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 Certificate Template
  - Enable and Configure Active Directory Services
  - Enable and Configure Certificate Services
  - Certificate Template Creation for CiscoRA
  - Make the Certificate Template Available to Issue
  - Active Directory CiscoRA Account Creation
- IIS Authentication and SSL Binding Configuration
  - Enable NTLM Authentication
  - Generate the Identity Certificate for the Web Server
  - Web Server SSL Binding
- CUCM Configuration

Verify

- Verify IIS Certificates
- Verify CUCM Configuration

Related Links

Introduction

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

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.

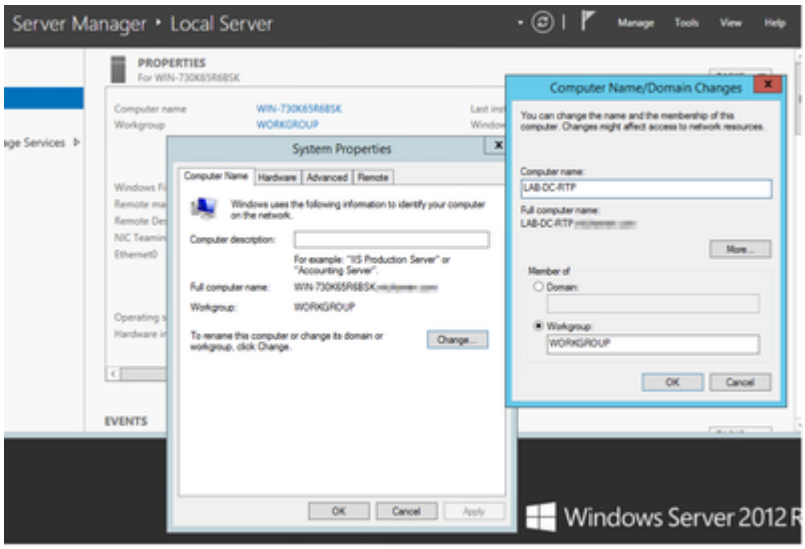
Validate the Server Time and Date

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

Update Server Computer Name

By default, the server computer name has a random name such as WIN-730K65R6BSK. First thing that needs to be done before you enable AD Domain Services is to ensure to update the server computer name to what you want the server 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.

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



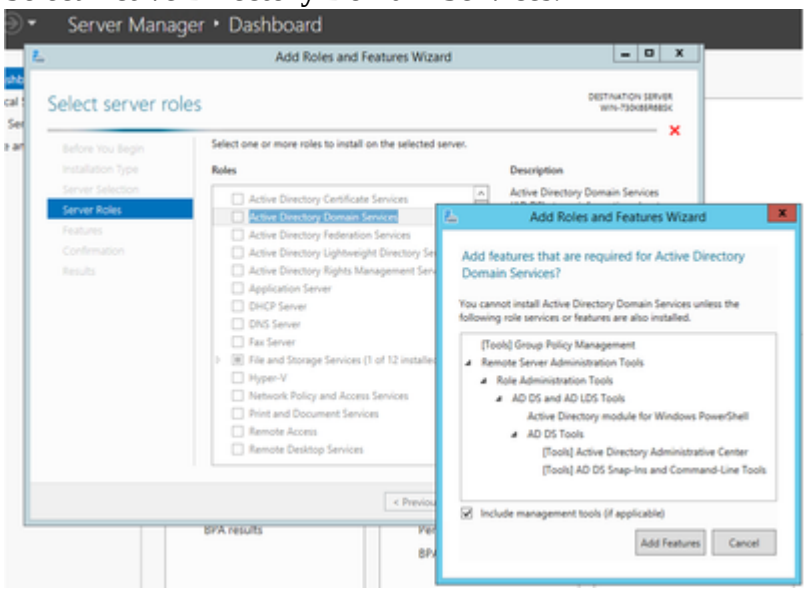
3. Restart the server for the changes to get applied.

Configure

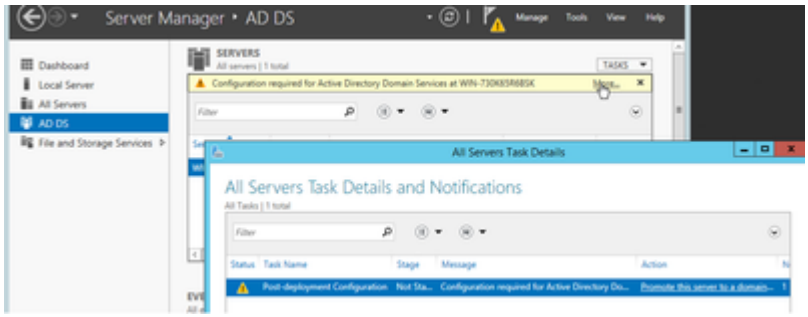
AD Services, User and Certificate Template

Enable and Configure Active Directory Services

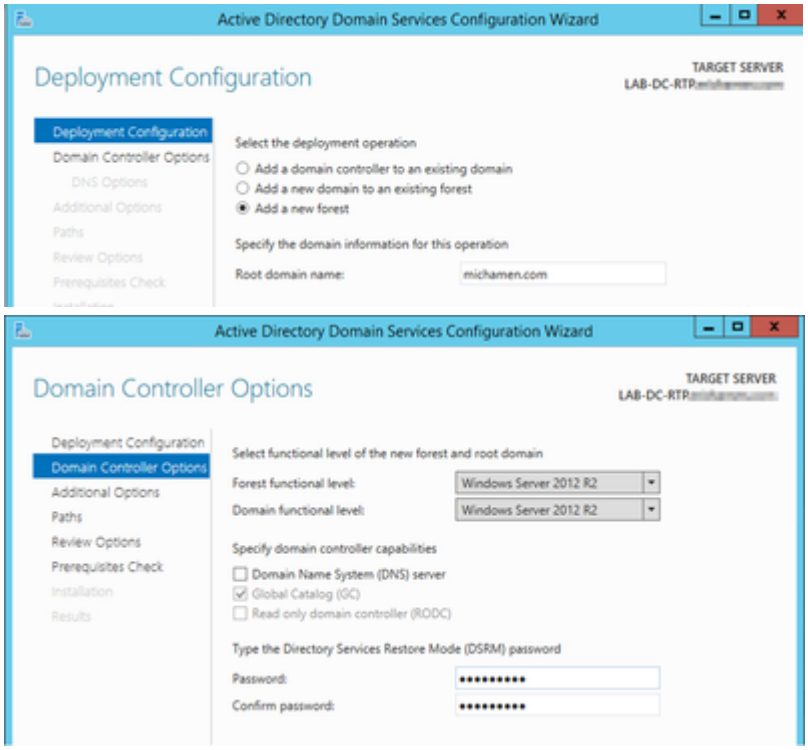
1. In **Server Manager**, select **Add Roles and Features**, select **Role-based** or **feature-based** installation.
2. Choose the **server** from the pool (there must only be one in the pool).
3. Select **Active Directory Domain Services**.



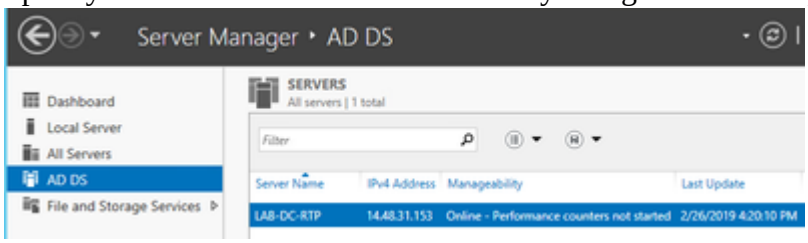
4. Continue to select **Next** button and then **Install**.
5. Select the **Close** button after it completes the installation.
6. A warning tab appears under **Server Manager** > **AD DS** with the title Configuration required for Active Directory Domain Services. Select **more** link and then **available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



7. Complete the prompts in the domain setup wizard, add a **new forest** with the desired Root Domain Name and uncheck the **DNS** box when available. Define the **DSRM password**.

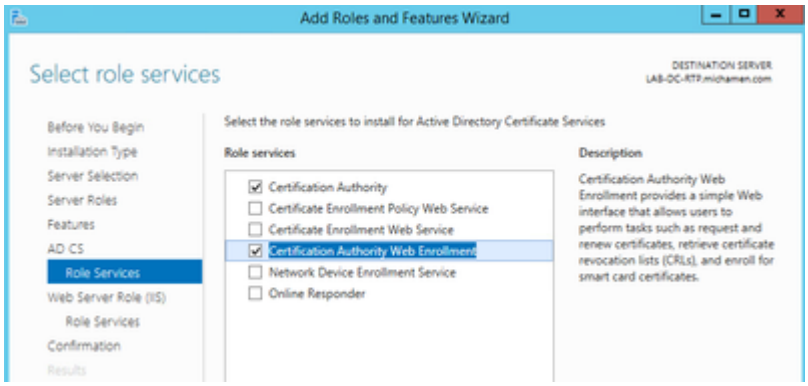


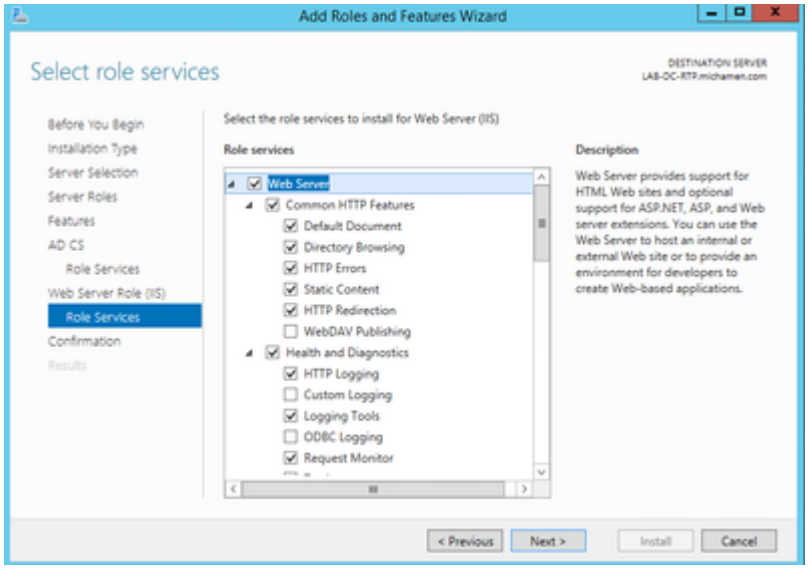
8. Specify a **NetBIOS domain name** (used MICHAMEN1 in this lab).
9. Complete the **wizard**. The server then reboots to complete the installation.
10. Specify the new **domain name** next time you log in. For example, MICHAMEN1\Administrator.



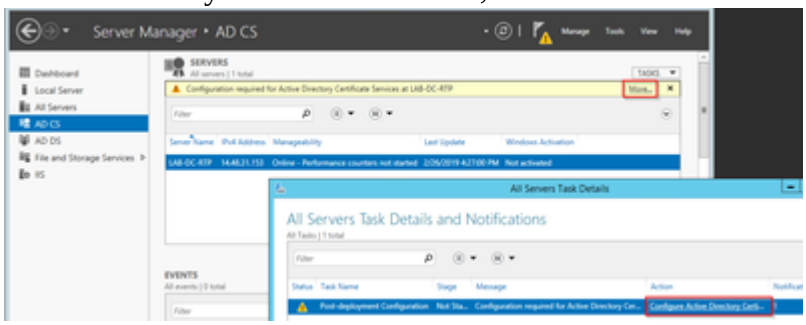
Enable and Configure Certificate Services

1. In Server Manager, select **Add Roles and Features**.
2. Select **Active Directory Certificate Services** and add the **required features** (all available features were selected from the role services that were enabled for this lab).
3. For Role Services, check **Certification Authority Web Enrollment**.



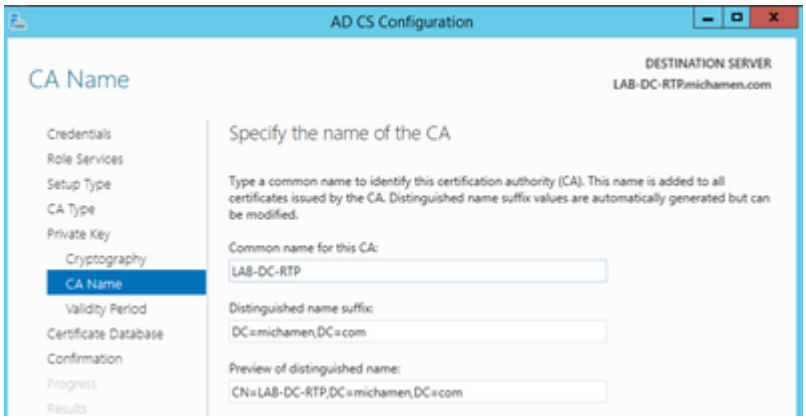


4. A warning tab must appear under **Server Manager** > **AD DS** with the title Configuration required for Active Directory Certificate Services; Select the **more link** and then **available action**.



Complete these steps in the AD-CS Post Install Configuration wizard:

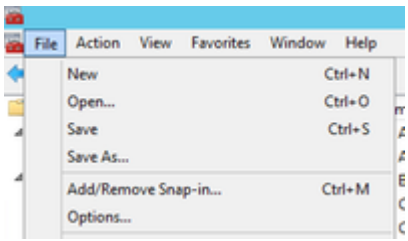
1. Select the **Certification Authority and Certification Authority Web Enrollment Roles**.
2. Choose **Enterprise CA** with options:
3. Root CA
4. Create a **new private key**.
5. Use Private Key – SHA1 with default settings.
6. Set a **Common Name** for the CA (Must match the hostname of the server).

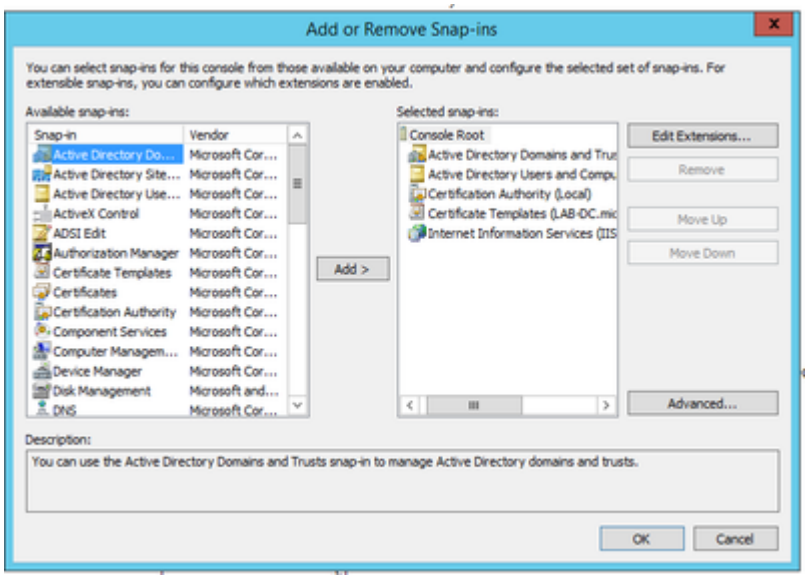


7. Set **Validity** for 5 years (or more if desired).
8. Select the **Next** button through the rest of the wizard.

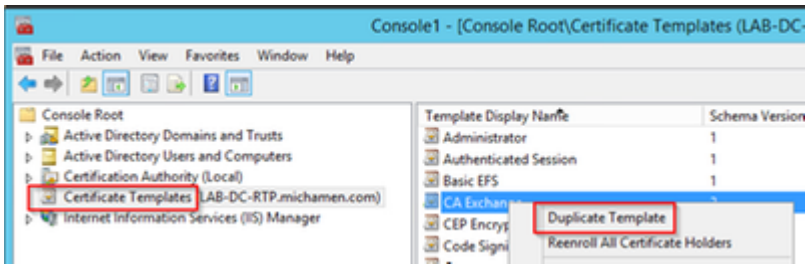
Certificate Template Creation for CiscoRA

1. Open **MMC**. Select the **windows start logo** and type **mmc from Run**.
2. Open an **MMC** window, add the **snap-ins** (used at different points of the configuration), and select **OK**.

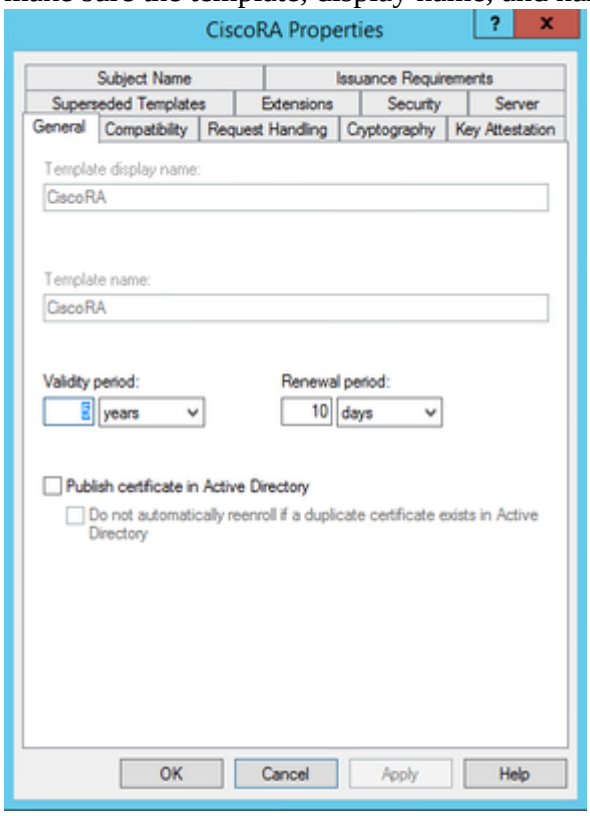




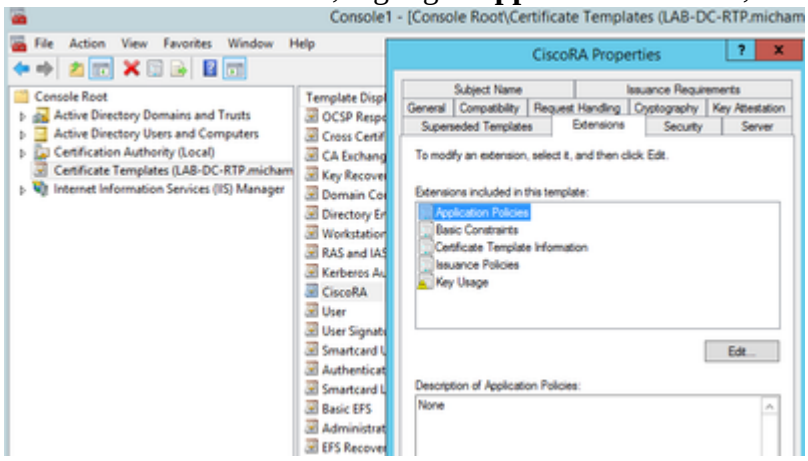
3. Select **File** > **Save** and save this **console session** to desktop for quick re-access.
4. From the snap-ins, Select **Certificate Templates**.
5. Create or clone a **template** (preferably the Root Certification Authority template if available) and name it **CiscoRA**.



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



8. Select the **Extensions** tab, highlight **Application Policies**, and select **Edit**.

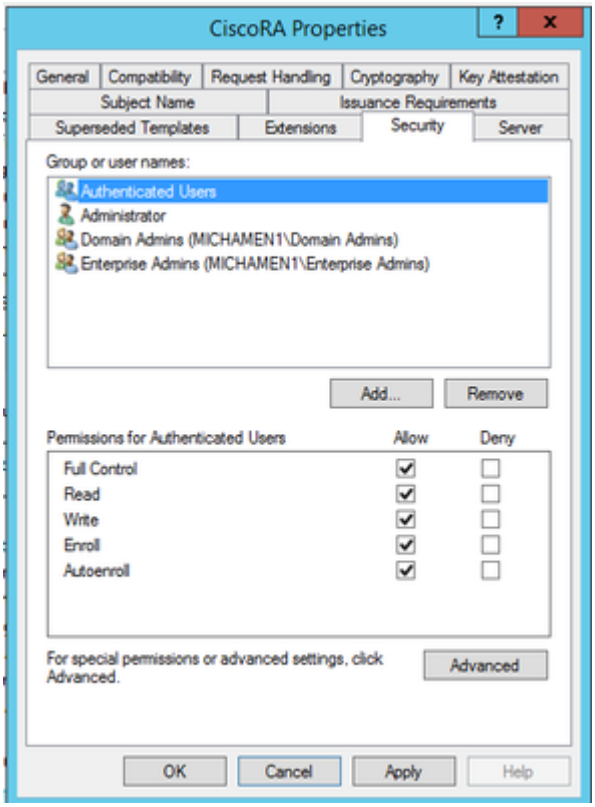


9. Remove any **policies** that are shown in the window that appears.
10. Select the **Subject Name** tab and select the **Supply in Request** radio button.
11. Select the **Security** tab and grant **permissions** according to your needs for groups/user names.

Note: In this example, full permissions were granted across the board for simplicity, but this

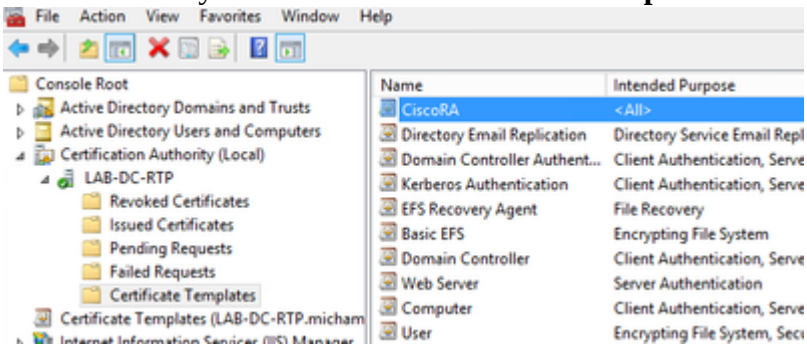
---

has security implications. In a production environment, write and enroll permissions must only be granted to those users and groups that require it. Please, refer to the Microsoft documentation for more information.



Make the Certificate Template Available to Issue

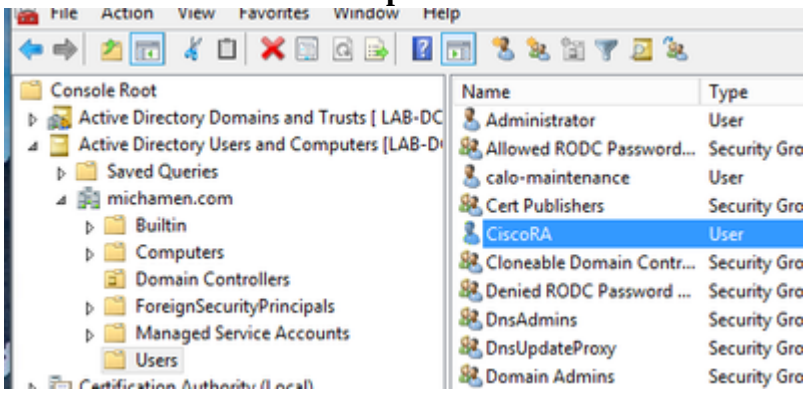
1. In the MMC snap-ins select **Certification Authority** and expand the **folder tree** to locate the Certificate Templates folder.
2. Right-click in the white space in the frame that contains Name and Intended Purpose.
3. Select **New** and **Certificate Template to Issue**.
4. Select the newly created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



Active Directory CiscoRA Account Creation

1. Navigate to **MMC snap-ins** and select **Active Directory Users and Computers**.
2. Select the **Users** folder in the tree in the leftmost pane.

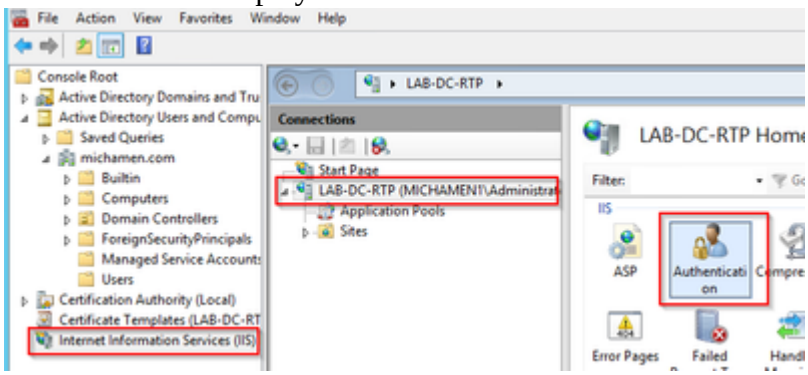
3. **Right-click** in the **white space** in the frame that contains Name, Type and Description.
4. Select **New** and **User**.
5. Create the **CiscoRA account** with username/password (ciscora/Cisco123 was used for this lab) and select the **Password never expires** checkbox when it is shown.



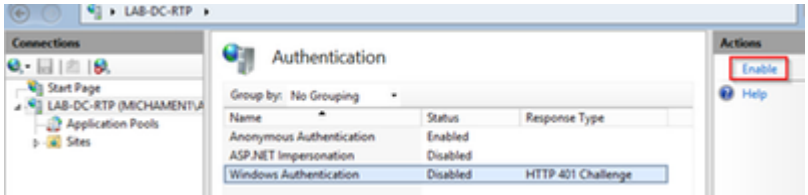
IIS Authentication and SSL Binding Configuration

Enable NTLM Authentication

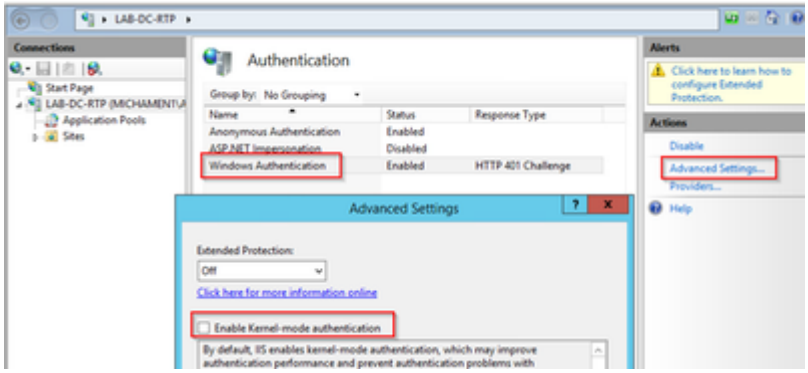
1. Navigate to **MMC snap-ins** and under the **Internet Information Services (IIS) Manager snap-in** select your **server name**.
2. The features list displays in the next frame. Double-click **Authentication**.



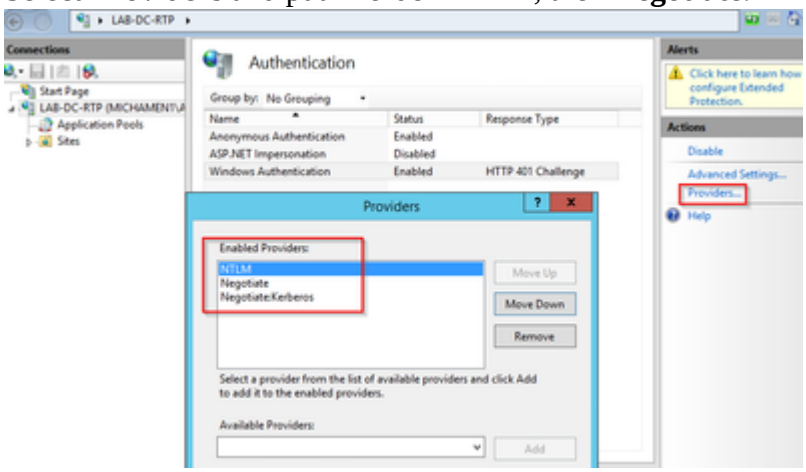
3. Select **Windows Authentication** and from the **Actions frame** (right pane) select **Enable**.



4. Seelct **Advanced Settings** and clear the **Enable Kernel-mode authentication** check box.



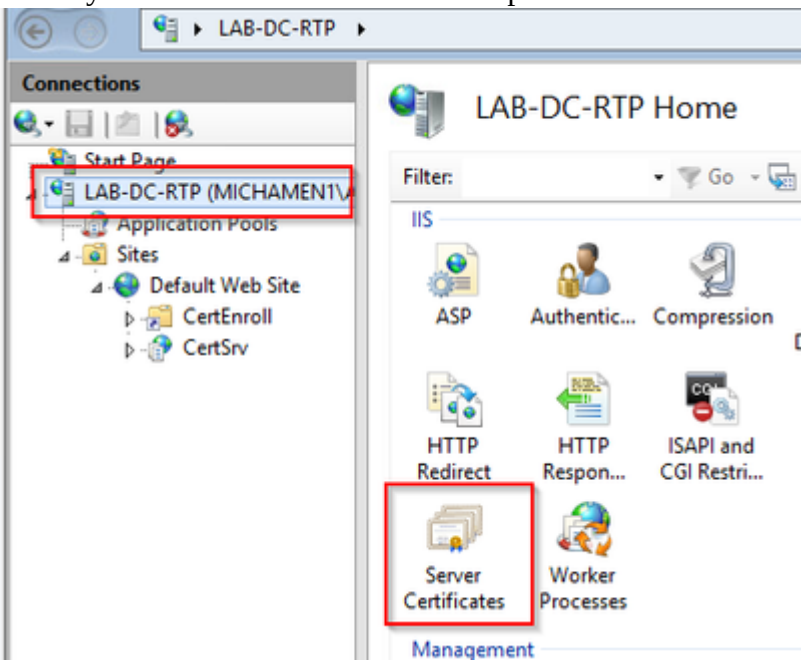
5. Select **Providers** and put in order NTML, then **Negotiate**.



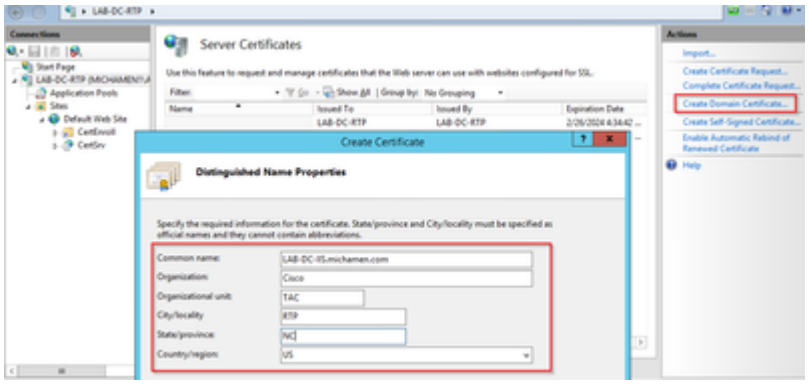
Generate the Identity Certificate for the Web Server

If you haven't yet, generate a certificate an identity certificate for your web service that is signed by the CA because CiscoRA can not connect to it if the web server certificate is self-signed.

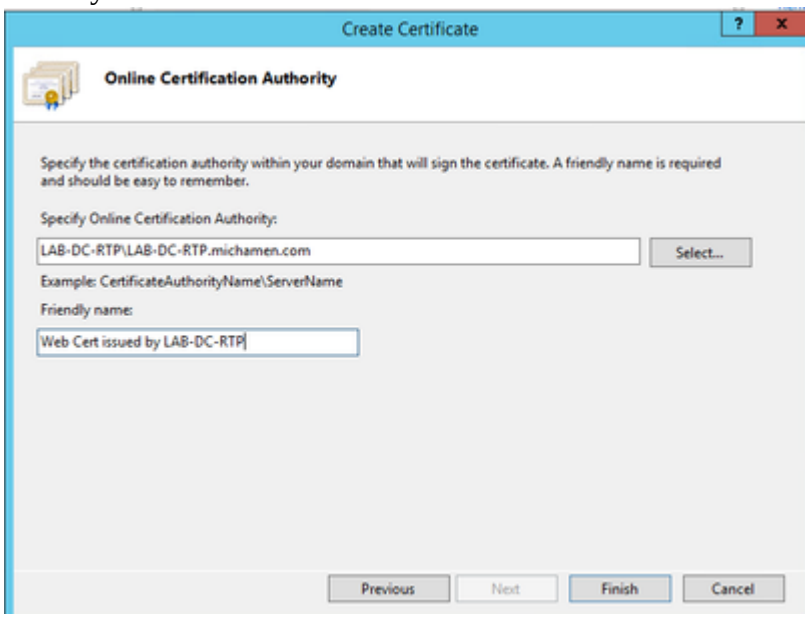
1. Select your web server from the IIS snap-in and double-click **Server Certificates**.



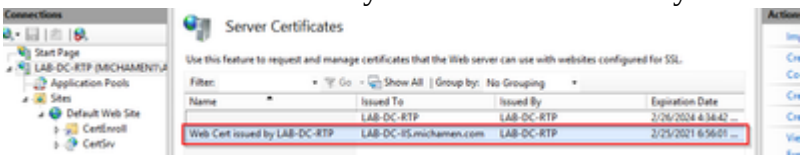
2. By default, one certificate is listed there, which is the self-signed root CA cert. From the **Actions** menu, select **Create Domain Certificate**. Enter the **values** in the configuration wizard to create your new certificate. Ensure the Common name is a resolvable Fully Qualified Domain Name (FQDN)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



3. Select your **root CA's certificate** to be the issuer and select **Finish**.

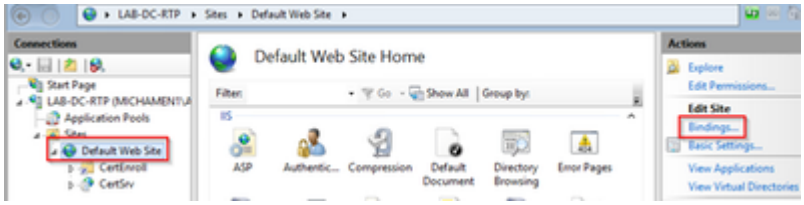


Both the CA certificate and your Web Server Identity certificate are listed.

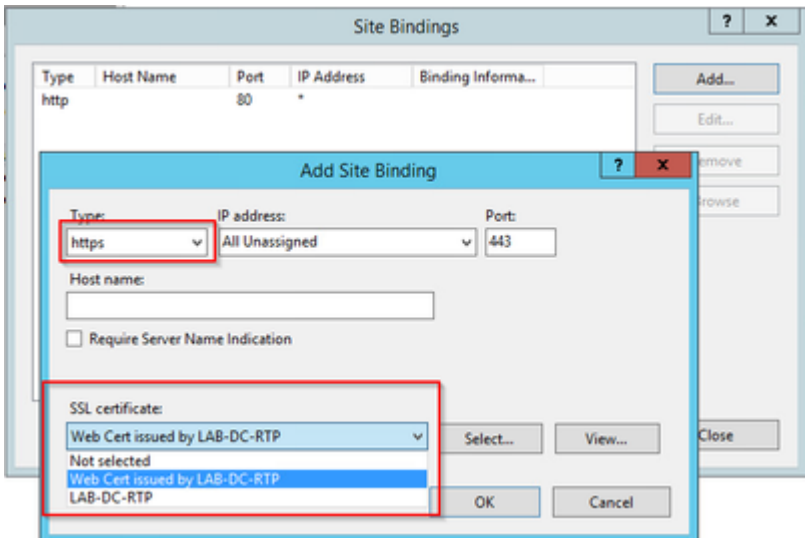


Web Server SSL Binding

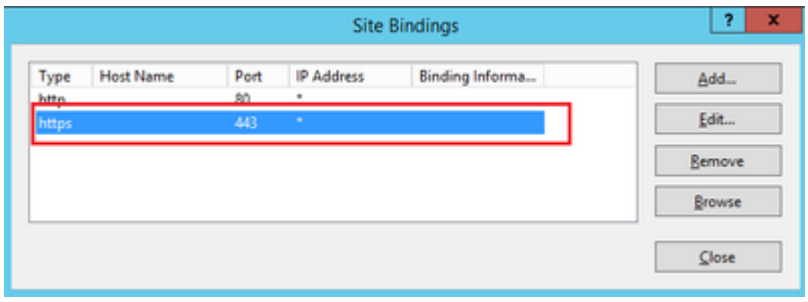
1. Select a site in the tree view (you can use the Default Web Site or make it more granular to specific sites) and select **Bindings** from the **Actions** pane. This brings up the bindings editor that allows you to create, edit, and delete bindings for your web site. Select **Add** to add your new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

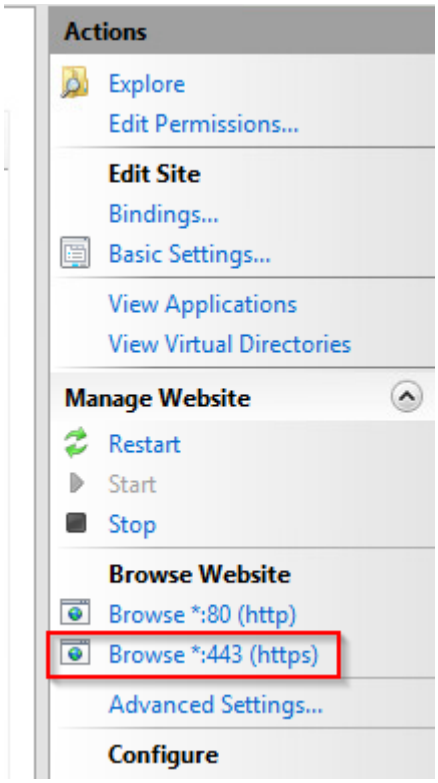


2. The default settings for a new binding are set to HTTP on port 80. For **Type** , select **https**. Select the **self-signed certificate** you created in the previous section from the SSL Certificate drop-down list and then **OK**.



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

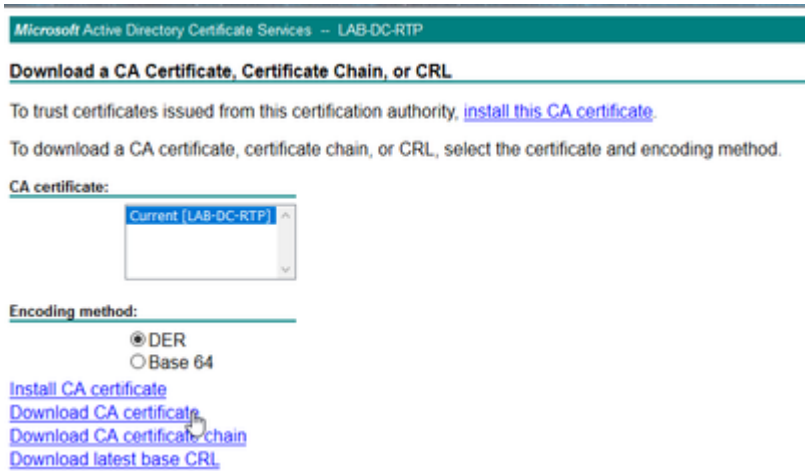




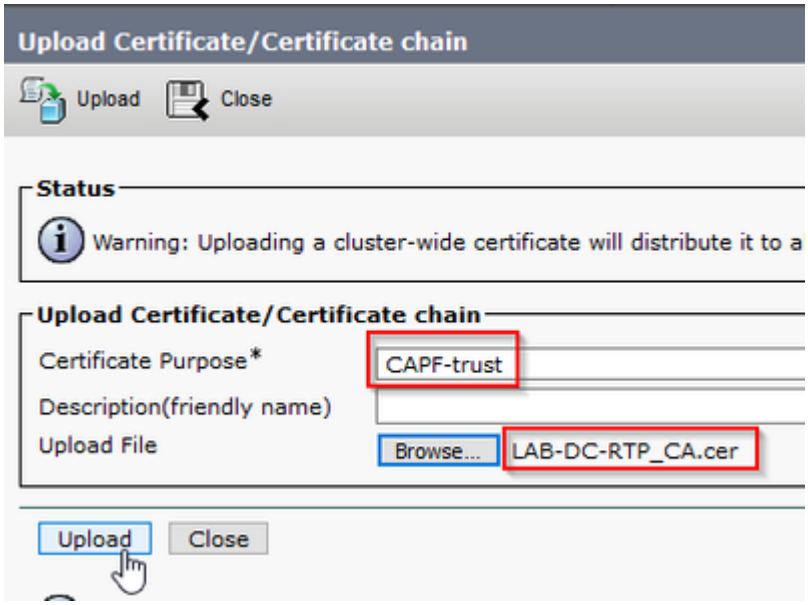
4. Remember to restart the IIS service after configuration changes. Use the **Restart** option from the **Actions** pane.

CUCM Configuration

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

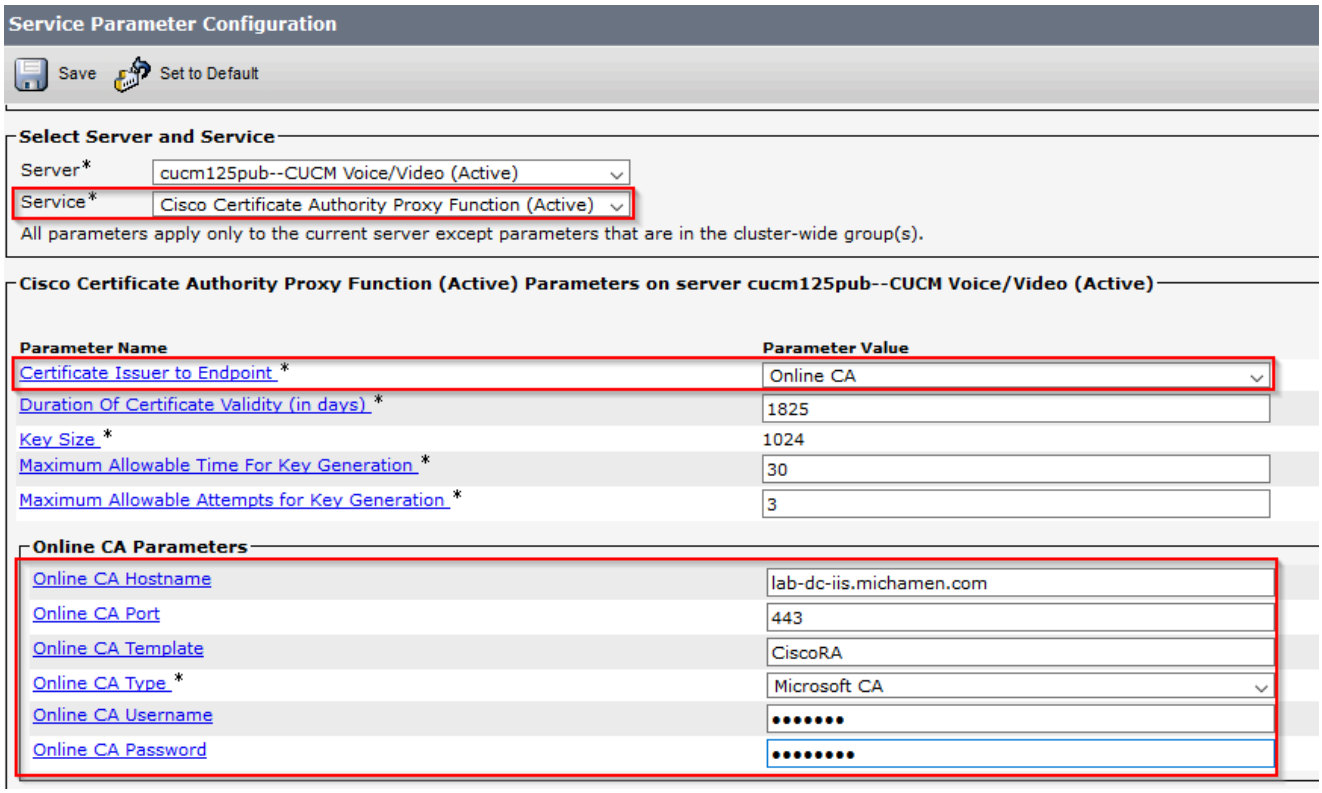


2. Navigate to **Security** > **Certificate Management** from the **OS Administration** page and select the **Upload Certificate/Certificate chain** button to upload the CA certificate with the purpose set to CAPF-trust.

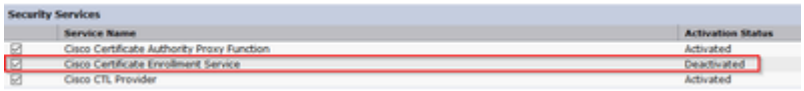


   Upload that same **CA certificate** as CallManager-trust because it is needed if secure signaling encryption is enabled for the endpoints, which is likely if the cluster is in Mixed-Mode.

3. 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**.
4. Set the value of **Certificate Issuer** to **Endpoint to Online CA** and enter the **values** for the **Online CA Parameters** fields. Ensure to use the Web server 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.



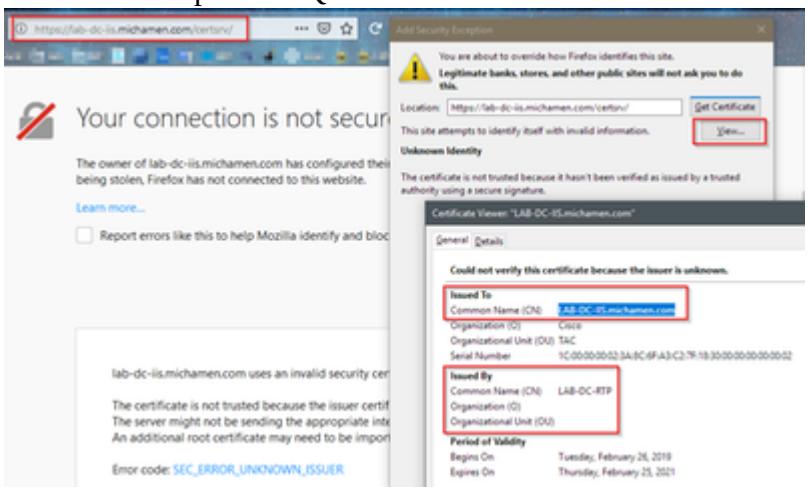
5. A pop-up window informs you that the CAPF service needs to be restarted. First, activate the **Cisco Certificate Enrollment Service** through **Cisco Unified Serviceability** > **Tools** > **Service Activation**, select the **Publisher** in the **server** field, select the **Cisco Certificate Enrollment Service** check box, then select the **Save** button.



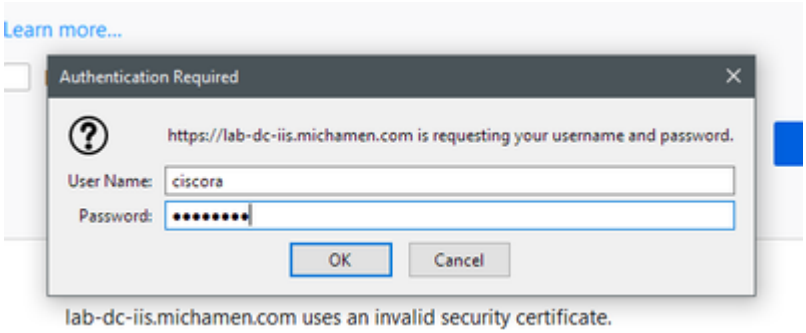
Verify

Verify IIS Certificates

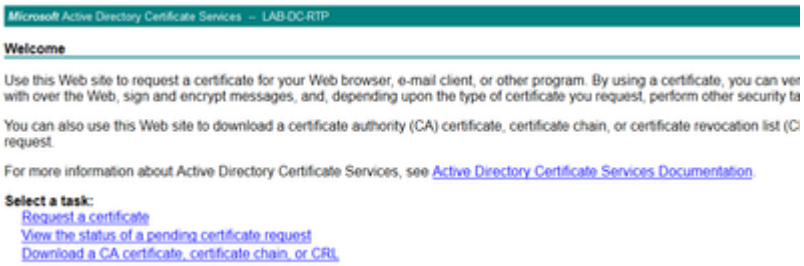
1. From a web browser in a PC with connectivity to the server (preferably in the same network as the CUCM Publisher), navigate to your server FQDN (https://YOUR_SERVER_FQDN/certsrv/).
2. Certificate not-trusted alert is displayed. Add the **exception** and check the **certificate**. Ensure it matches the expected FQDN.



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



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



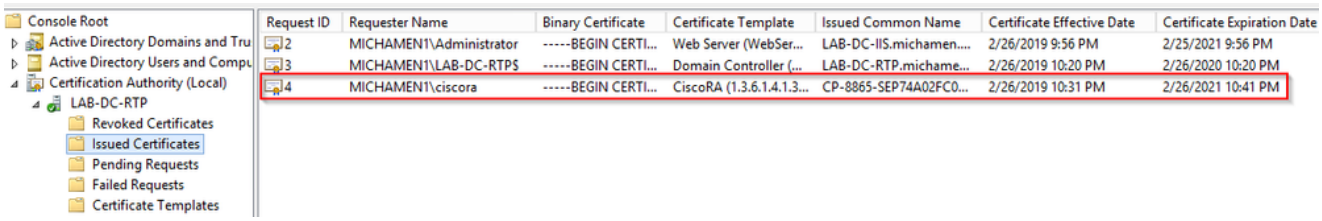
Verify CUCM Configuration

Perform the steps to install an LSC certificate on one of the phones.

1. Open the **CallManager Administration page**, **Device** and then **Phone**.
2. Select the **Find** button to display the phones.
3. Select the **phone** you wish to install the LSC on.
4. Scroll down to **Certification Authority Proxy Function (CAPF)** Information.
5. Select the **Install/Upgrade** from the Certificate Operation.
6. Select the **Authentication Mode**. (By Null String is fine for test purposes.)
7. Scroll to the **top of the page** and select **save** then **Apply Config** for the phone.
8. After the phone restarts and registers back, use the **LSC Status filter** to confirm the LSC installed successfully.

And continue:

1. From the AD server side, open **MMC** and expand the **Certification Authority snap-in** to select the **Issued Certificates** folder.
2. The entry for the phone is displayed Inside the summary view, including these details:
    - 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 phone's model appended by the device name must be displayed.
    - Certificate Effective Date and Certificate Expiration Date



Related Links

- Troubleshooting CAPF Online CA
- Technical Support & Documentation