Configurar o Registro e a Renovação Automáticos de Certificados por meio da CA Online da CAPF

Contents

Introdução

Este documento descreve a inscrição e a renovação automáticas de certificados por meio do recurso on-line Certificate Authority Proxy Function (CAPF) para o Cisco Unified Communications Manager (CUCM).

Contribuição de Michael Mendoza, engenheiro do Cisco TAC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager
- Certificados X.509
- Servidor Windows
- Windows Ative Diretory (AD)
- Serviços de Informações da Internet (IIS) do Windows
- Autenticação NT (New Technology) LAN Manager (NTLM)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CUCM versão 12.5.1.10000-22
- Windows Server 2012 R2
- Telefone IP CP-8865 / Firmware: SIP 12-1-1SR1-4 e 12-5-1SR2.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento aborda a configuração do recurso e os recursos relacionados para pesquisa adicional.

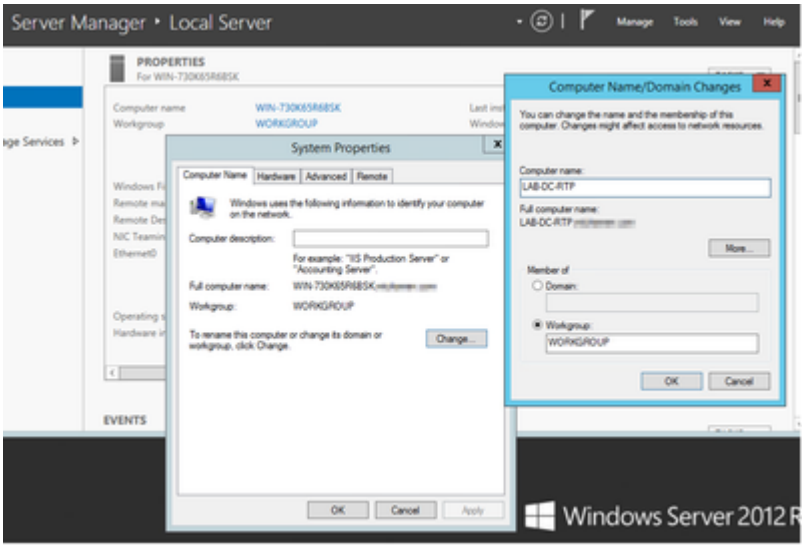
Validar a hora e a data do servidor

Verifique se o servidor Windows tem a data, a hora e o fuso horário corretos configurados, pois isso afeta os tempos de validade do certificado raiz de CA (Autoridade Certificadora) do servidor, bem como os certificados emitidos por ele.

Atualizar Nome do Computador do servidor

Por padrão, o nome do computador do servidor tem um nome aleatório, como WIN-730K65R6BSK. A primeira coisa a fazer antes de habilitar os Serviços de Domínio do AD é garantir a atualização do nome do computador do servidor para o nome de host e o nome do emissor da CA raiz do servidor até o final da instalação; caso contrário, serão necessárias várias etapas adicionais para alterar isso após a instalação dos serviços do AD.

- Navegue até **Servidor local**, selecione o nome do computador para abrir **Propriedades do sistema**
- Selecione o botão **Change** e digite o novo nome do computador:



- Reinicie o servidor para que as alterações sejam aplicadas

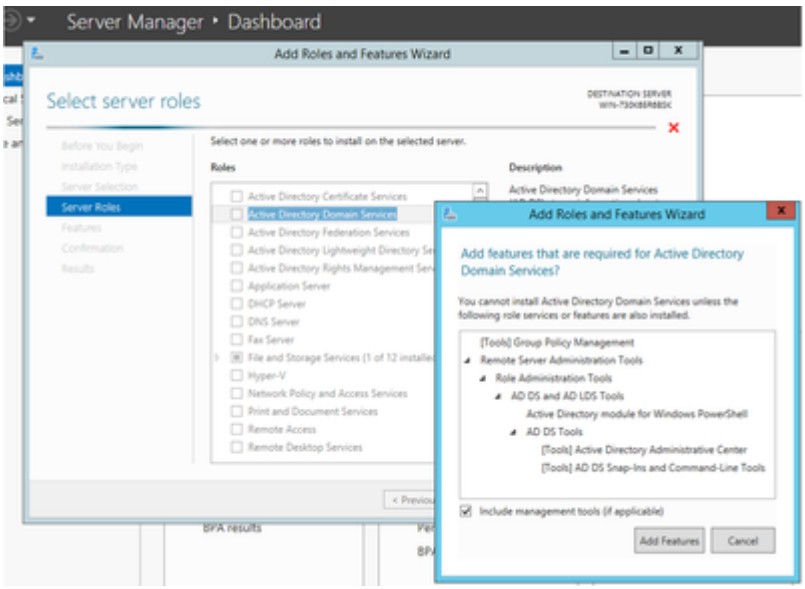
Configurar

Serviços do AD, Usuário e Modelo de Certificado

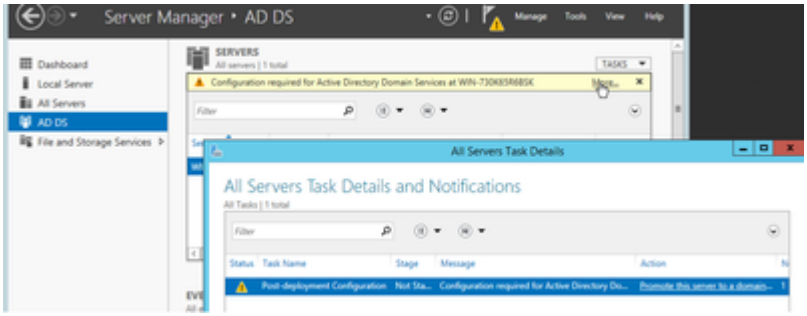
Habilitar e Configurar Serviços do Ative Diretory

- No Gerenciador do Servidor, selecione a opção **Adicionar Funções e Recursos**, selecione a **instalação baseada em funções ou recursos** e escolha o servidor no pool (deve haver apenas um no

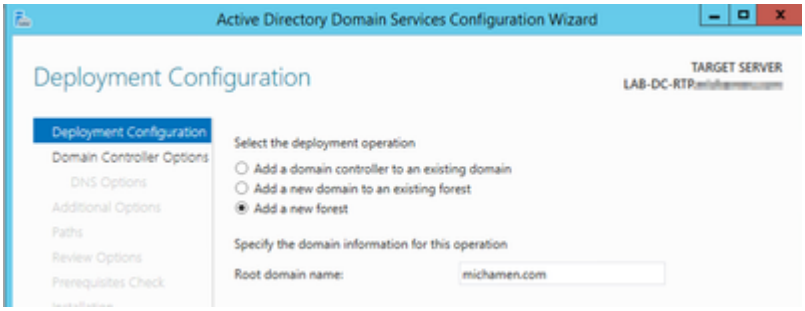
pool) e, em seguida, os Serviços de Domínio Ative Diretory:

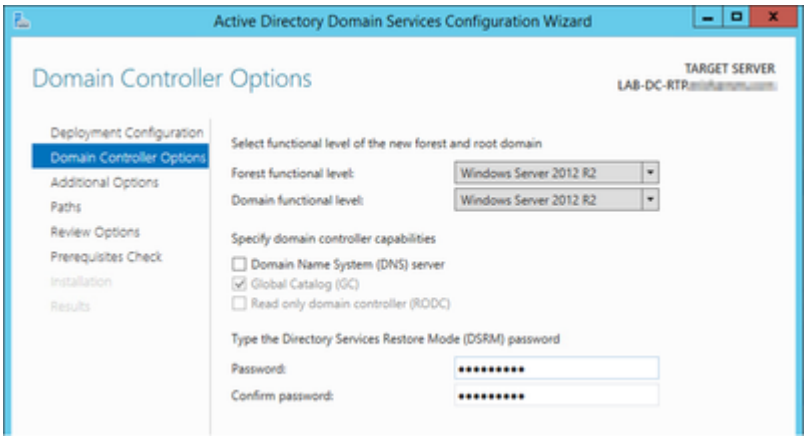


- Continue selecionando o botão **Avançar** e **Instalar**
- Selecione o botão **Close** após concluir a instalação
- Uma guia de aviso aparece em **Gerenciador de Servidores** > **AD DS** com o título Configuração necessária para Serviços de Domínio Ative Diretory; Selecione **mais** link e depois a ação disponível para iniciar o assistente de configuração:

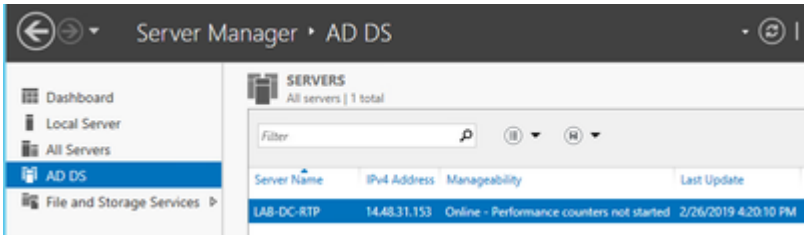


- Siga os prompts no assistente de configuração de domínio, adicione uma nova Floresta com o Nome de Domínio Raiz desejado (usado michamen.com para este laboratório) e desmarque a caixa DNS quando disponível, defina a senha DSRM (usada C1sc0123! para este laboratório):



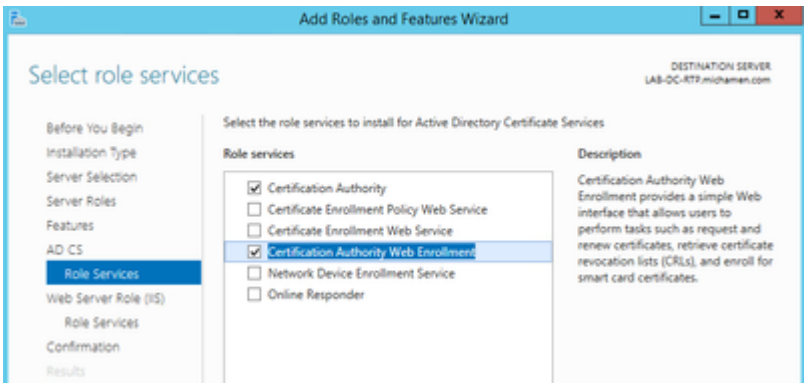


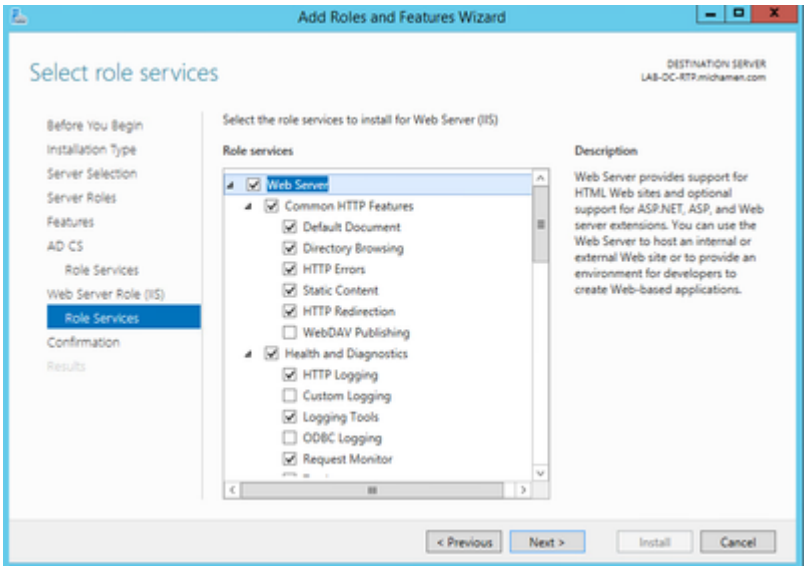
- É necessário especificar um nome de domínio NetBIOS (MICHAMEN1 usado neste laboratório).
- Siga o assistente até a conclusão. Em seguida, o servidor é reinicializado para concluir a instalação.
- Em seguida, será necessário especificar o novo nome de domínio na próxima vez que você fizer logon. Por exemplo, MICHAMEN1\Administrator.



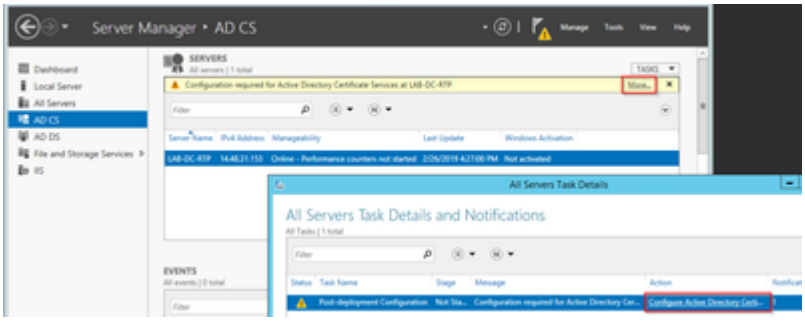
Habilitar e Configurar Serviços de Certificado

- No Gerenciador de Servidores, selecione Adicionar Funções e Recursos
- Selecione Serviços de Certificados do Ative Diretory e siga os avisos para adicionar os recursos necessários (todos os recursos disponíveis foram selecionados nos serviços de função que foram habilitados para este laboratório)
- Para Serviços de Função, verifique o Registro na Web da Autoridade de Certificação

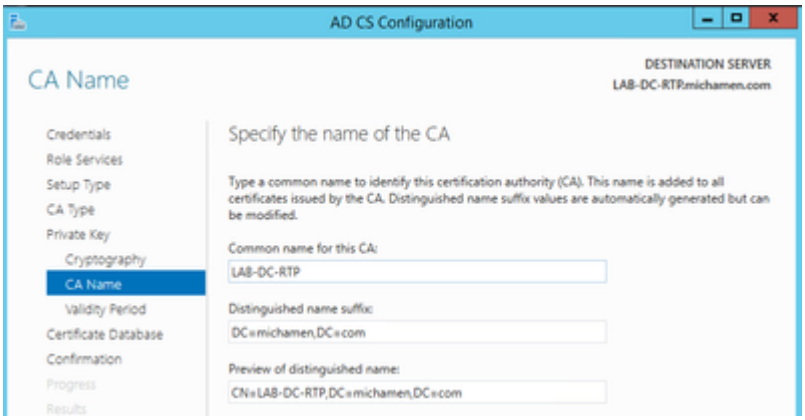




- Uma guia de aviso deve aparecer em **Gerenciador de servidores >AD DS** com o título Configuração necessária para Serviços de Certificados do Ative Diretory; Selecione o link **mais** e a ação disponível:



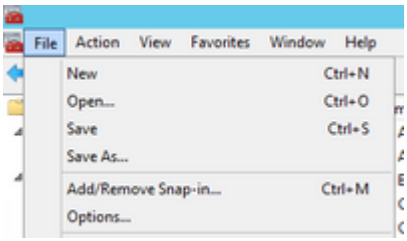
- No assistente de configuração pós-instalação do AD-CS, siga estas etapas:
- Selecione as Funções de **Inscrição na Web de Autoridade de Certificação** e **Autoridade de Certificação**
- Escolha CA Corporativa com opções:
- CA raiz
- Criar uma nova chave privada
- Usar chave privada - SHA1 com configurações padrão
- Defina um nome comum para a autoridade de certificação (deve corresponder ao nome de host do servidor):

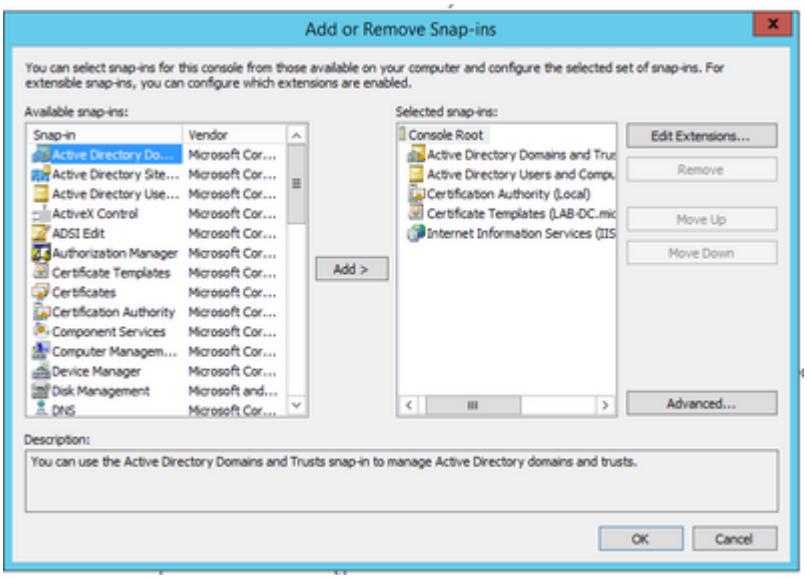


- Defina a validade por 5 anos (ou mais, se desejar)
- Selecione o botão **Avançar** no restante do assistente

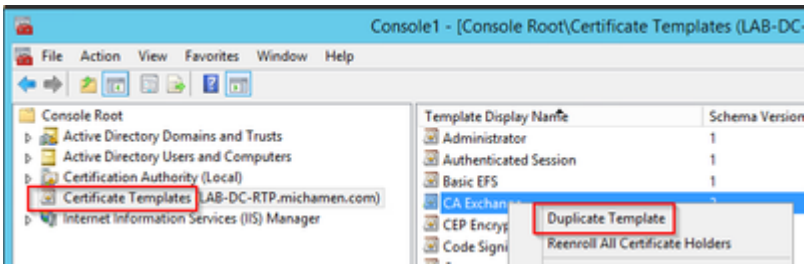
Criação de Modelo de Certificado para CiscoRA

- Abra o MMC. Selecione o logotipo de inicialização do Windows e digite *mmc* em Executar
- Abra uma janela do MMC e adicione os seguintes snap-ins (usados em diferentes pontos da configuração) e selecione **OK**:

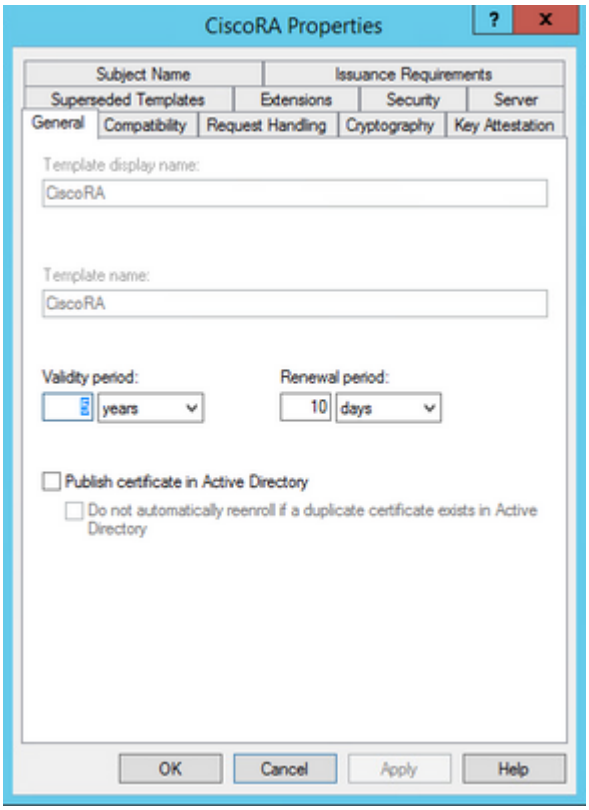




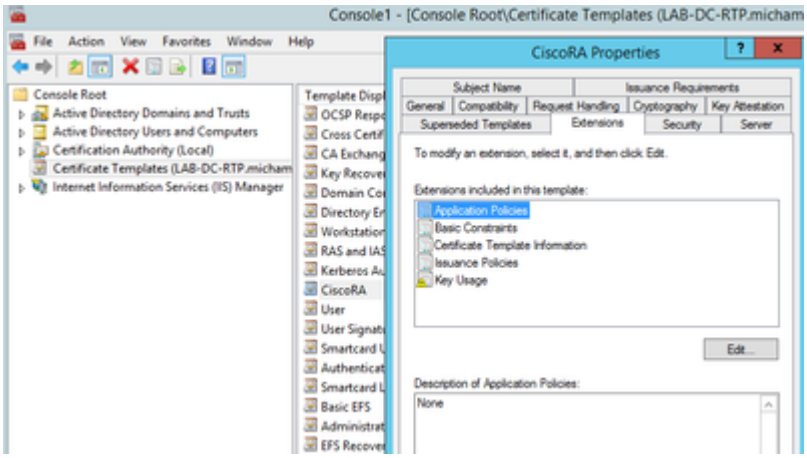
- Selecione **File > Save** e salve esta sessão de console na área de trabalho para ter acesso rápido novamente
- Nos snap-ins, selecione **Modelos de certificado**
- Crie ou clone um modelo (preferencialmente o modelo "*Autoridade de certificação raiz*", se disponível) e nomeie-o como CiscoRA



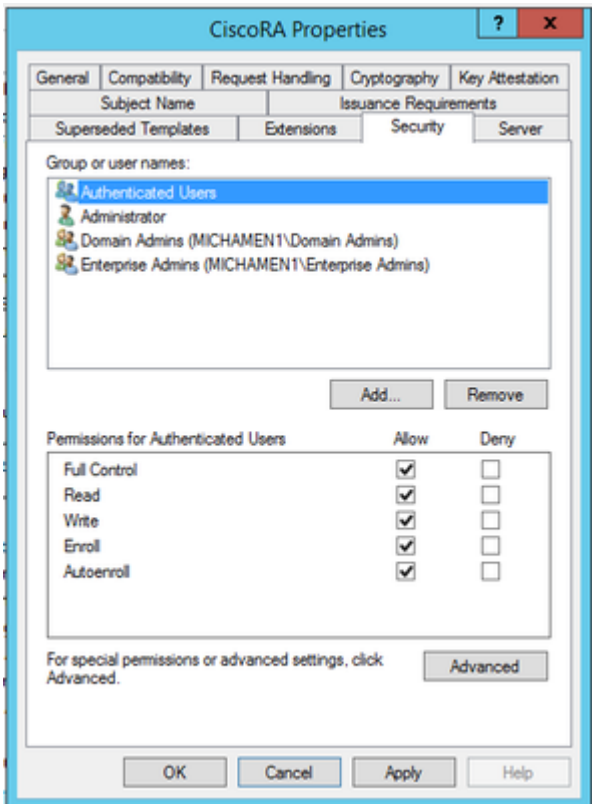
- Modifique o modelo. Clique com o botão direito do mouse nele e selecione **Propriedades**
- Selecione a guia **Geral** e defina o período de validade como 20 anos (ou outro valor, se desejar). Nesta guia, certifique-se de que os valores "nome para exibição" e "nome" do modelo correspondam



- Selecione a guia **Extensions**, realce **Application Policies** e selecione **Edit**

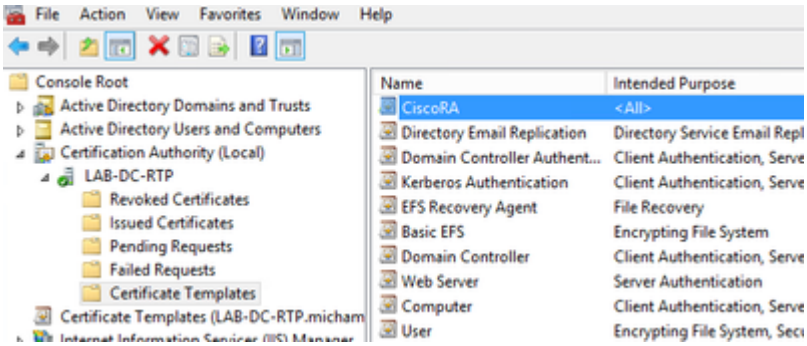


- Remova todas as políticas exibidas na janela exibida
- Selecione a guia **Nome do Assunto** e selecione o botão de opção **Suprimento na Solicitação**
- Selecione a guia **Segurança** e conceda todas as permissões para todos os grupos/nomes de usuário mostrados



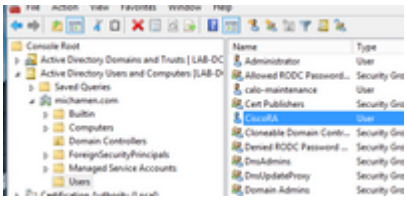
Disponibilizar o Modelo de Certificado para Emissão

- Nos snap-ins do MMC, selecione **Autoridade de certificação** e expanda a árvore de pastas para localizar a pasta **Modelos de certificado**
- Clique com o botão direito do mouse no espaço em branco no quadro que contém Nome e Finalidade
- Selecione **Novo** e **Modelo de certificado a ser emitido**
- Selecione o modelo do CiscoRA recém-criado e editado



Criação de Conta CiscoRA do Ative Diretory

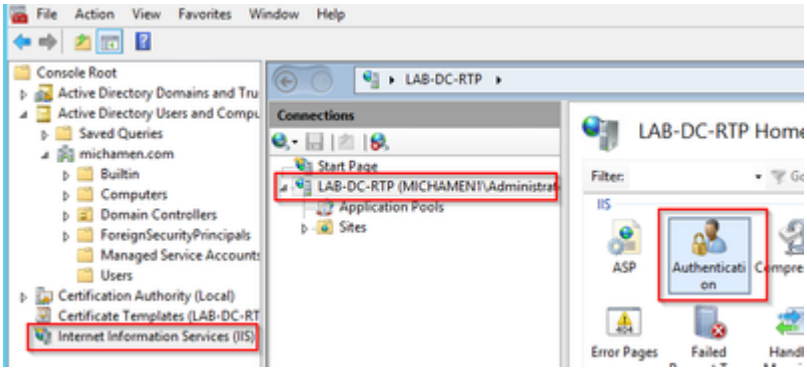
- Navegue até os snap-ins do MMC e selecione **Usuários e computadores do Ative Diretory**
- Selecione a pasta **Users** na árvore no painel mais à esquerda
- Clique com o botão direito do mouse no espaço em branco no quadro que contém Nome, Tipo e Descrição
- Selecione **Novo** e **Usuário**
- Crie a conta CiscoRA com nome de usuário/senha (*ciscora/Cisco123* foi usado para este laboratório)e marque a caixa de seleção **A senha nunca expira** quando for exibida



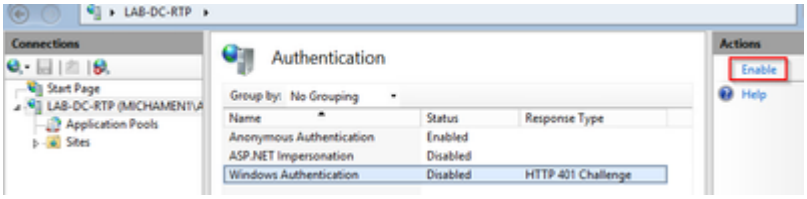
IIS Configuração de Autenticação e Associação SSL

Enable NTLM Autenticação

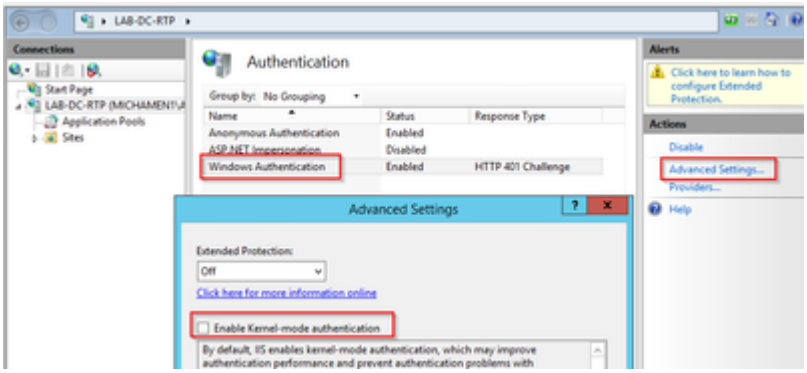
- Navegue até os snap-ins do MMC e, no snap-in Gerenciador dos Serviços de Informações da Internet (IIS), selecione o nome do seu servidor
- A lista de recursos é exibida no próximo quadro. Clique duas vezes no ícone do recurso **Autenticação**



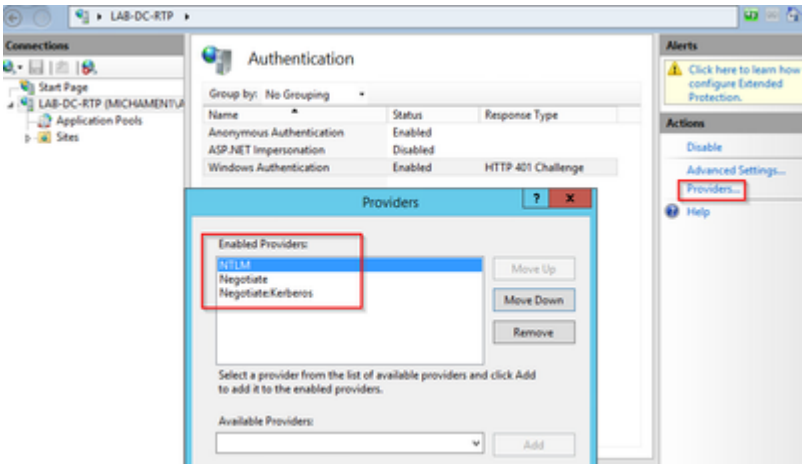
- Realce **Autenticação do Windows** e, no quadro Ações (painel direito), selecione a opção **Habilitar**



- O painel Ações exibe a opção **Configurações avançadas**; marque-a e desmarque **Ativar autenticação no modo kernel**



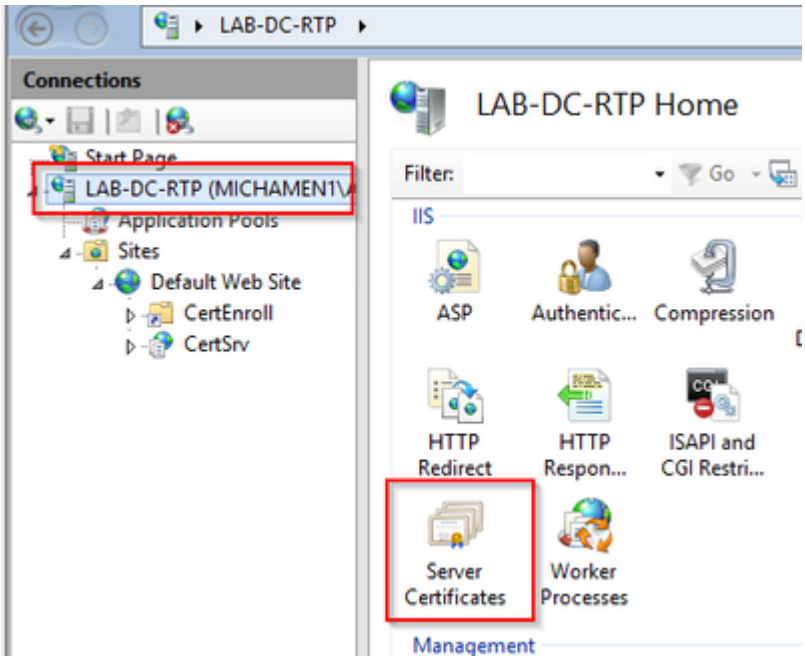
- Selecione **Provedores** e coloque na ordem **NTML** e **Negocie.**



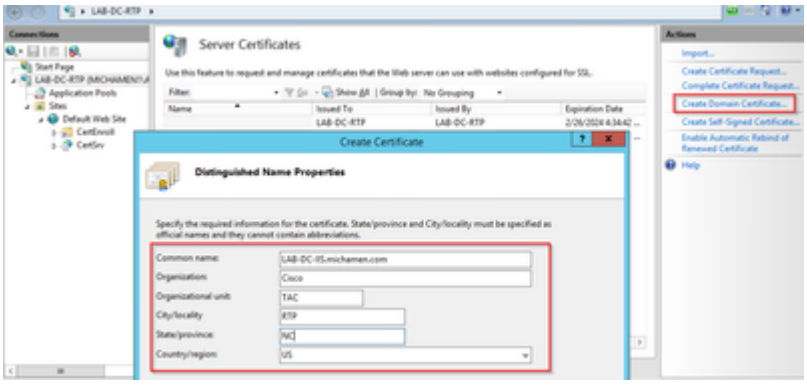
Gerar o Certificado de Identidade para o Servidor Web

Se ainda não for o caso, você precisará gerar um certificado de identidade para o serviço Web que seja assinado pela CA porque o CiscoRA não poderá se conectar a ele se o certificado do servidor Web for AutoAssinado:

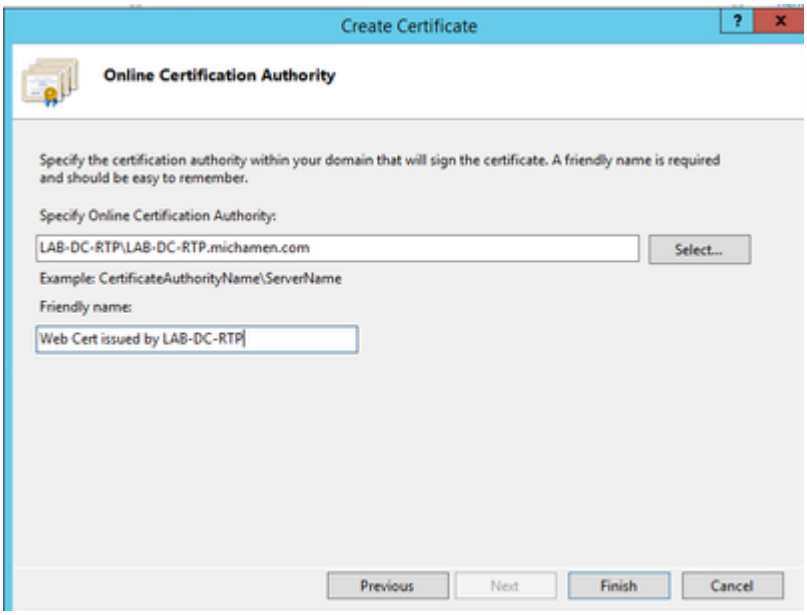
- Selecione o servidor Web no **snap-in IIS** e clique duas vezes no ícone do recurso **Certificados do Servidor**:



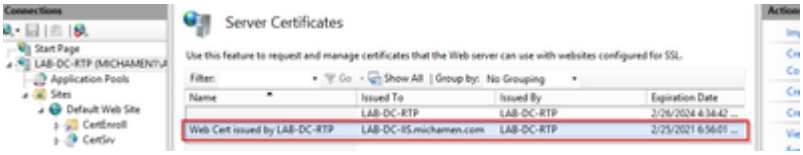
- Por padrão, você pode ver um certificado listado ali; que é o certificado CA raiz autoassinado; no menu **Ações** selecione a opção **Criar certificado de domínio**. Insira os valores no assistente de configuração para criar seu novo certificado. Verifique se o Nome comum é um FQDN (Nome de domínio totalmente qualificado) que pode ser resolvido e selecione **Avançar**:



- Selecione o certificado da CA raiz para ser o emissor e selecione **Concluir**:

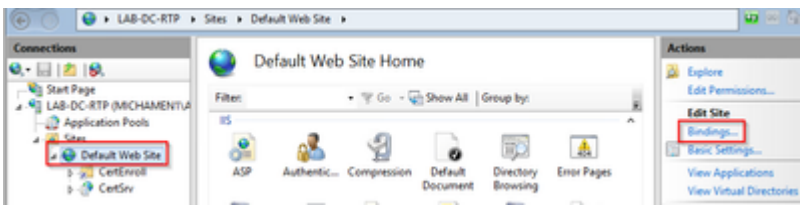


- Você pode ver ambos, o certificado CA e o certificado de identidade do servidor Web listados:

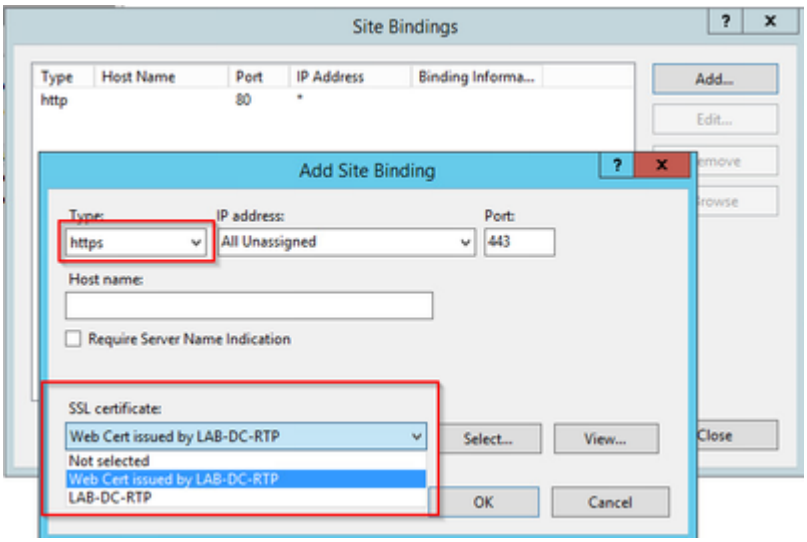


Associação SSL do Servidor Web

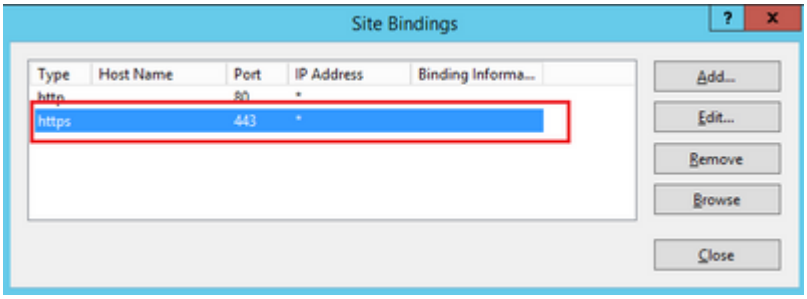
- Selecione um site na exibição de árvore (você pode usar o site padrão ou torná-lo mais granular para sites específicos) e selecione **Vinculações** no painel Ações. Isso exibe o editor de associações que permite criar, editar e excluir associações para o site. Selecione **Add** para adicionar sua nova associação SSL ao site.

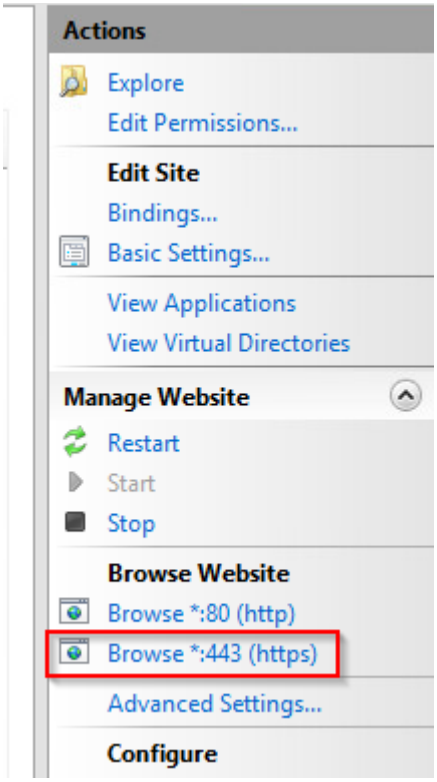


- As configurações padrão para uma nova associação são definidas como HTTP na porta 80. Selecione **https** na lista suspensa **Tipo**. Selecione o certificado autoassinado criado na seção anterior na lista suspensa **Certificado SSL** e selecione **OK**.



- Agora você tem uma nova associação SSL em seu site e tudo o que resta é verificar se ela funciona selecionando a opção **Browse *:443 (https)** no menu e garantir que a página da Web padrão do IIS use HTTPS:

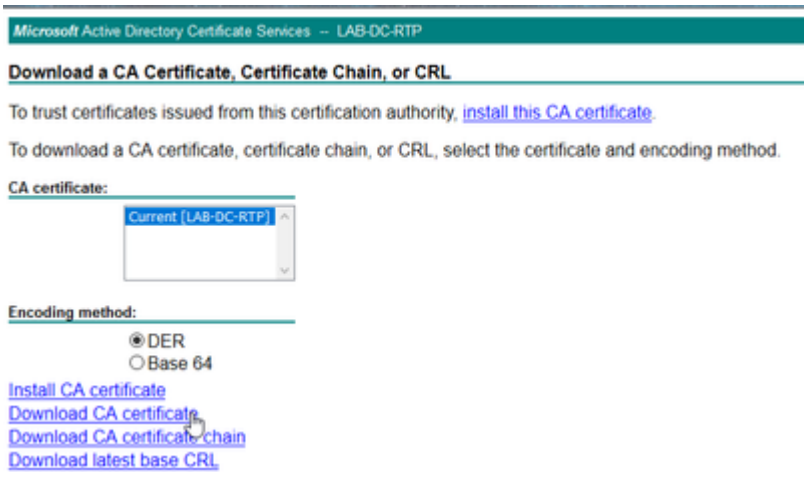




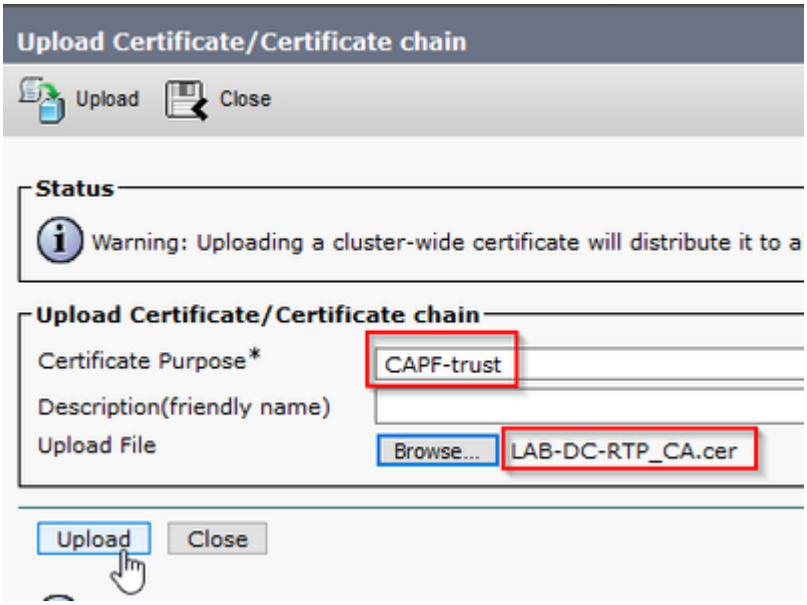
- Lembre-se de reiniciar o serviço IIS após as alterações de configuração. Use a opção **Reiniciar** no painel Ações.

Configuração do CUCM

- Navegue até a página da Web do AD CS (https://YOUR_SERVER_FQDN/certsrv/) e baixe o certificado CA

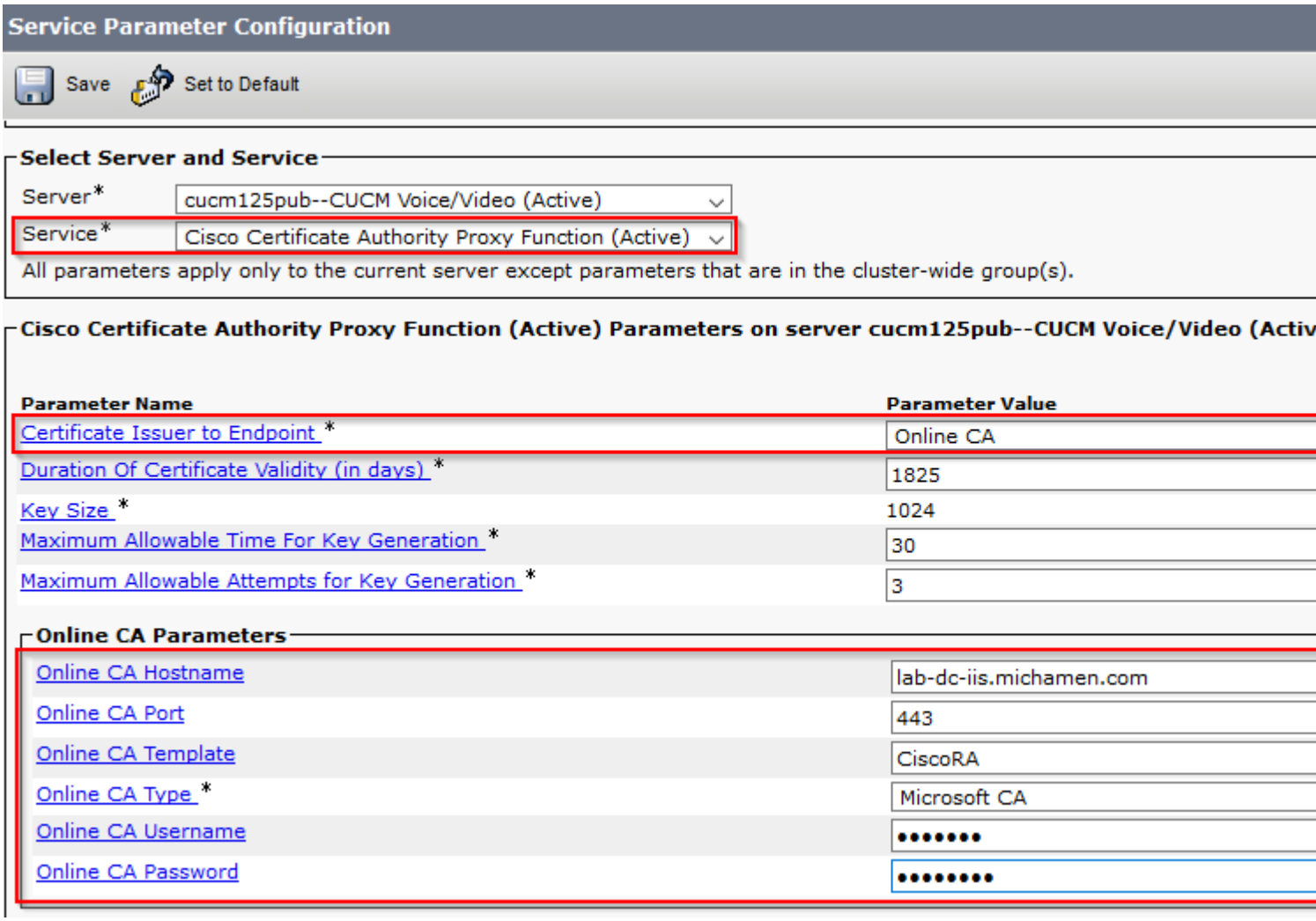


- Navegue para **Security > Certificate Management** na página OS Administration e selecione o botão **Upload Certificate/Certificate chain** para carregar o certificado CA com a **finalidade** definida como **CAPF-trust.**

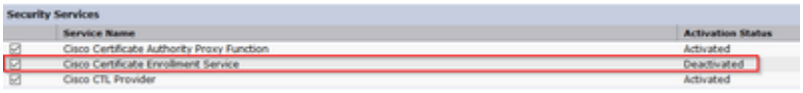


.. Neste ponto, também é uma boa ideia carregar o mesmo certificado CA como *CallManager-trust* porque ele é necessário se a criptografia de sinalização segura estiver habilitada (ou será habilitada) para os endpoints; o que provavelmente acontece se o cluster estiver no modo misto.

- Navegue até **Sistema > Parâmetros de serviço.** Selecione o servidor Editor do Unified CM no campo do servidor e **Cisco Certificate Authority Proxy Function** no campo Serviço
- Defina o valor do Emissor do Certificado como Ponto de Extremidade para a CA Online e insira os valores dos campos Parâmetros da CA Online. Certifique-se de usar o FQDN do servidor Web, o nome do modelo de certificado criado anteriormente (CiscoRA), o tipo de CA como Microsoft CA e use as credenciais da conta de usuário do CiscoRA criada anteriormente



- Uma janela pop-up informa que o serviço CAPF precisa ser reiniciado. Mas, primeiro, ative o Cisco Certificate Enrollment Service por meio do **Cisco Unified Serviceability > Tools > Service Ativation**, selecione o Publicador no campo Server e marque a caixa de seleção Cisco Certificate Enrollment Service e, em seguida, selecione o botão **Save** :



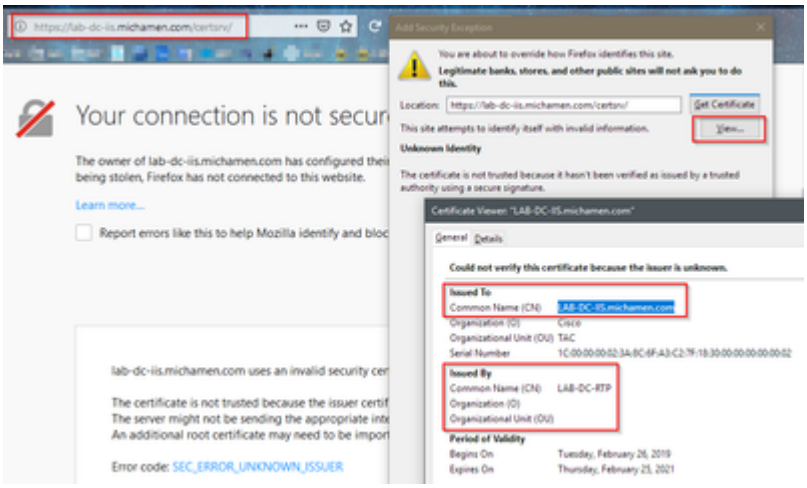
Verificar

Verificar Certificados do IIS

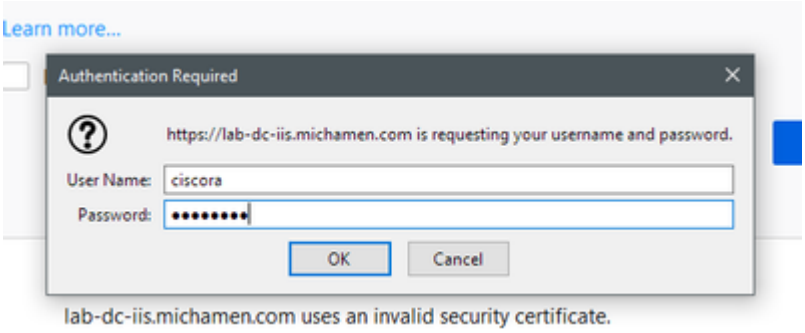
- Em um navegador da Web em um PC com conectividade com o servidor (preferencialmente na mesma rede que o Editor do CUCM), navegue até o URL:

  https://YOUR_SERVER_FQDN/certsrv/

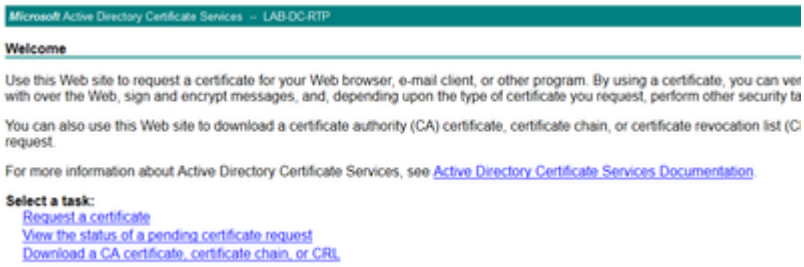
- Um alerta de certificado não confiável é exibido. Adicione a exceção e verifique o certificado. Certifique-se de que ele corresponda ao FQDN esperado:



- Depois de aceitar a exceção, você precisa se autenticar; neste ponto, você precisa usar as credenciais configuradas para a conta CiscoRA anteriormente:



- Após a autenticação, você deverá ver a página de boas-vindas do AD CS (Serviços de Certificados do Ative Diretory):



Verificar a configuração do CUCM

Execute as etapas normalmente seguidas para instalar um certificado LSC em um dos telefones.

Etapa 1. Abra a página Administração do CallManager, Dispositivo e Telefone

Etapa 2. Selecione o botão **Find** para exibir os telefones

Etapa 3. Selecione o telefone no qual deseja instalar o LSC

Etapa 4. Role até Certification Authority Proxy Function (CAPF) Information (Informações da função de proxy da autoridade de certificação)

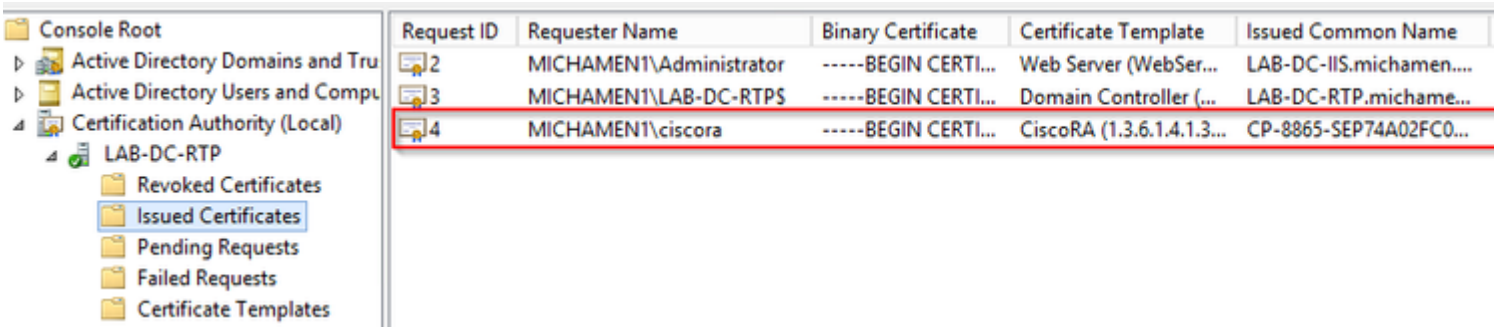
Etapa 5. Selecione Instalar/Atualizar na Operação de certificado.

Etapa 6. Selecione o Modo de autenticação. (Por sequência de caracteres nula é aceitável para fins de teste)

Passo 7. Role até o topo da página e selecione **salvar** e **Aplicar configuração** para o telefone.

Etapa 8. Depois que o telefone for reiniciado e se registrar novamente, use o filtro Status LSC para confirmar se o LSC foi instalado com êxito.

- No lado do servidor AD, abra o MMC e expanda o snap-in Autoridade de Certificação para selecionar a pasta Certificados Emitidos
- A entrada para o telefone é exibida Dentro da visualização resumida, estes são alguns dos detalhes exibidos:
  - ID da Solicitação: número de sequência exclusivo
  - Nome do solicitante: o nome de usuário da conta CiscoRA configurada deve ser exibido
  - Modelo de certificado: o nome do modelo do CiscoRA criado deve ser exibido
  - Nome comum emitido: o modelo do telefone anexado pelo nome do dispositivo deve ser exibido
  - Data efetiva do certificado e Data de vencimento do certificado



Links relacionados

- **Troubleshooting de CA On-line CAPF**
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.