Configurar o apoio ISE SCEP para BYOD

Índice

Introdução

Este documento descreve as etapas que são usadas a fim configurar com sucesso o serviço do registro do dispositivo da rede Microsoft (NDE) e o protocolo simple certificate enrollment (SCEP) para Bring Your Own Device (BYOD) em Cisco identifica o motor dos serviços (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Liberação 1.1.1 ISE ou mais atrasado
- Microsoft Windows server 2008 R2

- Padrão do Microsoft Windows server 2012
- Public Key Infrastructure (PKI) e Certificados

Componentes Utilizados

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

- Liberação 1.1.1 ISE ou mais atrasado
- Windows Server 2008 R2 SP1 com os hotfix KB2483564 e KB2633200 instalados
- Padrão de Windows Server 2012

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

O relativo à informação aos serviços certificados de Microsoft é fornecido como guia especificamente para Cisco BYOD. Refira o Microsoft TechNet como a fonte definitiva de verdade para a autoridade de certificação de Microsoft, o serviço do registro do dispositivo de rede (NDE), e configurações do servidor SCEP-relacionadas.

Informações de Apoio

Um dos benefícios da aplicação ISE-permitida Cisco BYOD é a capacidade dos utilizadores finais para executar o registro do dispositivo do autosserviço. Isto elimina a sobrecarga administrativa no TI a fim distribuir credenciais de autenticação e permitir dispositivos na rede. No centro de BYOD a solução é o processo de provisionamento do suplicante da rede, que procura distribuir os Certificados necessários aos dispositivos dos empregados. A fim satisfazer esta exigência, um Microsoft Certificate Authority (CA) pode ser configurado a fim automatizar o processo do certificado de registro com o SCEP.

O SCEP foi usado por anos em ambientes do Virtual Private Network (VPN) a fim facilitar o certificado de registro e a distribuição aos clientes de acesso remoto e ao Roteadores. A habilitação da funcionalidade SCEP em um server R2 de Windows 2008 exige a instalação dos NDE. Durante a instalação do papel NDE, o servidor de Web do Internet Information Services de Microsoft (IIS) é instalado igualmente. O IIS é usado a fim terminar o HTTP ou as requisições de registro e as respostas HTTPS SCEP entre nó da política de CA e ISE.

O papel NDE pode ser instalado em CA atual, ou pode ser instalado em um servidor membro. Em um desenvolvimento autônomo, o serviço NDE é instalado em CA existente que inclui o serviço da autoridade de certificação e, opcionalmente, o serviço do registro da Web da autoridade de certificação. Em um desenvolvimento distribuído, o serviço NDE é instalado em um servidor membro. O server distribuído NDE é configurado então a fim comunicar-se com uma raiz ou uma secundário-raiz ascendente CA. Nesta encenação, as alterações do registro esboçadas neste documento são feitas no server NDE com o molde personalizado, onde os Certificados residem em CA ascendente.

Cenários de distribuição testados CA/NDES

Esta seção fornece uma breve visão geral dos cenários de distribuição CA/NDES que foram testados no laboratório Cisco. Refira o Microsoft TechNet como a fonte definitiva de verdade para

Microsoft CA, NDE, e configurações do servidor SCEP-relacionadas.

Disposições autônomas

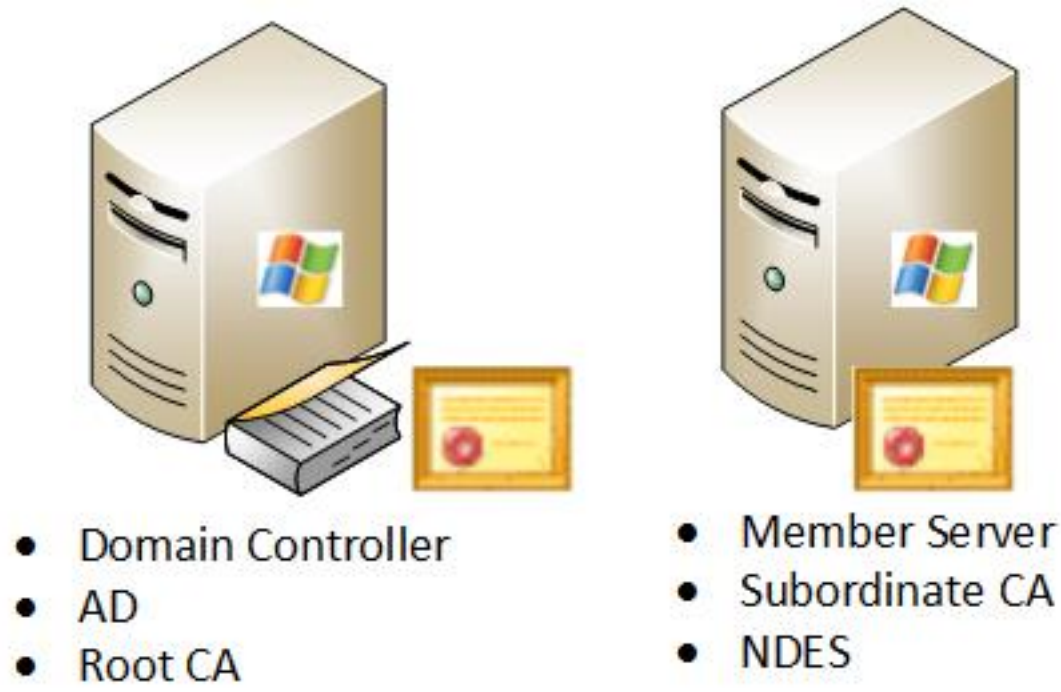
Quando o ISE está usado em uma encenação do teste de conceito (PoC), é comum distribuir Windows independente 2008 ou 2012 faz à máquina que atua como um controlador de domínio do diretório ativo (AD), a CA raiz, e o server NDE:

- Domain Controller
- AD
- Root CA
- NDES

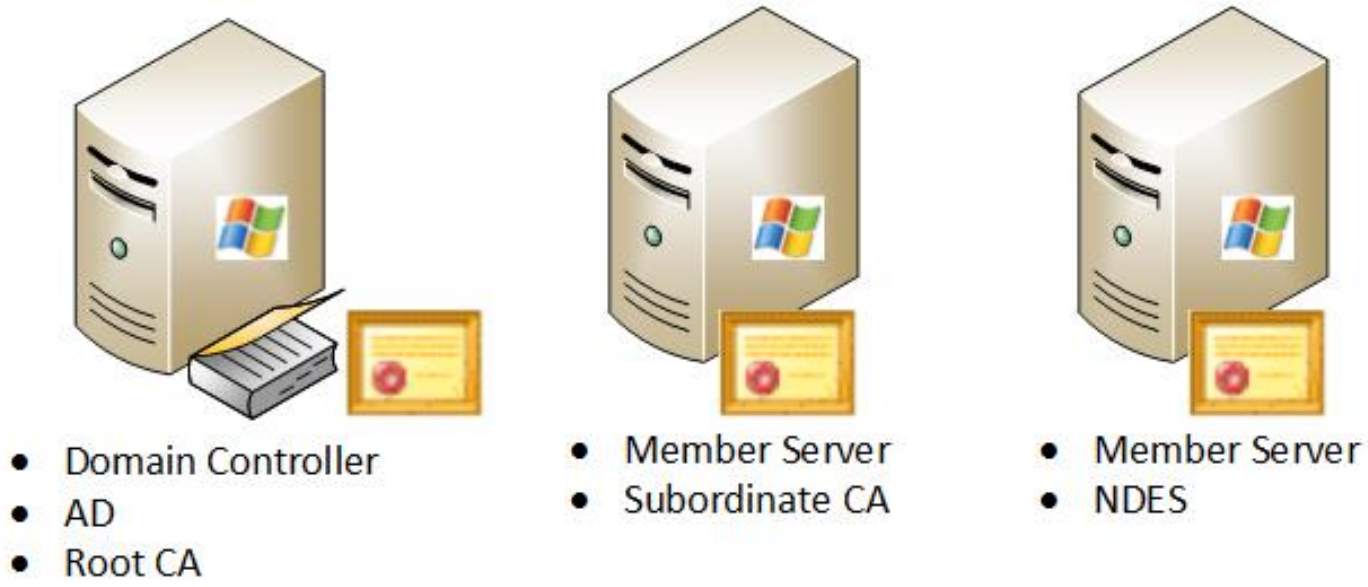
Disposições distribuídas

Quando o ISE é integrado em um ambiente de produção atual de Microsoft AD/PKI, é mais comum ver os serviços distribuídos através do múltiplo, dos server distintos de Windows 2008 ou 2012. Cisco testou duas encenações para disposições distribuídas.

Esta imagem ilustra a primeira encenação testada para disposições distribuídas:



Esta imagem ilustra a segunda encenação testada para disposições distribuídas:



Hotfix importantes de Microsoft

Antes que você configure o apoio SCEP para BYOD, assegure-se de que o server de Windows 2008 R2 NDE tenha estes hotfix de Microsoft instalado:

- A requisição de renovação para um certificado SCEP falha em Windows Server 2008 R2 se o certificado é controlado usando NDE - esta edição ocorre porque os NDE não apoiam a operação de **GetCACaps**.

- Os NDE não submetem pedidos do certificado depois que a empresa CA é reiniciada em Windows Server 2008 esta mensagem R2- aparece no **visualizador de eventos**: "O *serviço do registro do dispositivo de rede não pode submeter o pedido do certificado (0x800706ba). O servidor de Rpc é não disponível*."

aviso: Quando você configura Microsoft CA, é importante compreender que o ISE não apoia o algoritmo da assinatura RSASSA-PSS. Cisco recomenda que você configura a política de CA de modo que use sha1WithRSAEncryption ou sha256WithRSAEncryption pelo contrário.

Portas importantes & protocolos BYOD

Está aqui uma lista de portas e protocolo importantes BYOD:

- TCP: Abastecimento 8909: O assistente instala de Cisco ISE (Windows e sistemas operacionais de Macintosh (o OS))
- TCP: Abastecimento 443: O assistente instala de Google Play (Android)
- TCP: Abastecimento 8905: Processo de provisionamento do suplicante
- TCP: 80 ou TCP: 443 proxy SCEP a CA (baseado na configuração SCEP RA URL)

  Nota: Para a lista a mais atrasada de portas e protocolo exigidas, refira o guia de instalação de hardware ISE 1.2.

Configurar

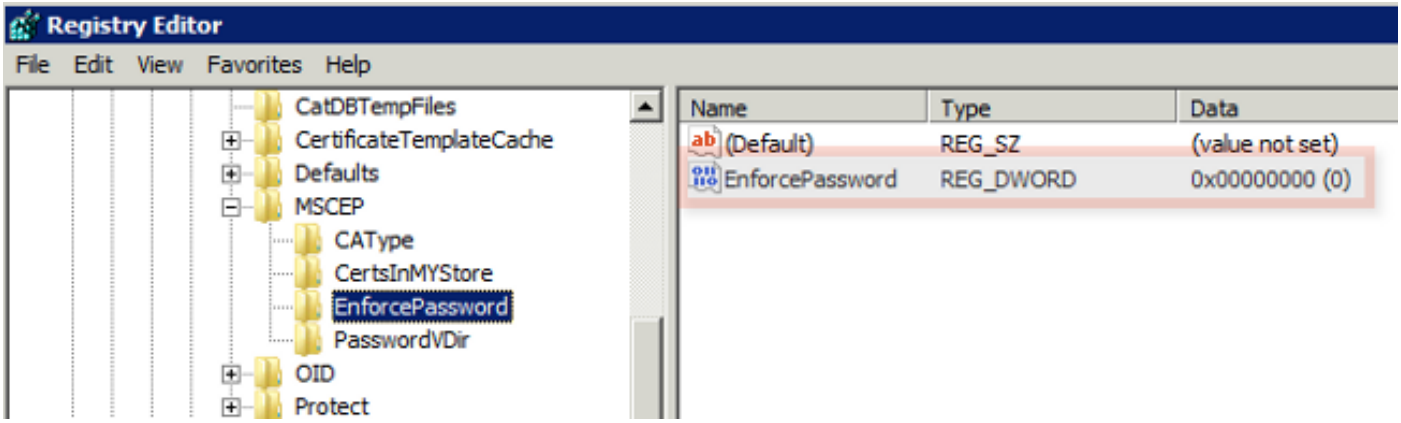
Use esta seção a fim configurar o apoio NDE e SCEP para BYOD no ISE.

Desabilite a exigência da senha do desafio do registro SCEP

Àrevelia, a aplicação de Microsoft SCEP (MSCEP) usa uma senha do desafio dinâmica a fim autenticar clientes e valores-limite durante todo o processo do certificado de registro. Com este requisito de configuração no lugar, você deve consultar à Web GUI MSCEP admin no server NDE a fim gerar uma senha por encomenda. Você deve incluir esta senha como parte da requisição de registro.

Em um desenvolvimento BYOD, a exigência de uma senha do desafio derrota a finalidade de uma solução do autosserviço do usuário. A fim remover esta exigência, você deve alterar esta chave de registro no server NDE:

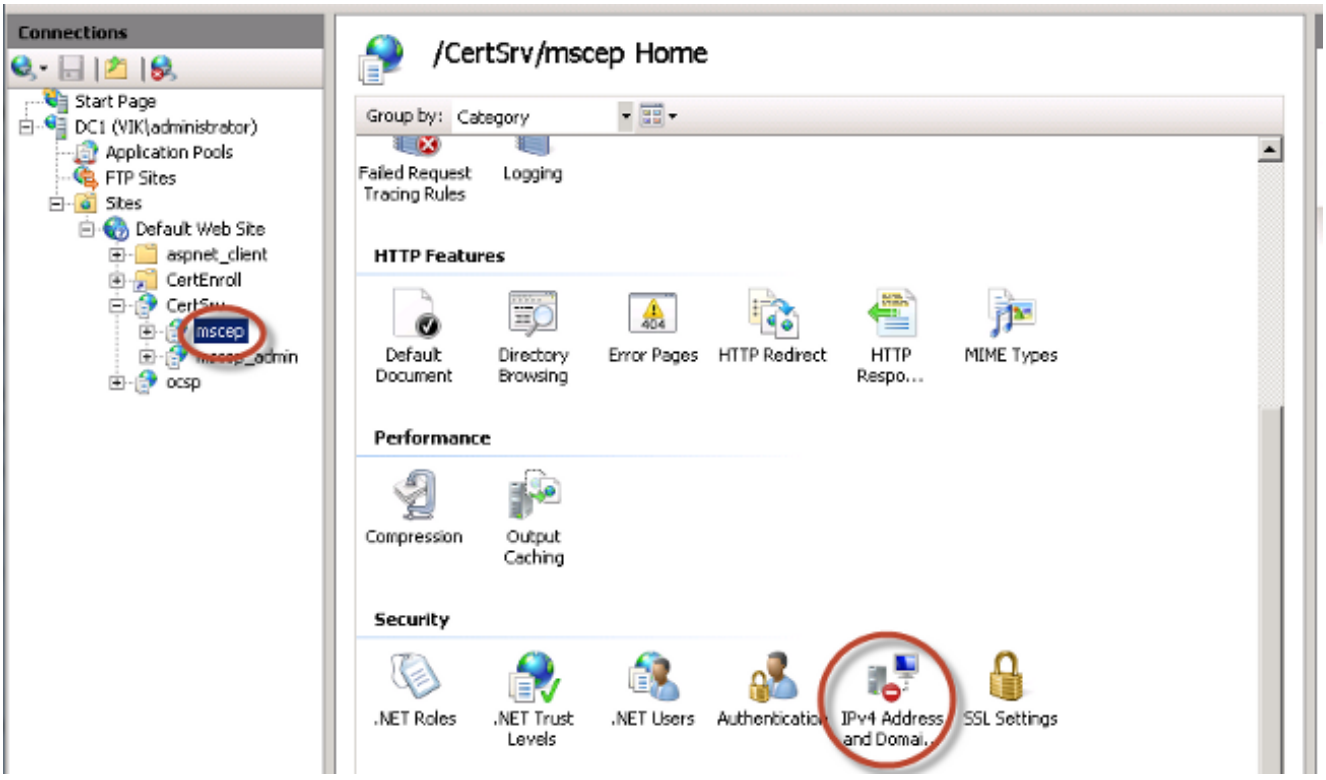
1. Clique o **começo** e incorpore o **regedit à** barra da busca.
2. Navegue ao **computador** > ao **HKEY_LOCAL_MACHINE** > ao **SOFTWARE** > ao **Microsoft** > à **criptografia** > ao **MSCEP** > ao **EnforcePassword**.
3. Assegure-se de que o valor de **EnforcePassword** esteja ajustado a **0** (o valor padrão é **1**).



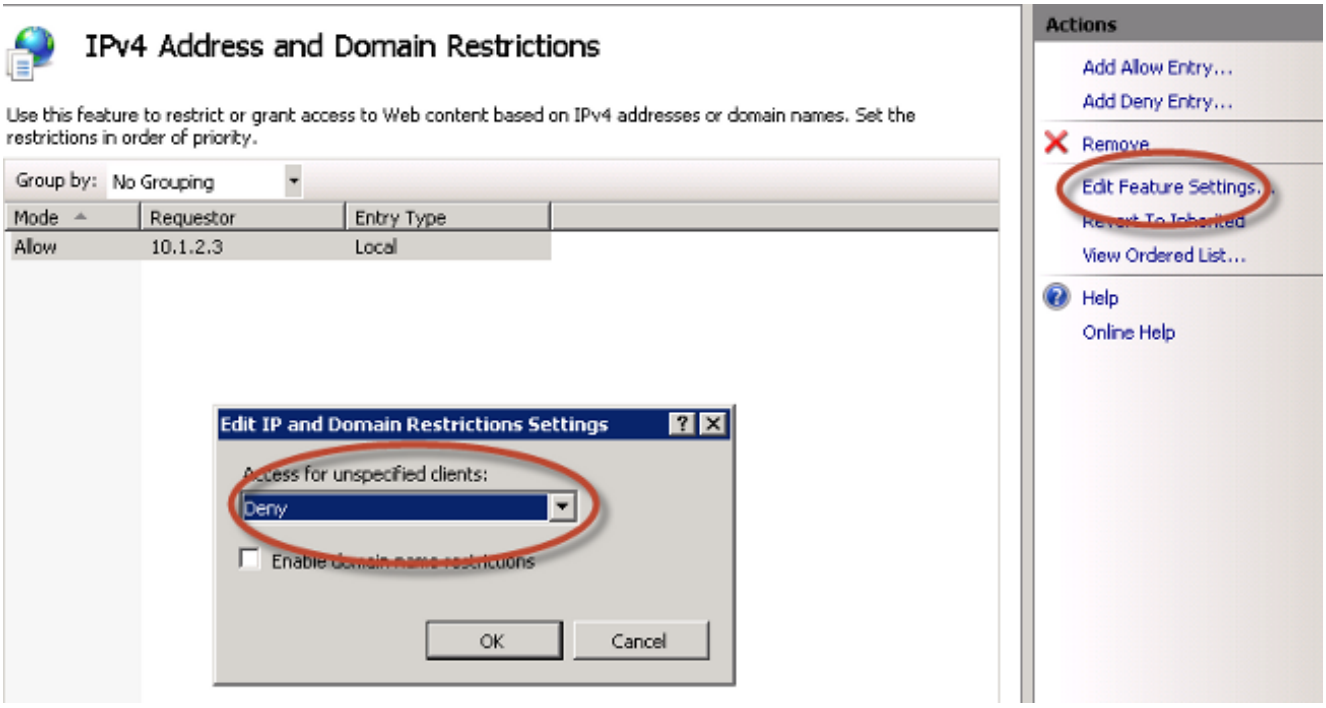
Restrinja o registro SCEP aos Nós conhecidos ISE

Em alguns cenários de distribuição, pôde-se preferir restringir comunicações SCEP a uma lista seleta de Nós conhecidos ISE. Isto pode ser realizado com a característica das limitações do endereço e do domínio do IPv4 no IIS:

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



2. Fazer duplo clique **limitações da Segurança > do endereço e do domínio do IPv4.** Use **adicionar permitem a entrada** e **adicionar-la negam** ações da **entrada** a fim permitir ou restringir o acesso ao conteúdo da Web baseado em endereços ou em Domain Name do IPv4 do nó ISE. Use a ação dos **conjuntos de recurso da edição** a fim definir uma regra do acesso do padrão para clientes não especificads.

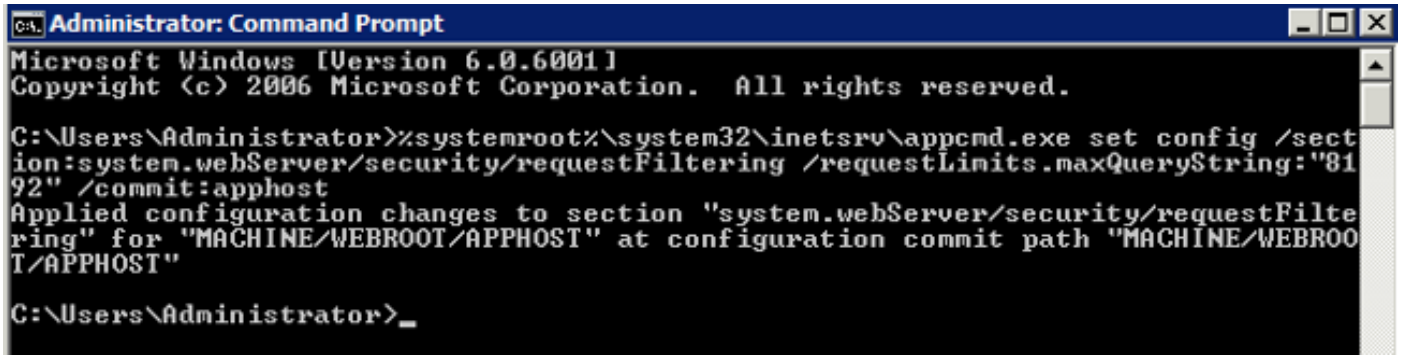


Estenda o comprimento URL no IIS

Épossível para o ISE gerar as URL que são demasiado longas para o servidor de Web IIS. A fim evitar este problema, a configuração de IIS do padrão pode ser alterada para permitir umas URL mais longas. Incorpore este comando do server CLI NDE:

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

> Nota: O tamanho de série da pergunta pôde variar o dependente em cima da configuração ISE e de valor-limite. Incorpore este comando do server CLI NDE com privilégios administrativos.



Vista geral do molde de certificado

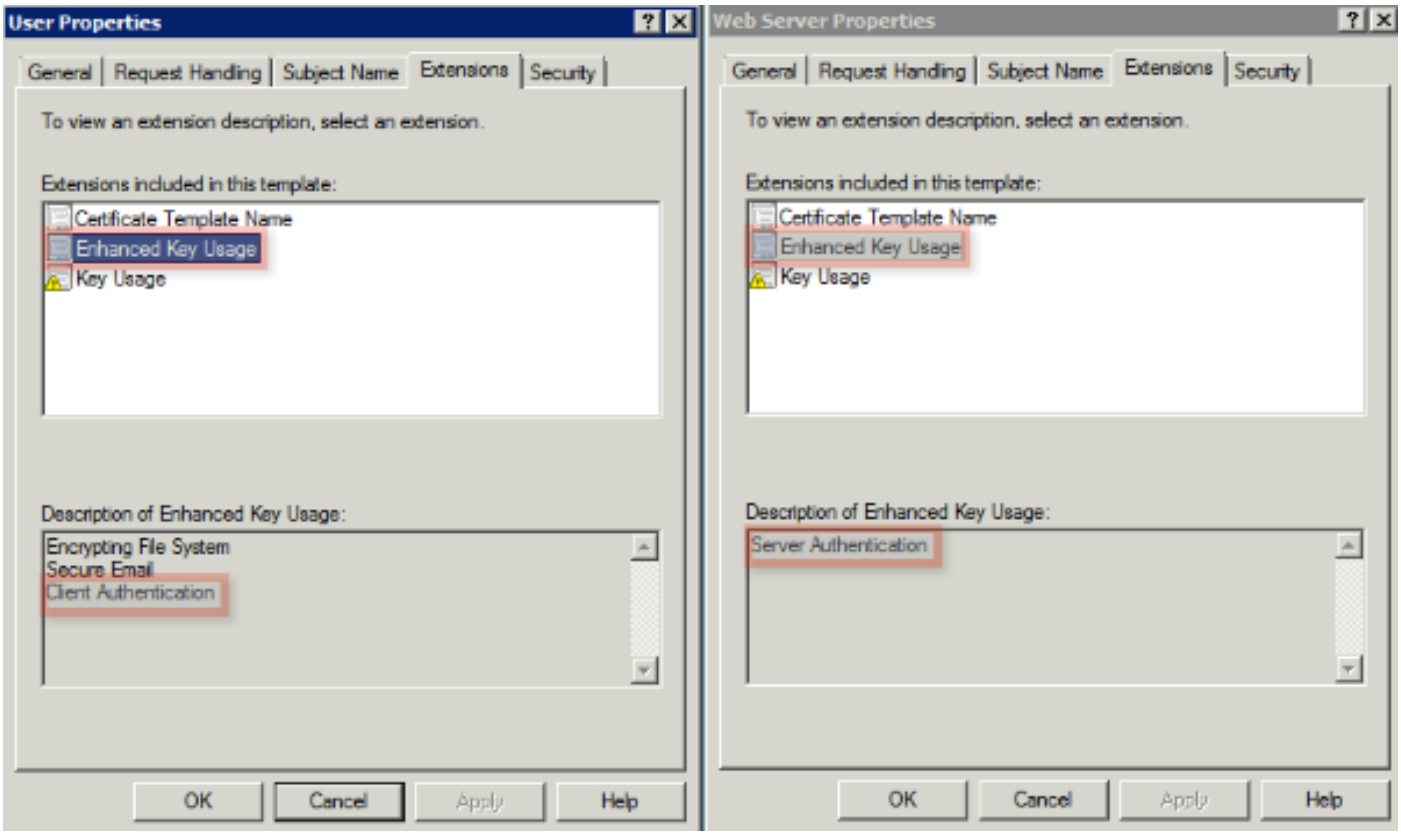
Os administradores de Microsoft CA podem configurar uns ou vários moldes que são usados a fim aplicar políticas do aplicativo a um grupo comum de Certificados. Estas políticas ajudam a identificar para que função o certificado e as chaves associadas são usados. Os valores de política do aplicativo são contidos no campo chave prolongado do uso (EKU) do certificado. O autenticador analisa gramaticalmente os valores no campo EKU a fim assegurar-se de que o certificado apresentado pelo cliente possa ser usado para a função pretendida. Alguns de mais usos comuns incluem a autenticação de servidor, a authenticação do cliente, o IPSec VPN, e o email. Em termos do ISE, os valores mais de uso geral EKU incluem o server e/ou a

authenticação do cliente.

Quando você consulta a um Web site seguro do banco, por exemplo, o servidor de Web que processa o pedido está configurado com um certificado que tenha uma política do aplicativo da autenticação de servidor. Quando o server recebe um pedido HTTPS, envia um certificado de autenticação de servidor ao navegador da Web de conexão para a autenticação. O ponto importante aqui é que esta é uma troca unidirecional do server ao cliente. Porque se relaciona ao ISE, um uso comum para um certificado de autenticação de servidor é acesso de GUI admin. O ISE envia o certificado configurado ao navegador conectado e não o espera receber para trás um certificado do cliente.

Quando se trata dos serviços tais como BYOD que usam o EAP-TLS, a autenticação mútua é preferida. A fim permitir esta troca bidirecional do certificado, o molde usado a fim gerar o certificado de identidade ISE deve possuir uma política mínima do aplicativo da autenticação de servidor. O molde de certificado do servidor de Web satisfaz esta exigência. O molde de certificado que gerencie os Certificados do valor-limite deve conter uma política mínima do aplicativo da authenticação do cliente. O molde do certificado de usuário satisfaz esta exigência. Se você configura o ISE para serviços tais como o ponto Inline do reforço de política (iPEP), o molde usado a fim gerar o certificado de identidade do server ISE deve conter ambos os atributos da autenticação de cliente e servidor se você usa a versão 1.1.x ou anterior ISE. Isto permite que o admin e os Nós inline autentiquem-se mutuamente. A validação EKU para o iPEP foi removida na versão 1.2 ISE, que faz esta exigência menos relevante.

Você pode reutilizar os moldes do servidor de Web e do usuário de Microsoft CA do padrão, ou você pode clonar e criar um molde novo com o processo que é esboçado neste documento. Baseado nestas exigências do certificado, a configuração de CA e o ISE resultante e os Certificados do valor-limite devem com cuidado ser planejados a fim minimizar todas as mudanças de configuração não desejada quando instalados em um ambiente de produção.



Configuração do molde de certificado

Como referido na introdução, o SCEP é amplamente utilizado em ambientes do IPSec VPN. Em consequência, a instalação do papel NDE configura automaticamente o server para utilizar o molde do **IPsec (pedido autônomo)** para o SCEP. Devido a isto, uma das primeiras etapas na preparação de Microsoft CA para BYOD é construir um molde novo com a política correta do aplicativo. Em um desenvolvimento autônomo, a autoridade de certificação e os serviços NDE são arranjados no mesmo server, e os moldes e as alterações exigidas do registro são contidos ao mesmo server. Em um desenvolvimento distribuído NDE, as alterações do registro são feitas no server NDE; contudo, os moldes reais são definidos no server de CA da raiz ou da secundário-raiz especificados na instalação do serviço NDE.

Termine estas etapas a fim configurar o molde de certificado:

1. Entre ao server de CA como o **admin**.

2. Clique o **Iniciar > Ferramentas Administrativas >** a **autoridade de certificação**.

3. Expanda os detalhes do server de CA e selecione o dobrador dos **moldes de certificado**. Este dobrador contém uma lista dos moldes que são permitidos atualmente.

4. A fim controlar os moldes de certificado, para clicar com o botão direito no dobrador dos **moldes de certificado** e para escolher **controle**.

5. **No console dos moldes de certificado**, um número de moldes inativos são indicados.

6. A fim configurar um molde novo para o uso com SCEP, clicar com o botão direito em um molde que já exista, como o **usuário**, e escolha o **molde duplicado**.

7. Escolha **Windows 2003** ou **Windows 2008**, dependente do OS mínimo de CA no ambiente.

8. **No tab geral**, adicionar um nome do indicador, tal como ISE-BYOD, e o período de validade; deixe todas as outras opções desmarcadas.
   Nota: O período de validade do molde deve ser inferior ou igual ao período de validade dos Certificados da raiz e do intermediário de CA.
9. Clique sobre a aba do **nome do sujeito**, e confirme que a **fonte no pedido** está selecionada.

10. Clique sobre a aba das **exigências da emissão**. Cisco recomenda que você deixa a placa das **políticas da emissão em um** ambiente hierárquico típico de CA.

11. Clique sobre a aba dos **Ramais**, **políticas do aplicativo**, e **edite-a** então.

12. O clique **adiciona**, e assegura-se de que a **authenticação do cliente** esteja adicionada como uma política do aplicativo. Clique em **OK**.

13. Clique sobre a **ABA de segurança**, e **adicionar-la** então**….** Assegure-se de que a conta de serviço SCEP definida na instalação do serviço NDE tenha o controle total do molde, e clique-se então a **APROVAÇÃO**.

14. Retorne à **interface GUI da autoridade de certificação**.

15. Clicar com o botão direito no diretório dos **moldes de certificado**. Navegue a **novo > molde de certificado a emitir**.

16. Selecione o molde **ISE-BYOD** configurado previamente, e clique a **APROVAÇÃO**.

    Nota: Alternativamente, você pode permitir o molde através do CLI com o **certutil -** comando de **SetCAtemplates +ISE-BYOD**.
    O molde ISE-BYOD deve agora ser alistado na lista permitida do molde de certificado.

Configuração do registro do molde de certificado

Termine estas etapas a fim configurar as chaves de registro do molde de certificado:

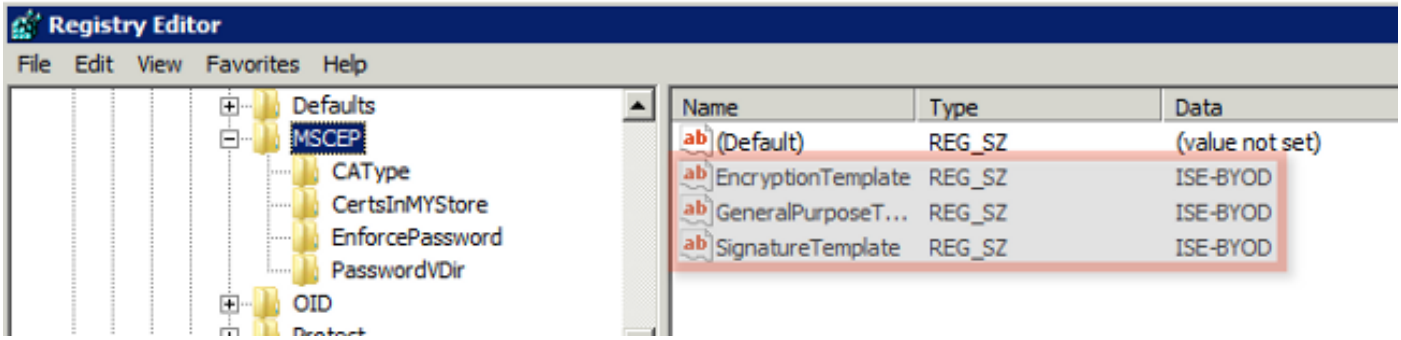
1. Conecte aos NDE o server.

2. Clique o **começo** e incorpore o **regedit à** barra da busca.

3. Navegue ao **computador** > ao **HKEY_LOCAL_MACHINE** > ao **SOFTWARE** > ao **Microsoft** > à **criptografia** > ao **MSCEP**.

4. Mude as chaves de **EncryptionTemplate**, de **GeneralPurposeTemplate**, e de **SignatureTemplate do IPsec (pedido autônomo) ao** molde **ISE-BYOD** criado previamente.

5. Recarregue o server NDE a fim aplicar a configuração de registro.



Configurar o ISE como um proxy SCEP

Em um desenvolvimento BYOD, o valor-limite não se comunica diretamente com o server backend NDE. Em lugar de, o nó da política ISE é configurado como um proxy SCEP e comunica-se com o server NDE em nome dos valores-limite. Os valores-limite comunicam-se diretamente com o ISE. O exemplo IIS no server NDE pode ser configurado a fim apoiar emperramentos HTTP e/ou HTTPS para os diretórios virtuais SCEP.

Termine estas etapas a fim configurar o ISE como um proxy SCEP:

1. Log no **ISE GUI** com credenciais admin.

2. **A administração do** clique, **Certificados**, e então **perfis SCEP CA**.

3. Clique em Add.

4. Incorpore o nome do servidor e a descrição.

5. Incorpore a URL para o server SCEP com o IP ou nome de domínio totalmente qualificado (FQDN) (http://10.10.10.10/certsrv/mscep/, por exemplo).

6. Clique a **Conectividade do teste**. Uma conexão bem sucedida conduz a uma mensagem bem sucedida do PNF-acima da resposta de servidor.

7. **Salvaguarda do** clique a fim aplicar a configuração.

8. A fim verificar, para clicar a **administração**, os **Certificados**, **Certificate a loja,** e confirmam que o certificado do server RA SCEP NDE esteve transferido automaticamente ao nó ISE.

Verificar

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

Troubleshooting

Use esta seção para fazer o troubleshooting da sua configuração.

Geral pesquise defeitos notas

Está aqui uma lista de observações importantes que você pode usar a fim pesquisar defeitos sua configuração:

- Divida a topologia de rede BYOD em pontos intermediários lógicos a fim ajudar a identificar debugam e capturam pontos ao longo do trajeto entre os valores-limite ISE, NDE, e de CA.
- Assegure-se de que isso o nó e CA ISE compartilhem de um origem de tempo comum do Network Time Protocol (NTP).
- Os valores-limite devem poder ajustar automaticamente sua hora com as opções NTP e de zona de hora (fuso horário) aprendidas do DHCP.
- O servidor DNS do cliente deve poder resolver o FQDN do nó ISE.
- Assegure-se de que o TCP 80 e/ou o TCP 443 estejam permitidos bidirecional entre o ISE e o server NDE.
- Teste com uma máquina de Windows devido ao registro melhorado do lado do cliente. Opcionalmente, use um iDevice de Apple junto com o utilitário de configuração do iPhone de Apple a fim monitorar logs do console do lado do cliente.
- Monitore logs do aplicativo de servidor de CA e NDE para erros de registro, e use Google ou TechNet a fim pesquisar aqueles erros.

- Ao longo da fase de teste, use o HTTP para o SCEP a fim facilitar capturas de pacote de informação entre o ISE, os NDE, e o CA.

- Use a utilidade da descarga TCP no nó do serviço da política ISE (PSN), e monitore o tráfego a e do server NDE. Isto é ficado situado sob **operações > ferramentas de diagnóstico > ferramentas gerais**.

- Instale Wireshark no server de CA e NDE, ou use o PERÍODO no Switches intermediário, a fim capturar o tráfego SCEP a e do ISE PSN.

- Assegure-se de que a corrente de certificado de CA apropriada esteja instalada no nó da política ISE para a autenticação dos certificados de cliente.

- Assegure-se de que a corrente de certificado de CA apropriada esteja instalada automaticamente nos clientes durante onboarding.

- Inspecione os certificados de identidade ISE e de valor-limite e confirme que os atributos corretos EKU estam presente.

- Monitore a autenticação viva entra o ISE GUI para falhas da authentication e autorização. Nota: Alguns suplicantes não inicializam uma troca do certificado de cliente se o EKU errado esta presente, como um certificado de cliente com o EKU da autenticação de servidor. Consequentemente, as falhas de autenticação não puderam estam presente sempre nos logs ISE.
- Quando os NDE são instalados em um desenvolvimento distribuído, uma raiz ou uma secundário-raiz remota CA estarão designadas pelo nome ou pelo nome de computador de CA na instalação do serviço. O server NDE envia requisições de registro do certificado a este server de CA do alvo. Se o processo de registro do certificado do valor-limite falha, as capturas de pacote de informação (PCAP) puderam mostrar ao retorno do server NDE um erro **404 não encontrado ao** nó ISE. A fim resolver esta edição, reinstale o serviço NDE e selecione a opção do nome de computador em vez do nome de CA.

- Evite alterações à corrente SCEP CA depois que os dispositivos onboarded. O valor-limite OS, tais como o iOS de Apple, não atualiza automaticamente um perfil previamente instalado BYOD. Neste exemplo iOS, o perfil atual deve ser suprimido do valor-limite, e do valor-limite removido do base de dados ISE, de modo que onboarding possa ser executado outra vez.

- Você pode configurar um Microsoft certificate server a fim conectar ao Internet e atualizar automaticamente Certificados do programa do certificado de raiz de Microsoft. Se você configura esta opção da recuperação da rede nos ambientes com políticas de internet restritas, os server CA/NDES que não podem conectar ao Internet podem tomar 15 segundos ao intervalo à revelia. Isto pode adicionar um atraso 15-second ao processamento de pedidos SCEP dos proxys SCEP tais como o ISE. O ISE é pedidos programados do intervalo SCEP após 12 segundos se uma resposta não é recebida. A fim resolver esta edição, permite o acesso ao Internet para os server CA/NDES, ou altera as configurações de timeout da recuperação da rede na política de segurança local dos server de Microsoft CA/NDES. A fim encontrar esta configuração no servidor Microsoft, navegue às **políticas do Iniciar >**

Ferramentas Administrativas > da política > da chave pública de segurança local > aos ajustes da validação de caminho do certificado > à recuperação da rede.

Registro do lado do cliente

Está aqui uma lista de técnicas úteis que são usadas a fim pesquisar defeitos edições de registro do lado do cliente:

- Incorpore o **comando do log %temp% \ spwProfileLog.txt** a fim ver os logs do lado do cliente para aplicativos do Windows de Mircosoft.
  Nota: WinHTTP é usado para a conexão entre o valor-limite de Microsoft Windows e o ISE. Proveja o artigo dos Mensagens de Erro de Microsoft Windows para uma lista de códigos de erro.
- Incorpore o comando de **/sdcards/downloads/spw.log** a fim ver os logs do lado do cliente para aplicativos de Android.

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

- Para o **iOS de Apple**, use o configurador 2.0 de Apple a fim ver mensagens.

Registro ISE

Termine estas etapas a fim ver o log ISE:

1. Navegue à **administração > registrando > debugam a configuração do log**, e selecionam o nó apropriado da política ISE.

2. Ajuste o **cliente** e os logs do **abastecimento** para debugar ou seguir, como necessário.

3. Reproduza o problema e documente a informação relevante da semente a fim facilitar procurar, como o MAC, o IP, e o usuário.

4. Navegue às **operações** > aos **logs da transferência**, e selecione o nó apropriado ISE.

5. **Nos logs debugar** catalogue, transfira os logs nomeados **ise-psc.log ao** desktop.

6. Use um editor inteligente, tal como o bloco de notas ++ a fim analisar gramaticalmente os arquivos de registro.

7. Quando a edição foi isolada, a seguir retorne os níveis do log ao nível padrão.

NDE que registram e que pesquisam defeitos

Para mais informação, refira o AD CS: Pesquisando defeitos o artigo de Windows Server do serviço do registro do dispositivo de rede.

Informações Relacionadas

- Guia das soluções BYOD - Configuração do servidor do Certificate Authority
- Vista geral NDE em Windows 2008 R2
- White Paper MSCEP
- Configurando o server NDE para apoiar o SSL
- Exigências do certificado quando você usar o EAP-TLS ou o PEAP com EAP-TLS
- Suporte técnico & documentação