ASA 8.x: Configuración de AnyConnect SSL VPN CAC-SmartCards para Windows

Contenido

Introducción

Este documento proporciona una configuración de muestra en Cisco Adaptive Security Appliance (ASA) para el acceso remoto de AnyConnect VPN para Windows con Common Access Card (CAC) para la autenticación.

El objetivo de este documento es cubrir la configuración de Cisco ASA con Adaptive Security Device Manager (ASDM), Cisco AnyConnect VPN Client y Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP).

La configuración de esta guía utiliza el servidor de Microsoft AD/LDAP. Este documento también cubre funciones avanzadas como OCSP, mapas de atributos LDAP y políticas de acceso dinámico (DAP).

Prerequisites

Requirements

Un conocimiento básico de Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP y Public Key Infrastructure (PKI) es beneficioso para la comprensión de la configuración completa. La familiaridad con la pertenencia al grupo AD, las propiedades de usuario y los objetos LDAP ayuda a correlacionar el proceso de autorización entre los atributos de certificado y los objetos AD/LDAP.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5500 Series Adaptive Security Appliance (ASA) que ejecuta la versión de software 8.0(x) y posteriores

- Cisco Adaptive Security Device Manager (ASDM) versión 6.x para ASA 8.x
- Cisco AnyConnect VPN Client para Windows

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configuración de Cisco ASA

Esta sección trata sobre la configuración de Cisco ASA a través de ASDM. Describe los pasos necesarios para implementar un túnel de acceso remoto VPN a través de una conexión SSL AnyConnect. El certificado CAC se utiliza para la autenticación y el atributo Nombre principal de usuario (UPN) del certificado se rellena en Active Directory para la autorización.

Consideraciones de implementación

- Esta guía NO cubre configuraciones básicas como interfaces, DNS, NTP, routing, acceso de dispositivos, acceso ASDM, etc. Se supone que el operador de red está familiarizado con estas configuraciones.

  Consulte Dispositivos de Seguridad Multifunción para obtener más información.

- Las secciones resaltadas en ROJO son configuraciones obligatorias necesarias para el acceso VPN básico. Por ejemplo, un túnel VPN se puede configurar con la tarjeta CAC sin realizar comprobaciones de OCSP, asignaciones LDAP y comprobaciones de política de acceso dinámico (DAP). DoD exige la verificación de OCSP, pero el túnel funciona sin OCSP configurado.
- Las secciones resaltadas en AZUL son funciones avanzadas que se pueden incluir para aportar más seguridad al diseño.
- ASDM y AnyConnect/SSL VPN no pueden utilizar los mismos puertos en la misma interfaz. Se recomienda cambiar los puertos de uno u otro para obtener acceso. Por ejemplo, utilice el puerto 445 para ASDM y deje 443 para AC/SSL VPN. El acceso a la URL de ASDM ha cambiado en 8.x. Utilice `https://<ip_address>:<port>/admin.html`.
- La imagen de ASA requerida es al menos 8.0.2.19 y ASDM 6.0.2.
- AnyConnect/CAC es compatible con Vista.
- Consulte el Apéndice A para ver ejemplos de mapeo de políticas de acceso dinámicas y LDAP para la aplicación de políticas adicionales.
- Consulte el Apéndice D para ver cómo verificar los objetos LDAP en MS.
- Consulte Información Relacionada para obtener una lista de puertos de aplicación para la

configuración del firewall.

Configuración de Autenticación, Autorización y Contabilización (AAA)

Se le autentica con el uso del certificado en su Common Access Card (CAC) a través del servidor de la autoridad certificadora (CA) de DISAC o del servidor de la CA de su propia organización. El certificado debe ser válido para el acceso remoto a la red. Además de la autenticación, también debe tener autorización para utilizar un objeto de Microsoft Active Directory o protocolo ligero de acceso a directorios (LDAP). El Departamento de defensa (DoD) requiere el uso del atributo de nombre principal de usuario (UPN) para la autorización, que forma parte de la sección de nombre alternativo de sujeto (SAN) del certificado. El UPN o EDI/PI debe estar en este formato, 1234567890@mil. Estas configuraciones muestran cómo configurar el servidor AAA en ASA con un servidor LDAP para autorización. Consulte el Apéndice A para obtener información sobre la configuración adicional con la asignación de objetos LDAP.

Configurar servidor LDAP

Complete estos pasos:

1. Elija Remote Access VPN > AAA Setup > AAA Server Group.
2. En la tabla de grupos de servidores AAA, haga clic en Add 3.
3. Ingrese el nombre del grupo de servidores y elija LDAP en el botón de opción protocol. Consulte la Figura 1.
4. En Servidores de la tabla de grupos seleccionada, haga clic en Agregar. Asegúrese de que el servidor que ha creado está resaltado en la tabla anterior.
5. En la ventana edit AAA server (editar servidor AAA), realice estos pasos. Consulte la Figura 2.

Nota: Elija la opción Enable LDAP over SSL si su LDAP/AD está configurado para este tipo de conexión.

---

a. Elija la interfaz donde se encuentra LDAP. Esta guía muestra el interior de la interfaz.

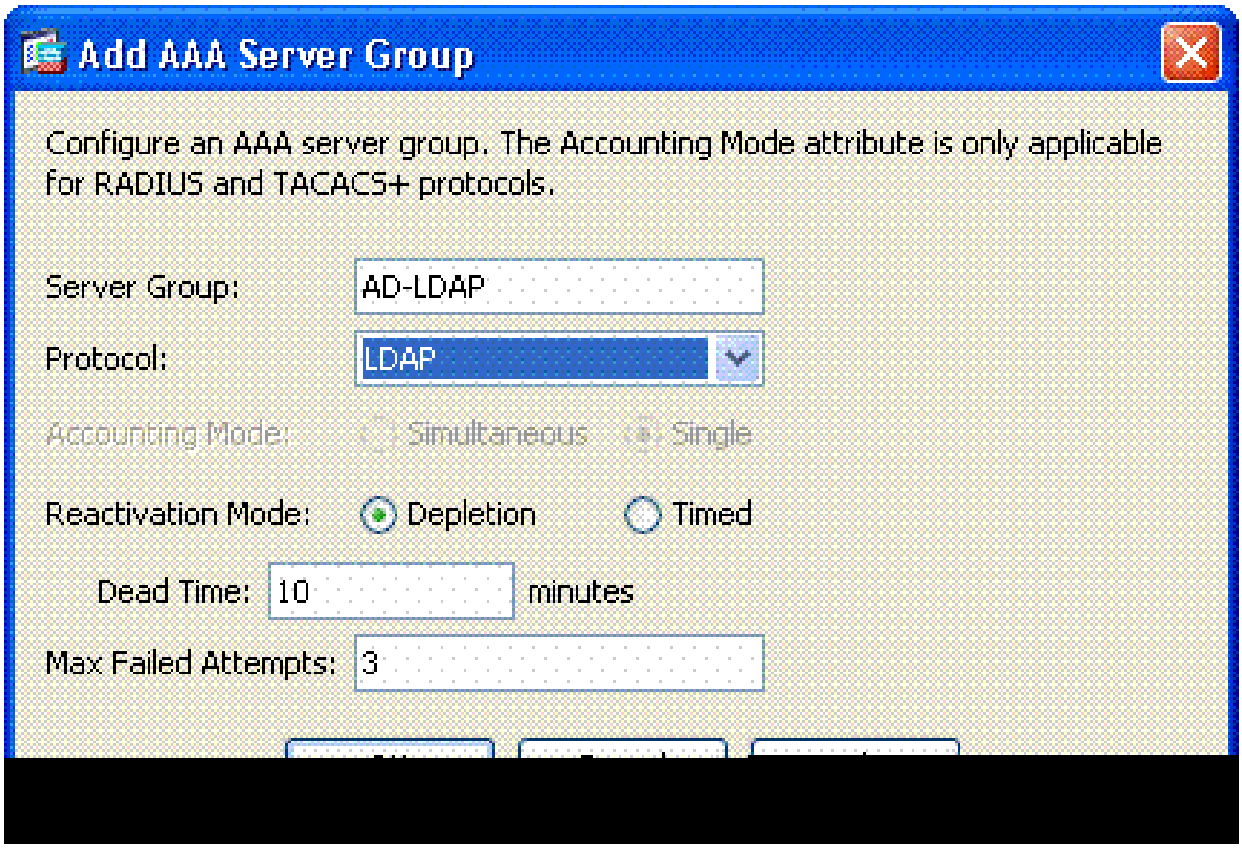
b. Introduzca la dirección IP del servidor.

c. Introduzca el puerto del servidor. El puerto LDAP predeterminado es 389.

d. Elija Tipo de servidor.

e. Introduzca DN base. Pida estos valores a su administrador de AD/LDAP.

Figura -1



f. En la opción alcance, elija la respuesta adecuada. Esto depende del DN base. Pida ayuda a su administrador de AD/LDAP.

g. En el atributo de nomenclatura, introduzca userPrincipalName. Este es el atributo que se utiliza para la autorización de usuario en el servidor AD/LDAP.

h. En el DN de inicio de sesión, introduzca el DN del administrador.

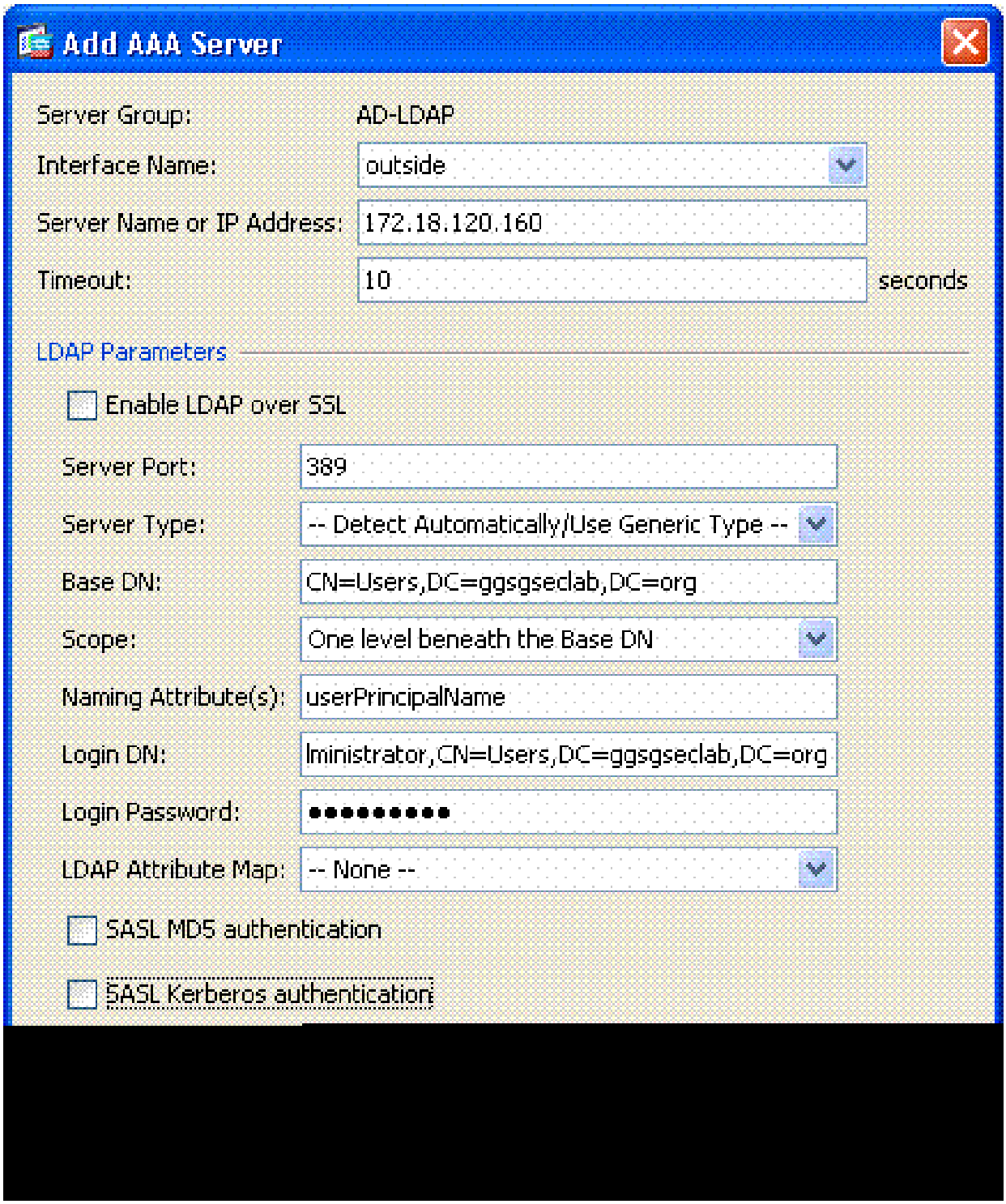
Nota: Tiene derechos administrativos o derechos para ver/buscar la estructura LDAP que incluye objetos de usuario y pertenencia a grupos.

---

i. En el campo Contraseña de inicio de sesión, introduzca la contraseña del administrador.

j. Deje el atributo LDAP en none.

Figura -2



Nota: Esta opción se utiliza más adelante en la configuración para agregar otro objeto AD/LDAP para autorización.

k. Elija Aceptar.

6. Elija Aceptar.

Administrar certificados

Hay dos pasos para instalar los certificados en el ASA. En primer lugar, instale los certificados de

CA (autoridad de certificados raíz y subordinada) necesarios. En segundo lugar, inscriba el ASA en una CA específica y obtenga el certificado de identidad. DoD PKI utiliza estos certificados, Root CA2, Class 3 Root, CA## Intermediate con el que está inscrito el ASA, ASA ID certificate y OCSP certificate. Sin embargo, si decide no utilizar OCSP, no es necesario instalar el certificado OCSP.

> Nota: Póngase en contacto con su POC de seguridad para obtener certificados raíz, así como instrucciones sobre cómo inscribirse en un certificado de identidad para un dispositivo. Un certificado SSL debe ser suficiente para ASA para el acceso remoto. No se requiere un certificado SAN dual.

> Nota: La máquina local también debe tener instalada la cadena DoD CA. Los certificados se pueden ver en el Almacén de certificados de Microsoft con Internet Explorer. DoD ha creado un archivo por lotes que agrega automáticamente todas las CA al equipo. Solicite más información a su PKI POC.

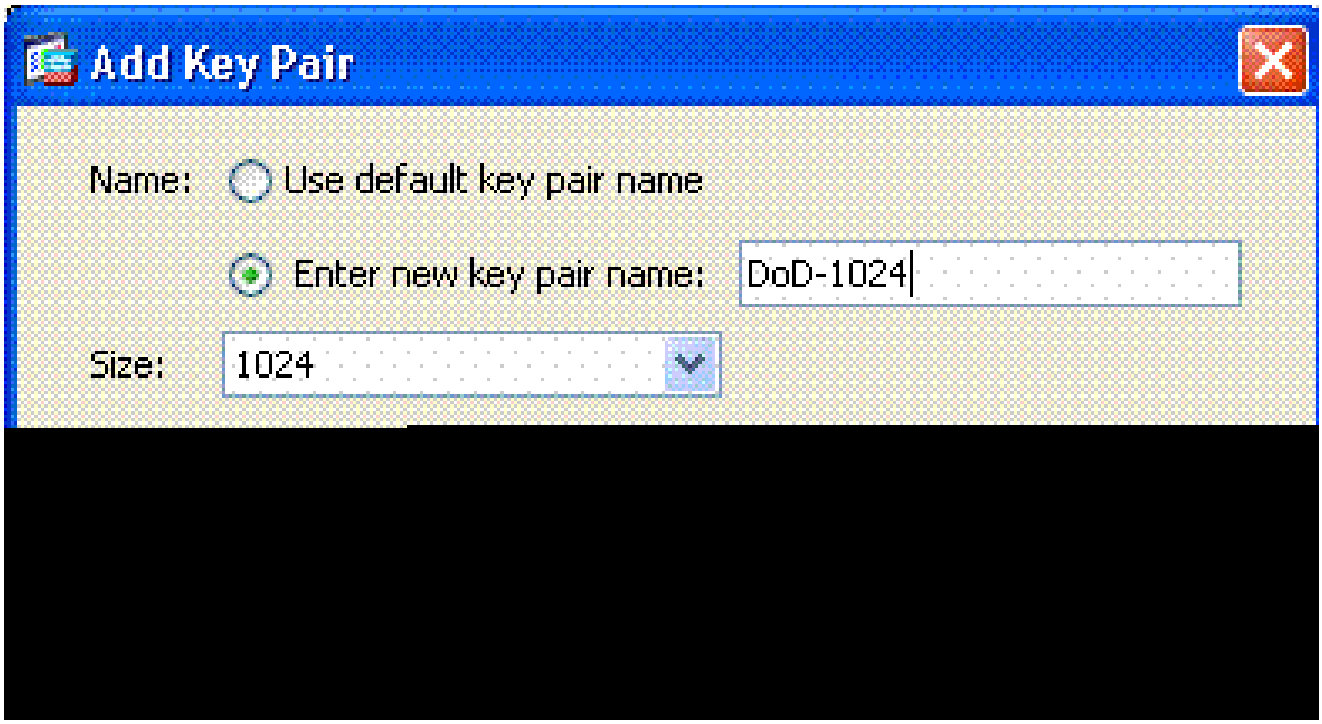
> Nota: DoD CA2 y la raíz de clase 3, así como el ID de ASA y el intermedio de CA que emitió el certificado de ASA, deben ser las únicas CA necesarias para la autenticación del usuario. Todos los intermediarios de CA actuales pertenecen a la cadena raíz de CA2 y Clase 3 y son de confianza siempre que se agreguen las raíces de CA2 y Clase 3.

Generar claves

Complete estos pasos:

1. Elija Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Elija Add a new id certificate y luego New by the key pair option.
3. En la ventana Add Key Pair, ingrese un nombre de clave, DoD-1024. Haga clic en la radio para agregar una nueva clave. Vea la figura 3.

   Figure 3



4. Elija el tamaño de la clave.
5. Mantenga el uso para uso general.
6. Haga clic en Generar ahora.

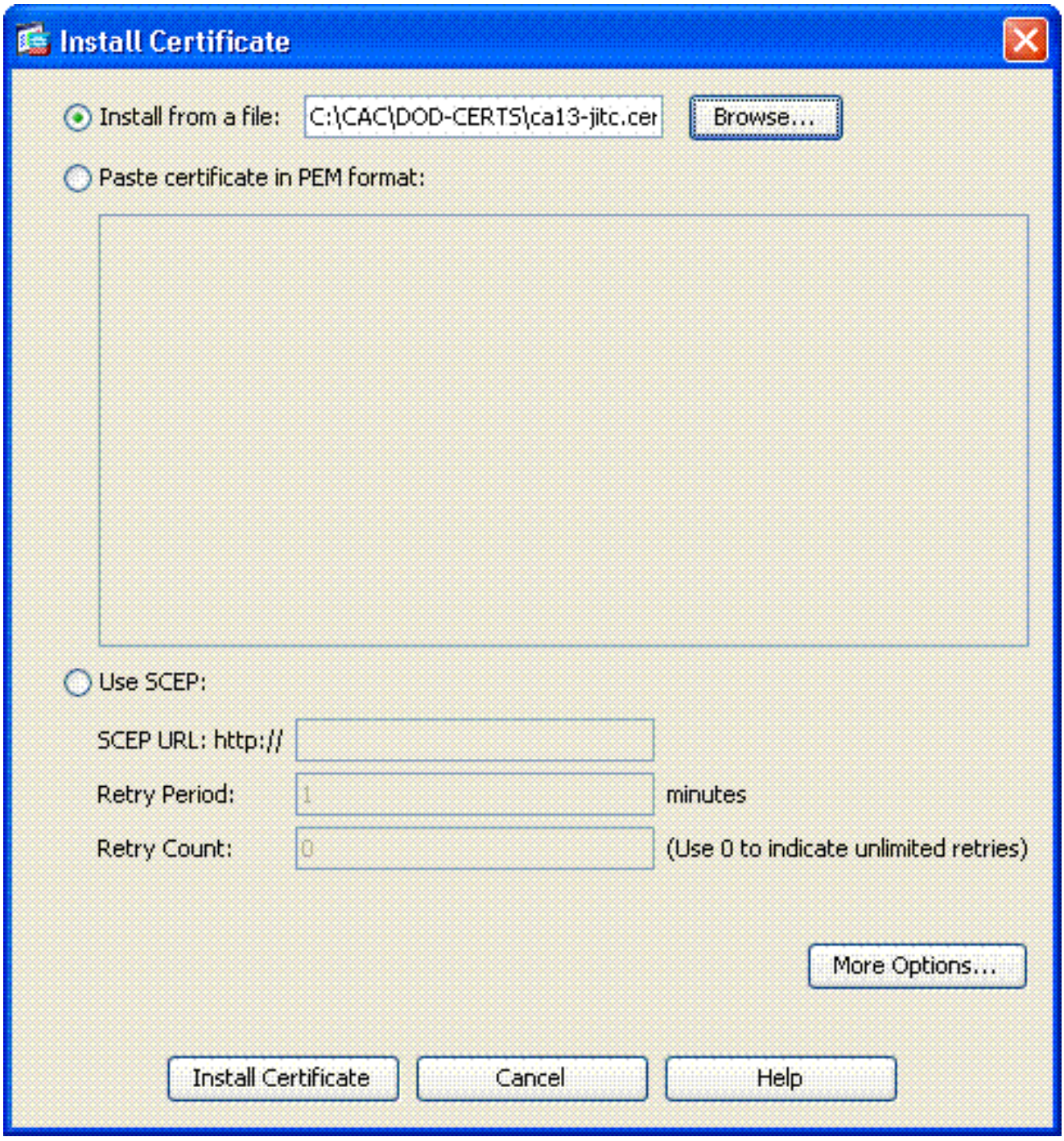
> Nota: DoD Root CA 2 utiliza una clave de 2048 bits. Se debe generar una segunda clave que utilice un par de claves de 2048 bits para poder utilizar esta CA. Complete los pasos anteriores para agregar una segunda clave.

Instalar certificados de CA raíz

Complete estos pasos:

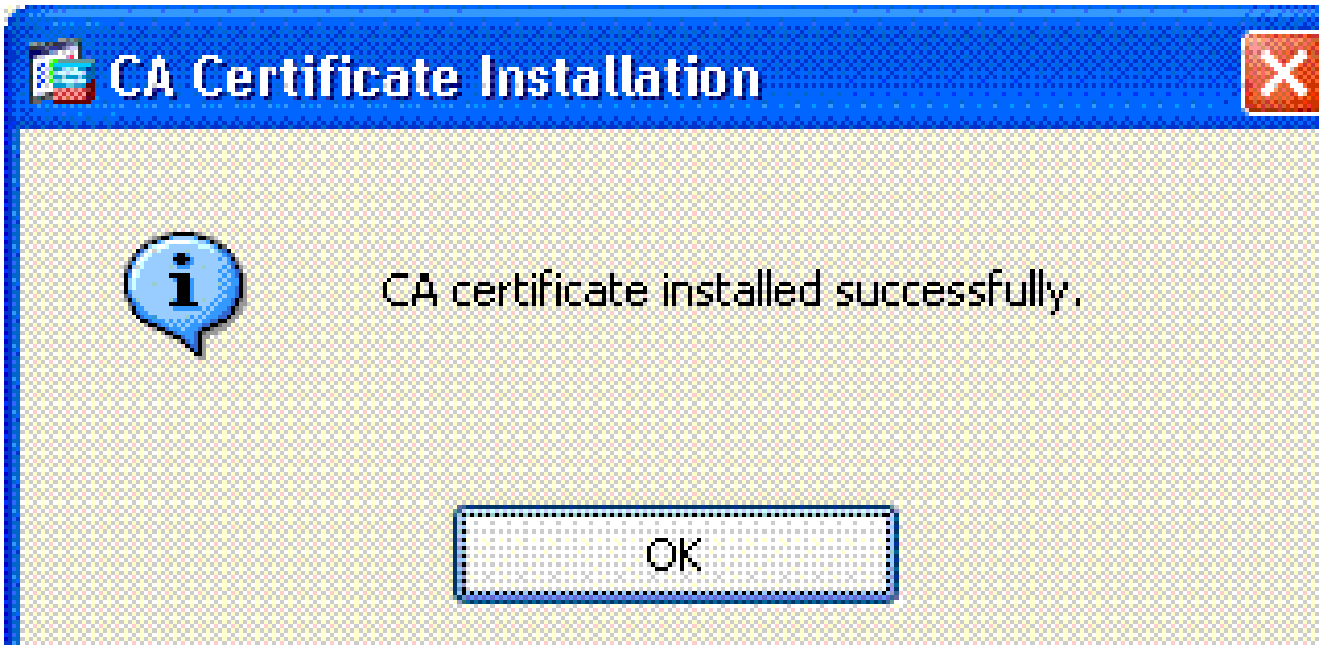
1. Elija Remote Access VPN > Certificate Management > CA Certificate > Add.
2. Elija Install from File y busque el certificado.
3. Elija Install Certificate.

Figura 4: Instalación del certificado raíz



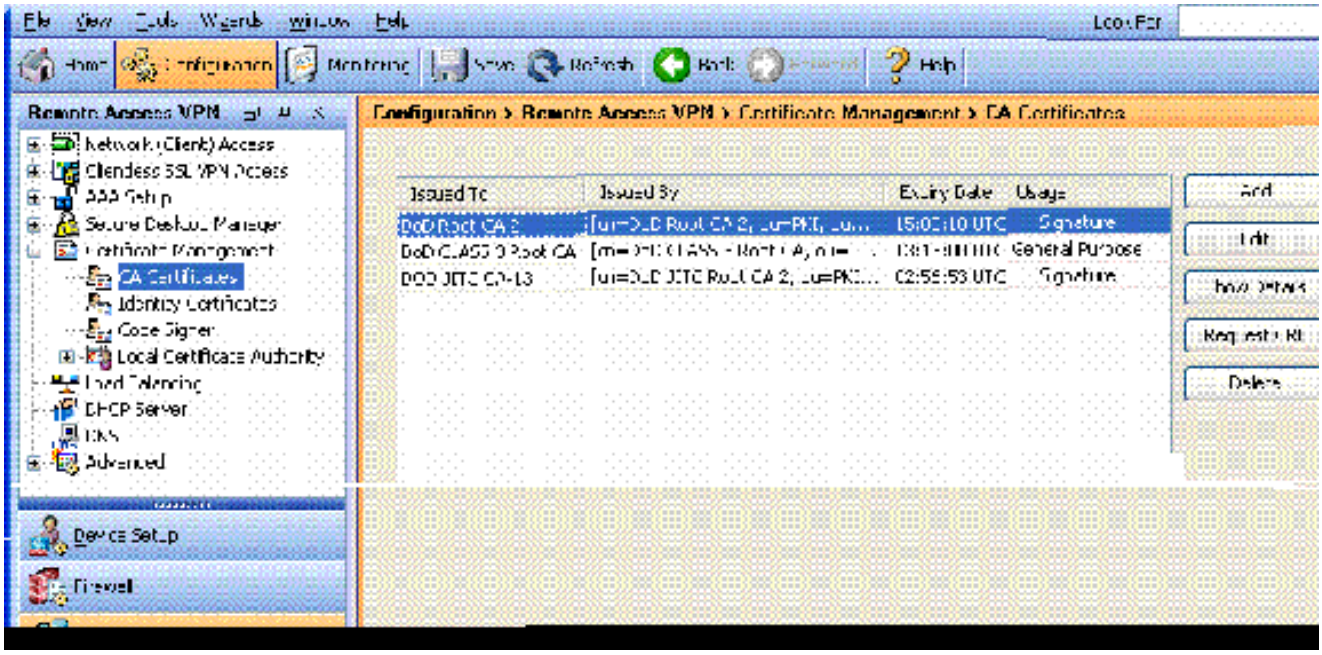
4. Debería aparecer esta ventana. Consulte la Figura 5.

Figure 5



Nota: Repita los pasos 1 a 3 para cada certificado que desee instalar. DoD PKI requiere un certificado para cada uno de estos elementos: raíz CA 2, raíz clase 3, CA## intermedio, ID de ASA y servidor OCSP. El certificado OCSP no es necesario si no utiliza OCSP.

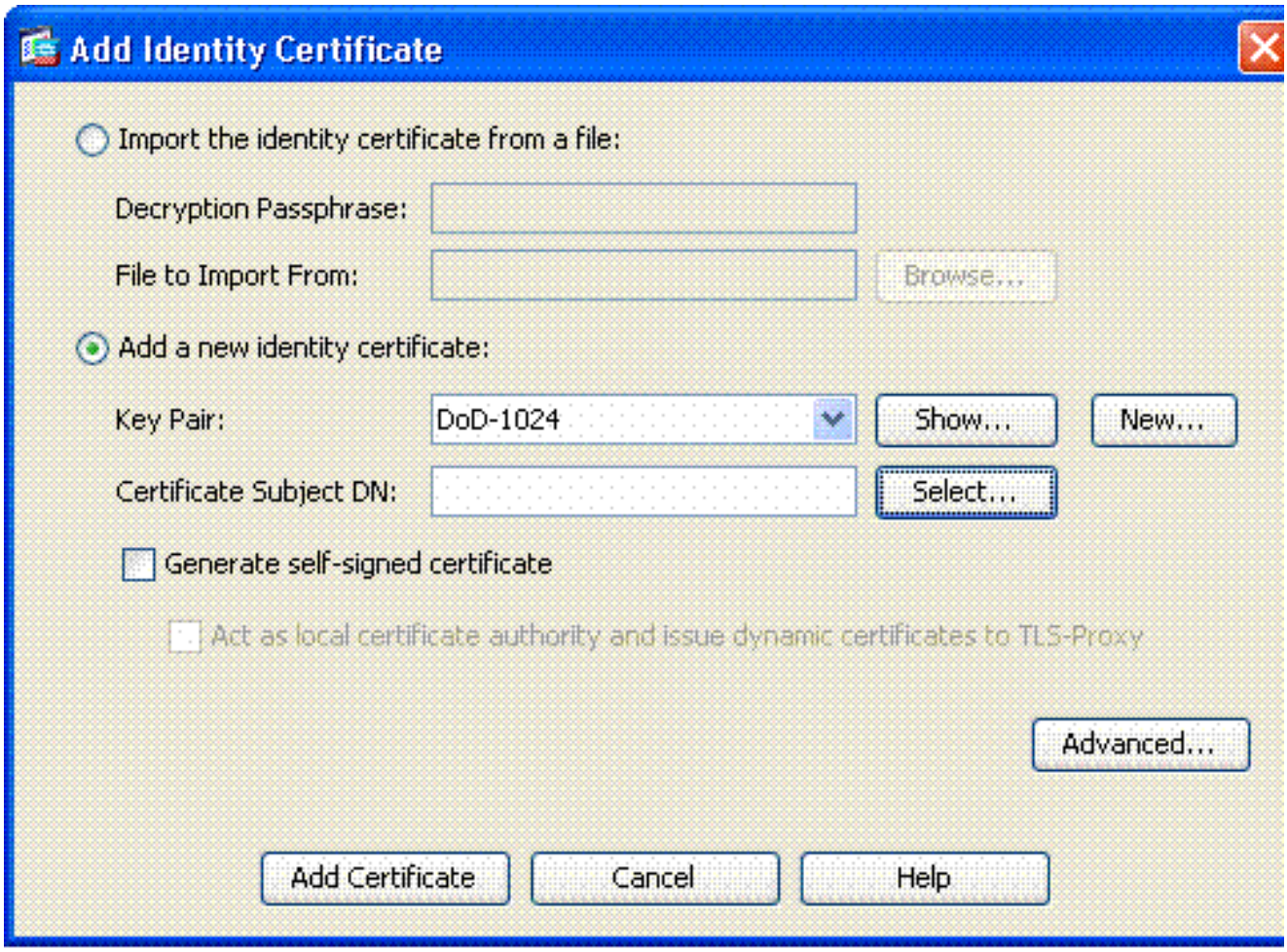
Figura 6: Instalación del certificado raíz



Inscripción de ASA e instalación del certificado de identidad

1. Elija Remote Access VPN > Certificate Management > Identity Certificate > Add.
2. Elija Add a new id certificate.
3. Elija el par de claves DoD-1024. Vea la figura 7

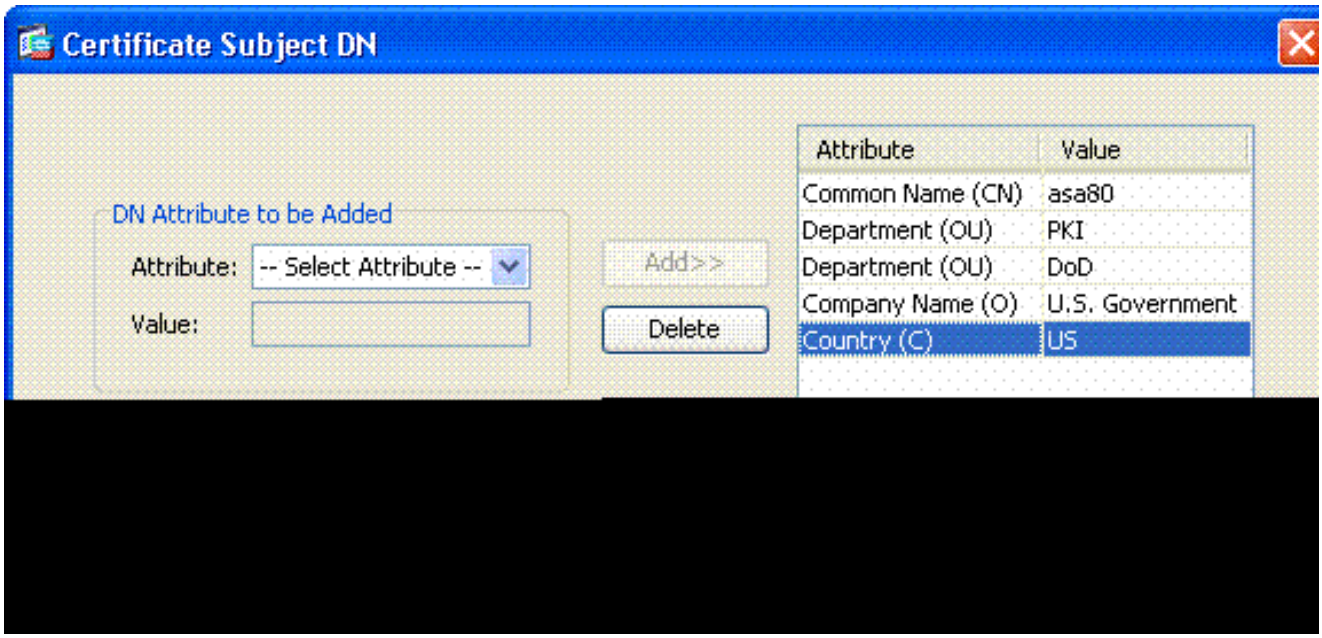
Figura 7: Parámetros del certificado de identidad



4. Vaya al cuadro DN del asunto del certificado y haga clic en Select.

5. En la ventana Certificate Subject DN, ingrese la información del dispositivo. Consulte la Figura 8 para ver un ejemplo.

Figura 8: Editar DN



6. Elija Aceptar.

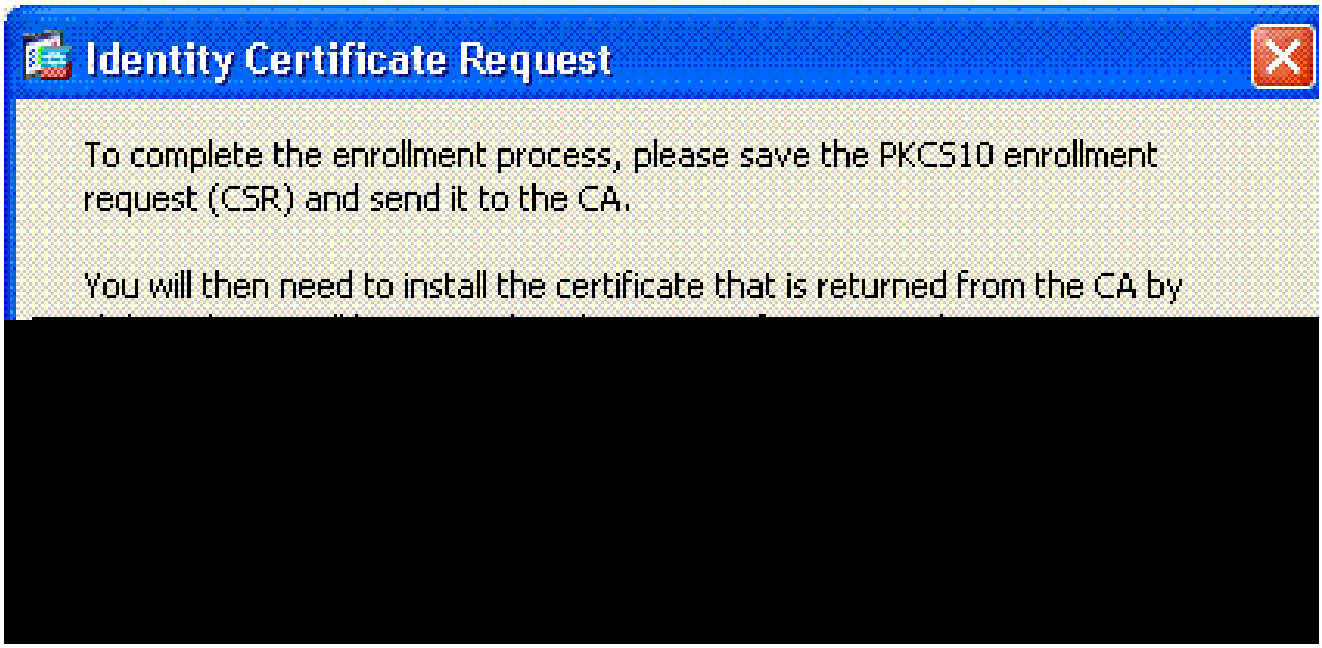
Nota: Asegúrese de utilizar el nombre de host del dispositivo configurado en el sistema cuando agregue el DN de asunto. El PKI POC puede indicarle los campos obligatorios necesarios.

---

7. Elija Agregar certificado.

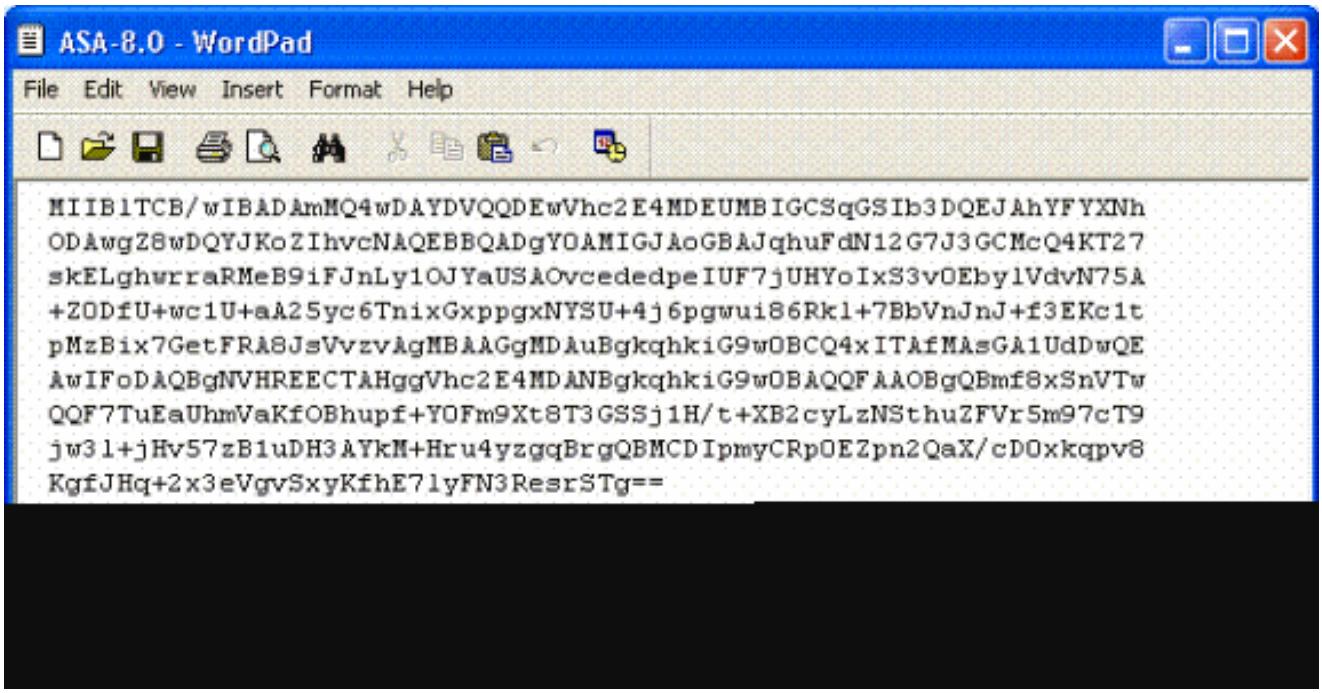
8. Haga clic en Browse para seleccionar el directorio donde desea guardar la solicitud. Consulte la Figura 9.

Figura 9: Solicitud de certificado



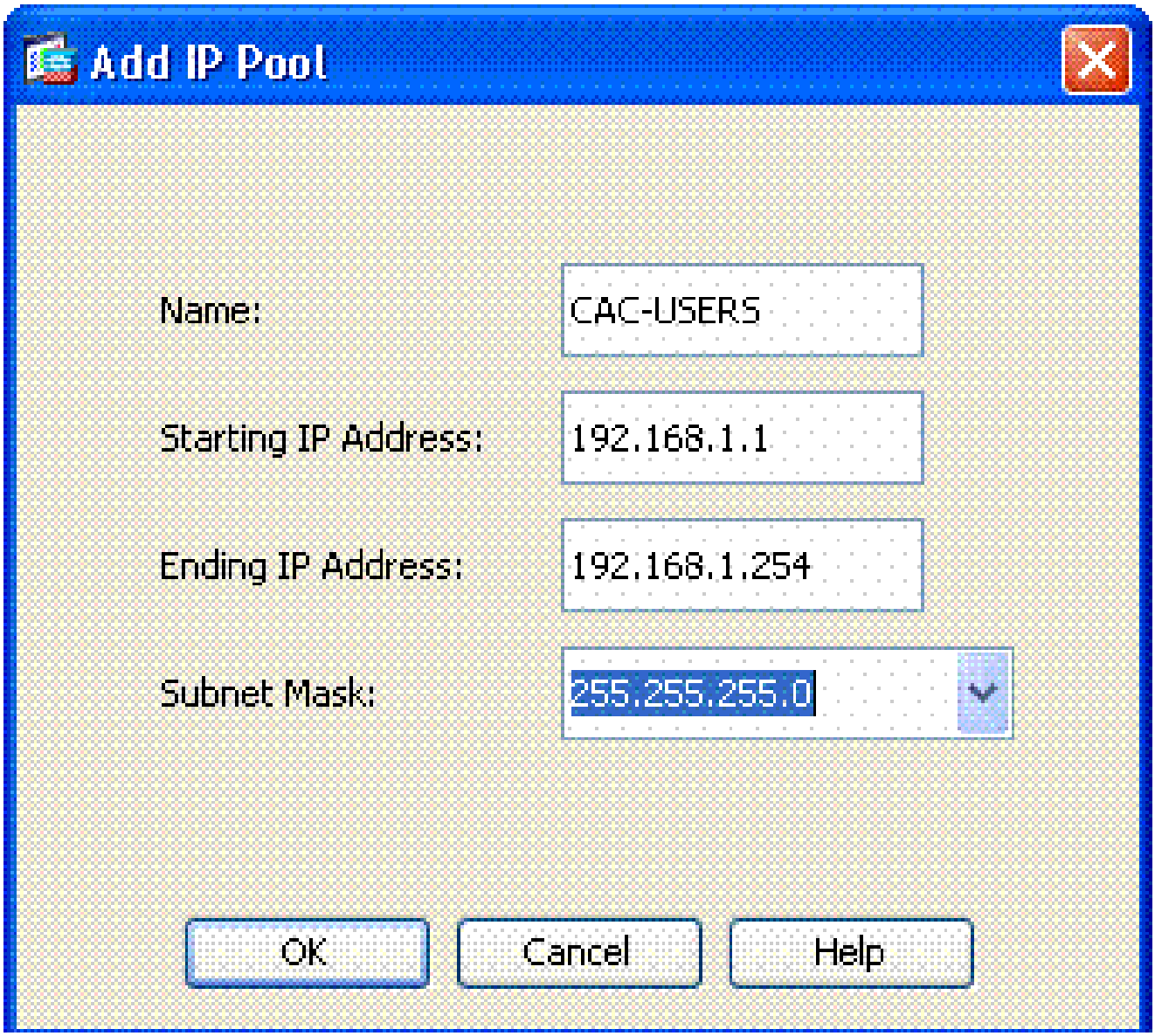
9. Abra el archivo con WordPad, copie la solicitud en la documentación apropiada y envíela a su POC PKI. Consulte la Figura 10.

Figura 10: Solicitud de inscripción



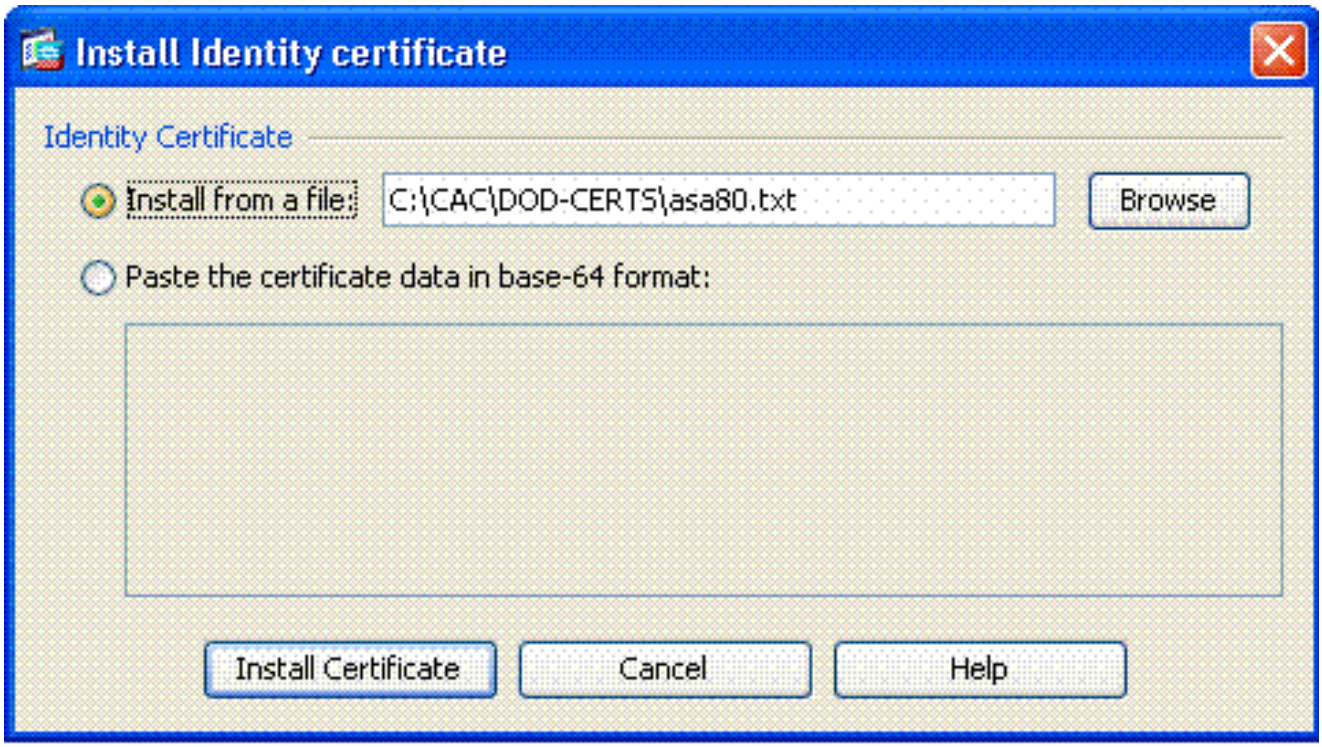
10. Una vez que haya recibido el certificado del administrador de la CA, elija Remote Access VPN > Certificate Management > ID Certificate > Install. Consulte la Figura 11.

    Figura 11: Importación del certificado de identidad



11. En la ventana Instalar certificado, busque el certificado de ID y elija Instalar certificado. Consulte la Figura 12 para ver un ejemplo.

    Figura 12: Instalación del certificado de identidad



Nota: se recomienda exportar el punto de confianza del certificado de ID para guardar el certificado emitido y los pares de claves. Esto permite al administrador de ASA importar el certificado y los pares de claves a un nuevo ASA en caso de falla de RMA o hardware. Consulte Exportación e importación de puntos de confianza para obtener más información.

Nota: Haga clic en SAVE para guardar la configuración en la memoria flash.

Configuración de VPN de AnyConnect

Hay dos opciones para configurar los parámetros VPN en ASDM. La primera opción es utilizar el asistente para SSL VPN. Esta es una herramienta fácil de usar para los usuarios que son nuevos en la configuración VPN. La segunda opción es hacerlo manualmente y pasar a través de cada opción. Esta guía de configuración utiliza el método manual.

Nota: Hay dos métodos para obtener el cliente AC para el usuario:

1. Puede descargar el cliente desde el sitio web de Cisco e instalarlo en su equipo.
2. El usuario puede acceder al ASA a través de un navegador web y el cliente se puede descargar.

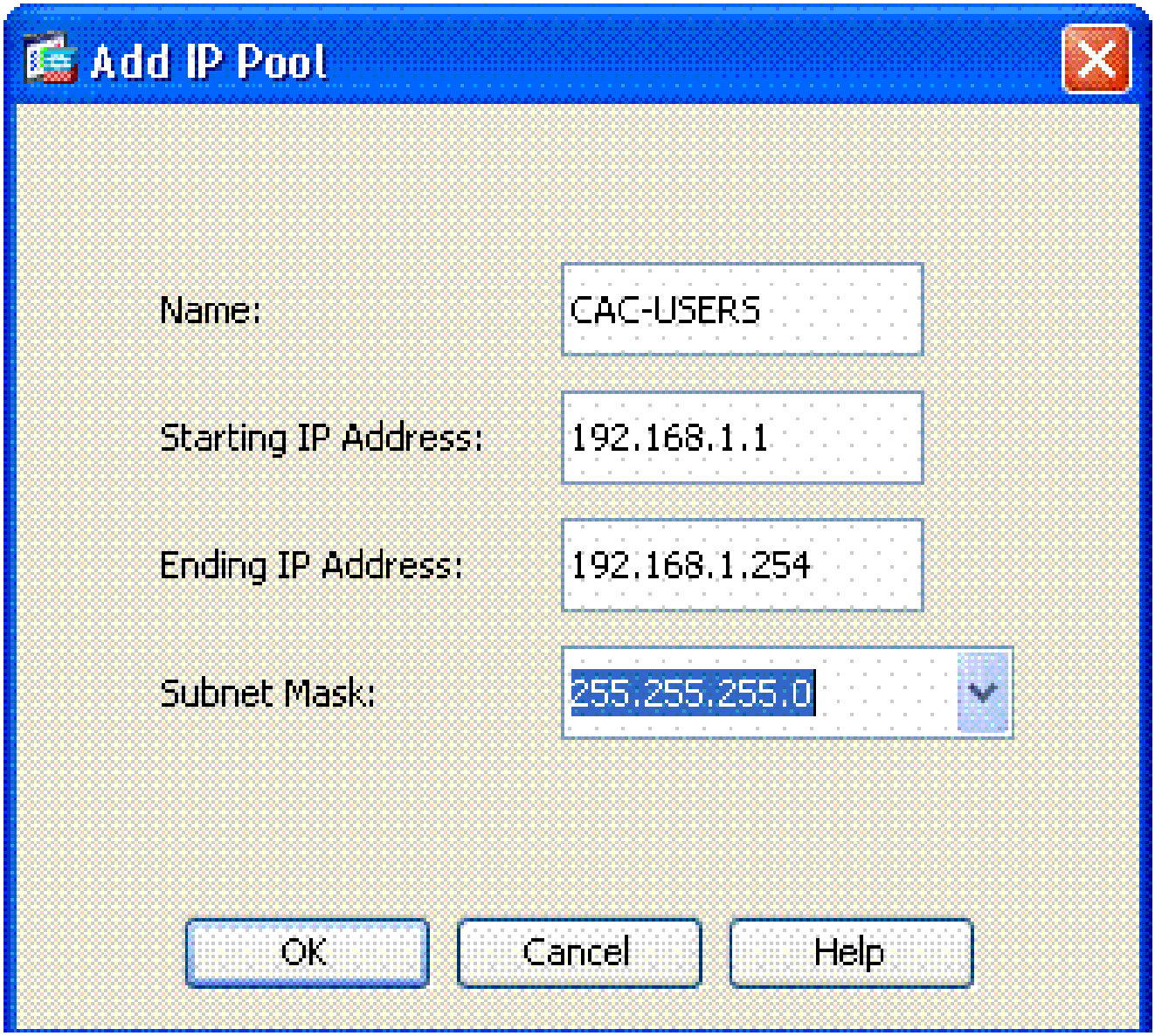
Nota: Por ejemplo, https://asa.test.com. Esta guía utiliza el segundo método. Una vez que el cliente AC está instalado en el equipo cliente permanentemente, simplemente inicie el cliente AC desde la aplicación.

Crear un conjunto de direcciones IP

Esto es opcional si utiliza otro método como DHCP.

1. Elija Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.
2. Haga clic en Add (Agregar).
3. En la ventana Add IP Pool, ingrese el nombre del pool IP, la dirección IP inicial y final y elija una máscara de subred. Ver Figura 13.

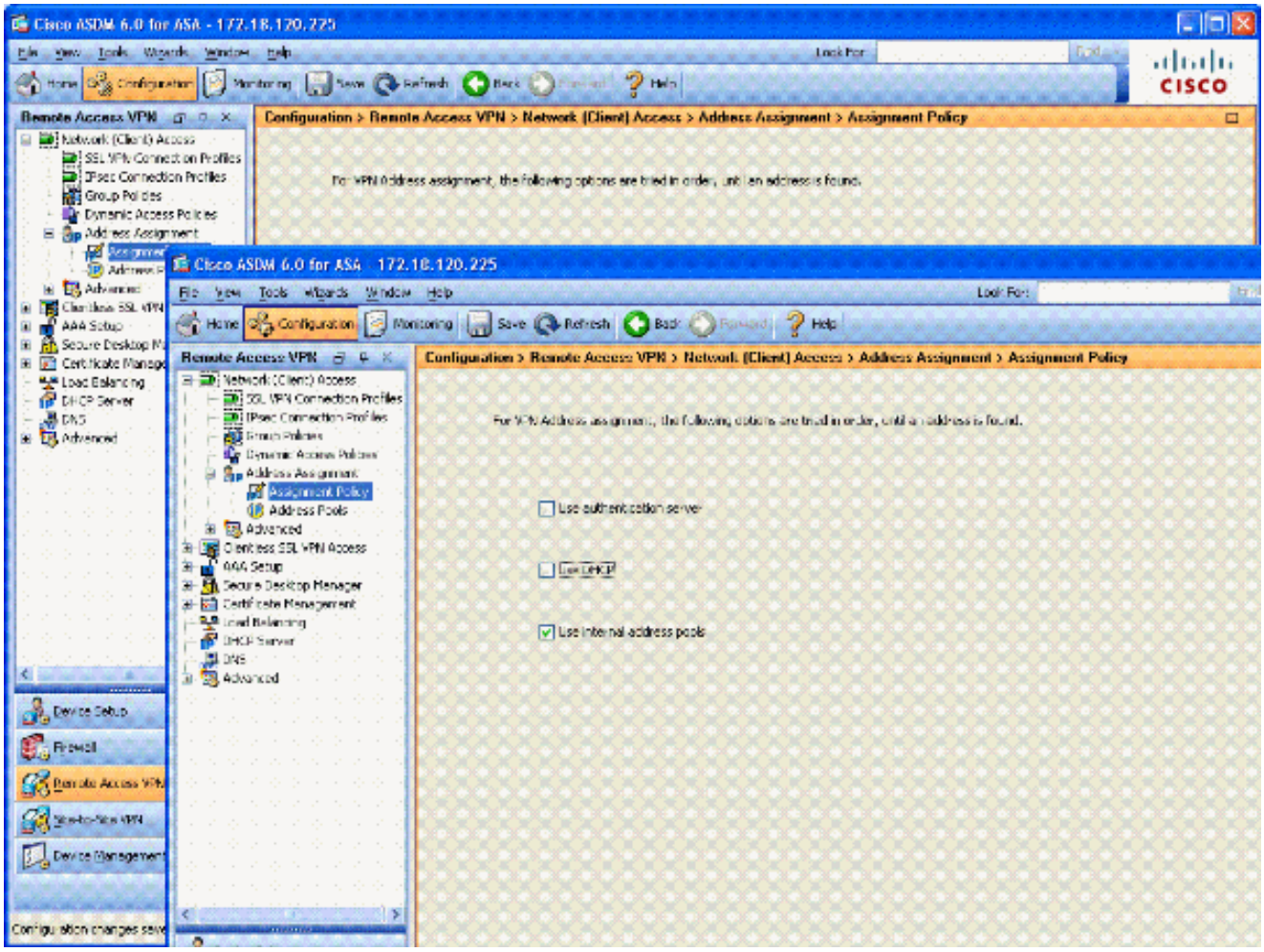
   Figura 13: Adición de un grupo de IP



4. Elija Aceptar.
5. Elija Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy.

6. Seleccione el método de asignación de dirección IP adecuado. Esta guía utiliza los conjuntos de direcciones internas. Consulte la Figura 14.

   Figura 14: Método de asignación de direcciones IP



7. Haga clic en Apply (Aplicar).

Crear Grupo de Túnel y Política de Grupo

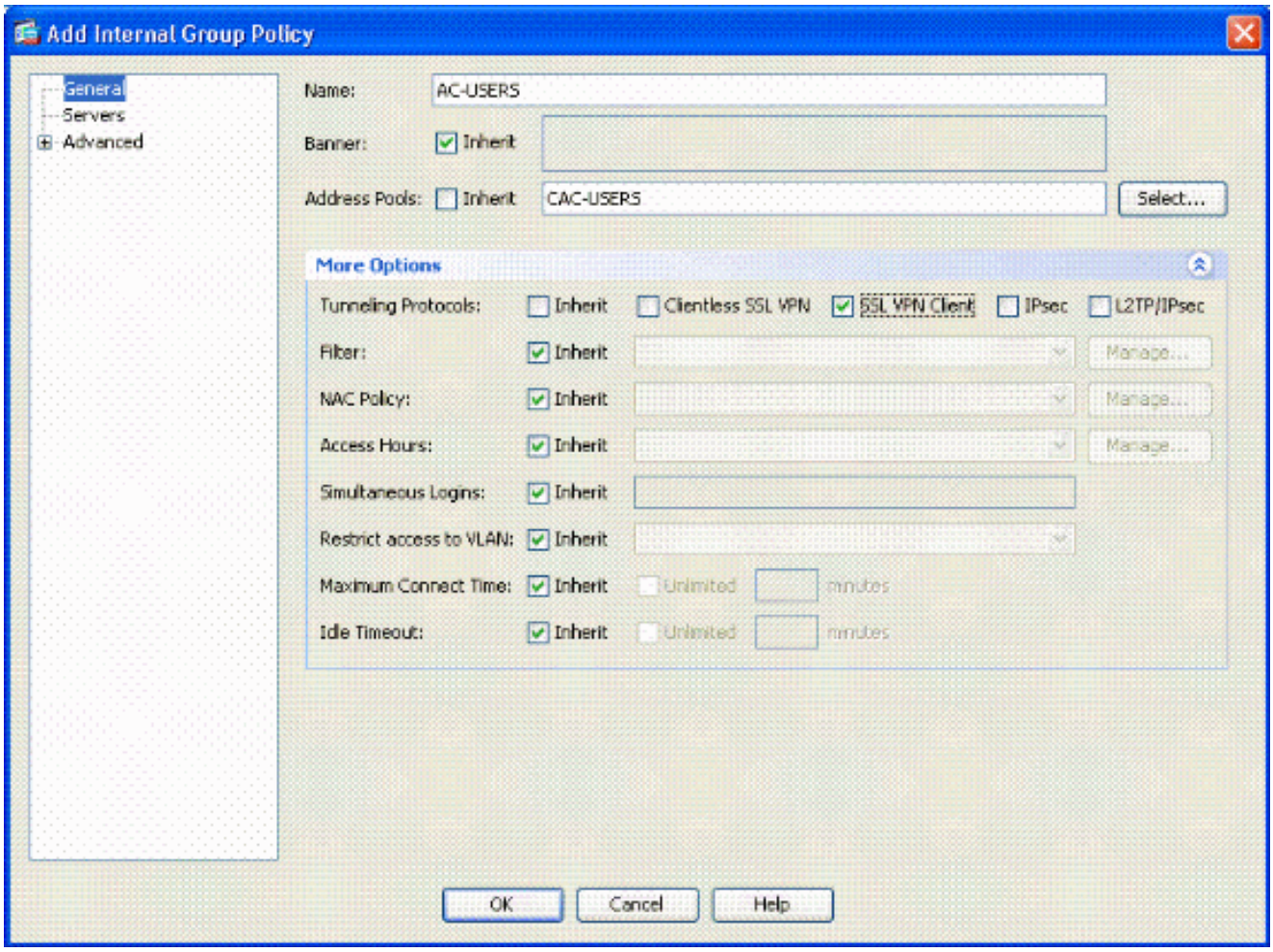
Directiva de grupo

Nota: Si no desea crear una nueva política, puede utilizar la política integrada en grupo por defecto.

---

1. Elija Remote Access VPN -> Network (Client) Access -> Group Policies.
2. Haga clic en Agregar y elija Directiva de grupo interna.
3. En la ventana Agregar directiva de grupo interna, escriba el nombre de la directiva de grupo en el cuadro de texto Nombre. Consulte la Figura 15.

   Figura 15: Adición de una política de grupo interna



a. En la pestaña General, elija la opción SSL VPN Client en Tunneling Protocols, a menos que utilice otros protocolos como Clientless SSL.

b. En la sección Servidores, desmarque la casilla de verificación inherit e ingrese la dirección IP de los servidores DNS y WINS. Introduzca el alcance de DHCP si procede.

c. En la sección Servidores, anule la selección de la casilla de verificación inherit en el Dominio predeterminado e ingrese el nombre de dominio apropiado.

d. En la ficha General, anule la selección de la casilla de verificación inherit en la sección de agrupación de direcciones y agregue la agrupación de direcciones creada en el paso anterior. Si utiliza otro método de asignación de dirección IP, deje que se herede y realice el cambio correspondiente.

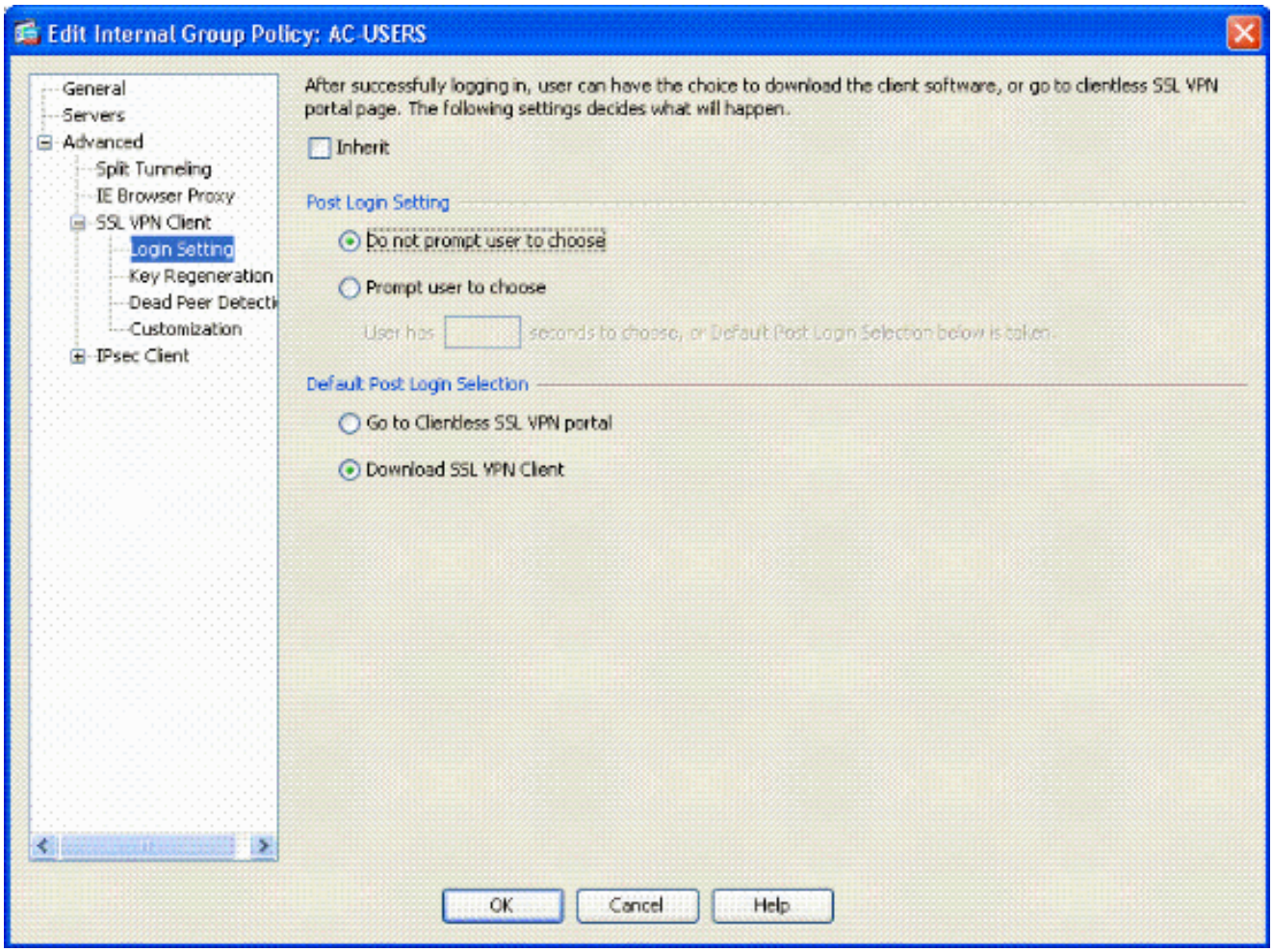
e. El resto de las fichas de configuración se dejan en los parámetros predeterminados.

> Nota: Hay dos métodos para obtener el cliente de CA a los usuarios finales. Uno de los métodos es ir a Cisco.com y descargar el cliente AC. El segundo método es hacer que ASA descargue el cliente al usuario cuando este intenta conectarse. En este ejemplo se muestra el último método.

---

4. A continuación, elija Advanced > SSL VPN Client > Login Settings. Consulte la Figura 16.

Figura 16: Adición de una política de grupo interna



a. Anule la selección de la casilla de verificación Heredar.

b. Elija la configuración posterior al inicio de sesión que mejor se adapte a su entorno.

c. Elija la selección predeterminada de inicio de sesión posterior que mejor se adapte a su entorno.

d. Elija Aceptar.

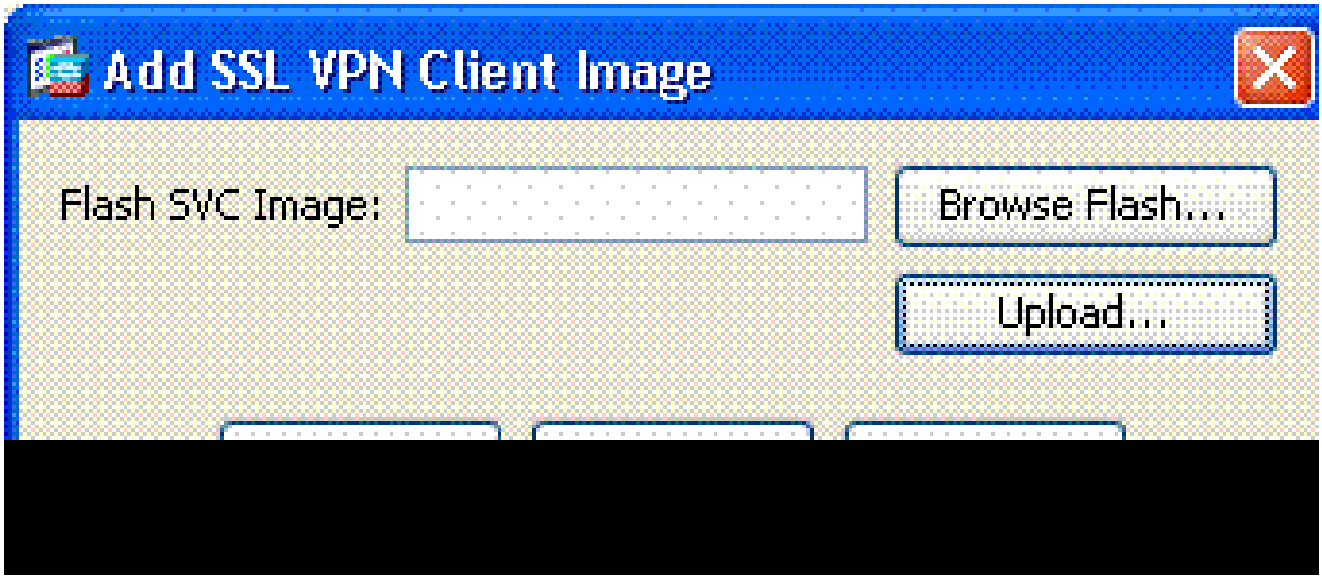
Interfaz de Grupo de Túnel y Configuración de Imagen

Nota: Si no desea crear un nuevo grupo, puede utilizar el grupo integrado por defecto.

1. Elija Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile.
2. Elija Enable Cisco AnyConnect Client.....
3. Aparece un cuadro de diálogo con la pregunta `¿Desea designar una imagen SVC?`
4. Elija Yes.

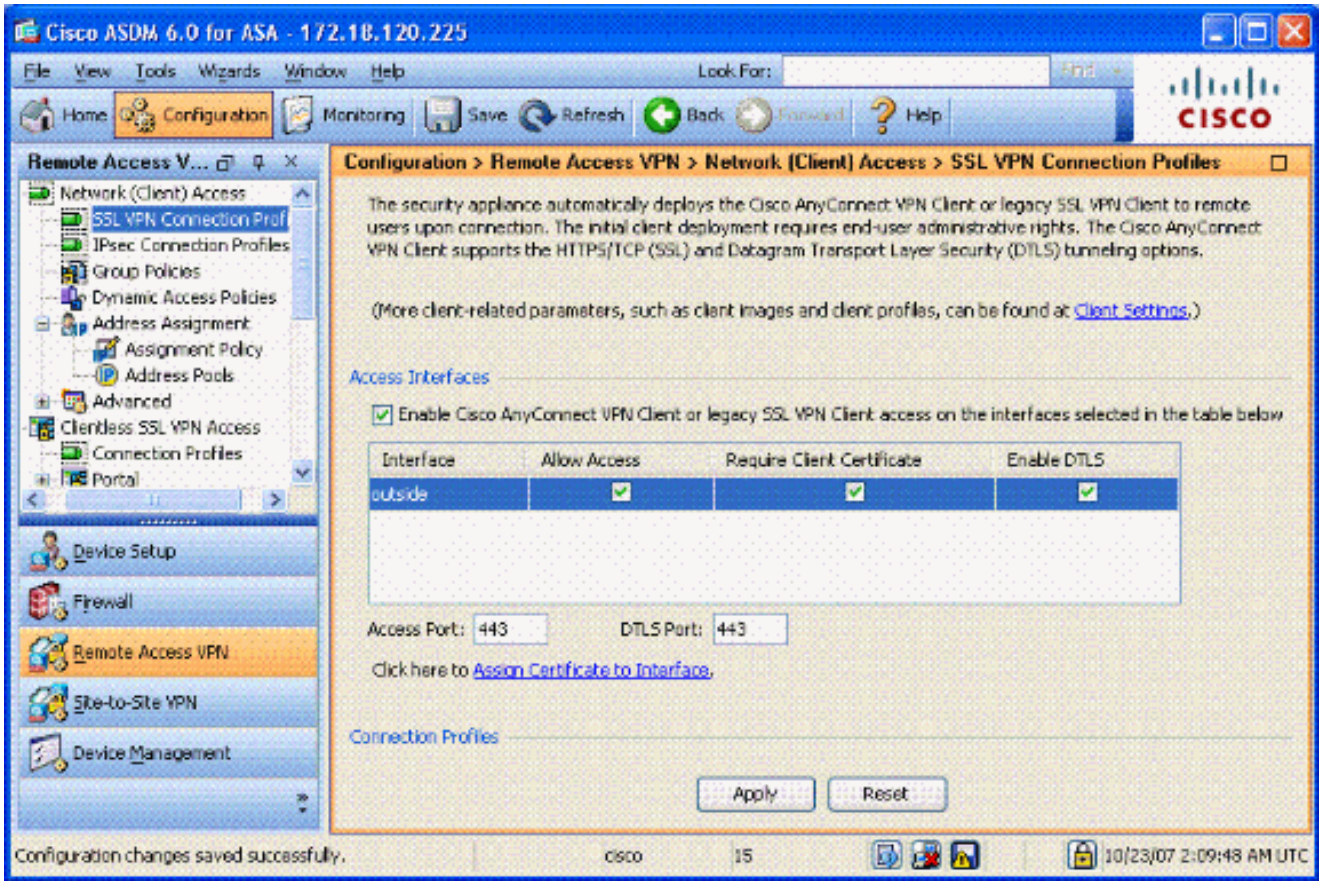
5. Si ya hay una imagen, elija la imagen que desea utilizar con Browse Flash. Si la imagen no está disponible, elija Cargar y busque el archivo en el equipo local. Consulte la Figura 17. Los archivos se pueden descargar desde Cisco.com; hay un archivo de Windows, MAC y Linux.

   Figura 17: Add SSL VPN Client Image



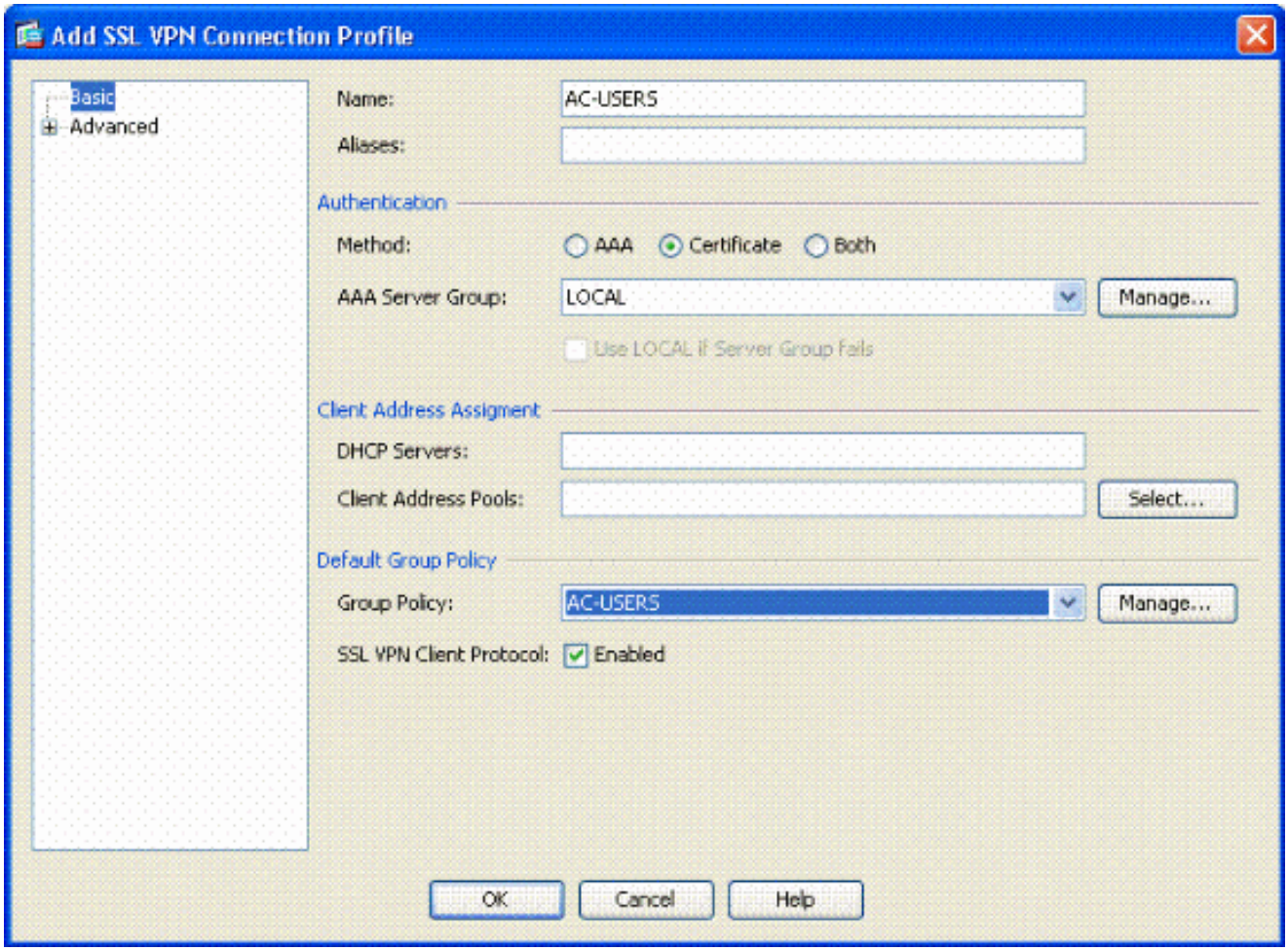
6. A continuación, habilite Allow Access, Require Client Cert y opcionalmente Enable DTLS. Consulte la Figura 18.

   Figura 18: Habilitación del acceso



7. Haga clic en Apply (Aplicar).
8. A continuación, cree un perfil de conexión/grupo de túnel. Elija Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile.
9. En la sección Perfiles de conexión, haga clic en Agregar.

   Figura 19: Adición de un perfil de conexión



   a. Nombre el grupo.

   b. Elija Certificate en el método de autenticación.

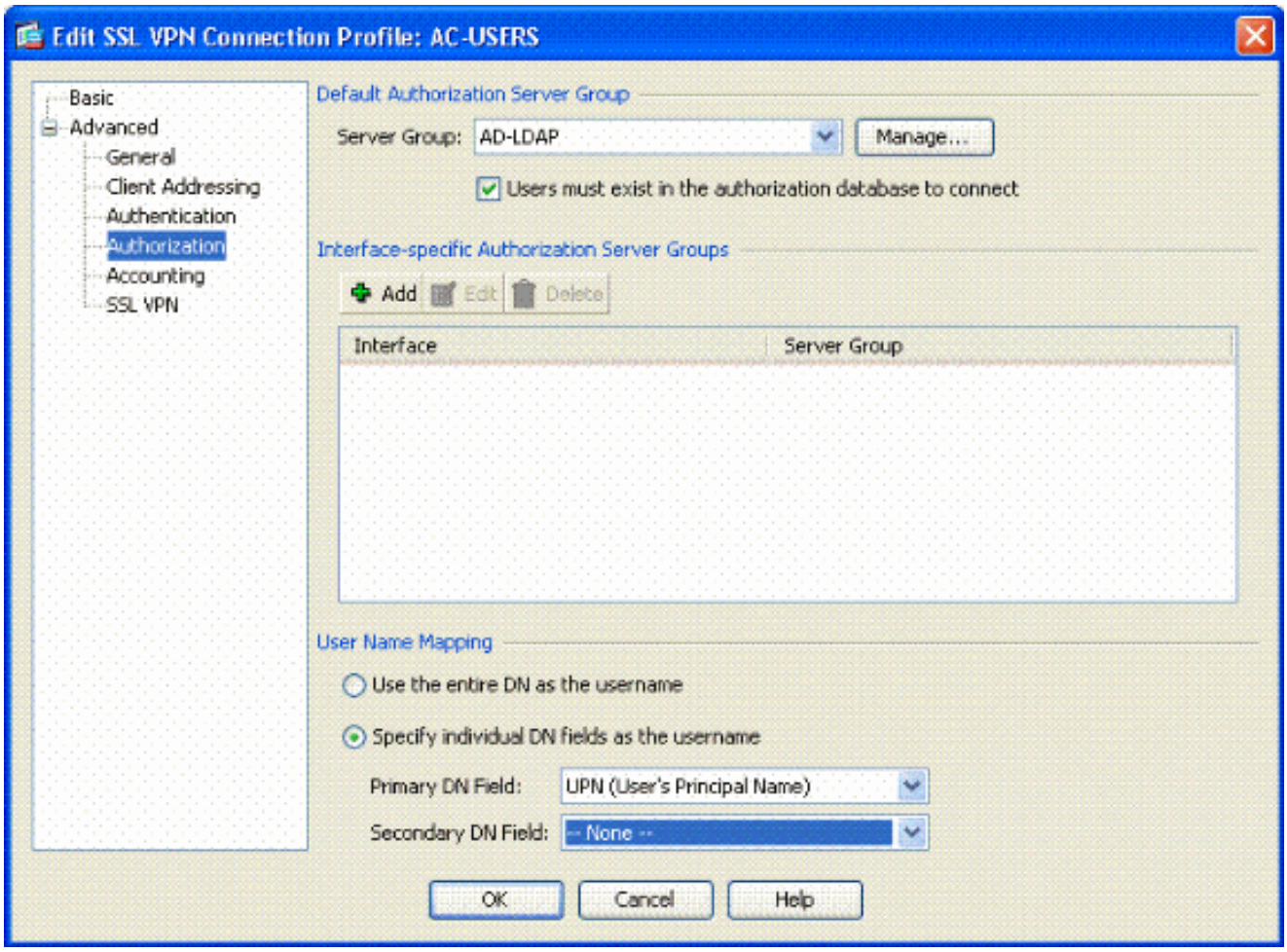
   c. Elija la política de grupo creada anteriormente.

   d. Asegúrese de que SSL VPN Client esté habilitado.

   e. Deje otras opciones como predeterminadas.

10. A continuación, elijaAvanzadas > Autorización. Vea la figura 20

    Figura 20: Autorización



a. Elija el grupo AD-LDAP creado anteriormente.

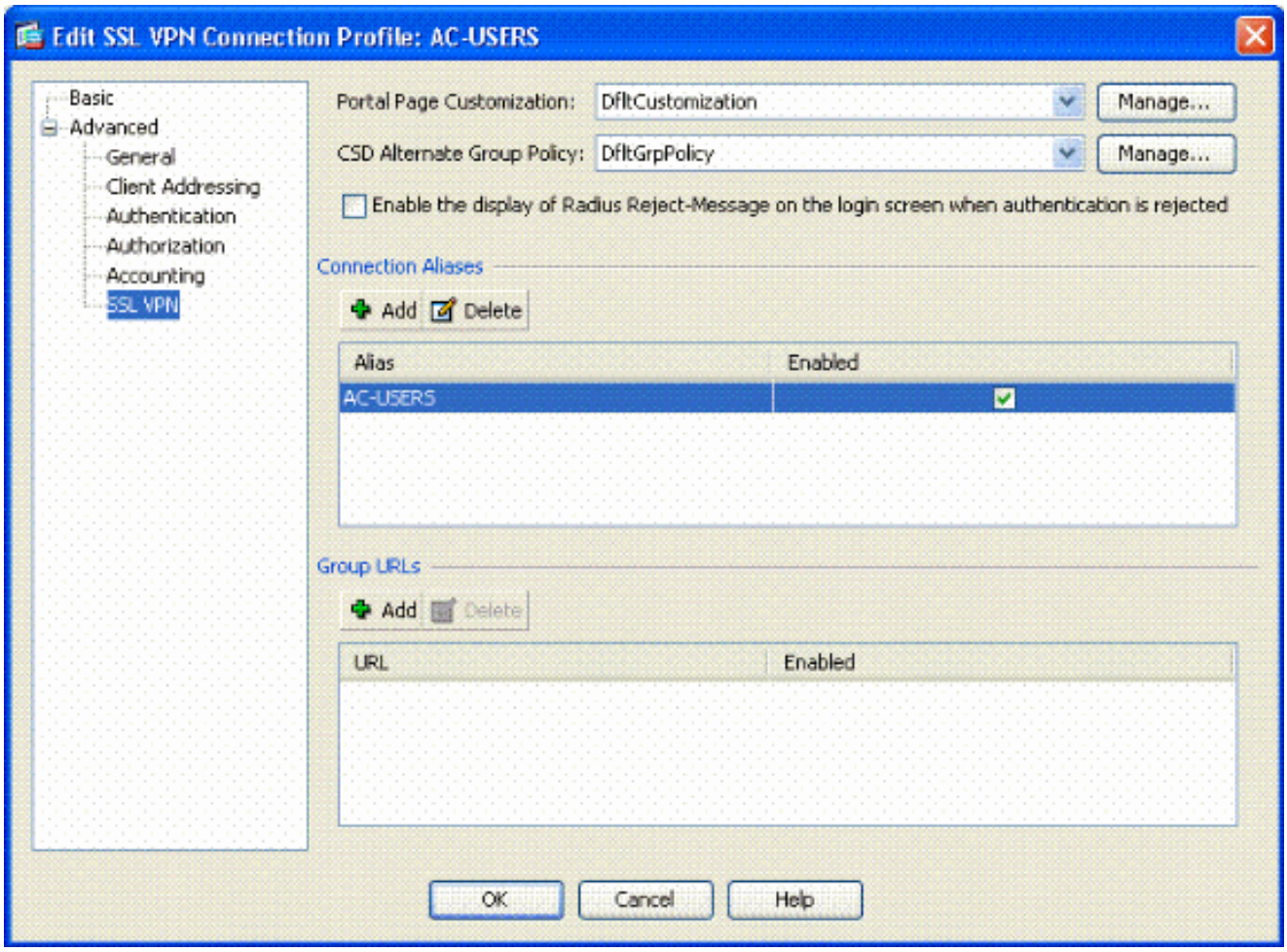
b. Comprobar que los usuarios deben existir... para conectarse.

c. En los campos de asignación, elija UPN para el principal y none para el secundario.

11. Elija la sección SSL VPN del menú.

12. En la sección Alias de Conexión, siga estos pasos:

Figura 21: Alias de conexión



a. Elija Agregar.

b. Introduzca el alias de grupo que desea utilizar.

c. Asegúrese de que Enabled esté marcado. Consulte la Figura 21.

13. Click OK.

Nota: Haga clic en Save para guardar la configuración en la memoria flash.

Reglas de coincidencia de certificados (si se utilizará OCSP)

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

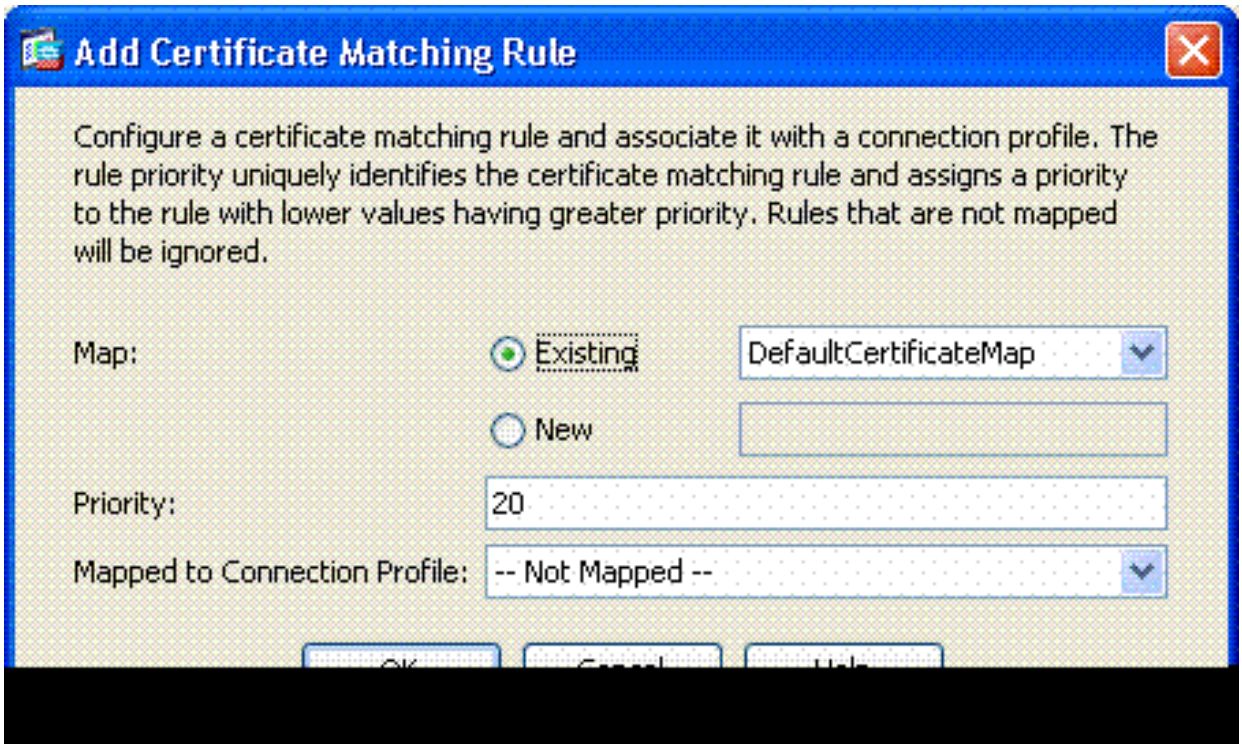
   a. Elija Add en la sección Certificate to Connection Profile Maps.

   b. Puede mantener el mapa existente como DefaultCertificateMap en la sección de mapa o crear uno nuevo si ya utiliza mapas de certificado para IPSec.

   c. Mantenga la prioridad de la regla.

   d. En el grupo asignado, deje como — No asignado —. Consulte la Figura 22.

Figura 22: Adición de la regla de coincidencia de certificados

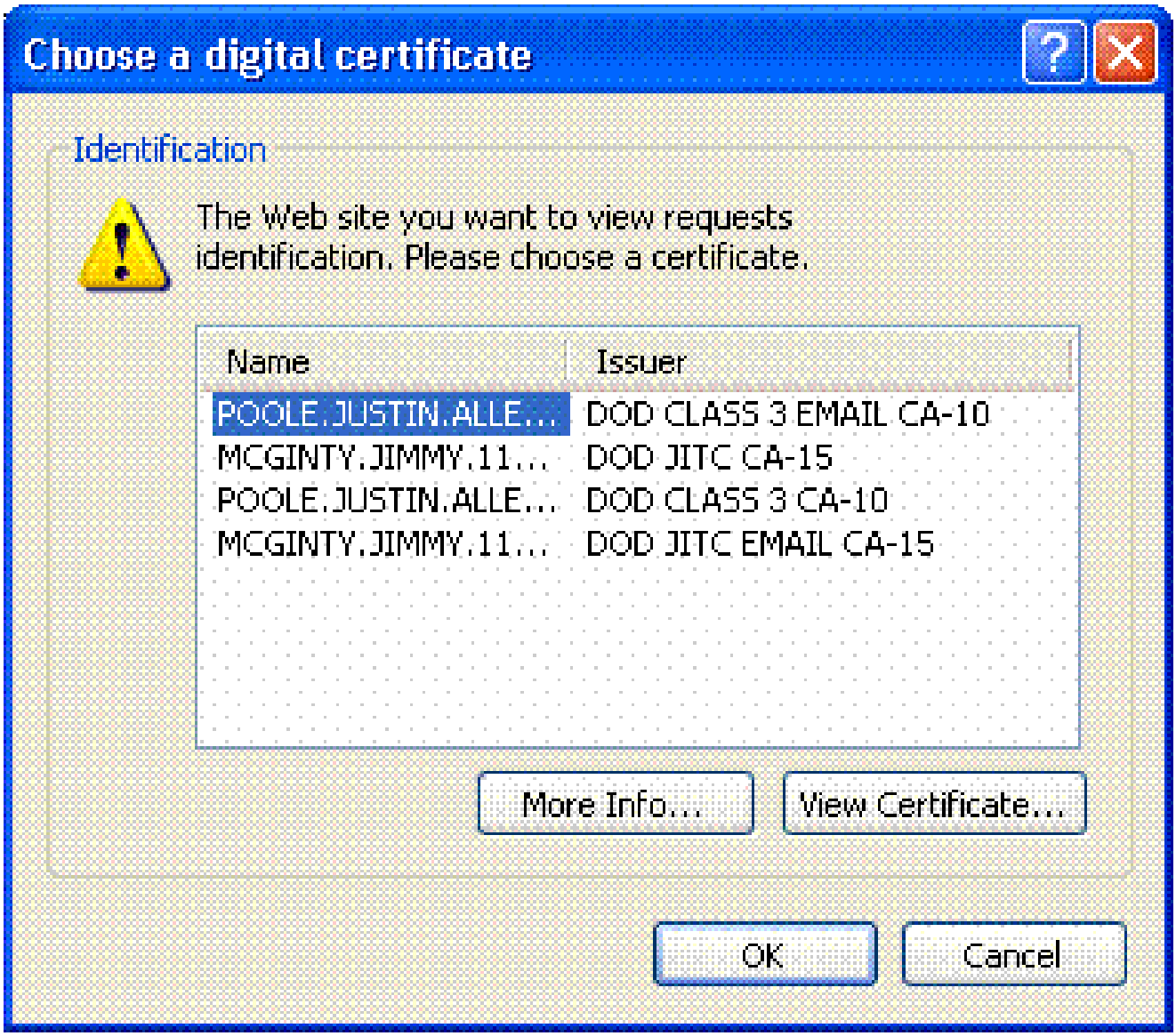


e. Click OK.

2. Haga clic en Agregar en la tabla inferior.

3. En la ventana Agregar criterio de regla coincidente de certificado, siga estos pasos:

Figura 23: Criterio de regla de coincidencia de certificados



a. Mantenga la columna Campo en Asunto.

b. Mantenga la columna Componente en Todo el campo.

c. Cambie la columna Operador a No es igual.

d. En la columna Valor, introduzca dos comillas dobles "".

e. Haga clic en Aceptar y Aplicar. Consulte la Figura 23 para ver un ejemplo.

Configurar OCSP

La configuración de un OCSP puede variar y depende del proveedor del respondedor de OCSP. Lea el manual del vendedor para más información.

Configurar certificado de Respondedor de OCSP

1. Obtenga un certificado autogenerado del respondedor de OCSP.

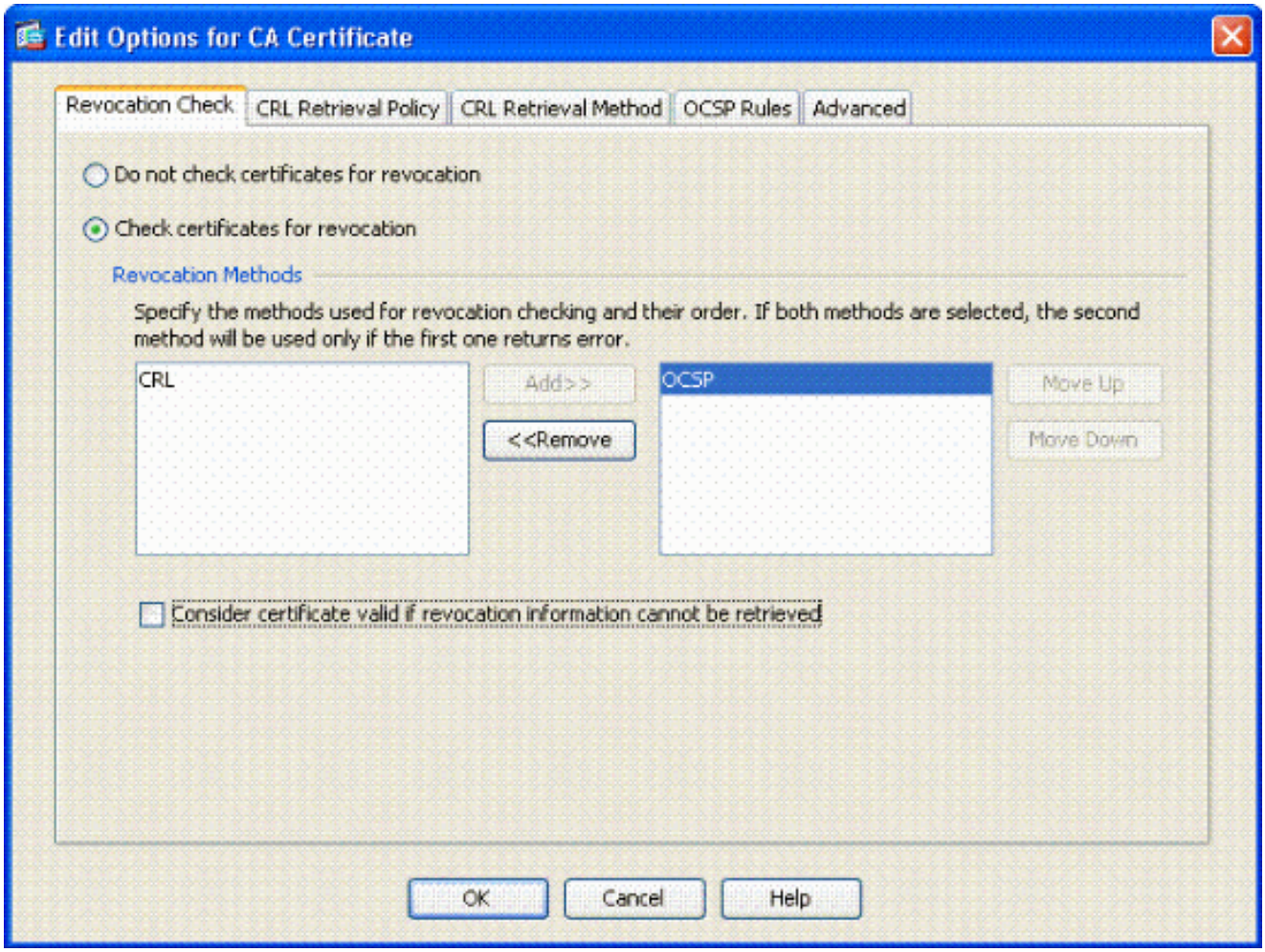
2. Complete los procedimientos mencionados anteriormente e instale un certificado para el servidor OSCP.

Nota: asegúrese de que la opción No comprobar la revocación de certificados está seleccionada para el punto de confianza de certificados de OCSP.

Configurar CA para usar OCSP

1. Elija Remote Access VPN> Certificate Management > CA Certificates.
2. Resalte un OCSP para elegir una CA que configurar para utilizar OCSP.
3. Haga clic en Editar.
4. Asegúrese de que la opción Comprobar certificado para revocación esté activada.
5. En la sección Métodos de revocación, agregue OCSP. Consulte la Figura 24.

   Comprobación de revocación de OCSP



6. Asegúrese de que la opción Considerar certificado válido...no se puede recuperar está desactivada si desea seguir una comprobación estricta de OCSP.

Nota: Configure/edite todo el servidor de la CA que utiliza OCSP para la revocación.

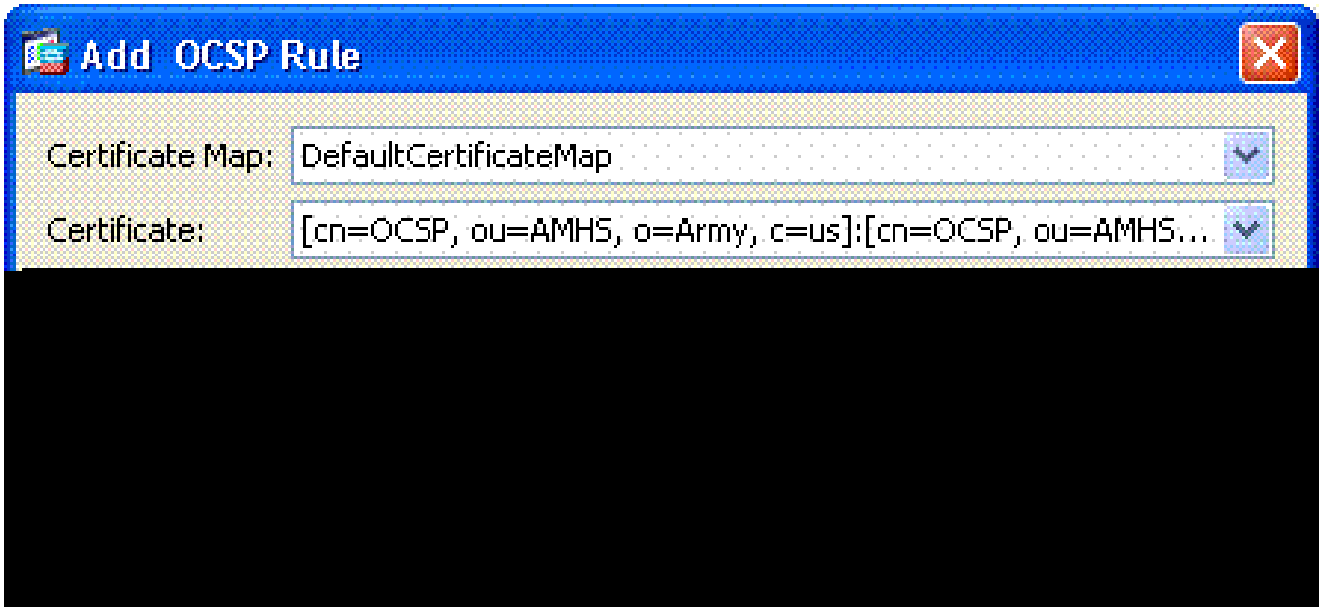
Configurar reglas OCSP

Nota: compruebe que se ha creado una directiva de coincidencia de grupos de certificados y que el respondedor de OCSP está configurado antes de completar estos pasos.

Nota: En algunas implementaciones de OCSP, se puede necesitar un registro A y PTR de DNS para el ASA. Esta comprobación se realiza para verificar que el ASA es de un sitio .mil.

1. Elija Remote Access VPN> Certificate Management > CA Certificates 2.
2. Resalte un OCSP para elegir una CA que configurar para utilizar OCSP.
3. Elija Edit.
4. Haga clic en la pestaña Regla OCSP.
5. Haga clic en Add (Agregar).
6. En la ventana Add OCSP Rule (Agregar regla OCSP), realice estos pasos. Consulte la Figura 25.

   Figura 25: Adición de reglas de OCSP



   a. En la opción Certificate Map, elija DefaultCertificateMap o un mapa creado previamente.
   b. En la opción Certificado, elija Respondedor OCSP.
   c. En la opción de índice, introduzca 10.

d. En la opción URL, introduzca la dirección IP o el nombre de host del respondedor de OCSP. Si utiliza el nombre de host, asegúrese de que el servidor DNS esté configurado en ASA.

e. Click OK.

f. Haga clic en Apply (Aplicar).

Configuración del cliente Cisco AnyConnect

Esta sección trata sobre la configuración del cliente Cisco AnyConnect VPN.

Suposiciones: la aplicación middleware y Cisco AnyConnect VPN Client ya está instalada en el equipo host. Se probaron ActivCard Gold y ActivClient.

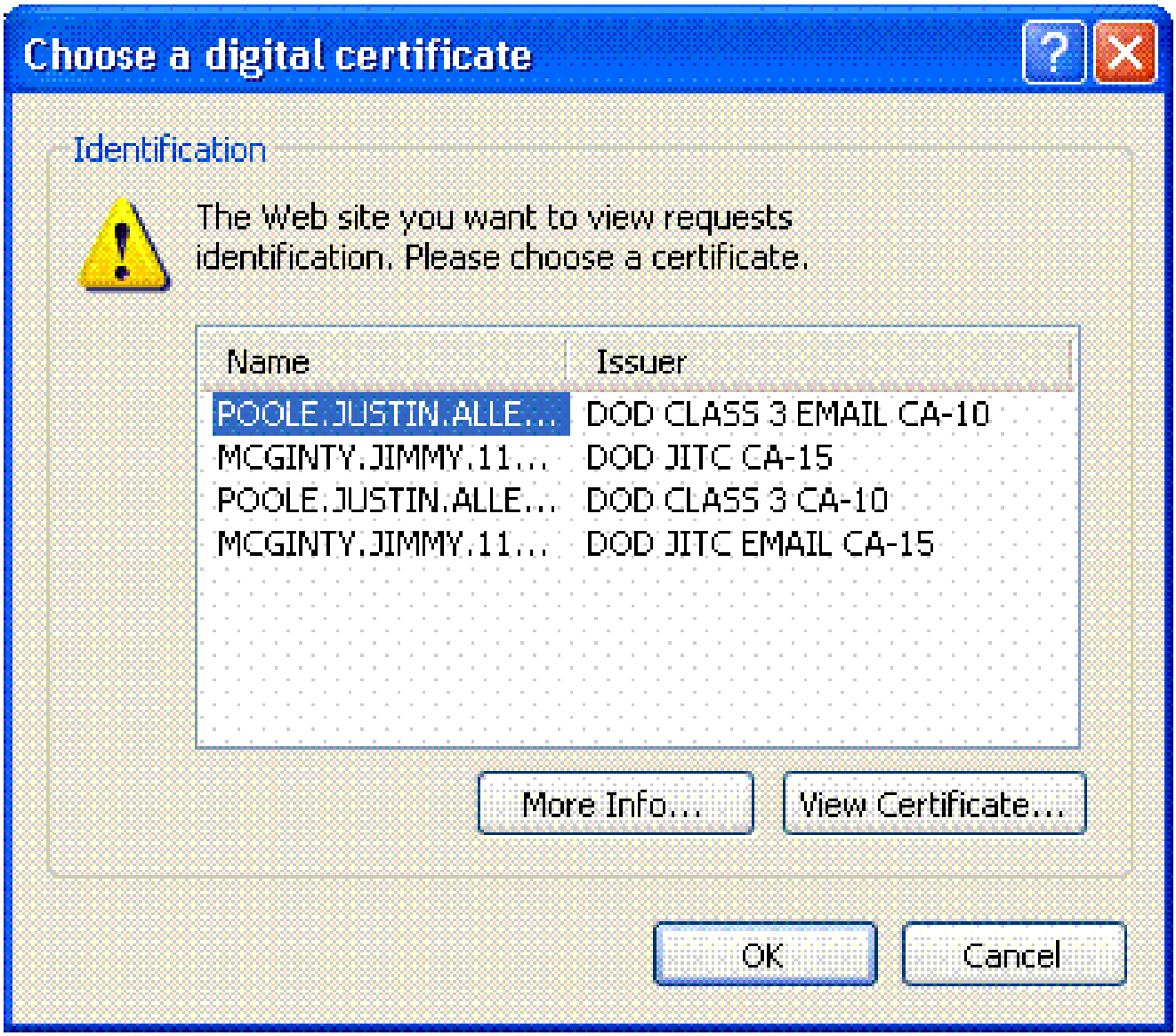
Nota: Esta guía utiliza el método group-url sólo para la instalación inicial del cliente AC. Una vez instalado el cliente AC, se inicia la aplicación AC igual que el cliente IPsec.

Nota: la cadena de certificados DoD debe instalarse en el equipo local. Verifique con el PKI POC para obtener el archivo de certificados/lote.

Descarga de Cisco Anyconnect VPN Client - Windows

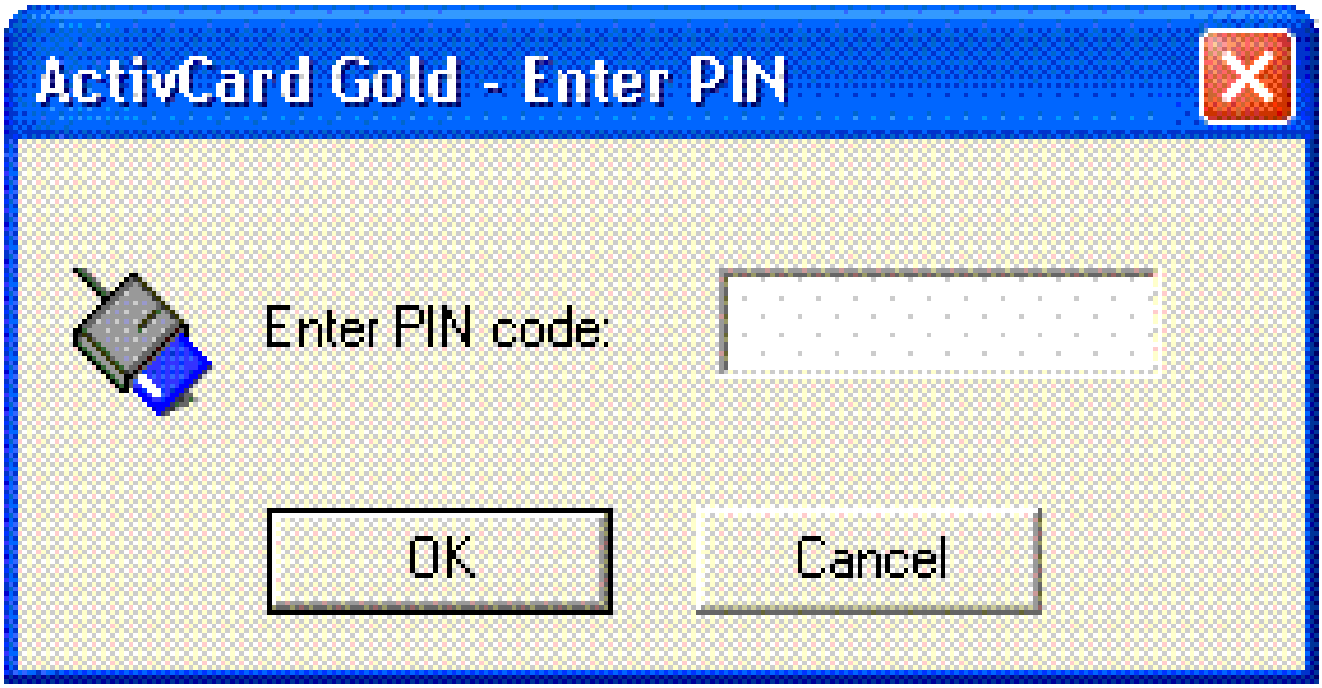
1. Inicie una sesión web en el ASA a través de Internet Explorer. La dirección debe tener el formato https://Outside-Interface. Por ejemplo, https://172.18.120.225.
2. Elija el certificado de firma que se utilizará para el acceso. Vea la Figura 26.

   Figura 26: Elija el certificado correcto



3. Introduzca el PIN cuando se le solicite.

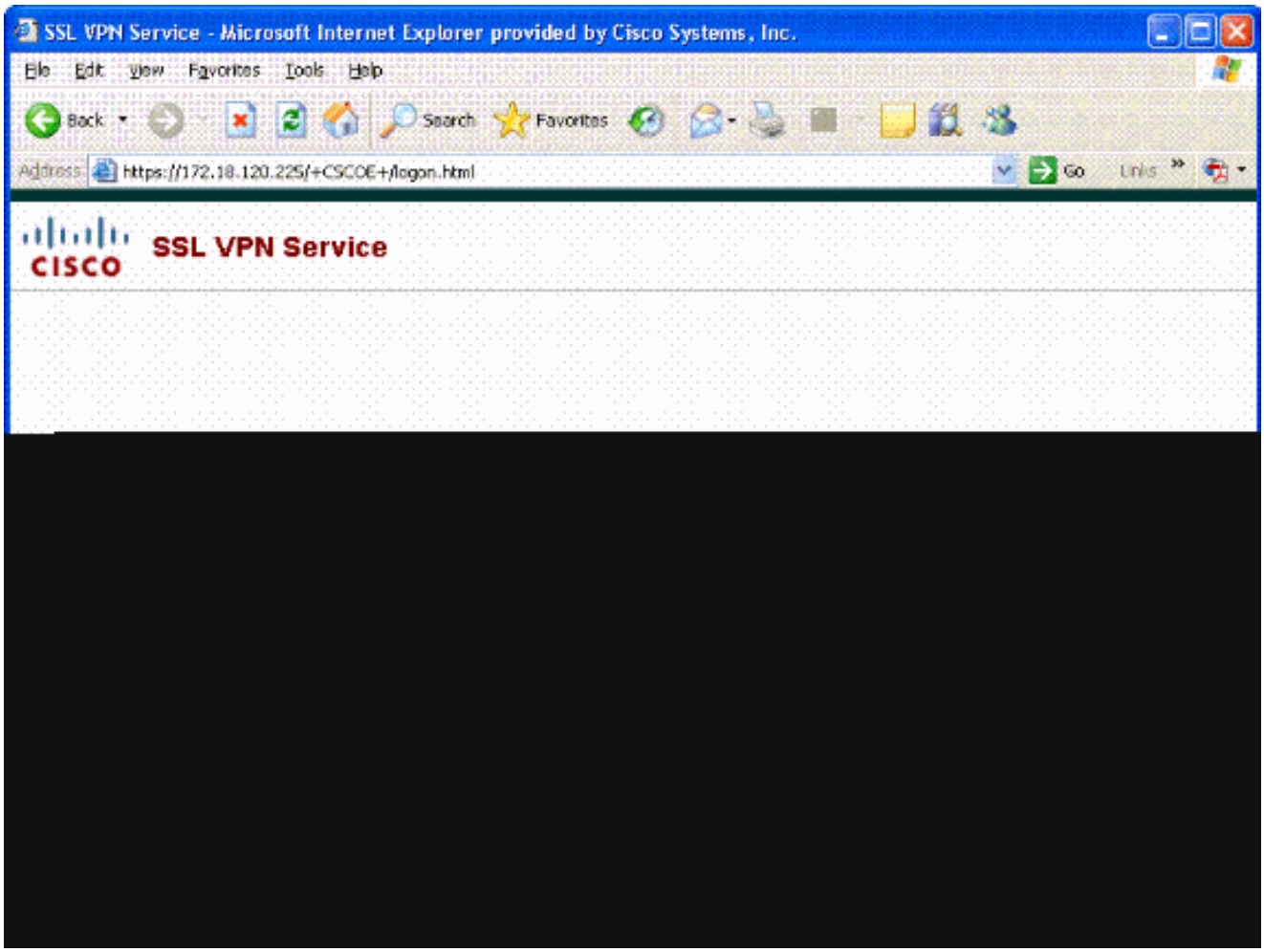
Figura 27: Introducir PIN



4. Elija Yes para aceptar la alerta de seguridad.

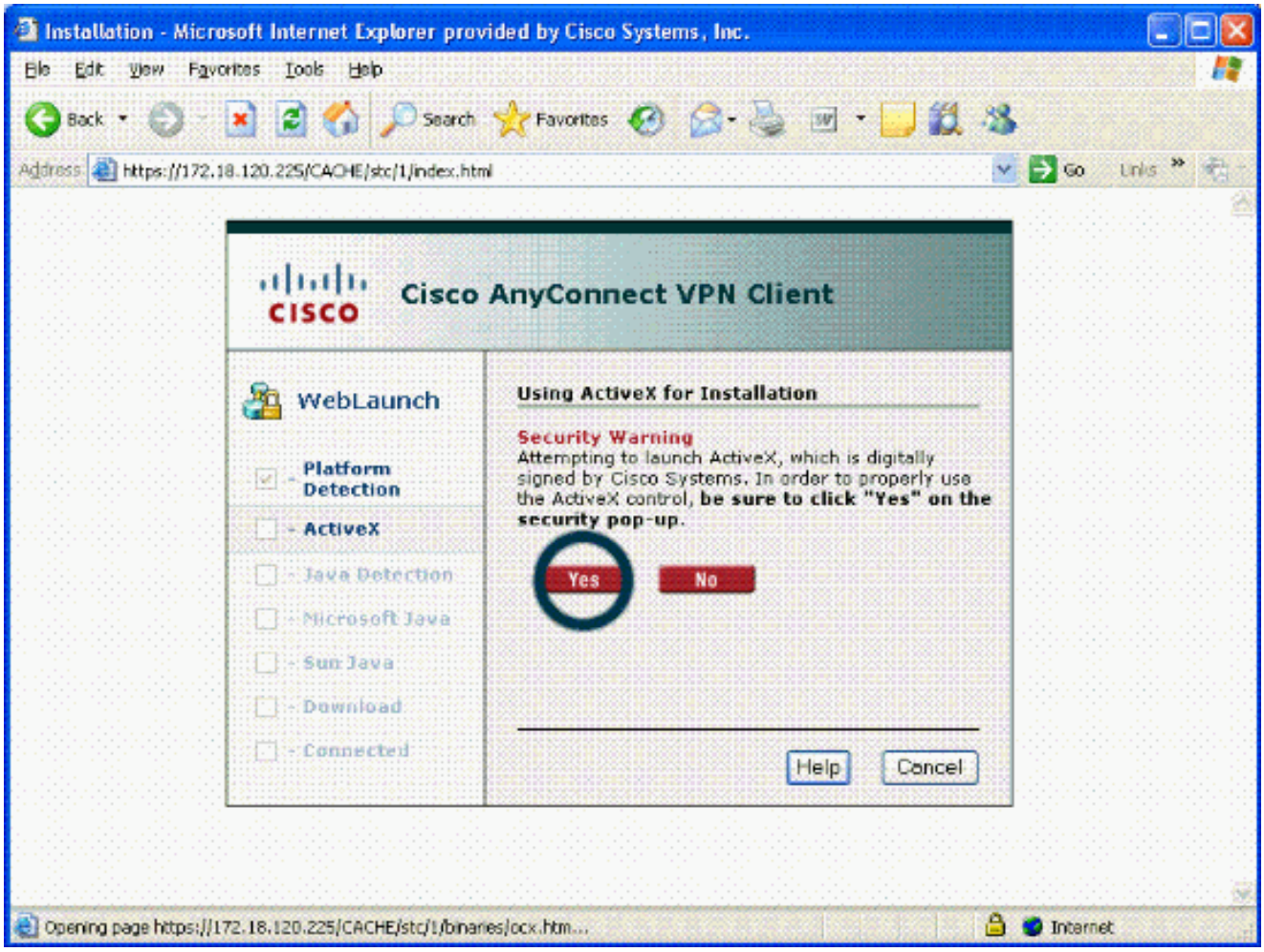
5. Una vez en la Página de Login de SSL, elija Login. El certificado de cliente se utiliza para iniciar sesión. Vea la Figura 28.

   Figura 28: Conexión SSL



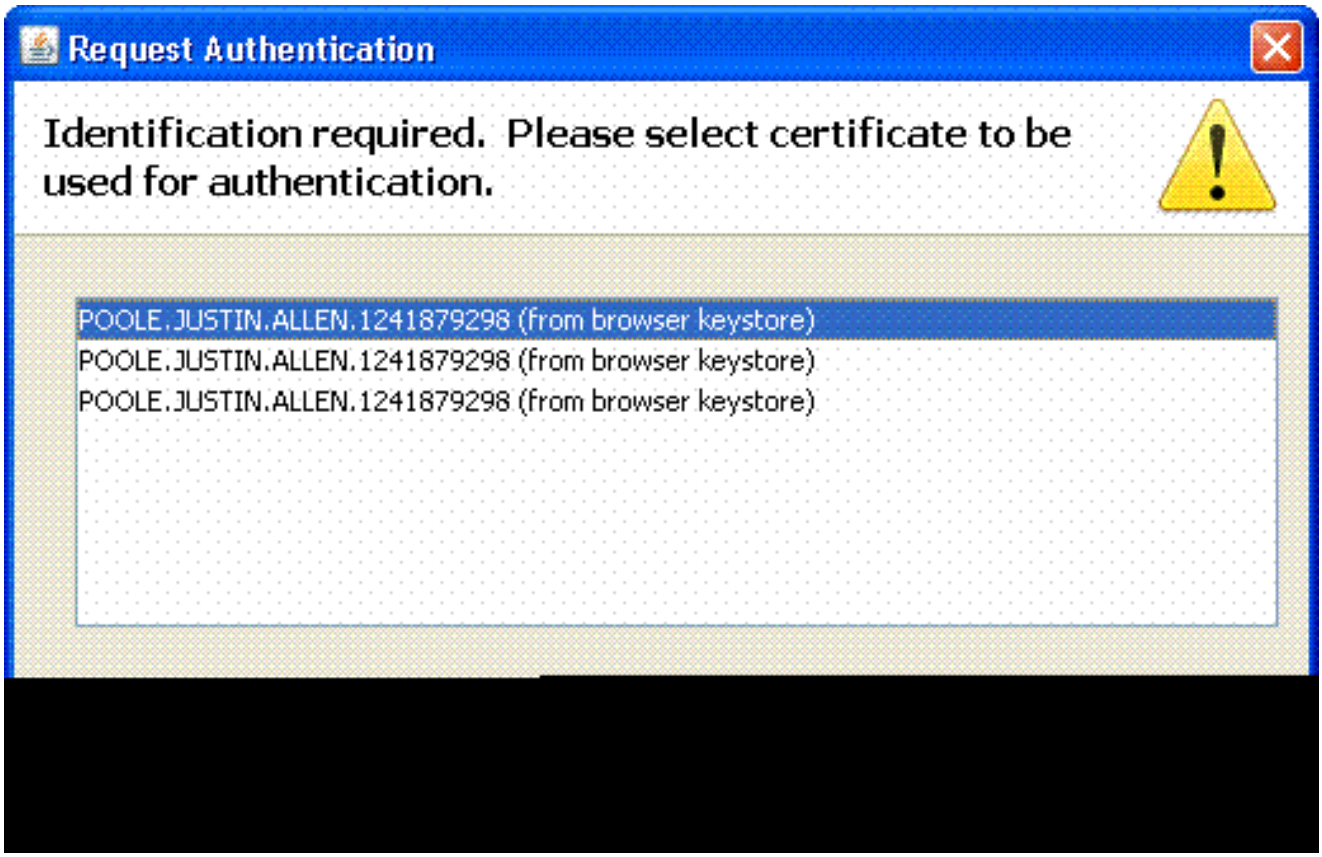
6. AnyConnect comienza a descargar el cliente. Consulte la Figura 29.

Figura 29: Instalación de AnyConnect



7. Elija el certificado adecuado que desea utilizar. Vea la Figura 30. AnyConnect continúa con la instalación. El administrador de ASA puede permitir que el cliente instale o instale de forma permanente en cada conexión de ASA.

Figura 30: Certificado



Inicio de Cisco AnyConnect VPN Client - Windows

En el equipo host, elija Inicio > Todos los programas > Cisco > AnyConnect VPN Client.

Nota: Consulte el Apéndice E para obtener información sobre la configuración opcional del perfil de cliente de AnyConnect.

Nueva conexión

1. Aparecerá la ventana AC. Consulte la Figura 34.

Figura 34: Nueva conexión VPN

2. Elija el host adecuado si AC no intenta la conexión automáticamente.

3. Introduzca el PIN cuando se le solicite. Consulte la Figura 35.

Figura 35: Introducir PIN

Iniciar acceso remoto

Elija el grupo y el host al que desea conectarse.

Dado que se utilizan certificados, elija Connect para establecer la VPN. Consulte la Figura 36.

Figura 36: Conexión


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.

Nota: Dado que la conexión utiliza certificados, no es necesario introducir un nombre de usuario y una contraseña.

Nota: Consulte el Apéndice E para obtener información sobre la configuración opcional del perfil de cliente de AnyConnect.

Apéndice A: Asignación LDAP y DAP

En ASA/PIX versión 7.1(x) y posteriores, se introdujo una función llamada mapeo LDAP. Se trata de una potente función que proporciona una asignación entre un atributo de Cisco y objetos/atributos LDAP, lo que elimina la necesidad de cambiar el esquema LDAP. Para la implementación de la autenticación CAC, esto puede admitir la aplicación de políticas adicionales en conexiones de acceso remoto. Estos son ejemplos de mapeo LDAP. Tenga en cuenta que necesita derechos de administrador para realizar cambios en el servidor AD/LDAP. En el software ASA 8.x, se introdujo la función de política de acceso dinámica (DAP). DAP puede trabajar en conjunto con CAC para observar múltiples grupos AD así como políticas de inserción, ACL y así sucesivamente.

Situación 1: aplicación de Active Directory mediante acceso telefónico con permiso de acceso remoto: permitir/denegar acceso

Este ejemplo asigna el atributo de AD msNPAllowDailin al atributo cVPN3000-Tunneling- Protocol de Cisco.

- El valor del atributo AD: TRUE = Allow; FALSE = Deny
- Valor del atributo de Cisco: 1 = FALSE, 4 (IPSec) o 20 (4 IPSEC + 16 WebVPN) = TRUE,

Para la condición ALLOW, asigne:

- TRUE = 20

Para la condición de acceso telefónico DENY, asigne:

- FALSO = 1

Nota: Asegúrese de que TRUE y FALSE estén en mayúsculas. Consulte Configuración de un Servidor Externo para la Autorización de Usuario del Dispositivo de Seguridad para obtener más información.

Configuración de Active Directory

1. En el Servidor de directorio activo, haga clic en Inicio > Ejecutar.
2. En el cuadro de texto Abrir, escriba dsa.msc y haga clic en Aceptar. Esto inicia la consola de

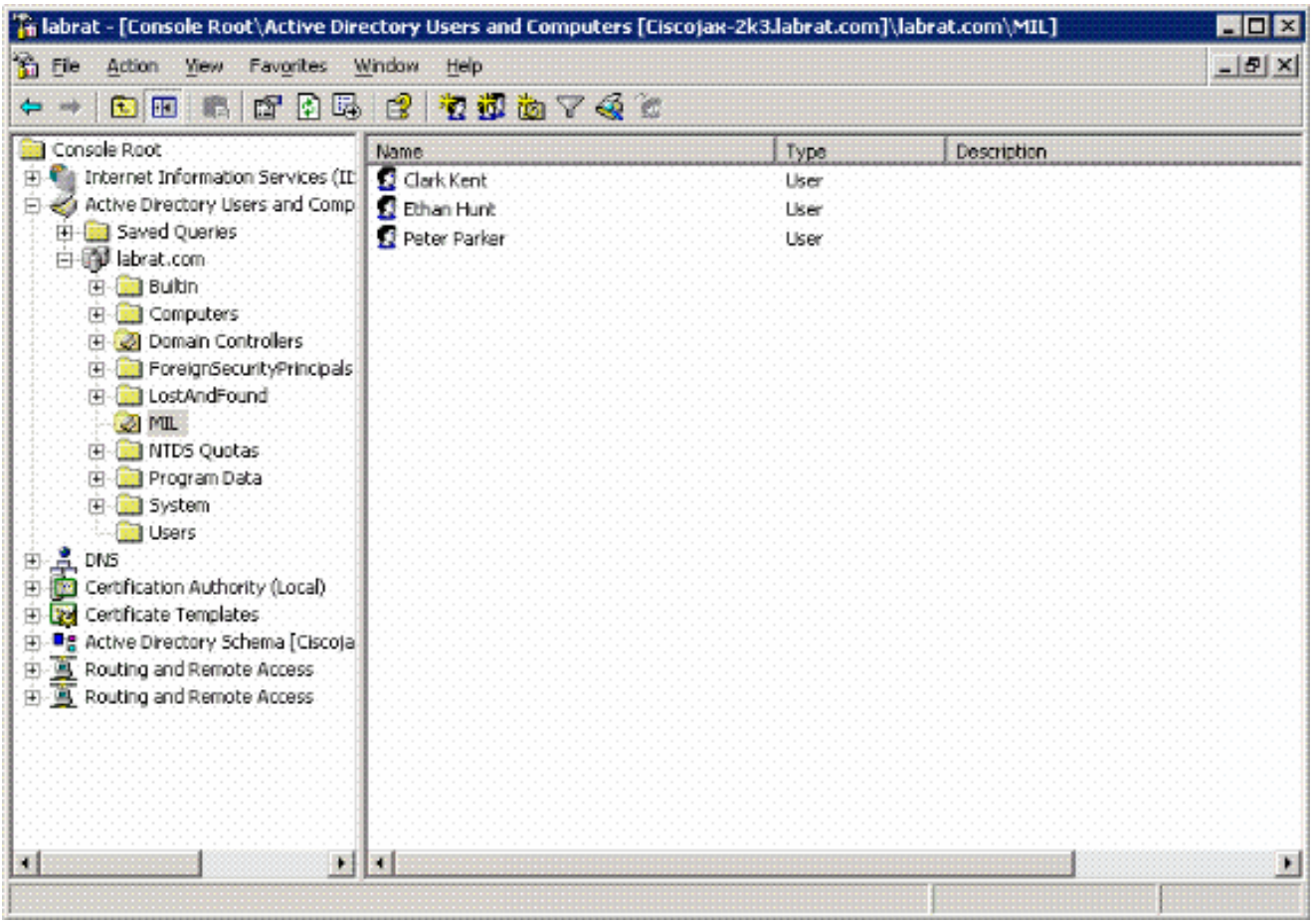
administración de Active Directory.

3. En la consola de administración de Active Directory, haga clic en el signo más para expandir Usuarios y equipos de Active Directory.

4. Haga clic en el signo más para expandir el nombre de dominio.

5. Si tiene una OU creada para sus usuarios, expanda la OU para ver todos los usuarios; si tiene todos los usuarios asignados en la carpeta Usuarios, expanda esa carpeta para verlos. Consulte la figura A1.

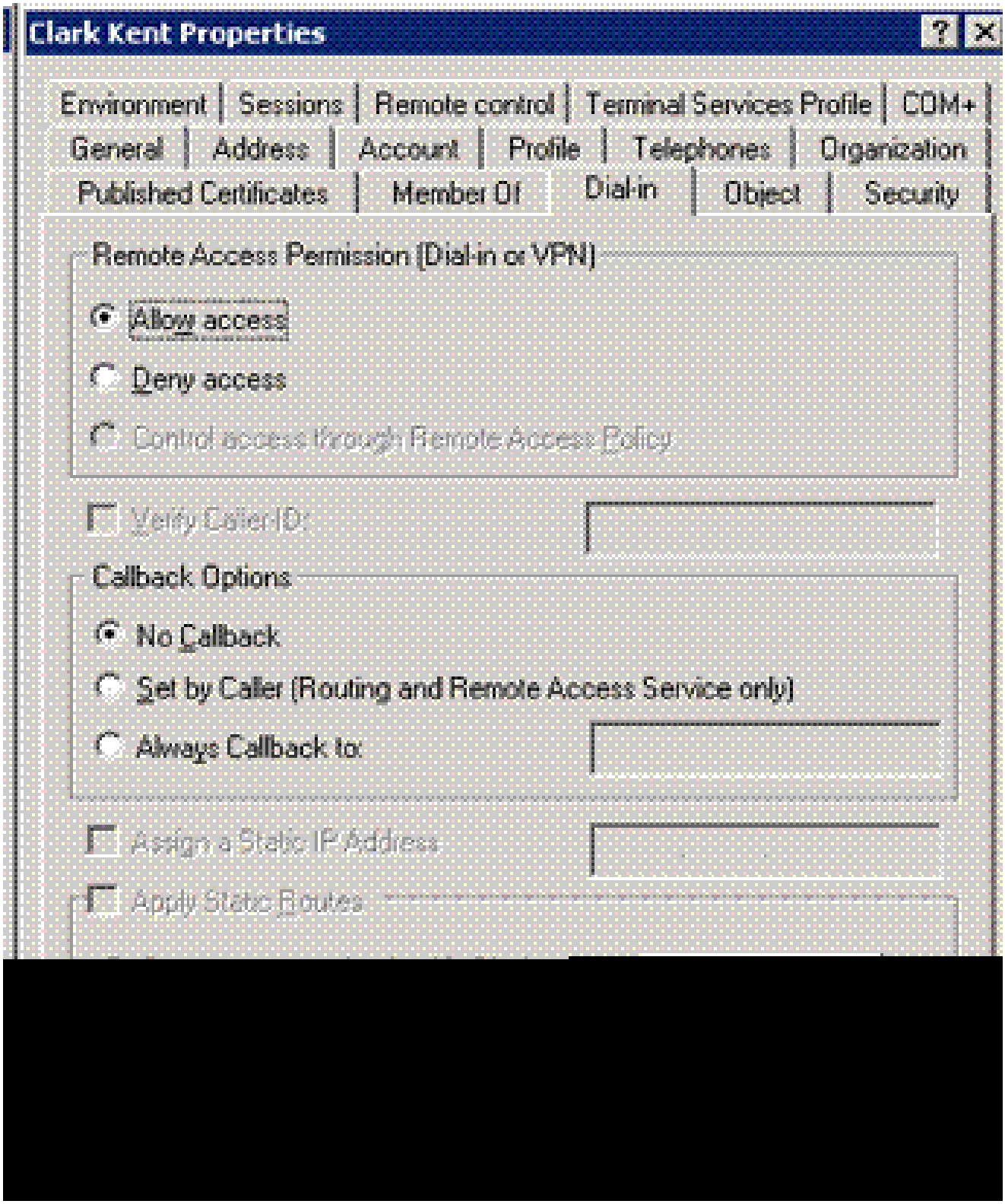
   Figura A1: Consola de administración de Active Directory



6. Haga doble clic en el usuario que desea editar.

   Haga clic en la ficha Dial-in en la página de propiedades del usuario y haga clic en allow o deny. Consulte la figura A2.

   Figura A2: Propiedades de usuario

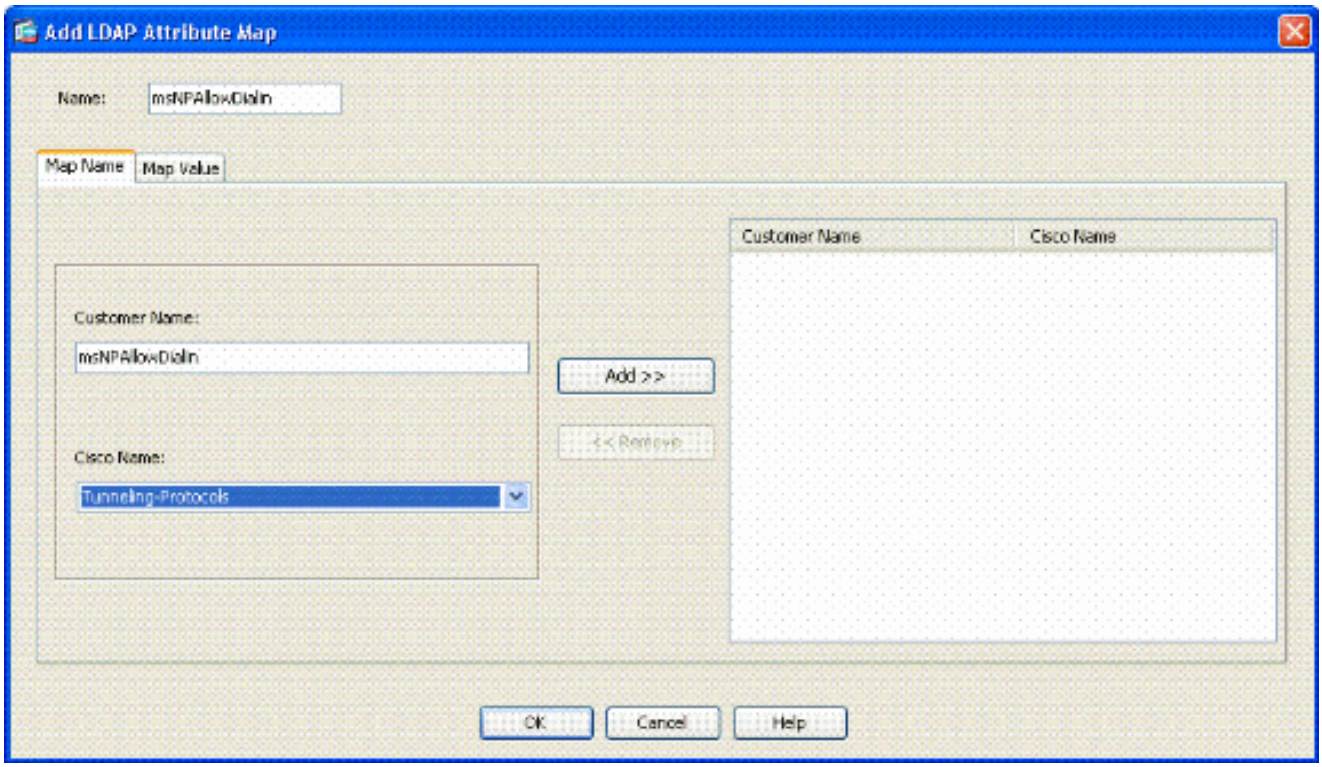


7. Luego haga clic en OK (Aceptar).

Configuración de ASA

1. En ASDM, elija Remote Access VPN> AAA Setup > LDAP Attribute Map.
2. Haga clic en Add (Agregar).
3. En la ventana Add LDAP Attribute Map , complete estos pasos. Consulte la figura A3.

Figura A3: Adición de un Mapa de Atributos LDAP



a. Introduzca un nombre en el cuadro de texto Nombre.

b. En la ficha Nombre de mapa, escriba msNPAllowDialin en el cuadro de texto Nombre del cliente.

c. En la pestaña Map Name, elija Tunneling-Protocols en la opción desplegable del nombre de Cisco.

d. Haga clic en Add (Agregar).

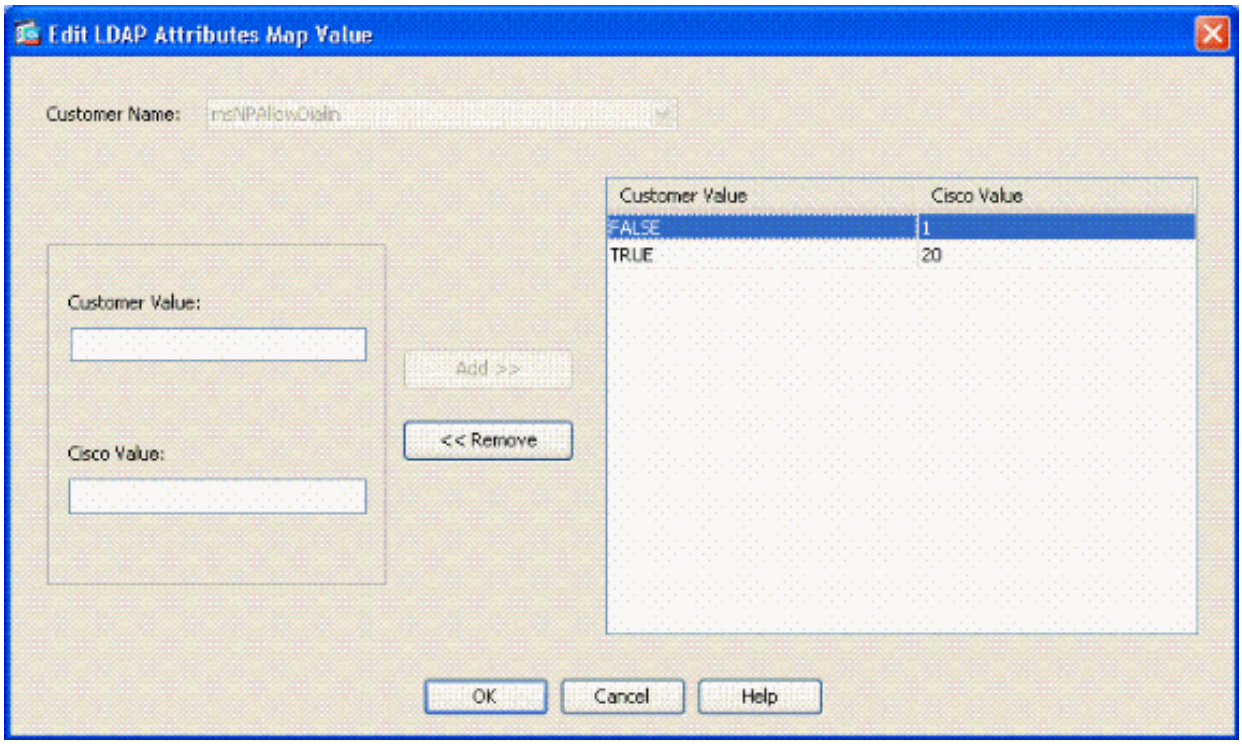
e. Elija la pestaña Asignar valor.

f. Haga clic en Add (Agregar).

g. En la ventana Add Attribute LDAP Map Value, escriba TRUE en el cuadro de texto Customer Name y escriba 20 en el cuadro de texto Cisco Value.

h. Haga clic en Add (Agregar).

i. Escriba FALSE en el cuadro de texto Nombre del cliente y escriba 1 en el cuadro de texto Valor de Cisco. Consulte la figura A4.



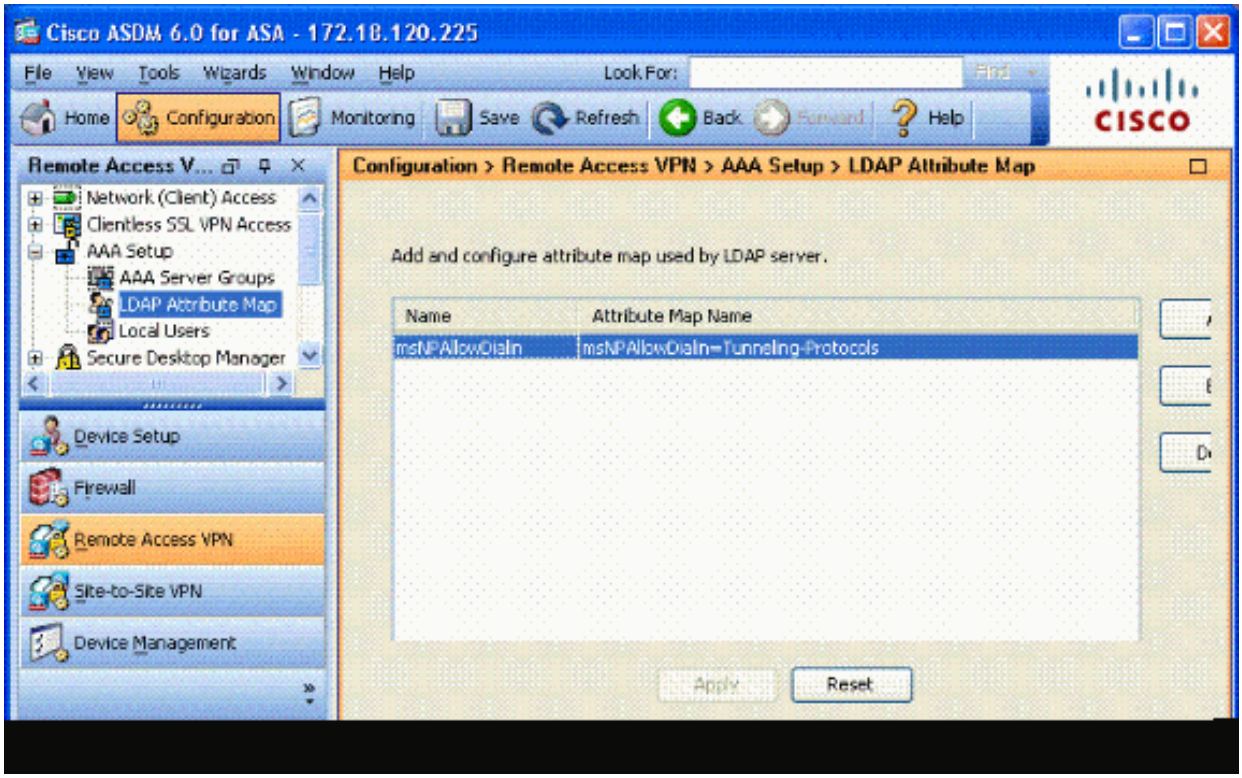
j. Click OK.

k. Click OK.

l. Haga clic en Apply (Aplicar).

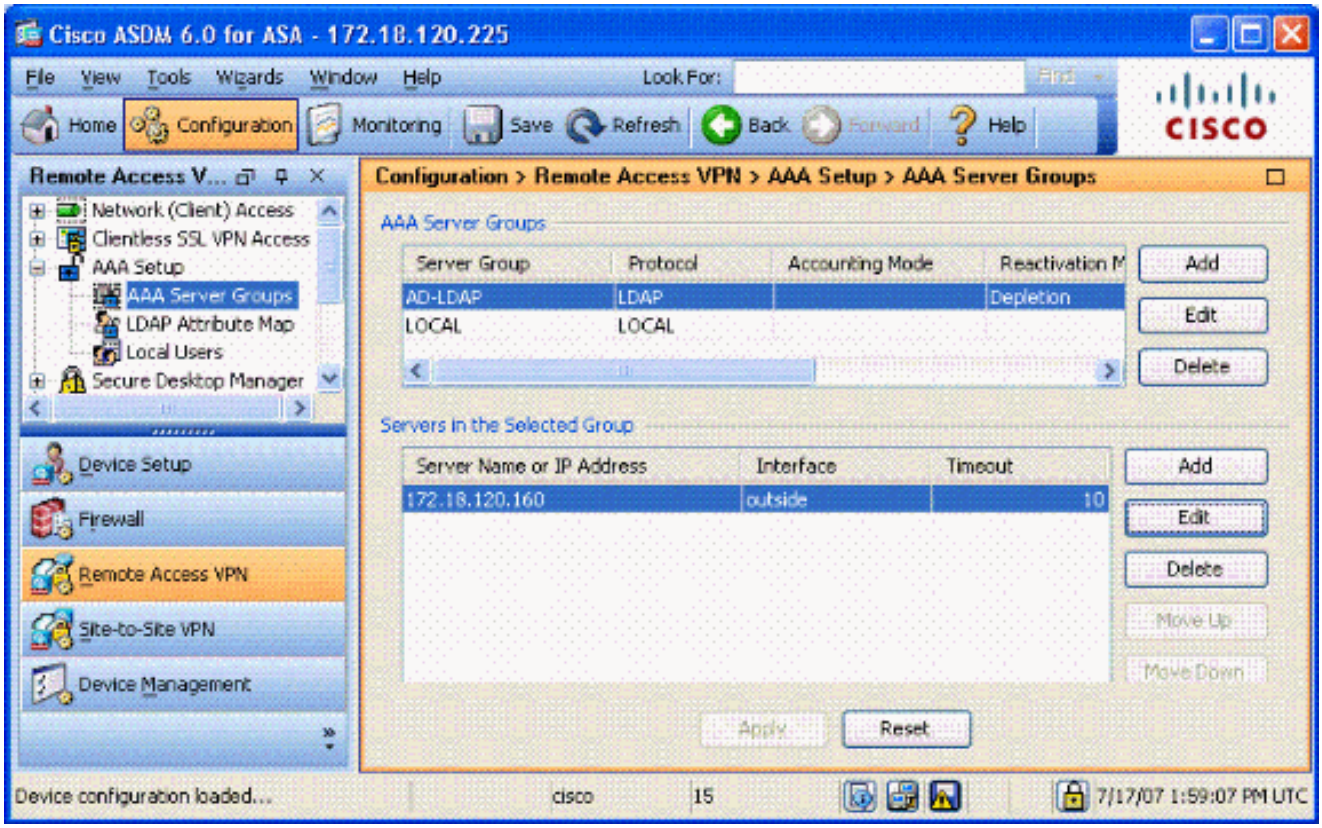
m. La configuración debe ser similar a la de la figura A5.

Figura A5: Configuración del mapa de atributos LDAP



4. Elija Remote Access VPN> AAA Setup > AAA Server Groups. Consulte la figura A6.

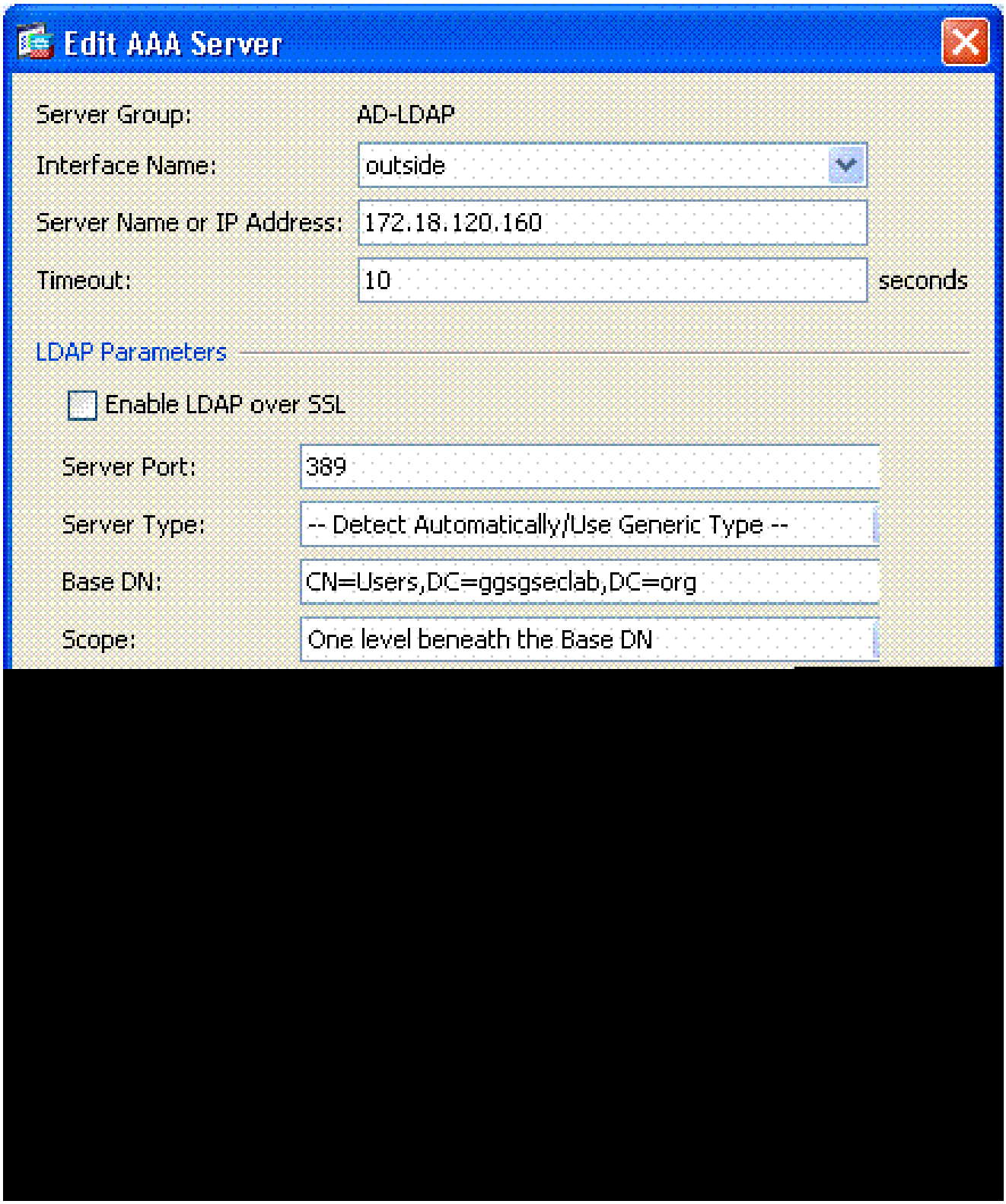
   Figura A6: Grupos de servidores AAA



5. Haga clic en el grupo de servidores que desea editar. En la sección Servidores del grupo seleccionado, elija la dirección IP o el nombre de host del servidor y, a continuación, haga clic en Editar.

6. En la ventana Edit AAA Server (Editar servidor AAA), en el cuadro de texto LDAP Attribute Map (Mapa de atributos LDAP), elija el mapa de atributos LDAP creado en el menú desplegable. Consulte la figura A7

   Figura A7: Adición de un Mapa de Atributos LDAP



7. Click OK.

Nota: Active la depuración LDAP mientras prueba para verificar si el enlace LDAP y la asignación de atributos funcionan correctamente. Consulte el Apéndice C para ver los comandos de solución de problemas.

Situación 2: aplicación de Active Directory utilizando la pertenencia al grupo para

permitir/denegar el acceso

Este ejemplo utiliza el atributo de LDAP memberOf para asignar al atributo de Protocolo de tunelación con el fin de establecer la pertenencia a un grupo como condición. Para que esta política funcione, debe tener estas condiciones:

- Utilice un grupo que ya exista o cree un nuevo grupo para que los usuarios de VPN ASA sean miembros de las condiciones ALLOW.
- Utilice un grupo que ya exista o cree un nuevo grupo para que los usuarios que no sean ASA sean miembros de para las condiciones DENY.
- Asegúrese de verificar en el visor LDAP que tiene el DN correcto para el grupo. Ver Apéndice D. Si el DN es incorrecto, la asignación no funciona correctamente.

Nota: Tenga en cuenta que ASA sólo puede leer la primera cadena del atributo memberOf en esta versión. Asegúrese de que el nuevo grupo creado se encuentra en la parte superior de la lista. La otra opción es colocar un carácter especial delante del nombre cuando AD mire primero a los caracteres especiales. Para evitar esta advertencia, utilice DAP en el software 8.x para ver varios grupos.

Nota: Asegúrese de que un usuario forme parte del grupo de denegación o al menos de otro grupo para que memberOf siempre se envíe de vuelta al ASA. No es necesario especificar la condición de denegación FALSE, pero se recomienda hacerlo. Si el nombre de grupo existente o el nombre de grupo contiene un espacio, introduzca el atributo de la siguiente manera:

```
CN=Operadores de copia de seguridad,CN=Builtin,DC=ggsgseclab,DC=org
```

Nota: DAP permite al ASA observar varios grupos en el atributo memberOf y la autorización base de los grupos. Consulte la sección DAP.

ASIGNACIÓN

- El valor del atributo AD:
  - memberOf CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
  - memberOf CN=TelnetClients,CN=Users,DC=laboratorio,DC=com
- Valor del atributo de Cisco: 1 = FALSE, 20 = TRUE,

Para la condición ALLOW, asigne:

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

Para la condición DENY, se asigna:

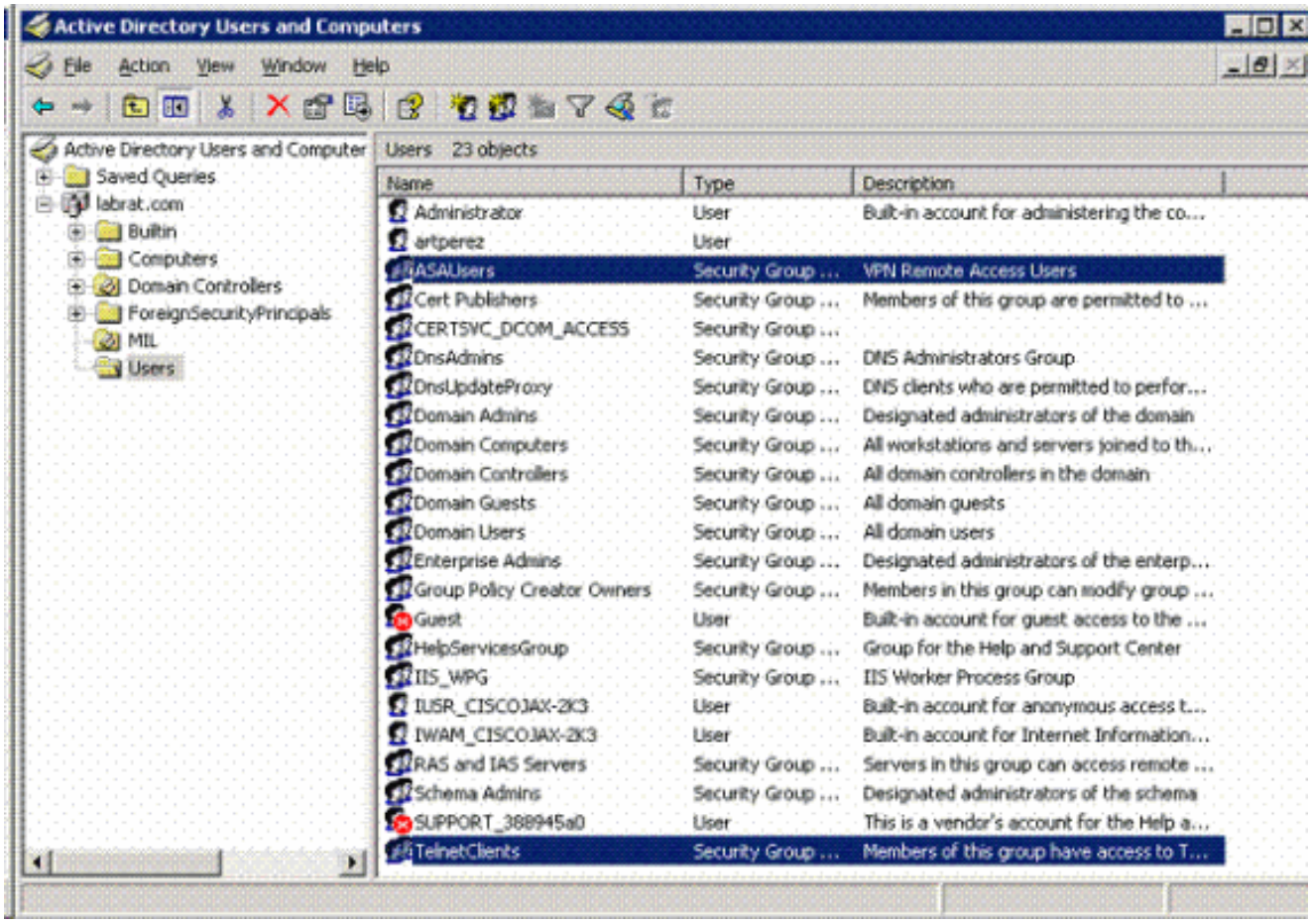
- memberOf CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org = 1

Nota: En versiones futuras, hay un atributo de Cisco para permitir y denegar la conexión. Consulte Configuración de un Servidor Externo para la Autorización de Usuario del Dispositivo de Seguridad para obtener más información sobre los atributos de Cisco.

Configuración de Active Directory

1. En el Servidor de directorio activo, elija Inicio > Ejecutar.
2. En el cuadro de texto Abrir, escriba dsa.msc y, a continuación, haga clic en Aceptar. Esto inicia la consola de administración de Active Directory.
3. En la consola de administración de Active Directory, haga clic en el signo más para expandir Usuarios y equipos de Active Directory. Consulte la figura A8

   Figura A8: Grupos de Active Directory



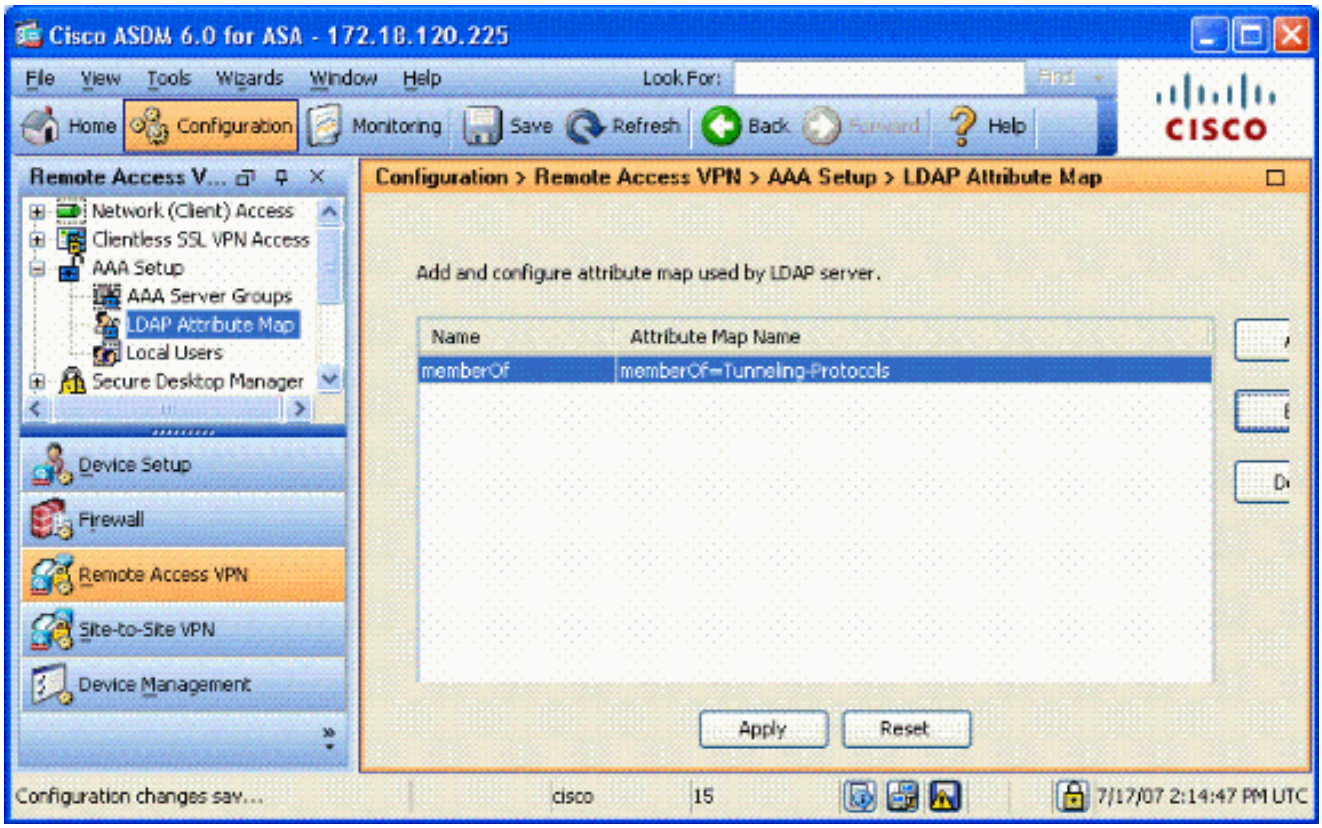
4. Haga clic en el signo más para expandir el nombre de dominio.
5. Haga clic con el botón derecho en la carpeta Users y elija New > Group.
6. Introduzca un nombre de grupo. Por ejemplo: ASAUsers.
7. Click OK.

8. Haga clic en la carpeta Users y luego haga doble clic en el grupo que acaba de crear.
9. Elija la pestaña Members y, a continuación, haga clic en Add.
10. Escriba el nombre del usuario que desea agregar y, a continuación, haga clic en Aceptar.

Configuración de ASA

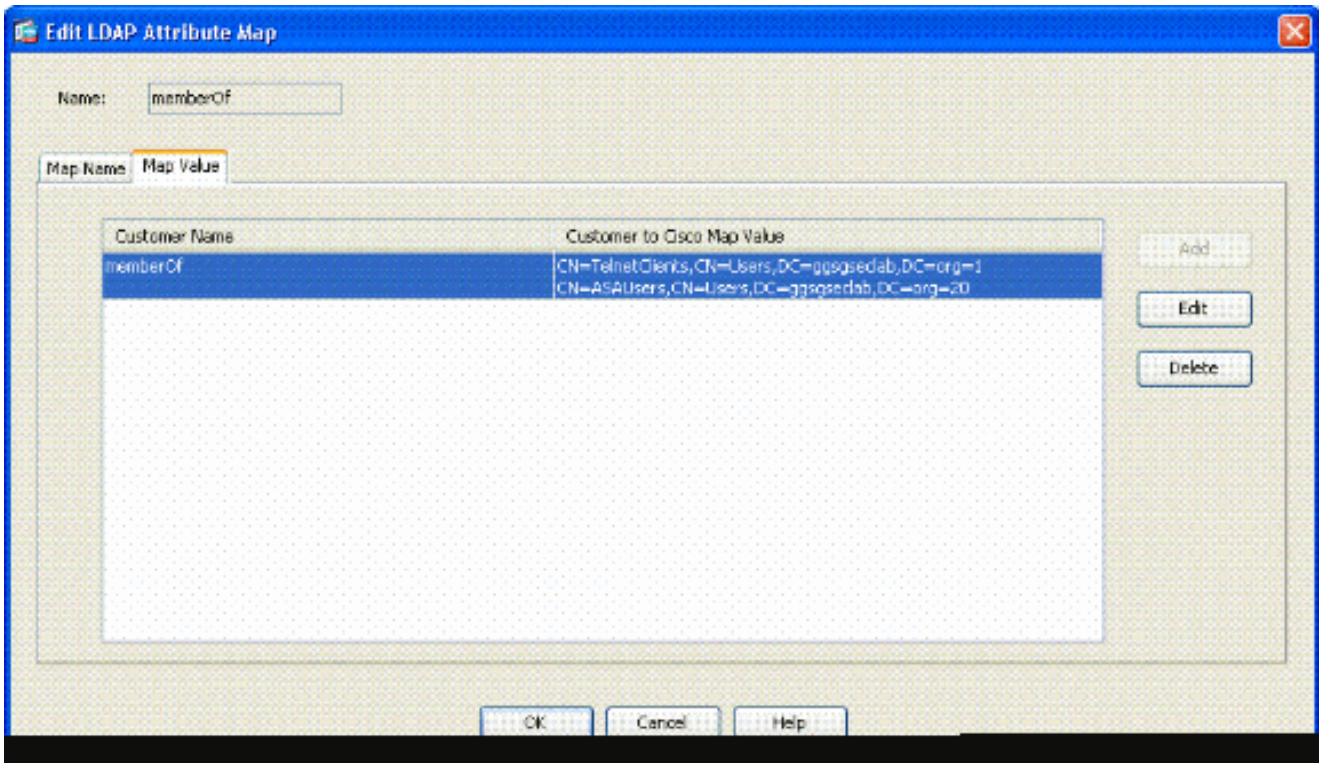
1. En ASDM, elija Remote Access VPN > AAA Setup > LDAP Attribute Map.
2. Haga clic en Add (Agregar).
3. En la ventana Add LDAP Attribute Map , complete estos pasos. Consulte la figura A3.
    a. Introduzca un nombre en el cuadro de texto Nombre.
    b. En la ficha Nombre del mapa, escriba memberOf en el cuadro de texto Nombre del cliente c.
    c. En la pestaña Map Name, elija Tunneling-Protocols en la opción desplegable del nombre de Cisco.
    d. Elija Agregar.
    e. Haga clic en la pestaña Asignar valor.
    f. Elija Agregar.
    g. En la ventana Add Attribute LDAP Map Value, escriba CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org en el cuadro de texto Customer Name y escriba 20 en el cuadro de texto Cisco Value.
    h. Haga clic en Add (Agregar).
    i. Escriba CN=TelnetClients,CN=Users,DC=ggsgseclab,DC=org en el cuadro de texto Nombre del cliente y escriba 1 en el cuadro de texto Valor de Cisco. Consulte la figura A4.
    j. Click OK.
    k. Click OK.
    l. Haga clic en Apply (Aplicar).
    m. La configuración debe ser similar a la de la figura A9.

Figura A9 Mapa de atributos LDAP



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

5. Haga clic en el grupo de servidores que desea editar. En la sección Servidores del grupo seleccionado, seleccione la dirección IP o el nombre de host del servidor y, a continuación, haga clic en Editar



6. En la ventana Edit AAA Server (Editar servidor AAA), en el cuadro de texto LDAP Attribute Map (Mapa de atributos LDAP), seleccione el mapa de atributos LDAP creado en el menú

desplegable.

7. Click OK.

Nota: Active la depuración LDAP mientras prueba para verificar que el enlace LDAP y las asignaciones de atributos funcionen correctamente. Consulte el Apéndice C para ver los comandos de solución de problemas.

Situación 3: Políticas de acceso dinámicas para varios atributos memberOf

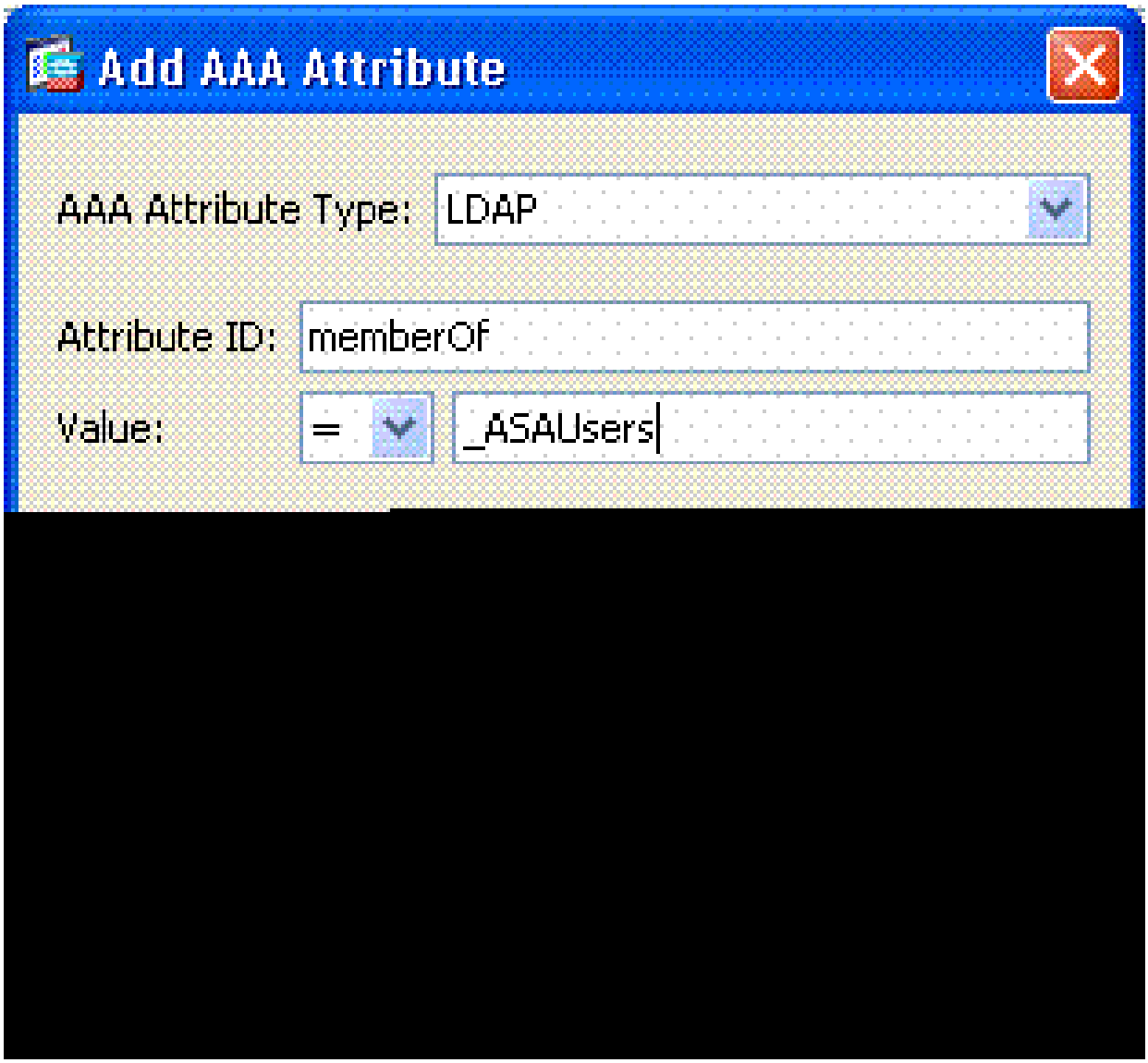
En este ejemplo se utiliza DAP para examinar varios atributos memberOf a fin de permitir el acceso basado en la pertenencia a grupos de Active Directory. Antes de 8.x, el ASA sólo leía el primer atributo memberOf. Con 8.x y versiones posteriores, ASA puede observar todos los atributos memberOf.

- Utilice un grupo que ya exista o cree un nuevo grupo (o varios grupos) para que los usuarios de VPN ASA sean miembros de las condiciones ALLOW.
- Utilice un grupo que ya exista o cree un nuevo grupo para que los usuarios que no sean ASA sean miembros de para las condiciones DENY.
- Asegúrese de verificar en el visor LDAP que tiene el DN correcto para el grupo. Ver Apéndice D. Si el DN es incorrecto, la asignación no funciona correctamente.

Configuración de ASA

1. En ASDM, elija Remote Access VPN> Network (Client) Access > Dynamic Access Policies.
2. Haga clic en Add (Agregar).
3. En Agregar directiva de acceso dinámica, siga estos pasos:
    a. Introduzca un nombre en el cuadro de texto Nombre b.
    b. En la sección de prioridad, introduzca 1 o un número mayor que 0.
    c. En los criterios de selección, haga clic en Agregar.
    d. En Add AAA Attribute , elija LDAP .
    e. En la sección ID de atributo, introduzca memberOf.
    f. En la sección de valores, elija = e introduzca el nombre del grupo de AD. Repita este paso para cada grupo al que desee hacer referencia. Consulte la figura A10.

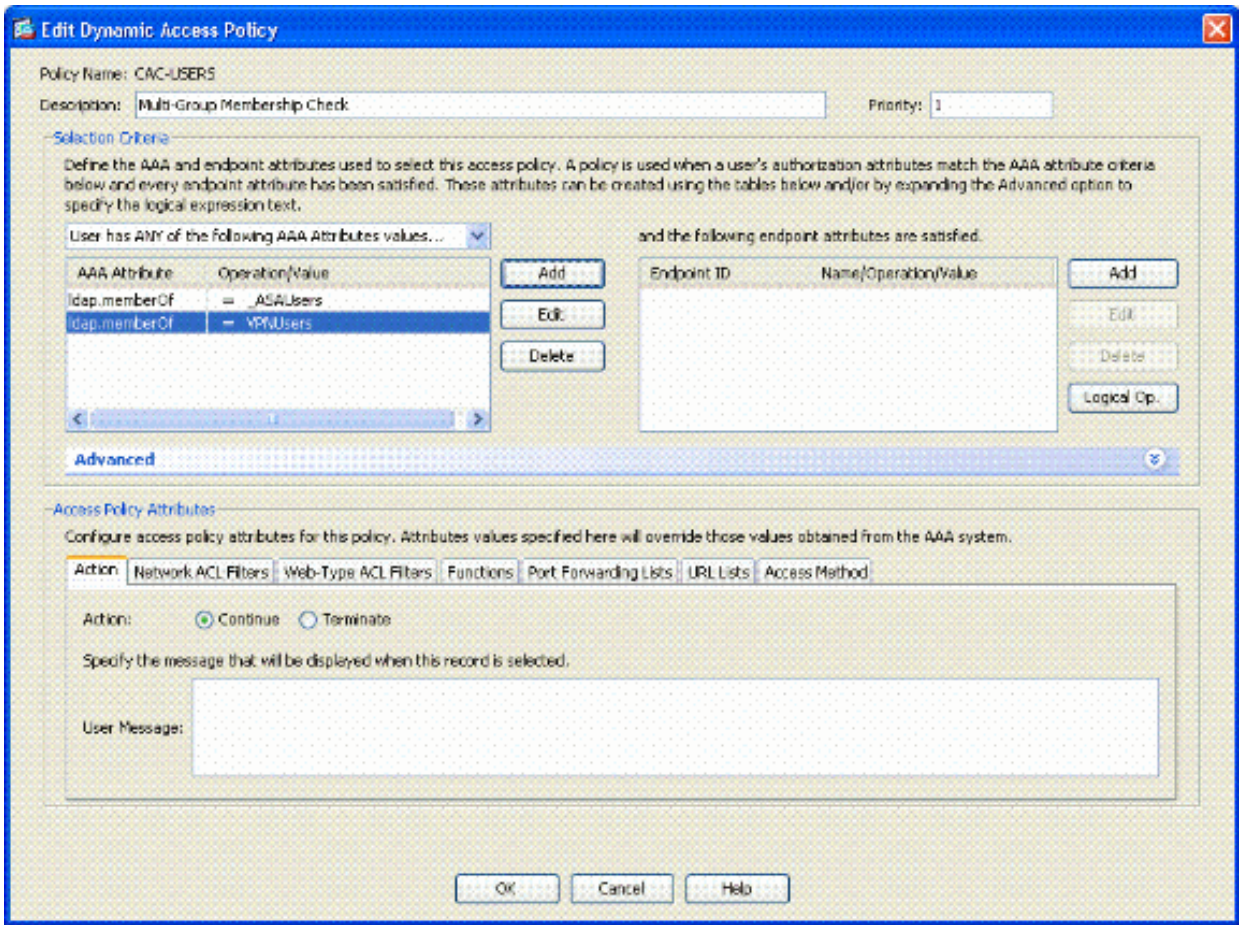
    Figura A10 Mapa de atributos AAA



g. Click OK.

h. En la sección Atributos de política de acceso, elija Continuar. Consulte la figura A11.

Figura A11: Agregar una política dinámica

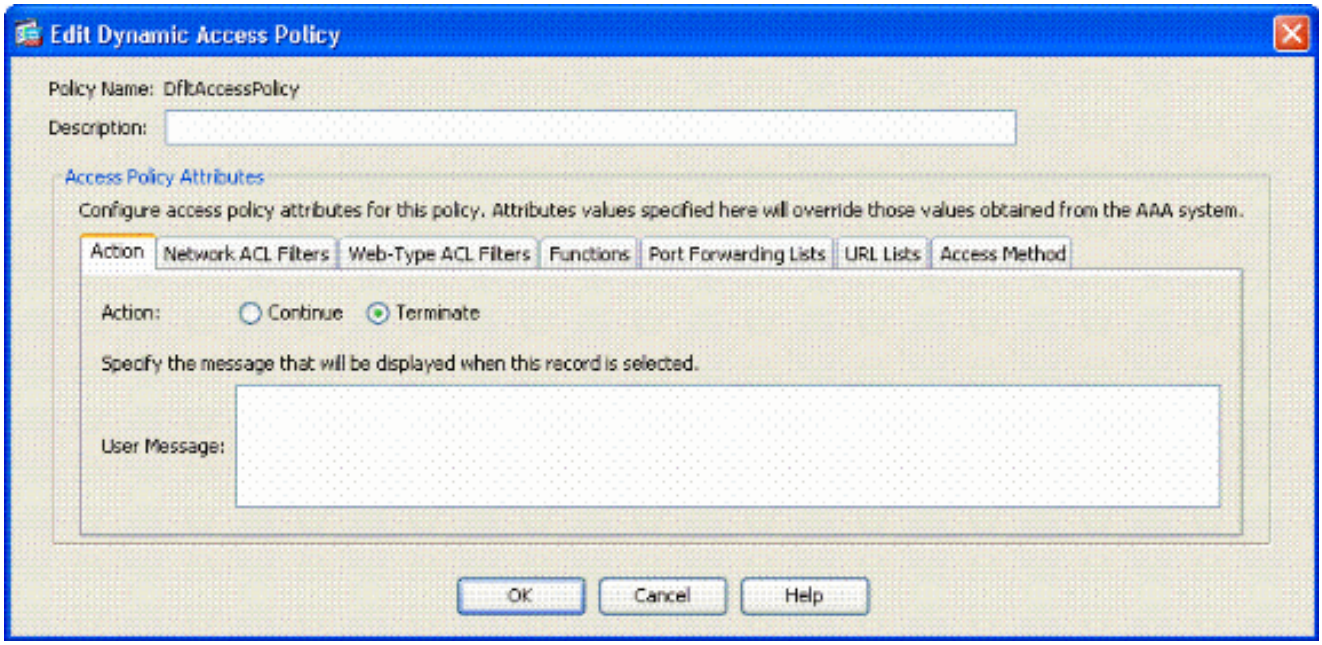


4. En ASDM, elija Remote Access VPN> Network (Client) Access > Dynamic Access Policies.

5. Elija Default Access Policy y elija Edit.

6. La acción predeterminada debe establecerse en Terminate. Consulte la figura A12.

   Figura A12 Editar política dinámica



7. Click OK.

Nota: Si la opción Terminar no está seleccionada, podrá entrar aunque no pertenezca a ningún grupo, ya que el valor predeterminado es Continuar.

Apéndice B: Configuración de 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
```

Apéndice C: Resolución de problemas

Resolución de problemas de AAA y LDAP

- debug ldap 255—Muestra intercambios LDAP
- debug aaa common 10—Muestra intercambios AAA

Ejemplo 1: Conexión permitida con asignación de atributos correcta

Este ejemplo muestra el resultado de debug ldap y debug aaa common durante una conexión exitosa con el escenario 2 mostrado en el Apéndice A.

Figura C1: resultado común de debug LDAP y debug aaa - asignación correcta

```
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..50........./........60...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[78] userCertificate: value =
0..'0........./..t.....50...*.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#
```

Ejemplo 2: Conexión permitida con asignación de atributos de Cisco mal configurada

Este ejemplo muestra el resultado de debug ldap y debug aaa common durante una conexión permitida con el escenario 2 mostrado en el Apéndice A.

Figura C2: resultado común de debug LDAP y debug aaa - asignación incorrecta

```
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—Muestra errores DAP
- debug dap trace: muestra el seguimiento de la función DAP

Ejemplo 1: conexión permitida con DAP

Este ejemplo muestra la salida de debug dap errors y debug dap trace durante una conexión exitosa con el escenario 3 que se muestra en el Apéndice A. Observe múltiples atributos memberOf. Puede pertenecer tanto a _ASAUsers como a VPNUsers o a cualquiera de los grupos, lo que depende de la configuración de ASA.

Figura C3: debug DAP

```
<#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.
```

Ejemplo 2: conexión denegada con DAP

Este ejemplo muestra la salida de debug dap errors y debug dap trace durante una conexión fallida con el escenario 3 que se muestra en el Apéndice A.

Figura C4: debug DAP

```
<#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
```

Resolución de problemas de Certificate Authority / OCSP

- debug crypto ca 3
- En el modo de configuración—logging class ca console(or buffer) debugging

Estos ejemplos muestran una validación de certificado exitosa con el respondedor OCSP y una política de coincidencia de grupo de certificados fallidos.

La figura C3 muestra el resultado de la depuración que tiene un certificado validado y un grupo de certificados de trabajo que coinciden con la directiva.

La figura C4 muestra la salida de depuración de una política de coincidencia de grupo de certificados mal configurada.

La figura C5 muestra la salida de depuración de un usuario con un certificado revocado.

Figura C5: Depuración de OCSP: validación de certificados correcta

```
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: Salida de una política de coincidencia de grupo de certificados fallida

Figura C5: Salida de un certificado revocado

```
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
```

Apéndice D: Verificación de objetos LDAP en MS

En el CD de Microsoft Server 2003, hay herramientas adicionales que se pueden instalar para ver la estructura LDAP así como los objetos/atributos LDAP. Para instalar estas herramientas, vaya al directorio Support en el CD y luego a Tools. Instale SUPTOOLS.MSI.

Visor LDAP

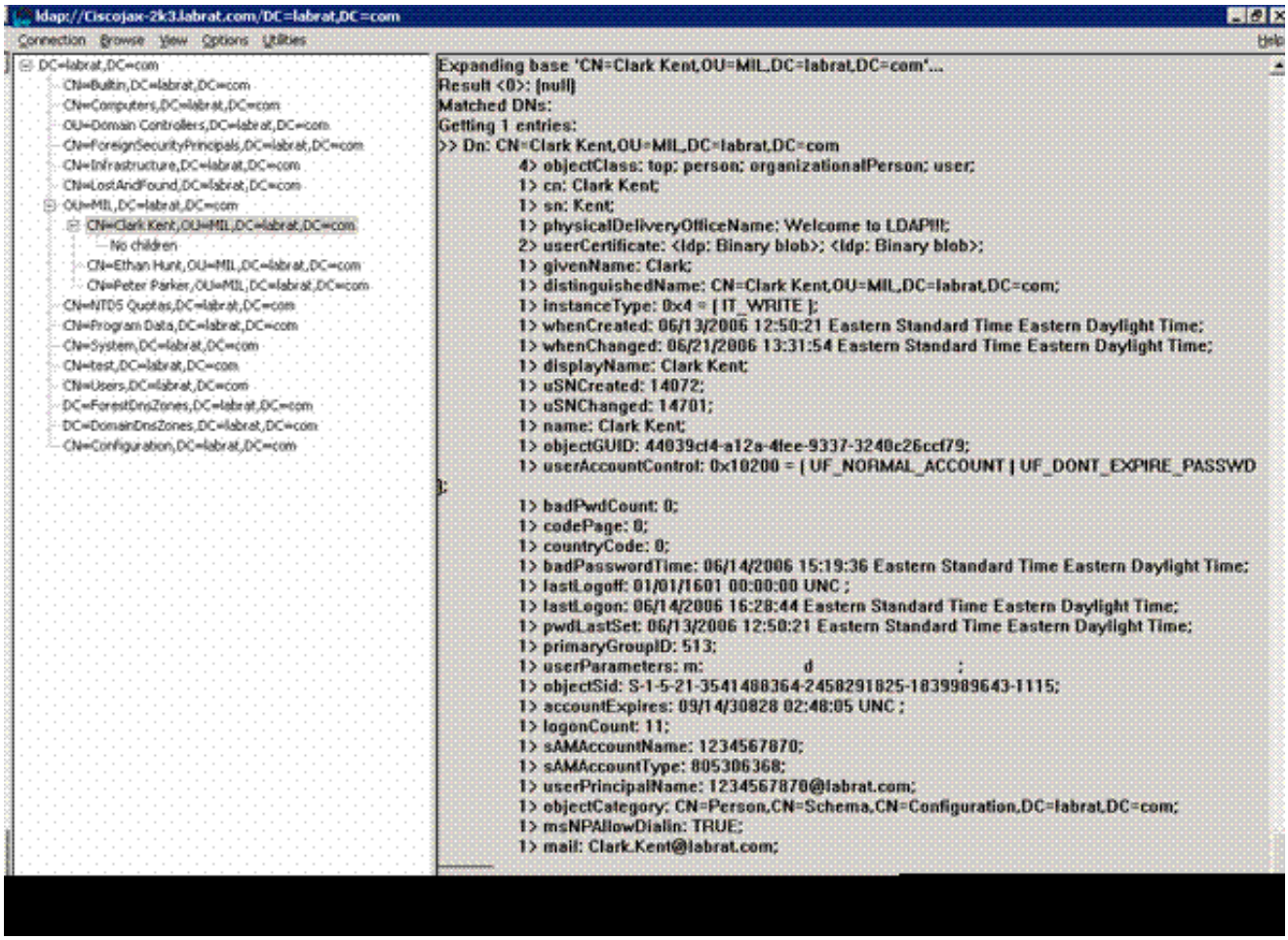
1. Después de la instalación, elija Start > Run.
2. Escriba ldp y haga clic en Aceptar. Esto inicia el visor LDAP.
3. Elija Connection > Connect.
4. Introduzca el nombre del servidor y haga clic en Aceptar.
5. Elija Connection > Bind.
6. Introduzca un nombre de usuario y una contraseña.

   Nota: Necesita derechos de administrador.

   ---

7. Click OK.
8. Ver objetos LDAP. Consulte la figura D1.

   Figura D1: Visor LDAP

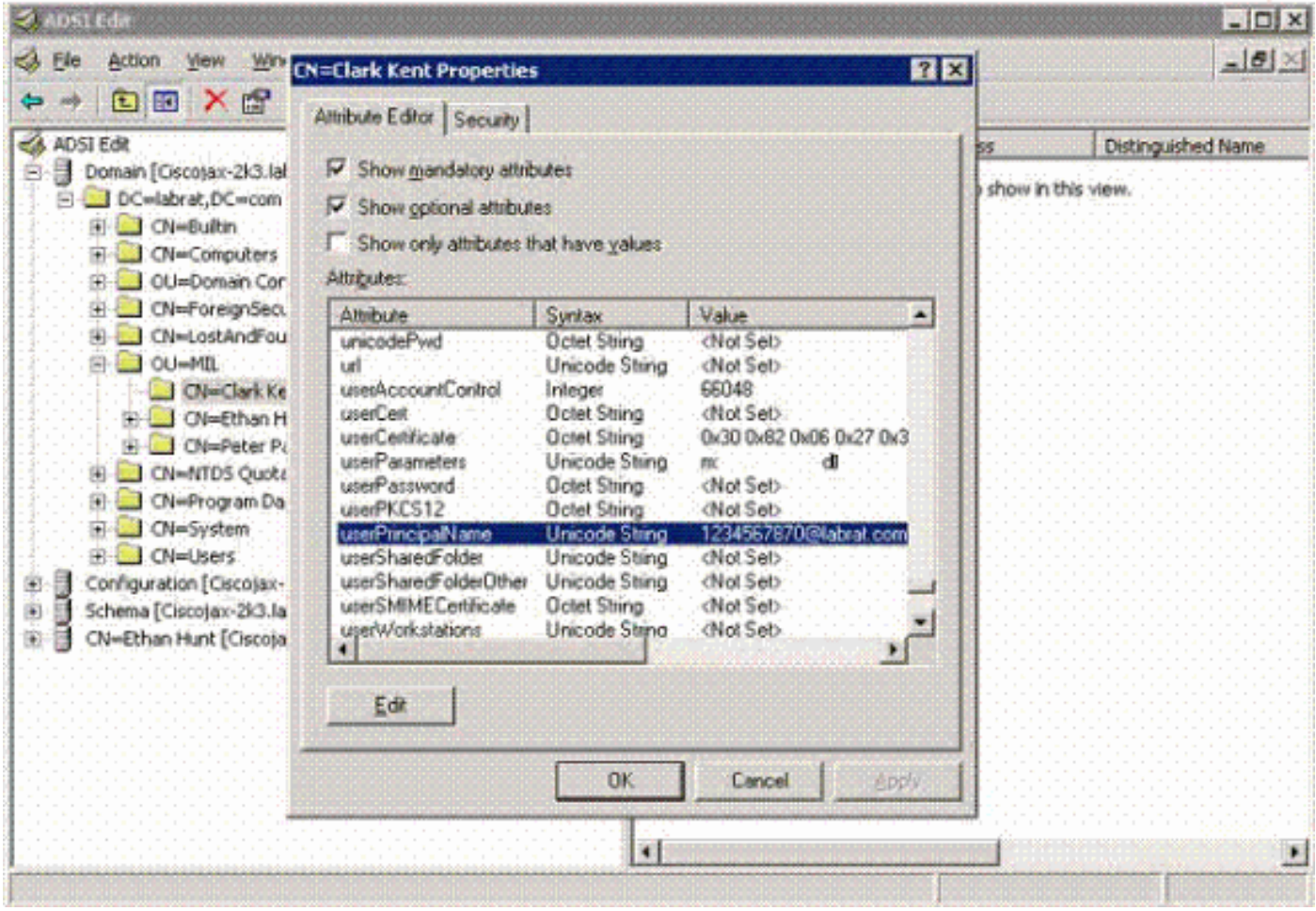


Editor de interfaz de Servicios de Active Directory

- En el servidor de Active Directory, elija Inicio > Ejecutar.
- Escriba adsiedit.msc. Esto inicia el editor.
- Haga clic con el botón derecho del ratón en un objeto y haga clic en Propiedades.

Esta herramienta muestra todos los atributos de objetos específicos. Consulte la figura D2.

Figura D2: Edición de ADSI



Apéndice E

Se puede crear un perfil de AnyConnect y agregarlo a una estación de trabajo. El perfil puede hacer referencia a varios valores, como hosts ASA o parámetros de coincidencia de certificados, como el nombre distinguido o el emisor. El perfil se almacena como un archivo .xml y se puede editar con el Bloc de notas. El archivo se puede agregar a cada cliente manualmente o extraerlo del ASA a través de una política de grupo. El archivo se almacena en:

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

Complete estos pasos:

1. Elija AnyConnectProfile.tmpl y abra el archivo con el Bloc de notas.
2. Realice las modificaciones adecuadas en el archivo, como la IP del host o del emisor. Consulte la figura F1 para ver un ejemplo.
3. Cuando haya terminado, guarde el archivo como un .xml.

Consulte la documentación de Cisco AnyConnect con respecto a la administración de perfiles. En

resumen:

- Un perfil debe tener un nombre exclusivo para su empresa. Ejemplo: CiscoProfile.xml
- El nombre del perfil debe ser el mismo, aunque sea diferente para grupos individuales dentro de la empresa.

Este archivo está pensado para que lo mantenga un administrador de gateway seguro y, a continuación, se distribuya con el software cliente. El perfil basado en este XML se puede distribuir a los clientes en cualquier momento. Los mecanismos de distribución admitidos son como un archivo agrupado con la distribución de software o como parte del mecanismo de descarga automática. El mecanismo de descarga automática sólo está disponible con determinados productos Cisco Secure Gateway.

> Nota: se recomienda encarecidamente a los administradores que validen el perfil XML que crean con una herramienta de validación en línea o mediante la funcionalidad de importación de perfiles en ASDM. La validación se puede realizar con AnyConnectProfile.xsd que se encuentra en este directorio. AnyConnectProfile es el elemento raíz que representa el perfil de cliente de AnyConnect.

Este es un ejemplo de un archivo XML de perfil de cliente VPN de Cisco AnyConnect.

```
<#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>
```

Información Relacionada

- Certificados y CRL especificados por X.509 y RFC 3280
- OCSP especificado por RFC 2560
- Introducción a la infraestructura de clave pública
- "OCSP ligero" definido por el borrador estándar
- SSL/TLS especificado por RFC 2246

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).