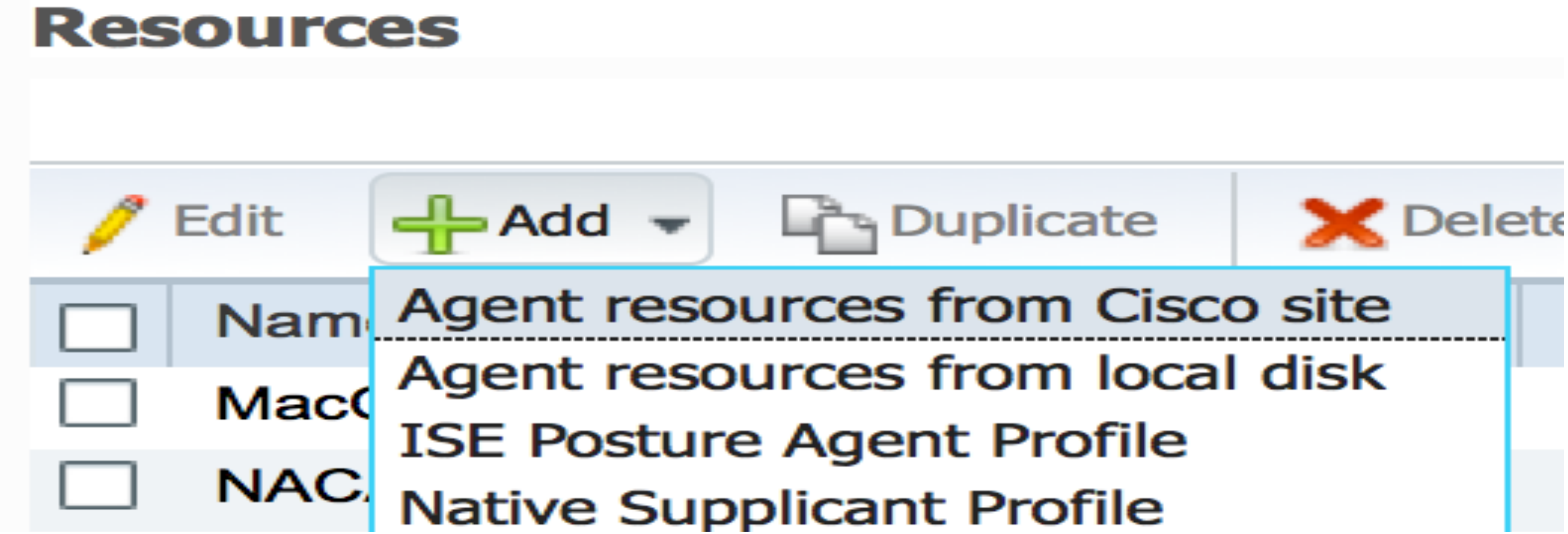
Supplicant Provisioning

Client Provisioning resources

Download SPWs (Supplicant Provisioning wizards) and all client software from CCO for all OS’s except Android

Pre-requisite: ISE needs Internet access either directly or through proxy

Policy→Results→Client Provisioning→Resources

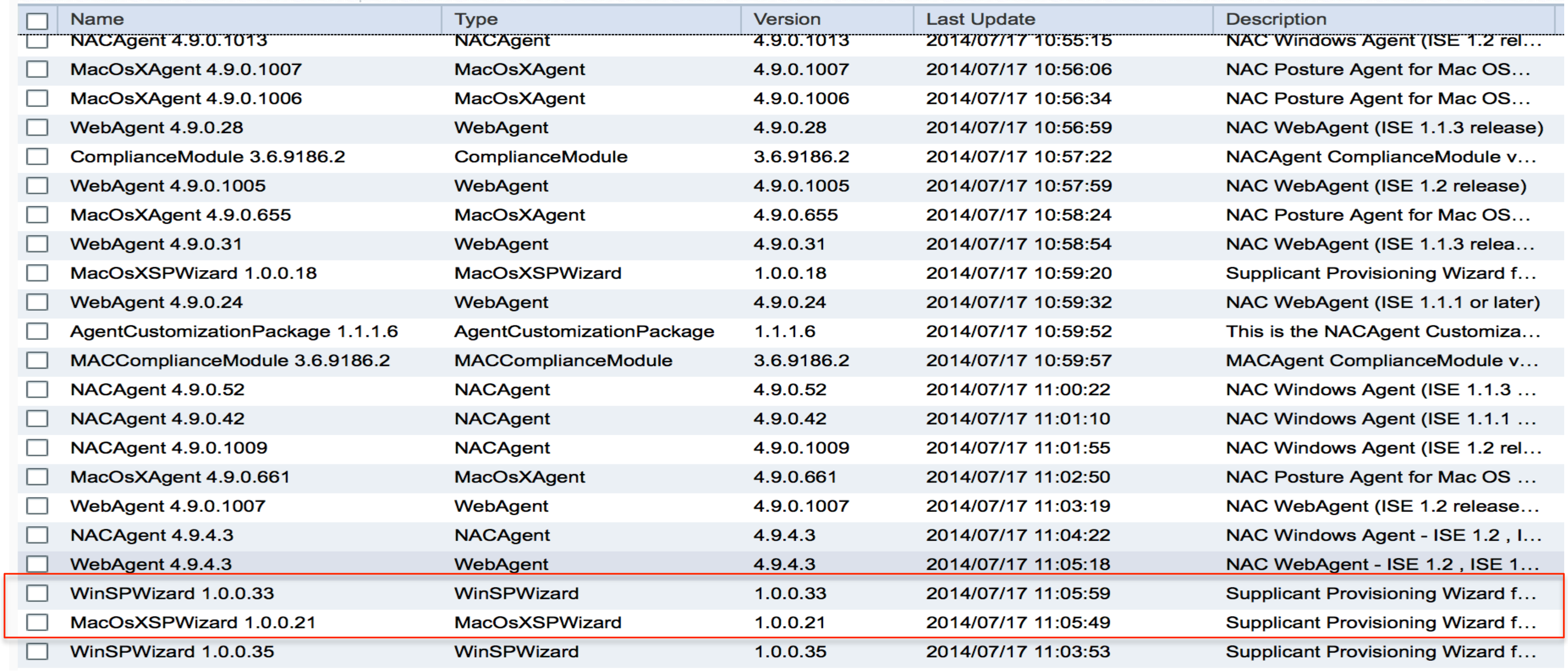


Resources

Edit
Add
Duplicate
Delete
Name
Mac
NAC
Agent resources from Cisco site
Agent resources from local disk
ISE Posture Agent Profile
Native Supplicant Profile

Client Provisioning resources (Contd)

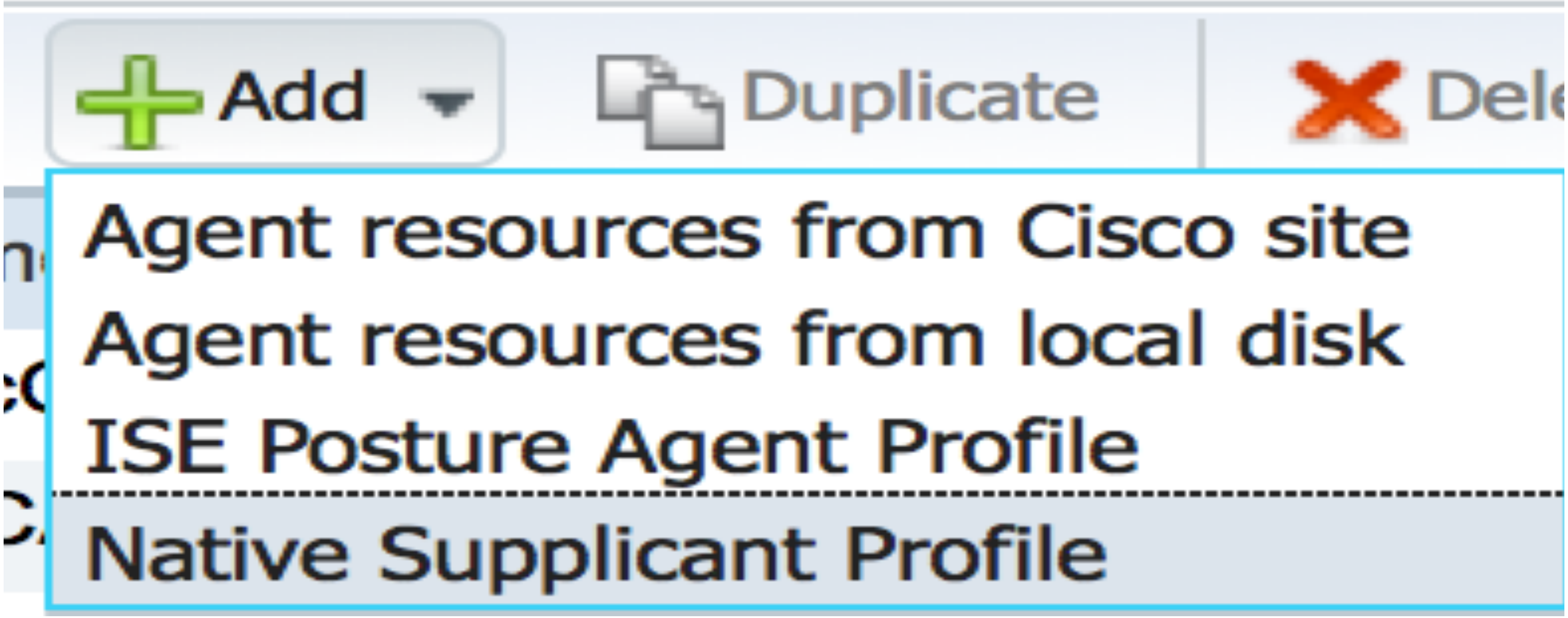
Download yields all clients given below



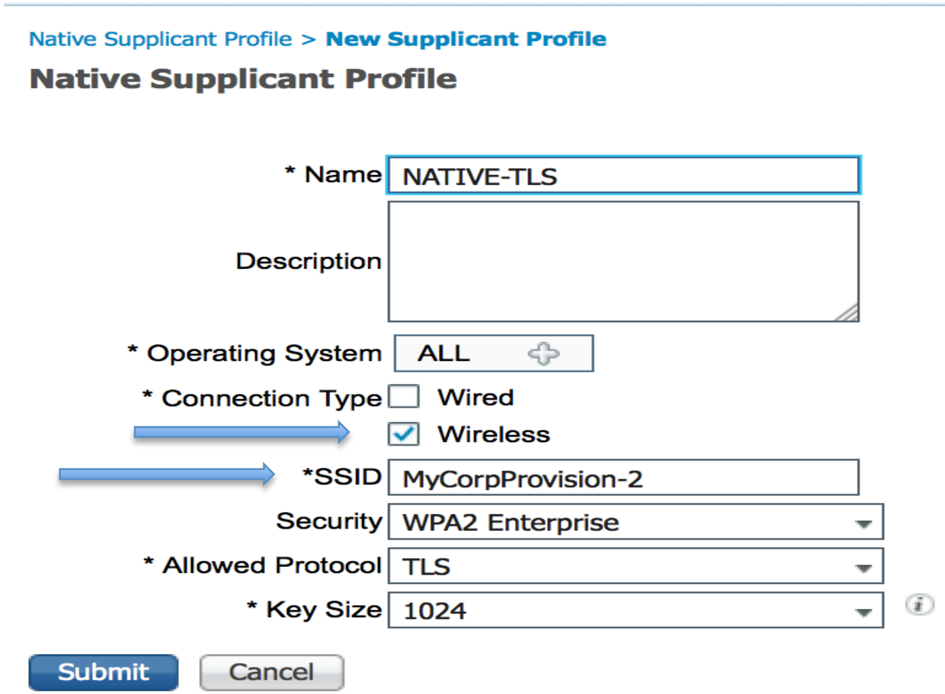
□	Name	Type	Version	Last Update	Description
□	NACAgent 4.9.0.1013	NACAgent	4.9.0.1013	2014/07/17 10:55:15	NAC Windows Agent (ISE 1.2 rel...
□	MacOsXAgent 4.9.0.1007	MacOsXAgent	4.9.0.1007	2014/07/17 10:56:06	NAC Posture Agent for Mac OS...
□	MacOsXAgent 4.9.0.1006	MacOsXAgent	4.9.0.1006	2014/07/17 10:56:34	NAC Posture Agent for Mac OS...
□	WebAgent 4.9.0.28	WebAgent	4.9.0.28	2014/07/17 10:56:59	NAC WebAgent (ISE 1.1.3 release)
□	ComplianceModule 3.6.9186.2	ComplianceModule	3.6.9186.2	2014/07/17 10:57:22	NACAgent ComplianceModule v...
□	WebAgent 4.9.0.1005	WebAgent	4.9.0.1005	2014/07/17 10:57:59	NAC WebAgent (ISE 1.2 release)
□	MacOsXAgent 4.9.0.655	MacOsXAgent	4.9.0.655	2014/07/17 10:58:24	NAC Posture Agent for Mac OS...
□	WebAgent 4.9.0.31	WebAgent	4.9.0.31	2014/07/17 10:58:54	NAC WebAgent (ISE 1.1.3 relea...
□	MacOsXSPWizard 1.0.0.18	MacOsXSPWizard	1.0.0.18	2014/07/17 10:59:20	Supplicant Provisioning Wizard f...
□	WebAgent 4.9.0.24	WebAgent	4.9.0.24	2014/07/17 10:59:32	NAC WebAgent (ISE 1.1.1 or later)
□	AgentCustomizationPackage 1.1.1.6	AgentCustomizationPackage	1.1.1.6	2014/07/17 10:59:52	This is the NACAgent Customiza...
□	MACComplianceModule 3.6.9186.2	MACComplianceModule	3.6.9186.2	2014/07/17 10:59:57	MACAgent ComplianceModule v...
□	NACAgent 4.9.0.52	NACAgent	4.9.0.52	2014/07/17 11:00:22	NAC Windows Agent (ISE 1.1.3 ...
□	NACAgent 4.9.0.42	NACAgent	4.9.0.42	2014/07/17 11:01:10	NAC Windows Agent (ISE 1.1.1 ...
□	NACAgent 4.9.0.1009	NACAgent	4.9.0.1009	2014/07/17 11:01:55	NAC Windows Agent (ISE 1.2 rel...
□	MacOsXAgent 4.9.0.661	MacOsXAgent	4.9.0.661	2014/07/17 11:02:50	NAC Posture Agent for Mac OS ...
□	WebAgent 4.9.0.1007	WebAgent	4.9.0.1007	2014/07/17 11:03:19	NAC WebAgent (ISE 1.2 release...
□	NACAgent 4.9.4.3	NACAgent	4.9.4.3	2014/07/17 11:04:22	NAC Windows Agent - ISE 1.2 , I...
□	WebAgent 4.9.4.3	WebAgent	4.9.4.3	2014/07/17 11:05:18	NAC WebAgent - ISE 1.2 , ISE 1...
□	WinSPWizard 1.0.0.33	WinSPWizard	1.0.0.33	2014/07/17 11:05:59	Supplicant Provisioning Wizard f...
□	MacOsXSPWizard 1.0.0.21	MacOsXSPWizard	1.0.0.21	2014/07/17 11:05:49	Supplicant Provisioning Wizard f...
□	WinSPWizard 1.0.0.35	WinSPWizard	1.0.0.35	2014/07/17 11:03:53	Supplicant Provisioning Wizard f...

NSP (Native Supplicant Profile)

Create supplicant profile that contains the authentication protocol and SSID information


Add
Duplicate
Dele
Agent resources from Cisco site
Agent resources from local disk
ISE Posture Agent Profile
Native Supplicant Profile

Supplicant Profile

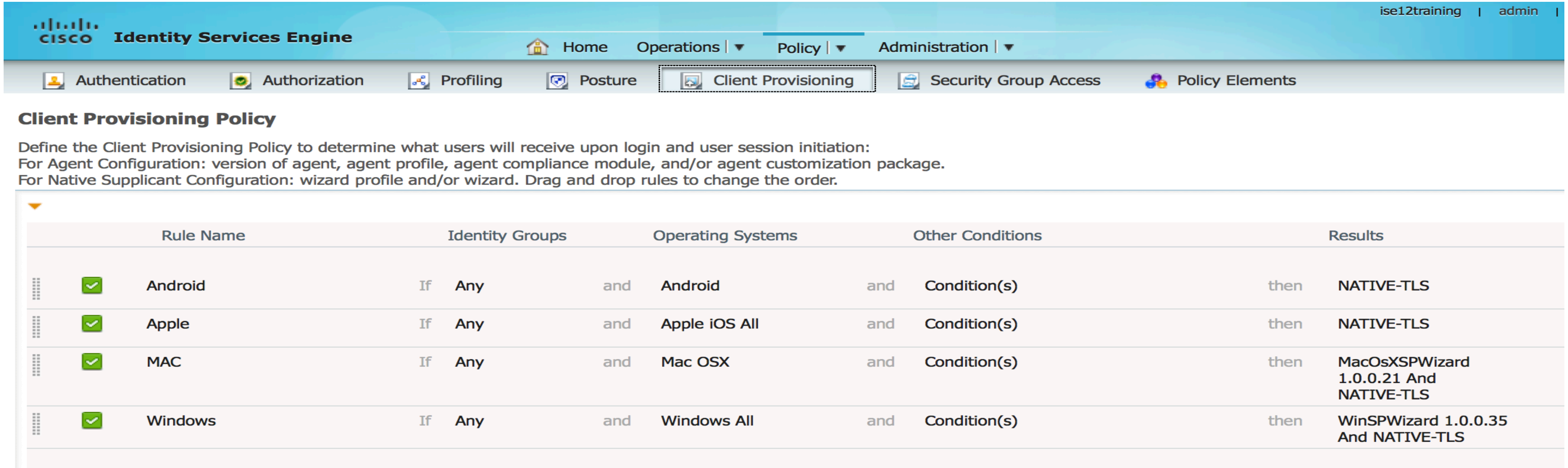


Native Supplicant Profile

* Name	NATIVE-TLS
Description	
* Operating System	ALL
* Connection Type	□ Wired ☑ Wireless
*SSID	MyCorpProvision-2
Security	WPA2 Enterprise
* Allowed Protocol	TLS
* Key Size	1024

CPP (Client Provisioning Policy)

Policy→Client Provisioning

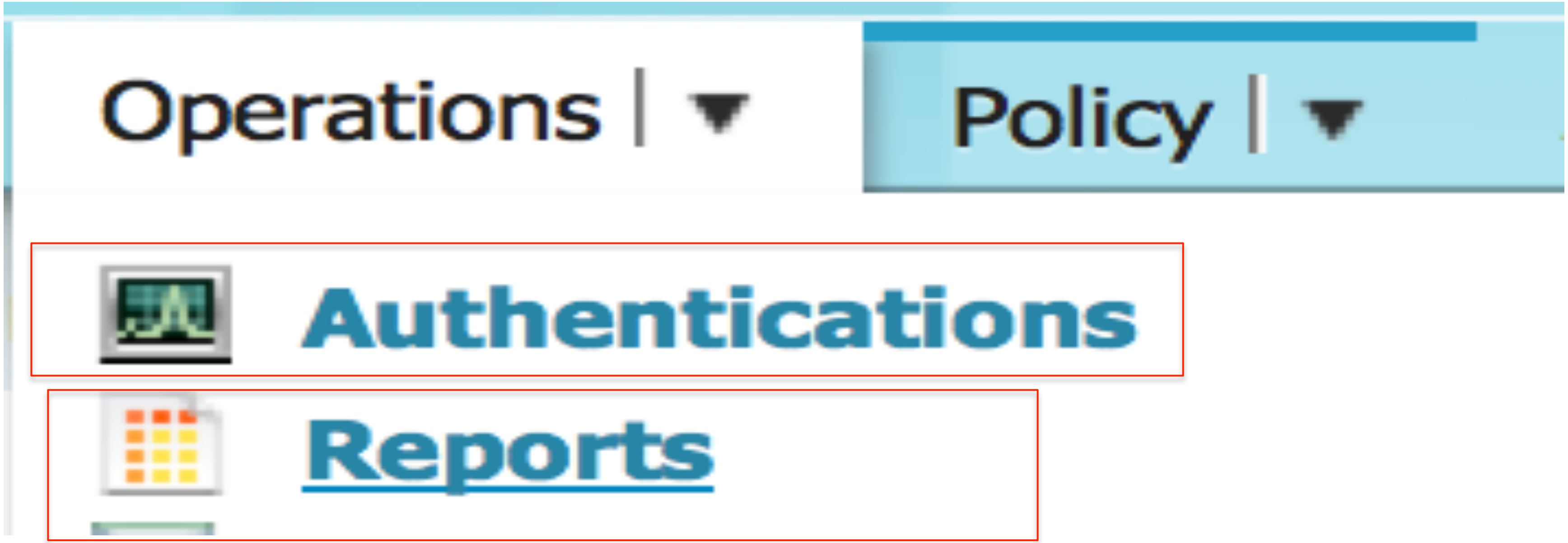


Client Provisioning Policy

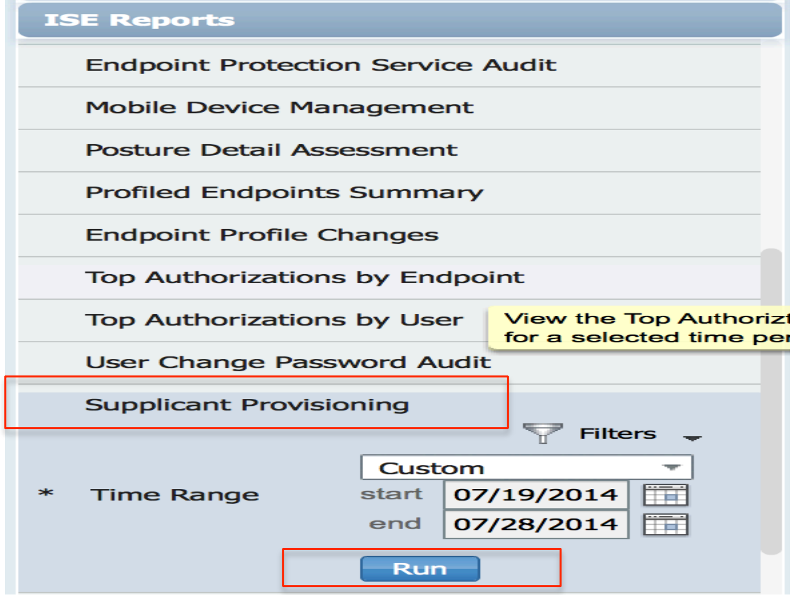
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
✓	Android	If	Any	and	Android	and	Condition(s)	then	NATIVE-TLS
✓	Apple	If	Any	and	Apple iOS All	and	Condition(s)	then	NATIVE-TLS
✓	MAC	If	Any	and	Mac OSX	and	Condition(s)	then	MacOsXSPWizard 1.0.0.21 And NATIVE-TLS
✓	Windows	If	Any	and	Windows All	and	Condition(s)	then	WinSPWizard 1.0.0.35 And NATIVE-TLS

Monitoring supplicants



Reports - Supplicant Provisioning

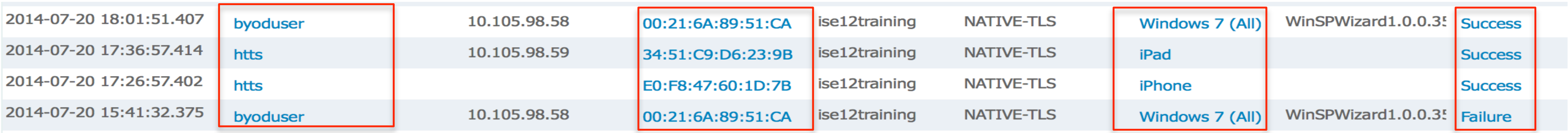


ISE Reports

- Endpoint Protection Service Audit
- Mobile Device Management
- Posture Detail Assessment
- Profiled Endpoints Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Top Authorizations by User
- User Change Password Audit
- Supplicant Provisioning

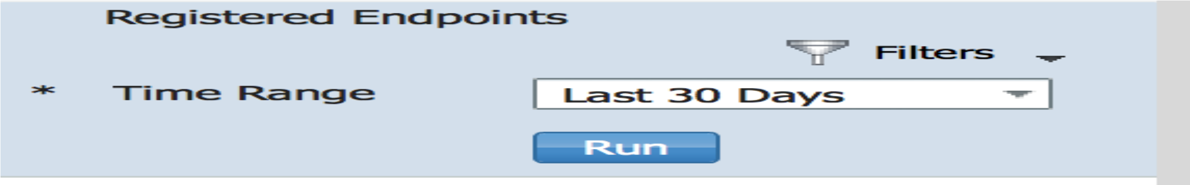
View the Top Authorizt
for a selected time per

* Time Range: Custom
start 07/19/2014
end 07/28/2014



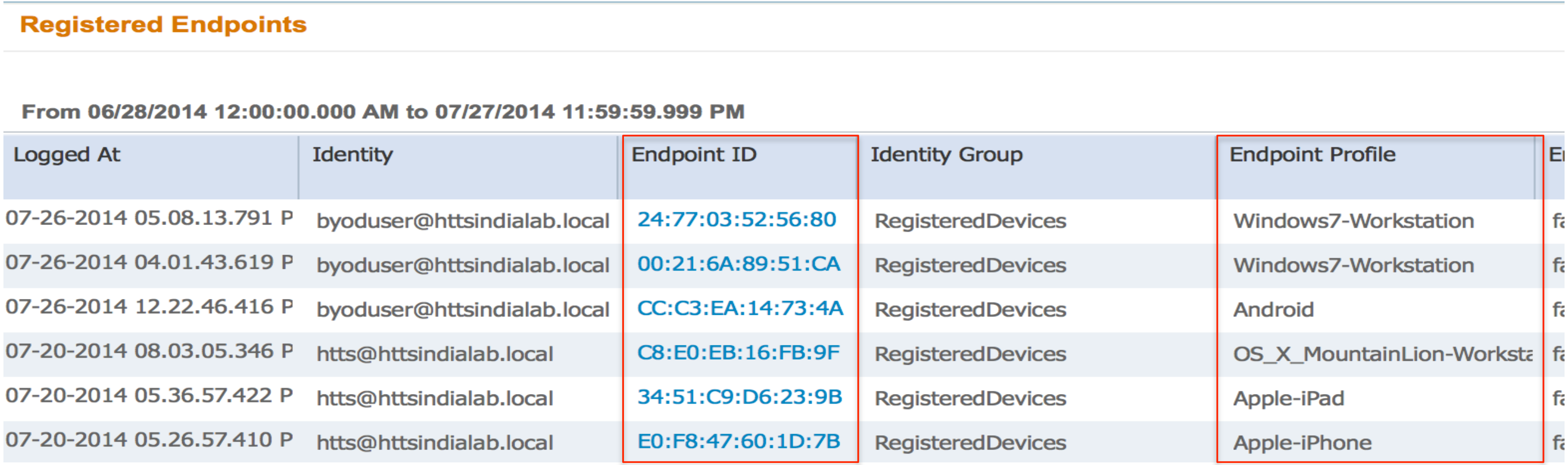
2014-07-20 18:01:51.407	byoduser	10.105.98.58	00:21:6A:89:51:CA	ise12training	NATIVE-TLS	Windows 7 (All)	WinSPWizard1.0.0.3	Success
2014-07-20 17:36:57.414	htts	10.105.98.59	34:51:C9:D6:23:9B	ise12training	NATIVE-TLS	iPad		Success
2014-07-20 17:26:57.402	htts		E0:F8:47:60:1D:7B	ise12training	NATIVE-TLS	iPhone		Success
2014-07-20 15:41:32.375	byoduser	10.105.98.58	00:21:6A:89:51:CA	ise12training	NATIVE-TLS	Windows 7 (All)	WinSPWizard1.0.0.3	Failure

Reports – Registered Devices



Registered Endpoints

* Time Range: Last 30 Days



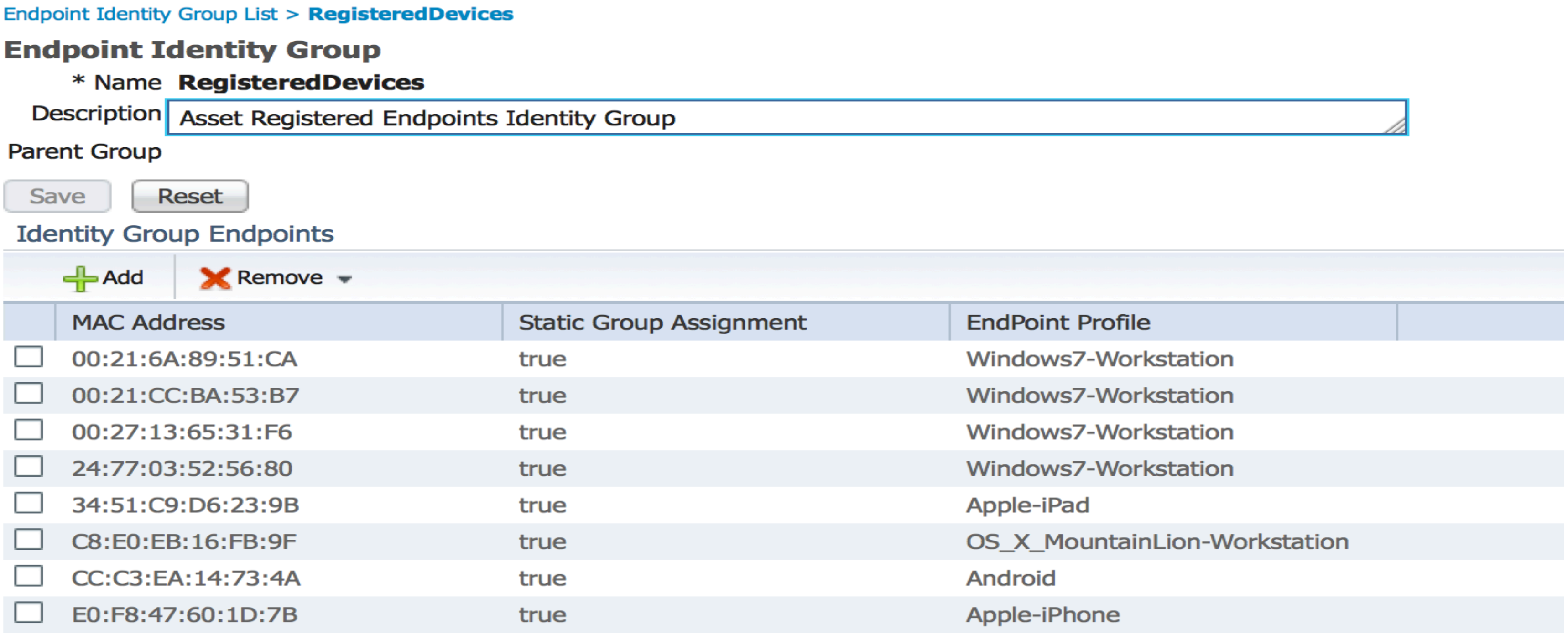
Registered Endpoints

From 06/28/2014 12:00:00.000 AM to 07/27/2014 11:59:59.999 PM

Logged At	Identity	Endpoint ID	Identity Group	Endpoint Profile	E
07-26-2014 05.08.13.791 P	byoduser@httsindialab.local	24:77:03:52:56:80	RegisteredDevices	Windows7-Workstation	fa
07-26-2014 04.01.43.619 P	byoduser@httsindialab.local	00:21:6A:89:51:CA	RegisteredDevices	Windows7-Workstation	fa
07-26-2014 12.22.46.416 P	byoduser@httsindialab.local	CC:C3:EA:14:73:4A	RegisteredDevices	Android	fa
07-20-2014 08.03.05.346 P	htts@httsindialab.local	C8:E0:EB:16:FB:9F	RegisteredDevices	OS_X_MountainLion-Workst	fa
07-20-2014 05.36.57.422 P	htts@httsindialab.local	34:51:C9:D6:23:9B	RegisteredDevices	Apple-iPad	fa
07-20-2014 05.26.57.410 P	htts@httsindialab.local	E0:F8:47:60:1D:7B	RegisteredDevices	Apple-iPhone	fa

Registered Endpoints Identity Group

Administration→Identities→Groups→Endpoint Identity Group→Registered Devices.



Endpoint Identity Group List > RegisteredDevices

Endpoint Identity Group

* Name **RegisteredDevices**

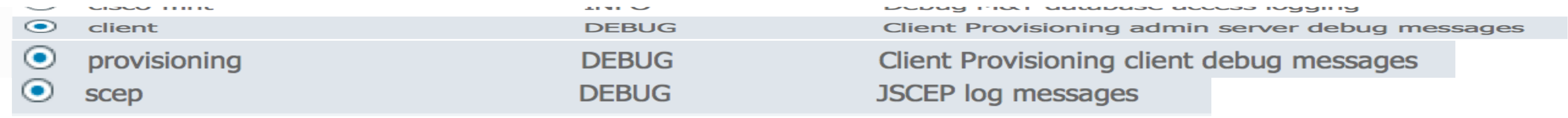
Description: Asset Registered Endpoints Identity Group

Parent Group

Identity Group Endpoints

	MAC Address	Static Group Assignment	EndPoint Profile
□	00:21:6A:89:51:CA	true	Windows7-Workstation
□	00:21:CC:BA:53:B7	true	Windows7-Workstation
□	00:27:13:65:31:F6	true	Windows7-Workstation
□	24:77:03:52:56:80	true	Windows7-Workstation
□	34:51:C9:D6:23:9B	true	Apple-iPad
□	C8:E0:EB:16:FB:9F	true	OS_X_MountainLion-Workstation
□	CC:C3:EA:14:73:4A	true	Android
□	E0:F8:47:60:1D:7B	true	Apple-iPhone

ISE – Debug log configuration



○	cisco-mnt	INFO	Debug M&T database access logging
◉	client	DEBUG	Client Provisioning admin server debug messages
◉	provisioning	DEBUG	Client Provisioning client debug messages
◉	scep	DEBUG	JSCEP log messages

Administration→Logging→Debug Log configuration

Supplicant Logs

Windows - %TEMP%\spwProfileLog.txt

MAC OS X – Console logs

iPhone – iPhone configuration utility

Troubleshooting BYOD - WLC

- Symptom = Wireless connectivity and performance issues while using Apple iOS devices.
  - Check if = Captive portal bypass for www.apple.com is allowed by using:

    config network web-auth captive-bypass enable

- Symptom = Configured ACL appears to not allow user to connect to ISE.
  - Check if = Permit ICMP, UDP, DNS and DHCP traffic has been configured.
  - Check if = Permit traffic to ISE has been configured.

- Symptom = WLC is unable to find a valid Authentication / Accounting server.
  - Check if = The WLC has the ISE as both the Authentication and Accounting Server.
  - Check if = The Radius server is configured for RFC 3576 which ISE uses for ISE.
  - Check if = The WLC has enable ‘AAA override’ enabled – WLAN > Advanced.

CLI – Debug Commands

- Suggested WLC debug commands when troubleshooting BYOD:

```
debug client <mac address>
debug mac addr <mac-address>
debug profiling
debug aaa all
debug aaa detail
debug aaa events
debug web-auth redirect enable mac <mac address>
```

Device Profiling Debug Command

- To debug Device Profiling on the controller:

  debug profiling

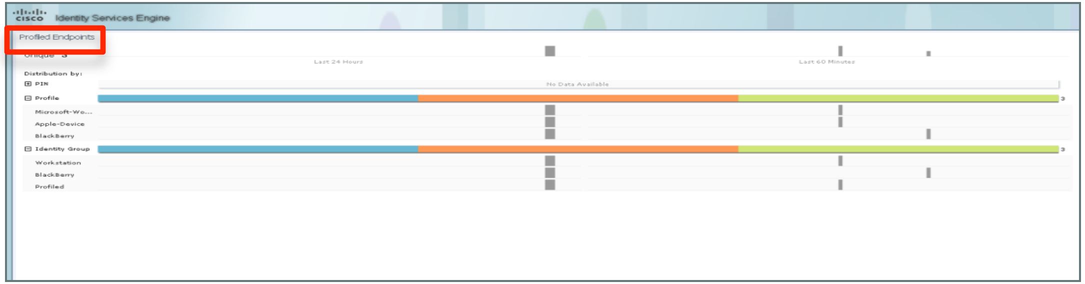
```
Dot1x_NW_MsgTask_3: Apr 11 16:05:53.306: 40:5f:be:a4:82:c3 Sending DHCP option hostname BLACKBERRY
Dot1x_NW_MsgTask_3: Apr 11 16:05:53.306: 40:5f:be:a4:82:c3 Sending DHCP option classId BlackBerry 10
Dot1x_NW_MsgTask_3: Apr 11 16:05:53.306: Sending Accounting request (1) for station 40:5f:be:a4:82:c3  and deleting client
Dot1x_NW_MsgTask_3: Apr 11 16:05:53.306: 40:5f:be:a4:82:c3 Profiling entry deleted.
aaaQueueReader: Apr 11 16:05:53.306: Adding the DHCP option Hostname to AVP BLACKBERRY
aaaQueueReader: Apr 11 16:05:53.306: Adding the DHCP option ClassID to AVP BlackBerry
DHCP Socket Task: Apr 11 16:05:53.314: 40:5f:be:a4:82:c3 Sending message to the profiler Client Profiler queue
Radius Client Profiler Task: Apr 11 16:05:53.314: Received message from Client Profiler queue
Radius Client Profiler Task: Apr 11 16:05:53.314: 40:5f:be:a4:82:c3 Func: radiusClProfilerPktRecv Line: 355 Sending
information to create client entry
Radius Client Profiler Task: Apr 11 16:05:53.314: Func: apfProfilerCreateClient Line: 144 The key is 40:5f:be:a4:82:c3
hostname BLACKBERRY-<BlackBerry= hostLen 15  vendorName BlackBerry= vendorLen 10
```

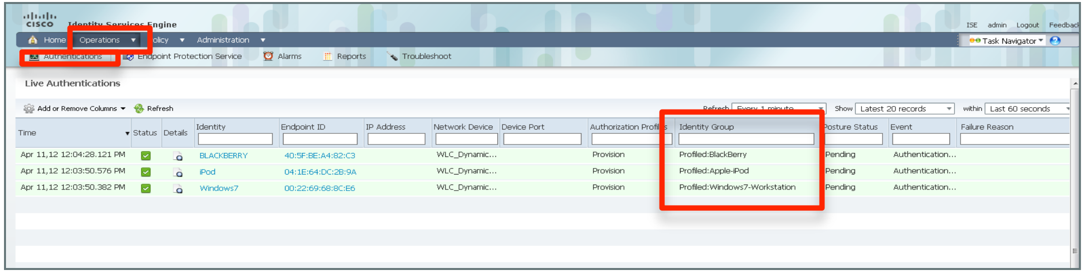
Viewing Profiled Devices in ISE

- From the Home page, locate the Profiled Devices dashlet.

- For detailed analysis Operations > Authentications

- From Administration > Identity Management > Identities > Endpoints.

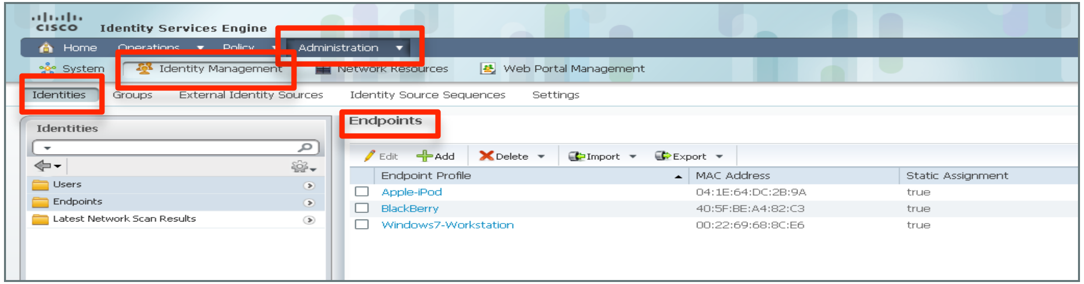




Live Authentications

Refresh Every 1 minute Show Latest 20 records within Last 60 seconds

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason
Apr 11,12 12:04:28.121 PM	✓		BLACKBERRY	40:5F:BE:A4:82:C3		WLC_Dynamic...		Provision	Profiled:BlackBerry	Pending	Authentication...	
Apr 11,12 12:03:50.576 PM	✓		iPod	04:1E:64:DC:2B:9A		WLC_Dynamic...		Provision	Profiled:Apple-iPod	Pending	Authentication...	
Apr 11,12 12:03:50.382 PM	✓		Windows7	00:22:69:68:8C:E6		WLC_Dynamic...		Provision	Profiled:Windows7-Workstation	Pending	Authentication...	

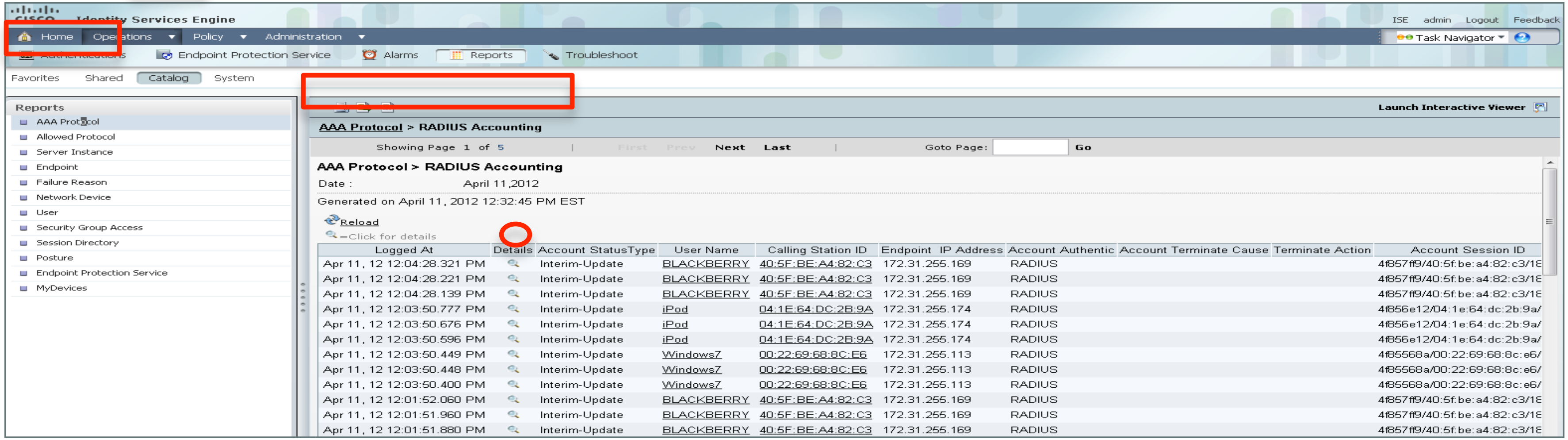


Endpoints

	Endpoint Profile	MAC Address	Static Assignment
□	Apple-iPod	04:1E:64:DC:2B:9A	true
□	BlackBerry	40:5F:BE:A4:82:C3	true
□	Windows7-Workstation	00:22:69:68:8C:E6	true

Troubleshooting Profiled Devices in ISE

- To see a Accounting details for a particular device, navigate to: Operations > Catalog > AAA Protocol > RADIUS Accounting
- Click on the magnifying glass to see client specific details.



AAA Protocol > RADIUS Accounting

Date : April 11 ,2012

Generated on April 11, 2012 12:32:45 PM EST

Logged At	Details	Account StatusType	User Name	Calling Station ID	Endpoint IP Address	Account Authentic	Account Terminate Cause	Terminate Action	Account Session ID
Apr 11, 12 12:04:28.321 PM	🔍	Interim-Update	BLACKBERRY	40:5F:BE:A4:82:C3	172.31.255.169	RADIUS			4f857ff9/40:5f:be:a4:82:c3/1
Apr 11, 12 12:04:28.221 PM	🔍	Interim-Update	BLACKBERRY	40:5F:BE:A4:82:C3	172.31.255.169	RADIUS			4f857ff9/40:5f:be:a4:82:c3/1
Apr 11, 12 12:04:28.139 PM	🔍	Interim-Update	BLACKBERRY	40:5F:BE:A4:82:C3	172.31.255.169	RADIUS			4f857ff9/40:5f:be:a4:82:c3/1
Apr 11, 12 12:03:50.777 PM	🔍	Interim-Update	iPod	04:1E:64:DC:2B:9A	172.31.255.174	RADIUS			4f856e12/04:1e:64:dc:2b:9a/
Apr 11, 12 12:03:50.676 PM	🔍	Interim-Update	iPod	04:1E:64:DC:2B:9A	172.31.255.174	RADIUS			4f856e12/04:1e:64:dc:2b:9a/
Apr 11, 12 12:03:50.596 PM	🔍	Interim-Update	iPod	04:1E:64:DC:2B:9A	172.31.255.174	RADIUS			4f856e12/04:1e:64:dc:2b:9a/
Apr 11, 12 12:03:50.449 PM	🔍	Interim-Update	Windows7	00:22:69:68:8C:E6	172.31.255.113	RADIUS			4f85568a/00:22:69:68:8c:e6/
Apr 11, 12 12:03:50.448 PM	🔍	Interim-Update	Windows7	00:22:69:68:8C:E6	172.31.255.113	RADIUS			4f85568a/00:22:69:68:8c:e6/
Apr 11, 12 12:03:50.400 PM	🔍	Interim-Update	Windows7	00:22:69:68:8C:E6	172.31.255.113	RADIUS			4f85568a/00:22:69:68:8c:e6/
Apr 11, 12 12:01:52.060 PM	🔍	Interim-Update	BLACKBERRY	40:5F:BE:A4:82:C3	172.31.255.169	RADIUS			4f857ff9/40:5f:be:a4:82:c3/1
Apr 11, 12 12:01:51.960 PM	🔍	Interim-Update	BLACKBERRY	40:5F:BE:A4:82:C3	172.31.255.169	RADIUS			4f857ff9/40:5f:be:a4:82:c3/1
Apr 11, 12 12:01:51.880 PM	🔍	Interim-Update	BLACKBERRY	40:5F:BE:A4:82:C3	172.31.255.169	RADIUS			4f857ff9/40:5f:be:a4:82:c3/1

Thank you.

cisco