ASA 8.x: configuração de SmartCards CAC de VPN SSL do AnyConnect para Windows

Contents

Introdução

Este documento fornece uma configuração de exemplo no Cisco Adaptive Security Appliance (ASA) para o acesso remoto a AnyConnect VPN para Windows com a placa comum do acesso (CAC) para a autenticação.

O escopo deste documento é cobrir a configuração do Cisco ASA com Adaptive Security Device Manager (ASDM), Cisco AnyConnect VPN Client e Microsoft Ative Diretory (AD)/Lightweight Diretory Access Protocol (LDAP).

A configuração neste guia usa o servidor Microsoft AD/LDAP. Este documento também aborda recursos avançados como OCSP, mapas de atributos LDAP e Políticas de acesso dinâmico (DAP).

Pré-requisitos

Requisitos

Uma compreensão básica do Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP e Public Key Infrastructure (PKI) é benéfica na compreensão da configuração completa. A familiaridade com a associação de grupo do AD, as propriedades do usuário e os objetos LDAP ajudam na correlação do processo de autorização entre os atributos do certificado e os objetos do AD/LDAP.

Componentes Utilizados

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) que executa a versão de software 8.0(x) e posterior
- Cisco Adaptive Security Device Manager (ASDM) versão 6.x para ASA 8.x

- Cisco AnyConnect VPN Client para Windows

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.

Configuração do Cisco ASA

Esta seção aborda a configuração do Cisco ASA via ASDM. Ele aborda as etapas necessárias para implantar um túnel de acesso remoto VPN por meio de uma conexão AnyConnect SSL. O certificado CAC é usado para autenticação e o atributo UPN no certificado é preenchido no Ative Diretory para autorização.

Considerações de implantação

- Este guia NÃO aborda configurações básicas, como interfaces, DNS, NTP, roteamento, acesso a dispositivos, acesso ASDM e assim por diante. Supõe-se que o operador de rede esteja familiarizado com essas configurações.

  Consulte Dispositivos de segurança multifuncionais para obter mais informações.

- As seções destacadas em VERMELHO são configurações obrigatórias necessárias para o acesso básico à VPN. Por exemplo, um túnel VPN pode ser configurado com a placa CAC sem fazer verificações de OCSP, mapeamentos LDAP e verificações de Política de Acesso Dinâmico (DAP). O DoD exige a verificação do OCSP, mas o túnel funciona sem o OCSP configurado.

- As seções destacadas em AZUL são recursos avançados que podem ser incluídos para adicionar mais segurança ao design.

- O ASDM e o AnyConnect/SSL VPN não podem usar as mesmas portas na mesma interface. É recomendável alterar as portas em uma ou outra para obter acesso. Por exemplo, use a porta 445 para ASDM e deixe 443 para AC/SSL VPN. O acesso ao URL do ASDM foi alterado no 8.x. Use `https://<ip_address>:<port>/admin.html`.

- A imagem do ASA necessária é pelo menos 8.0.2.19 e ASDM 6.0.2.

- O AnyConnect/CAC é compatível com o Vista.

- Consulte o Apêndice A para obter exemplos de mapeamento de LDAP e de política de acesso dinâmico para aplicação de política adicional.

- Consulte o Apêndice D para saber como verificar objetos LDAP em MS.

- Consulte Informações Relacionadas para obter uma lista de portas de aplicativos para a configuração do firewall.

Configuração de Autenticação, Autorização, Tarifação (AAA - Authentication, Authorization, Accounting)

Você é autenticado com o uso do certificado em seu Cartão de Acesso Comum (CAC) através do Servidor de Autoridade de Certificação (CA) DISAC ou do servidor de CA de sua própria organização. O certificado deve ser válido para acesso remoto à rede. Além da autenticação, você também deve estar autorizado a usar um objeto do Microsoft Ative Diretory ou do Lightweight Diretory Access Protocol (LDAP). O Department of Defense (DoD) requer o uso do atributo UPN para autorização, que faz parte da seção SAN (Nome Alternativo do Assunto) do certificado. O UPN ou EDI/PI deve estar neste formato, 1234567890@mil. Essas configurações mostram como configurar o servidor AAA no ASA com um servidor LDAP para autorização. Consulte o Apêndice A para obter configurações adicionais com mapeamento de objeto LDAP.

Configurar servidor LDAP

Conclua estes passos:

1. Selecione Remote Access VPN > AAA Setup > AAA Server Group.
2. Na tabela de grupos de servidores AAA, clique em Add 3.
3. Insira o nome do grupo de servidores e escolha LDAP no botão de opção de protocolo. Consulte a Figura 1.
4. Em Servidores na tabela de grupos selecionada, clique em Adicionar. Verifique se o servidor criado está realçado na tabela anterior.
5. Na janela de edição do servidor AAA, conclua estas etapas. Consulte a Figura 2.

Observação: escolha a opção Ativar LDAP sobre SSL se o LDAP/AD estiver configurado para esse tipo de conexão.

---

a. Escolha a interface onde o LDAP está localizado. Este guia mostra o interior da interface.

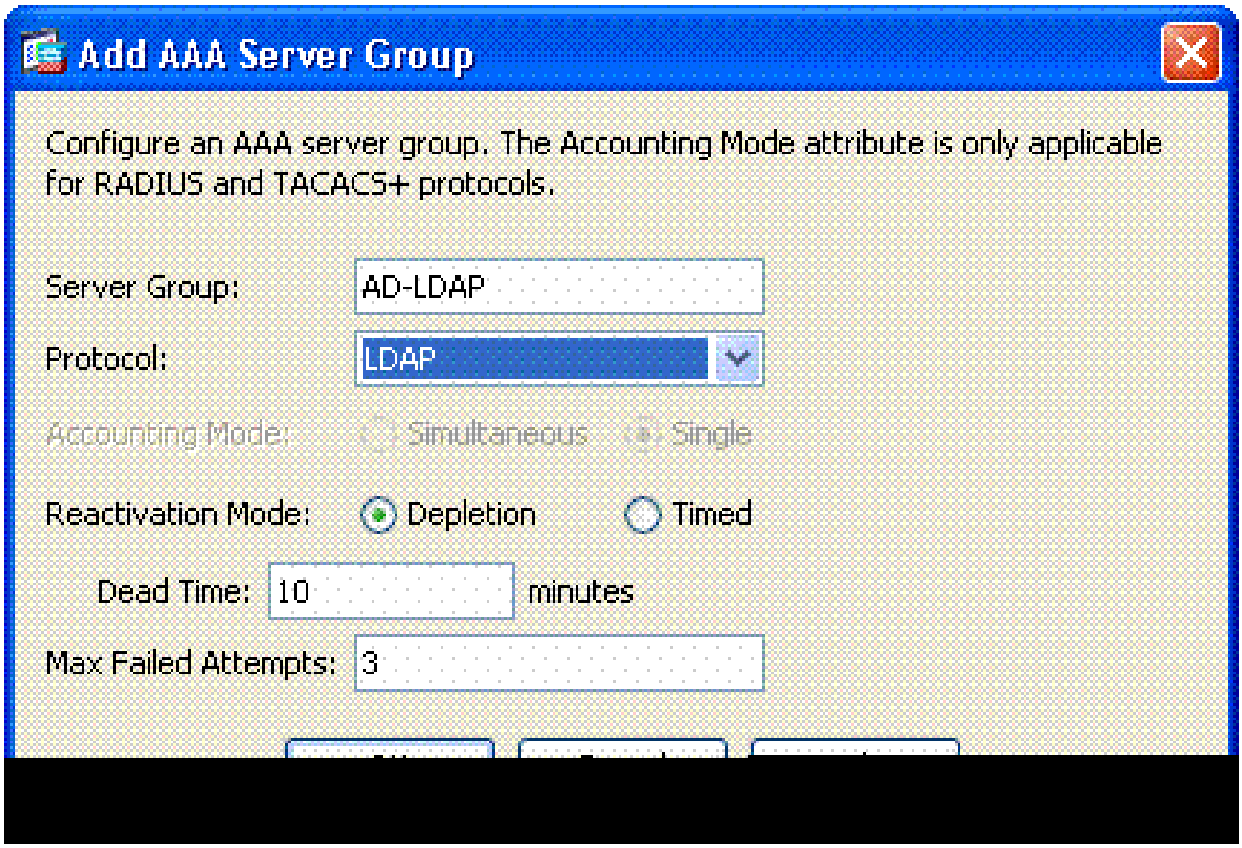
b. Insira o endereço IP do servidor.

c. Digite server port. A porta LDAP padrão é 389.

d. Escolha Tipo de servidor.

e. Digite DN base. Pergunte esses valores ao administrador do AD/LDAP.

Figura -1



f. Na opção scope, escolha a resposta apropriada. Isso depende do DN base. Peça ajuda ao administrador do AD/LDAP.

g. No atributo de nomeação, insira userPrincipalName. Este é o atributo usado para autorização do usuário no servidor AD/LDAP.

h. No DN de Login, insira o DN do administrador.

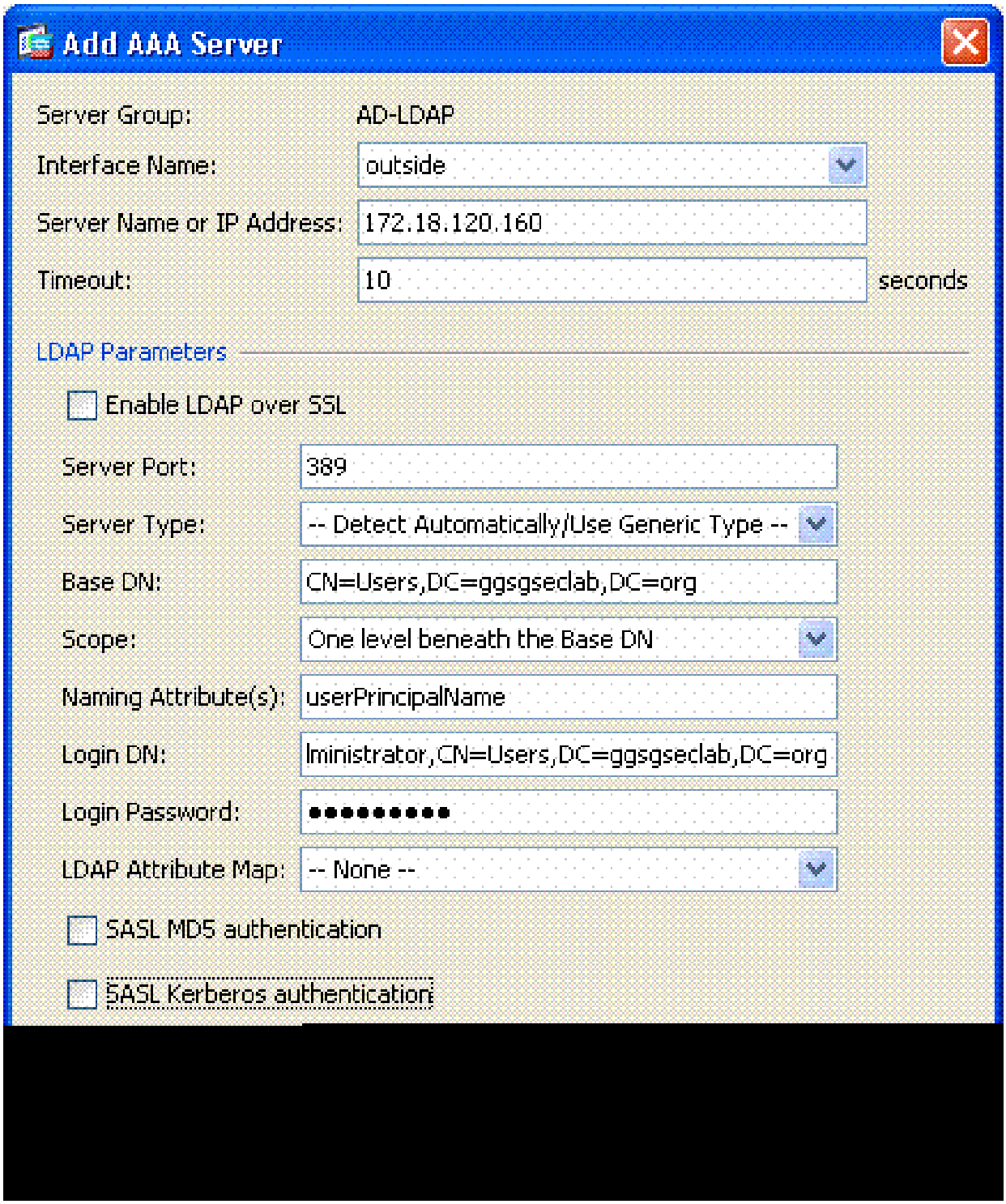
Observação: você tem direitos administrativos ou direitos para exibir/pesquisar a estrutura LDAP que inclui objetos de usuário e associação de grupo.

---

i. Em Senha de login, digite a senha do administrador.

j. Deixe o atributo LDAP como none.

Figura -2



> Observação: use esta opção posteriormente na configuração para adicionar outro objeto AD/LDAP para autorização.

k. Escolha OK.

6. Escolha OK.

Gerenciar certificados

Há duas etapas para instalar certificados no ASA. Primeiro, instale os certificados de CA (Root

and Subordinate Certificate Authority) necessários. Em segundo lugar, inscreva o ASA em uma CA específica e obtenha o certificado de identidade. O DoD PKI utiliza esses certificados, Raiz CA2, Raiz Classe 3, CA## Intermediário no qual o ASA está inscrito, certificado de ID do ASA e certificado OCSP. Mas, se você optar por não usar o OCSP, o certificado OCSP não precisará ser instalado.

Observação: entre em contato com a POC de segurança para obter certificados raiz, bem como instruções sobre como se inscrever para obter um certificado de identidade para um dispositivo. Um certificado SSL deve ser suficiente para o ASA para acesso remoto. Um certificado SAN duplo não é necessário.

Observação: a máquina local também precisa ter a cadeia de CA do DoD instalada. Os certificados podem ser visualizados no Repositório de Certificados da Microsoft com o Internet Explorer. O DoD produziu um arquivo em lotes que adiciona automaticamente todas as CAs à máquina. Peça mais informações à POC PKI.

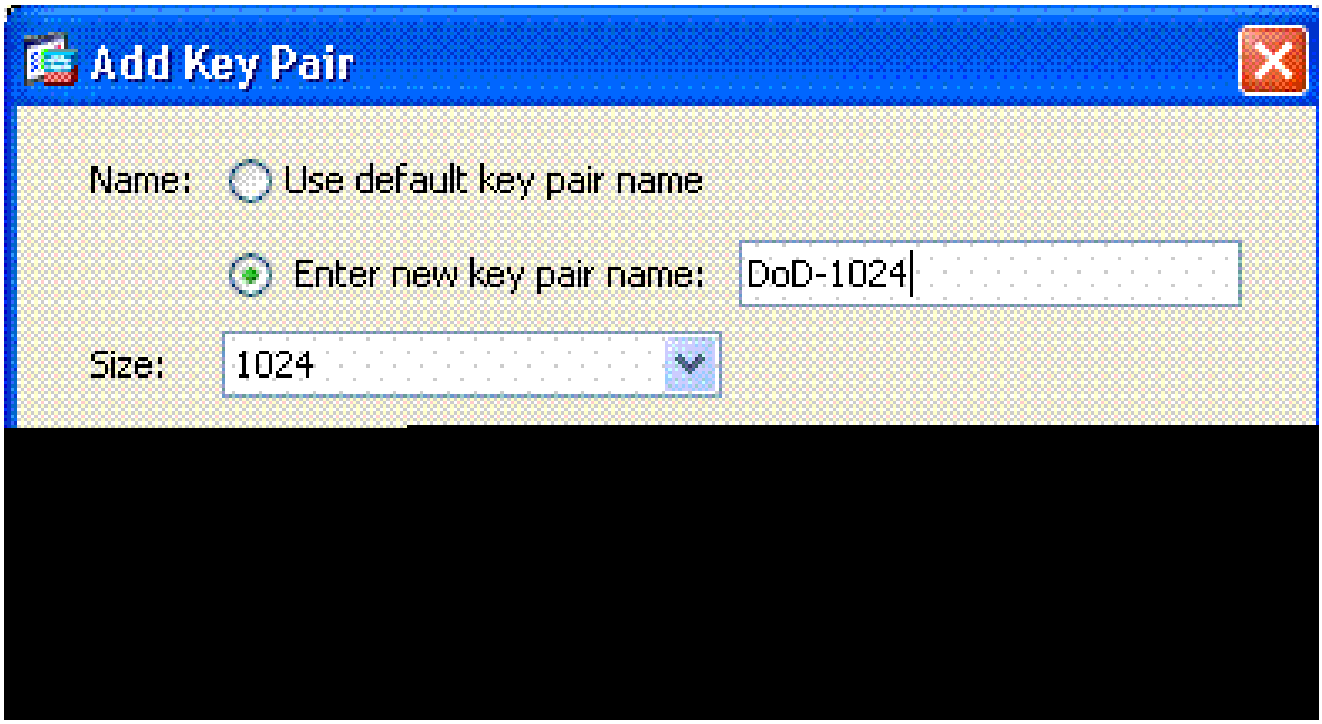
Observação: DoD CA2 e raiz de classe 3, bem como o ASA ID e CA intermediário que emitiu o certificado ASA devem ser as únicas CAs necessárias para autenticação de usuário. Todos os intermediários de CA atuais estão na cadeia raiz de CA2 e classe 3 e são confiáveis, desde que as raízes de CA2 e classe 3 sejam adicionadas.

Gerar chaves

Conclua estes passos:

1. Escolha Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Escolha Add a new id certificate e, em seguida, New pela opção de par de chaves.
3. Na janela Adicionar par de chaves, insira um nome de chave, DoD-1024. Clique no rádio para adicionar uma nova chave. Consulte a figura 3.

   Figure 3



4. Escolha o tamanho da chave.
5. Mantenha o uso de acordo com a finalidade geral.
6. Clique em Generate CSR (Gerar CSR).

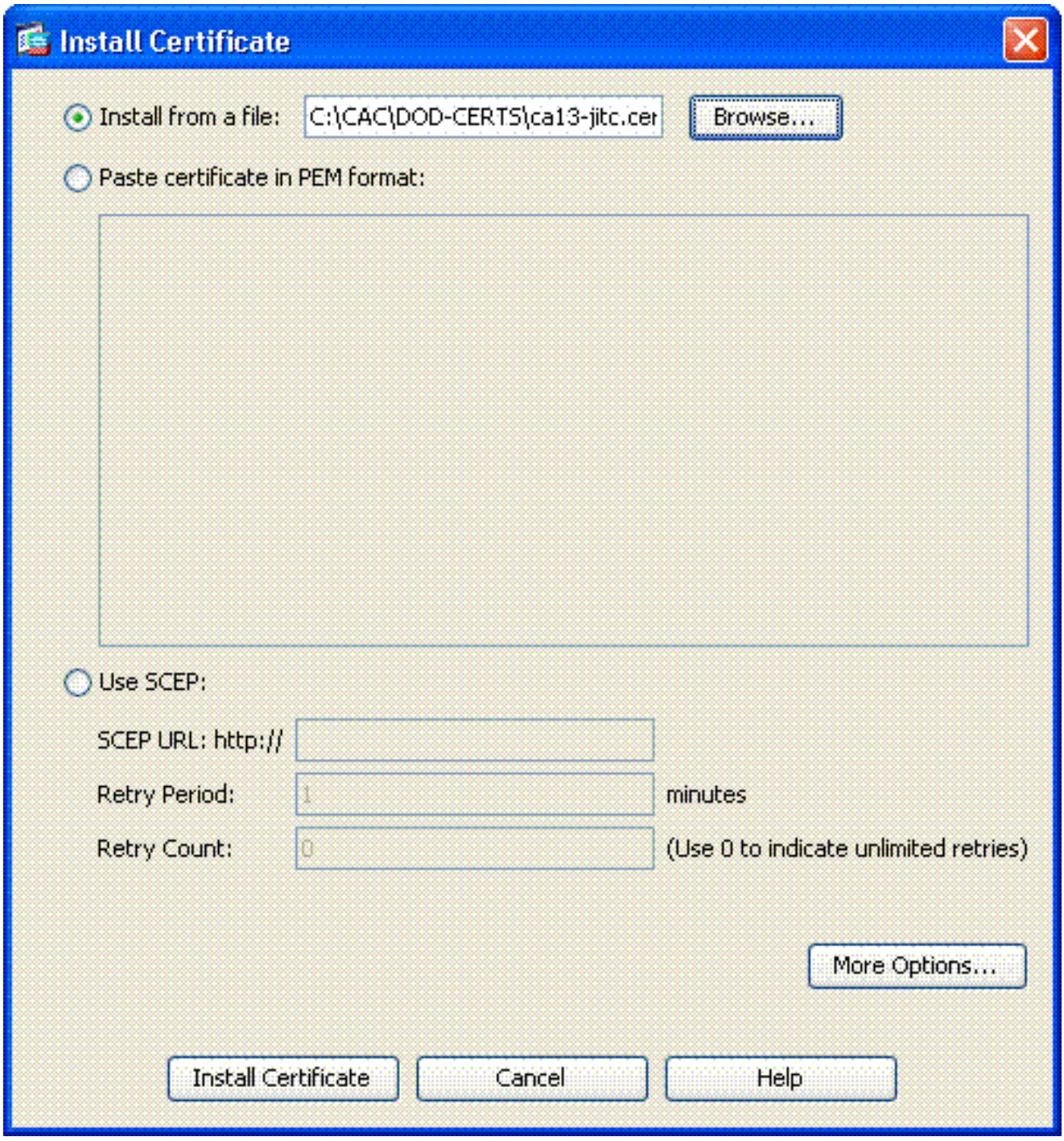
Observação: DoD Root CA 2 usa uma chave de 2048 bits. Uma segunda chave que usa um par de chaves de 2048 bits deve ser gerada para poder usar essa CA. Conclua as etapas anteriores acima para adicionar uma segunda chave.

Instalar Certificados CA Raiz

Conclua estes passos:

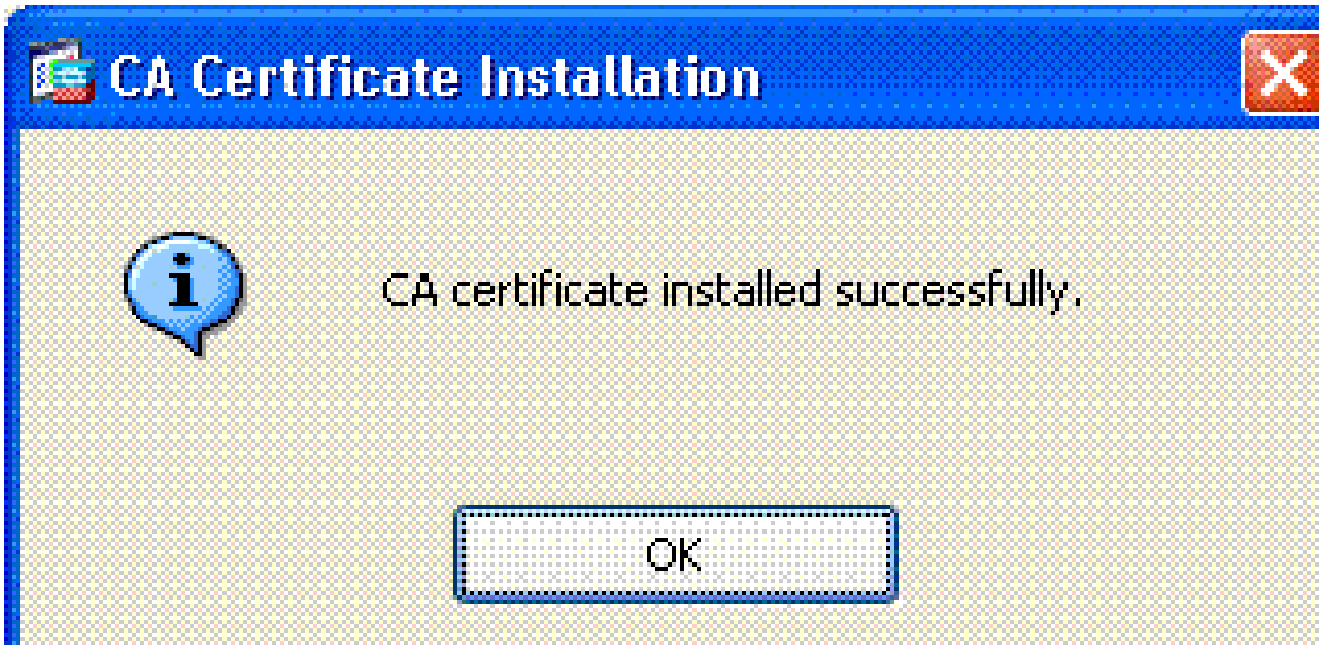
1. Escolha Remote Access VPN > Certificate Management > CA Certificate > Add.
2. Escolha Instalar do arquivo e navegue até o certificado.
3. Escolha Instalar certificado.

Figura 4: Instalação do certificado raiz



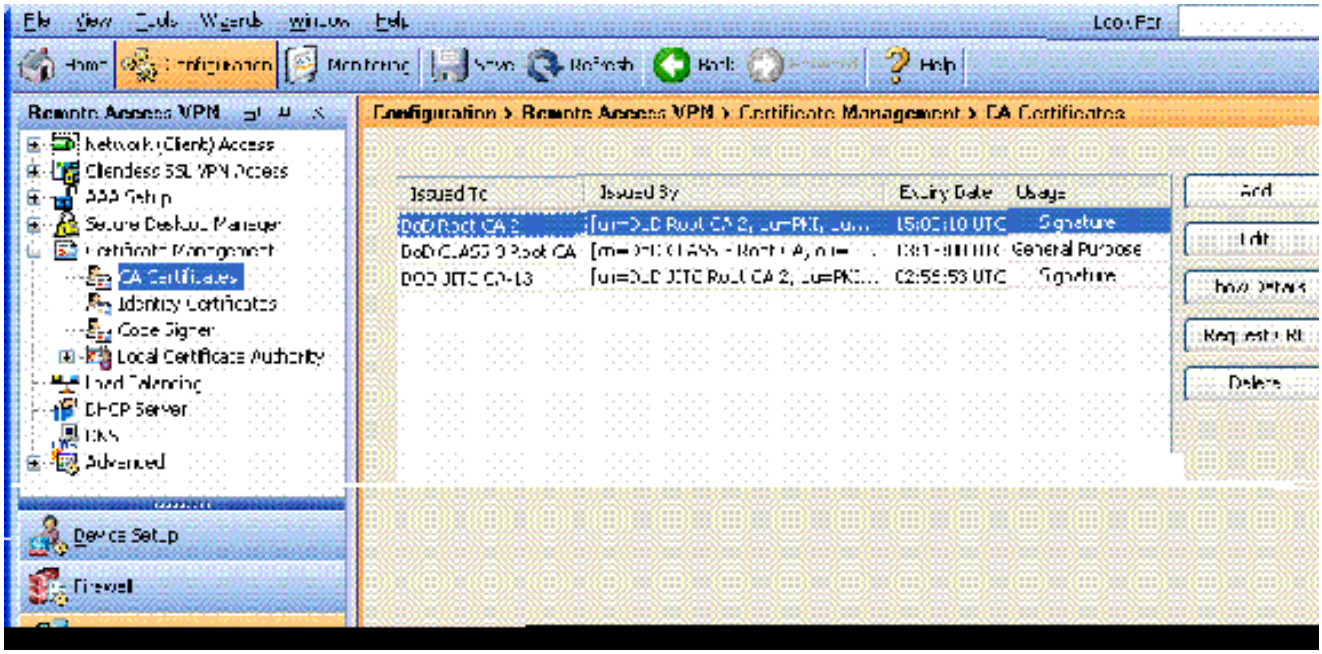
4. Essa janela deve ser exibida. Consulte a Figura 5.

Figure 5



Observação: repita as etapas de 1 a 3 para cada certificado que você deseja instalar. A PKI do DoD requer um certificado para cada um destes: CA 2 raiz, raiz classe 3, CA## intermediária, ID do ASA e servidor OCSP. O certificado OCSP não será necessário se você não usar o OCSP.

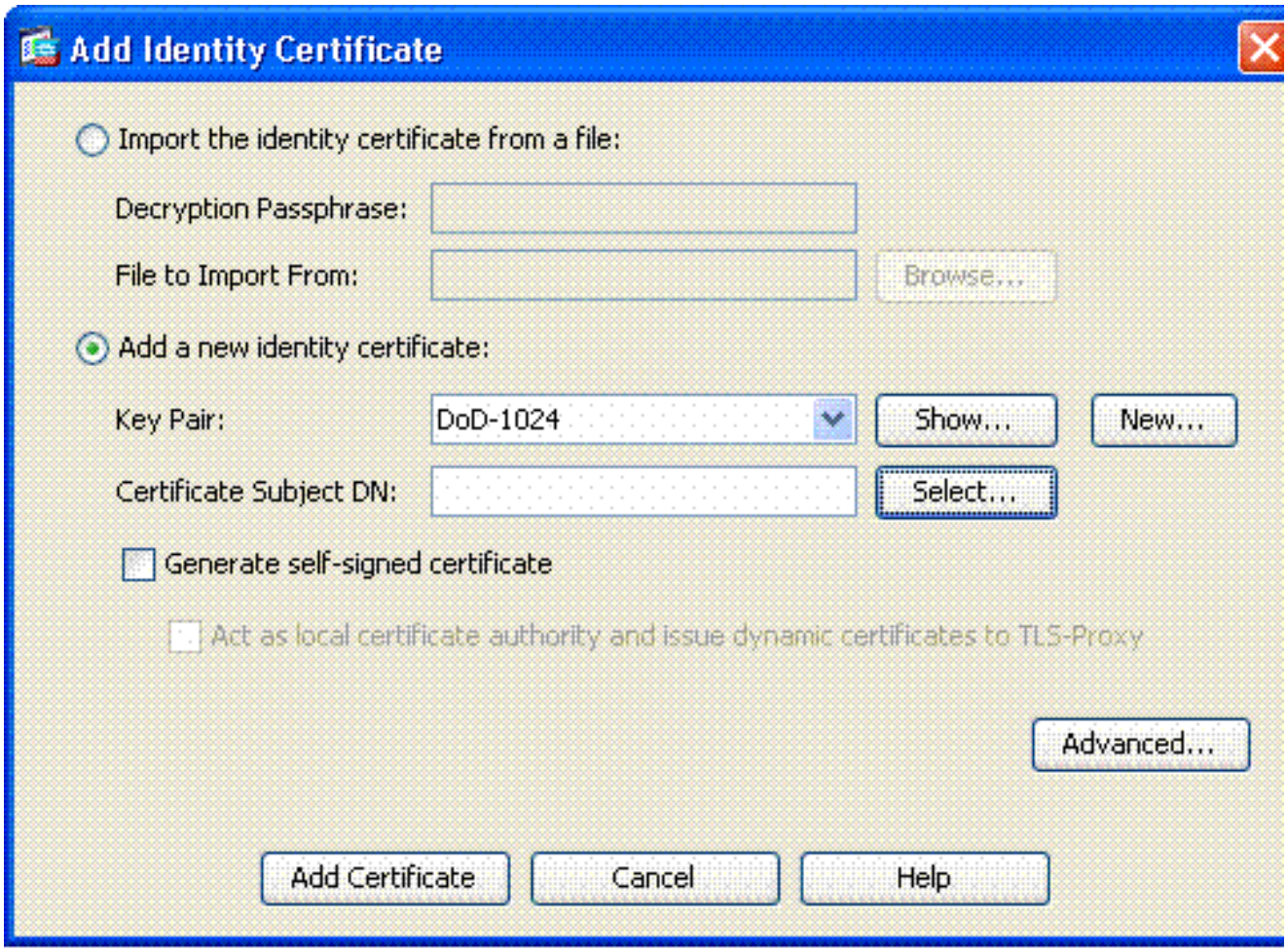
Figura 6: Instalação do certificado raiz



Inscrever o ASA e instalar o certificado de identidade

1. Escolha Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Escolha Adicionar um novo certificado de id.
3. Escolha o par de chaves DoD-1024. Consulte a figura 7

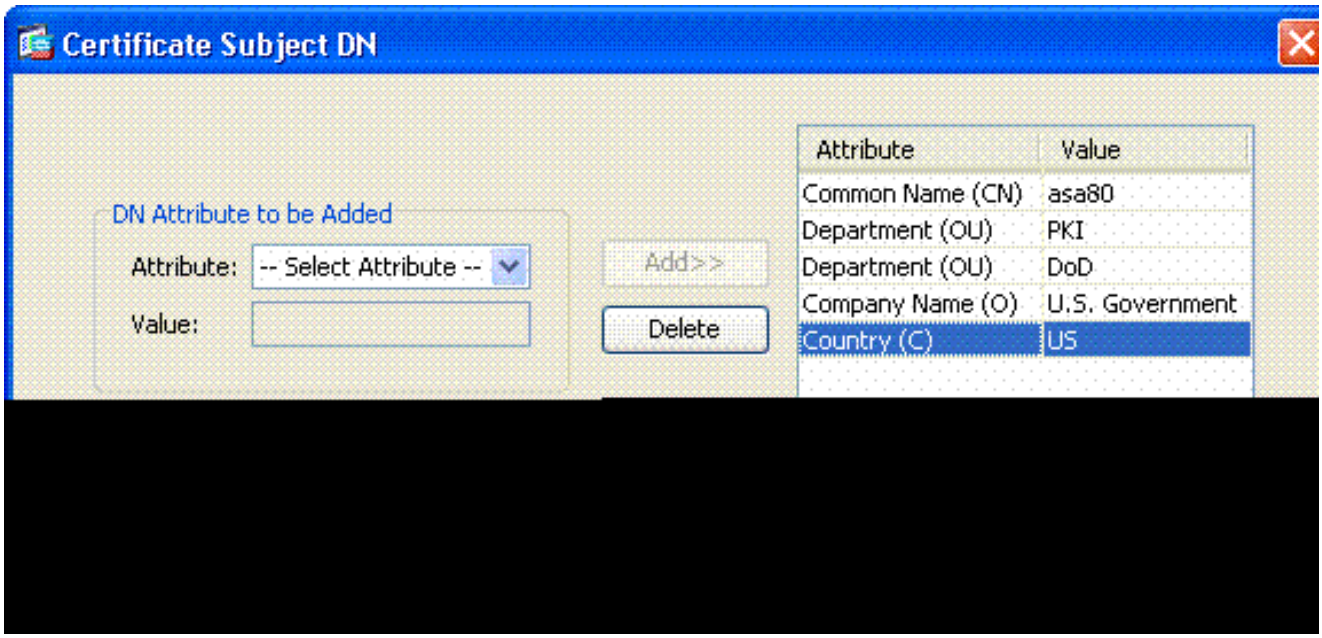
Figura 7: Parâmetros do certificado de identidade



4. Vá para a caixa DN do assunto do certificado e clique em Selecionar.

5. Na janela DN do assunto do certificado, digite as informações do dispositivo. Veja a Figura 8, por exemplo.

Figura 8: Editar DN



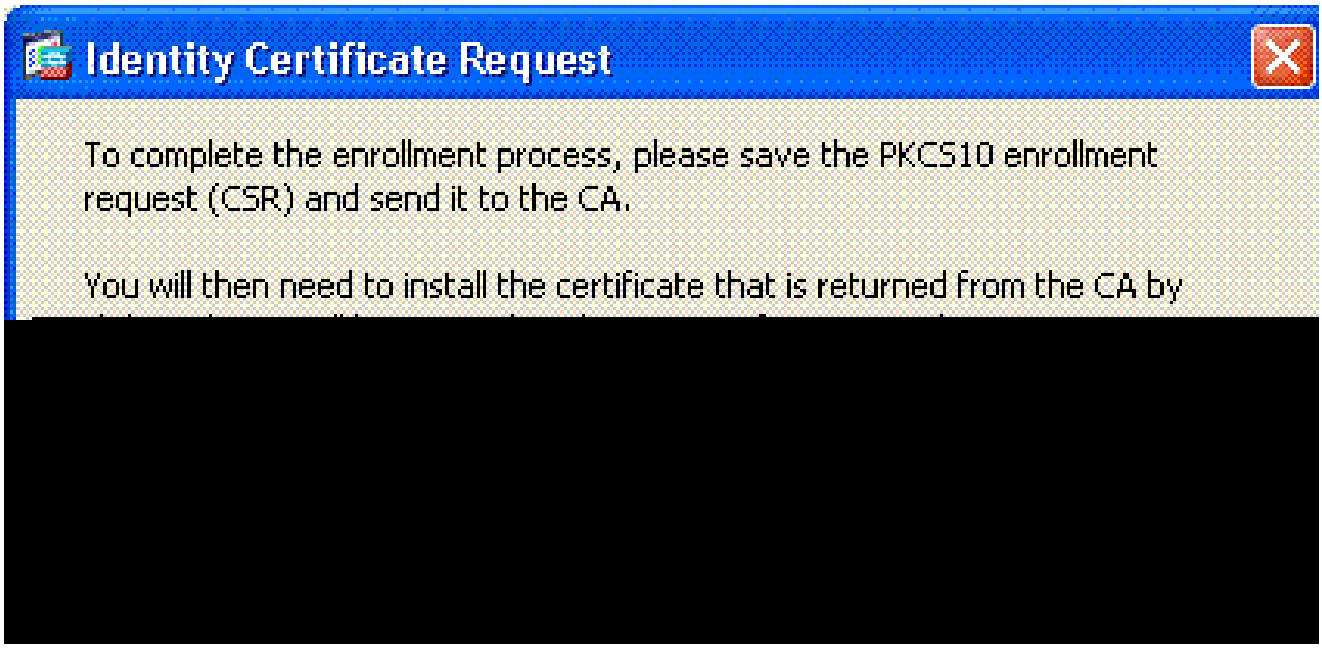
6. Escolha OK.

> Observação: certifique-se de usar o nome de host do dispositivo configurado em seu sistema ao adicionar o DN do assunto. A POC PKI pode informar os campos obrigatórios necessários.

7. Escolha Add certificate.

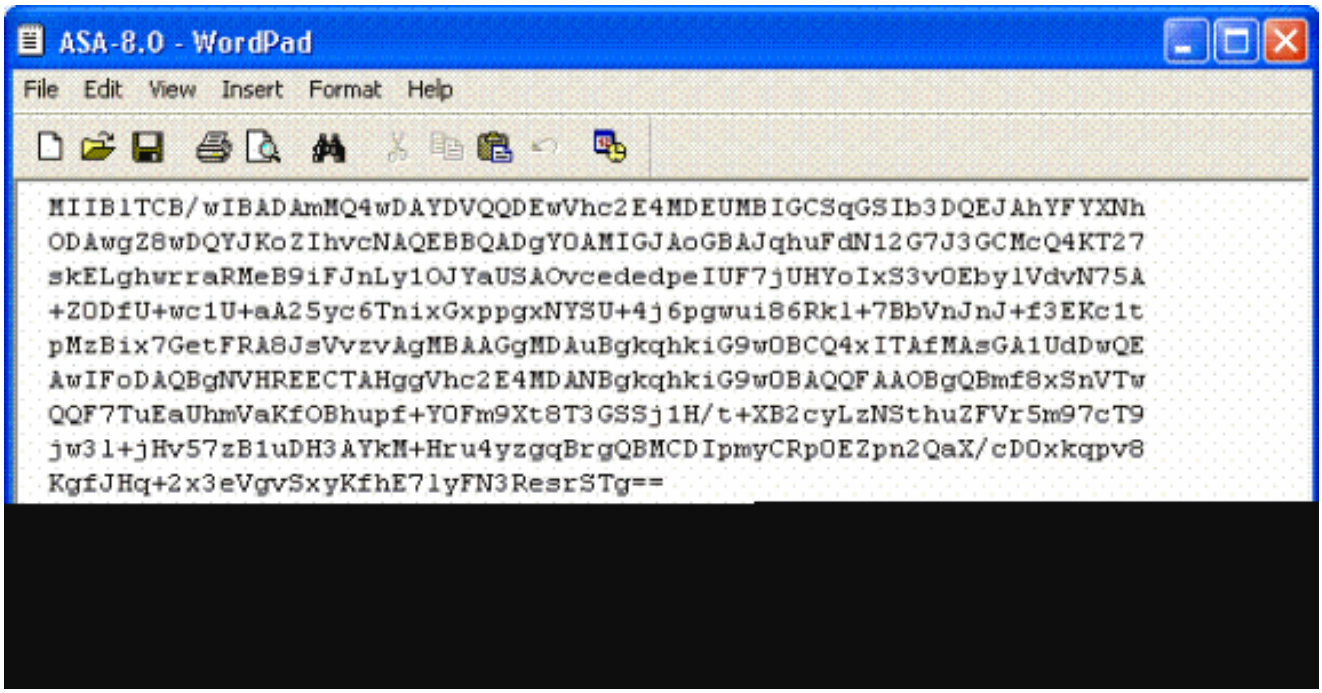
8. Clique em Browse para selecionar o diretório onde você deseja salvar a solicitação. Consulte a Figura 9.

   Figura 9: Solicitação de certificado



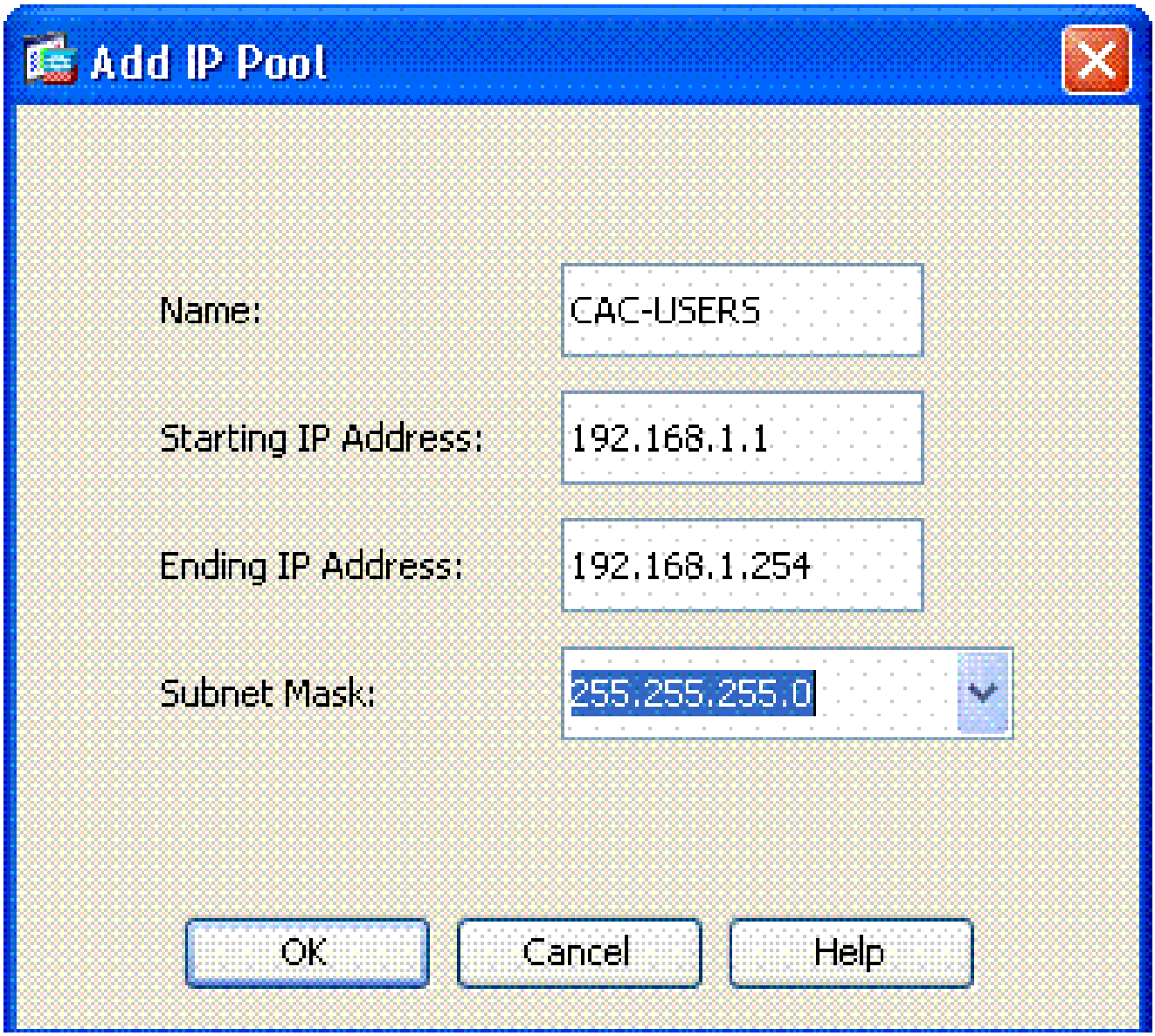
9. Abra o arquivo com o WordPad, copie a solicitação para a documentação apropriada e envie para o POC PKI. Consulte a Figura 10.

   Figura 10: Solicitação de inscrição



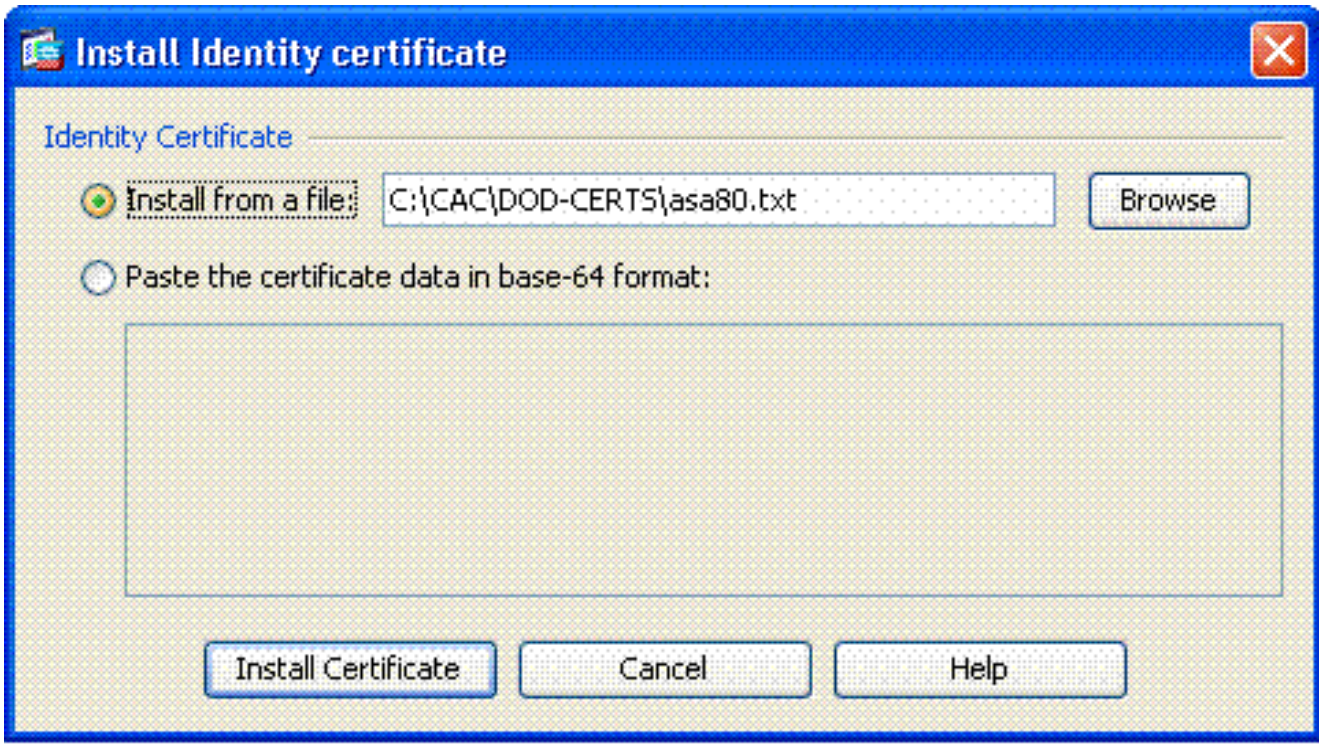
10. Depois de receber o certificado do administrador da autoridade de certificação, escolha Remote Access VPN > Certificate Management > ID Certificate > Install. Consulte a Figura 11.

    Figura 11: Importando o certificado de identidade



11. Na janela Instalar certificado, navegue até o certificado de ID e escolha Instalar certificado. Veja a Figura 12, por exemplo.

    Figura 12: Instalando o certificado de identidade



Observação: é recomendável exportar o ponto confiável do certificado de ID para salvar o certificado e os pares de chaves emitidos. Isso permite que o administrador do ASA importe o certificado e os pares de chaves para um novo ASA em caso de falha de RMA ou hardware. Consulte Exportando e Importando Pontos Confiáveis para obter mais informações.

Observação: clique em SAVE para salvar a configuração na memória flash.

Configuração do AnyConnect VPN

Há duas opções para configurar os parâmetros de VPN no ASDM. A primeira opção é usar o assistente de VPN SSL. Essa é uma ferramenta fácil de usar para usuários que não conhecem a configuração da VPN. A segunda opção é fazer isso manualmente e examinar cada opção. Este guia de configuração usa o método manual.

Observação: há dois métodos para levar o cliente AC ao usuário:

1. Você pode baixar o cliente do site da Cisco e instalá-lo em sua máquina.
2. O usuário pode acessar o ASA por meio de um navegador da Web e o cliente pode ser baixado.

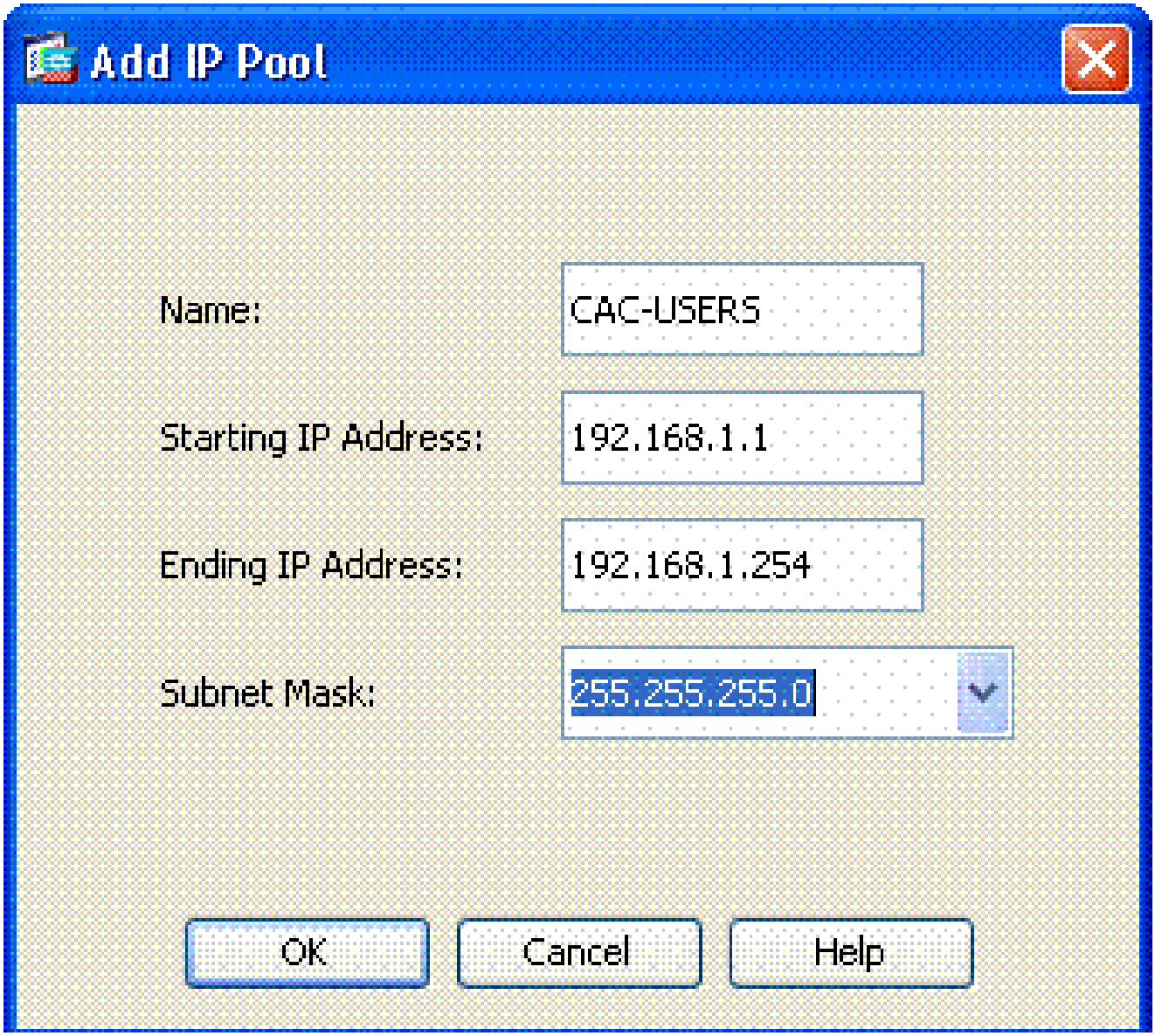
Observação: por exemplo, https://asa.test.com. Este guia usa o segundo método. Uma vez que o cliente CA é instalado permanentemente na máquina do cliente, você apenas inicia o cliente CA a partir do aplicativo.

Criar um pool de endereços IP

Isso é opcional se você usar outro método, como DHCP.

1. Escolha Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.
2. Clique em Add.
3. Na janela Add IP Pool, digite o nome do pool de IPs, o endereço IP inicial e final e escolha uma máscara de sub-rede. Consulte a Figura 13.

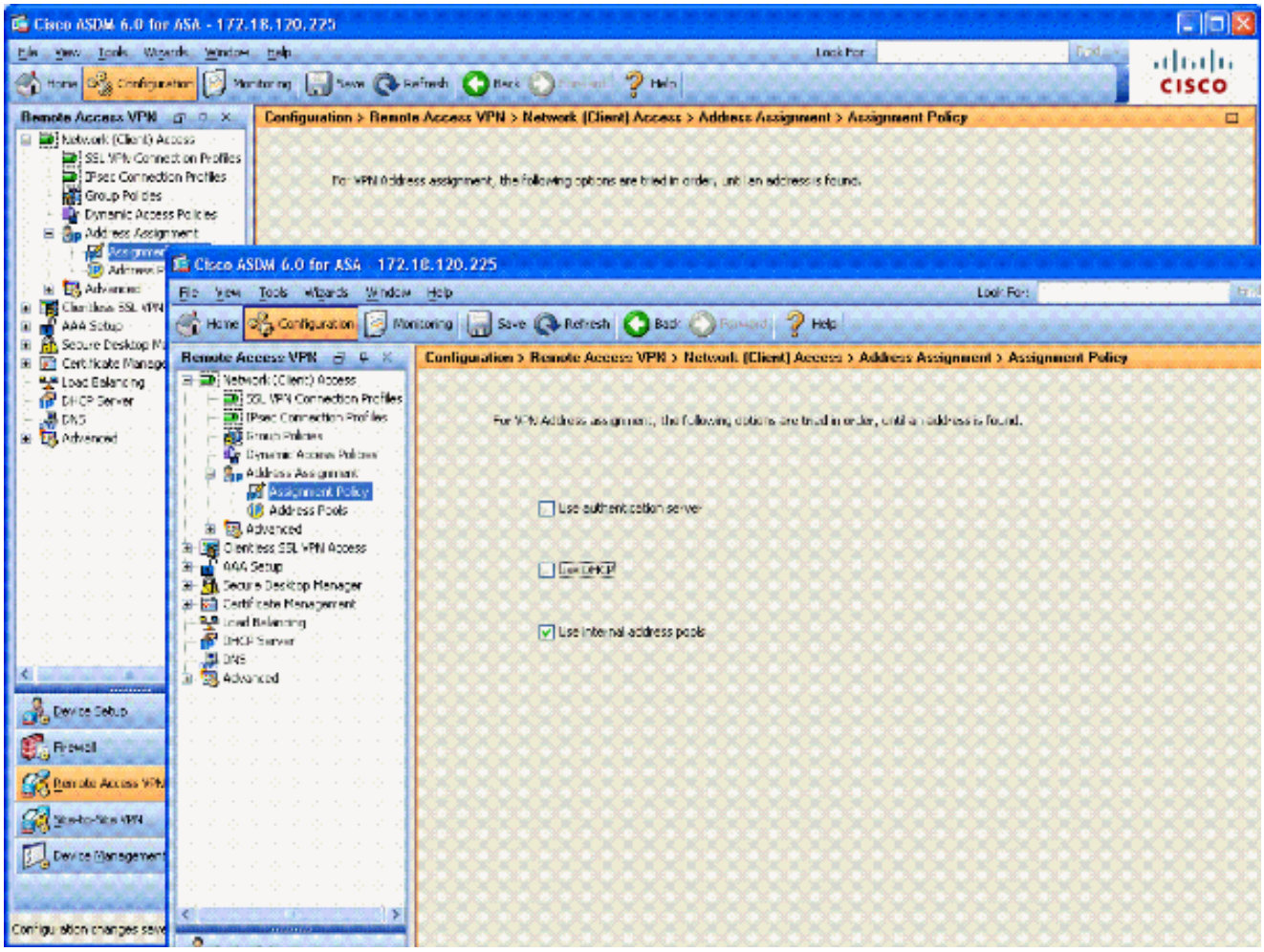
   Figura 13: Adicionando o pool de IPs



4. Escolha Ok.
5. Escolha Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy.

6. Selecione o método de atribuição de endereço IP apropriado. Este guia usa os pools de endereços internos. Consulte a Figura 14.

   Figura 14: Método de atribuição de endereço IP



7. Clique em Apply.

Criar Grupo de Túneis e Política de Grupo

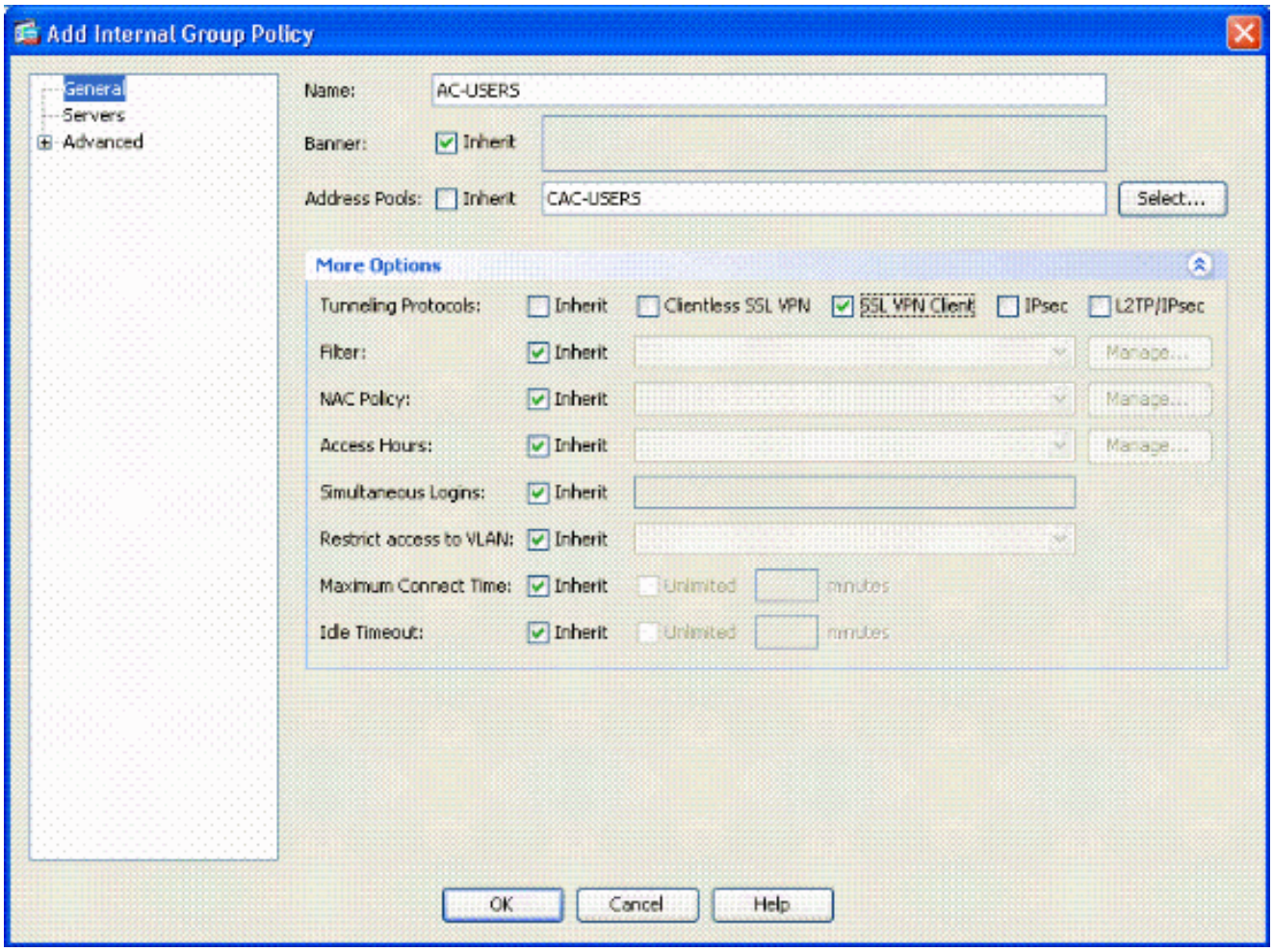
Política de grupo

Observação: se você não quiser criar uma nova política, poderá usar a política interna padrão do grupo.

---

1. Escolha Remote Access VPN -> Network (Client) Access -> Group Policies.
2. Clique em Add e escolha Internal Group Policy.
3. Na janela Adicionar diretiva de grupo interna, digite o nome da diretiva de grupo na caixa de texto Nome. Consulte a Figura 15.

   Figura 15: Adicionando a política de grupo interna



a. Na guia Geral, escolha a opção SSL VPN Client na opção Tunneling Protocols, a menos que você use outros protocolos como o SSL sem Clientes.

b. Na seção Servidores, desmarque a caixa de seleção inherit e insira o endereço IP dos servidores DNS e WINS. Insira o escopo do DHCP, se aplicável.

c. Na seção Servidores, desmarque a caixa de seleção inherit no Domínio Padrão e insira o nome de domínio apropriado.

d. Na guia Geral, desmarque a caixa de seleção inherit na seção address pool e adicione o pool de endereços criado na etapa anterior. Se você usar outro método de atribuição de endereço IP, deixe-o herdar e faça a alteração apropriada.

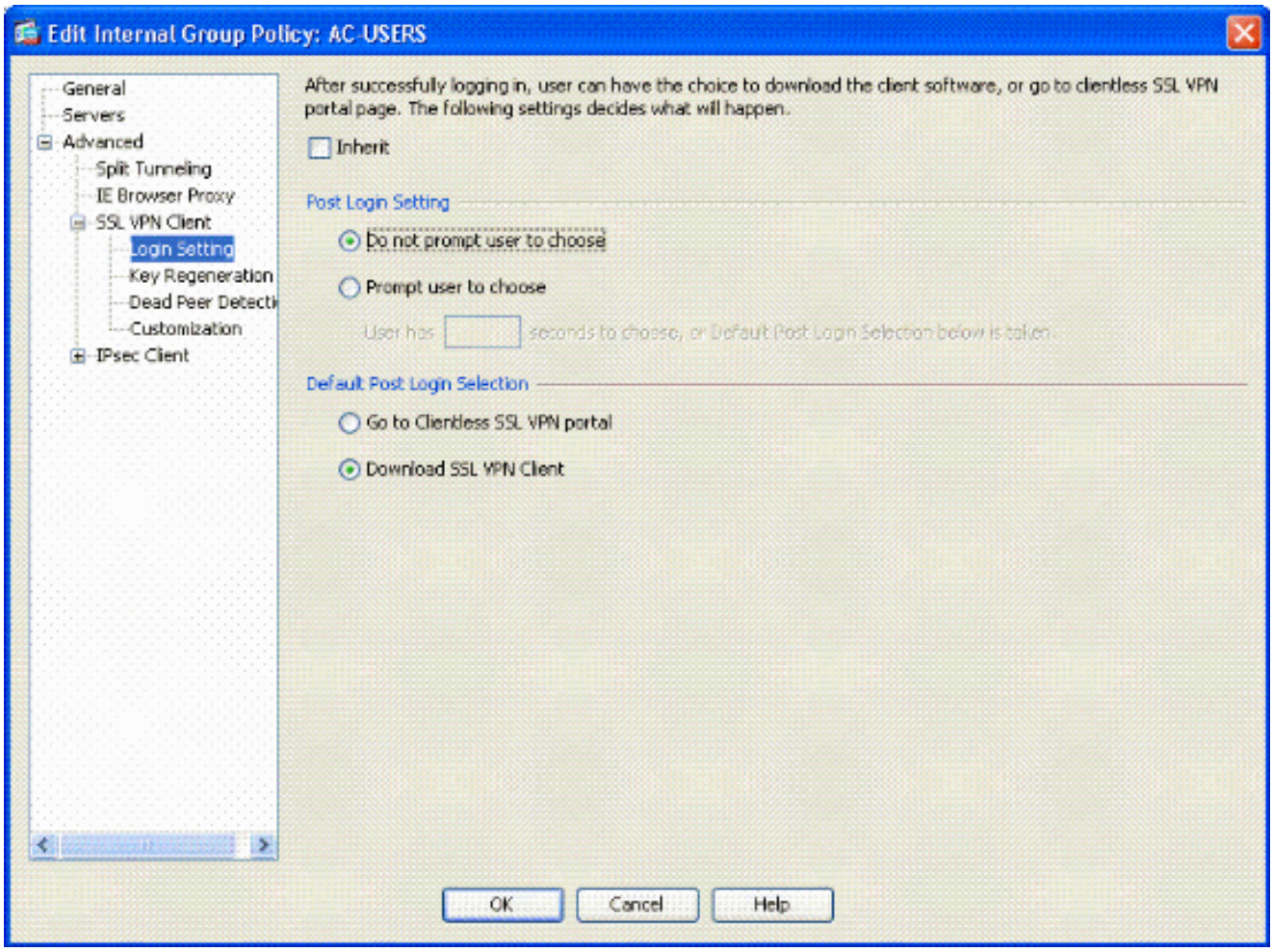
e. Todas as outras guias de configuração são deixadas com as configurações padrão.

> Observação: há dois métodos para levar o cliente AC aos usuários finais. Um método é acessar Cisco.com e fazer o download do cliente AC. O segundo método é fazer com que o ASA baixe o cliente para o usuário quando o usuário tentar se conectar. Este exemplo mostra o último método.

---

4. Em seguida, escolha Advanced > SSL VPN Client > Login Settings. Consulte a Figura 16.

Figura 16: Adicionando a política de grupo interna



a. Desmarque a caixa de seleção Inherit.

b. Escolha a Configuração de pós-login adequada ao seu ambiente.

c. Escolha a Seleção padrão pós-login adequada ao seu ambiente.

d. Escolha OK.

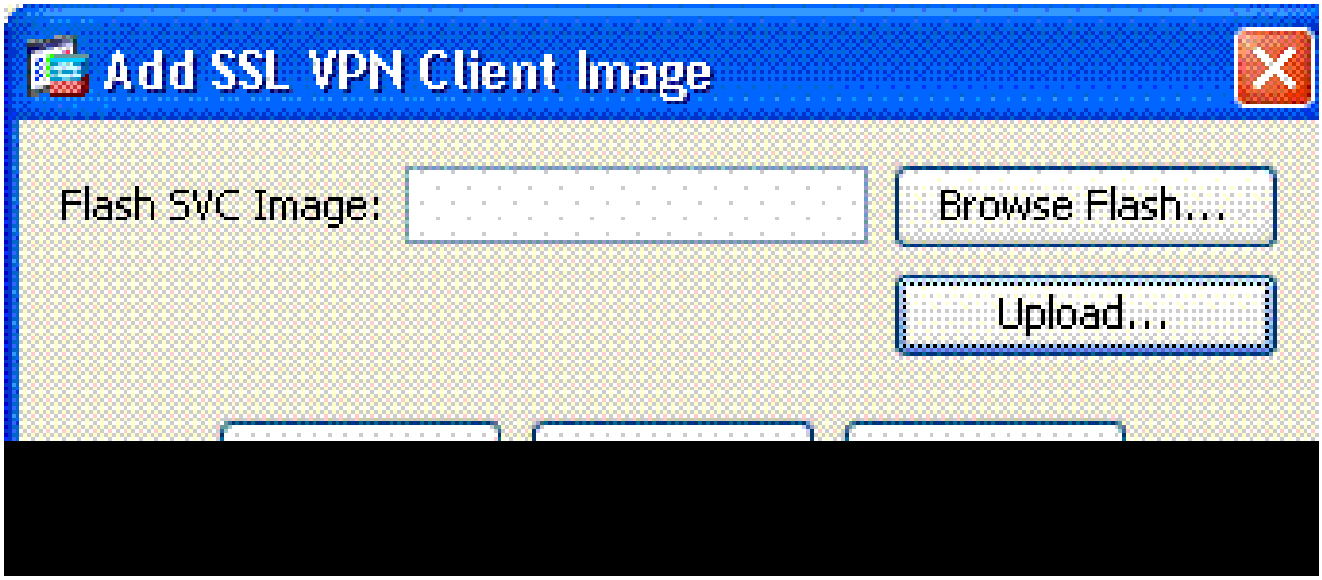
Configurações de interface e imagem do grupo de túneis

Observação: se não quiser criar um novo grupo, você poderá usar o grupo interno padrão.

1. Escolha Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile.
2. Escolha Habilitar Cisco AnyConnect Client.....
3. Uma caixa de diálogo é exibida com a pergunta `Você gostaria de designar uma imagem SVC?`
4. Escolha Sim.
5. Se já houver uma imagem, escolha a imagem a ser usada com o Browse Flash. Se a imagem não estiver disponível, escolha Carregar e procure o arquivo no computador local. Consulte a Figura 17. Os arquivos podem ser baixados de Cisco.com; há um arquivo

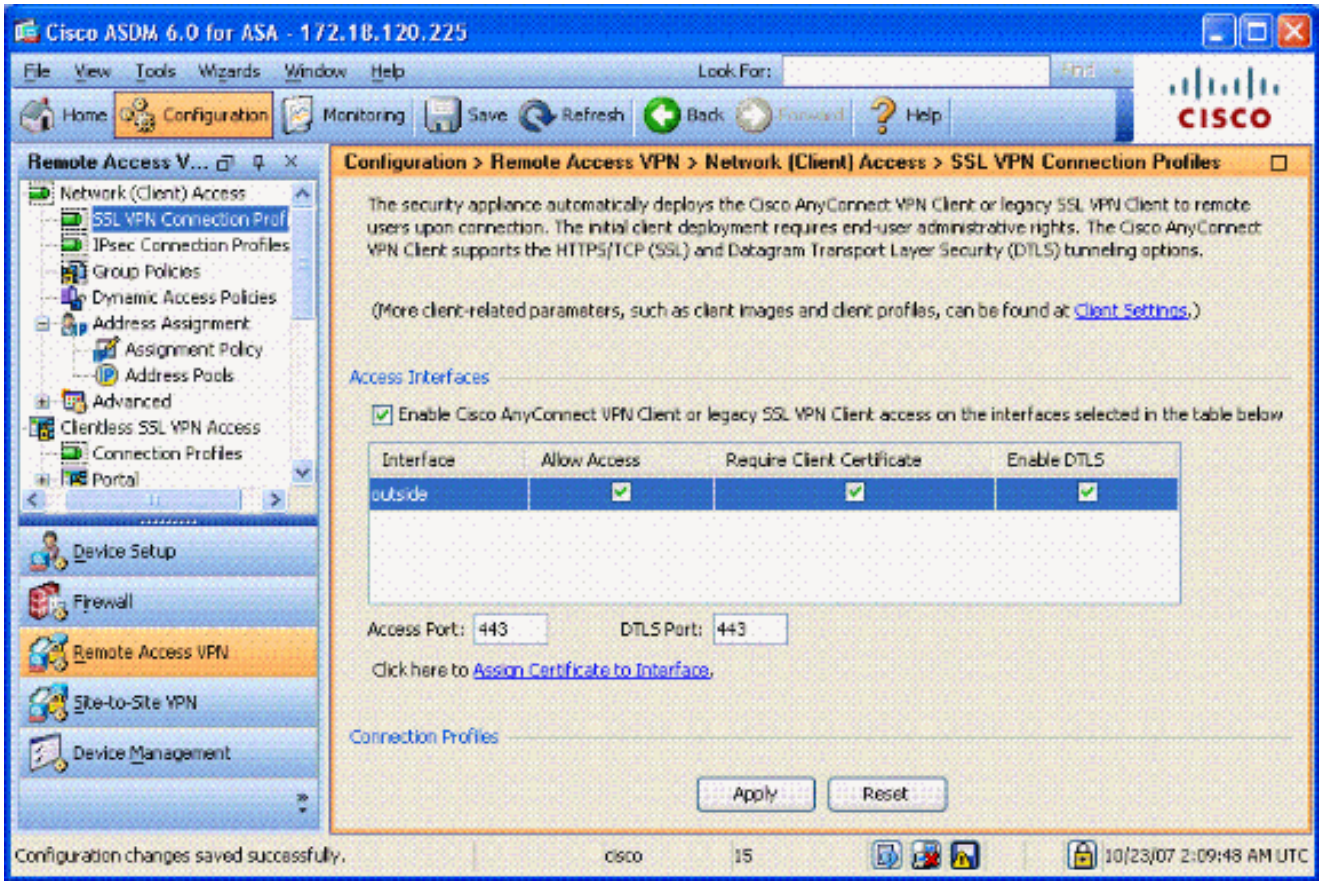
Windows, MAC e Linux.

Figura 17: Adicionar imagem de cliente VPN SSL



6. Em seguida, habilite Allow Access, Require Client Cert e, opcionalmente, Enable DTLS. Consulte a Figura 18.

Figura 18: Habilitando o acesso



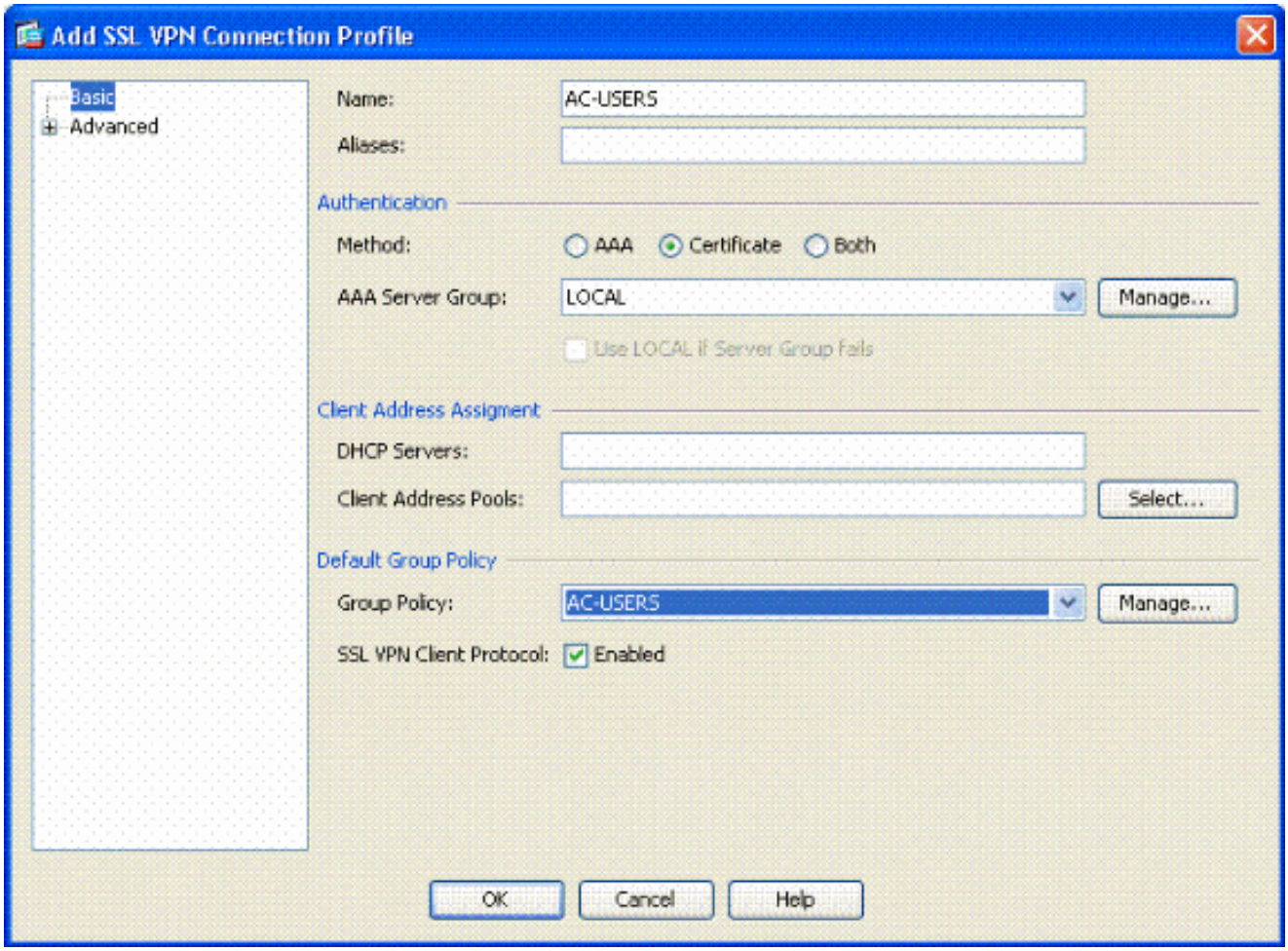
7. Clique em Apply.

8. Em seguida, crie um perfil de conexão/grupo de túneis. Escolha Remote Access VPN >

Network (Client) Access > SSL VPN Connection Profile.

9. Na seção Perfis de conexão, clique em Adicionar.

Figura 19: Adicionando o perfil de conexão



a. Nomeie o grupo.

b. Escolha Certificate no método de autenticação.

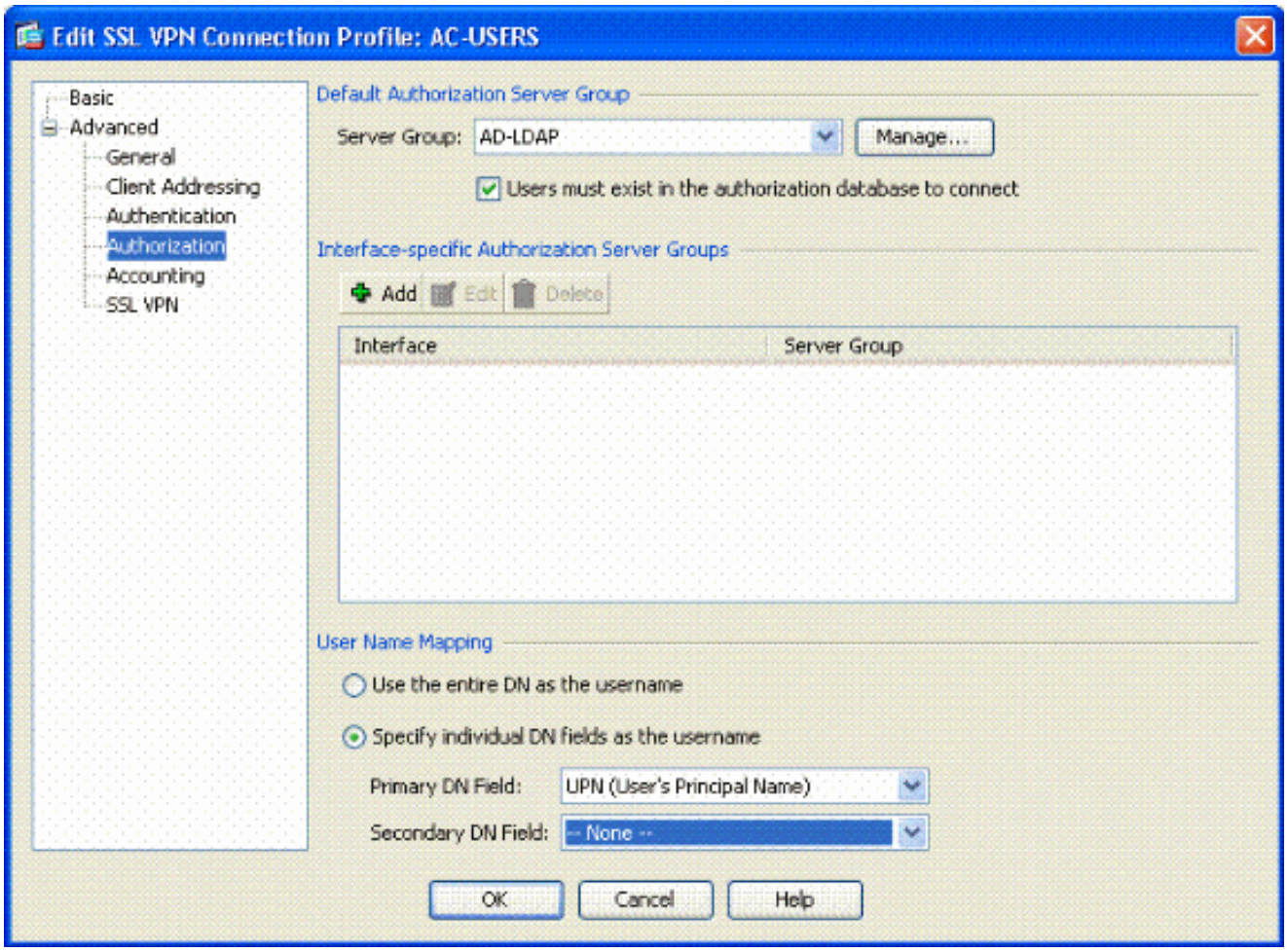
c. Escolha a política de grupo criada anteriormente.

d. Verifique se o SSL VPN Client está habilitado.

e. Deixe outras opções como padrão.

10. Em seguida, escolhaAvançado > Autorização. Consulte a figura 20

Figura 20: Autorização



a. Escolha o grupo AD-LDAP criado anteriormente.

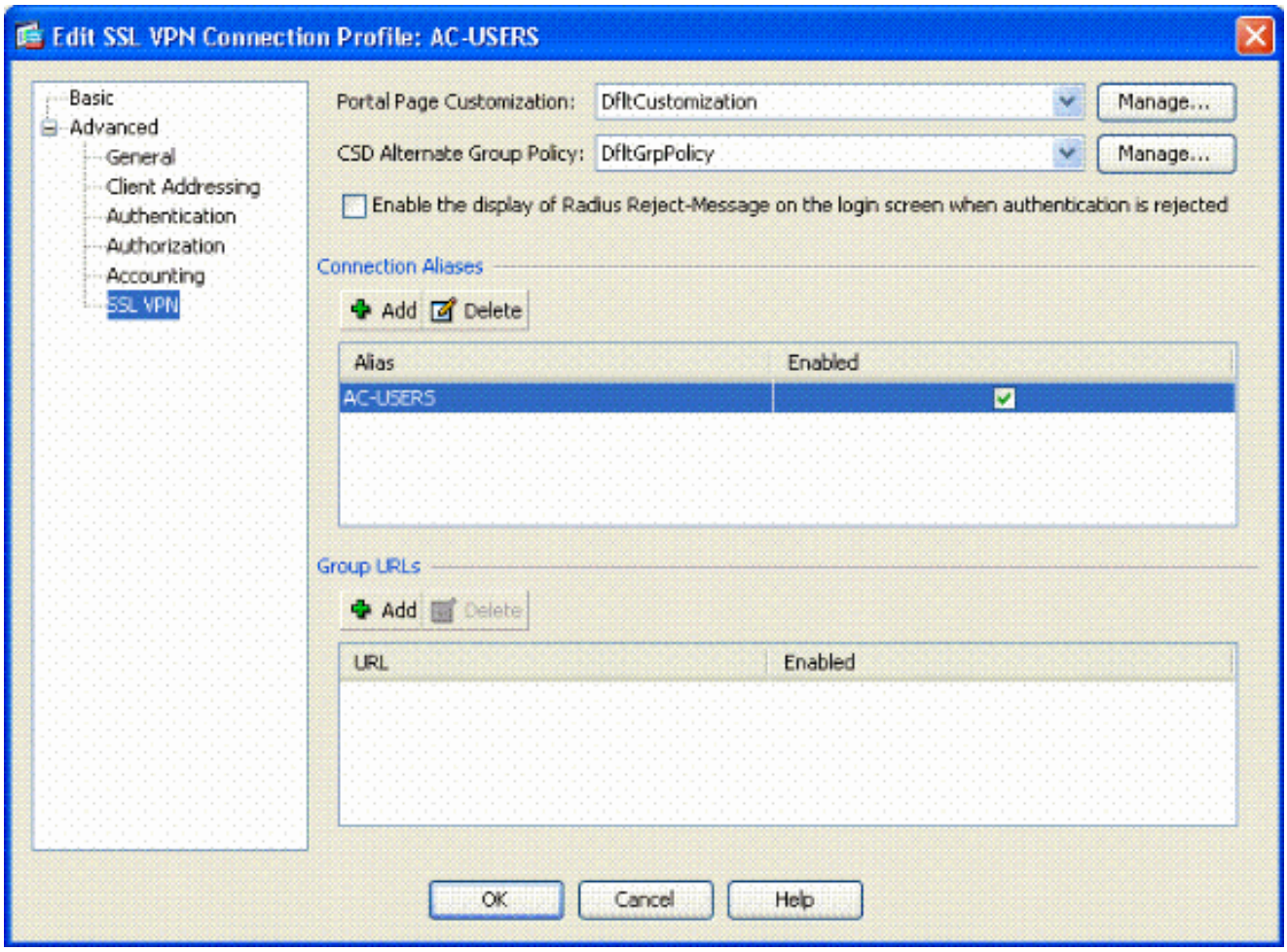
b. Marque Os usuários devem existir... para se conectarem.

c. Nos campos de mapeamento, escolha UPN para o primário e nenhum para o secundário.

11. Escolha a seção VPN SSL do menu.

12. Na seção Aliases de Conexão, faça o seguinte:

Figura 21: Aliases da conexão



a. Escolha Adicionar.

b. Insira o alias de grupo que deseja usar.

c. Certifique-se de que Enabled esteja marcado. Consulte a Figura 21.

13. Click OK.

Observação: clique em Save para salvar a configuração na memória flash.

Regras de correspondência de certificado (se o OCSP for usado)

1. Escolha Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps. Consulte a Figura 22.

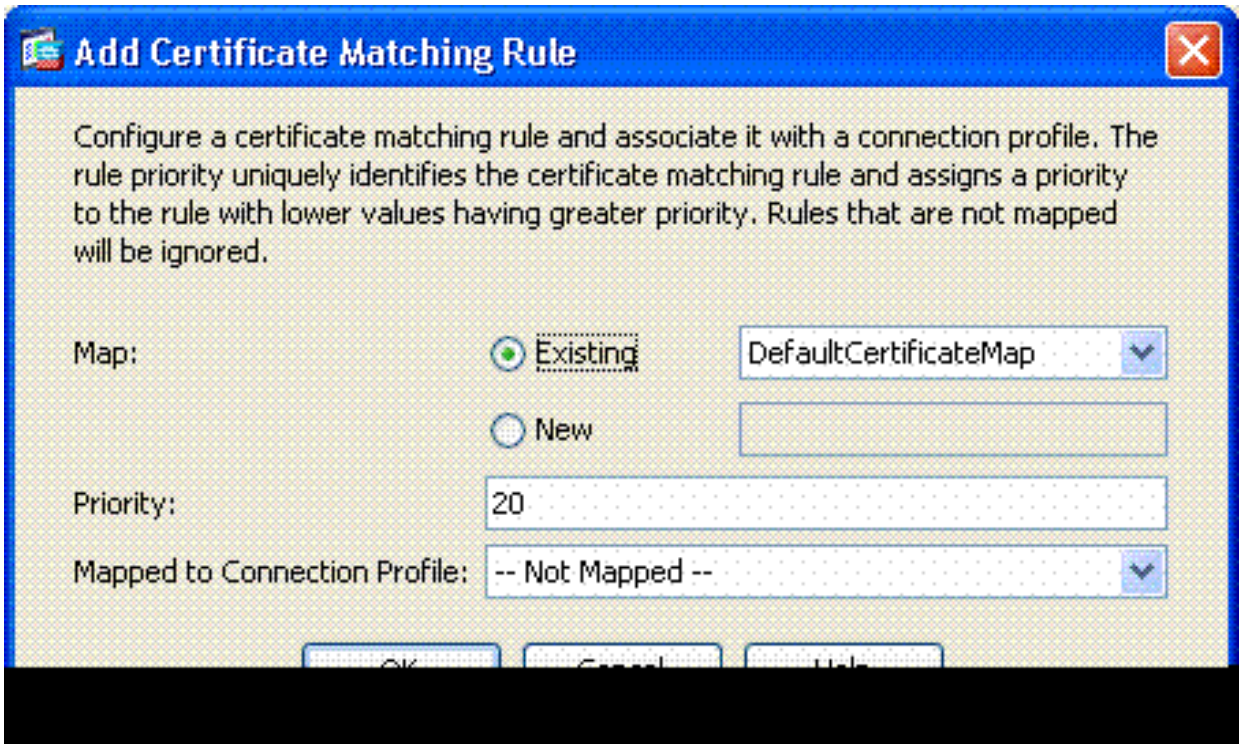
   a. Escolha Add na seção Certificate to Connection Profile Maps .

   b. Você pode manter o mapa existente como DefaultCertificateMap na seção de mapa ou criar um novo se já usar mapas de certificado para IPsec.

   c. Mantenha a prioridade da regra.

   d. Em grupo mapeado, deixe como — Não mapeado —. Consulte a Figura 22.

Figura 22: Adicionando regra de correspondência de certificado

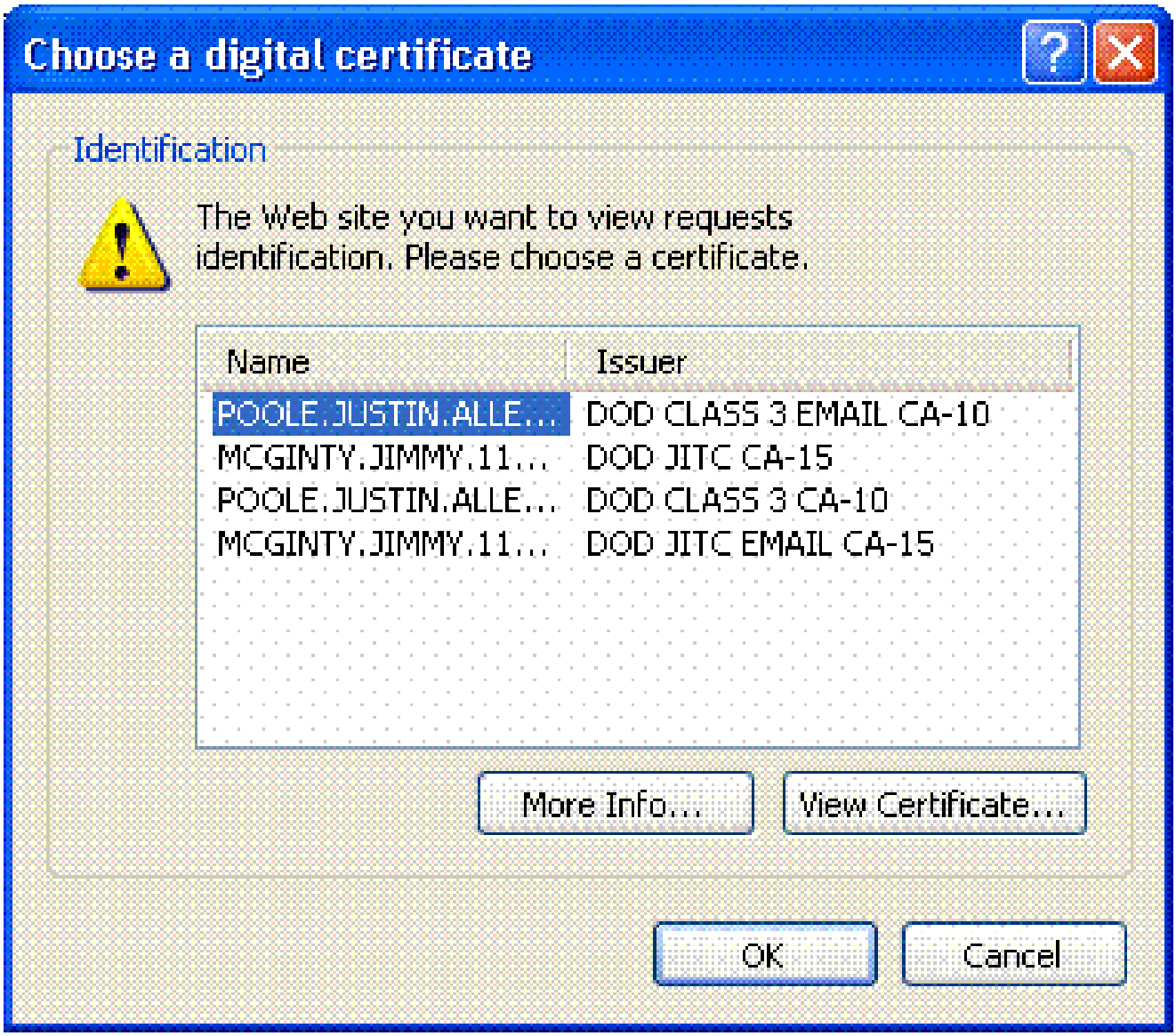


e. Click OK.

2. Clique em Adicionar na tabela inferior.

3. Na janela Adicionar critério de regra de correspondência de certificado, siga estas etapas:

Figura 23: Critério da regra de correspondência de certificado



a. Mantenha a coluna Campo como Assunto.

b. Mantenha a coluna Componente em Campo Inteiro.

c. Altere a coluna Operador para Não é igual.

d. Na coluna Valor, insira duas aspas duplas "".

e. Clique em Ok e em Aplicar. Veja a Figura 23, por exemplo.

Configurar o OCSP

A configuração de um OCSP pode variar e depende do fornecedor do respondente OCSP. Leia o manual do fornecedor para obter mais informações.

Configurar Certificado de Respondente OCSP

1. Obtenha um certificado gerado automaticamente do respondente OCSP.

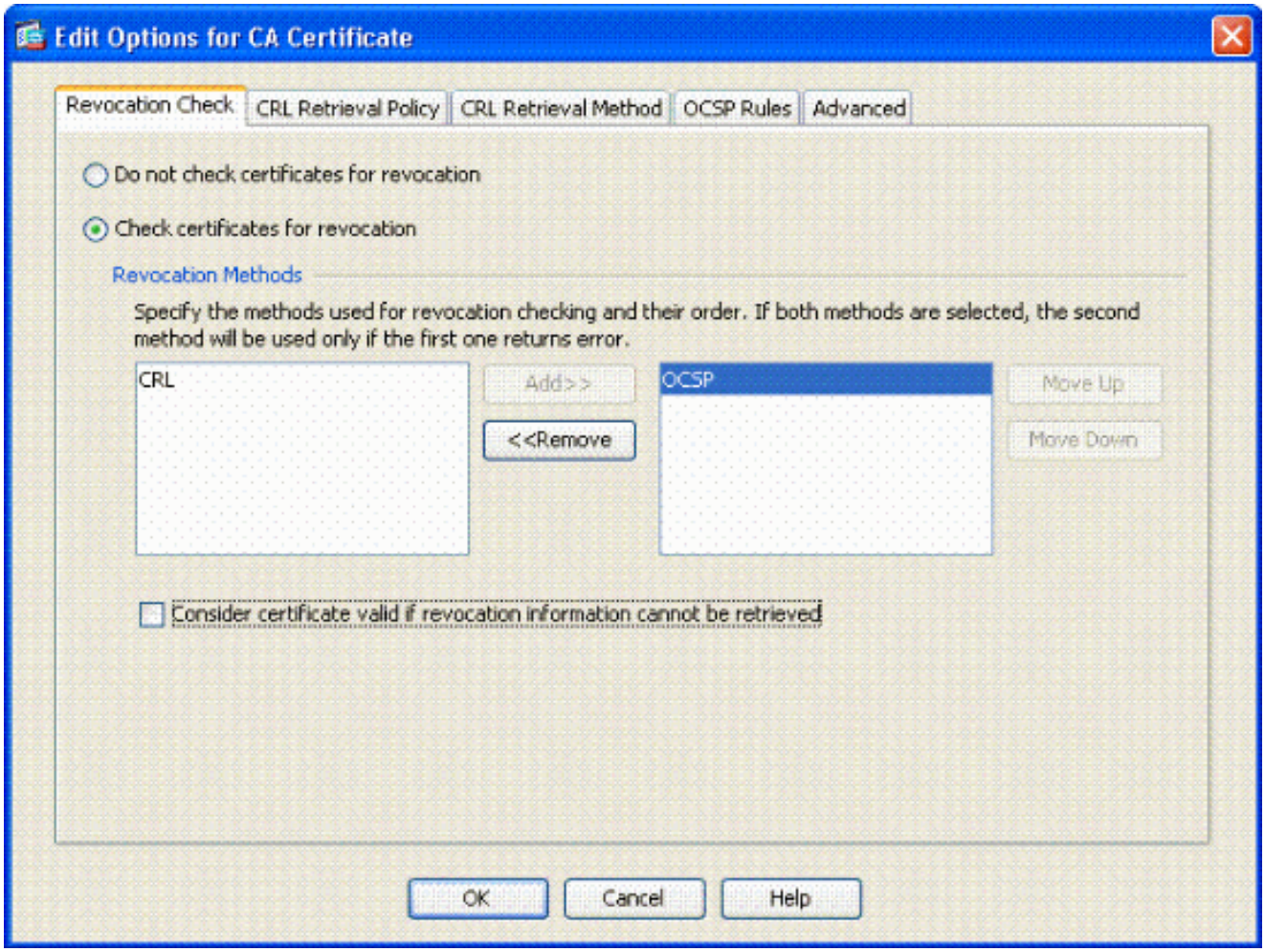
2. Conclua os procedimentos mencionados anteriormente e instale um certificado para o servidor OSCP.

> Observação: certifique-se de que Não verificar certificados para revogação esteja selecionado para o ponto de confiança do certificado OCSP.

Configurar CA para usar OCSP

1. Escolha Remote Access VPN> Certificate Management > CA Certificates.
2. Destaque um OCSP para escolher uma CA a ser configurada para usar o OCSP.
3. Clique em Editar.
4. Verifique se Check certificate for revocation está marcado.
5. Na seção Métodos de Revogação, adicione OCSP. Consulte a Figura 24.

   Verificação de Revogação OCSP



6. Verifique se Considerar certificado válido...não pode ser recuperado está desmarcado se você quiser seguir a verificação OCSP estrita.

Observação: configure/edite todos os servidores de autoridade de certificação que usam OCSP para revogação.

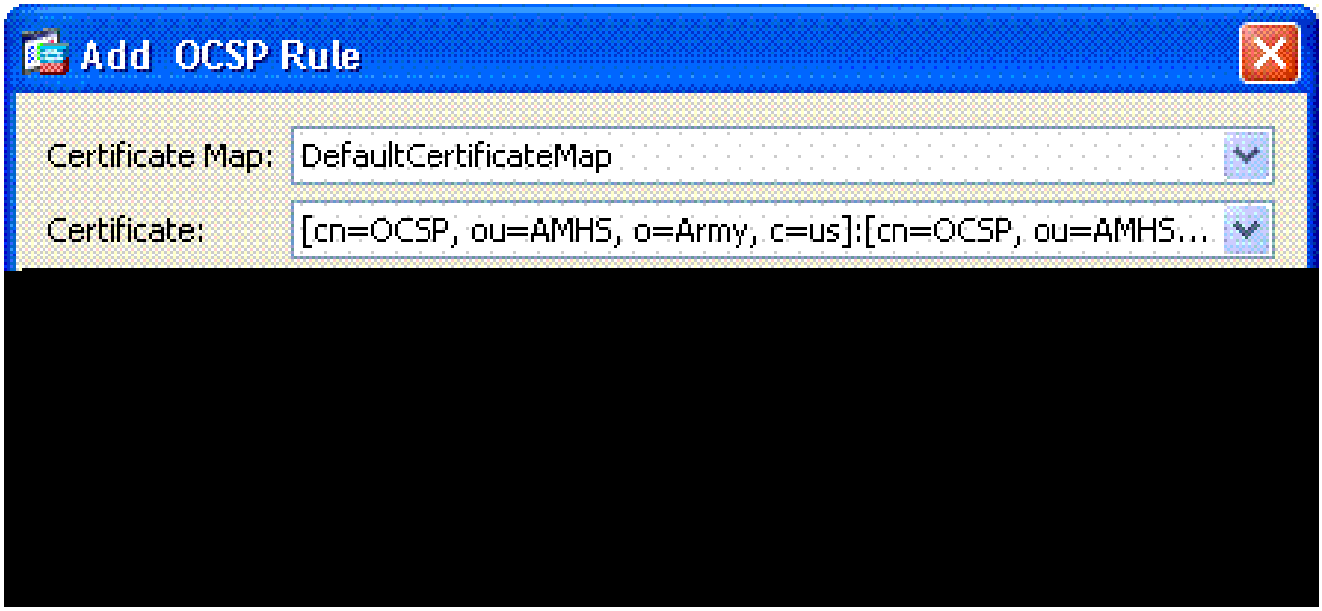
Configurar regras OCSP

Observação: antes de concluir essas etapas, verifique se foi criada uma Política de Correspondência de Grupo de Certificados e se o respondente OCSP está configurado.

Observação: em algumas implementações OCSP, um registro DNS A e PTR pode ser necessário para o ASA. Esta verificação é feita para verificar se o ASA é de um site .mil.

1. Escolha Remote Access VPN> Certificate Management > CA Certificates 2.
2. Destaque um OCSP para escolher uma CA a ser configurada para usar o OCSP.
3. Escolha Editar.
4. Clique na guia Regra OCSP.
5. Clique em Add.
6. Na janela Add OCSP Rule (Adicionar regra OCSP), siga estas etapas. Consulte a Figura 25.

   Figura 25: Adicionando regras OCSP



   a. Na opção Mapa do certificado, escolha DefaultCertificateMap ou um mapa criado anteriormente.

   b. Na opção Certificate, selecione OCSP responder.

   c. Na opção de índice, digite 10.

d. Na opção URL, digite o endereço IP ou o nome de host do respondente OCSP. Se você usar o nome de host, certifique-se de que o servidor DNS esteja configurado no ASA.

e. Click OK.

f. Clique em Apply.

Configuração do Cisco AnyConnect Client

Esta seção aborda a configuração do Cisco AnyConnect VPN Client.

Hipóteses - O Cisco AnyConnect VPN Client e o aplicativo de middleware já estão instalados no PC host. O ActivCard Gold e o ActivClient foram testados.

Observação: este guia usa o método group-url somente para a instalação inicial do cliente AC. Uma vez que o cliente AC esteja instalado, você inicia o aplicativo AC como o cliente IPsec.

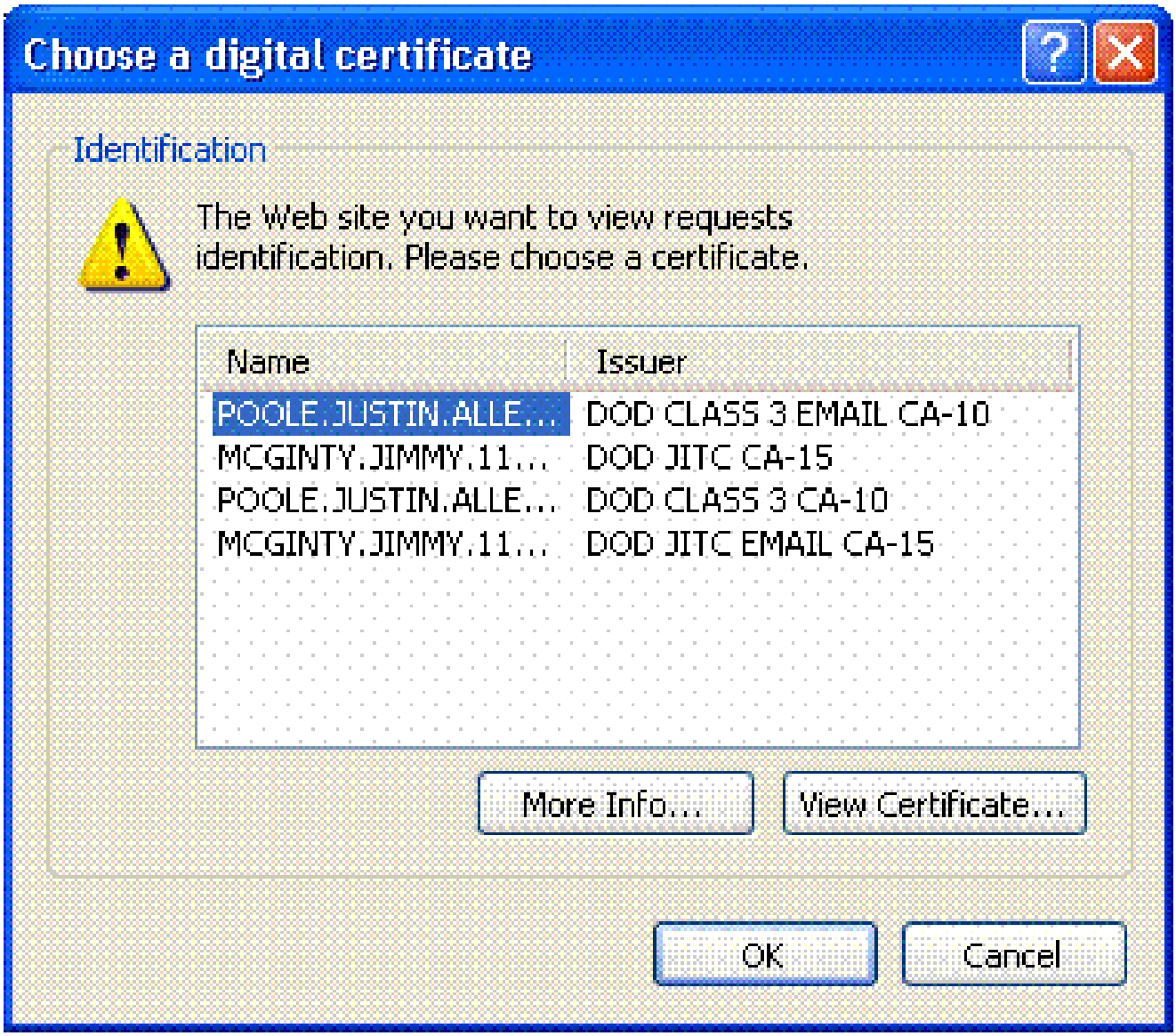
Observação: a cadeia de certificados DoD precisa ser instalada no computador local. Verifique com a POC PKI para obter o arquivo de certificados/lote.

Baixando o Cisco Anyconnect VPN Client - Windows

1. Inicie uma sessão da Web para o ASA através do Internet Explorer. O endereço deve estar no formato https://Outside-Interface. Por exemplo, https://172.18.120.225.

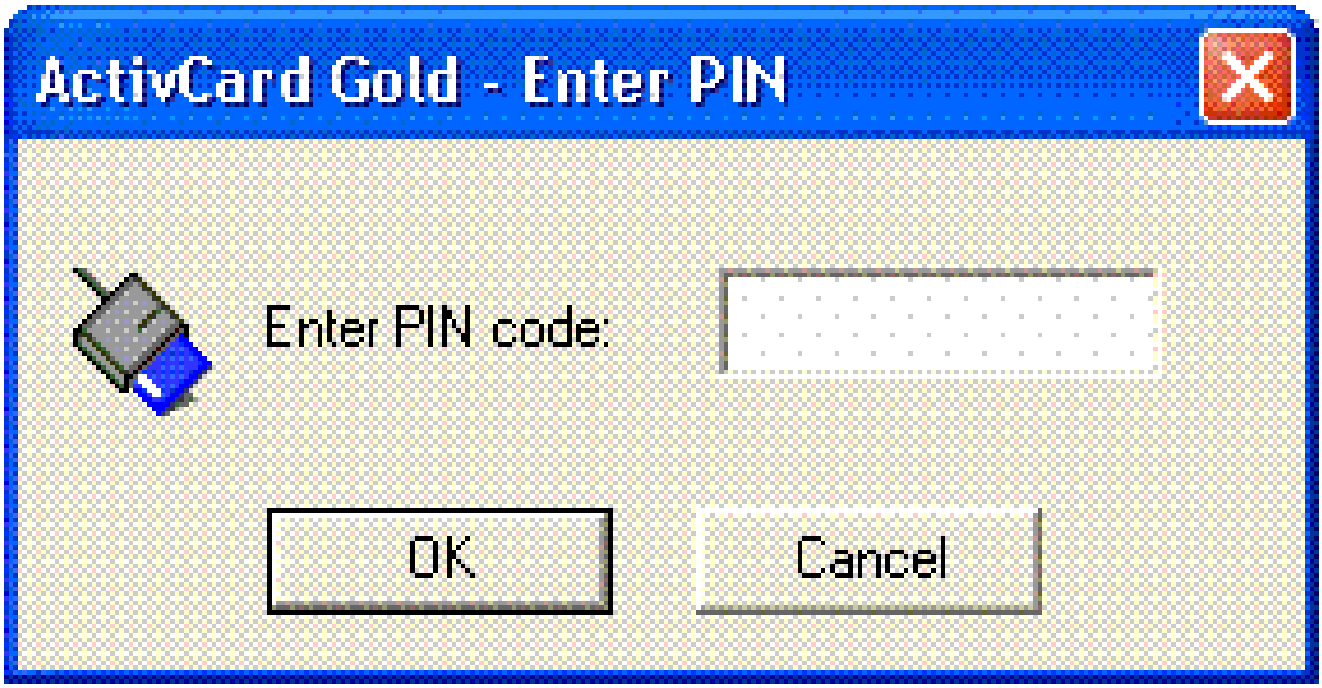
2. Escolha o certificado de assinatura a ser usado para acessar. Consulte a Figura 26.

   Figura 26: Escolha o certificado correto



3. Insira seu pin quando solicitado.

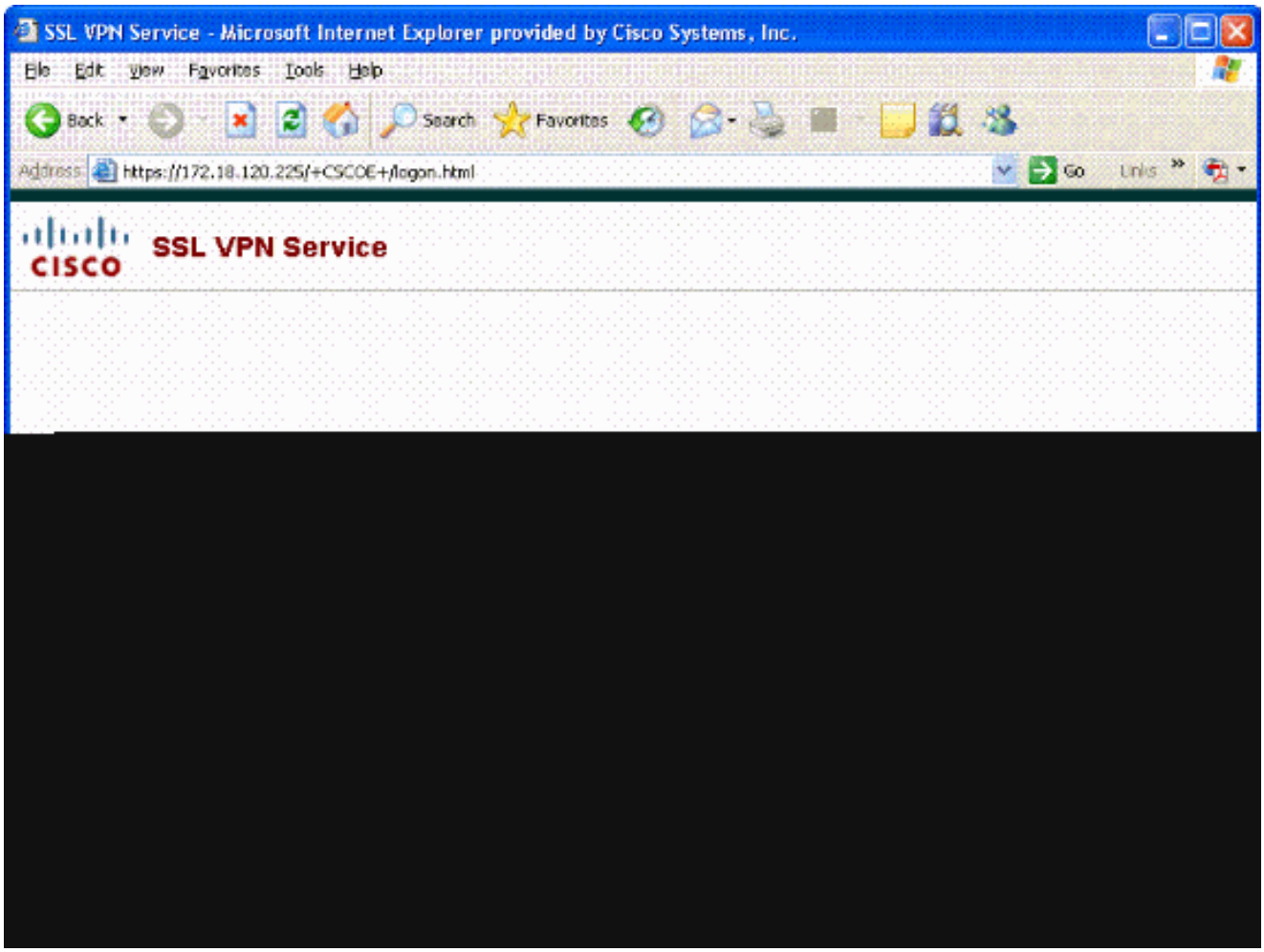
Figura 27: Inserir PIN



4. Escolha Sim para aceitar o alerta de segurança.

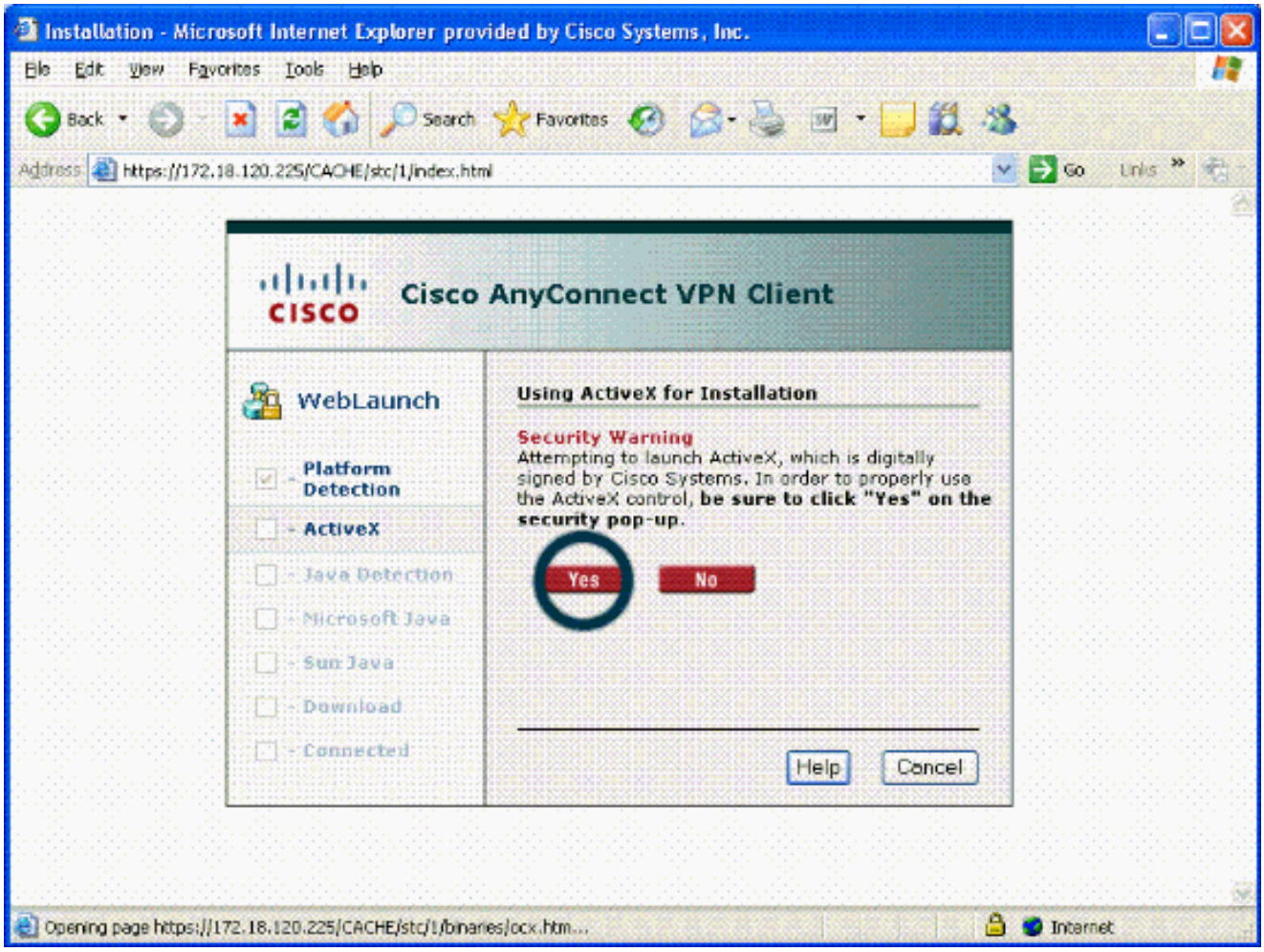
5. Na página Login SSL, escolha Login. O certificado do cliente é usado para fazer logon. Consulte a Figura 28.

   Figura 28: Logon SSL



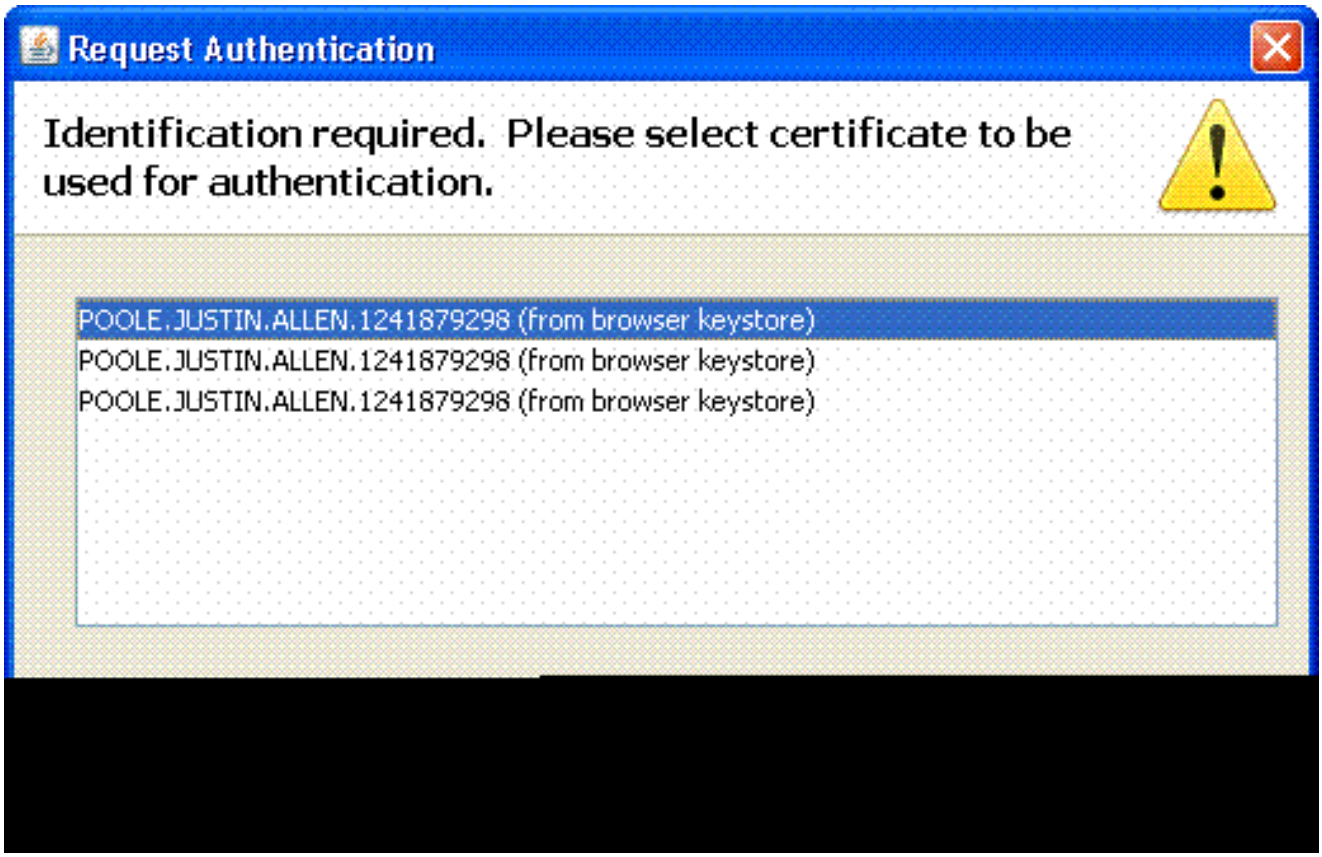
6. O AnyConnect começa a baixar o cliente. Consulte a Figura 29.

Figura 29: Instalação do AnyConnect



7. Escolha o certificado apropriado a ser usado. Ver figura 30. O AnyConnect continua a ser instalado. O administrador do ASA pode permitir que o cliente instale ou instale permanentemente em cada conexão do ASA.

Figura 30: Certificado



Iniciar o Cisco AnyConnect VPN Client - Windows

No PC host, escolha Iniciar > Todos os programas > Cisco > AnyConnect VPN Client.

Observação: consulte o Apêndice E para obter a configuração opcional do AnyConnect Client Profile.

Nova conexão

1. A janela AC é exibida. Consulte a Figura 34.

Figura 34: Nova conexão VPN

2. Escolha o host apropriado se o AC não tentar a conexão automaticamente.

3. Insira seu PIN quando solicitado. Consulte a Figura 35.

Figura 35: Inserir PIN

Iniciar acesso remoto

Escolha o grupo e o host ao qual deseja se conectar.

Como os certificados são usados, escolha Connect para estabelecer a VPN. Consulte a Figura 36.

Figura 36: Conexão


Cisco AnyConnect VPN Client
Connection
Statistics
About
CISCO
Connect to:
172.18.120.225
Group:
AC-USERS
Username:
Password:
Connect
Please enter your username and password.

Observação: como a conexão usa certificados, não há necessidade de inserir um nome de usuário e uma senha.

Observação: consulte o Apêndice E para obter a configuração opcional do AnyConnect Client Profile.

Apêndice A - Mapeamento LDAP e DAP

No ASA/PIX versão 7.1(x) e posterior, foi introduzido um recurso chamado mapeamento LDAP. Este é um recurso poderoso que fornece um mapeamento entre um atributo da Cisco e objetos/atributos LDAP, o que nega a necessidade de alteração do esquema LDAP. Para a implementação da autenticação CAC, isso pode suportar a aplicação de política adicional na conexão de acesso remoto. Estes são exemplos de mapeamento LDAP. Esteja ciente de que você precisa de direitos de administrador para fazer alterações no servidor AD/LDAP. No software ASA 8.x, o recurso Dynamic Access Policy (DAP) foi introduzido. O DAP pode trabalhar em conjunto com o CAC para examinar vários grupos AD, bem como políticas de envio, ACLs e assim por diante.

Cenário 1: Aplicação do Ative Diretory usando a Discagem de Permissão de Acesso Remoto - Permitir/Negar Acesso

Este exemplo mapeia o atributo do AD msNPAllowDailin para o atributo da Cisco cVPN3000-Tunneling-Protocol.

- O valor do atributo AD: TRUE = Allow; FALSE = Deny
- Valor do atributo Cisco: 1 = FALSE, 4 (IPSec) ou 20 (4 IPSEC + 16 WebVPN) = TRUE,

Para a condição PERMITIR, você mapeia:

- VERDADEIRO = 20

Para a condição de discagem DENY, você mapeia:

- FALSO = 1

Observação: certifique-se de que TRUE e FALSE estejam em maiúsculas. Consulte Configuração de um Servidor Externo para Autorização do Usuário do Security Appliance para obter mais informações.

Configuração do Ative Diretory

1. No Servidor Ative Diretory, clique em Iniciar > Executar.
2. Na caixa de texto Abrir, digite dsa.msc e clique em Ok. Inicia o console de gerenciamento

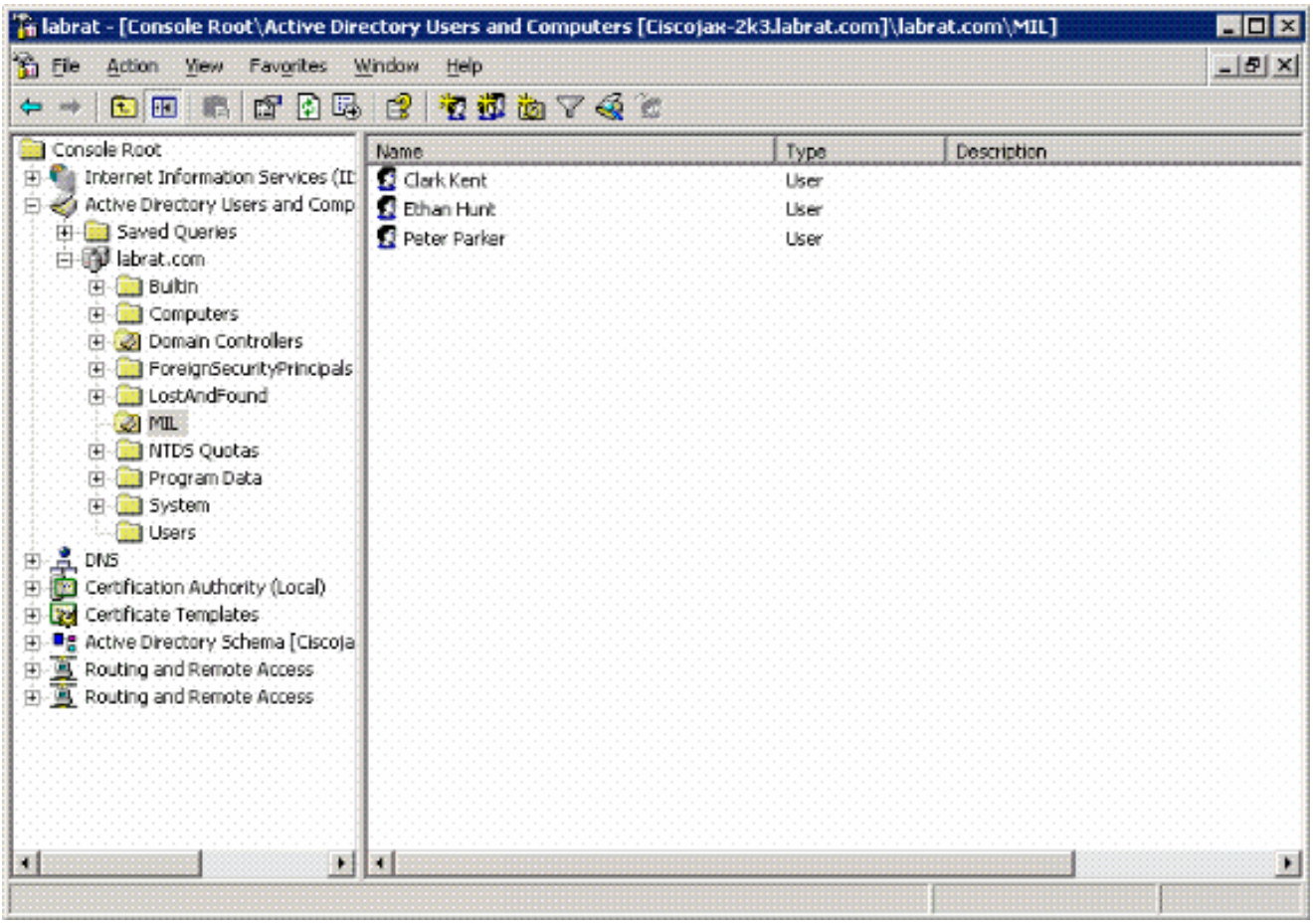
do ative diretory.

3. No console de gerenciamento do Ative Diretory, clique no sinal de mais para expandir Usuários e Computadores do Ative Diretory.

4. Clique no sinal de mais para expandir o nome de domínio.

5. Se você tiver uma OU criada para seus usuários, expanda a OU para exibir todos os usuários; se todos os usuários estiverem atribuídos na pasta Usuários, expanda essa pasta para exibi-los. Veja a Figura A1.

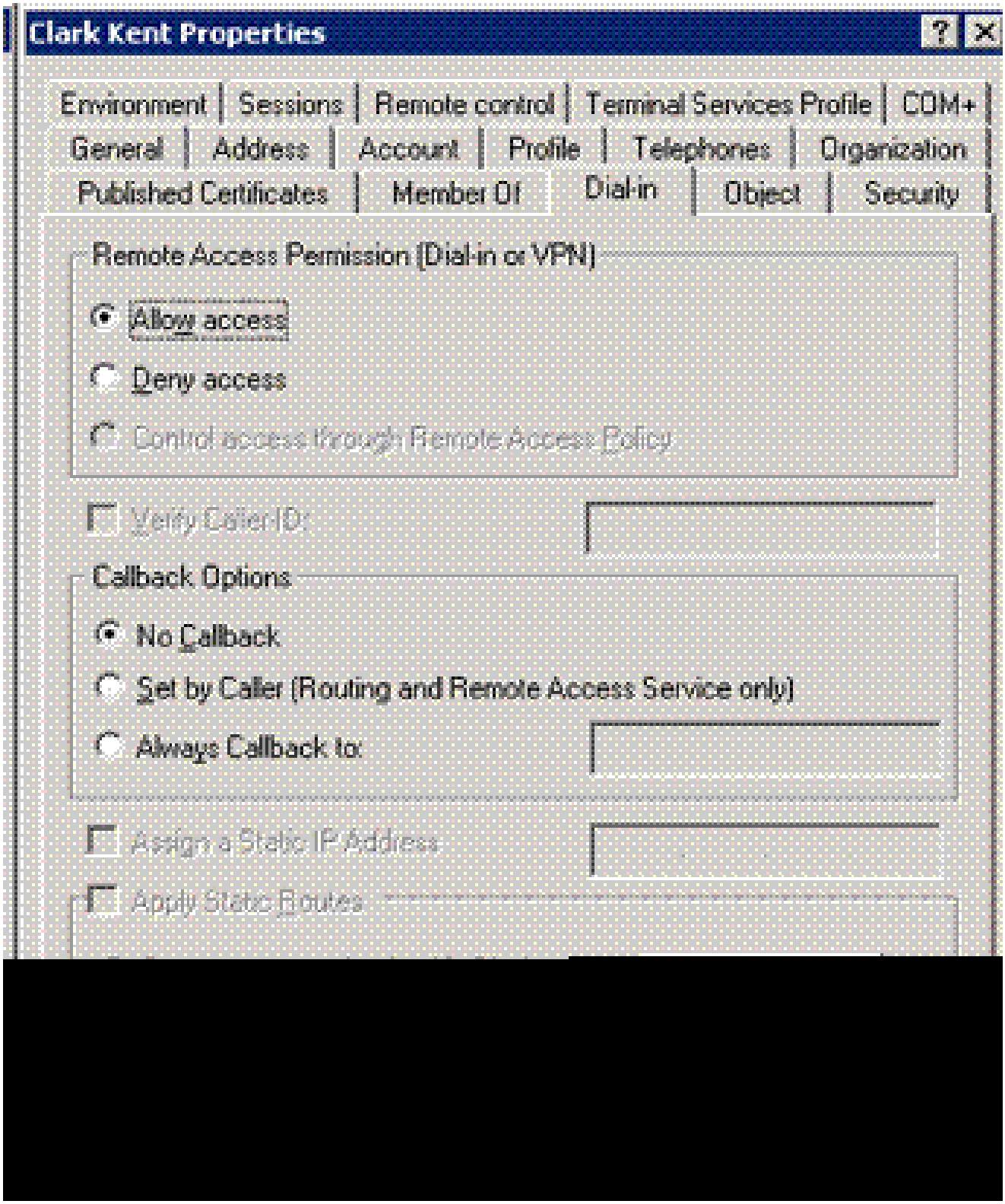
   Figura A1: Console de gerenciamento do Ative Diretory



6. Clique duas vezes no usuário que deseja editar.

   Clique na guia Discagem na página de propriedades do usuário e clique em permitir ou negar. Veja a Figura A2.

   Figura A2: Propriedades do usuário

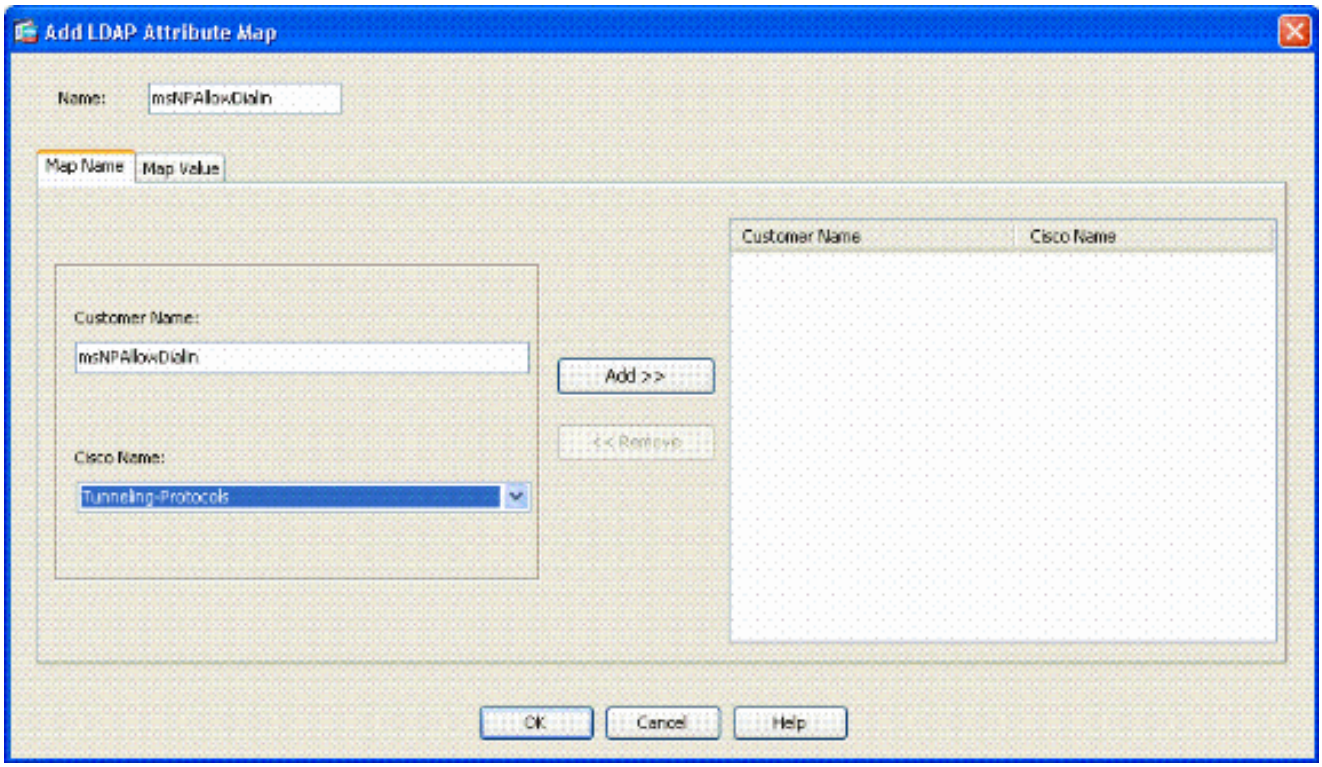


7. Em seguida, clique em “OK”.

Configuração do ASA

1. No ASDM, escolha Remote Access VPN> AAA Setup > LDAP Attribute Map.
2. Clique em Add.
3. Na janela Adicionar mapa de atributos LDAP, siga estas etapas. Veja a Figura A3.

Figura A3: Adicionando mapa de atributos LDAP



a. Digite um nome na caixa de texto Nome.

b. Na guia Nome do mapa, digite msNPAllowDialin na caixa de texto Nome do cliente.

c. Na guia Nome do mapa, escolha Tunneling-Protocols na opção suspensa no Nome da Cisco.

d. Clique em Add.

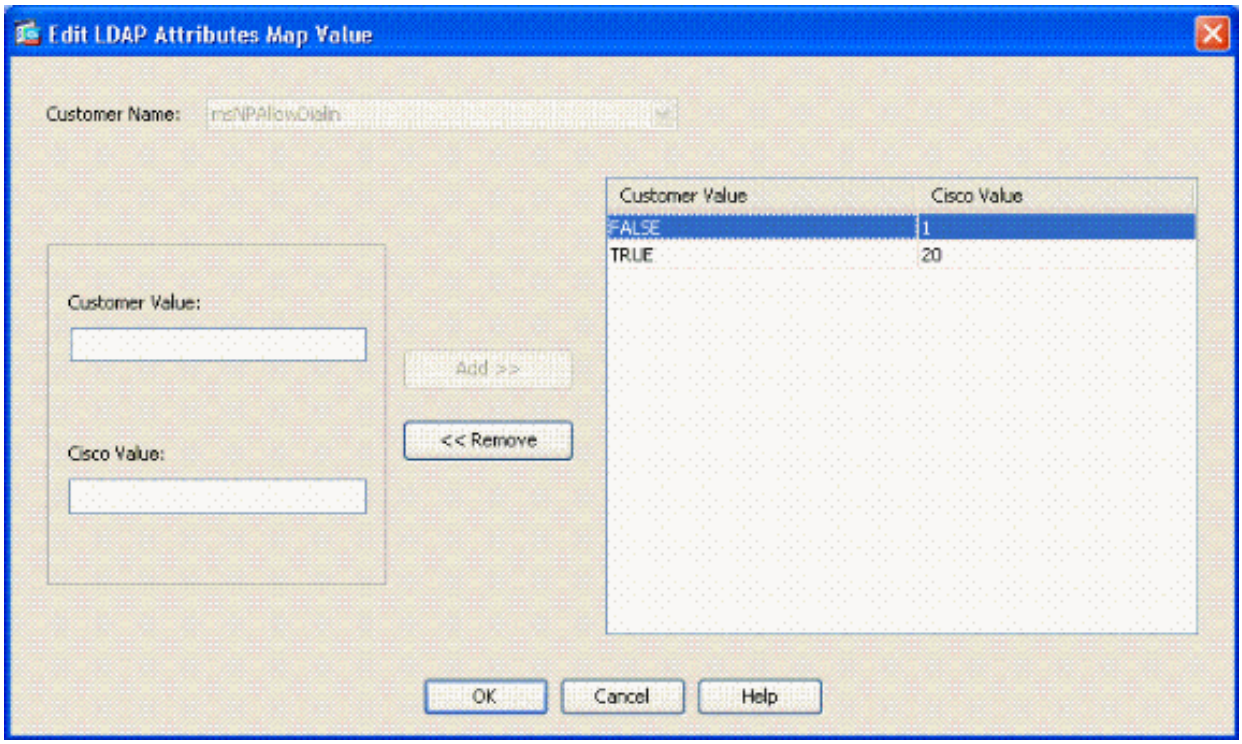
e. Escolha a guia Mapear Valor.

f. Clique em Add.

g. Na janela Adicionar valor de mapa LDAP de atributo, digite TRUE na caixa de texto Nome do cliente e digite 20 na caixa de texto Valor da Cisco.

h. Clique em Add.

i. Digite FALSE na caixa de texto Nome do cliente e digite 1 na caixa de texto Valor da Cisco. Veja a Figura A4.



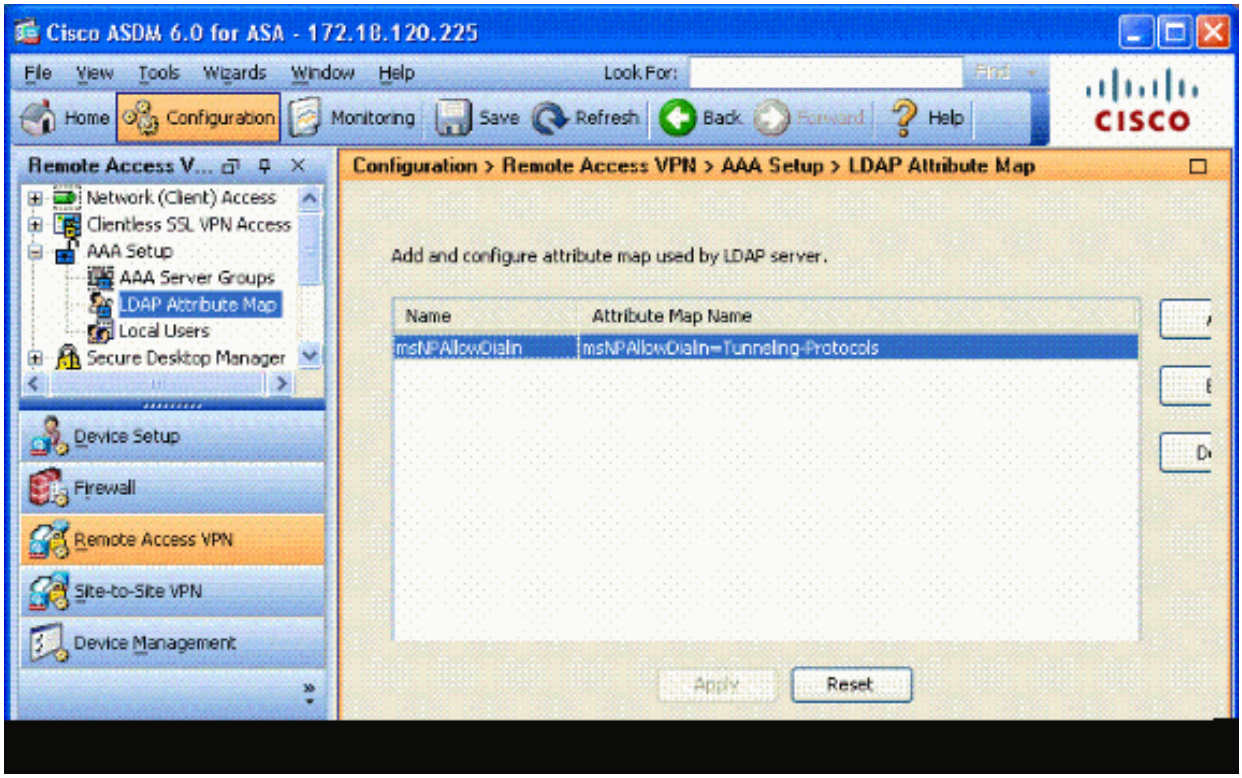
j. Click OK.

k. Click OK.

l. Clique em Apply.

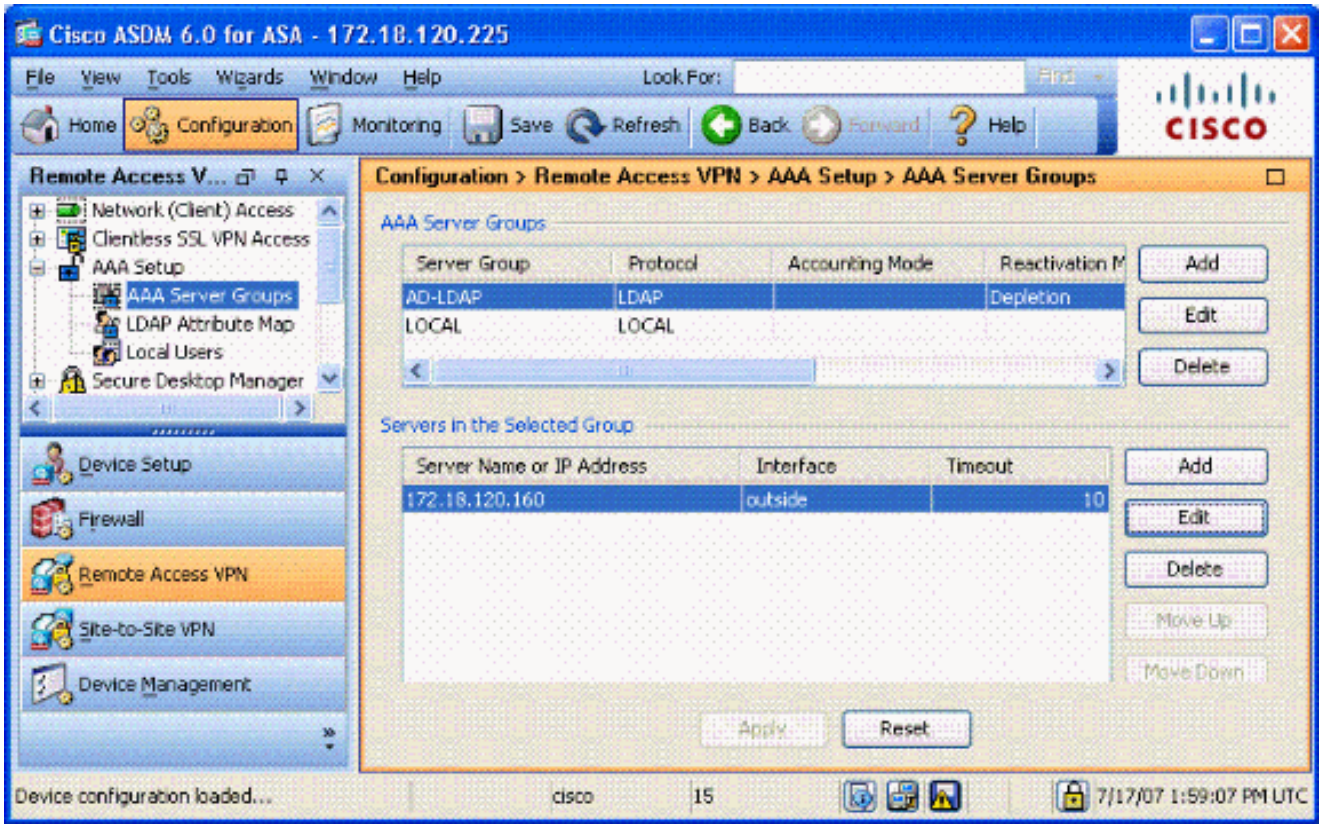
m. A configuração deve ser semelhante à Figura A5.

Figura A5: Configuração do mapa de atributos LDAP



4. Selecione Remote Access VPN> AAA Setup > AAA Server Groups. Veja a Figura A6.

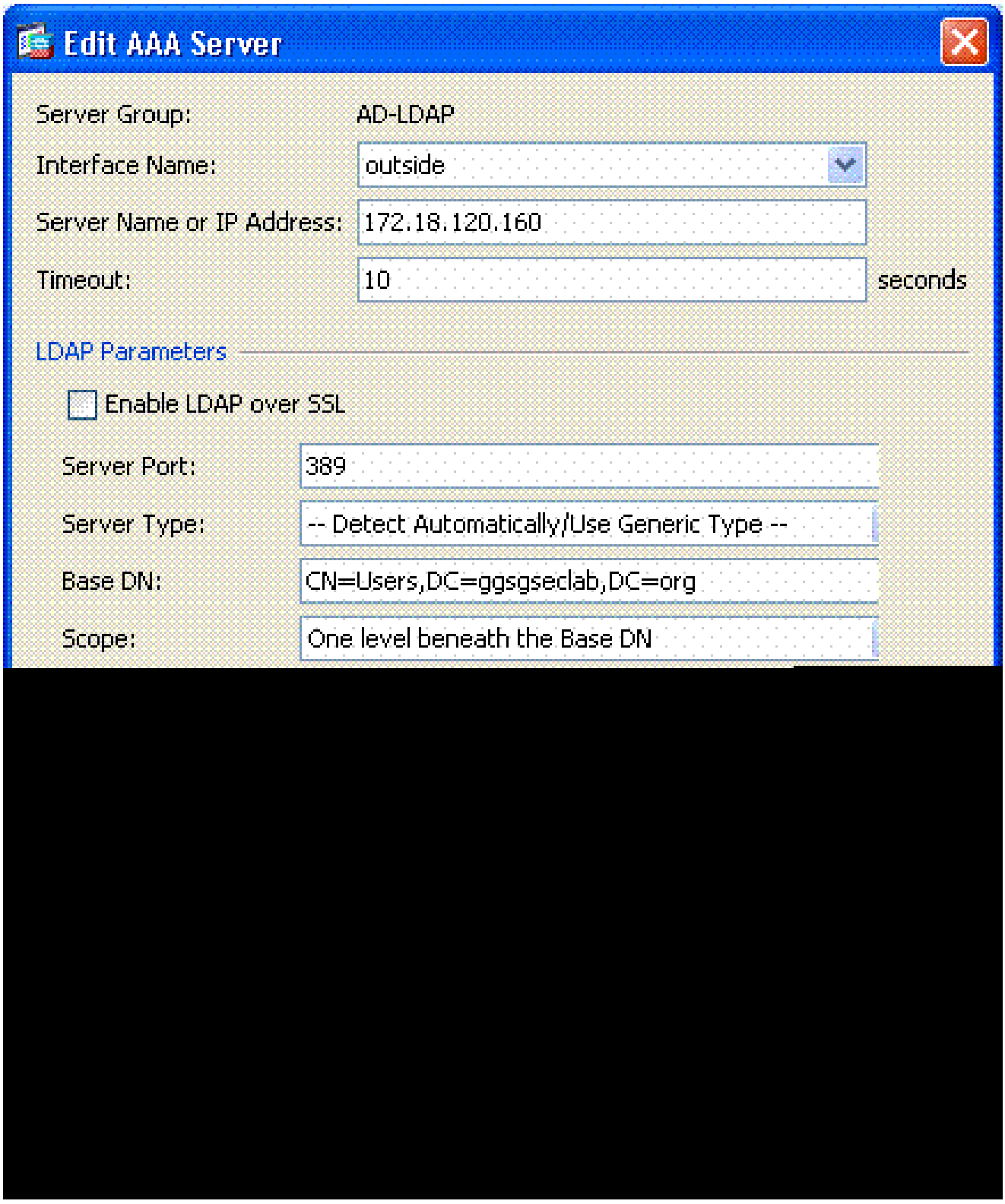
   Figura A6: Grupos de servidores AAA



5. Clique no grupo de servidores que deseja editar. Na seção Servidores do grupo selecionado, escolha o endereço IP ou o nome do host do servidor e clique em Editar.

6. Na janela Editar servidor AAA, na caixa de texto Mapa de atributos LDAP, escolha o mapa de atributos LDAP criado no menu suspenso. Veja a Figura A7

   Figura A7: Adicionando mapa de atributos LDAP



7. Click OK.

Observação: ative a depuração LDAP enquanto testa para verificar se a associação LDAP e o mapeamento de atributos funcionam corretamente. Consulte o Apêndice C para obter informações sobre comandos de solução de problemas.

Cenário 2: Aplicação do Ative Diretory usando a associação de Grupo para

Permitir/Negar Acesso

Este exemplo usa o atributo LDAP memberOf para mapear para o atributo Tunneling Protocol para estabelecer uma associação de grupo como uma condição. Para que essa política funcione, você deve ter estas condições:

- Use um grupo que já existe ou crie um novo grupo para usuários do ASA VPN para ser membro do para condições ALLOW.
- Use um grupo que já exista ou crie um novo grupo para usuários que não sejam do ASA para ser membro de condições DENY.
- Certifique-se de verificar no visualizador LDAP se você tem o DN correto para o grupo. Consulte o Apêndice D. Se o DN estiver errado, o mapeamento não funcionará corretamente.

Observação: lembre-se de que o ASA só pode ler a primeira string do atributo memberOf nesta versão. Verifique se o novo grupo criado está no topo da lista. A outra opção é colocar um caractere especial na frente do nome quando o AD observar os caracteres especiais primeiro. Para contornar esse problema, use o DAP no software 8.x para examinar vários grupos.

Observação: verifique se um usuário faz parte do grupo de negação ou de pelo menos um outro grupo para que o memberOf seja sempre enviado de volta ao ASA. Você não precisa especificar a condição de negação FALSA, mas a prática recomendada é fazê-lo. Se o nome do grupo existente ou o nome do grupo contiver um espaço, insira o atributo desta maneira:

```
CN=Operadores de backup,CN=Interno,DC=ggsgseclab,DC=org
```

Observação: o DAP permite que o ASA examine vários grupos no atributo memberOf e a autorização base dos grupos. Consulte a seção DAP.

MAPEAMENTO

- O valor do atributo do AD:
    - membroDe CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
    - membroDe CN=TelnetClients,CN=Users,DC=labrat,DC=com
- Valor do atributo Cisco: 1 = FALSE, 20 = TRUE,

Para a condição ALLOW, você mapeia:

- membroDe CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org= 20

Para a condição DENY, você mapeia:

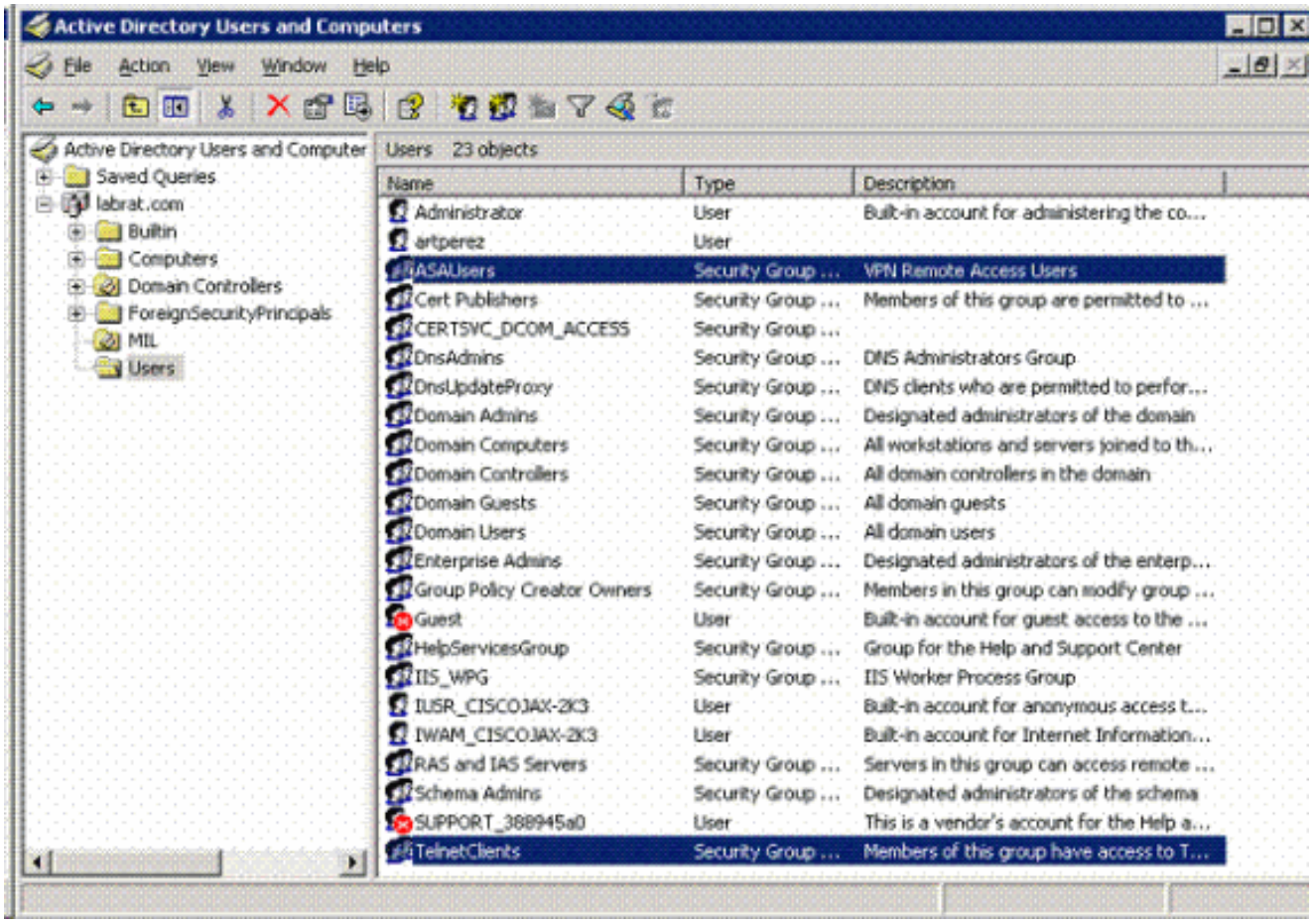
- memberOf CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org = 1

Observação: em uma versão futura, há um atributo Cisco para permitir e negar a conexão. Consulte Configuração de um Servidor Externo para Autorização de Usuário de Dispositivo de Segurança para obter mais informações sobre atributos da Cisco.

Configuração do Ative Diretory

1. No Servidor Ative Diretory, escolha Iniciar > Executar.
2. Na caixa de texto Abrir, digite dsa.msc e clique em Ok. Inicia o console de gerenciamento do ative diretory.
3. No console de gerenciamento do Ative Diretory, clique no sinal de mais para expandir Usuários e Computadores do Ative Diretory. Consulte a Figura A8

   Figura A8: Grupos do Ative Diretory



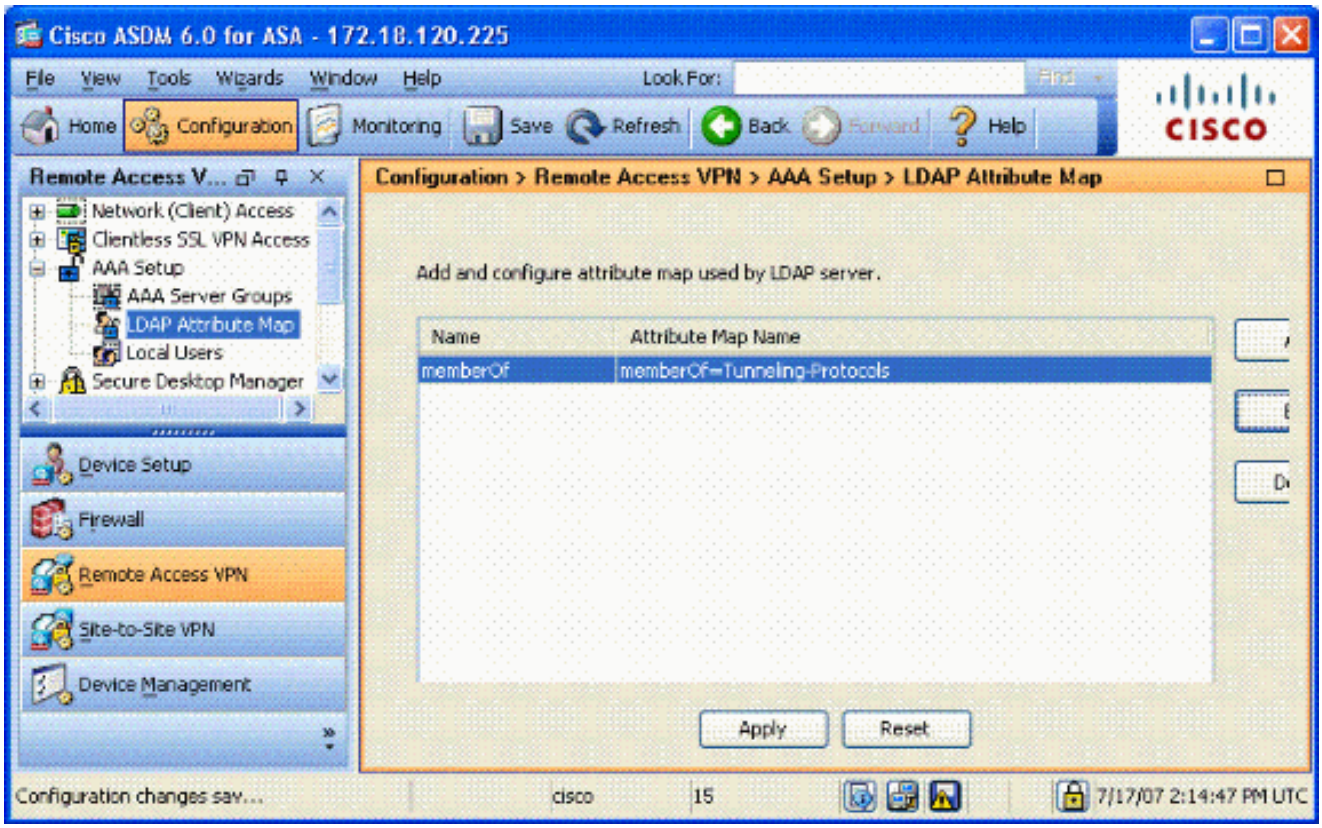
4. Clique no sinal de mais para expandir o nome de domínio.
5. Clique com o botão direito do mouse na pasta Users e escolha New > Group.
6. Insira um nome de grupo. Por exemplo: ASAUsers.

7. Click OK.
8. Clique na pasta Users e clique duas vezes no grupo que acabou de criar.
9. Escolha a guia Membros e clique em Adicionar.
10. Digite o Nome do usuário que deseja adicionar e clique em Ok.

Configuração do ASA

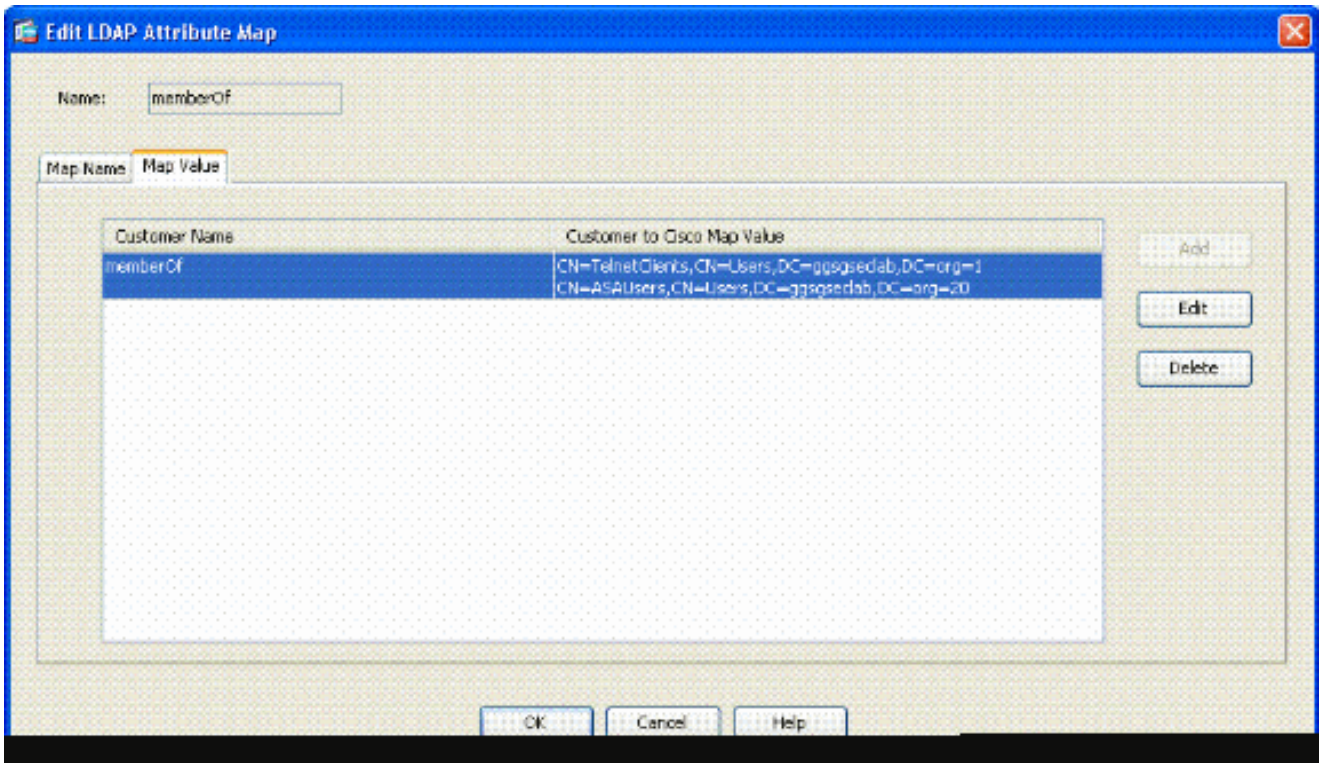
1. No ASDM, escolha Remote Access VPN > AAA Setup > LDAP Attribute Map.
2. Clique em Add.
3. Na janela Adicionar mapa de atributos LDAP, siga estas etapas. Veja a Figura A3.
    a. Digite um nome na caixa de texto Nome.
    b. Na guia Nome do Mapa, digite memberOf na caixa de texto Nome do Cliente c.
    c. Na guia Nome do mapa, escolha Tunneling-Protocols na opção suspensa no Nome da Cisco.
    d. Escolha Adicionar.
    e. Clique na guia Mapear Valor.
    f. Escolha Adicionar.
    g. Na janela Adicionar valor de mapa LDAP de atributo, digite CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org na caixa de texto Nome do cliente e digite 20 na caixa de texto Valor da Cisco.
    h. Clique em Add.
    i. Digite CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org na caixa de texto Nome do cliente e digite 1 na caixa de texto Valor da Cisco. Veja a Figura A4.
    j. Click OK.
    k. Click OK.
    l. Clique em Apply.
    m. A configuração deve ser semelhante à Figura A9.

Figura A9 Mapa de atributos LDAP



4. Selecione Remote Access VPN> AAA Setup > AAA Server Groups.

5. Clique no grupo de servidores que deseja editar. Na seção Servidores do grupo selecionado, selecione o endereço IP ou o nome do host do servidor e clique em Editar



6. Na janela Editar servidor AAA, na caixa de texto Mapa de atributos LDAP, selecione o mapa de atributos LDAP criado no menu suspenso.

7. Click OK.

Observação: ative a depuração LDAP enquanto testa para verificar se a associação LDAP e os mapeamentos de atributos funcionam corretamente. Consulte o Apêndice C para obter informações sobre comandos de solução de problemas.

Cenário 3: Políticas de acesso dinâmico para vários atributos memberOf

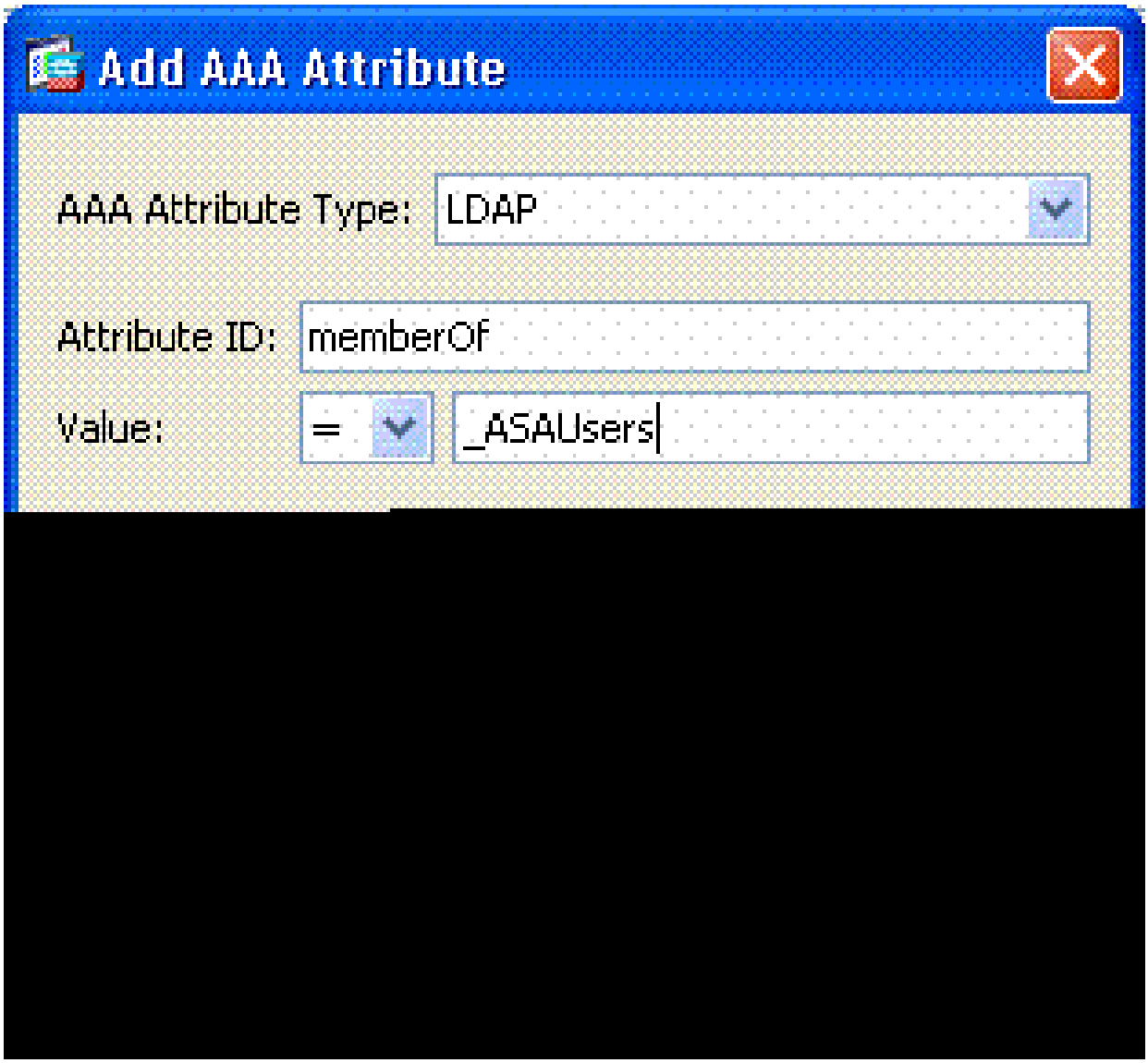
Este exemplo usa o DAP para examinar vários atributos memberOf a fim de permitir o acesso com base na associação de grupo do Ative Diretory. Antes do 8.x, o ASA lia apenas o primeiro atributo memberOf. Com o 8.x e posterior, o ASA pode examinar todos os atributos memberOf.

- Use um grupo que já existe ou crie um novo grupo (ou vários grupos) para usuários do ASA VPN para ser membro do para condições ALLOW.
- Use um grupo que já exista ou crie um novo grupo para usuários que não sejam do ASA para ser membro de condições DENY.
- Certifique-se de verificar no visualizador LDAP se você tem o DN correto para o grupo. Consulte o Apêndice D. Se o DN estiver errado, o mapeamento não funcionará corretamente.

Configuração do ASA

1. No ASDM, escolha Remote Access VPN> Network (Client) Access > Dynamic Access Policies.
2. Clique em Add.
3. Em Adicionar política de acesso dinâmico, siga estas etapas:
    a. Digite um nome na caixa de texto Nome b.
    b. Na seção de prioridade, digite 1 ou um número maior que 0.
    c. Em Critérios de Seleção, clique em Adicionar.
    d. Em Add AAA Attribute, escolha LDAP .
    e. Na seção ID do atributo, insira memberOf.
    f. Na seção de valor, escolha = e insira o nome do grupo do AD. Repita essa etapa para cada grupo que você deseja referenciar. Veja a figura A10.

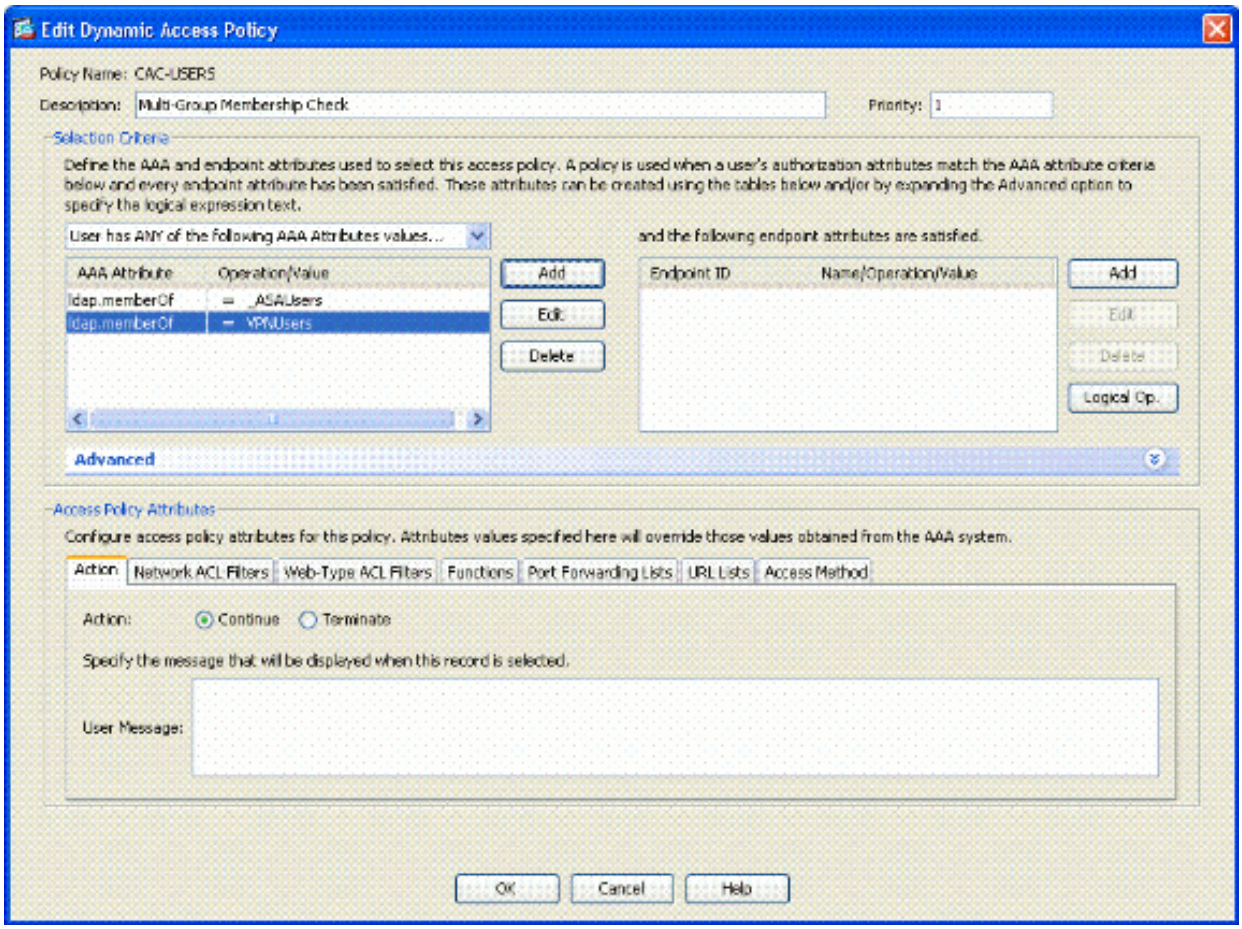
    Figura A10 Mapa de Atributos AAA



g. Click OK.

h. Na seção Atributos da política de acesso, escolhaContinuar. Veja a figura A11.

Figura A11 - Adicionar política dinâmica

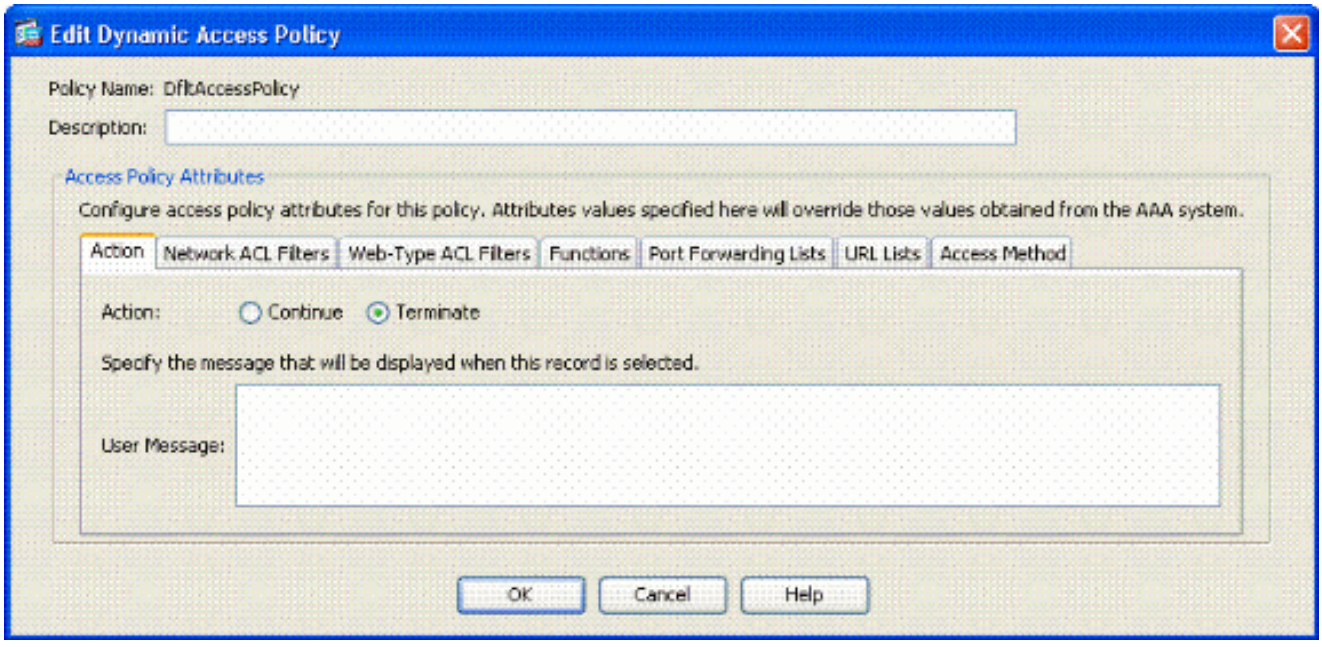


4. No ASDM, escolha Remote Access VPN> Network (Client) Access > Dynamic Access Policies.

5. Escolha Default Access Policy e escolha Edit.

6. A ação padrão deve ser definida como Terminar. Veja a figura A12.

   Figura A12 Editar política dinâmica



7. Click OK.

Observação: se a opção Terminar não estiver selecionada, você poderá entrar, mesmo que não esteja em nenhum grupo, pois o padrão é Continuar.

Apêndice B - Configuração do ASA CLI

ASA 5510

```
<#root>

ciscoasa#

show running-config

: Saved
:
ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
--------------ACL's-----------------------------------------------
access-list out extended permit ip any any
------------------------------------------------------------------
pager lines 24
logging console debugging
mtu outside 1500
!
---------------VPN Pool-------------------------------------------
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
------------------------------------------------------------------
!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout uauth 0:05:00 absolute
!
-------------------------LDAP Maps & DAP--------------------------
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
March 11, 2008 ASA - CAC Authentication for AnyConnect VPN Access
Company Confidential. A printed copy of this document is considered uncontrolled.
49
map-value memberOf CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
------------------------------------------------------------------------
!
--------------------LDAP Server-------------------------------------
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=ggsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=ggsgseclab,DC=org
------------------------------------------------------------------------
!
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
----------------CA Trustpoints-----------------------------------
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint2
```

```
revocation-check ocsp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check ocsp none
enrollment terminal
crl configure
!
------------------Certificate Map-----------------------------
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
--------------------CA Certificates (Partial Cert is Shown)------------
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74
crypto ca certificate chain ASDM_TrustPoint1
certificate 319e
30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01
01050500
305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
crypto ca certificate chain ASDM_TrustPoint2
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5
6fc20a76
crypto ca certificate chain ASDM_TrustPoint3
certificate ca 05
30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101
05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032
301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a
305b310b
30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
1303504b
49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
```

```
30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353 20332052
6f6f7420
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
!
-------------------------SSL/WEBvpn-windows-----------------------------------
ssl certificate-authentication interface outside port 443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
-----------------------------------------------------------------------
-----------------------VPN Group/Tunnel Policy--------------------
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-windows-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-windows-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
```

```
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
------------------------------------------------------------------
prompt hostname context
```

Apêndice C - Solução de problemas

Troubleshooting de AAA e LDAP

- debug ldap 255 — Exibe trocas de LDAP
- debug aaa common 10 — Exibe trocas de AAA

Exemplo 1: Conexão permitida com mapeamento de atributo correto

Este exemplo mostra a saída de debug ldap e debug aaa common durante uma conexão bem-sucedida com o cenário 2 mostrado no Apêndice A.

Figura C1: debug LDAP e debug aaa common output - mapeamento correto

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap:// 172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160, status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
```

```
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..5O........../........6O...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[78] userCertificate: value =
0..'0........../..t.....5O...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = ................q......mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-----------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
```

```
User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#
```

Exemplo 2: Conexão permitida com mapeamento de atributo Cisco configurado incorretamente

Este exemplo mostra a saída de debug ldap e debug aaa common durante uma conexão permitida com o cenário 2 mostrado no Apêndice A.

Figura C2: debug LDAP e debug aaa common output - mapeamento incorreto

```
AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
```

```
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389, status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50........../........60...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[82] userCertificate: value =
0..'0........../..t.....50...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = ................q......mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
```

```
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
```

```
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

Troubleshooting de DAP

- debug dap errors — Exibe erros DAP
- debug dap trace — Exibe o rastreamento da função DAP

Exemplo 1: Conexão permitida com DAP

Este exemplo mostra a saída de debug dap errors e debug dap trace durante uma conexão bem-sucedida com o cenário 3 mostrado no Apêndice A. Observe vários atributos memberOf. Você pode pertencer a _ASAUsers e VPNUsers ou a ambos os grupos, que dependem da configuração do ASA.

Figura C3: DAP de depuração

```
<#root>

#

debug dap errors

debug dap errors enabled at level 1
#

debug dap trace

debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
-----------------------------------------------------------------------
---
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
```

```
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2 = _ASAUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
```

```
"VPNUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

Exemplo 2: Conexão negada com DAP

Este exemplo mostra a saída de debug dap errors e debug dap trace durante uma conexão malsucedida com o cenário 3 mostrado no Apêndice A.

Figura C4: DAP de depuração

```
<#root>
```

```
#

debug dap errors

debug dap errors enabled at level 1
#

debug dap trace

debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
------------------------------------------------------------------------
---
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
```

```
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] = "DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
```

Solução de problemas de Autoridade de certificação / OCSP

- debug crypto ca 3
- No modo de configuração—logging class ca console(or buffer) debugging

Estes exemplos mostram uma validação de certificado bem-sucedida com o respondente OCSP e uma política de correspondência de grupo de certificados com falha.

A Figura C3 mostra a saída de depuração que tem um certificado validado e um grupo de certificados de trabalho correspondentes à Política.

A Figura C4 mostra a saída de depuração de uma política de correspondência de grupo de certificados mal configurada.

A Figura C5 mostra a saída de depuração de um usuário com um certificado revogado.

Figura C5: Depuração OCSP - validação de certificado bem-sucedida

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
```

```
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap, index 10 for
WebVPN group map processing. No tunnel group is configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for WebVPN group map
```

Figura C5: Saída de uma política de correspondência de grupo de certificados com falha

Figura C5: Resultado de um certificado revogado

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,valdid cor =noct
oamuthori,zed.
map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence # 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name:
cn=ggsgseclab,dc=ggsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule: subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
```

```
Hunt,ou=MIL,dc=ggsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

Apêndice D - Verificar objetos LDAP no MS

No CD do Microsoft Server 2003, há ferramentas adicionais que podem ser instaladas para exibir a estrutura LDAP, bem como os objetos/atributos LDAP. Para instalar essas ferramentas, vá para o diretório Support no CD e depois Tools. Instale o SUPTOOLS.MSI.

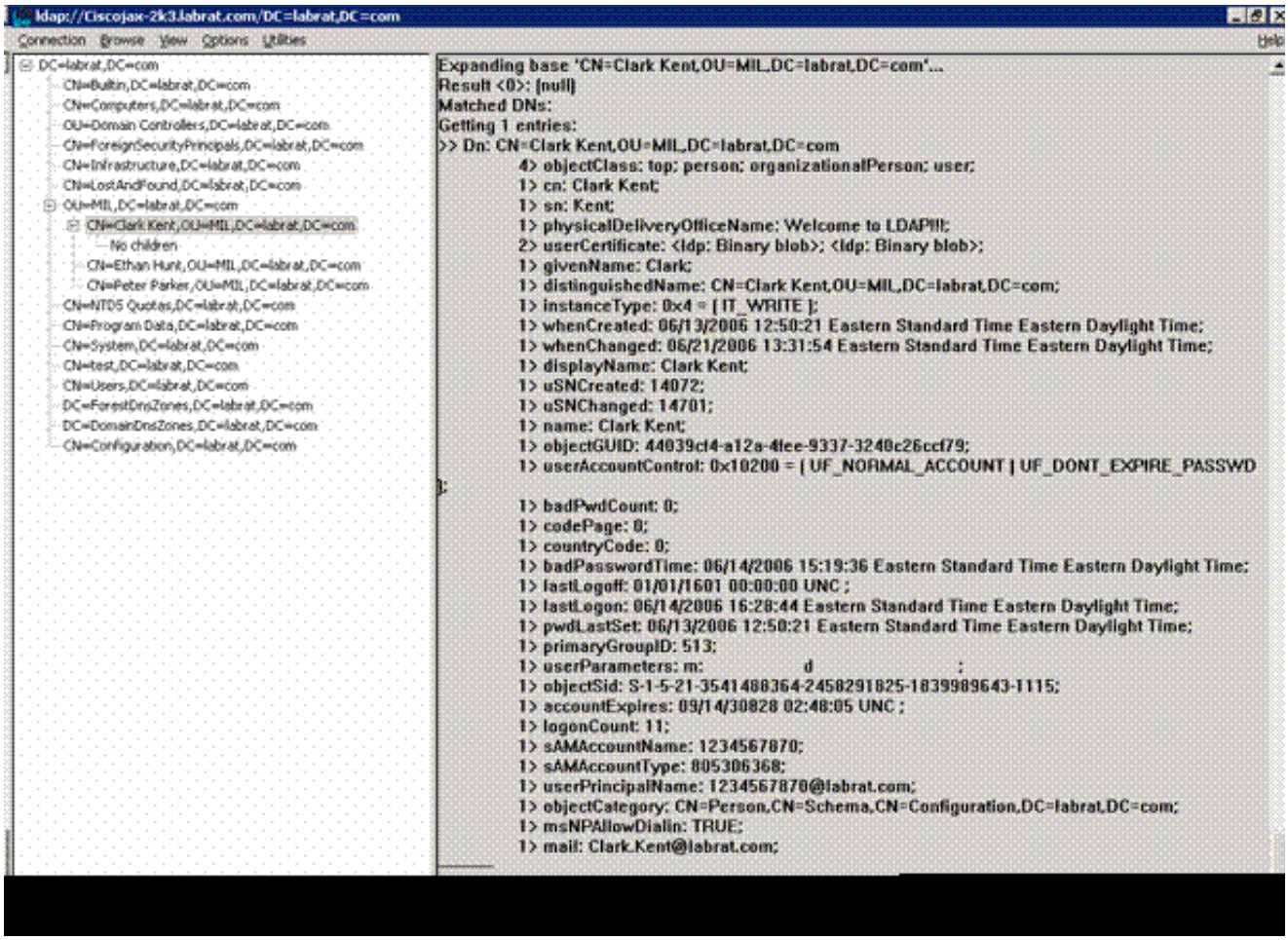
Visualizador LDAP

1. Após a instalação, escolha Start > Run.
2. Digite ldp e clique em Ok. Isso inicia o visualizador LDAP.
3. Escolha Connection > Connect.
4. Insira o nome do servidor e clique em Ok.
5. Escolha Connection > Bind.
6. Insira um nome de usuário e uma senha.

   > Observação: você precisa de direitos de administrador.

7. Click OK.
8. Exibir objetos LDAP. Veja a Figura D1.

   Figura D1: Visualizador LDAP

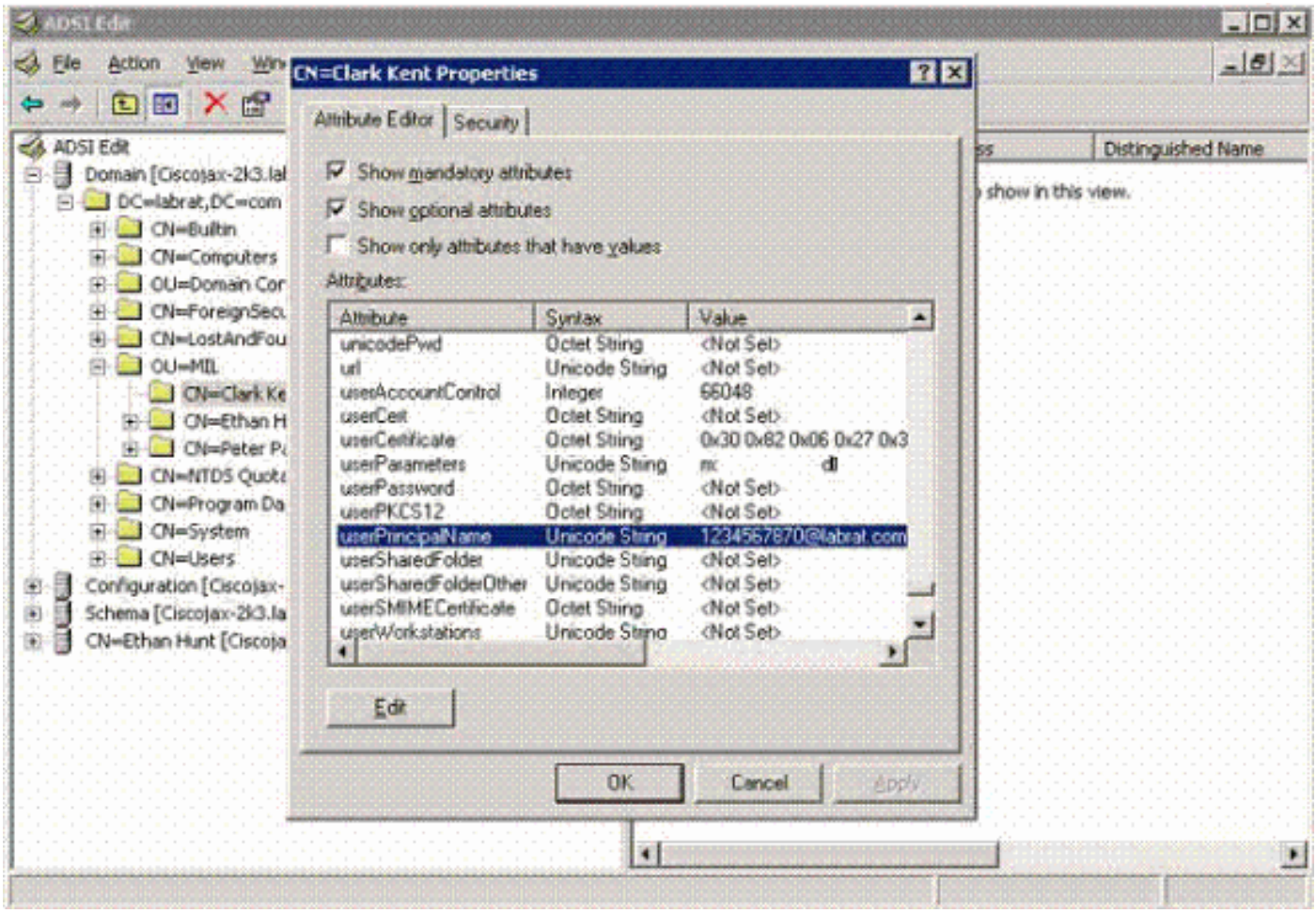


Editor de Interface de Serviços do Ative Diretory

- No servidor Ative Diretory, escolha Iniciar > Executar.
- Digite adsiedit.msc. Isso inicia o editor.
- Clique com o botão direito do mouse em um objeto e clique em Propriedades.

Esta ferramenta mostra todos os atributos para objetos específicos. Veja a Figura D2.

Figura D2: Edição de ADSI



Apêndice E

Um perfil do AnyConnect pode ser criado e adicionado a uma estação de trabalho. O perfil pode fazer referência a vários valores, como hosts ASA ou parâmetros de correspondência de certificado, como nome distinto ou emissor. O perfil é armazenado como um arquivo .xml e pode ser editado com o Bloco de Notas. O arquivo pode ser adicionado a cada cliente manualmente ou enviado do ASA por meio de uma política de grupo. O arquivo está armazenado em:

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile
```

Conclua estes passos:

1. Escolha o AnyConnectProfile.tmpl e abra o arquivo com o Bloco de Notas.
2. Faça as modificações apropriadas no arquivo, como o IP do emissor ou do host. Veja a Figura F1, por exemplo.
3. Quando terminar, salve o arquivo como .xml.

Consulte a documentação do Cisco AnyConnect com relação ao gerenciamento de perfil.

Resumindo:

- Um perfil deve ter um nome exclusivo para sua empresa. Um exemplo é: CiscoProfile.xml
- O nome do perfil deve ser o mesmo, mesmo que seja diferente para grupos individuais dentro da empresa.

Esse arquivo deve ser mantido por um administrador do Secure Gateway e distribuído com o software cliente. O perfil baseado nesse XML pode ser distribuído aos clientes a qualquer momento. Os mecanismos de distribuição suportados são como um arquivo empacotado com a distribuição de software ou como parte do mecanismo de download automático. O mecanismo de download automático está disponível somente com determinados produtos Cisco Secure Gateway.

> Observação: os administradores são altamente incentivados a validar o perfil XML que criam com uma ferramenta de validação on-line ou através da funcionalidade de importação de perfil no ASDM. A validação pode ser realizada com o AnyConnectProfile.xsd encontrado nesse diretório. AnyConnectProfile é o elemento raiz que representa o AnyConnect Client Profile.

Este é um exemplo de um arquivo XML do Perfil do Cisco AnyConnect VPN Client.

```
<#root>

xml version="1.0" encoding="UTF-8"
- - <AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">


!--- The ClientInitialization section represents global settings !--- for the client. In some cases, fo
!--

-->
-
 <ClientInitialization>


!--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence.


-->

<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>


!--- This control enables an administrator to have a one time !--- message displayed prior to a users t
```

```
<ShowPreConnectMessage>false</ShowPreConnectMessage>

!-- This section enables the definition of various attributes !--- that can be used to refine client ce


-->
-
<CertificateMatch>

!--- Certificate Distinguished Name matching allows !--- for exact match criteria in the choosing of ac


- <DistinguishedName>
- <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>

-
!-- This section contains the list of hosts from which !--- the user is able to select.

-
<ServerList>



!--- This is the data needed to attempt a connection to !--- a specific host.

-->
-
<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntry>
- <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Informações Relacionadas

- Certificados e CRLs especificados por X.509 e RFC 3280
- OCSP especificado pelo RFC 2560
- Introdução à infraestrutura de chave pública
- "OCSP leve" perfilado pelo padrão de rascunho
- SSL / TLS especificado pelo RFC 2246

- 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.