Configure Automatic Certificate Enrollment and Renewal Via CAPF Online CA

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Validate the server time and date
Update server Computer Name
Configure
AD Services, User and and Certificate Template
IIS Authentication and SSL Binding Configuration
CUCM Configuration
Verify
Verify IIS Certificates
Verify CUCM Configuration
Related Links

Introduction

This document describes Automatic Certificate Enrollment and Renewal via the Certificate Authority Proxy Function (CAPF) Online feature for Cisco Unified Communications Manager (CUCM).

Contributed by Michael Mendoza, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager
- X.509 certificates
- Windows Server
- Windows Active Directory (AD)
- Windows Internet Information Services (IIS)
- NT (New Technology) LAN Manager (NTLM) Authentication

Components Used

The information in this document is based on these software and hardware versions:

- CUCM version 12.5.1.10000-22
- Windows Server 2012 R2
- IP Phone CP-8865 / Firmware: SIP 12-1-1SR1-4 and 12-5-1SR2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document covers the configuration of the feature and related resources for additional research.

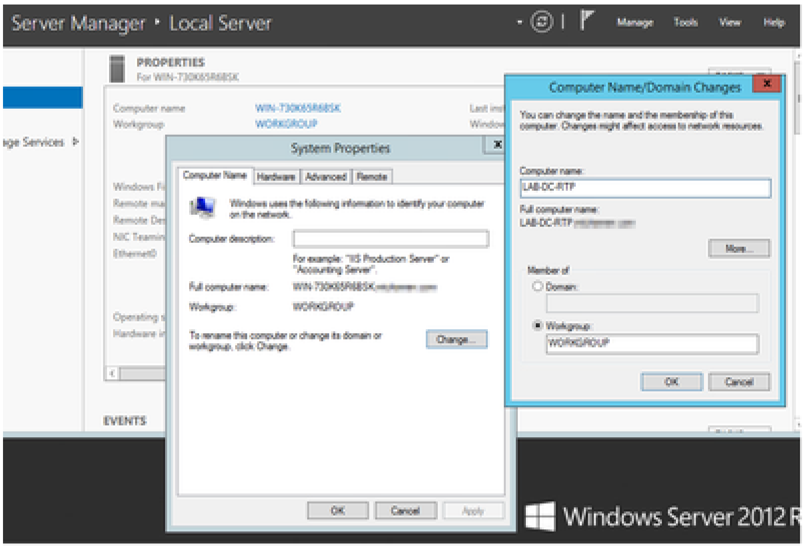
Validate the server time and date

Ensure the Windows server has the correct date, time and time zone configured as it affects the validity times for the server's root CA (Certificate Authority) certificate as well as those certificates issued by it.

Update server Computer Name

By default the serverâ€™s computer name has a random name such as WIN-730K65R6BSK. First thing needs to be done before you enable AD Domain Services is to ensure to update the serverâ€™s computer name to what you want the serverâ€™s hostname and root CA Issuer Name to be by the end of the installation; otherwise it takes a lot of extra steps to change this after AD services are installed.

- Navigate to **Local Server**, select the Computer name to open the **System Properties**
- Select the **Change** button and type in the new Computer name:



Computer name WIN-730K65R6BSK
Workgroup WORKGROUP

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-730K65R6BSK.[redacted]

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change. Change...

Computer Name/Domain Changes

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

Computer name: LAB-DC-RTP

Full computer name: LAB-DC-RTP.[redacted]

More...

Member of
○ Domain:
● Workgroup: WORKGROUP

OK Cancel

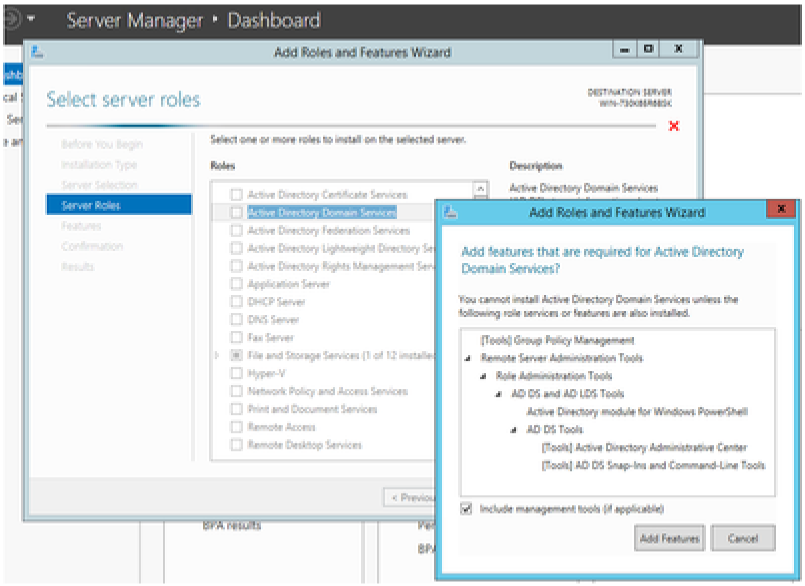
- Restart the server for the changes to get applied

Configure

AD Services, User and and Certificate Template

Enable and Configure Active Directory Services

- In Server Manager select **Add Roles and Features** option, select **Role-based or feature-based installation** and choose the server from the pool (there must only be one in the pool) and then Active Directory Domain Services:



Select server roles

DESTINATION SERVER
WIN-730K8SR68SK

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Se
- □ Active Directory Rights Management Serv
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File and Storage Services (1 of 12 installed
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Domain Services

Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

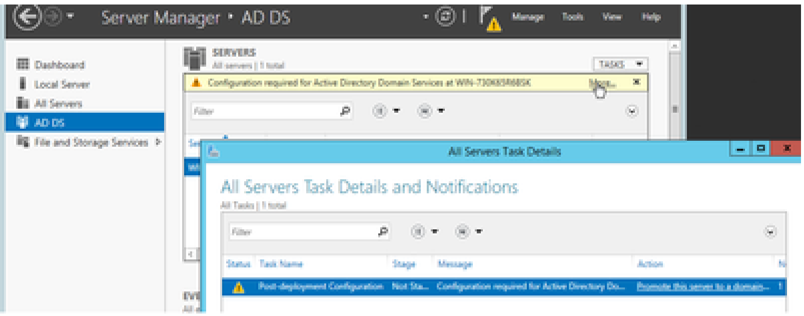
You cannot install Active Directory Domain Services unless the following role services or features are also installed.

- [Tools] Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - AD DS Tools
        - [Tools] Active Directory Administrative Center
        - [Tools] AD DS Snap-Ins and Command-Line Tools

☑ Include management tools (if applicable)

Add Features | Cancel

- Continue to select **Next** button and then **Install**
- Select the **Close** button after it completes the installation
- A warning tab appears under **Server Manager > AD DS** with the title Configuration required for Active Directory Domain Services; Select **more** link and then available action to start the setup wizard:



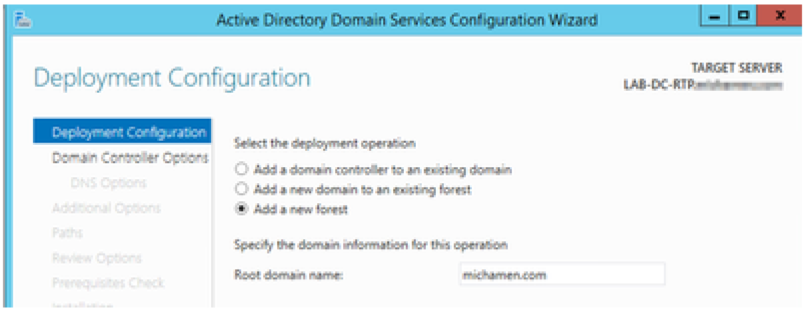
Configuration required for Active Directory Domain Services at WIN-730K8SR68SK More...

All Servers Task Details and Notifications

All Tasks | 1 total

Status	Task Name	Stage	Message	Action
⚠	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Do...	Promote this server to a domain...

- Follow the prompts in the domain setup wizard, add a new Forest with the desired Root Domain Name (used michamen.com for this lab) and uncheck the DNS box when available, define the DSRM password (used *C1sc0123!* for this lab):



Deployment Configuration

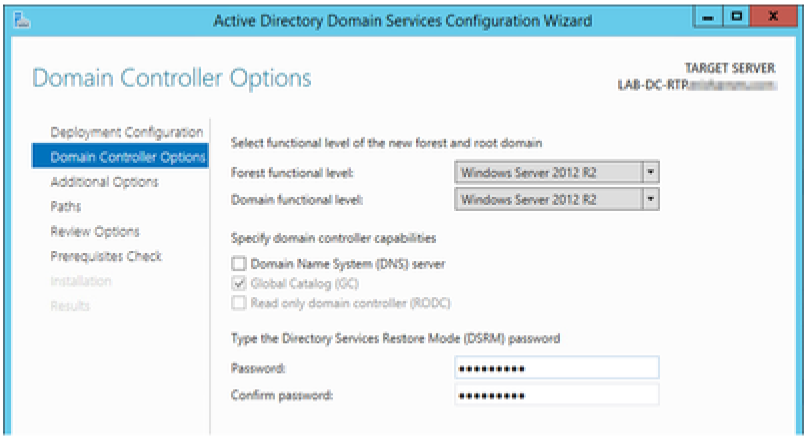
TARGET SERVER
LAB-DC-RTP.[redacted]

Select the deployment operation

- ○ Add a domain controller to an existing domain
- ○ Add a new domain to an existing forest
- ● Add a new forest

Specify the domain information for this operation

Root domain name: michamen.com



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
LAB-DC-RTP.[redacted]

- Deployment Configuration
- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

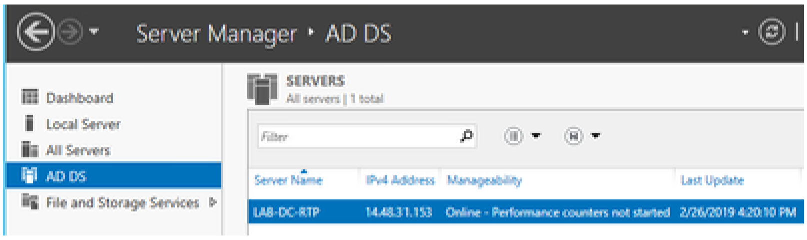
☐ Domain Name System (DNS) server
☑ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

- Need to specify a NetBIOS domain name (used MICHAMEN1 in this lab).
- Follow the wizard to completion. The server then reboots to complete the installation.
- hen need to specify the new domain name next time you log in. E.g MICHAMEN1\Administrator.



Server Manager ▸ AD DS

- Dashboard
- Local Server
- All Servers
- AD DS
- File and Storage Services ▸

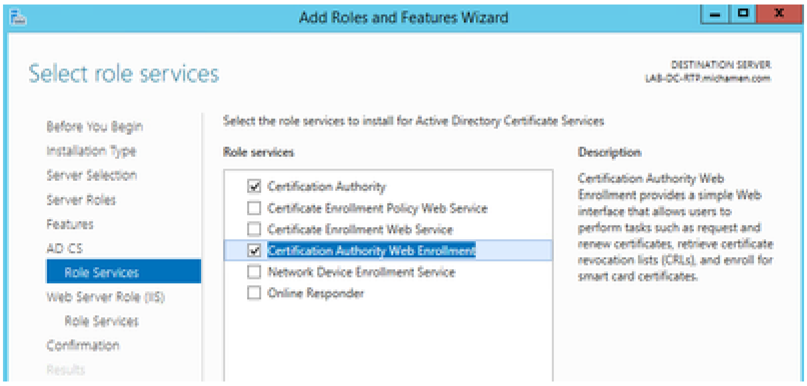
SERVERS
All servers | 1 total

Filter

Server Name	IPv4 Address	Manageability	Last Update
LAB-DC-RTP	14.48.31.153	Online - Performance counters not started	2/26/2019 4:20:10 PM

Enable and Configure Certificate Services

- In Server Manager select Add Roles and Features
- Select Active Directory Certificate Services and follow the prompts to add the required features (all available features were selected from the role services that were enabled for this lab)
- For Role Services check Certification Authority Web Enrollment



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
LAB-DC-RTP.michamen.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD CS
- Role Services
- Web Server Role (IIS)
- Role Services
- Confirmation
- Results

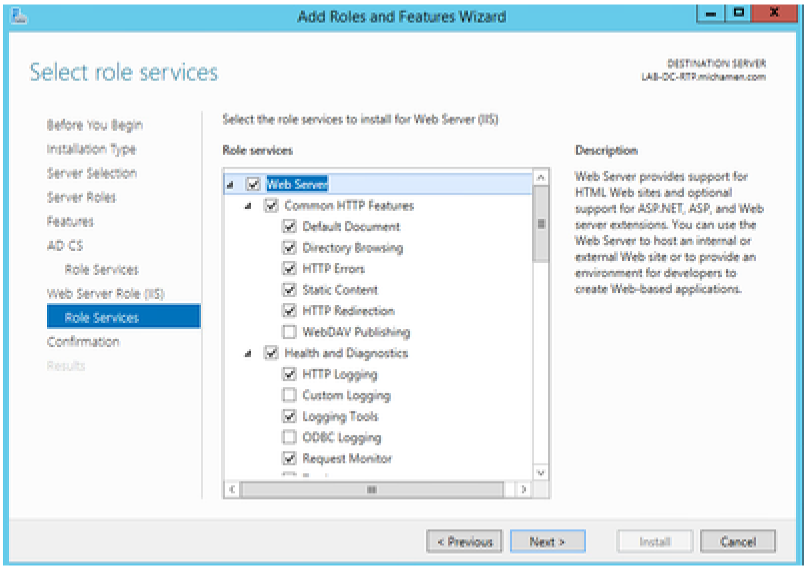
Select the role services to install for Active Directory Certificate Services

Role services

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

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.



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

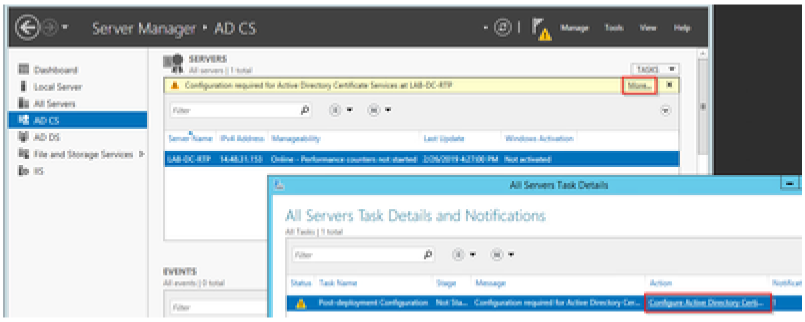
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - ☑ Logging Tools
    - □ ODBC Logging
    - ☑ Request Monitor

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

- A warning tab must appear under **Server Manager >AD DS** with the title Configuration required for Active Directory Certificate Services; Select the **more** link and then available action:

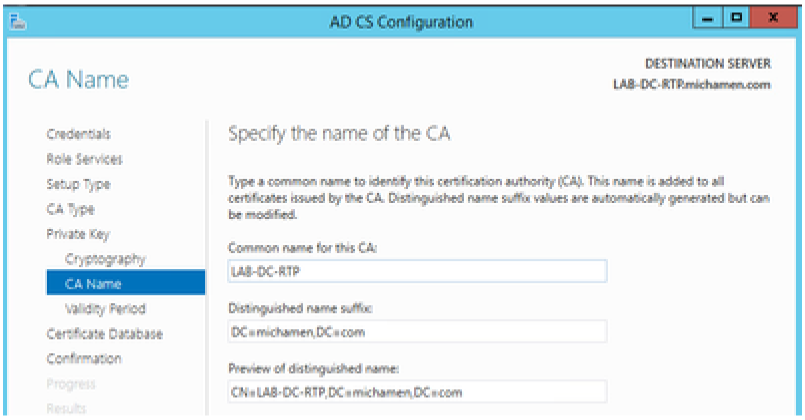


Configuration required for Active Directory Certificate Services at LAB-DC-RTP

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
LAB-DC-RTP	14.48.31.153	Online - Performance counters not started	2/26/2019 4:27:00 PM	Not activated

Status	Task Name	Stage	Message	Action	Notificat
⚠	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Cer...	Configure Active Directory Certi...	

- In the AD-CS Post Install Configuration wizard navigate through these steps:
- Select the **Certification Authority** and **Certification Authority Web Enrollment Roles**
- Choose Enterprise CA with options:
- Root CA
- Create a new private key
- Use Private Key â€“ SHA1 with default settings
- Set a Common Name for the CA (Must match the hostname of the server):



Specify the name of the CA

Type a common name to identify this certification authority (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-DC-RTP

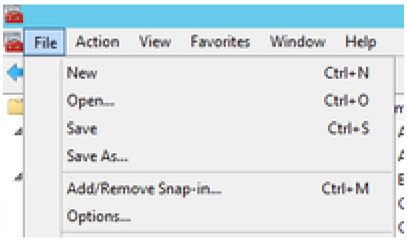
Distinguished name suffix: DC=michamen,DC=com

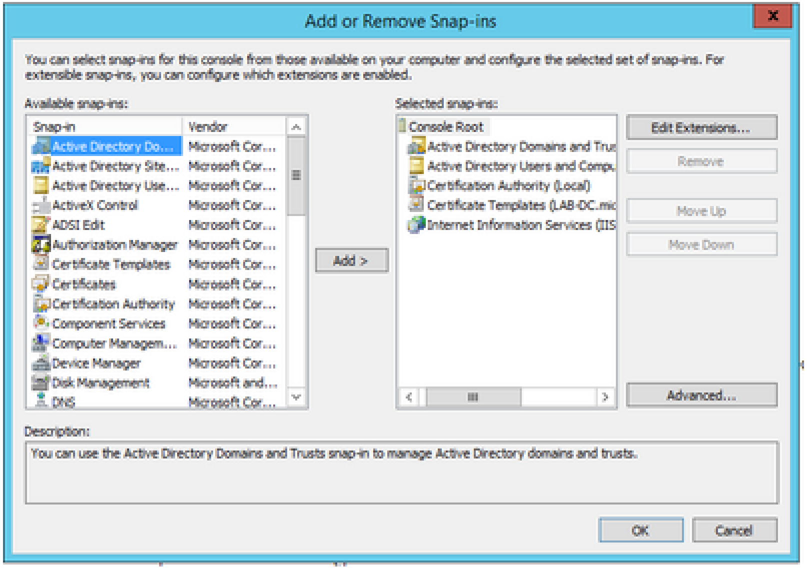
Preview of distinguished name: CN=LAB-DC-RTP,DC=michamen,DC=com

- Set Validity for 5 years (or more if desired)
- Select the **Next** button through the rest of the wizard

Certificate Template Creation for CiscoRA

- Open MMC. Select the windows start logo and type *mmc* from Run
- Open an MMC window and add the follow snap-ins (Used at different points of the configuration) then select **OK**:





You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...

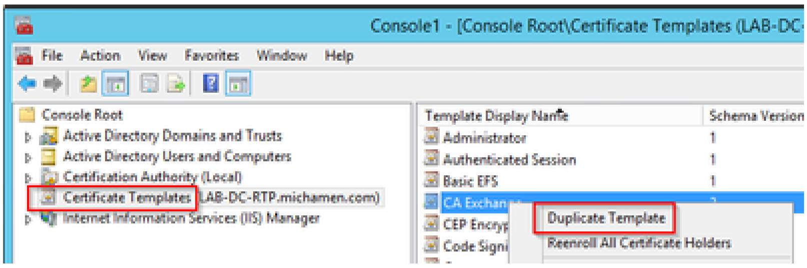
Selected snap-ins:

- Console Root
  - Active Directory Domains and Trus
  - Active Directory Users and Compu
  - Certification Authority (Local)
  - Certificate Templates (LAB-DC.mic
  - Internet Information Services (IIS

Description:

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

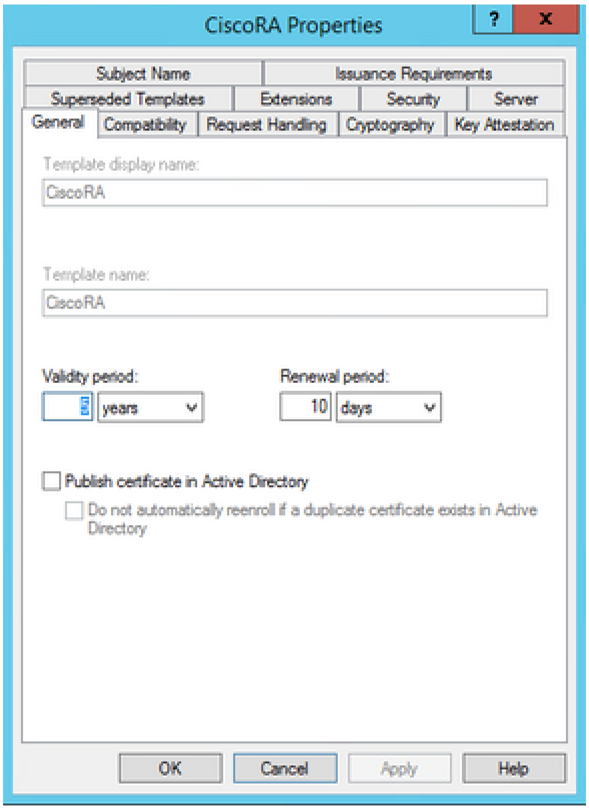
- Select **File** > **Save** and save this console session to desktop for quick re-access
- From the snap-ins, Select **Certificate Templates**
- Create or clone a template (preferably the "*Root Certification Authority*" template if available) and name it CiscoRA


Console1 - [Console Root\Certificate Templates (LAB-DC-
File
Action
View
Favorites
Window
Help
Duplicate Template
Reenroll All Certificate Holders

- Console Root
  - Active Directory Domains and Trusts
  - Active Directory Users and Computers
  - Certification Authority (Local)
  - Certificate Templates (LAB-DC-RTP.michamen.com)
  - Internet Information Services (IIS) Manager

Template Display Name	Schema Version
Administrator	1
Authenticated Session	1
Basic EFS	1
CA Exchan	2
CEP Encryp	
Code Signi	

- Modify the template. Right-click on it and select **Properties**
- Select the **General** tab and set the validity period to 20 years (or other value if desired). In this tab, make sure the template's "display name" and "name" values match



Template display name:
CiscoRA

Template name:
CiscoRA

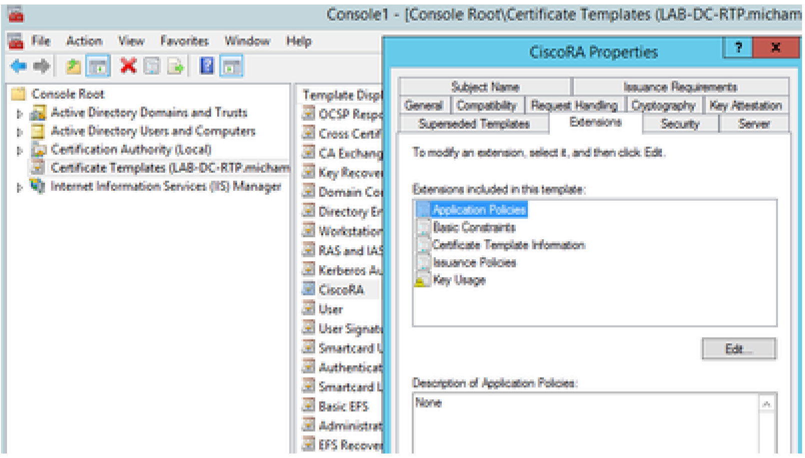
Validity period: 5 years

Renewal period: 10 days

□ Publish certificate in Active Directory

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

- Select the **Extensions** tab, highlight **Application Policies,** and then select **Edit**

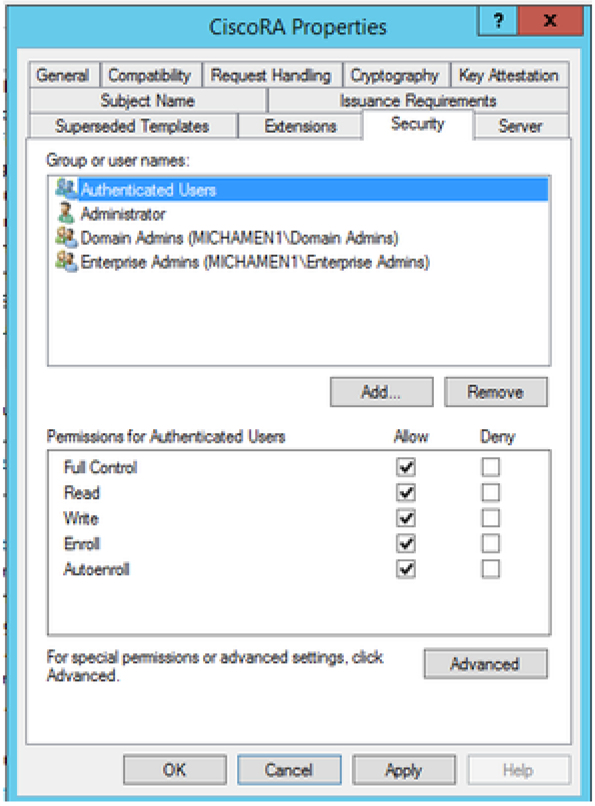


To modify an extension, select it, and then click Edit.

Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage

Description of Application Policies:
None

- Remove any policies that are shown in the window that appears
- Select the **Subject Name** tab and select the **Supply in Request** radio button
- Select the **Security** tab and grant all permissions for all groups/user names that are shown



Group or user names:

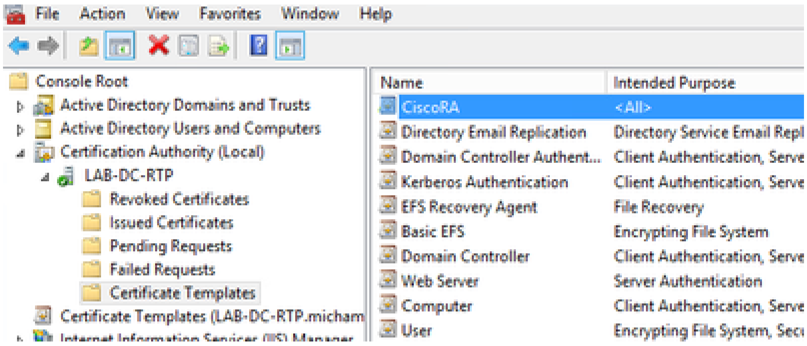
- Authenticated Users
- Administrator
- Domain Admins (MICHAMEN1\Domain Admins)
- Enterprise Admins (MICHAMEN1\Enterprise Admins)

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

For special permissions or advanced settings, click Advanced.

Make the Certificate Template Available to Issue

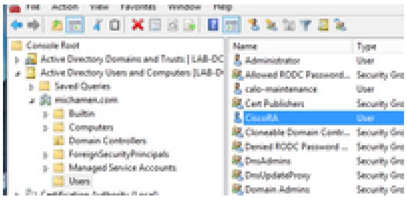
- In the MMC snap-ins select **Certification Authority** and expand the folder tree in order to locate the **Certificate Templates** folder
- Right-click in the white space in the frame that contains Name and Intended Purpose
- Select **New** and **Certificate Template to Issue**
- Select the newly created and edited CiscoRA template


File
Action
View
Favorites
Window
Help
Console Root
Active Directory Domains and Trusts
Active Directory Users and Computers
Certification Authority (Local)
LAB-DC-RTP
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Certificate Templates (LAB-DC-RTP.micham
Internet Information Services (IIS) Manager

Name	Intended Purpose
CiscoRA	<All>
Directory Email Replication	Directory Service Email Repl
Domain Controller Authent...	Client Authentication, Serve
Kerberos Authentication	Client Authentication, Serve
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Serve
Web Server	Server Authentication
Computer	Client Authentication, Serve
User	Encrypting File System, Secu

Active Directory CiscoRA Account Creation

- Navigate to MMC snap-ins and select **Active Directory Users and Computers**
- Select the **Users** folder in the tree in the leftmost pane
- Right-click in the white space in the frame that contains Name, Type and Description
- Select **New** and **User**
- Create the CiscoRA account with username/password (*ciscora/Cisco123* was used for this lab) and select the **Password never expires** checkbox when it is shown

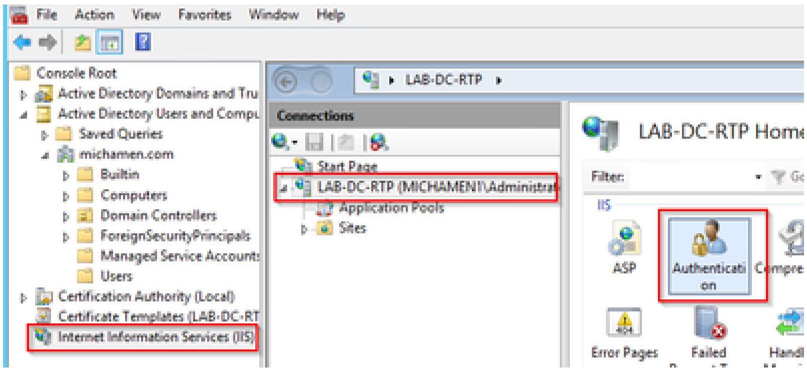


Name	Type
Administrator	User
Allowed RODC Password...	Security Gro
calo-maintenance	User
Cert Publishers	Security Gro
CiscoRA	User
Cloneable Domain Contr...	Security Gro
Denied RODC Password ...	Security Gro
DnsAdmins	Security Gro
DnsUpdateProxy	Security Gro
Domain Admins	Security Gro

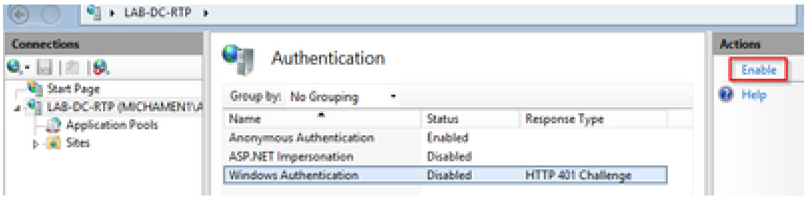
IIS Authentication and SSL Binding Configuration

Enable NTLM Authentication

- Navigate to MMC snap-ins and under the Internet Information Services (IIS) Manager snap-in select your serverâ€™s name
- The features list displays in the next frame. Double-click the **Authentication** feature icon

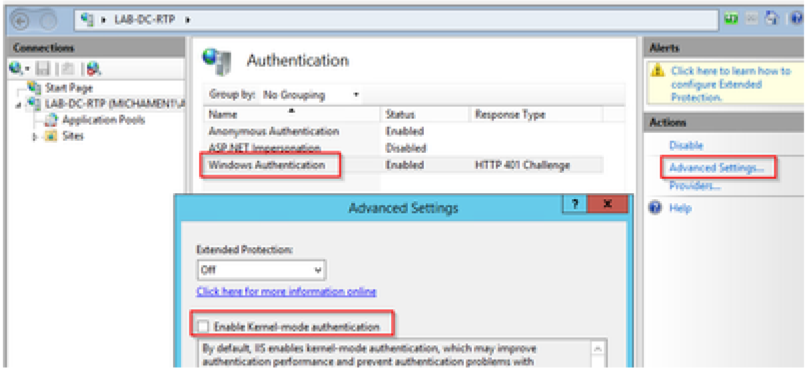


- Highlight **Windows Authentication** and from the Actions frame (Right pane) select the **Enable** option



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Windows Authentication	Disabled	HTTP 401 Challenge

- Actions pane displays **Advanced Settings** option; select it and uncheck **Enable Kernel-mode authentication**



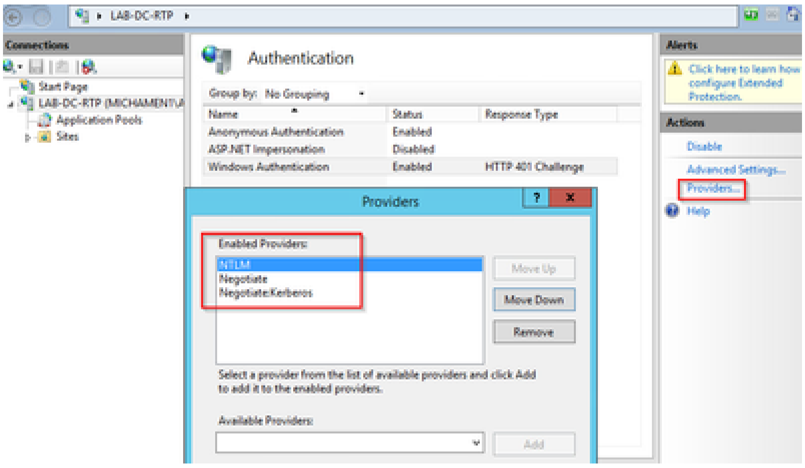
Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Windows Authentication	Enabled	HTTP 401 Challenge

Extended Protection: Off

□ Enable Kernel-mode authentication

By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with

- Select **Providers** and put in order **NTML** then **Negotiate.**



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Windows Authentication	Enabled	HTTP 401 Challenge

Click here to learn how configure Extended Protection.

Enabled Providers:

NTLM
Negotiate
Negotiate:Kerberos

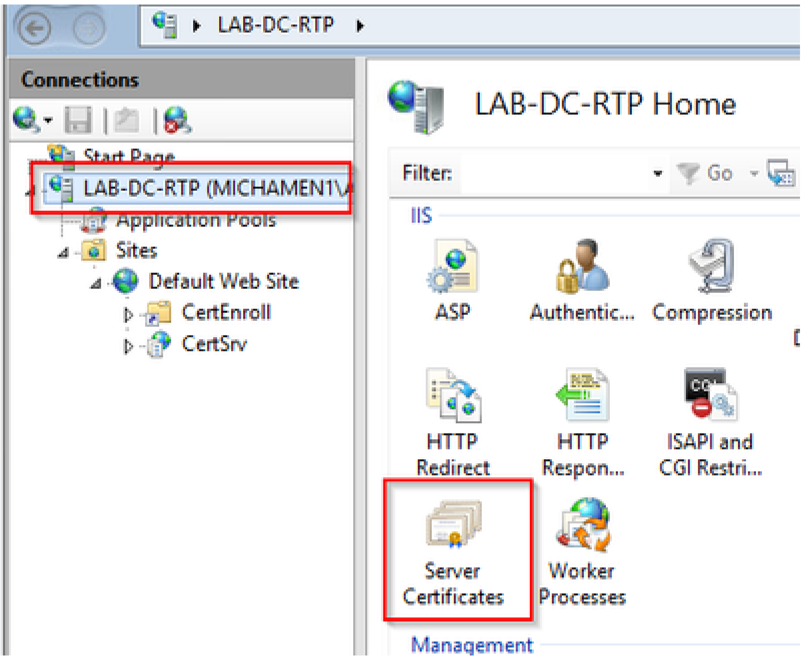
Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

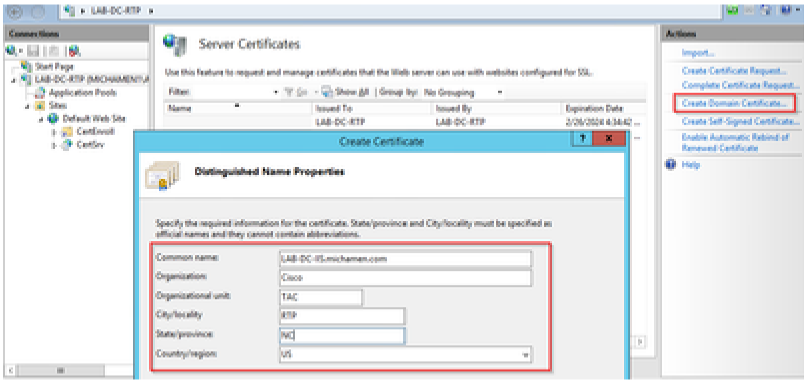
Generate the Identity Certificate for the Web Server

If not already the case, you need to generate a certificate an identity certificate for your Web service that is signed by the CA because CiscoRA is not able to connect to it if the Web serverâ€™s certificate is Self-Signed:

- Select your Web server from the **IIS snap-in** and double-click the **Server Certificates** feature icon:



- By default, you are able to see one certificate listed there; which is the self-signed root CA cert; From the **Actions** menu select the **Create Domain Certificate** option. Enter the values in the configuration wizard in order to create your new certificate. Ensure the Common name is a resolvable FQDN (Fully Qualified Domain Name) and then select **Next**:


LAB-DC-RTP
Connections
Start Page
LAB-DC-RTP (MICHAMEN\A
Application Pools
Sites
Default Web Site
CertEnroll
CertSrv
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Create Certificate
Distinguished Name Properties

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

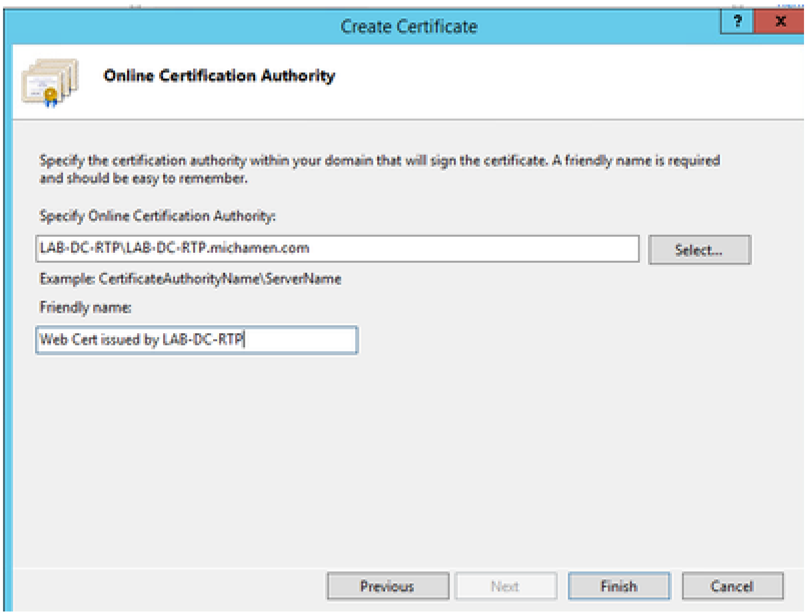
Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date
	LAB-DC-RTP	LAB-DC-RTP	2/26/2024 4:34:42 ...

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: LAB-DC-IIS.michamen.com
Organization: Cisco
Organizational unit: TAC
City/locality: RTP
State/province: NC
Country/region: US

- Select your root CAâ€™s certificate to be the issuer and select **Finish**:



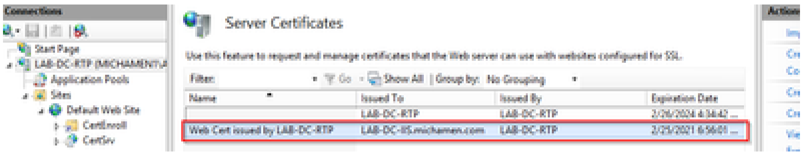
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.

Specify Online Certification Authority:
LAB-DC-RTP\LAB-DC-RTP.michamen.com

Example: CertificateAuthorityName\ServerName

Friendly name:
Web Cert issued by LAB-DC-RTP

- You are able to see both, the CA certificate and your Web Serverâ€™s Identity certificate listed:



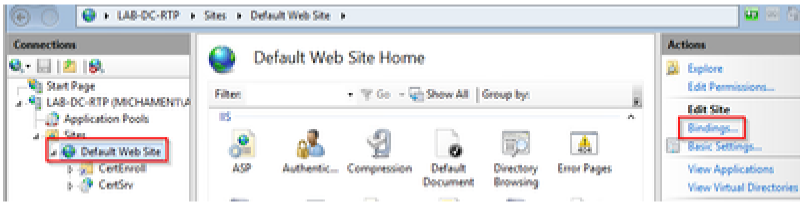
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

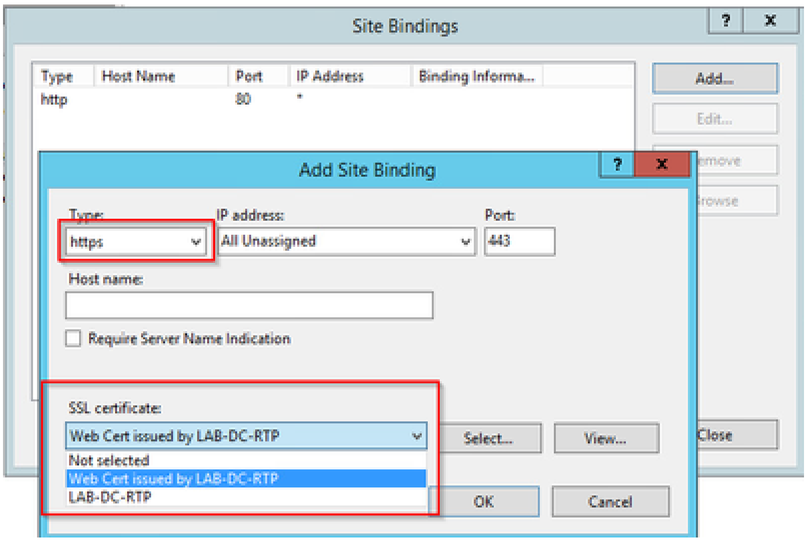
Name	Issued To	Issued By	Expiration Date
	LAB-DC-RTP	LAB-DC-RTP	2/26/2024 4:34:42 ...
Web Cert issued by LAB-DC-RTP	LAB-DC-IIS.michamen.com	LAB-DC-RTP	2/25/2021 6:56:01 ...

Web Server SSL Binding

- Select a site in the tree view (you can use the Default Web Site or make it more granular to specific sites) and select **Bindings** from the Actions pane. This brings up the bindings editor that allows you to create, edit, and delete bindings for your Web site. Select **Add** in order to add your new SSL binding to the site.



- The default settings for a new binding are set to HTTP on port 80. Select **https** in the **Type** drop-down list. Select the self-signed certificate you created in the previous section from the **SSL Certificate** drop-down list and then select **OK**.



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

Type: https

IP address: All Unassigned

Port: 443

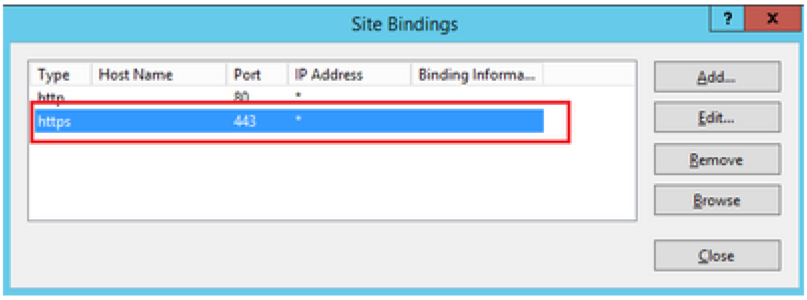
Host name:

□ Require Server Name Indication

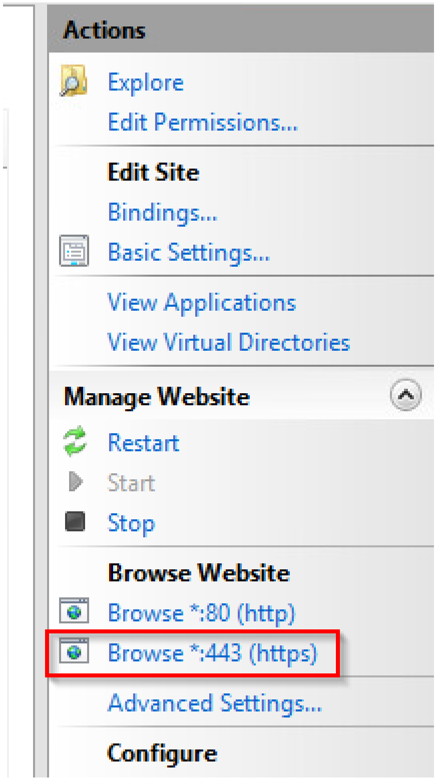
SSL certificate: Web Cert issued by LAB-DC-RTP

Not selected
Web Cert issued by LAB-DC-RTP
LAB-DC-RTP

- Now you have a new SSL binding on your site and all that remains is to verify that it works by select **Browse *:443 (https)** option from the menu and ensure the default IIS Web page uses HTTPS:



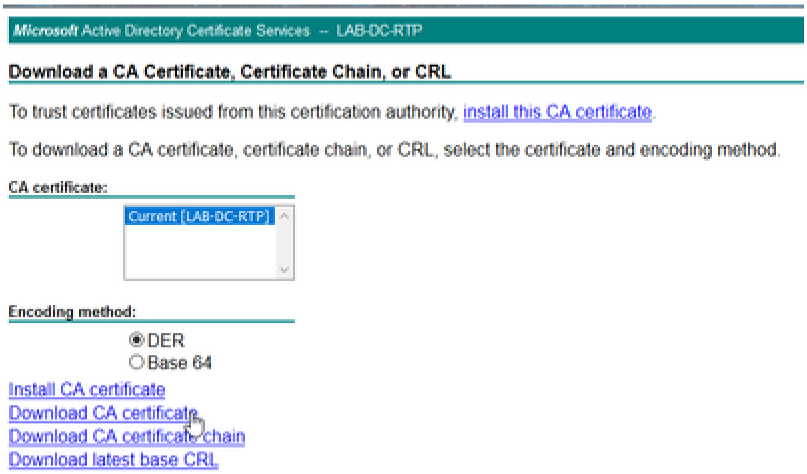
Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	



- Remember to restart the IIS service after configuration changes. Use the **Restart** option from the Actions pane.

CUCM Configuration

- Navigate to your AD CS Web page (https://YOUR_SERVER_FQDN/certsrv/) and download the CA certificate



Microsoft Active Directory Certificate Services -- LAB-DC-RTP

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

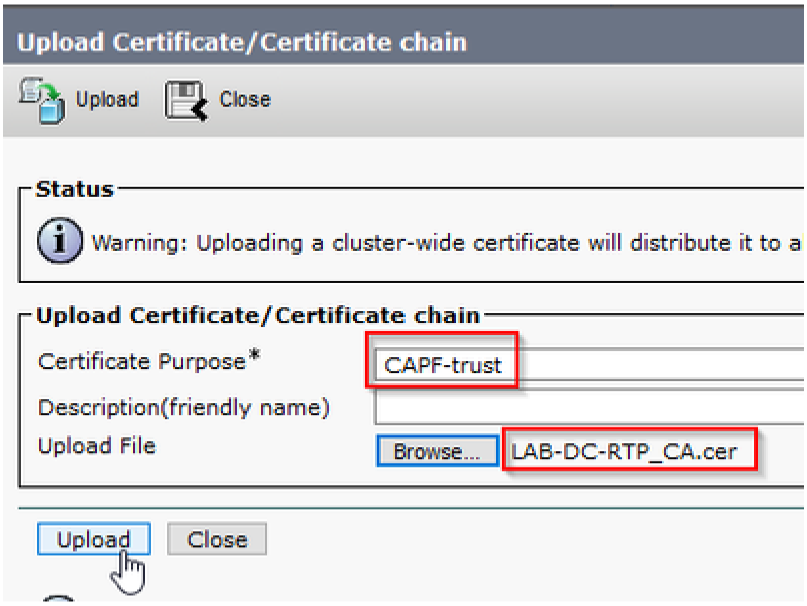
Current [LAB-DC-RTP]

Encoding method:

● DER
○ Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL

- Navigate to **Security** > **Certificate Management** from the OS Administration page and select the **Upload Certificate/Certificate chain** button in order to upload the CA certificate with the *purpose* set to *CAPF-trust.*



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to a

Upload Certificate/Certificate chain

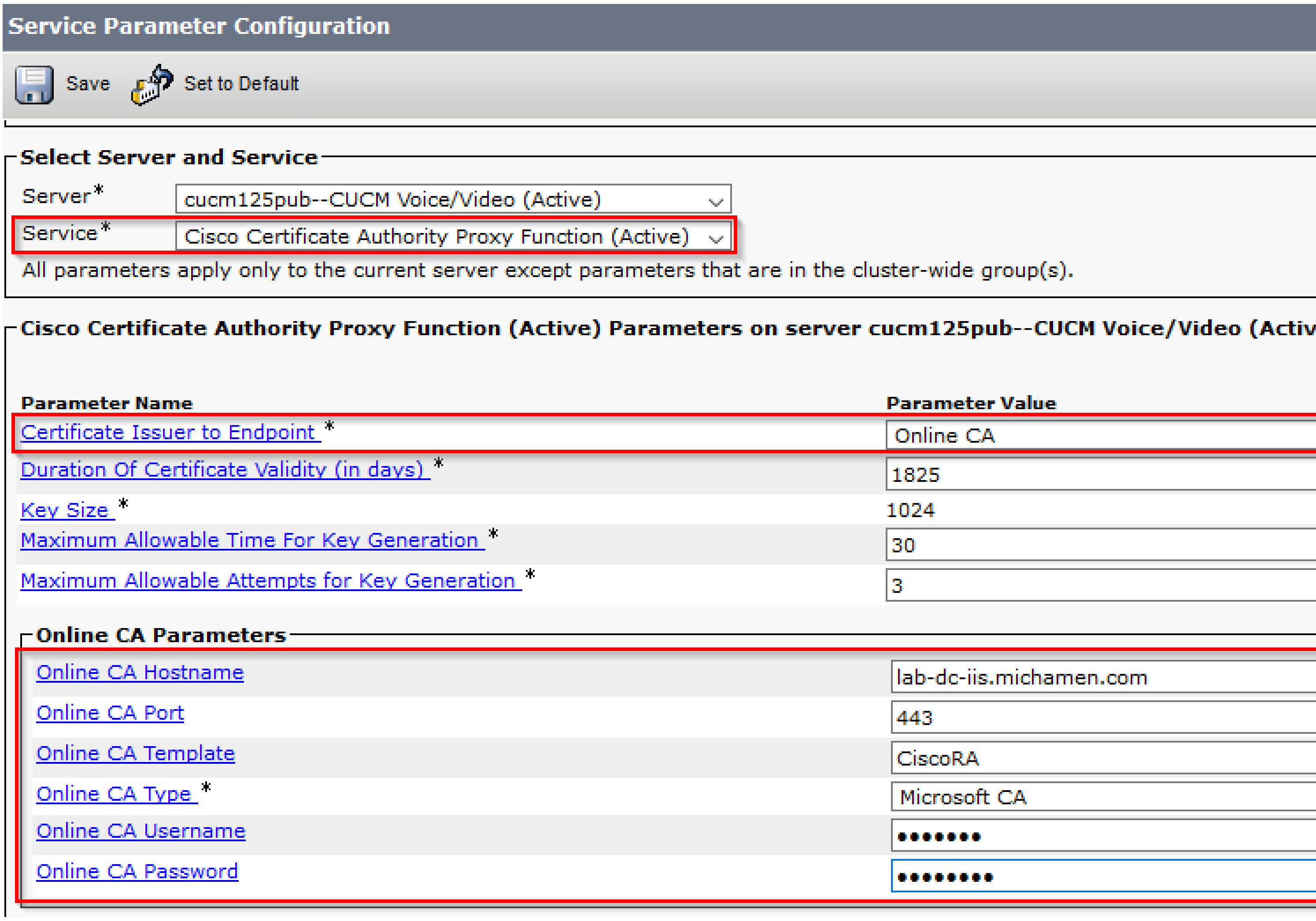
Certificate Purpose* CAPF-trust

Description(friendly name)

Upload File Browse... LAB-DC-RTP_CA.cer

... At this point it's also be a good idea to upload that same CA certificate as *CallManager-trust* because it is needed if secure signaling encryption is enabled (or will be enabled) for the endpoints; which is likely if the cluster is in Mixed-Mode.

- Navigate to **System** > **Service Parameters.** Select the Unified CM Publisher server in the server field and **Cisco Certificate Authority Proxy Function** in the Service field
- Set the vale of Certificate Issuer to Endpoint to Online CA and enter the values for the Online CA Parameters fields. Ensure to use the Web serverâ€™s FQDN, the name of the certificate template created earlier (CiscoRA), the CA type as Microsoft CA and use the credentials of the CiscoRA user account created earlier



Service Parameter Configuration

Select Server and Service

Server *	cucm125pub--CUCM Voice/Video (Active)
Service *	Cisco Certificate Authority Proxy Function (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

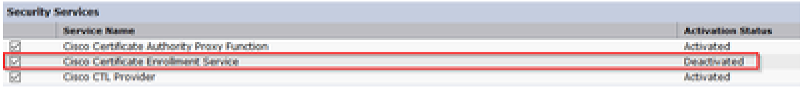
Cisco Certificate Authority Proxy Function (Active) Parameters on server cucm125pub--CUCM Voice/Video (Activ

Parameter Name	Parameter Value
Certificate Issuer to Endpoint *	Online CA
Duration Of Certificate Validity (in days) *	1825
Key Size *	1024
Maximum Allowable Time For Key Generation *	30
Maximum Allowable Attempts for Key Generation *	3

Online CA Parameters

Online CA Hostname	lab-dc-iis.michamen.com
Online CA Port	443
Online CA Template	CiscoRA
Online CA Type *	Microsoft CA
Online CA Username	•••••••
Online CA Password	••••••••

- A pop window informs you that the CAPF service needs to be restarted. But first, activate the Cisco Certificate Enrollment Service through **Cisco Unified Serviceability** > **Tools** > **Service Activation**, select the Publisher in the Server field and check the Cisco Certificate Enrollment Service checkbox, and then select the **Save** button:



Security Services

	Service Name	Activation Status
☑	Cisco Certificate Authority Proxy Function	Activated
☑	Cisco Certificate Enrollment Service	Deactivated
☑	Cisco CTL Provider	Activated

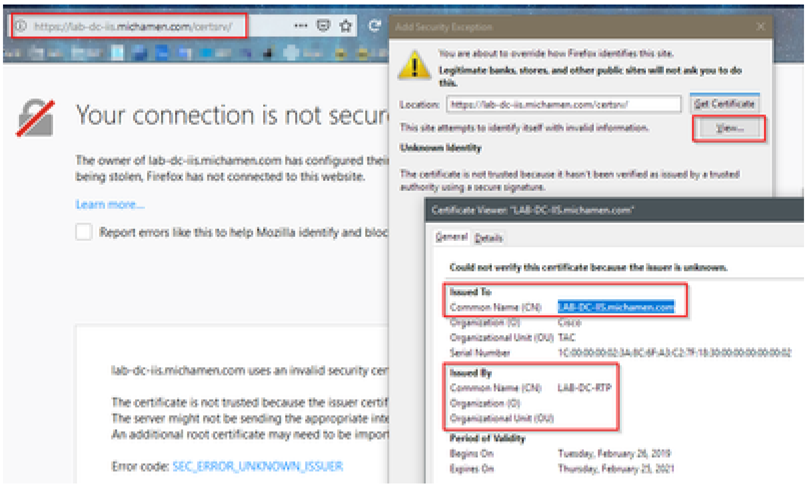
Verify

Verify IIS Certificates

- From a Web browser in a PC with connectivity to the server (preferably in the same network as the CUCM Publisher) navigate to URL:

  https://**YOUR_SERVER_FQDN**/certsrv/

- Certificate not-trusted alert is displayed. Add the exception and check the certificate. Ensure it matches the expected FQDN:



https://lab-dc-iis.michamen.com/certsrv/

Your connection is not secur

The owner of lab-dc-iis.michamen.com has configured thei being stolen, Firefox has not connected to this website.

Learn more...

□ Report errors like this to help Mozilla identify and bloc

lab-dc-iis.michamen.com uses an invalid security cer

The certificate is not trusted because the issuer certif The server might not be sending the appropriate inte An additional root certificate may need to be impor

Error code: SEC_ERROR_UNKNOWN_ISSUER

Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://lab-dc-iis.michamen.com/certsrv/ Get Certificate

This site attempts to identify itself with invalid information. View...

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

Certificate Viewer: "LAB-DC-IIS.michamen.com"

General Details

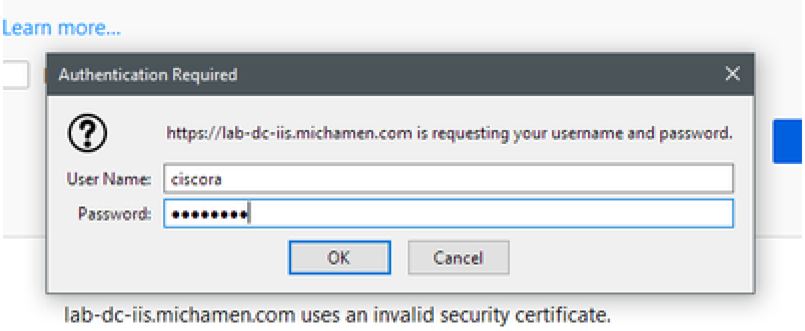
Could not verify this certificate because the issuer is unknown.

Issued To
Common Name (CN) LAB-DC-IIS.michamen.com
Organization (O) Cisco
Organizational Unit (OU) TAC
Serial Number 1C:00:00:00:02:3A:0C:6F:A3:C2:7F:18:30:00:00:00:00:00:02

Issued By
Common Name (CN) LAB-DC-RTP
Organization (O)
Organizational Unit (OU)

Period of Validity
Begins On Tuesday, February 26, 2019
Expires On Thursday, February 25, 2021

- After you accept the exception, you need to authenticate; at this point you need to use the credentials configured for the CiscoRA account earlier:



Learn more...

Authentication Required

https://lab-dc-iis.michamen.com is requesting your username and password.

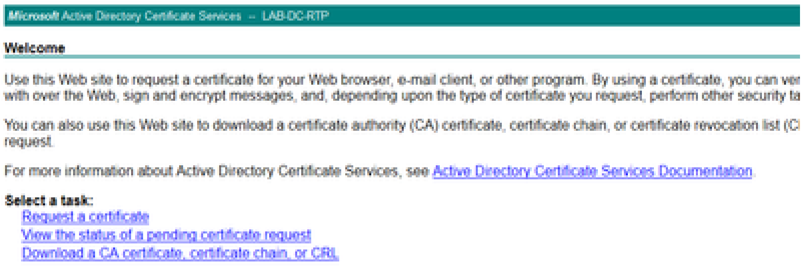
User Name: ciscora

Password: ••••••••

OK Cancel

lab-dc-iis.michamen.com uses an invalid security certificate.

- After authentication you must be able to see the AD CS (Active Directory Certificate Services) Welcome page:



Microsoft Active Directory Certificate Services -- LAB-DC-RTP

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 ver with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security ta

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (C request.

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

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Verify CUCM Configuration

Perform the steps you normally follow in order to install an LSC certificate on one of the phones.

Step 1. Open the CallManager Administration page, Device and then Phone

Step 2. Select the **Find** button to display the phones

Step 3. Select the phone you wish to install the LSC on

Step 4. Scroll down to Certification Authority Proxy Function (CAPF) Information

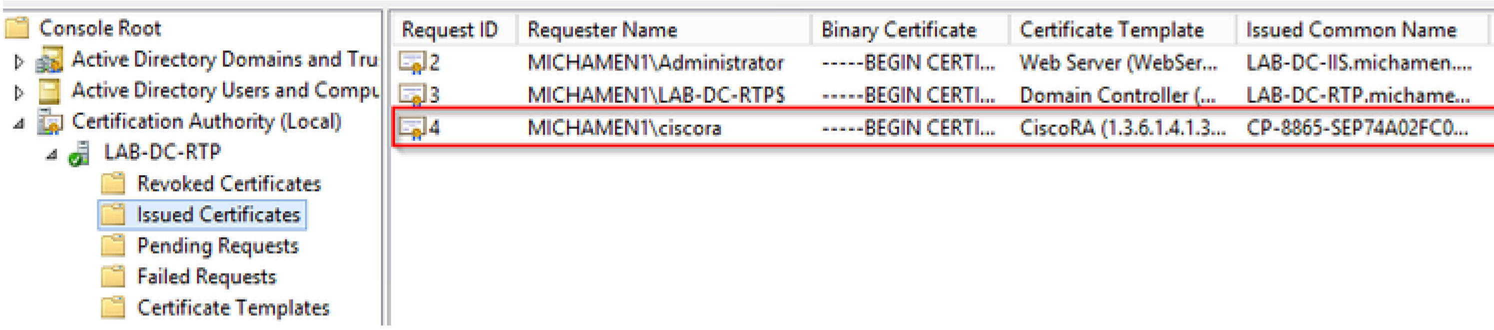
Step 5. Select the Install/Upgrade from the Certificate Operation.

Step 6. Select the Authentication Mode. (By Null String is fine for test purposes)

Step 7. Scroll to the top of the page and select **save** then **Apply Config** for the phone.

Step 8. After the phone restarts and registers back use the LSC Status filter to confirm the LSC installed successfully.

- From the AD serverâ€™s side open MMC and expand the Certification Authority snap-in to select the Issued Certificates folder
- The entry for the phone is displayed Inside the summary view, these are some of the details displayed:
  - Request ID: Unique sequence number
  - Requester Name: The username of the configured CiscoRA account must be displayed
  - Certificate Template: The name of the CiscoRA template created must be displayed
  - Issued Common Name: The phoneâ€™s model appended by the device name must be displayed
  - Certificate Effective Date and Certificate Expiration Date



Request ID	Requester Name	Binary Certificate	Certificate Template	Issued Common Name
2	MICHAMEN1\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	LAB-DC-IIS.michamen....
3	MICHAMEN1\LAB-DC-RTP$	-----BEGIN CERTI...	Domain Controller (...	LAB-DC-RTP.michame...
4	MICHAMEN1\ciscora	-----BEGIN CERTI...	CiscoRA (1.3.6.1.4.1.3...	CP-8865-SEP74A02FC0...

Related Links

- [Troubleshooting CAPF Online CA]()
- [Technical Support & Documentation - Cisco Systems]()