

Configurazione della registrazione e del rinnovo automatici dei certificati tramite la CA CAPF Online

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Convalida la data e l'ora del server](#)

[Aggiorna nome computer server](#)

[Configurazione](#)

[Servizi AD, utenti e modello di certificato](#)

[Configurazione autenticazione IIS e binding SSL](#)

[Configurazione CUCM](#)

[Verifica](#)

[Verifica certificati IIS](#)

[Verifica configurazione CUCM](#)

[Collegamenti correlati](#)

Introduzione

In questo documento viene descritta la registrazione e il rinnovo automatici dei certificati tramite la funzionalità online CAPF (Certificate Authority Proxy Function) per Cisco Unified Communications Manager (CUCM).

Contributo di Michael Mendoza, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM versione 12.5.1.10000-22

- Windows Server 2012 R2
- IP Phone CP-8865 / Firmware: SIP 12-1-1SR1-4 e 12-5-1SR2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento descrive la configurazione della funzione e le risorse correlate per ulteriori ricerche.

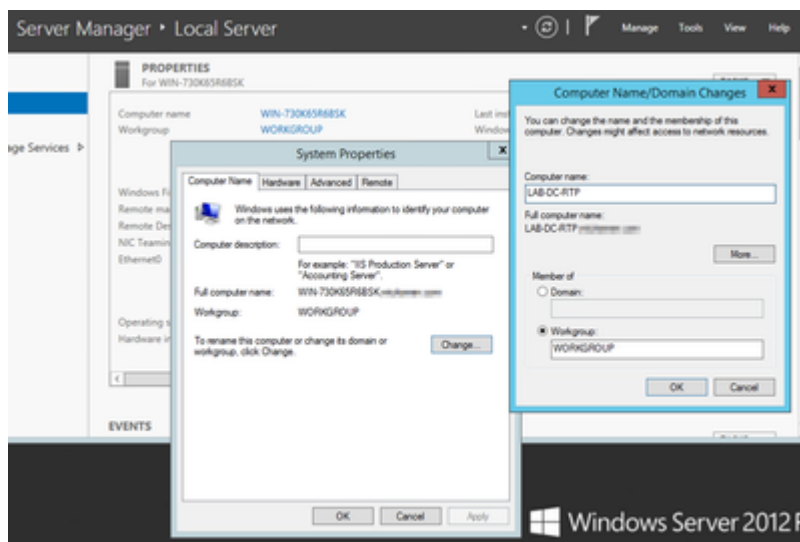
Convalida la data e l'ora del server

Verificare che nel server Windows siano configurati la data, l'ora e il fuso orario corretti in quanto influiscono sui tempi di validità del certificato CA radice (Certification Authority) del server e dei certificati da esso rilasciati.

Aggiorna nome computer server

Per impostazione predefinita, il nome del computer del server è casuale, ad esempio WIN-730K65R6BSK. Prima di abilitare Servizi di dominio Active Directory, è necessario innanzitutto verificare che il nome del computer del server venga aggiornato in base al nome host e al nome autorità emittente della CA radice del server entro la fine dell'installazione. In caso contrario, è necessario eseguire molti passaggi aggiuntivi per modificare questa impostazione dopo l'installazione dei servizi Active Directory.

- Passare a **Server locale**, selezionare il nome del computer per aprire **Proprietà del sistema**
- Selezionare il pulsante **Cambia** e immettere il nuovo nome del computer:



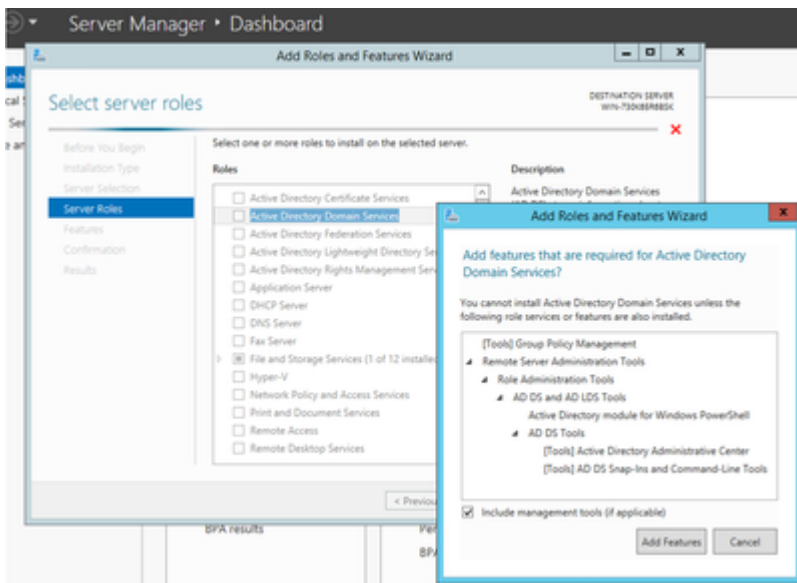
- Riavviare il server per applicare le modifiche

Configurazione

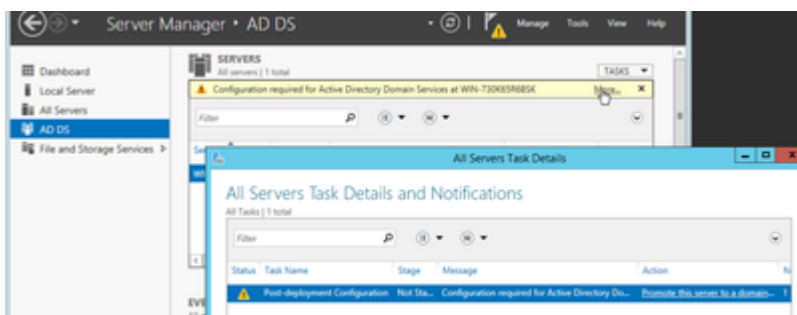
Servizi AD, utente e modello di certificato

Abilitare e configurare i servizi Active Directory

- In Server Manager selezionare l'opzione **Aggiungi ruoli e funzionalità**, selezionare l'**installazione basata su ruoli o su funzionalità** e scegliere il server dal pool (è sufficiente che ne sia presente uno solo nel pool), quindi Servizi di dominio Active Directory:

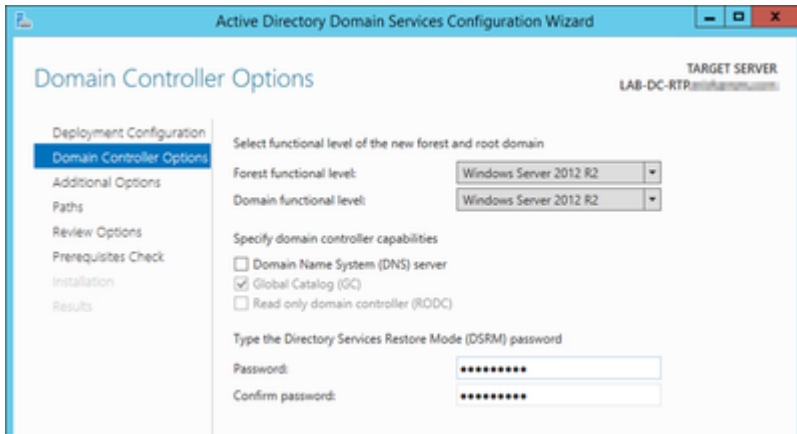


- Continuare a selezionare il pulsante **Next (Avanti)**, quindi **Install (Installa)**
- Selezionare il pulsante **Chiudi** al termine dell'installazione
- In **Server Manager > Servizi di dominio Active Directory** viene visualizzata una scheda di avviso con il titolo Configurazione richiesta per Servizi di dominio Active Directory. Selezionare **altro** collegamento, quindi scegliere un'azione disponibile per avviare l'installazione guidata:

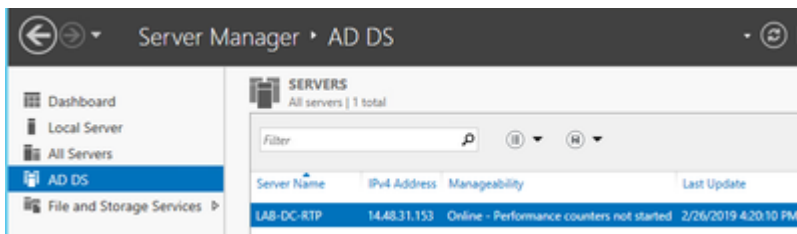


- Seguire le istruzioni della procedura guidata per l'installazione del dominio, aggiungere una nuova foresta con il nome di dominio radice desiderato (utilizzato michamen.com per questa esercitazione) e deselezionare la casella DNS quando disponibile, definire la password DSRM (utilizzata *C1sc0123!* per questa esercitazione):



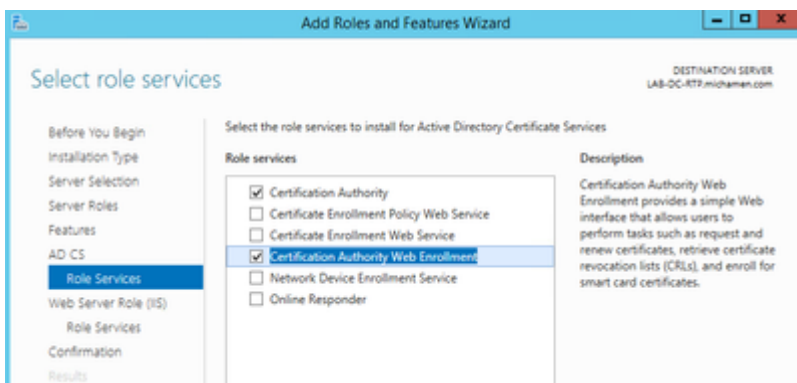


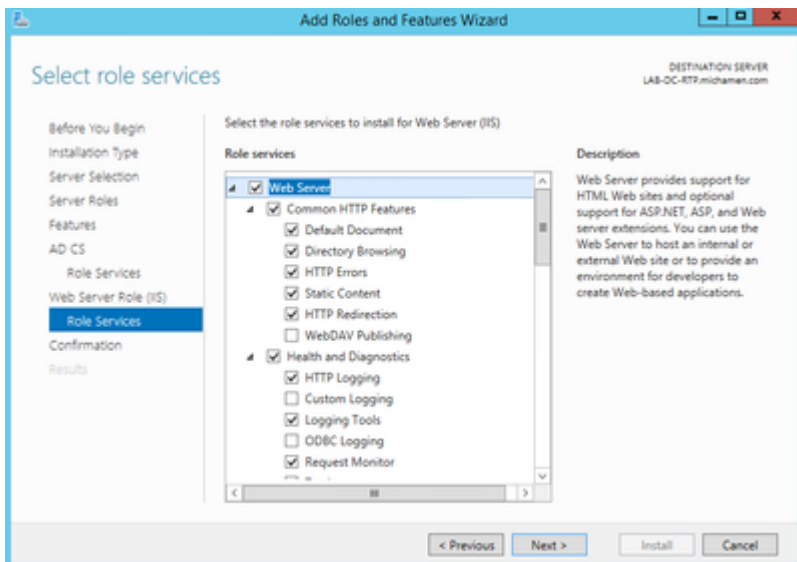
- È necessario specificare un nome di dominio NetBIOS (utilizzato da MICHAMEN1 in questa esercitazione).
- Seguire la procedura guidata fino al completamento. Il server viene quindi riavviato per completare l'installazione.
- Quando è necessario specificare il nuovo nome di dominio al prossimo accesso. Ad esempio MICHAMEN1\Administrator.



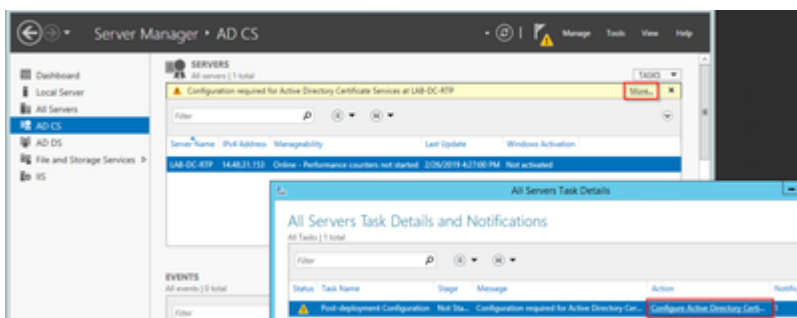
Abilitare e configurare Servizi certificati

- In Server Manager selezionare Aggiungi ruoli e funzionalità
- Selezionare Servizi certificati Active Directory e seguire le istruzioni per aggiungere le funzionalità necessarie (tutte le funzionalità disponibili sono state selezionate dai servizi ruolo abilitati per questa esercitazione)
- Per i servizi ruolo, selezionare Registrazione Web Autorità di certificazione

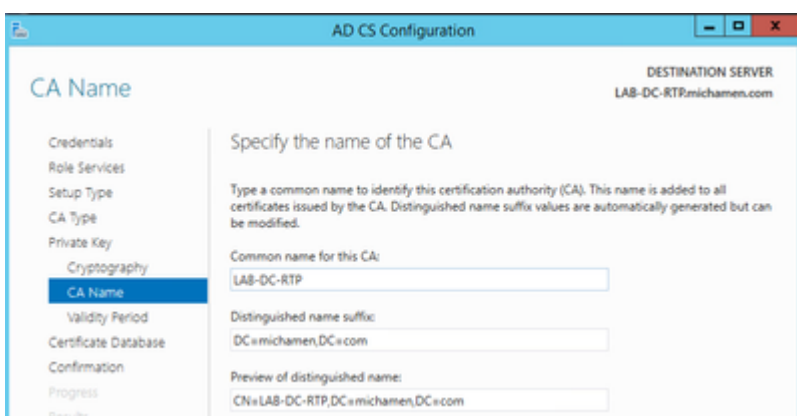




- In **Server Manager** > **Servizi di dominio Active Directory** deve essere visualizzata una scheda di avviso con il titolo **Configurazione richiesta per Servizi certificati Active Directory**. Selezionare il collegamento **altro** e quindi l'azione disponibile:



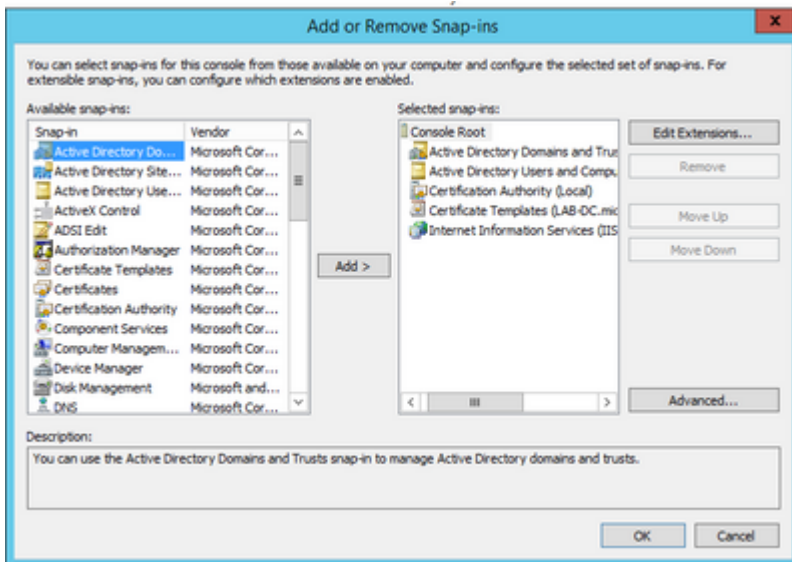
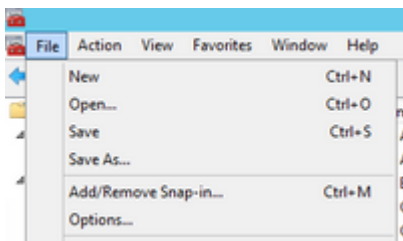
- Nella Configurazione guidata post-installazione di AD-CS passare ai passaggi seguenti:
- Selezionare i **ruoli di registrazione Web Autorità di certificazione e Autorità di certificazione**
- Scegliere CA Enterprise con le opzioni seguenti:
- CA radice
- Crea una nuova chiave privata
- Usa chiave privata - SHA1 con impostazioni predefinite
- Impostare un nome comune per la CA (deve corrispondere al nome host del server):



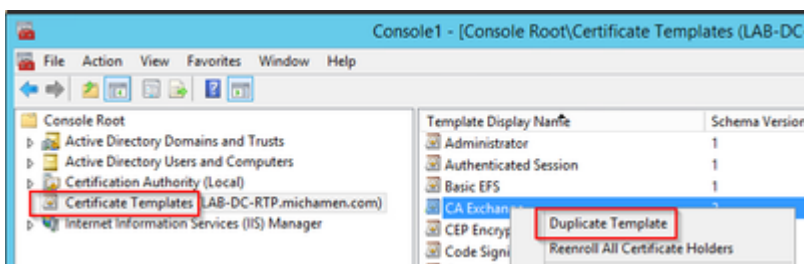
- Impostare la validità per 5 anni (o più, se desiderato)
- Selezionare il pulsante **Avanti** nel resto della procedura guidata

Creazione di modelli di certificato per CiscoRA

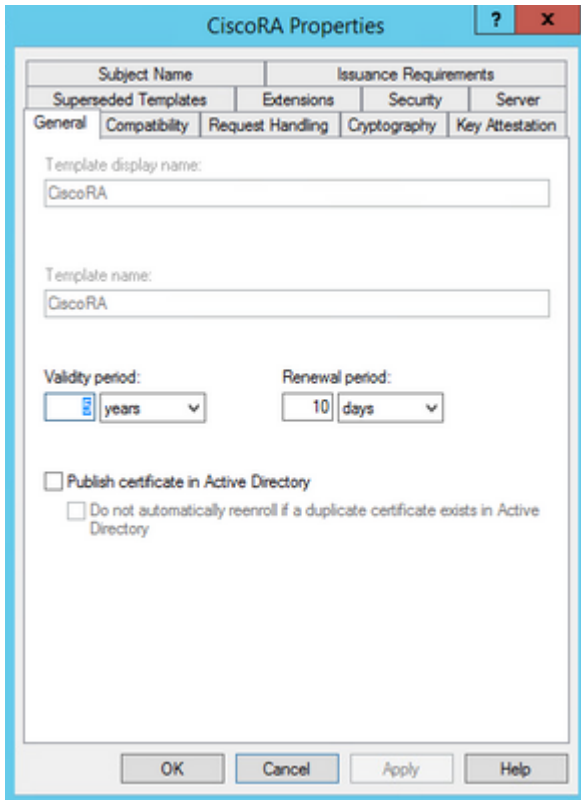
- Aprire MMC. Selezionare il logo di avvio di Windows e digitare *mmc* da Esegui
- Aprire una finestra di MMC e aggiungere i seguenti snap-in (utilizzati in punti diversi della configurazione), quindi selezionare **OK**:



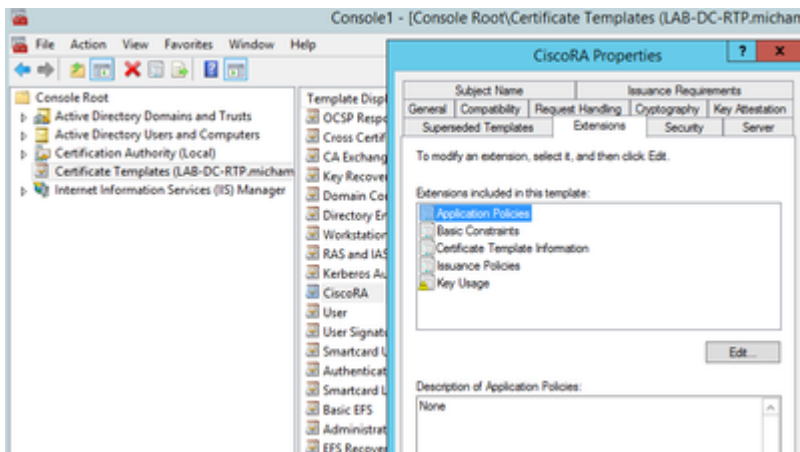
- Selezionare **File > Salva** e salvare la sessione della console sul desktop per un rapido riaccesso
- Dagli snap-in, selezionare **Modelli di certificato**
- Creare o clonare un modello (preferibilmente il modello "*Root Certification Authority*", se disponibile) e denominarlo CiscoRA



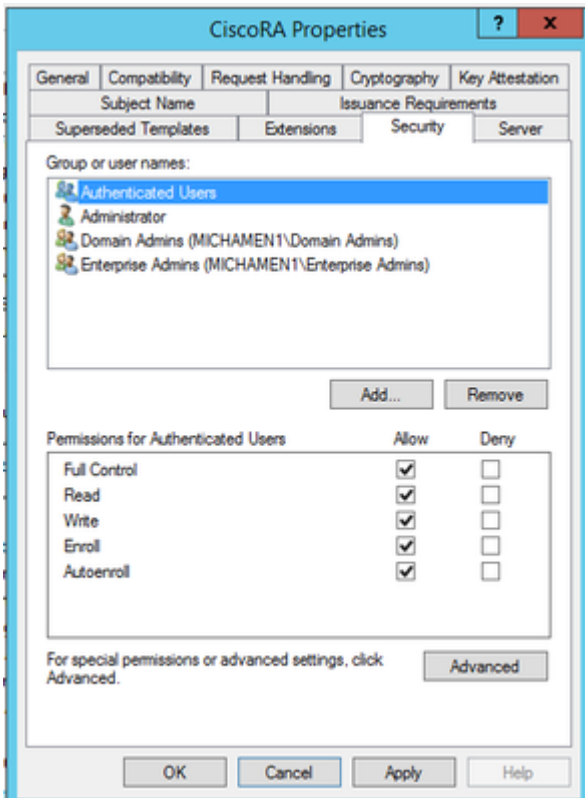
- Modificare il modello. Fare clic con il pulsante destro del mouse e selezionare **Proprietà**
- Selezionare la scheda **Generale** e impostare il periodo di validità su 20 anni (o su un altro valore se desiderato). In questa scheda, assicurarsi che i valori di "nome visualizzato" e "nome" del modello corrispondano



- Selezionare la scheda **Estensioni**, evidenziare **Criteri di applicazione** e quindi selezionare **Modifica**

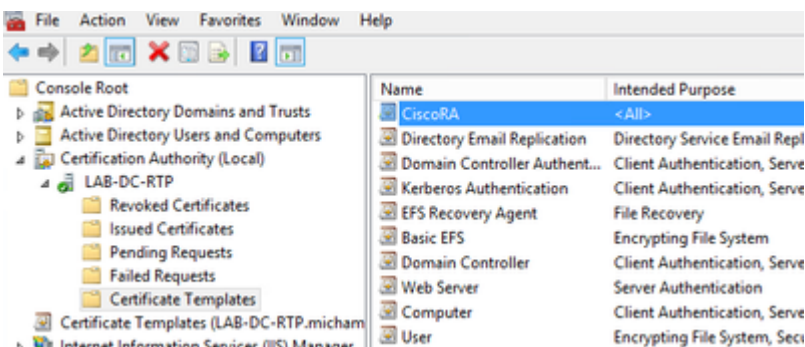


- Rimuovere tutti i criteri visualizzati nella finestra visualizzata
- Selezionare la scheda **Nome soggetto** e selezionare il pulsante di opzione **Fornitura in richiesta**
- Selezionare la scheda **Protezione** e concedere tutte le autorizzazioni per tutti i gruppi/nomi utente visualizzati



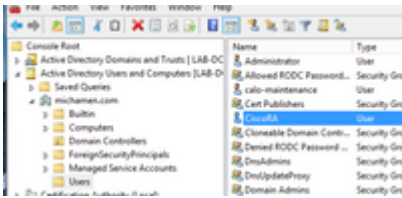
Rendere il modello di certificato disponibile per il rilascio

- Negli snap-in di MMC selezionare **Autorità di certificazione** ed espandere la struttura di cartelle per individuare la cartella **Modelli di certificato**
- Fare clic con il pulsante destro del mouse nello spazio vuoto della cornice contenente Nome e Scopo designato
- Selezionare **Nuovo** e **Modello di certificato da rilasciare**
- Selezionare il modello CiscoRA appena creato e modificato



Creazione account CiscoRA Active Directory

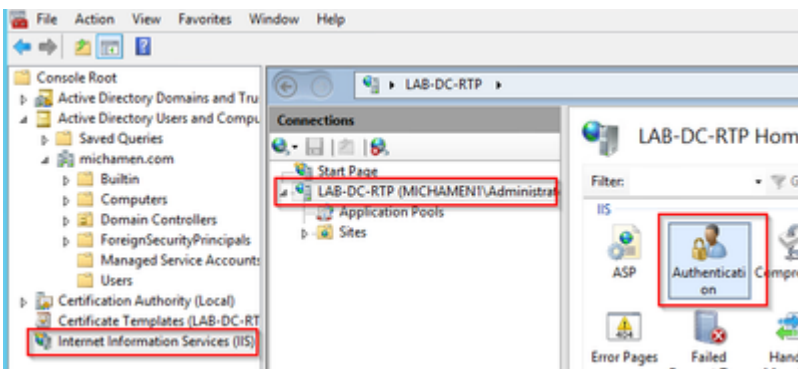
- Passare agli snap-in di MMC e selezionare **Utenti e computer di Active Directory**
- Selezionare la cartella **Users** nella struttura nel riquadro all'estrema sinistra
- Fare clic con il pulsante destro del mouse nello spazio vuoto della cornice contenente Nome, Tipo e Descrizione
- Seleziona **nuovo** e **utente**
- Creare l'account CiscoRA con nome utente/password (*ciscora/Cisco123* è stato utilizzato per questa esercitazione) e selezionare la casella di controllo **Nessuna scadenza password** quando viene visualizzata



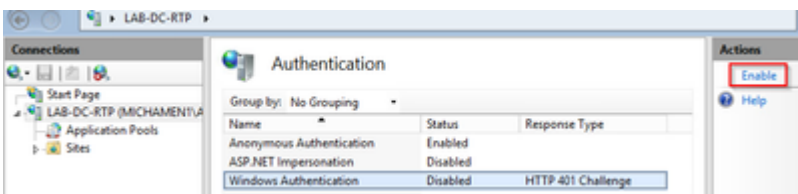
IIS Configurazione autenticazione e binding SSL

Abilita NTLM Autenticazione

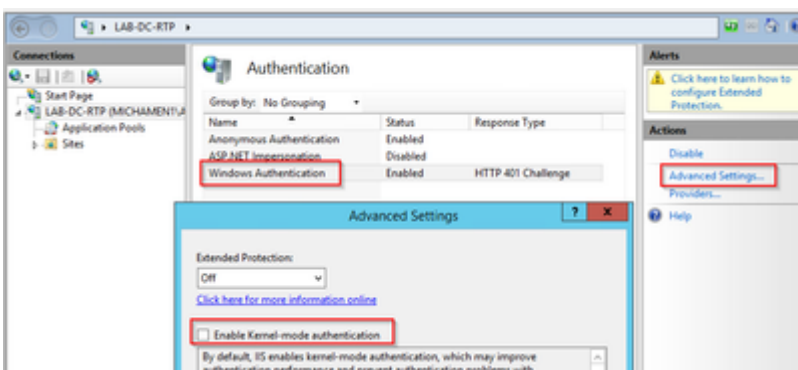
- Passare agli snap-in di MMC e selezionare il nome del server nello snap-in Gestione Internet Information Services (IIS)
- L'elenco delle funzioni viene visualizzato nel fotogramma successivo. Fare doppio clic sull'icona della funzione di **autenticazione**



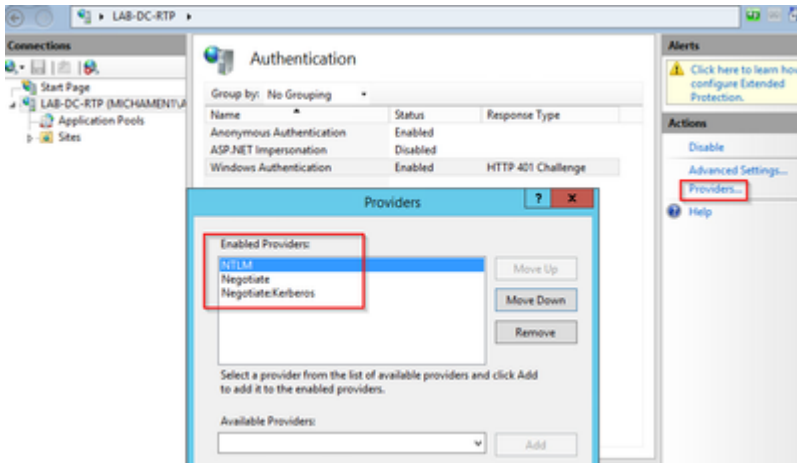
- Evidenziare **Autenticazione di Windows** e nel riquadro Azioni (riquadro di destra) selezionare l'opzione **Abilita**



- Nel riquadro Azioni viene visualizzata l'opzione **Impostazioni avanzate**; selezionarla e deselezionare **Abilita autenticazione in modalità kernel**



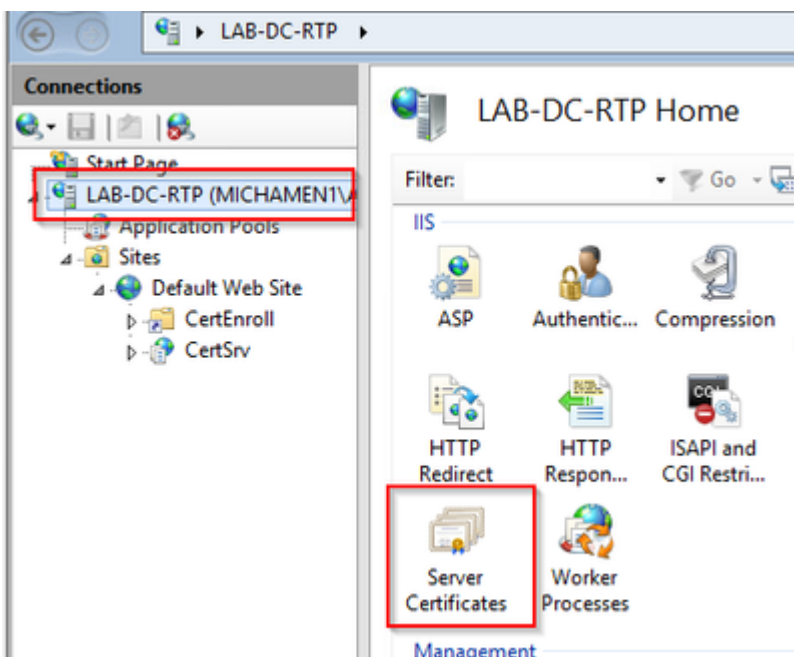
- Selezionare **Provider** e mettere in ordine NTML quindi **Negozia**.



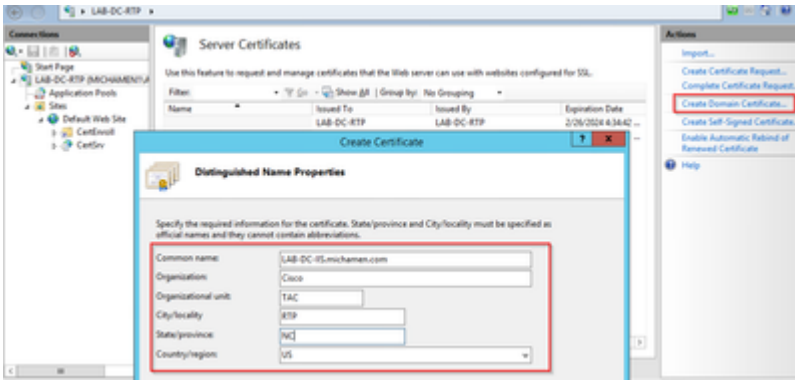
Genera il certificato di identità per il server Web

In caso contrario, è necessario generare un certificato di identità per il servizio Web firmato dalla CA perché CiscoRA non è in grado di connettersi a tale servizio se il certificato del server Web è autofirmato:

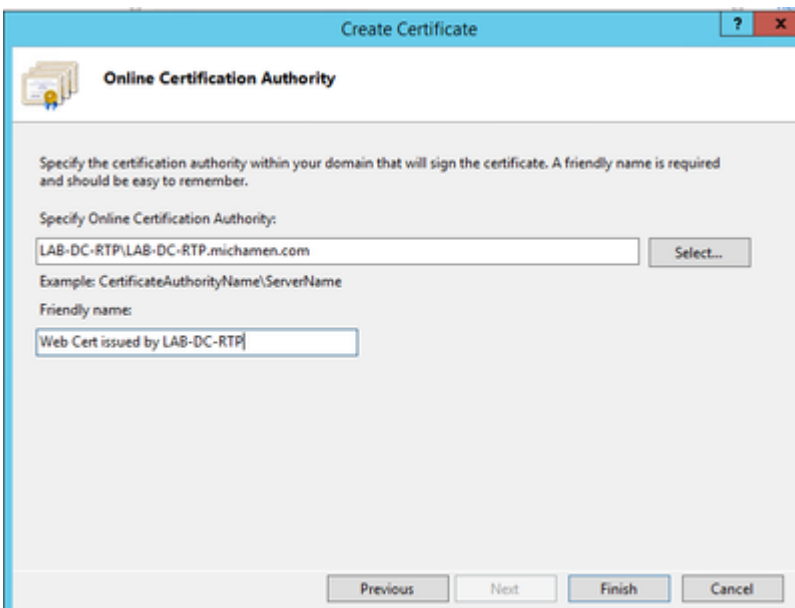
- Selezionare il server Web dallo **snap-in IIS** e fare doppio clic sull'icona della funzionalità **Certificati server**:



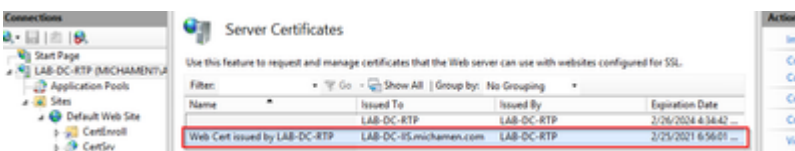
- Per impostazione predefinita, nell'elenco è presente un certificato, ovvero il certificato CA radice autofirmato. Dal menu **Azioni** selezionare l'opzione **Crea certificato di dominio**. Immettere i valori nella configurazione guidata per creare il nuovo certificato. Verificare che il nome comune sia un nome di dominio completo risolvibile, quindi selezionare **Avanti**:



- Selezionare il certificato della CA radice come autorità di certificazione e scegliere **Fine**:

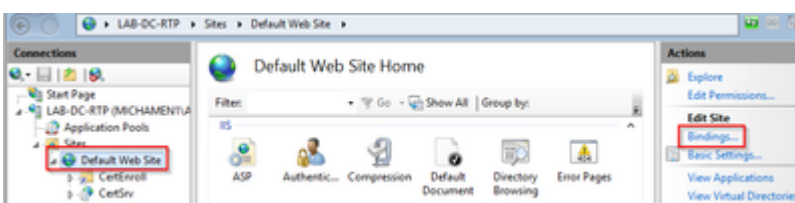


- È possibile visualizzare sia il certificato CA che il certificato di identità del server Web:

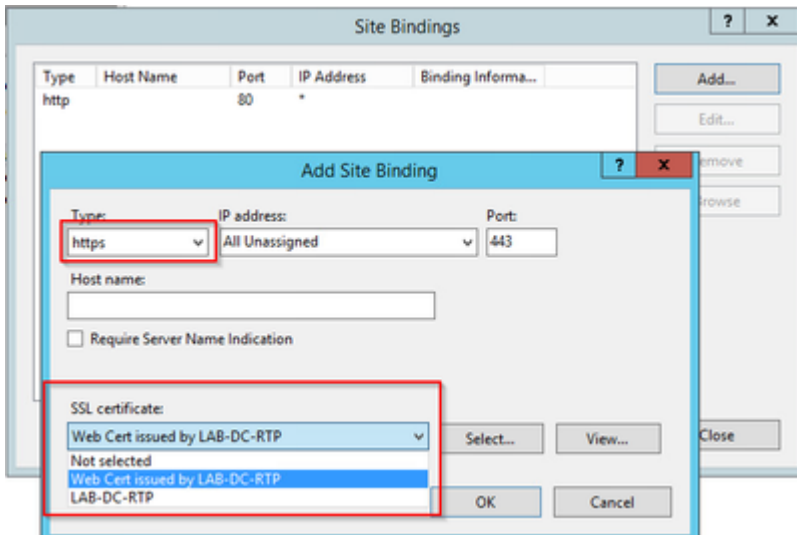


Associazione SSL server Web

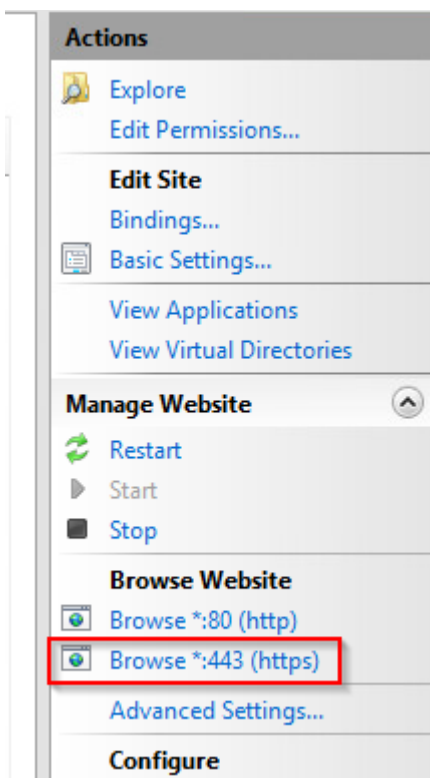
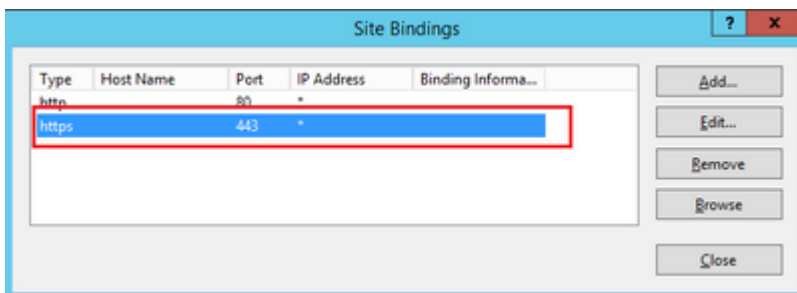
- Selezionare un sito nella visualizzazione struttura (è possibile utilizzare il sito Web predefinito o renderlo più granulare per siti specifici) e selezionare **Associazioni** dal riquadro Azioni. Verrà visualizzato l'editor delle associazioni che consente di creare, modificare ed eliminare associazioni per il sito Web. Per aggiungere il nuovo binding SSL al sito, selezionare **Add** (Aggiungi).



- Le impostazioni predefinite per una nuova associazione sono impostate su HTTP sulla porta 80. Selezionare **https** dall'elenco a discesa **Type**. Selezionare il certificato autofirmato creato nella sezione precedente dall'elenco a discesa **Certificato SSL** e quindi scegliere **OK**.



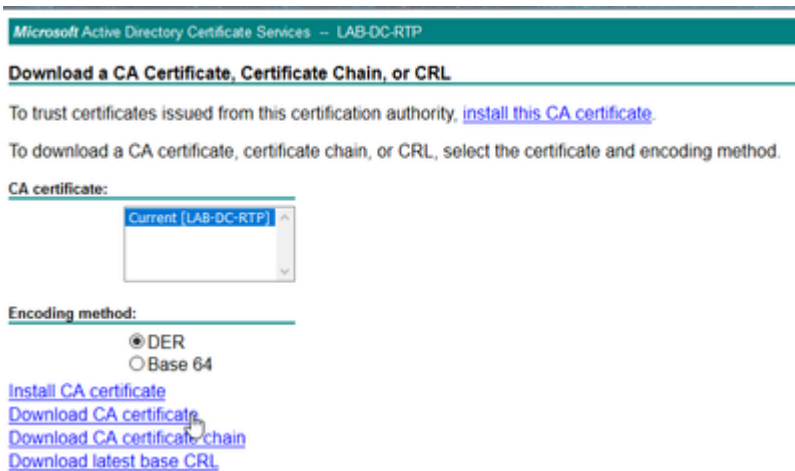
- Ora si dispone di un nuovo binding SSL nel sito e tutto ciò che rimane è verificare che funzioni selezionando l'opzione **Sfogliare *:443 (https)** dal menu e assicurarsi che la pagina Web IIS predefinita utilizzi HTTPS:



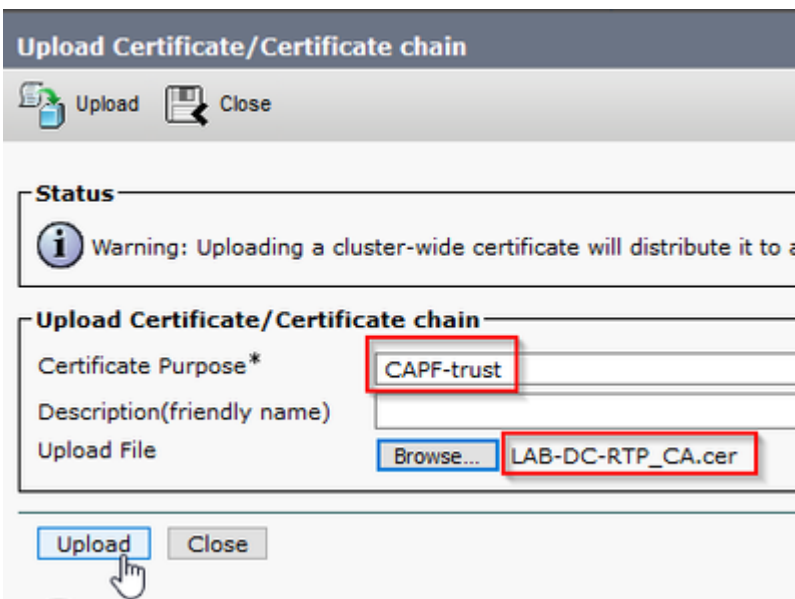
- Ricordarsi di riavviare il servizio IIS dopo le modifiche alla configurazione. Utilizzare l'opzione **Restart** (Riavvia) nel riquadro Azioni.

Configurazione CUCM

- Accedere alla pagina Web di Servizi certificati Active Directory (https://YOUR_SERVER_FQDN/certsrv/) e scaricare il certificato CA



- Passare a **Sicurezza > Gestione certificati** dalla pagina Amministrazione del sistema operativo e selezionare il pulsante **Carica catena certificati/certificati** per caricare il certificato CA con lo *scopo* impostato su *CAPF-trust*.



... A questo punto, è consigliabile caricare lo stesso certificato CA di *CallManager-trust* perché è necessario se la crittografia di segnalazione sicura è abilitata (o verrà abilitata) per gli endpoint, il che è probabile se il cluster è in modalità mista.

- Passare a **Sistema > Parametri servizio**. Selezionare il server Unified CM Publisher nel campo server e **Cisco Certificate Authority Proxy Function** nel campo Servizio.
- Impostare il valore di Autorità di certificazione su Endpoint nella CA in linea e immettere i valori nei campi Parametri CA in linea. Assicurarsi di utilizzare l'FQDN del server Web, il nome del modello di certificato creato in precedenza (CiscoRA), il tipo di CA come Microsoft CA e utilizzare le credenziali dell'account utente CiscoRA creato in precedenza

Service Parameter Configuration

 Save  Set to Default

Select Server and Service

Server*
 Service*

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 (Active)

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	••••••••

- Una finestra pop indica che è necessario riavviare il servizio CAPF. Innanzitutto, attivare il servizio di registrazione certificati Cisco tramite **Cisco Unified Serviceability > Strumenti > Attivazione servizio**, selezionare l'entità di pubblicazione nel campo Server e selezionare la casella di controllo Servizio di registrazione certificati Cisco, quindi selezionare il pulsante **Salva**:

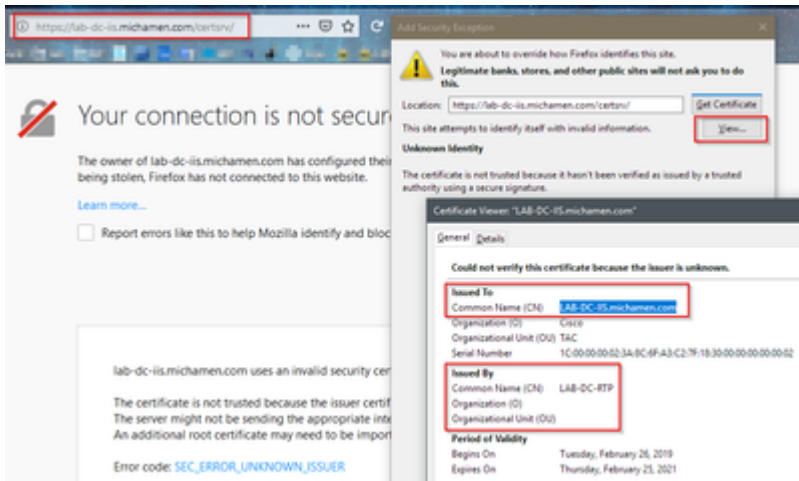
Service Name	Activation Status
<input checked="" type="checkbox"/> Cisco Certificate Authority Proxy Function	Activated
<input checked="" type="checkbox"/> Cisco Certificate Enrollment Service	Deactivated
<input checked="" type="checkbox"/> Cisco CTL Provider	Activated

Verifica

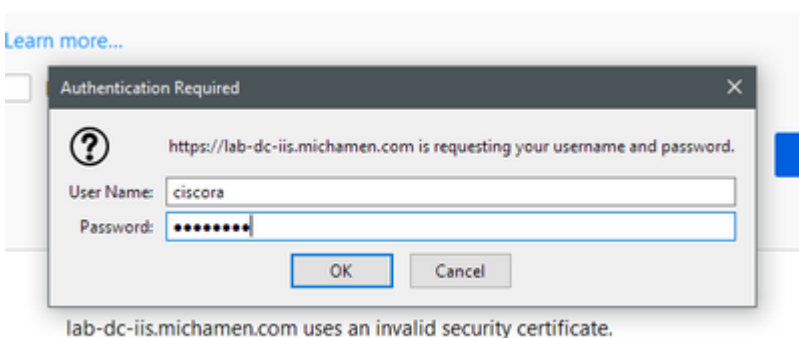
Verifica certificati IIS

- Da un browser Web in un PC con connettività al server (preferibilmente nella stessa rete dell'editore CUCM) passare a URL:

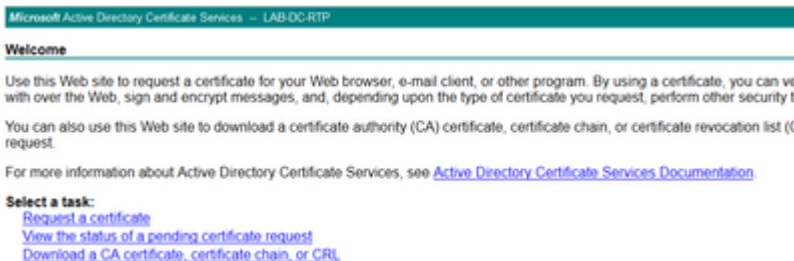
https://YOUR_SERVER_FQDN/certsrv/
- Viene visualizzato l'avviso di certificato non attendibile. Aggiungere l'eccezione e controllare il certificato. Verificare che corrisponda all'FQDN previsto:



- Dopo aver accettato l'eccezione, è necessario eseguire l'autenticazione. A questo punto è necessario utilizzare in precedenza le credenziali configurate per l'account CiscoRA:



- Dopo l'autenticazione è necessario essere in grado di visualizzare la pagina iniziale di Servizi certificati Active Directory:



Verifica configurazione CUCM

Eeguire la procedura normalmente descritta per installare un certificato LSC su uno dei telefoni.

Passaggio 1. Aprire la pagina Amministrazione di CallManager, Periferica e quindi Telefono

Passaggio 2. Selezionare il pulsante **Trova** per visualizzare i telefoni

Passaggio 3. Selezionare il telefono su cui installare LSC

Passaggio 4. Scorri verso il basso fino alle informazioni sulla funzione proxy dell'autorità di certificazione (CAPF)

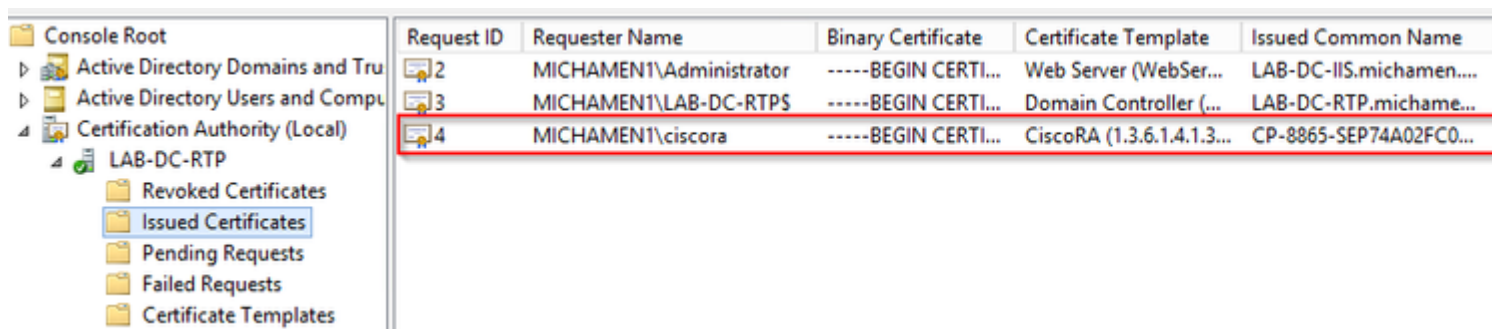
Passaggio 5. Selezionare Installa/Aggiorna da Operazione certificato.

Passaggio 6. Selezionare la modalità di autenticazione. (By Null String è adatto ai fini del test)

Passaggio 7. Scorrere fino alla parte superiore della pagina e selezionare **save** (salva), quindi **Apply Config** (Applica configurazione) per il telefono.

Passaggio 8. Una volta riavviato il telefono e registrato di nuovo, usare il filtro Stato LSC per confermare che LSC è stato installato correttamente.

- Dal lato del server AD aprire MMC ed espandere lo snap-in Autorità di certificazione per selezionare la cartella Certificati rilasciati
- La voce relativa al telefono è visualizzata Nella visualizzazione di riepilogo, sono riportati alcuni dettagli:
 - ID richiesta: numero di sequenza univoco
 - Nome richiedente: è necessario visualizzare il nome utente dell'account CiscoRA configurato
 - Modello di certificato: è necessario visualizzare il nome del modello CiscoRA creato
 - Issued Common Name: è necessario visualizzare il modello del telefono aggiunto dal nome del dispositivo
 - Data di validità e data di scadenza del certificato



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-RTPS	-----BEGIN CERTI...	Domain Controller (...	LAB-DC-RTP.michame...
4	MICHAMEN1\ciscora	-----BEGIN CERTI...	CiscoRA (1.3.6.1.4.1.3...	CP-8865-SEP74A02FC0...

Collegamenti correlati

- [Risoluzione dei problemi relativi a CAPF Online CA](#)
- [Documentazione e supporto tecnico â€“ Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).