Configurar o suporte ISE SCEP para BYOD

Contents

Introduction

Este documento descreve as etapas usadas para configurar com êxito o Microsoft Network Device Enrollment Service (NDES) e o Simple Certificate Enrollment Protocol (SCEP) para BYOD (Bring Your Own Device) no Cisco Identify Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE versão 1.1.1 ou posterior
- Microsoft Windows Server 2008 R2

- Microsoft Windows Server 2012 Standard
- Public Key Infrastructure (PKI) e certificados

Componentes Utilizados

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

- ISE versão 1.1.1 ou posterior
- Windows Server 2008 R2 SP1 com hotfixes KB2483564 e KB2633200 instalados
- Windows Server 2012 Standard

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, make sure that you understand the potential impact of any command.

As informações relacionadas aos serviços de certificado da Microsoft são fornecidas como um guia especificamente para o Cisco BYOD. Consulte o Microsoft TechNet como a fonte definitiva da verdade para a autoridade de certificação da Microsoft, Network Device Enrollment Service (NDES) e configurações de servidor relacionadas ao SCEP.

Informações de Apoio

Um dos benefícios da implementação de BYOD habilitada para o Cisco ISE é a capacidade dos usuários finais de executar o registro de dispositivos de autoatendimento. Isso elimina a carga administrativa sobre a TI para distribuir credenciais de autenticação e ativar dispositivos na rede. No centro da solução BYOD está o processo de provisionamento suplicante de rede, que busca distribuir os certificados necessários para os dispositivos de propriedade dos funcionários. Para atender a esse requisito, uma autoridade de certificação (AC) da Microsoft pode ser configurada para automatizar o processo de inscrição de certificado com o SCEP.

O SCEP é usado há anos em ambientes de VPN (Virtual Private Network) para facilitar a inscrição e distribuição de certificados para clientes e roteadores de acesso remoto. A ativação da funcionalidade SCEP em um servidor Windows 2008 R2 exige a instalação do NDES. Durante a instalação da função NDES, o servidor Web do Microsoft Internet Information Services (IIS) também está instalado. O IIS é usado para encerrar solicitações de registro e respostas HTTP ou HTTPS SCEP entre a CA e o nó de política do ISE.

A função NDES pode ser instalada em uma CA atual ou em um servidor membro. Em uma implantação autônoma, o serviço NDES é instalado em uma CA existente que inclui o serviço Autoridade de Certificação e, opcionalmente, o serviço de Inscrição na Web da Autoridade de Certificação. Em uma implantação distribuída, o serviço NDES é instalado em um servidor membro. O servidor NDES distribuído é então configurado para se comunicar com uma CA raiz upstream ou sub-raiz. Neste cenário, as modificações de registro descritas neste documento são feitas no servidor NDES com o modelo personalizado, onde os certificados residem na CA upstream.

Cenários de implantação de CA/NDES testados

Esta seção fornece uma breve visão geral dos cenários de implantação de CA/NDES que foram testados no laboratório da Cisco. Consulte o Microsoft TechNet como a fonte definitiva da verdade para as configurações de servidor relacionadas a Microsoft CA, NDES e SCEP.

Implantações independentes

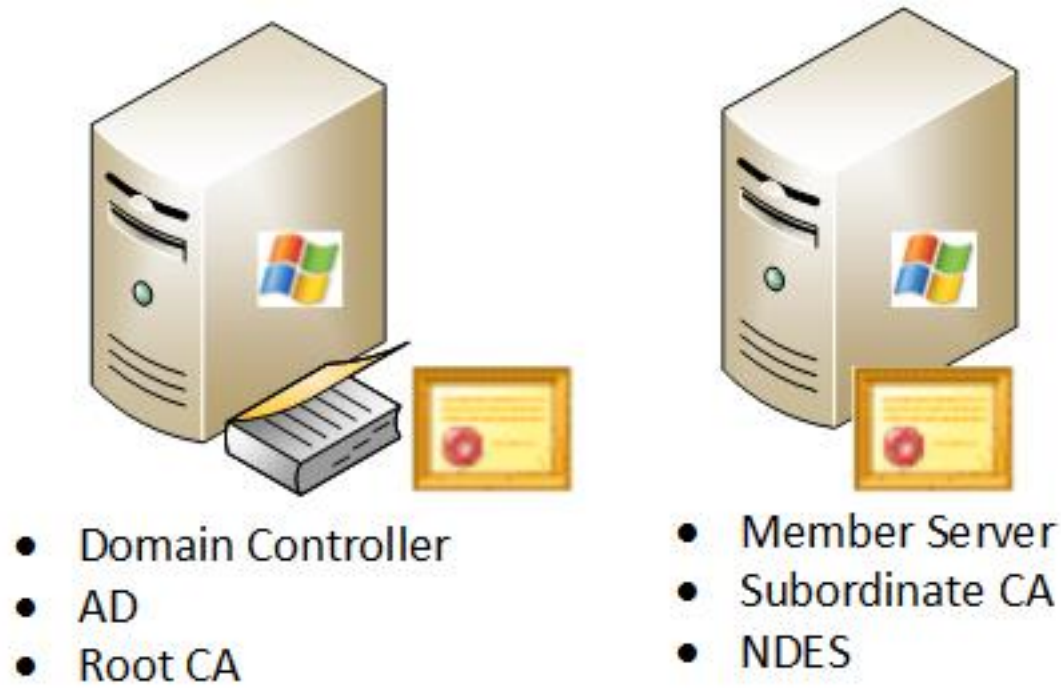
Quando o ISE é usado em um cenário de prova de conceito (PoC), é comum implantar uma máquina Windows 2008 ou 2012 independente que atue como um controlador de domínio do Ative Diretory (AD), CA raiz e servidor NDES:

- Domain Controller
- AD
- Root CA
- NDES

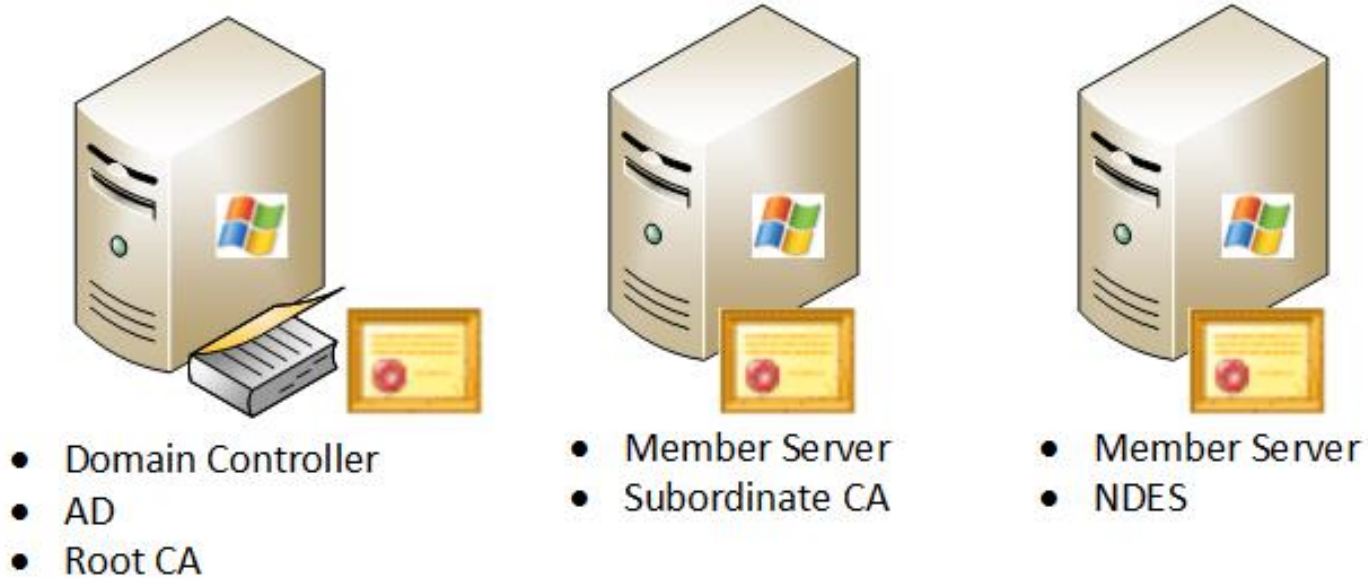
Implantações distribuídas

Quando o ISE é integrado em um ambiente de produção atual do Microsoft AD/PKI, é mais comum ver os serviços distribuídos em vários servidores Windows 2008 ou 2012 distintos. A Cisco testou dois cenários para implantações distribuídas.

Esta imagem ilustra o primeiro cenário testado para implantações distribuídas:



Esta imagem ilustra o segundo cenário testado para implantações distribuídas:



Hotfixes importantes da Microsoft

Antes de configurar o suporte SCEP para BYOD, certifique-se de que o servidor NDES do Windows 2008 R2 tenha estes hotfixes da Microsoft instalados:

- Falha na solicitação de renovação de um certificado SCEP no Windows Server 2008 R2 se o certificado for gerenciado usando NDES - Esse problema ocorre porque o NDES não oferece suporte à operação **GetCACaps**.

- O NDES não envia solicitações de certificado depois que a CA corporativa é reiniciada no Windows Server 2008 R2 - Esta mensagem aparece no **Visualizador de Eventos**: "*O Network Device Enrollment Service não pode enviar a solicitação de certificado (0x800706ba). O servidor RPC não está disponível*."

aviso: Quando você configura a CA da Microsoft, é importante entender que o ISE não suporta o algoritmo de assinatura RSASSA-PSS. A Cisco recomenda que você configure a política de CA para que ela use sha1WithRSAEncryption ou sha256WithRSAEncryption.

Portas e protocolos BYOD importantes

Aqui está uma lista de portas e protocolos BYOD importantes:

- TCP: Provisionamento 8909: Assistente de instalação do Cisco ISE (sistemas operacionais Windows e Macintosh (OS))
- TCP: 443 Provisionamento: Assistente de instalação do Google Play (Android)
- TCP: Provisionamento 8905: Processo de provisionamento do requerente
- TCP: 80 ou TCP: 443 Proxy SCEP para CA (com base na configuração da URL do SCEP RA)

Note: Para obter a lista mais recente de portas e protocolos necessários, consulte o Guia de instalação de hardware do ISE 1.2.

Configurar

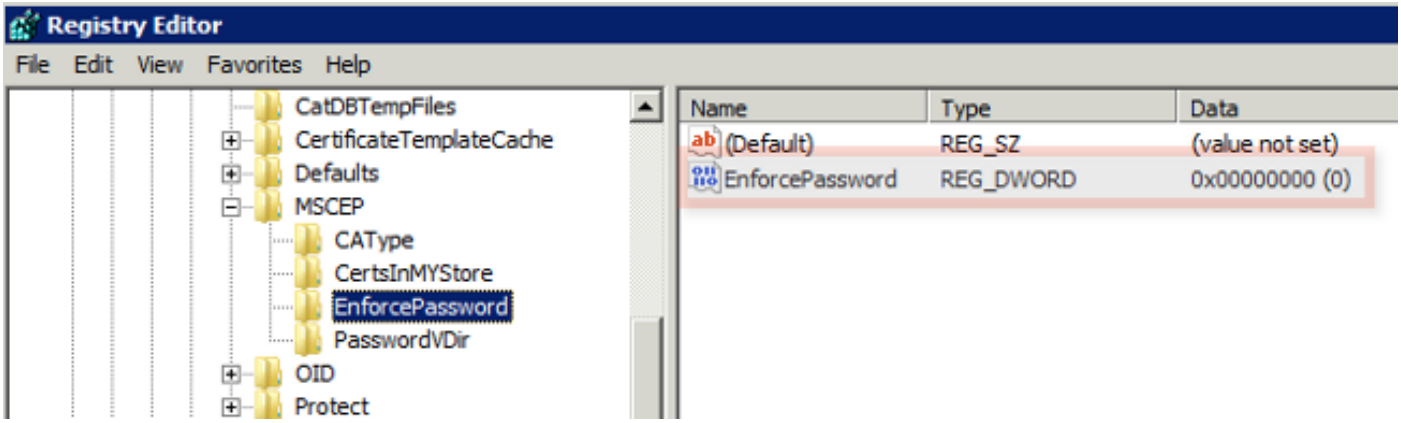
Use esta seção para configurar o suporte NDES e SCEP para BYOD no ISE.

Desativar o requisito de senha do desafio de inscrição do SCEP

Por padrão, a implementação do Microsoft SCEP (MSCEP) usa uma senha de desafio dinâmico para autenticar clientes e endpoints durante todo o processo de inscrição de certificado. Com esse requisito de configuração em vigor, você deve navegar até a GUI da Web do administrador do MSCEP no servidor NDES para gerar uma senha sob demanda. Você deve incluir essa senha como parte da solicitação de registro.

Em uma implantação de BYOD, a exigência de uma senha de desafio derrota a finalidade de uma solução de autoatendimento do usuário. Para remover este requisito, você deve modificar esta chave do registro no servidor NDES:

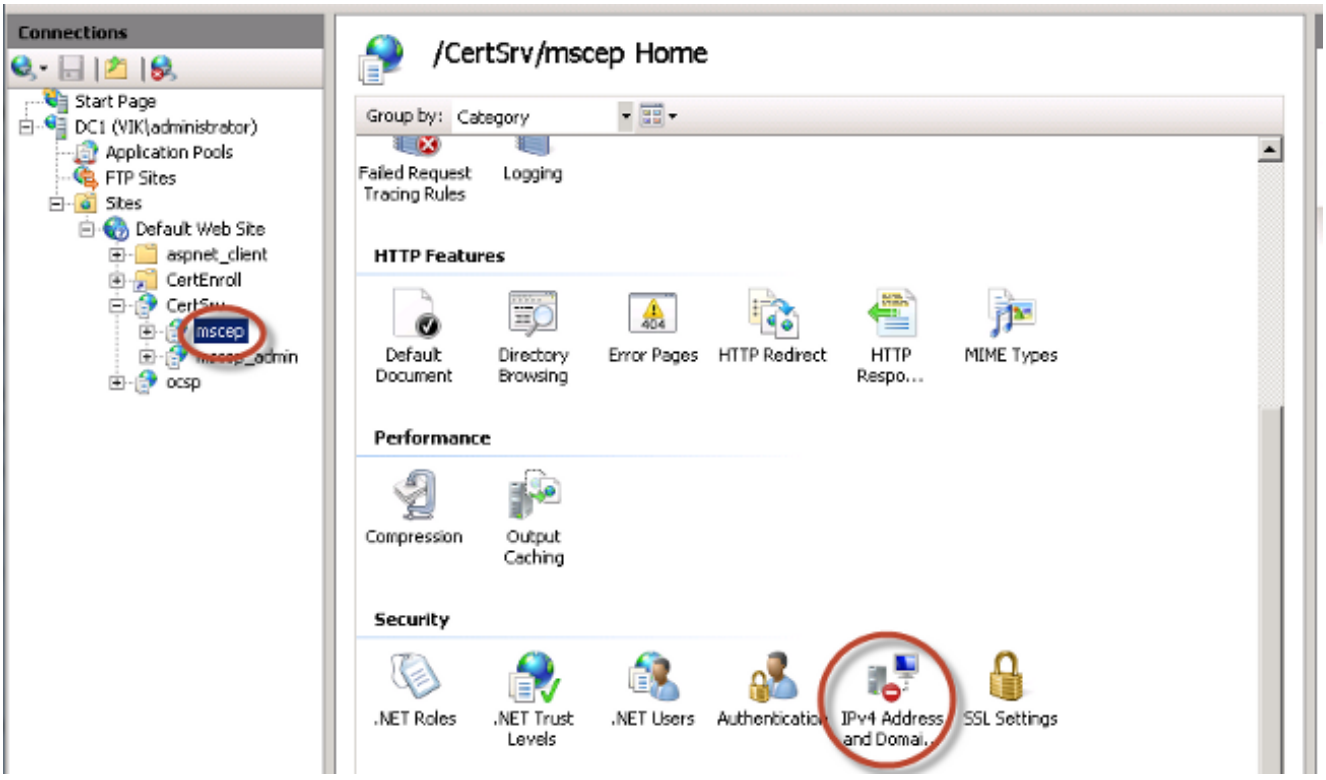
1. Clique em **Iniciar** e digite **regedit** na barra de pesquisa.
2. Navegue até Computador > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografia > **MSCEP** > **Aplicar senha**.
3. Verifique se o valor **EnforcePassword** está definido como **0** (o valor padrão é **1**).



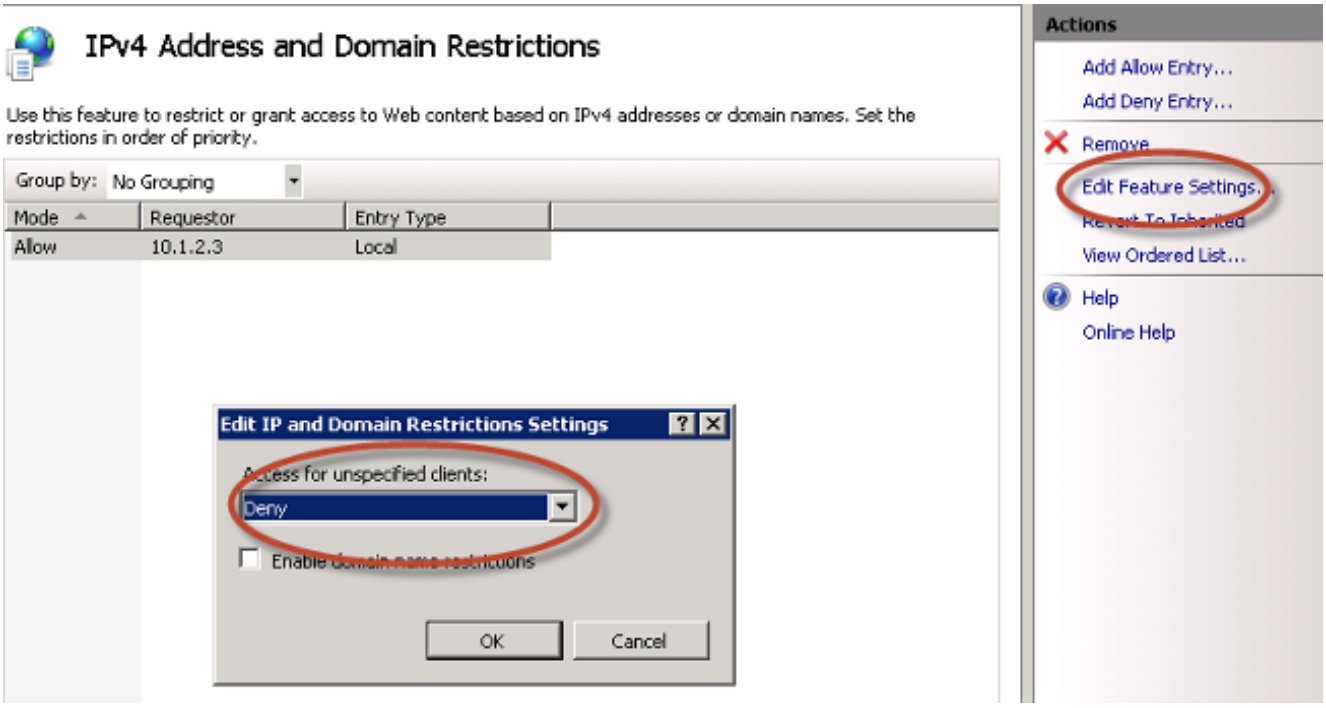
Restrinja a inscrição do SCEP a nós conhecidos do ISE

Em alguns cenários de implantação, pode ser preferível restringir as comunicações SCEP a uma lista selecionada de nós ISE conhecidos. Isso pode ser realizado com o recurso de Restrições de Endereço IPv4 e Domínio no IIS:

1. Abra o IIS e navegue até o site **/CertSrv/mscep**.



2. Clique duas vezes em **Segurança > Endereço IPv4 e Restrições de domínio.** Use as ações **Add Allow Entry** and **Add Deny Entry** para permitir ou restringir o acesso ao conteúdo da Web com base nos endereços IPv4 do nó do ISE ou nos nomes de domínio. Use a ação **Editar configurações de recurso** para definir uma regra de acesso padrão para clientes não especificados.

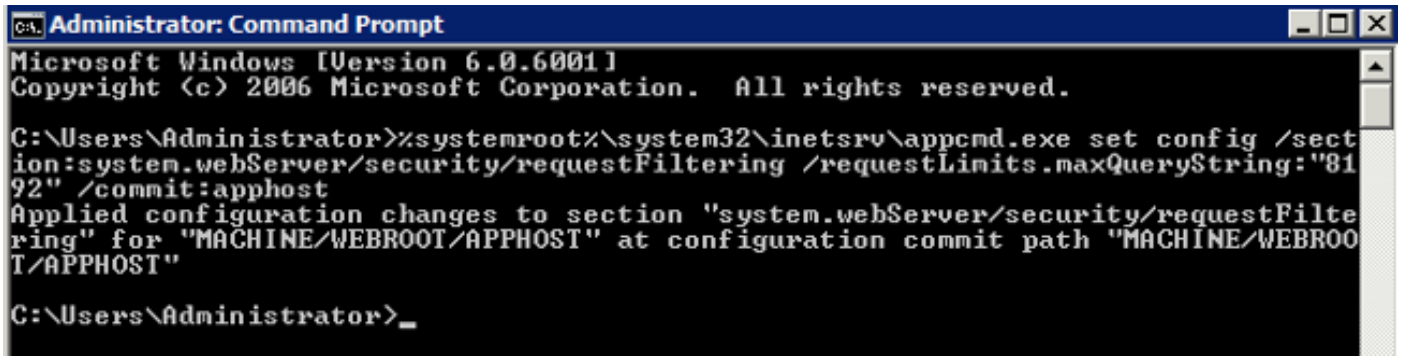


Estender o comprimento do URL no IIS

Épossível que o ISE gere URLs muito longas para o servidor Web do IIS. Para evitar esse problema, a configuração padrão do IIS pode ser modificada para permitir URLs mais longos. Insira este comando na CLI do servidor NDES:

```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/
 security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
```

> **Note**: O tamanho da string de consulta pode variar dependendo do ISE e da configuração do ponto de extremidade. Insira este comando na CLI do servidor NDES com privilégios administrativos.



Visão geral do modelo de certificado

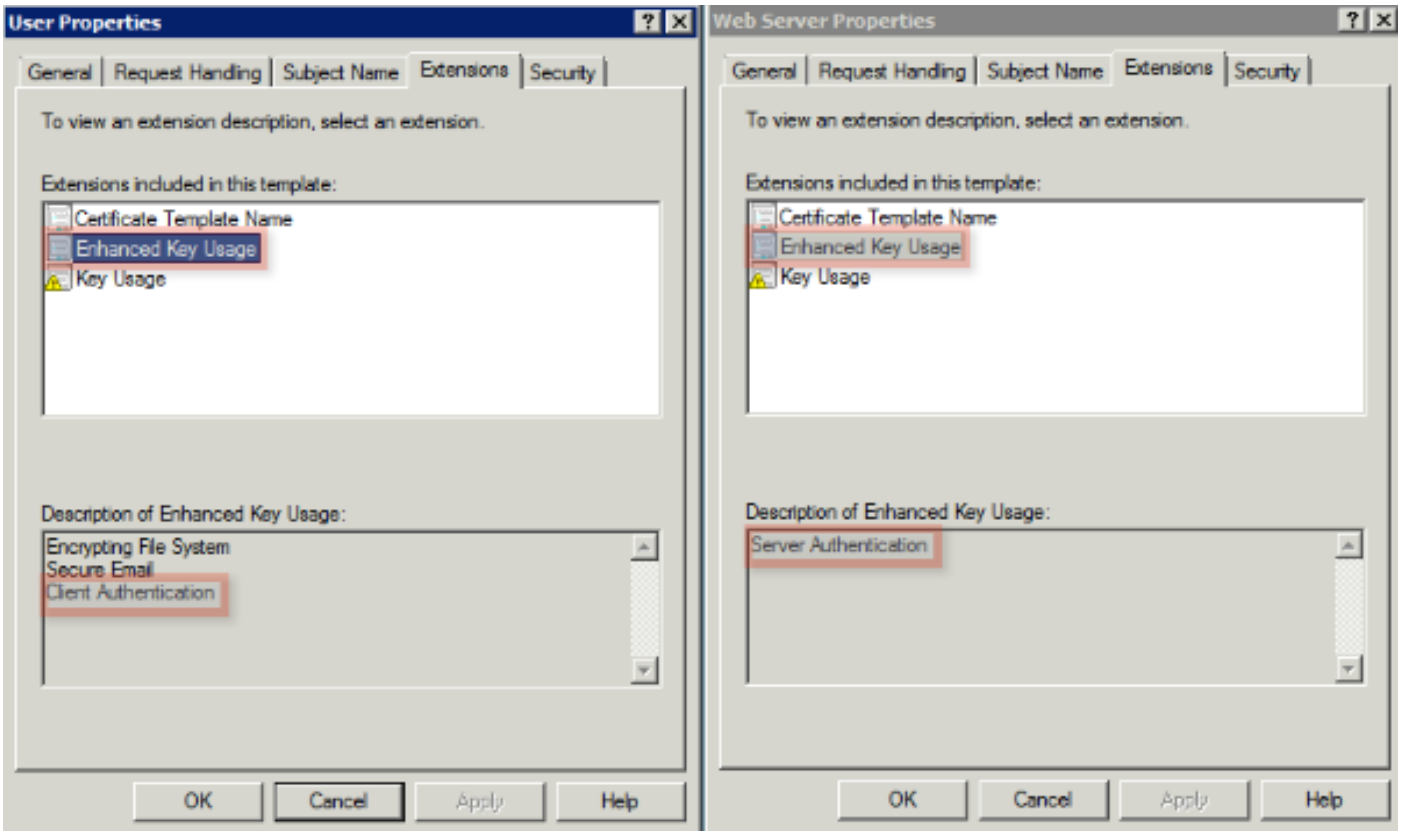
Os administradores de uma AC Microsoft podem configurar um ou mais modelos que são usados para aplicar políticas de aplicativos a um conjunto comum de certificados. Essas políticas ajudam a identificar para qual função o certificado e as chaves associadas são usados. Os valores da política do aplicativo estão contidos no campo Extended Key Usage (EKU) do certificado. O autenticador analisa os valores no campo EKU para garantir que o certificado apresentado pelo cliente possa ser usado para a função pretendida. Alguns dos usos mais comuns incluem autenticação de servidor, autenticação de cliente, VPN IPSec e e-mail. Em termos de ISE, os

valores EKU mais comumente usados incluem autenticação de servidor e/ou cliente.

Quando você navega para um site bancário seguro, por exemplo, o servidor Web que processa a solicitação é configurado com um certificado que tem uma política de aplicativo de autenticação de servidor. Quando o servidor recebe uma solicitação HTTPS, ele envia um certificado de autenticação de servidor ao navegador da Web de conexão para autenticação. O ponto importante aqui é que essa é uma troca unidirecional do servidor para o cliente. Em relação ao ISE, um uso comum para um certificado de autenticação de servidor é o acesso à GUI do administrador. O ISE envia o certificado configurado para o navegador conectado e não espera receber um certificado de volta do cliente.

Quando se trata de serviços como o BYOD que usam EAP-TLS, a autenticação mútua é preferida. Para habilitar essa troca de certificado bidirecional, o modelo usado para gerar o certificado de identidade do ISE deve possuir uma política de aplicativo mínima de autenticação de servidor. O modelo de certificado do Servidor Web atende a este requisito. O modelo de certificado que gera os certificados de ponto de extremidade deve conter uma política de aplicativo mínima de autenticação de cliente. O modelo de certificado do usuário atende a este requisito. Se você configurar o ISE para serviços como o iPEP (Inline Policy Implementation Point), o modelo usado para gerar o certificado de identidade do servidor ISE deverá conter atributos de autenticação de cliente e servidor se você usar o ISE versão 1.1.x ou anterior. Isso permite que os nós de administrador e em linha se autentiquem mutuamente. A validação EKU para iPEP foi removida no ISE versão 1.2, o que torna esse requisito menos relevante.

Você pode reutilizar os modelos padrão do Microsoft CA Web Server e do usuário ou clonar e criar um novo modelo com o processo descrito neste documento. Com base nesses requisitos de certificado, a configuração da CA e os certificados ISE e endpoint resultantes devem ser cuidadosamente planejados para minimizar quaisquer alterações de configuração indesejadas quando instalados em um ambiente de produção.



Configuração do modelo de certificado

Como observado na introdução, o SCEP é amplamente usado em ambientes VPN IPSec. Como resultado, a instalação da função NDES configura automaticamente o servidor para utilizar o modelo **IPSec (Solicitação Offline)** para SCEP. Por causa disso, uma das primeiras etapas na preparação de uma CA da Microsoft para BYOD é criar um novo modelo com a política de aplicativos correta. Em uma implantação autônoma, a Autoridade de Certificação e os serviços NDES são colocados no mesmo servidor, e os modelos e as modificações de registro necessárias estão contidos no mesmo servidor. Em uma implantação NDES distribuída, as modificações de registro são feitas no servidor NDES; no entanto, os modelos reais são definidos no servidor CA raiz ou sub-raiz especificado na instalação do serviço NDES.

Conclua estes passos para configurar o Modelo de certificado:

1. Inicie sessão no servidor CA como **admin**.

2. Clique em **Iniciar > Ferramentas administrativas > Autoridade de certificação**.

3. Expanda os detalhes do servidor CA e selecione a pasta **Modelos de certificado**. Esta pasta contém uma lista dos modelos atualmente ativados.

4. Para gerenciar os modelos de certificado, clique com o botão direito do mouse na pasta **Modelos de certificado** e escolha **Gerenciar**.

5. No **Console de modelos de certificado**, vários modelos inativos são exibidos.

6. Para configurar um novo modelo para uso com o SCEP, clique com o botão direito do mouse em um modelo que já existe, como **Usuário**, e escolha **Modelo Duplicado**.

7. Escolha **Windows 2003** ou **Windows 2008**, dependendo do SO de CA mínimo no ambiente.

8. Na guia **Geral**, adicione um nome de exibição, como ISE-BYOD e período de validade; deixe todas as outras opções desmarcadas.
   Note: O período de validade do modelo deve ser menor ou igual ao período de validade dos certificados raiz e intermediários da CA.
9. Clique na guia **Nome do assunto** e confirme se **Suprimento na solicitação** está selecionado.

10. Clique na guia **Issuance Requirements (Requisitos de problema)**. A Cisco recomenda que você deixe as **políticas de Emissão** em branco em um ambiente de CA hierárquico típico.

11. Clique na guia **Extensions**, **Application Policies** e depois **Edit**.

12. Clique em **Adicionar** e certifique-se de que a **Autenticação de Cliente** seja adicionada como uma política de aplicação. Click **OK**.

13. Clique na guia **Segurança** e em **Adicionar...**. Certifique-se de que a conta de serviço SCEP definida na instalação do serviço NDES tem o controlo total do modelo e, em seguida, clique em **OK**.

14. Retorne à interface **GUI da Autoridade de Certificação**.

15. Clique com o botão direito do mouse no diretório **Modelos de certificado**. Navegue até **New > Certificate Template to Issue**.

16. Selecione o modelo **ISE-BYOD** configurado anteriormente e clique em **OK**.

    Note: Como alternativa, você pode habilitar o modelo via CLI com o comando **certutil -SetCAtemplates +ISE-BYOD**.
    O modelo ISE-BYOD agora deve estar listado na lista de modelos de certificado habilitados.

Configuração do Registro do Modelo de Certificado

Conclua estes passos para configurar as chaves do Registro do Modelo de Certificado:

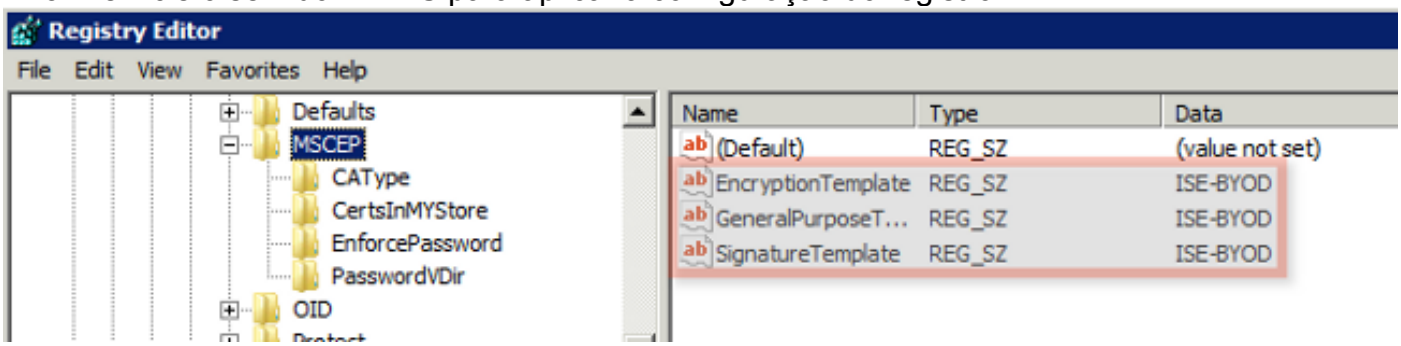
1. Conecte-se ao servidor NDES.

2. Clique em **Iniciar** e digite **regedit** na barra de pesquisa.

3. Navegue até Computador > HKEY_LOCAL_MACHINE > SOFTWARE > **Microsoft** > **Criptografia** > **MSCEP**.

4. Altere as chaves EncryptionTemplate, **GeneralPurposeTemplate** e **SignatureTemplate** de **IPSec (Solicitação off-line)** para o modelo **ISE-BYOD criado anteriormente.**

5. Reinicie o servidor NDES para aplicar a configuração do registro.



Configurar o ISE como um proxy SCEP

Em uma implantação de BYOD, o endpoint não se comunica diretamente com o servidor NDES de back-end. Em vez disso, o nó de política do ISE é configurado como um proxy SCEP e se comunica com o servidor NDES em nome dos endpoints. Os endpoints se comunicam diretamente com o ISE. A instância do IIS no servidor NDES pode ser configurada para suportar associações HTTP e/ou HTTPS para os diretórios virtuais SCEP.

Conclua estes passos para configurar o ISE como um proxy SCEP:

1. Efetue login na **GUI do ISE** com credenciais de administrador.

2. Clique em **Administração**, **Certificados** e **Perfis CA SCEP**.

3. Clique em Add.

4. Digite o nome e a descrição do servidor.

5. Insira o URL do servidor SCEP com o IP ou o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) (http://10.10.10.10/certsrv/mscep/, por exemplo).

6. Clique em **Testar conectividade**. Uma conexão bem-sucedida resulta em uma mensagem pop-up de resposta do servidor bem-sucedida.

7. Clique em **Salvar** para aplicar a configuração.

8. Para verificar, clique em **Administração**, **Certificados**, **Repositório de Certificados** e confirme se o certificado RA do servidor SCEP NDES foi baixado automaticamente para o nó ISE.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Use esta seção para fazer o troubleshooting da sua configuração.

Notas gerais de solução de problemas

Aqui está uma lista de notas importantes que você pode usar para solucionar problemas de sua configuração:

- Divida a topologia de rede BYOD em pontos de conexão lógicos para ajudar a identificar pontos de depuração e captura ao longo do caminho entre os terminais ISE, NDES e CA.
- Assegure-se de que o nó ISE e a CA compartilhem uma fonte de tempo comum do Network Time Protocol (NTP).
- Os endpoints devem ser capazes de definir sua hora automaticamente com o NTP e as opções de fuso horário aprendidas com o DHCP.
- O servidor DNS do cliente deve ser capaz de resolver o FQDN do nó ISE.
- Certifique-se de que o TCP 80 e/ou o TCP 443 sejam permitidos bidirecionalmente entre o ISE e o servidor NDES.
- Teste com uma máquina Windows devido ao registro melhorado no lado do cliente. Opcionalmente, use um iDevice da Apple junto com o Utilitário de Configuração do iPhone da Apple para monitorar registros de console do lado do cliente.
- Monitore os registros de aplicativos do servidor CA e NDES para verificar se há erros de

registro e use o Google ou TechNet para pesquisar esses erros.

- Durante a fase de teste, use HTTP para SCEP para facilitar capturas de pacotes entre ISE, NDES e CA.

- Use o utilitário TCP Dump no nó de serviço de política ISE (PSN) e monitore o tráfego de e para o servidor NDES. Ela está localizada em **Operações > Ferramentas de diagnóstico > Ferramentas gerais**.

- Instale o Wireshark no servidor CA e NDES ou use o SPAN em switches intermediários para capturar o tráfego SCEP de e para o ISE PSN.

- Verifique se a cadeia de certificados CA apropriada está instalada no nó de política ISE para a autenticação dos certificados do cliente.

- Certifique-se de que a cadeia de certificados CA apropriada é automaticamente instalada nos clientes durante a integração.

- Visualize os certificados de identidade do ISE e do endpoint e confirme se os atributos EKU corretos estão presentes.

- Monitore os registros de autenticação ao vivo na GUI do ISE para falhas de autenticação e autorização.
  Note: Alguns suplicantes não inicializam uma troca de certificado de cliente se a EKU incorreta estiver presente, como um certificado de cliente com EKU de autenticação de servidor. Portanto, as falhas de autenticação podem não estar sempre presentes nos registros do ISE.
- Quando o NDES é instalado em uma implantação distribuída, uma CA raiz ou sub-raiz remota será designada por Nome da CA ou Nome do computador na instalação do serviço. O servidor NDES envia solicitações de registro de certificado para este servidor CA de destino. Se o processo de registro de certificado de endpoint falhar, as capturas de pacote (PCAP) podem mostrar que o servidor NDES retorna um erro **404 não encontrado** ao nó ISE. Para resolver esse problema, reinstale o serviço NDES e selecione a opção Nome do computador em vez do Nome da CA.

- Evite alterações na cadeia de CA do SCEP depois que os dispositivos forem integrados. Os SOs de endpoint, como o Apple iOS, não atualizam automaticamente um perfil de BYOD instalado anteriormente. Neste exemplo do iOS, o perfil atual deve ser excluído do endpoint e o endpoint removido do banco de dados do ISE, para que a integração possa ser executada novamente.

- Você pode configurar um servidor de certificados da Microsoft para se conectar à Internet e atualizar automaticamente certificados do Programa de Certificados Raiz da Microsoft. Se você configurar essa opção de recuperação de rede em ambientes com políticas de Internet restritas, os servidores CA/NDES que não podem se conectar à Internet podem levar 15 segundos para o tempo limite por padrão. Isso pode adicionar um atraso de 15 segundos ao processamento de solicitações SCEP de proxies SCEP, como o ISE. O ISE é programado para expirar as solicitações SCEP após 12 segundos se uma resposta não for recebida. Para

resolver esse problema, permita o acesso à Internet para os servidores CA/NDES ou modifique as configurações de tempo limite de recuperação de rede na política de segurança local dos servidores CA/NDES da Microsoft. Para localizar essa configuração no servidor Microsoft, navegue para **Iniciar > Ferramentas Administrativas > Política de Segurança Local > Políticas de Chave Pública > Configurações de Validação de Caminho de Certificado > Recuperação de Rede**.

Registro do lado do cliente

Aqui está uma lista de técnicas úteis usadas para solucionar problemas de registro no lado do cliente:

- Digite o **log %temp%\spwProfileLog.txt.** para exibir os logs do lado do cliente para aplicativos Microsoft Windows.
  Note: O WinHTTP é usado para a conexão entre o ponto de extremidade do Microsoft Windows e o ISE. Consulte o artigo Mensagens de Erro do Microsoft Windows para obter uma lista de códigos de erro.
- Insira o comando **/sdcards/downloads/spw.log** para exibir os registros do lado do cliente para aplicativos Android.

- Para **MAC OSX**, use o aplicativo Console e procure o processo **SPW**.

- Para o **Apple iOS**, use o Apple Configurator 2.0 para exibir mensagens.

Registro do ISE

Conclua estes passos para visualizar o log do ISE:

1. Navegue até **Administration > Logging > Debug Log Configuration** e selecione o nó apropriado da política do ISE.

2. Defina o **cliente** e os logs de **provisionamento** como debug ou trace, conforme necessário.

3. Reproduza o problema e documente as informações de propagação relevantes para facilitar a pesquisa, como MAC, IP e usuário.

4. Navegue até **Operations > Download Logs** e selecione o nó ISE apropriado.

5. Na guia **Debug Logs**, faça o download dos registros chamados **ise-psc.log** para a área de trabalho.

6. Use um editor inteligente, como o Notepad ++ para analisar os arquivos de log.

7. Quando o problema tiver sido isolado, retorne os níveis de log ao nível padrão.

Registro e solução de problemas do NDES

Para obter mais informações, consulte o AD CS: Artigo sobre Troubleshooting Network Device

Enrollment Service Windows Server.

Informações Relacionadas

- Guia de soluções BYOD - Configuração do servidor da autoridade de certificação
- Visão geral do NDES no Windows 2008 R2
- White paper do MSCEP
- Configurando o servidor NDES para suportar SSL
- Requisitos de certificado ao utilizar EAP-TLS ou PEAP com EAP-TLS
- Suporte técnico e documentação