

ASA 8.x: Configuración de las CAC-tarjetas inteligentes de AnyConnect SSL VPN con el soporte MAC

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración de ASA de Cisco](#)

[Consideraciones sobre la instrumentación](#)

[Autenticación, autorización, configuración que considera \(AAA\)](#)

[Servidor LDAP de la configuración](#)

[Maneje los Certificados](#)

[Genere las claves](#)

[Instale raíz CA los Certificados](#)

[Aliste el ASA y instale el certificado de identidad](#)

[Configuración VPN de AnyConnect](#)

[Cree un pool de la dirección IP](#)

[Cree la directiva del grupo de túnel y del grupo](#)

[Interfaz y configuraciones de imagen del grupo de túnel](#)

[Reglas que corresponden con del certificado \(si OCSP es utilizado\)](#)

[Configuración OCSP](#)

[Certificado del respondedor de la configuración OCSP](#)

[Configuración CA para utilizar OCSP](#)

[Reglas de la configuración OCSP](#)

[Configuración del cliente de Cisco AnyConnect](#)

[Descargando al Cliente Cisco AnyConnect VPN – Mac OS X](#)

[Cliente Cisco AnyConnect VPN del comienzo – Mac OS X](#)

[Nueva conexión](#)

[Comience el Acceso Remoto](#)

[Apéndice A – Sincronización LDAP y DAP](#)

[Escenario 1: Aplicación del Active Directory usando el dial-in del Permiso de acceso remoto – Permita/niegue el acceso](#)

[Configuración del Active Directory](#)

[Configuración ASA](#)

[Escenario 2: La aplicación del Active Directory usando la membresía del grupo a permitir/niega el acceso](#)

[Configuración del Active Directory](#)

[Configuración ASA](#)

[Escenario 3: Directivas del acceso dinámico para los atributos múltiples del memberOf](#)

[Configuración ASA](#)

[Apéndice B – Configuración CLI ASA](#)

[Troubleshooting del apéndice c](#)

[Resolver problemas el AAA y el LDAP](#)

[Ejemplo 1: Conexión permitida con la asignación correcta del atributo](#)

[Ejemplo 2: Conexión permitida con la asignación mis configurada del atributo de Cisco](#)

[Resolver problemas el DAP](#)

[Ejemplo 1: Conexión permitida con el DAP](#)

[Ejemplo 2: Conexión negada con el DAP](#)

[Resolver problemas el Certificate Authority/OCSP](#)

[Apéndice D – Verifique los objetos LDAP en el MS](#)

[Visualizador LDAP](#)

[Editor de la interfaz de los servicios de Active Directory](#)

[Apéndice E](#)

[Información Relacionada](#)

Introducción

Este documento proporciona una configuración de muestra en el dispositivo de seguridad adaptante de Cisco (ASA) para el Acceso Remoto de AnyConnect VPN para el soporte MAC con el indicador luminoso LED amarillo de la placa muestra gravedad menor común del acceso (CAC) para la autenticación.

El alcance de este documento es cubrir la configuración de Cisco ASA con el Directory Access Protocol adaptante del Administrador de dispositivos de seguridad (ASDM), del Cliente Cisco AnyConnect VPN y del Microsoft Active Directory (AD) /Lightweight (LDAP).

La configuración en esta guía utiliza el servidor de Microsoft AD/LDAP. Este documento también cubre las funciones avanzadas tales como OCSP, las correspondencias del atributo LDAP y el acceso dinámico limpia (DAP).

prerrequisitos

Requisitos

Una comprensión básica del cliente de Cisco ASA, de Cisco AnyConnect, de Microsoft AD/LDAP y del Public Key Infrastructure (PKI) es beneficiosa en la comprensión de la configuración completa. La familiaridad con la membresía del grupo AD, las propiedades del usuario así como los objetos LDAP ayudan en la correlación del proceso de la autorización entre los atributos del certificado y los objetos AD/LDAP.

Componentes Utilizados

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

hardware.

- El dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) ese funciona con la versión de software 8.0(x) y posterior
- Versión 6.x del Cisco Adaptive Security Device Manager (ASDM) para ASA 8.x
- Cliente Cisco AnyConnect VPN 2.2 con el soporte MAC

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Configuración de ASA de Cisco

Esta sección cubre la configuración de Cisco ASA vía el ASDM. Cubre los pasos necesarios para desplegar un túnel de acceso remoto VPN a través de una conexión SSL AnyConnect. El certificado CAC se utiliza para la autenticación y el atributo del nombre principal del usuario (UPN) en el certificado se puebla en el Active Directory para la autorización.

Consideraciones sobre la instrumentación

- Esta guía no cubre las configuraciones básicas tales como interfaces, DNS, NTP, encaminamiento, acceso del dispositivo, acceso del ASDM y así sucesivamente. Se asume que el operador de la red es familiar con estas configuraciones. Refiera a los [dispositivos de seguridad multifuncionales](#) para más información.
- Las secciones resaltadas en el ROJO son configuraciones obligatorias necesarias para el acceso básico VPN. Por ejemplo, un túnel VPN se puede poner con el indicador luminoso LED amarillo de la placa muestra gravedad menor CAC sin hacer los controles OCSP, las sincronizaciones LDAP y los controles de la directiva del acceso dinámico (DAP). Los mandatos el marcar OCSP del DoD pero el túnel trabajan sin OCSP configurado.
- Las secciones resaltadas en el AZUL son las funciones avanzadas que se pueden incluir para agregar más Seguridad al diseño.
- El ASDM y AnyConnect/SSL VPN no pueden utilizar los mismos puertos en la misma interfaz. Se recomienda para cambiar los puertos en uno o el otro para acceder. Por ejemplo, utilice el puerto 445 para el ASDM y deje 443 para AC/SSL VPN. El acceso del ASDM URL ha cambiado en 8.x. Utilice `https:// <ip_address>: <port>/admin.html`.
- La imagen ASA requerida es por lo menos 8.0.2.19 y el ASDM 6.0.2.
- AnyConnect/CAC se soporta con Vista.
- Vea el [Apéndice A](#) para el LDAP y los ejemplos de la asignación de la directiva del acceso dinámico para la aplicación de políticas adicional.
- Vea el [apéndice D](#) en cómo marcar los objetos LDAP en el MS.
- Vea la información relacionada para los puertos de una lista de aplicaciones para la configuración de escudo de protección.

Autenticación, autorización, configuración que considera (AAA)

Le autentican con el uso del certificado en su indicador luminoso LED amarillo de la placa muestra gravedad menor común del acceso (CAC) a través del servidor de la autoridad de DISACertificate (CA) o del servidor de CA de su propia organización. El certificado debe ser válido para el Acceso Remoto a la red. Además de la autenticación, usted debe también ser autorizado a utilizar un objeto del Microsoft Active Directory o del Lightweight Directory Access Protocol (LDAP). El Departamento de defensa (DoD) requiere el uso del atributo del nombre principal de usuario (UPN) para la autorización, que es parte de la sección alternativa sujeta del nombre (SAN) del certificado. El UPN o el EDI/PI debe estar en este formato, 1234567890@mil. Estas configuraciones muestran cómo configurar al servidor de AAA en el ASA con un servidor LDAP para la autorización. Vea el [Apéndice A](#) para la configuración adicional con el LDAP oponerse la asignación.

Configure al servidor LDAP

Complete estos pasos:

1. Elija el **VPN de acceso remoto >AAA ponen >AAA al grupo de servidores.**
2. En los Grupos de servidores AAA presente, tecleo **agregan 3.**
3. Ingrese el nombre de grupo de servidores y elija el **LDAP** en el botón Protocol Radio Button. Véase el cuadro 1.
4. En los servidores en la tabla seleccionada del grupo, haga click en Add Aseegurese que el servidor que usted creó está resaltado en la tabla anterior.
5. En la ventana del servidor de AAA del editar, complete estos pasos. Véase el cuadro 2.**Nota:** Elija el **permiso LDAP sobre la opción de SSL** si su LDAP/AD se configura para este tipo de conexión.Elija la interfaz donde se localiza el LDAP. Esta guía muestra dentro de la interfaz.Ingrese el IP Address del servidor.Ingrese el **puerto de servidor**. El puerto del valor por defecto LDAP es 389.Elija el **tipo de servidor**.Ingrese el **DN bajo**. Pida a su administrador AD/LDAP estos valores.**Figure-1**

Configure an AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.

Server Group: AD-LDAP

Protocol: LDAP

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

OK Cancel Help

Bajo opción

de alcance, elija la respuesta apropiada. Esto es dependiente en la base DN. Pida a su administrador AD/LDAP ayuda. En el atributo de nombramiento, ingrese el **userPrincipalName**. Éste es el atributo que se utiliza para la autorización de usuario en el servidor AD/LDAP. En el login DN, ingrese el DN del administrador. **Nota:** Usted tiene opinión/búsqueda de los derechos administrativos o de las derechas la estructura LDAP que incluye los objetos de usuario y la membresía del grupo. En la contraseña de inicio de sesión, ingrese la contraseña del administrador. Deje el atributo LDAP a **ningunos**. **Figure-2**

The screenshot shows the 'Add AAA Server' configuration dialog. The 'Server Group' is set to 'AD-LDAP'. The 'Interface Name' is 'outside'. The 'Server Name or IP Address' is '172.18.120.160'. The 'Timeout' is '10 seconds'. Under the 'LDAP Parameters' section, the 'Enable LDAP over SSL' checkbox is unchecked. The 'Server Port' is '389'. The 'Server Type' is '-- Detect Automatically/Use Generic Type --'. The 'Base DN' is 'CN=Users,DC=gsgseclab,DC=org'. The 'Scope' is 'One level beneath the Base DN'. The 'Naming Attribute(s)' is 'userPrincipalName'. The 'Login DN' is 'lministrator,CN=Users,DC=gsgseclab,DC=org'. The 'Login Password' is masked with dots. The 'LDAP Attribute Map' is '-- None --'. There are also checkboxes for 'SASL MD5 authentication' and 'SASL Kerberos authentication', both of which are unchecked. A 'Kerberos Server Group' field is present but empty. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Nota: Uste

d utiliza esta opción después la configuración para agregar el otro objeto AD/LDAP para la autorización. Elija **OK**.

6. Elija **OK**.

Maneje los Certificados

Hay dos pasos para instalar los Certificados en el ASA. Primero, instale los Certificados de CA (Certificate Authority de la raíz y del subordinado) necesitó. En segundo lugar, aliste el ASA a un

específico CA y obtenga el certificado de identidad. El DoD PKI utiliza estos Certificados, la raíz CA2, la raíz de la clase 3, el intermedio CA## que el ASA está alistado con, el certificado ASA ID y el certificado OCSP. Pero, si usted elige no utilizar OCSP, el certificado OCSP no necesita ser instalado.

Nota: Entre en contacto su PC de la Seguridad para obtener los certificados raíz así como las instrucciones en cómo alistar para un certificado de identidad para un dispositivo. Un certificado SSL debe ser suficiente para el ASA para el Acceso Remoto. Un certificado dual SAN no se requiere.

Nota: La máquina local también tiene que tener el encadenamiento de CA del DoD instalado. Los Certificados se pueden ver en el almacén de certificados de Microsoft con el Internet Explorer. El DoD ha presentado un archivo por lote que agrega automáticamente todos los CA a la máquina. Pida su PC PKI más información.

Nota: El DoD CA2 y la clase 3 arraigan así como el intermedio ASA ID y de CA que publicó el CERT ASA debe ser los únicos CA necesarios para la autenticación de usuario. Todos los intermedios actuales de CA caen bajo el encadenamiento de la raíz CA2 y de la clase 3 y se confían en mientras se agreguen las raíces CA2 y de la clase 3.

Genere las claves

Complete estos pasos:

1. Elija el **Certificate Management (Administración de certificados) > el certificado de identidad del VPN de acceso remoto > Add.**
2. Elija **agregar un nuevo certificado identificación** y entonces **nuevo** por la opción del par clave.
3. En la ventana de los pares de agregar clave, ingrese un nombre dominante, **DoD-1024**. Haga clic en la radio para agregar una nueva clave. Vea la figura 3. **Figura 3**

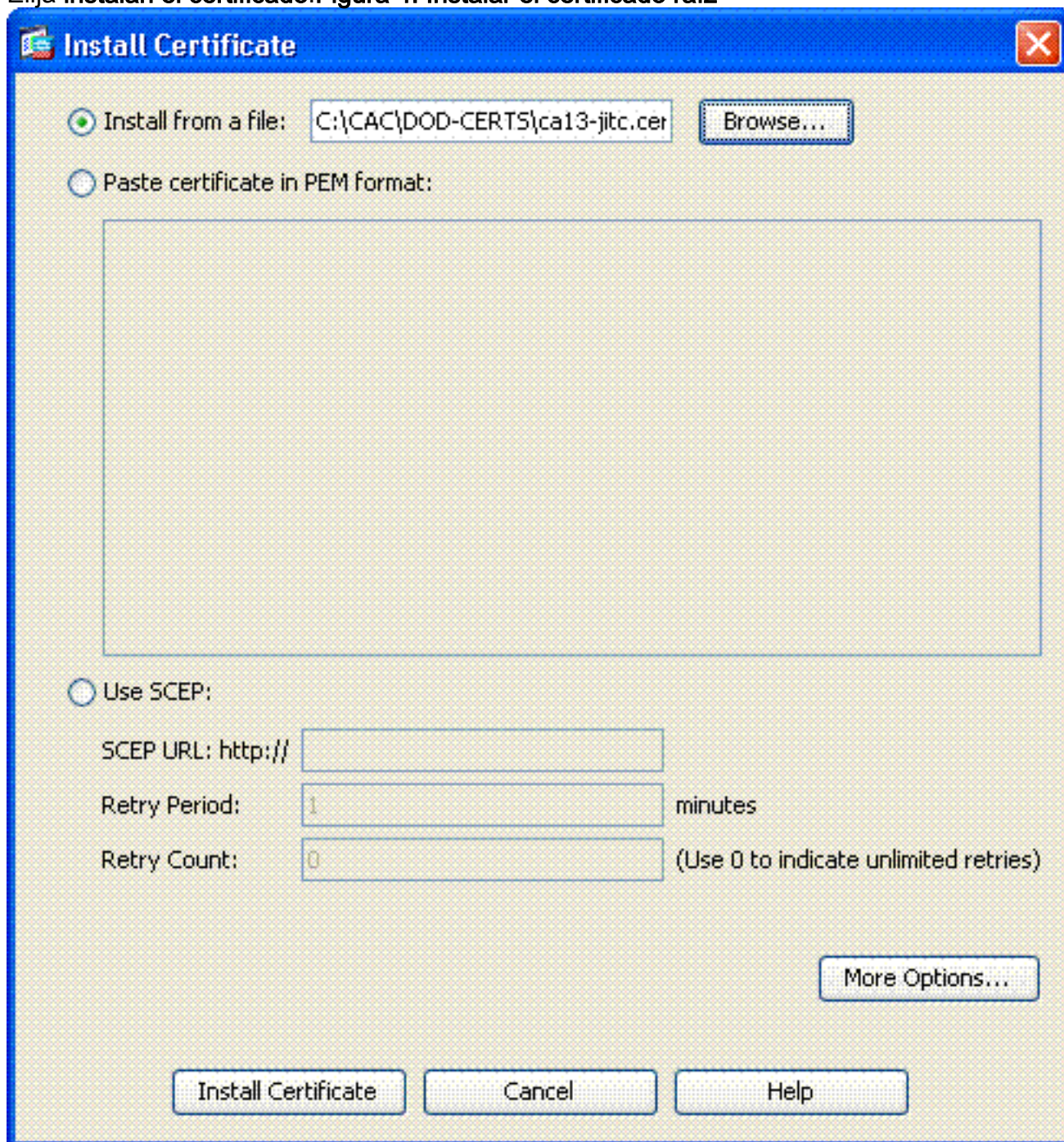


4. Elija el tamaño de la clave.
5. Guarde el uso a los **finos generales**.
6. El tecleo **ahora genera**. **Nota:** El DoD raíz CA 2 utiliza una clave de 2048 bits. Una segunda clave que utiliza un par clave de 2048 bits se debe generar para poder utilizar este CA completa el anterior sobre los pasos para agregar una segunda clave.

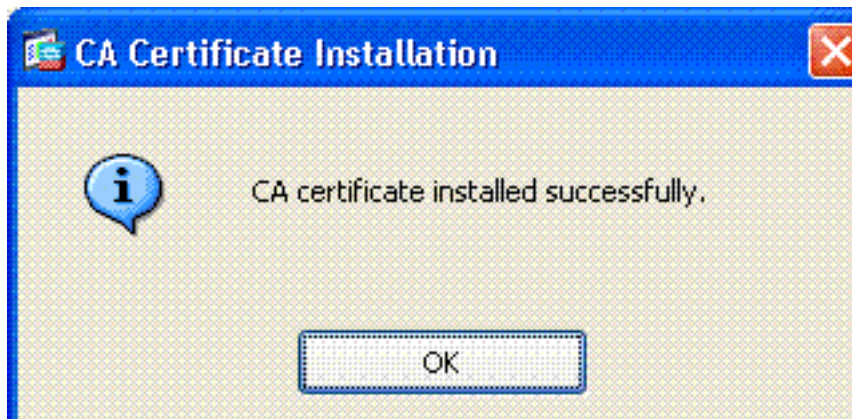
Instale raíz CA los Certificados

Complete estos pasos:

1. Elija el **Certificate Management (Administración de certificados)** > el certificado de CA del **VPN de acceso remoto** > **Add**.
2. Elija **instalar del archivo** y hojear al certificado.
3. Elija **instalar el certificado**. **Figura 4: Instalar el certificado raíz**

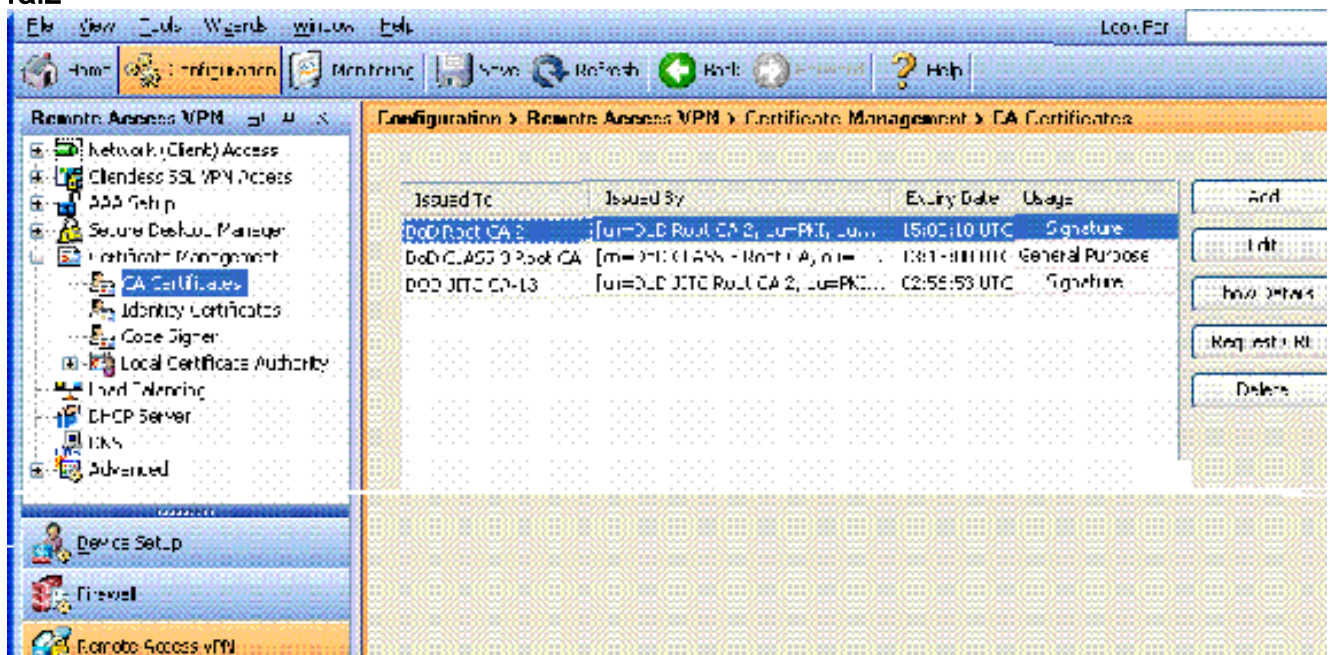


4. Esta ventana debe aparecer. Véase el cuadro 5. **Figura 5**



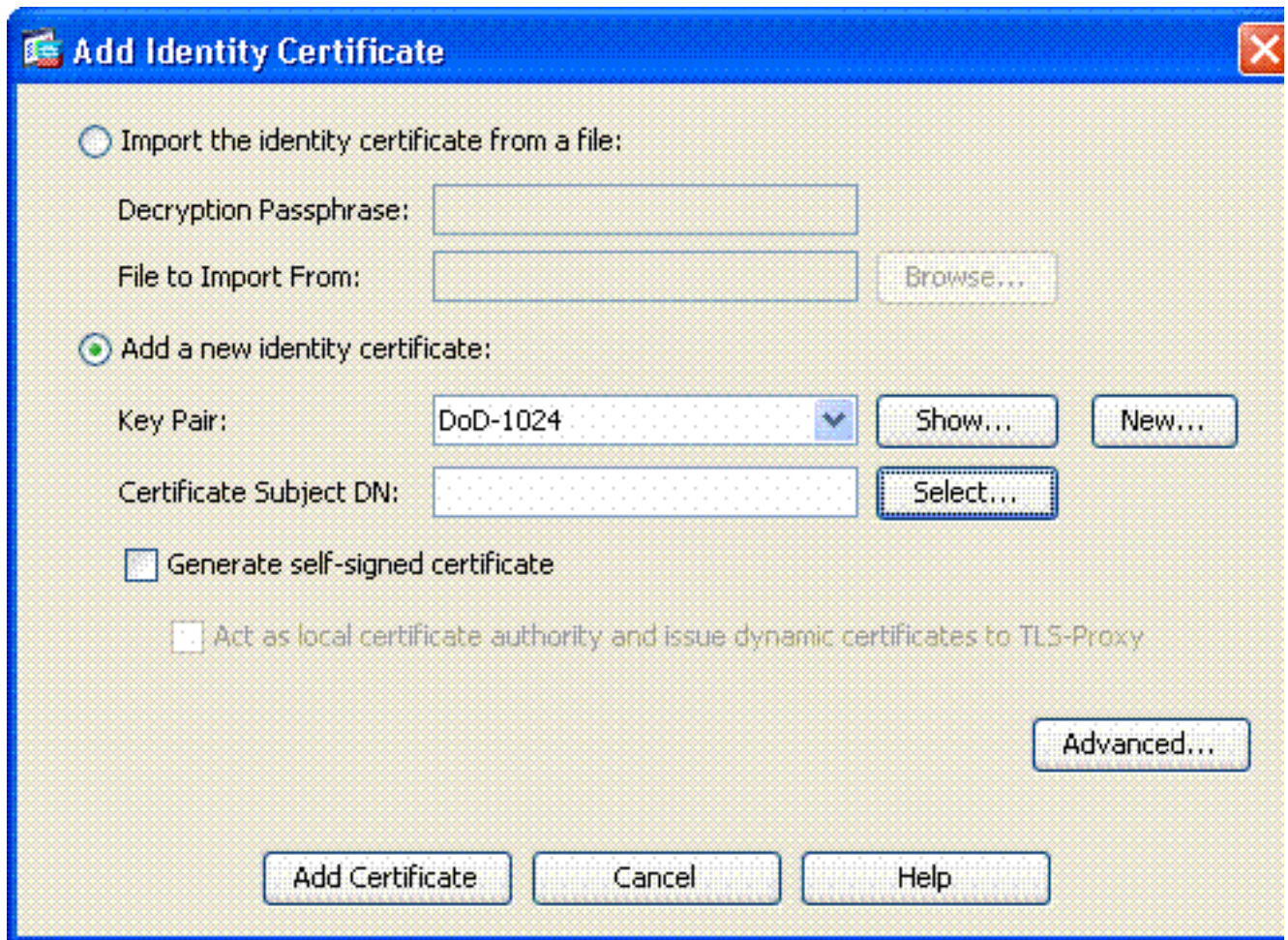
Nota: Relance los pasos 1 a 3 para cada certificado que usted quiera instalar. El DoD PKI requiere un certificado para cada uno de éstos: Raíz CA 2, raíz de la clase 3, intermedio CA##, servidor ASA ID y OCSP. El certificado OCSP no es necesario si usted no utiliza OCSP.

Figura 6: Instalar el certificado raíz



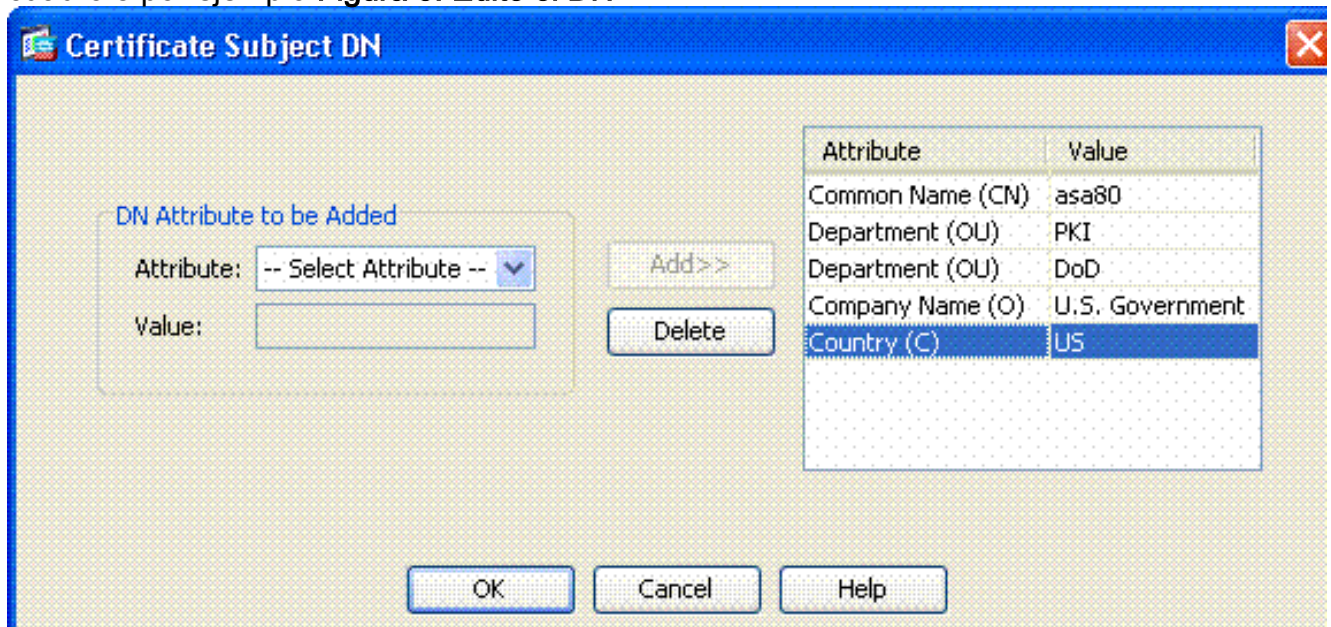
[Aliste el ASA y instale el certificado de identidad](#)

1. Elija el Certificate Management (Administración de certificados) > el certificado de identidad del VPN de acceso remoto > Add.
 2. Elija agregar un nuevo certificado identificación.
 3. Elija el par clave del DoD-1024. Véase el cuadro 7
- Figura 7: Parámetros del certificado de identidad**



4. Vaya al cuadro del tema DN del certificado y haga clic **selecto**.

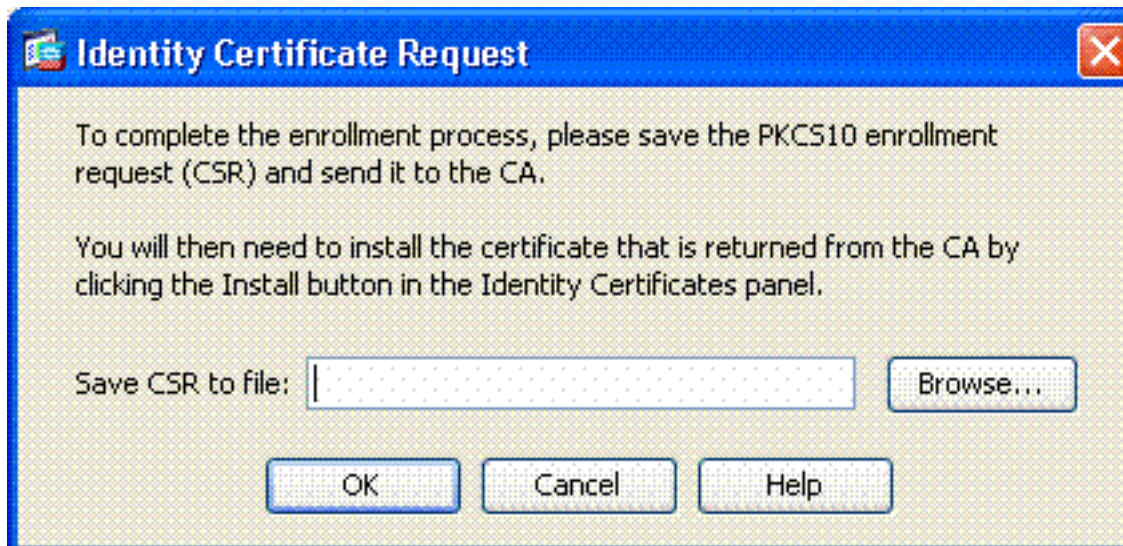
5. En la ventana del tema DN del certificado, ingrese la información del dispositivo. Véase el cuadro 8 por ejemplo. **Figura 8: Edite el DN**



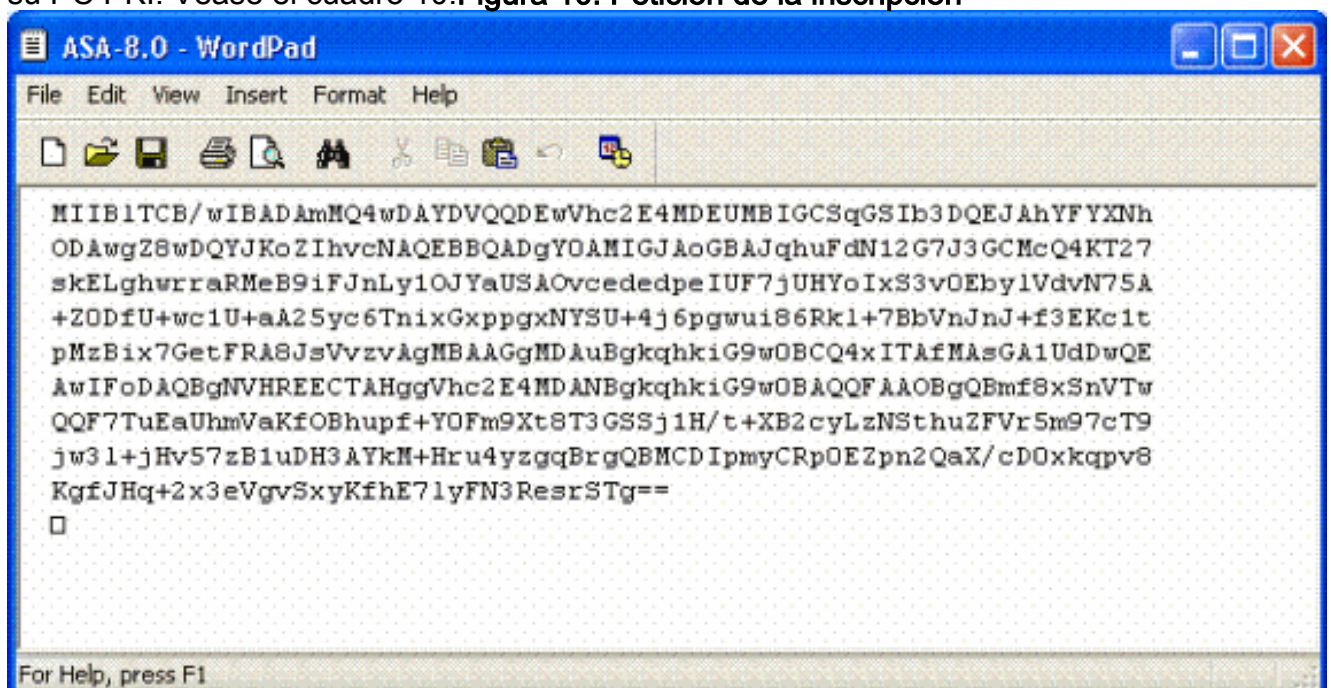
6. Elija **OK**. **Nota:** Asegurese que usted utiliza el nombre de host del dispositivo que se configura en su sistema cuando usted agrega el tema DN. El PC PKI puede decirle los campos obligatorios requeridos.

7. Elija **agregan el certificado**.

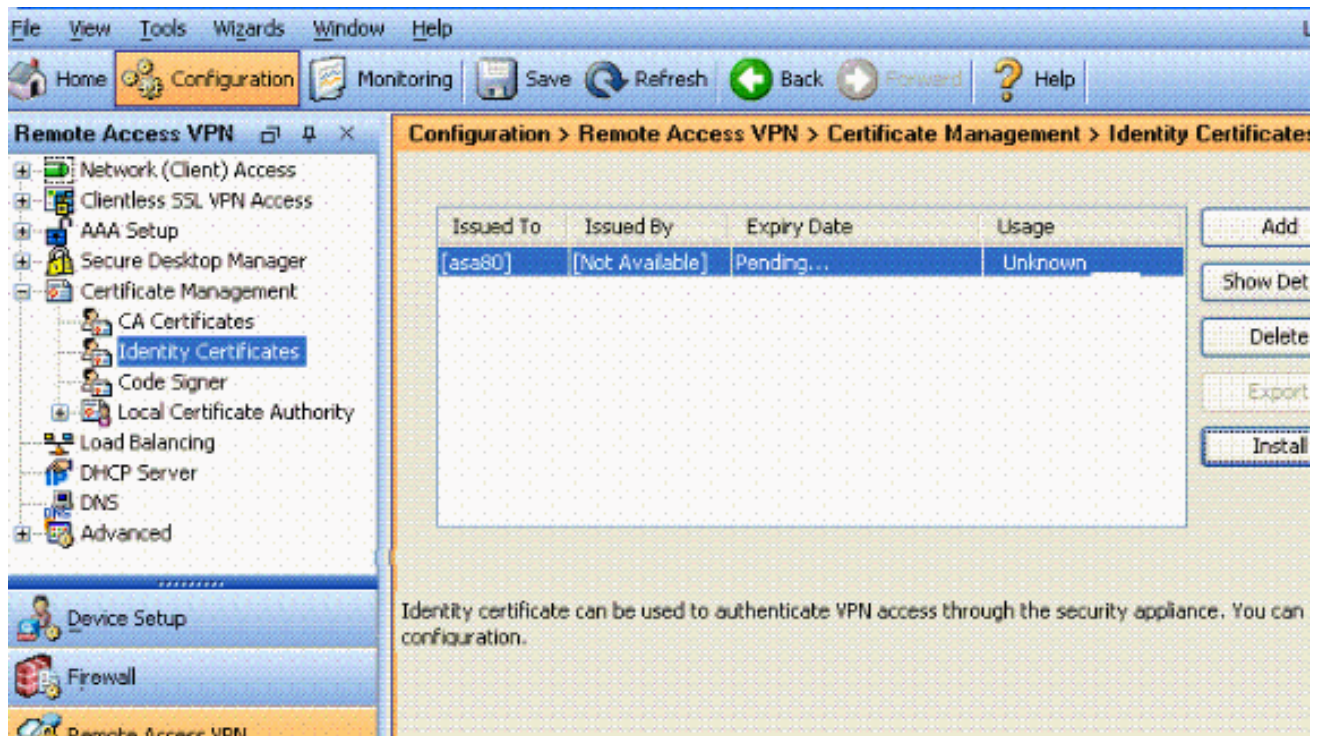
8. El teclado **hojea** para seleccionar el directorio donde usted quiere salvar la petición. Véase el cuadro 9. **Cuadro 9 pedido de certificado**



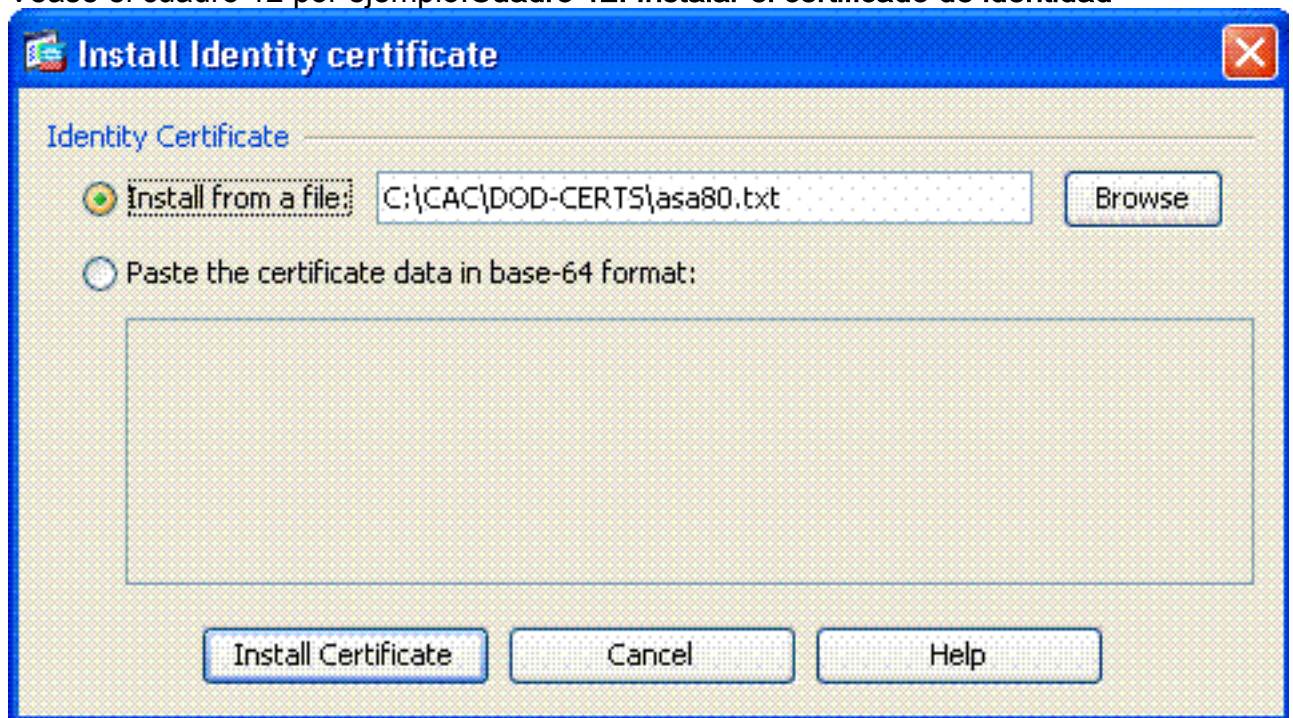
9. Abra el archivo con el WordPad, copie la petición a la documentación apropiada y envíela a su PC PKI. Véase el cuadro 10. **Figura 10: Petición de la inscripción**



10. Una vez que usted ha recibido el certificado del administrador de CA, elija el **Certificate Management (Administración de certificados)** del VPN de acceso remoto > el certificado ID > instalan. Véase el cuadro 11. **Cuadro 11: Importación del certificado de identidad**



11. En la ventana del certificado del instalar, hojee al **certificado CERT** y del chooseInstall ID. Véase el cuadro 12 por ejemplo. **Cuadro 12: Instalar el certificado de identidad**



Nota: Se recomienda para exportar el trustpoint del certificado ID en el orderw para salvar el certificado y los pares claves publicados. Esto permite que el administrador ASA importe el certificado y los pares claves a un nuevo ASA en caso del RMA o de la falla de hardware. Refiera a [exportar y a importar el trustpoints](#) para más información. **Nota:** **SALVAGUARDIA** del teclado para salvar la configuración en memoria flash.

[Configuración VPN de AnyConnect](#)

Hay dos opciones para configurar los parámetros VPN en el ASDM. La primera opción es utilizar al Asistente VPN SSL. Esto es una herramienta fácil a utilizar para los usuarios que son nuevos a

la configuración VPN. La segunda opción es hacerlo manualmente y pasar con cada opción. Esta guía de configuración utiliza el método manual.

Nota: Hay dos métodos para conseguir al cliente AC al usuario:

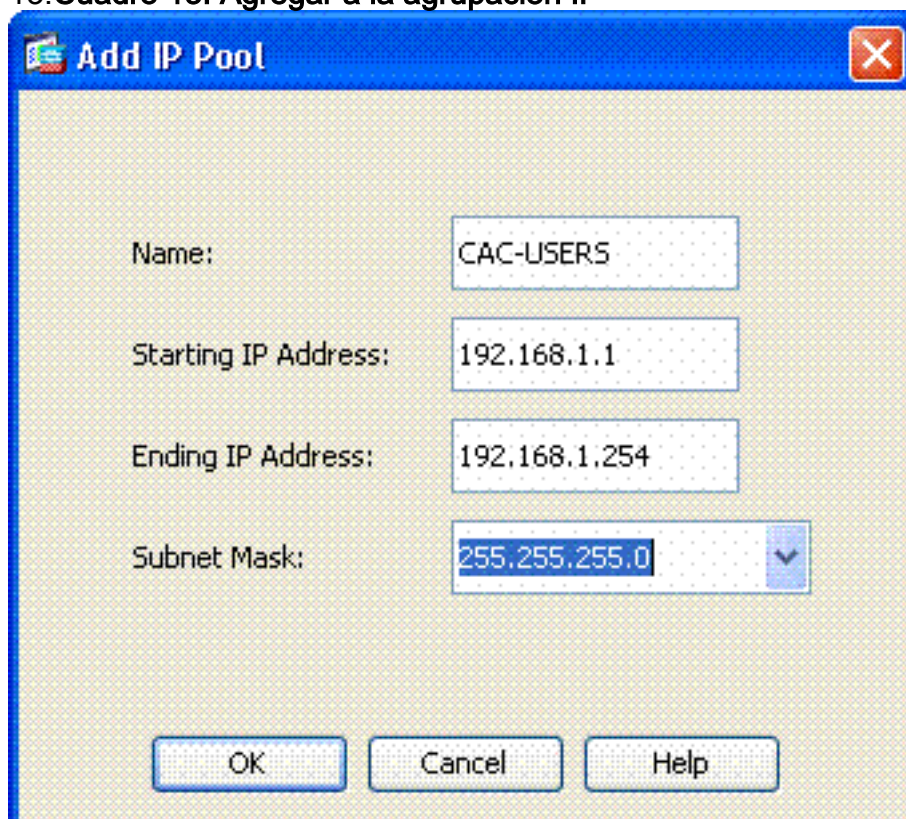
1. Usted puede descargar al cliente del sitio Web de Cisco y instalarlo en su máquina.
2. El usuario puede acceder el ASA vía un buscador Web y el cliente puede ser descargado.

Nota: Por ejemplo, <https://asa.test.com>. Esta guía utiliza el segundo método. Una vez que el cliente AC está instalado en la máquina del cliente permanentemente, usted apenas inicia al cliente AC de la aplicación.

[Cree un pool de la dirección IP](#)

Esto es opcional si usted utiliza otro método tal como DHCP.

1. Elija el **VPN de acceso remoto > el acceso > la asignación de dirección > a las agrupaciones de direcciones de la red (cliente)**.
2. Haga clic en Add (Agregar).
3. En la ventana de la agrupación IP del agregar, ingrese el nombre de la agrupación IP, comenzando y terminando el IP Address y elija a una máscara de subred. Ver Figura 13. **Cuadro 13: Agregar a la agrupación IP**

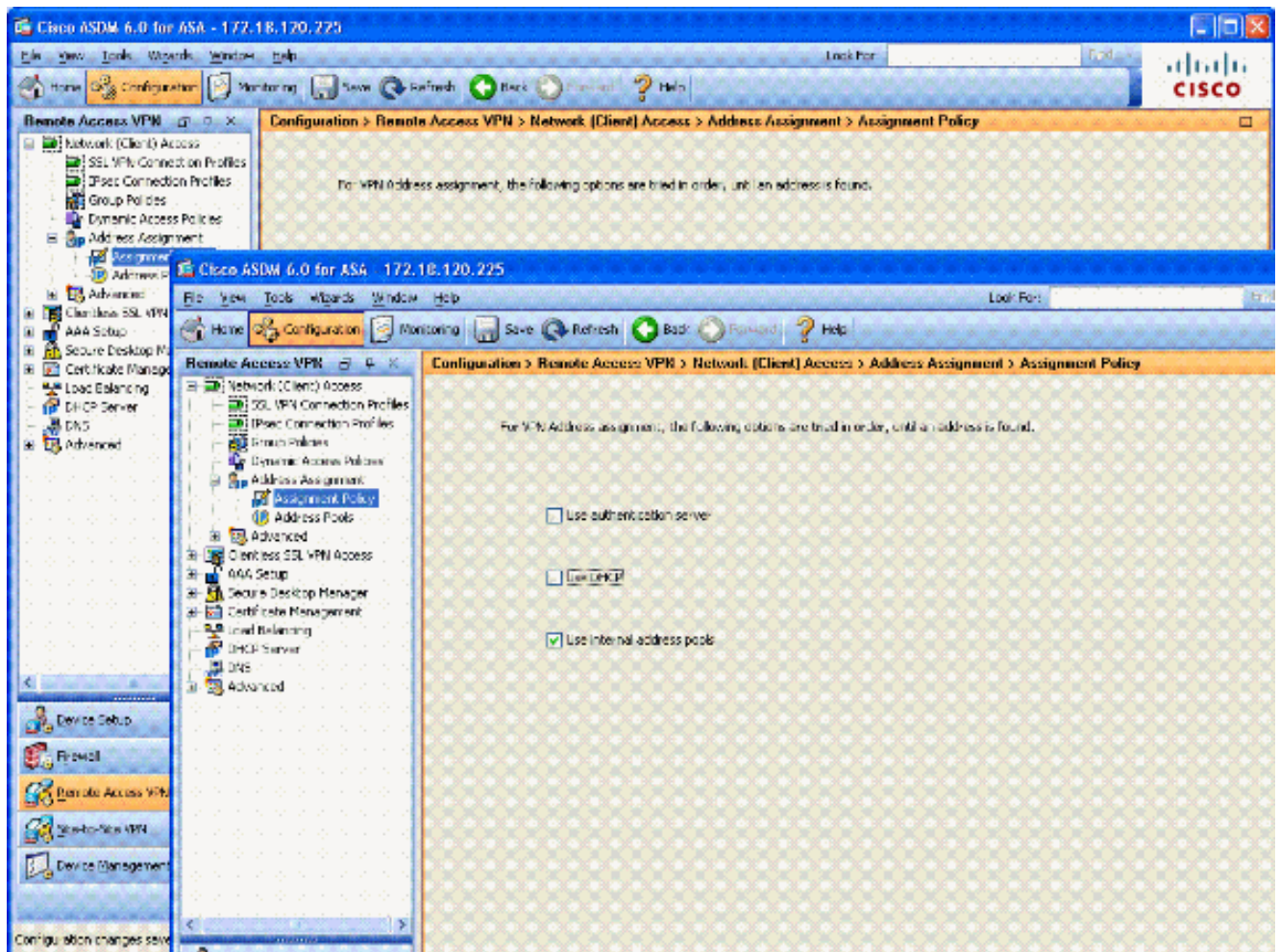


The screenshot shows a dialog box titled "Add IP Pool". It contains the following fields and values:

Name:	CAC-USERS
Starting IP Address:	192.168.1.1
Ending IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

4. Elija OK.
5. Elija la **directiva del VPN de acceso remoto > del acceso > de la asignación de dirección > de la asignación de la red (cliente)**.
6. Seleccione el método de asignación apropiado de la dirección IP. Esta guía utiliza a los pools de la dirección interna. Véase el cuadro 14. **Figura 14: Método de asignación de la dirección IP**



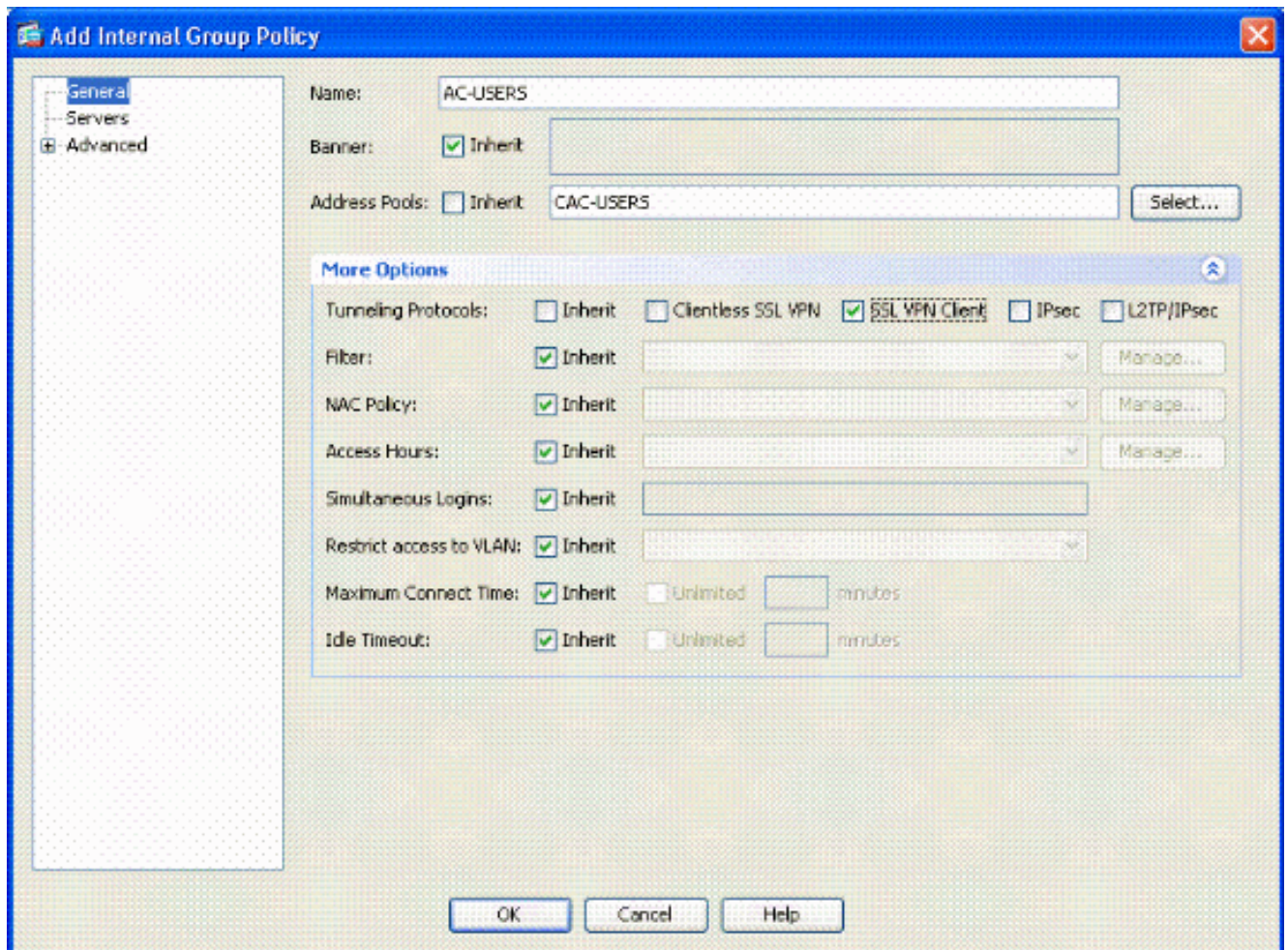
7. Haga clic en Apply (Aplicar).

[Cree la directiva del grupo de túnel y del grupo](#)

Agrupe la directiva

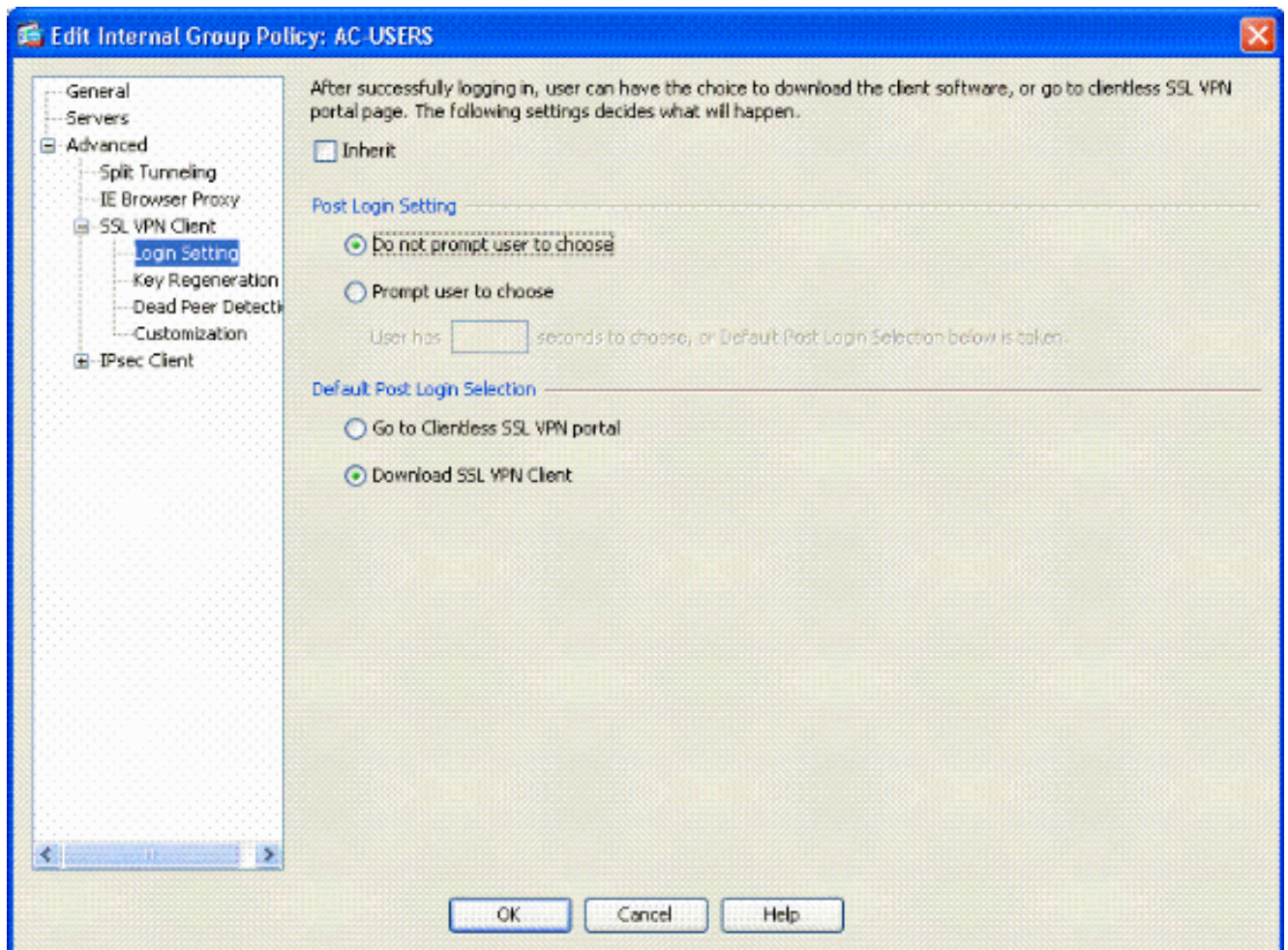
Nota: Si usted no quiere crear una nueva directiva, usted puede utilizar la directiva construida predeterminada del en-grupo.

1. Elija el VPN de acceso remoto -> acceso de la red (cliente) -> las directivas del grupo.
2. El teclado agrega y elige el Internal group policy (política grupal interna).
3. En la ventana del Internal group policy (política grupal interna) del agregar, ingrese el nombre para la directiva del grupo en el cuadro de texto del nombre. Véase el cuadro 15. **Figura 15: Agregar el Internal group policy (política grupal interna)**



En la ficha general, elija al **cliente VPN SSL** en la opción de los **protocolos de túneles**, a menos que usted utilice otros protocolos tales como clientless SSL. En los servidores seccione, desmarque la casilla de verificación de la **herencia** e ingrese el IP Address del DNS y GANA los servidores. Ingrese el alcance de DHCP si procede. En los servidores seccione, no reelija como candidato la casilla de verificación de la **herencia** en el Default Domain y ingrese el Domain Name apropiado. En la ficha general, no reelija como candidato la casilla de verificación de la **herencia** en la sección de la agrupación de direcciones y agregue a la agrupación de direcciones creada en el paso anterior. Si el you use otro método de asignación de la dirección IP, sale de esto para heredar y para realizar el cambio apropiado. El resto de las fichas de configuración se dejan a las configuraciones predeterminadas. **Nota:** Hay dos métodos para conseguir al cliente AC a los usuarios finales. Un método es ir al cisco.com y descargar al cliente AC. El segundo método es tener la descarga ASA el cliente al usuario cuando el usuario intenta conectar. Este ejemplo muestra el último método.

4. Después, elija **avanzado > las configuraciones del cliente VPN > del login SSL**. Véase el cuadro 16. **Figura 16: Agregar el Internal group policy (política grupal interna)**

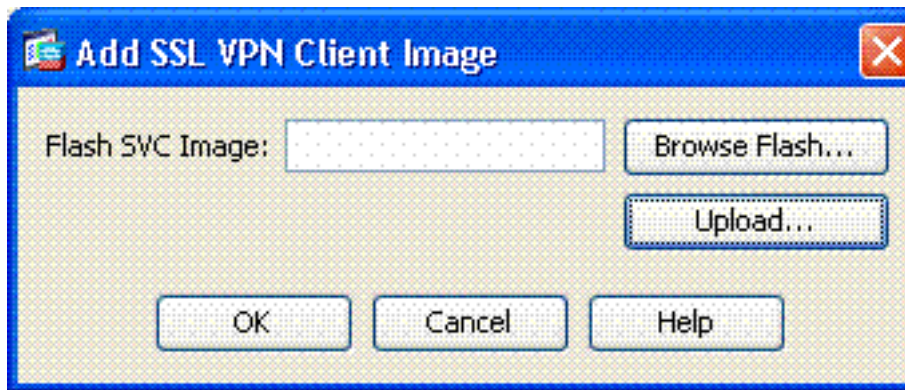


No reeija como candidato el checkbox de la **herencia**.Elija la configuración apropiada del login del poste que cabe su entorno.Elija la selección predeterminada apropiada del login del poste que cabe su entorno.Elija **OK**.

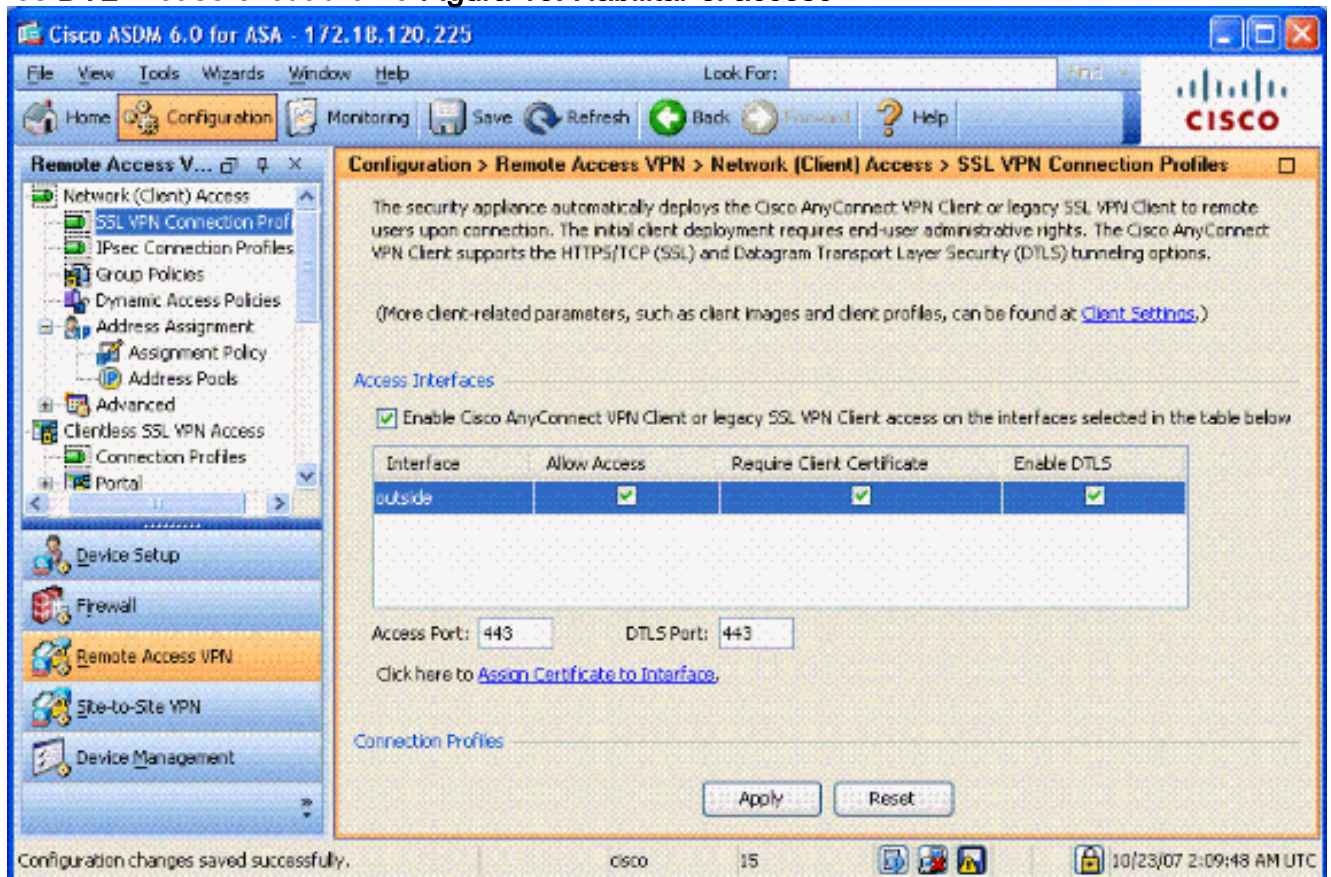
[Interfaz y configuraciones de imagen del grupo de túnel](#)

Nota: Si usted no quiere crear a un nuevo grupo, usted puede utilizar al grupo incorporado predeterminado.

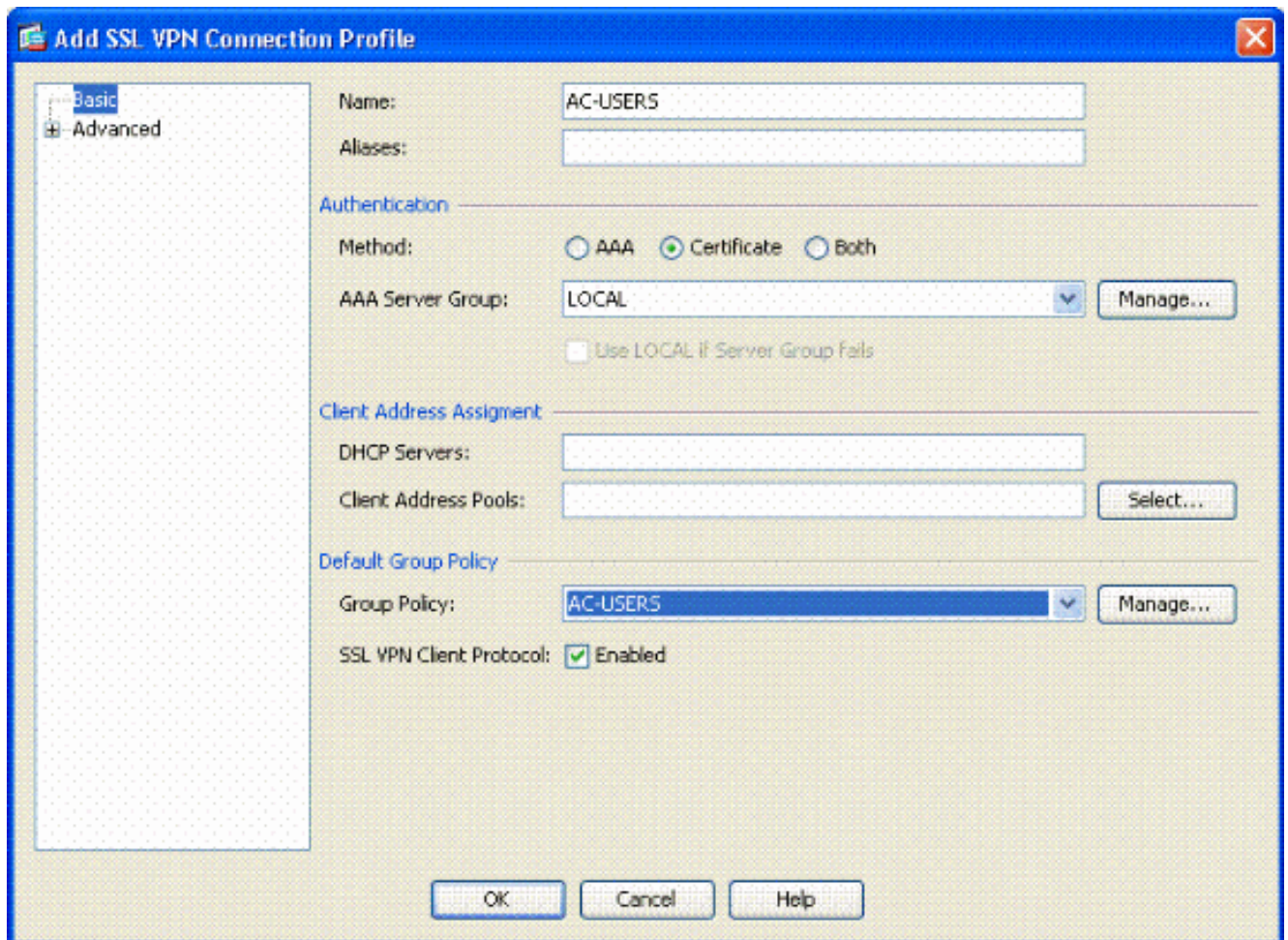
1. Elija el **acceso del VPN de acceso remoto > de la red (cliente) > perfil de la conexión VPN SSL**.
2. Elija al **cliente de Cisco AnyConnect del permiso**
3. ¿Un cuadro de diálogo aparece con la pregunta *usted quisiera señalar una imagen de SVC?*
4. Elija **sí**.
5. Si hay ya una imagen, elija la imagen para utilizar con hojean el Flash. Si la imagen no está disponible, elija la **carga** y hojee para el archivo en la computadora local. Véase el cuadro 17. Los archivos se pueden descargar del cisco.com; hay Windows, un MAC y un archivo de Linux.**Figura 17: Agregue la imagen del cliente VPN SSL**



6. El permiso siguiente **permite el acceso, requiere el CERT del cliente y habilita opcionalmente los DTL**. Véase el cuadro 18.**Figura 18: Habilitar el acceso**

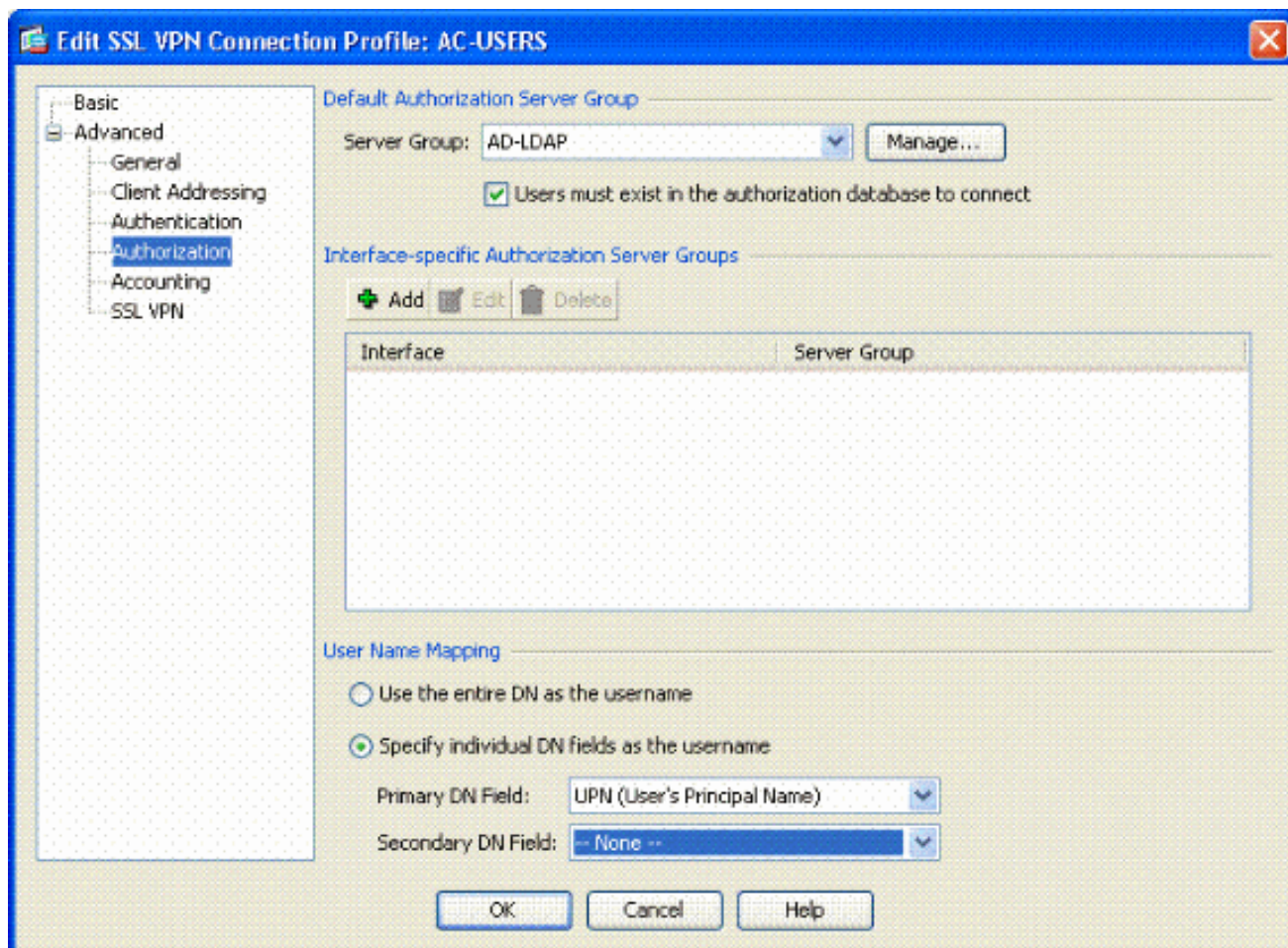


7. Haga clic en Apply (Aplicar).
8. Después, cree un perfil de la conexión/a un grupo de túnel. Elija el **acceso del VPN de acceso remoto > de la red (cliente) > perfil de la conexión VPN SSL**.
9. En la sección de los perfiles de la conexión, haga clic en **Add** **Figura 19: Agregar el perfil de la conexión**



Nombre al grupo. Elija el **certificado** en el método de autenticación. Elija la directiva del grupo creada previamente. Asegúrese de que habiliten al **cliente VPN SSL**. Deje las otras opciones como valor por defecto.

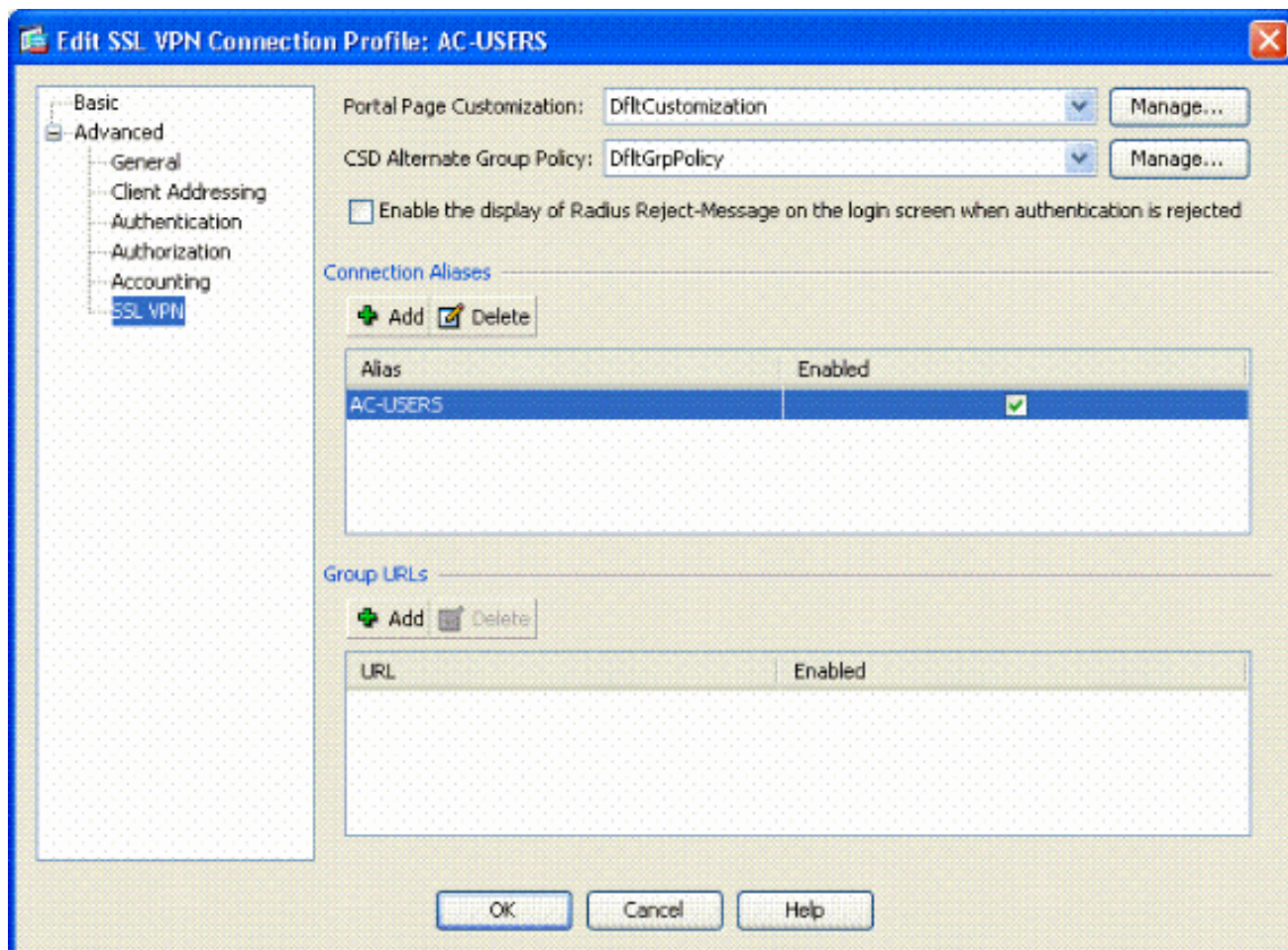
10. Después, choose **Advanced > autorización**. Véase el cuadro 20 **Figura 20: Autorización**



Elija al grupo AD-LDAP creado previamente. **Los usuarios del control deben existir... para conectar.** En los campos de la asignación, no elija el UPN para el primario y ninguno para secundario.

11. Elija la sección **SSL VPN** del menú.

12. En la sección de alias de la conexión, complete estos pasos: **Cuadro 21: Alias de la conexión**



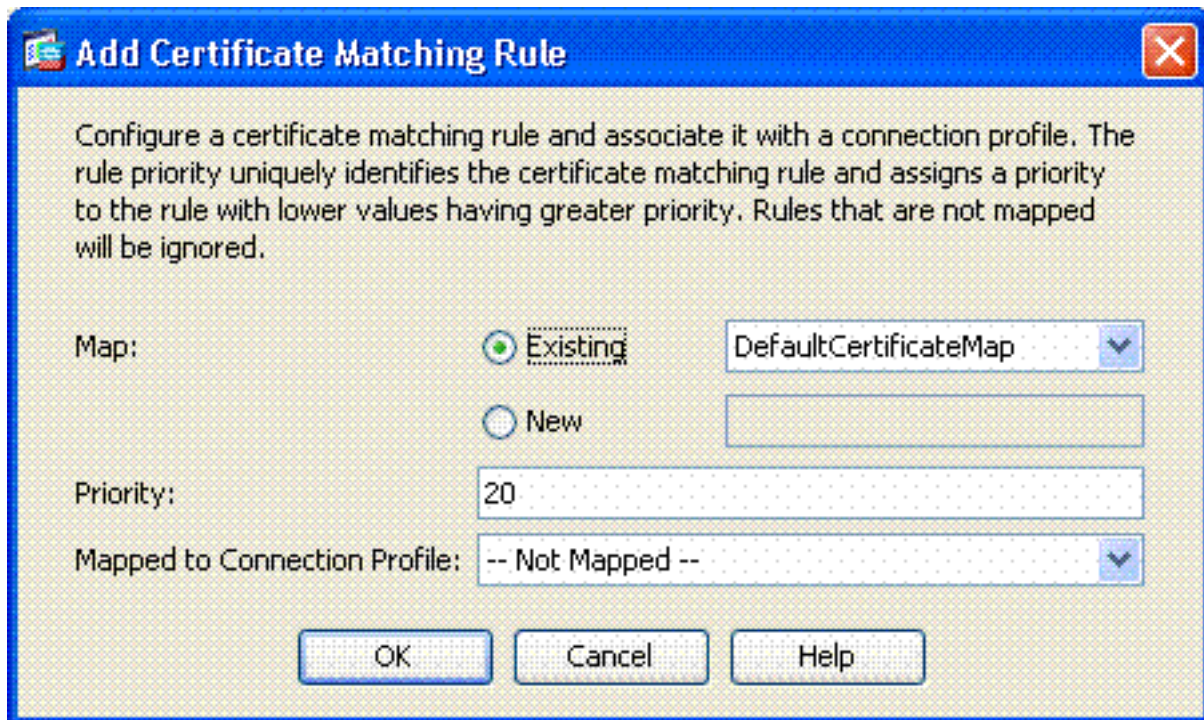
Elija **agregar**. Ingrese al grupo alias que usted quiere utilizar. Asegúrese que **habilitó** se marca. Consulte la [Figura 21](#).

13. Haga clic en OK.

Nota: Salvaguardia del teclado para salvar la configuración en memoria flash.

[Reglas que corresponden con del certificado \(si OCSP es utilizado\)](#)

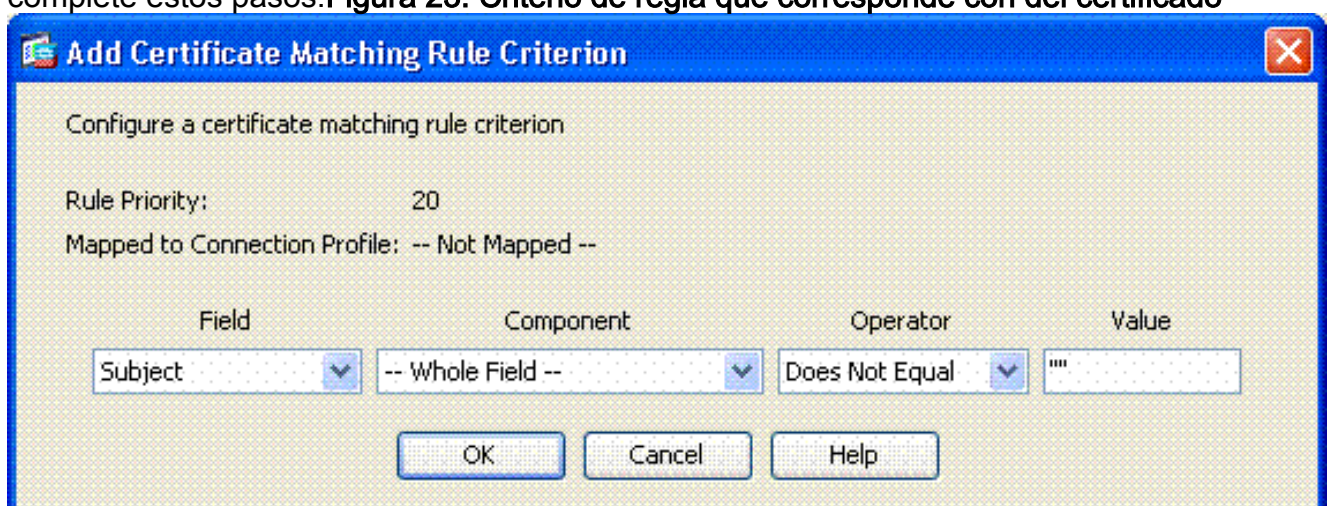
1. Elija el VPN de acceso remoto > avanzó > certificado a las correspondencias del perfil de la conexión VPN SSL. Véase el cuadro 22. Elija **agregar** en el certificado a la sección de las correspondencias del perfil de la conexión. Usted puede mantener la correspondencia existente como DefaultCertificateMap la sección de la correspondencia o crear un nuevo si usted utiliza ya las correspondencias CERT para el IPSec. Guarde la prioridad de la regla. Bajo grupo asociado, váyase como -- **No asociado** --. Véase el cuadro 22. **Cuadro 22:** Agregar la regla que corresponde con del certificado



Haga

clic en OK.

2. El tecleo **agrega** en la tabla inferior.
3. En del agregar que corresponde con de la ventana del certificado el criterio de regla, complete estos pasos:**Figura 23: Criterio de regla que corresponde con del certificado**



Guarde la columna del campo **para sujetar**.Guarde la columna componente al **campo entero**.Cambie al operador que la columna **no iguala**.En la columna de valor, ingrese dos comillas dobles """.Haga clic la **autorización** y **aplique**se. Véase el cuadro 23 por ejemplo.

[Configure OCSP](#)

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

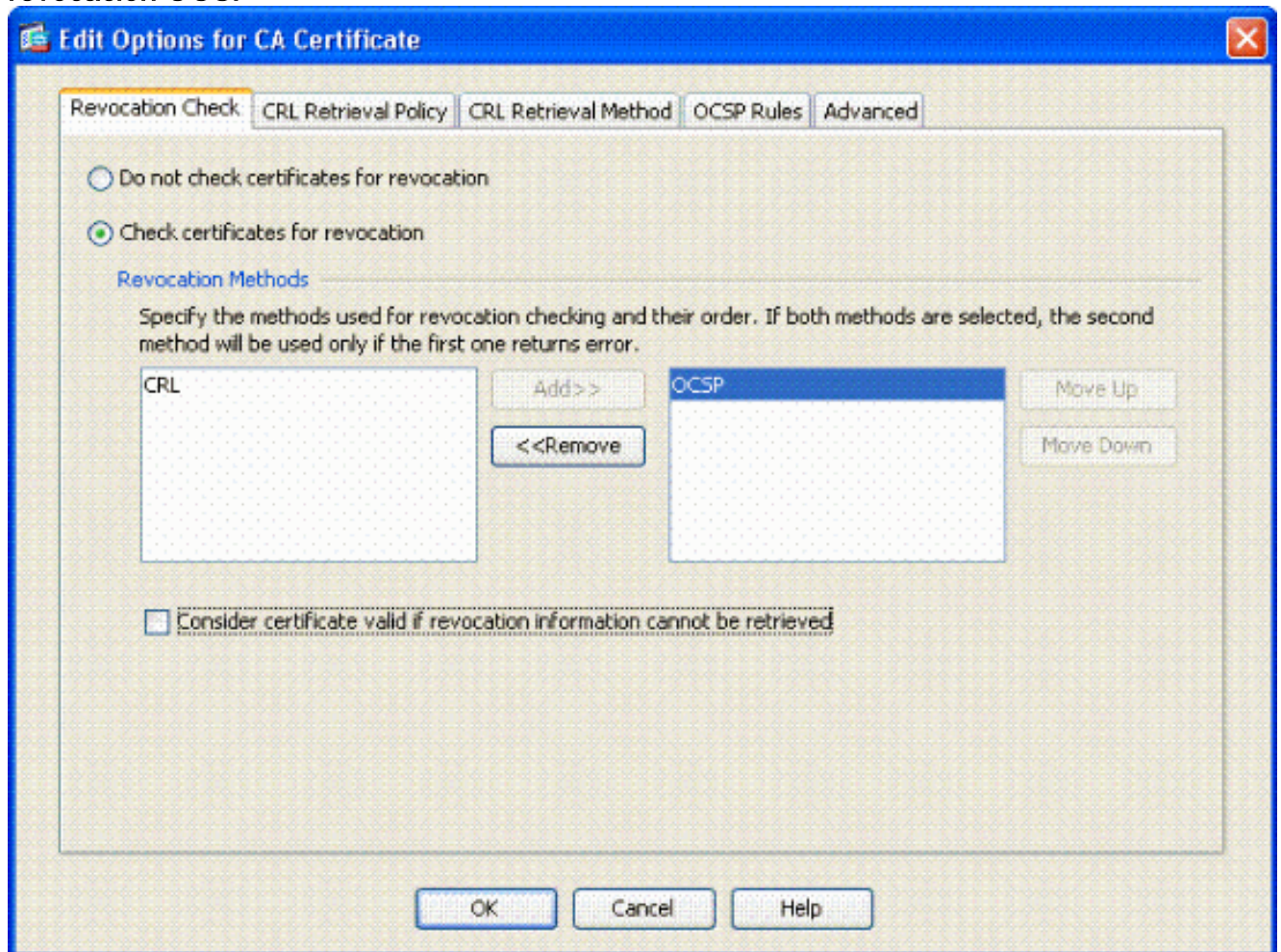
[Configure el certificado del respondedor OCSP](#)

1. Obtenga un certificado uno mismo-generado del respondedor OCSP.
2. Complete los procedimientos mencionados previamente y instale un certificado para el servidor OSCP.**Nota:** Asegurese que **no marque los Certificados para la revocación** está

seleccionado para el trustpoint del certificado OCSP.

Configure CA para utilizar OCSP

1. Elija la **administración de certificados del Acceso Remoto VPN** > > los **Certificados de CA**.
2. Resalte un OCSP para elegir CA para configurar para utilizar OCSP.
3. Haga clic en **Editar**.
4. Asegúrese de que el **certificado del control para la revocación** esté marcado.
5. En los métodos de la revocación seccione, agregue **OCSP**. Véase el cuadro 24. **Control de la revocación OCSP**



6. Asegure **consideran el certificado válido... no puede ser extraído** se desmarca si usted quiere seguir marcar estricto OCSP.

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

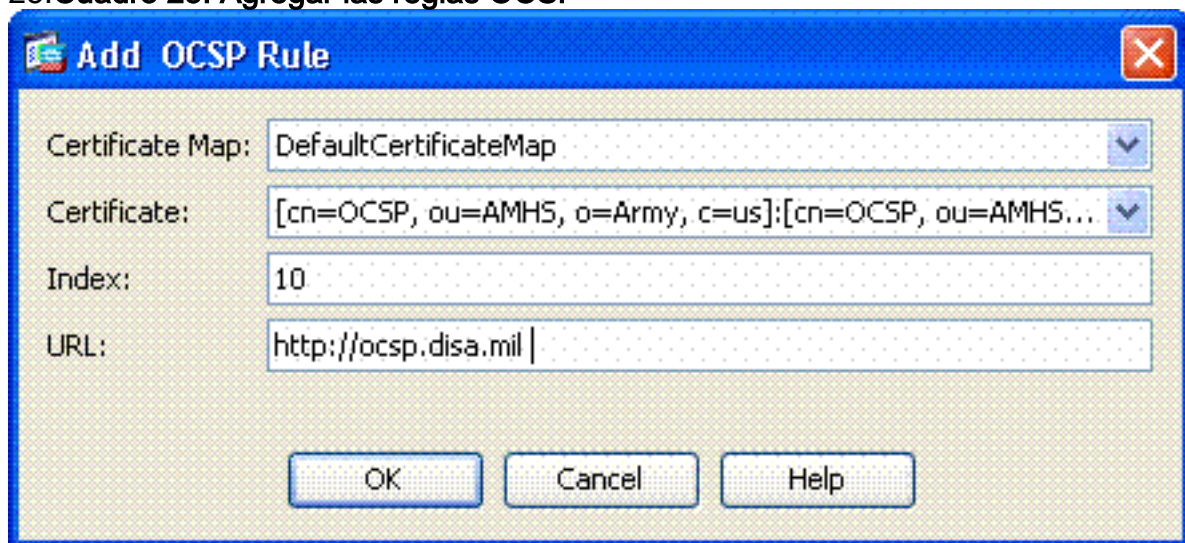
Configure las reglas OCSP

Nota: Verifique que una directiva que corresponde con del grupo del certificado esté creada y configuran al respondedor OCSP antes de que usted complete estos pasos.

Nota: En las implementaciones algún OCSP, un expediente DNS A y PTR puede ser necesario para el ASA. Este control se hace para verificar que el ASA es de un sitio .mil.

1. Elija la **administración de certificados** > los **Certificados de CA 2. del Acceso Remoto VPN**.
2. Resalte un OCSP para elegir CA para configurar para utilizar OCSP.
3. Elija **editan**.

4. Haga clic la lengüeta de la **regla OCSP**.
5. Haga clic en Add (Agregar).
6. En la ventana de la regla del agregar OCSP, complete estos pasos. Véase el cuadro 25. **Cuadro 25: Agregar las reglas OCSP**



En la opción del mapa del certificado, elija **DefaultCertificateMap** o una correspondencia creada previamente. En la opción del certificado, elija al **respondedor OCSP**. En la opción de índice, ingrese **10**. En la opción URL, ingrese el IP Address o el nombre de host del respondedor OCSP. Si usted utiliza el nombre de host, asegúrese al servidor DNS se configura en el ASA. Haga clic la **autorización**. Haga clic en Apply (Aplicar).

[Configuración del cliente de Cisco AnyConnect](#)

Esta sección cubre la configuración del Cliente Cisco AnyConnect VPN.

Suposiciones — La aplicación del Cliente Cisco AnyConnect VPN y del software intermediario está instalada ya en el host PC. El oro y ActivClient de ActivCard fueron probados.

Nota: Esta guía utiliza el método grupo-URL para el cliente inicial AC instala solamente. Una vez que el cliente AC está instalado, usted pone en marcha la aplicación AC apenas como el cliente IPsec.

Nota: La Cadena de certificados del DoD necesita ser instalada en la máquina local. Marque con el PC PKI para obtener los Certificados/archivo por lote.

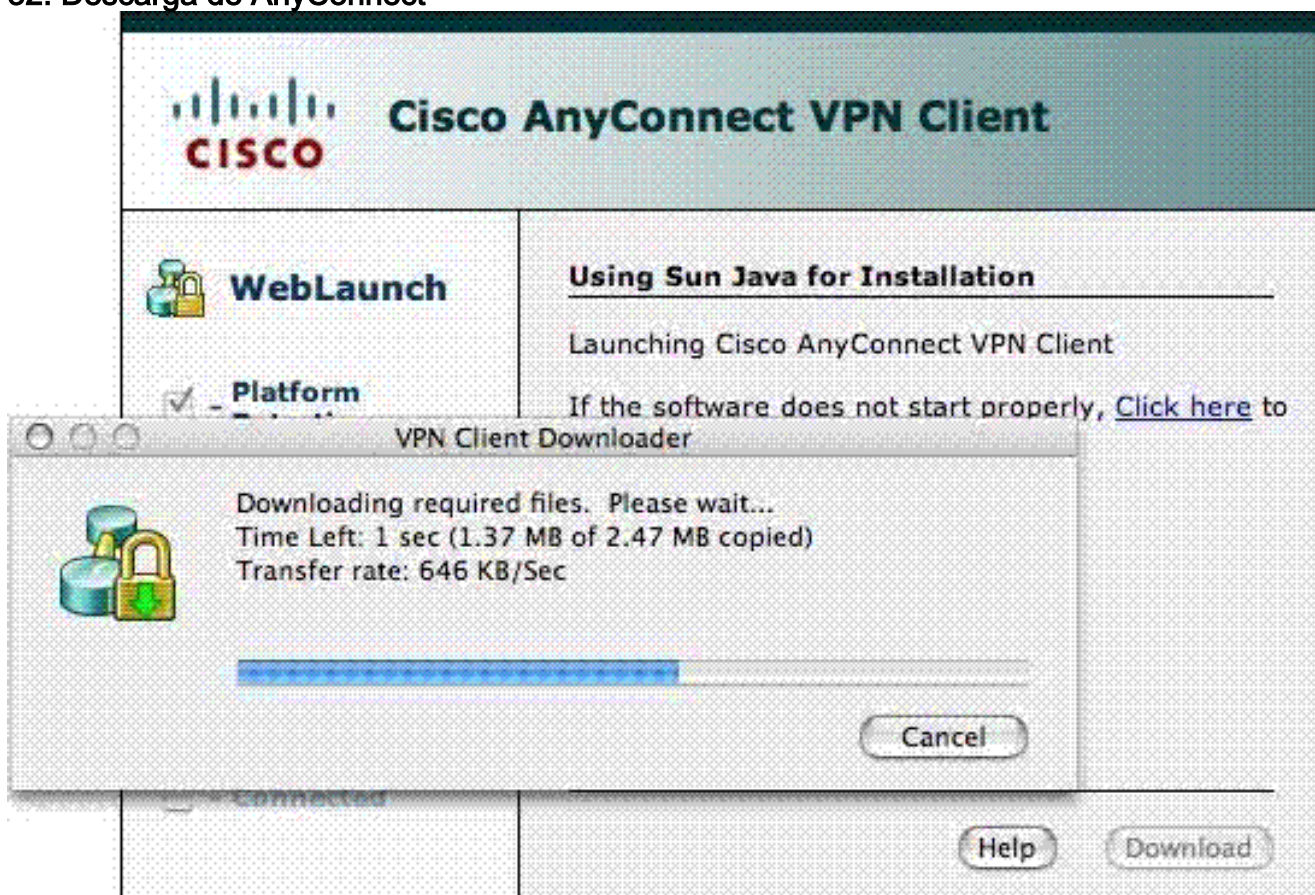
Nota: El driver del lector de tarjetas para el MAC OSX es instalado ya y compatible con la versión de OS actual que usted utiliza.

[Descargando al Cliente Cisco AnyConnect VPN – Mac OS X](#)

1. Ponga en marcha a una sesión web al ASA con el safari. El direccionamiento debe estar en el formato de https://Outside-Interface. Por ejemplo, https://172.18.120.225.
2. Una ventana emergente pide verificar el certificado del ASA. Haga clic en **Continue** (Continuar).
3. Otra ventana emergente aparece para desbloquear el llavero CAC. Ingrese su número de pin. Véase el cuadro 31. **Cuadro 31: Ingrese el PIN**



4. Después de que aparezca la página web del VPN-servicio SSL, el tecleo **continúa**.
5. Después de que usted desbloquee el llavero, el navegador le indica si usted confía en el certificado del ASA. **Confianza del tecleo**.
6. Ingrese la contraseña de raíz para abrir el keychain para establecer la conexión segura, y después haga clic la **autorización**.
7. Elija el certificado para utilizar para la autenticación de cliente, y después haga clic la **autorización**.
8. El navegador entonces pide la raíz/la contraseña del usuario para tener en cuenta descargar de los clientes de AnyConnect.
9. Si está autenticado, el cliente de AnyConnect comienza a descargar. Vea la [figura 32](#). **Figura 32: Descarga de AnyConnect**



10. Después de que se descargue la aplicación, el navegador le indica a que valide el certificado ASA. El tecleo **valida**.
11. Se establece la conexión. **Cuadro 33.Figura 33:AnyConnect conectada**



[Cliente Cisco AnyConnect VPN del comienzo – Mac OS X](#)

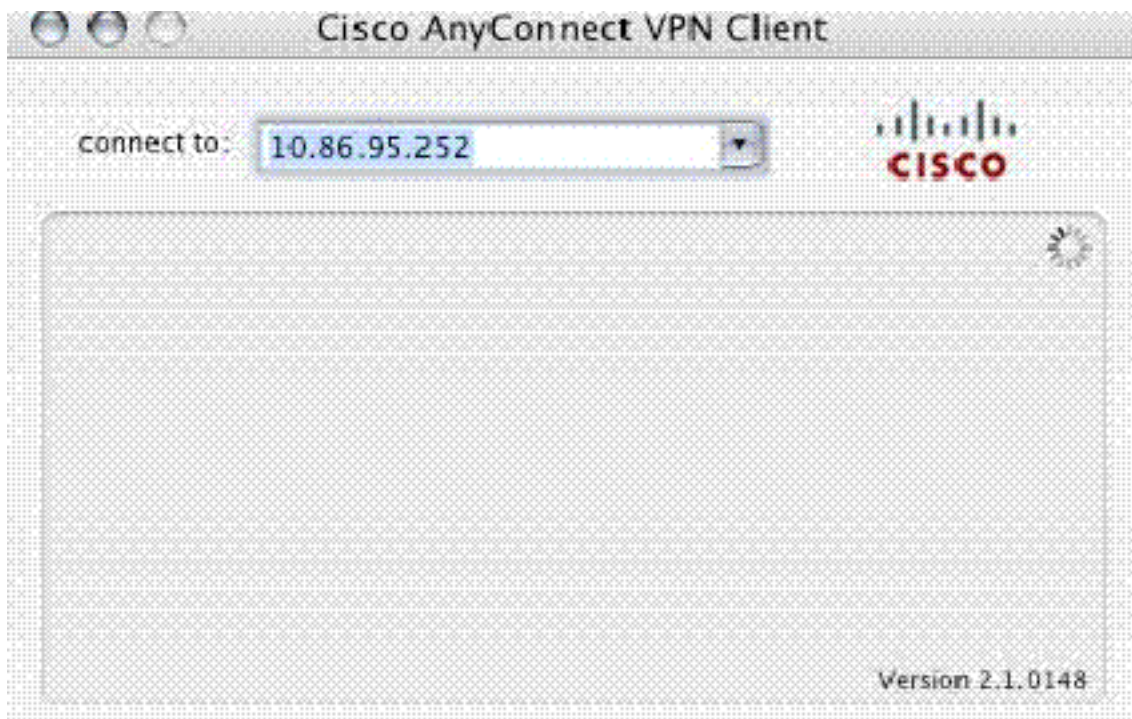
Del buscador — **Aplicaciones > Cliente Cisco AnyConnect VPN**

Nota: Vea el apéndice E para la configuración del perfil opcional del cliente de AnyConnect.

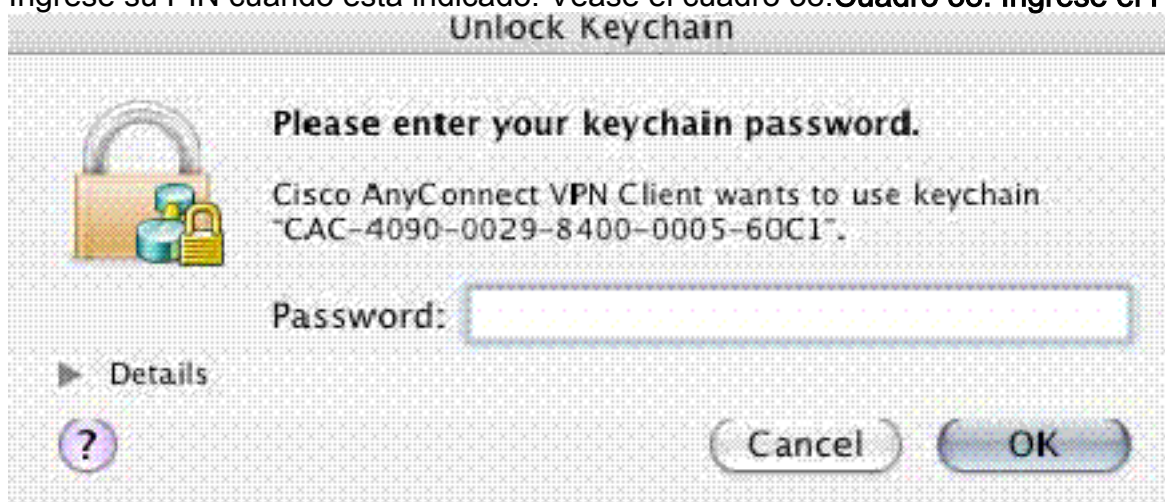
[Nueva conexión](#)

La ventana AC aparece. Véase el cuadro 37.

Cuadro 37: Nueva conexión VPN

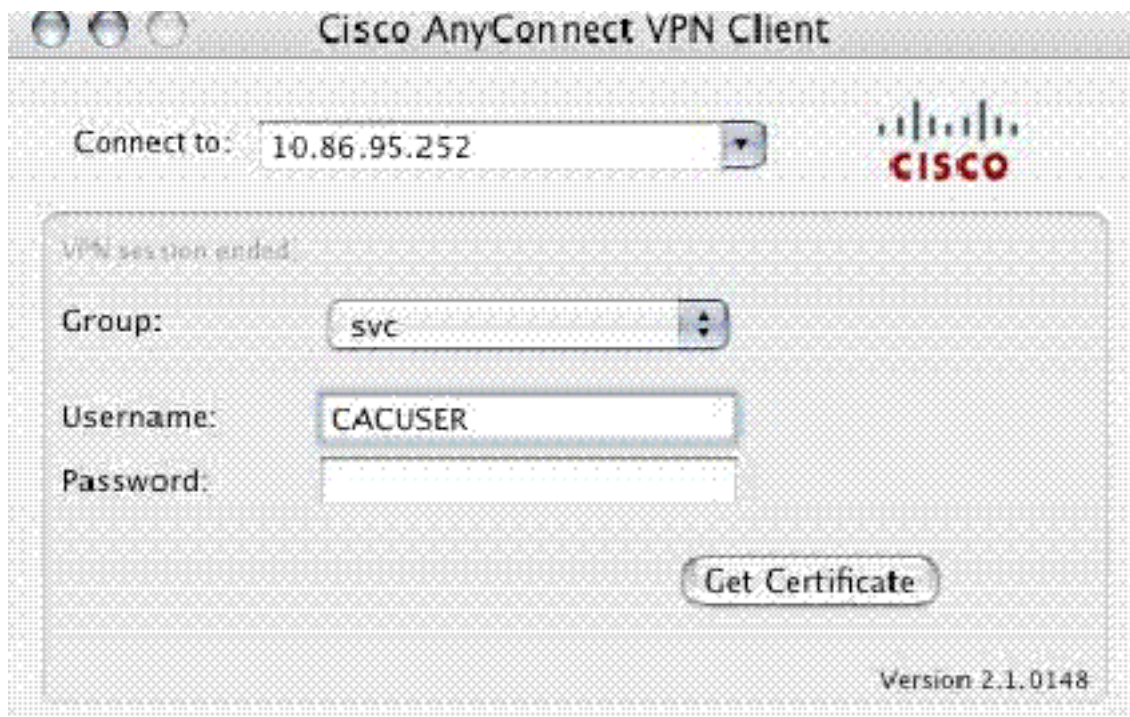


1. Elija el host apropiado si el AC no intenta automáticamente la conexión.
2. Ingrese su PIN cuando está indicado. Véase el cuadro 38.



[Comience el Acceso Remoto](#)

1. Elija al grupo y recíbalo a cuál usted quiere conectar.
2. Puesto que se utilizan los Certificados, elija **conectan** para establecer el VPN. Véase el cuadro 39. **Nota:** Puesto que la conexión utiliza los Certificados, no hay necesidad de ingresar un nombre de usuario y contraseña. **Cuadro 39:** Conectado



Nota: Vea el apéndice E para la configuración del perfil opcional del cliente de AnyConnect.

[Apéndice A – Sincronización LDAP y DAP](#)

En ASA/PIX la versión 7.1(x) y posterior, una característica llamada sincronización LDAP fue introducida. Ésta es una característica potente que proporciona una asignación entre un atributo y los objetos/atributo de Cisco LDAP, que niega la necesidad del cambio del esquema LDAP. Para la implementación de la autenticación CAC, esto puede soportar la aplicación de políticas adicional en la conexión de acceso remoto. Éstos son ejemplos de la sincronización LDAP. Sea consciente que usted necesita las derechos del administrador para realizar los cambios en el servidor AD/LDAP. En el software ASA 8.x, la característica de la directiva del acceso dinámico (DAP) fue introducida. El DAP puede trabajar conjuntamente con el CAC para mirar a los grupos múltiples AD así como para avanzar las directivas, los ACL y así sucesivamente.

[Escenario 1: Aplicación del Active Directory usando el dial-in del Permiso de acceso remoto – Permita/niegue el acceso](#)

Este ejemplo asocia el msNPAllowDailin del atributo AD al protocolo del atributo cVPN3000-Tunneling- de Cisco.

- El valor de atributo AD: VERDAD = permita; FALSO = niegue
 - Valor de atributo de Cisco: 1 = FALSO, 4 (IPSec) o 20 (4 IPSEC + 16 WebVPN) = VERDAD,
- Para la condición ALLOW, usted asocia:

- VERDAD = 20

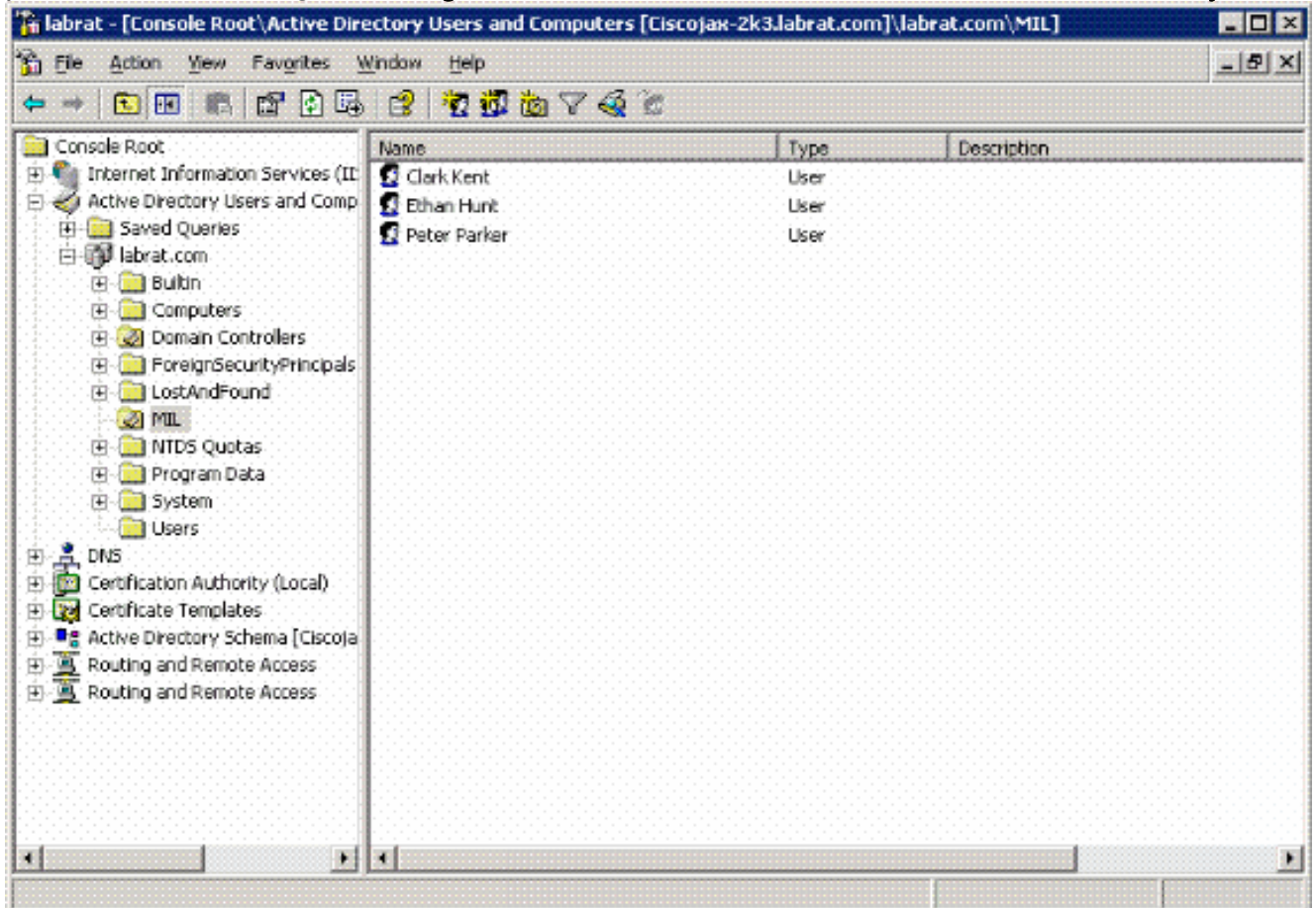
Para la condición del dial-in DENY, usted asocia:

- = 1 FALSO

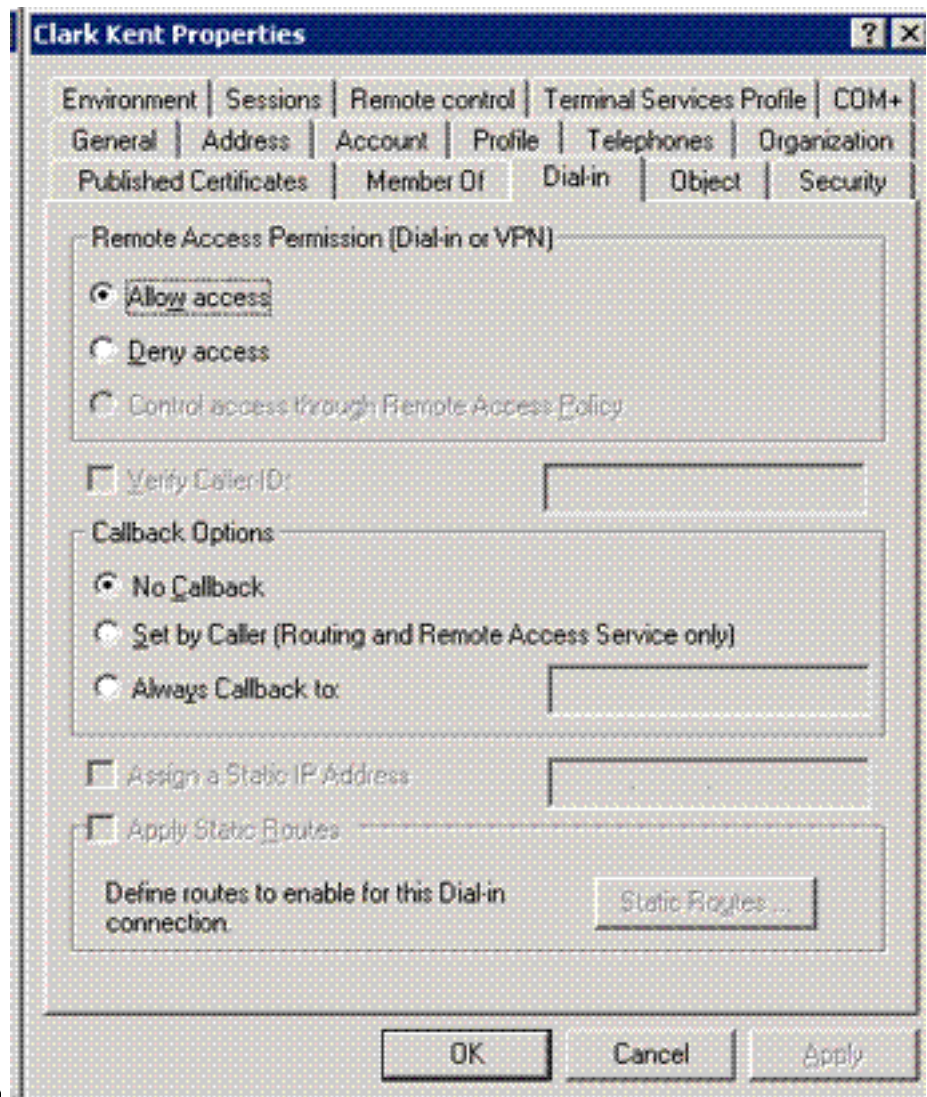
Nota: Asegúrese que VERDAD y FALSO esté en todos los casquillos. Refiera a [configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad](#) para más información.

Configuración del Active Directory

1. En el servidor Active Directory, **Start (Inicio) > Run (Ejecutar)** del teclado.
2. En el cuadro de texto abierto, el tipo **dsa.msc** entonces hace clic la autorización. **Esto** enciende la consola de administración del Active Directory.
3. En la consola de administración del Active Directory, haga clic el signo más para ampliar a los usuarios de directorio activo y computadora.
4. Haga clic el signo más para ampliar el Domain Name.
5. Si usted tiene un OU creado para sus usuarios, amplíe el OU para ver a todos los usuarios; si usted tiene todos los usuarios asignados en la carpeta del usuario, ampliése que carpeta para verlos. Vea la figura A1.



6. Clic doble en el usuario que usted quiere editar. Haga clic en el dial-in tab en la página de las propiedades del usuario y haga clic en **permiten** o **niegan**. Vea la figura a2.

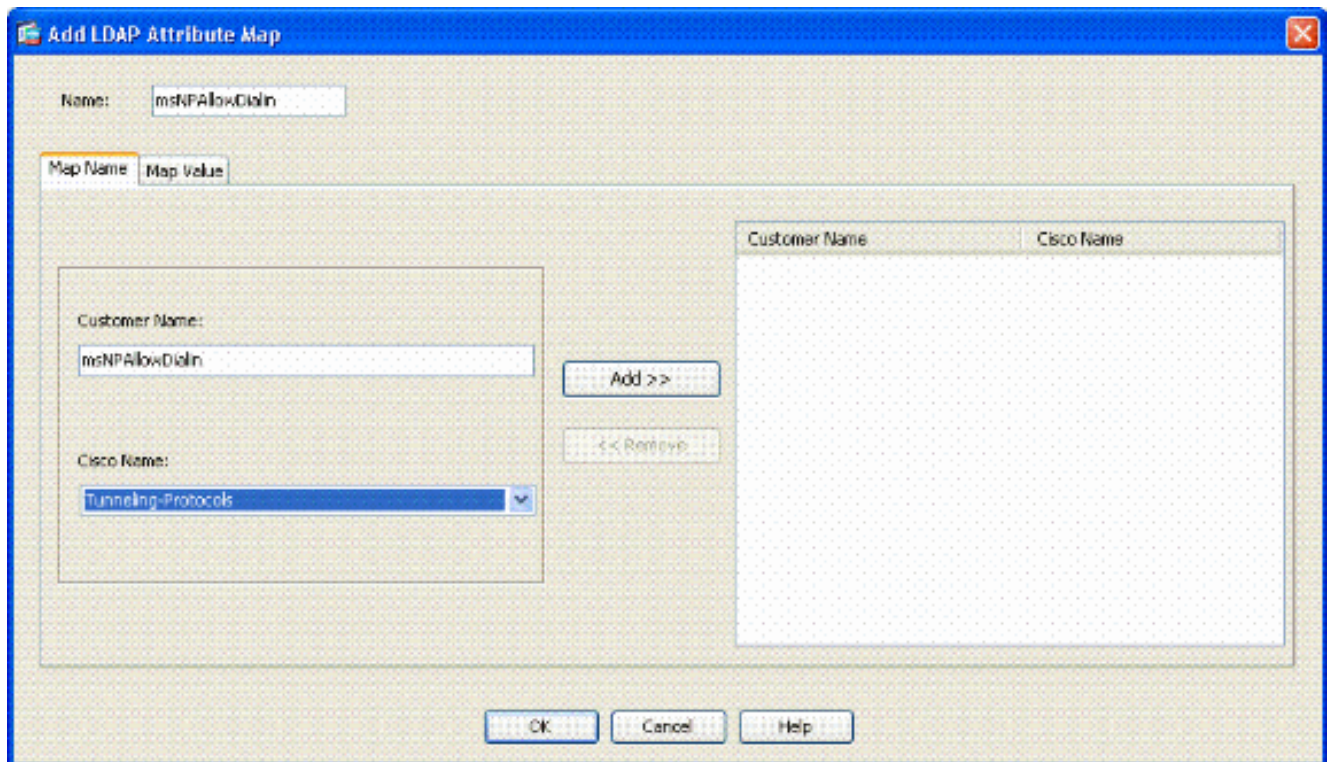


Propiedades del usuario

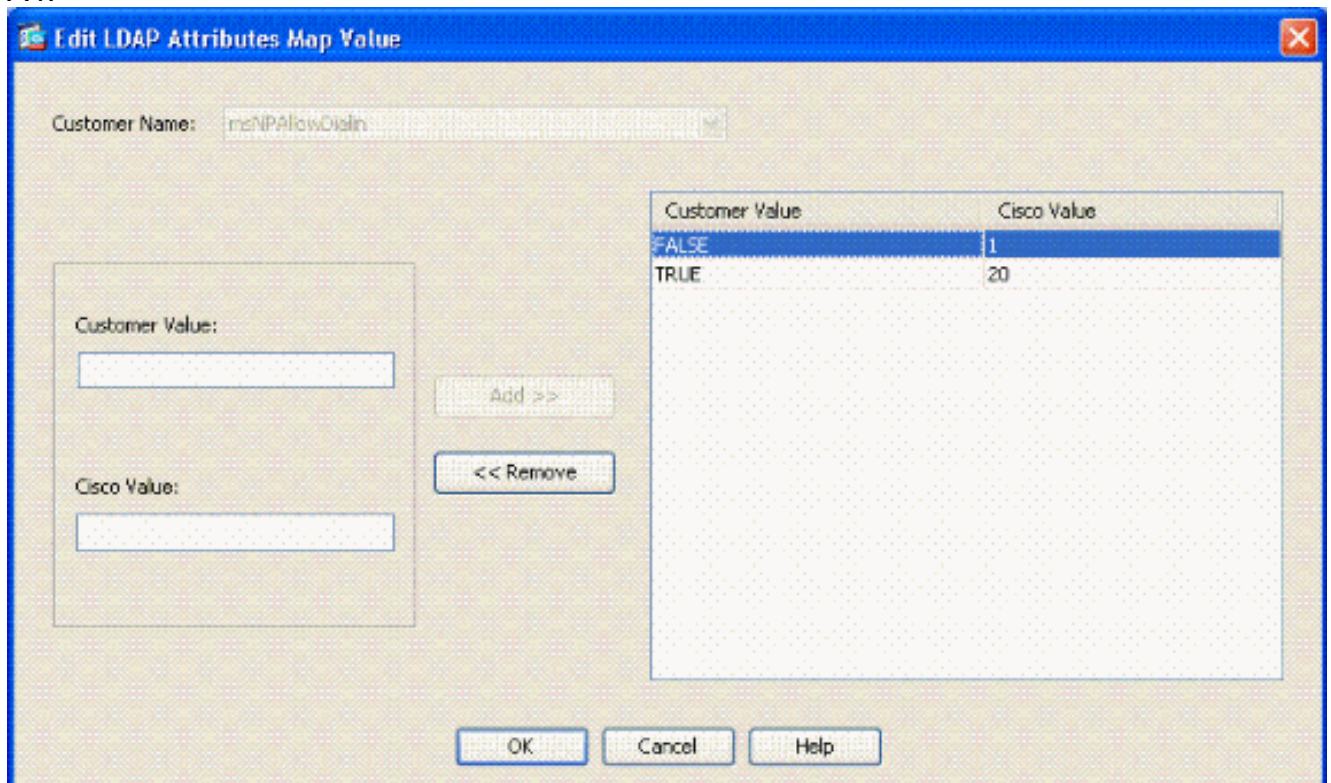
7. Entonces haga clic la autorización.

[Configuración ASA](#)

1. En el ASDM, elija el Acceso Remoto VPN> AAA puesto > mapa del atributo LDAP.
2. Haga clic en Add (Agregar).
3. En la ventana del mapa del atributo del agregar LDAP, complete estos pasos. Vea la figura A3.Figura A3: Agregar el mapa del atributo LDAP

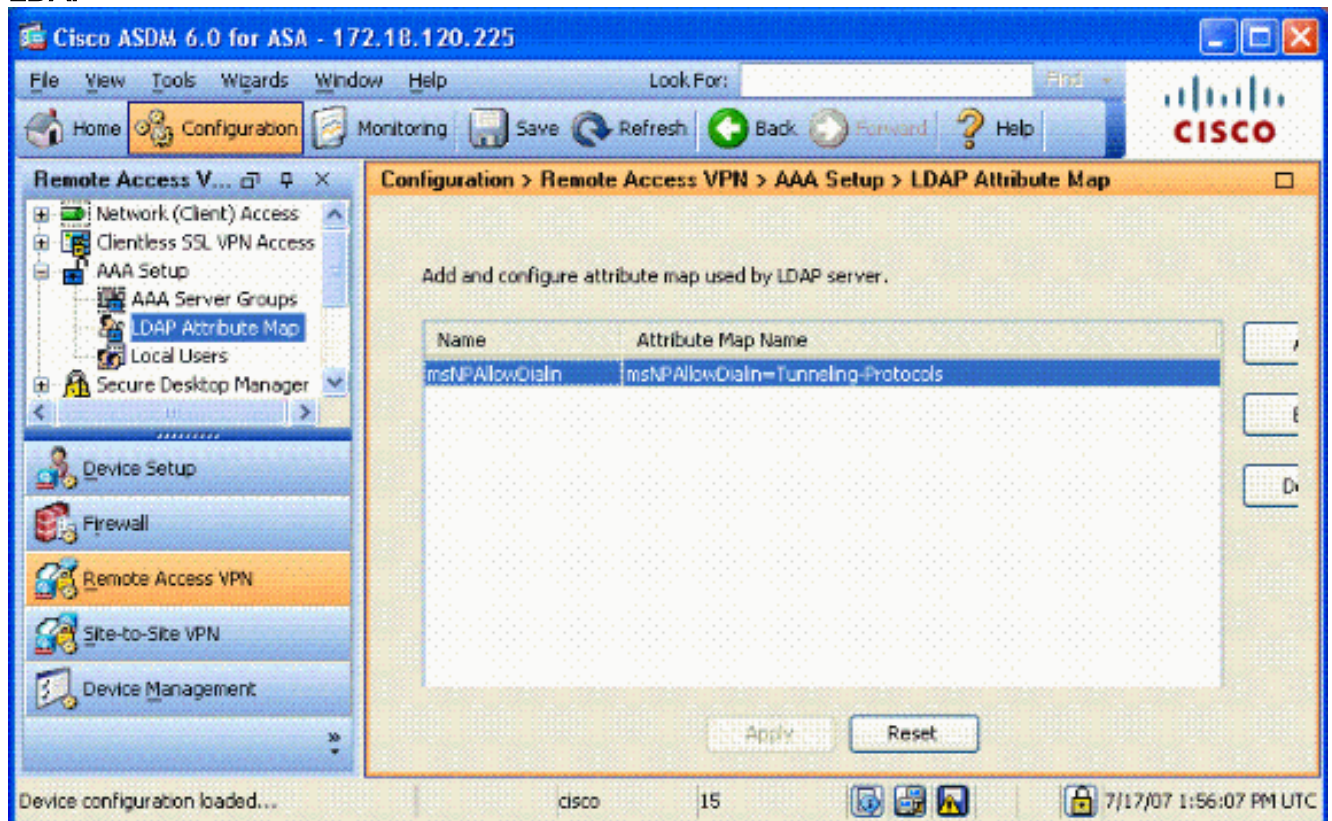


Ingrese un nombre en el textbox del nombre. En la lengüeta del nombre de asignación, teclee el **msNPAllowDialIn** en el cuadro de texto del nombre del cliente. En la lengüeta del nombre de asignación, elija los **protocolos de túneles** en la opción del descenso-abajo en el nombre de Cisco. Haga clic en Add (Agregar). Elija la lengüeta del **valor del mapa**. Haga clic en Add (Agregar). En la ventana del valor del mapa del atributo LDAP del agregar, teclee **VERDAD** en el cuadro de texto y el tipo **20** del nombre del cliente en el cuadro de texto del valor de Cisco. Haga clic en Add (Agregar). Teclee **FALSO** en el cuadro de texto y el tipo **1** del nombre del cliente en el cuadro de texto del valor de Cisco. Vea la figura A4.

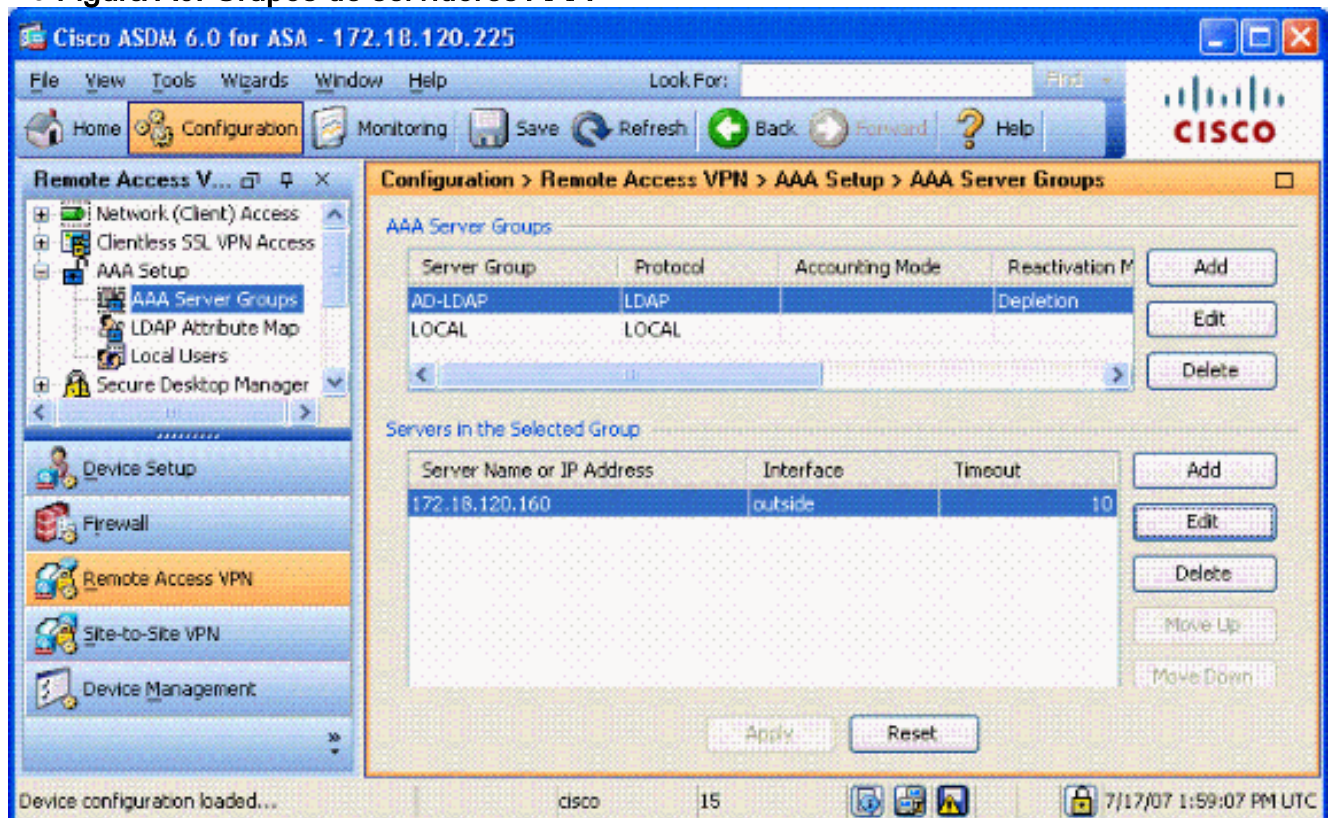


Haga clic la **autorización**. Haga clic la **autorización**. Haga clic en Apply (Aplicar). La configuración debe parecer la figura A5. **Figura A5: Configuración de asignación del atributo**

LDAP



4. Elija a los grupos de servidores puestos AAA del Acceso Remoto VPN>>AAA. Vea la figura A6. **Figura A6: Grupos de servidores AAA**



5. Haga clic en el grupo de servidores que usted quiere editar. En los servidores en la sección de grupo seleccionada, elija el dirección IP del servidor o el nombre de host, y después haga clic **editan**.
6. En edite la ventana del servidor de AAA, en el cuadro de texto del mapa del atributo LDAP, eligen la correspondencia del atributo LDAP creada en el menú desplegable. Vea la figura A7. **Figura A7: Agregar el mapa del atributo LDAP**

Edit AAA Server

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

LDAP Parameters

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

Naming Attribute(s): userPrincipalName

Login DN: CN=Administrator,CN=Users,DC=gsgseclab,DC=o

Login Password: ●●●●●●●●

LDAP Attribute Map: msNPAllowDialin

SASL MD5 authentication

SASL Kerberos authentication

Kerberos Server Group:

OK Cancel Help

7. Autorización del teclado.

Nota: Gire el debugging LDAP mientras que usted prueba para verificar si el atascamiento LDAP y la asignación del atributo trabajan correctamente. Vea el C del apéndice para los comandos de Troubleshooting.

[Escenario 2: La aplicación del Active Directory usando la membresía del grupo a permitir/niega el acceso](#)

Este ejemplo utiliza el memberOf del atributo LDAP para asociar al Tunneling Protocol el atributo para establecer una membresía del grupo como condición. Para que esta directiva trabaje, usted debe tener estas condiciones:

- Utilice a un grupo que exista ya o cree a un nuevo grupo para que los usuarios de VPN ASA sean un miembro para de las condiciones ALLOW.
- Utilice a un grupo que exista ya o cree a un nuevo grupo para que no los usuarios ASA sean

un miembro para de las condiciones DENY.

- Asegúrese al incorporar el Visualizador LDAP que usted tiene el DN derecho para el grupo. Ver Apéndice D. Si el DN es incorrecto, la asignación no trabaja correctamente.

Nota: Sea consciente que el ASA puede leer solamente la primera cadena del atributo del memberOf en esta versión. Asegúrese que el nuevo grupo creado está en el top de la lista. La otra opción es poner un carácter especial delante del nombre pues el AD mira los caracteres especiales primero. Para trabajar alrededor de esta advertencia, utilice el DAP en el software 8.x para mirar a los múltiples grupos.

Nota: Asegúrese a un usuario es parte del grupo de la negación o por lo menos otro grupo para devolver el memberOf siempre al ASA. Usted no tiene que especificar el FALSO niega la condición pero la mejor práctica es hacer tan. Si el nombre de grupo existente o el nombre del grupo contiene un espacio, ingrese el atributo de este modo:

CN=Backup Operators,CN=BuiltIn,DC=gsgseclab,DC=org

Nota: El DAP permite que el ASA mire a los múltiples grupos en el atributo del memberOf y la autorización baja de los grupos. Vea la sección DAP.

EL ASOCIAR

- El valor de atributo AD:memberOf CN=ASAUsers, cn=Users, DC=gsgseclab, DC=org
memberOf CN=TelnetClients, cn=Users, DC=labrat, dc=com
- Valor de atributo de Cisco: 1 = FALSO, 20 = VERDAD,

Para la condición **ALLOW**, usted asocia:

- memberOf CN=ASAUsers, cn=Users, DC=gsgseclab, DC=org= 20

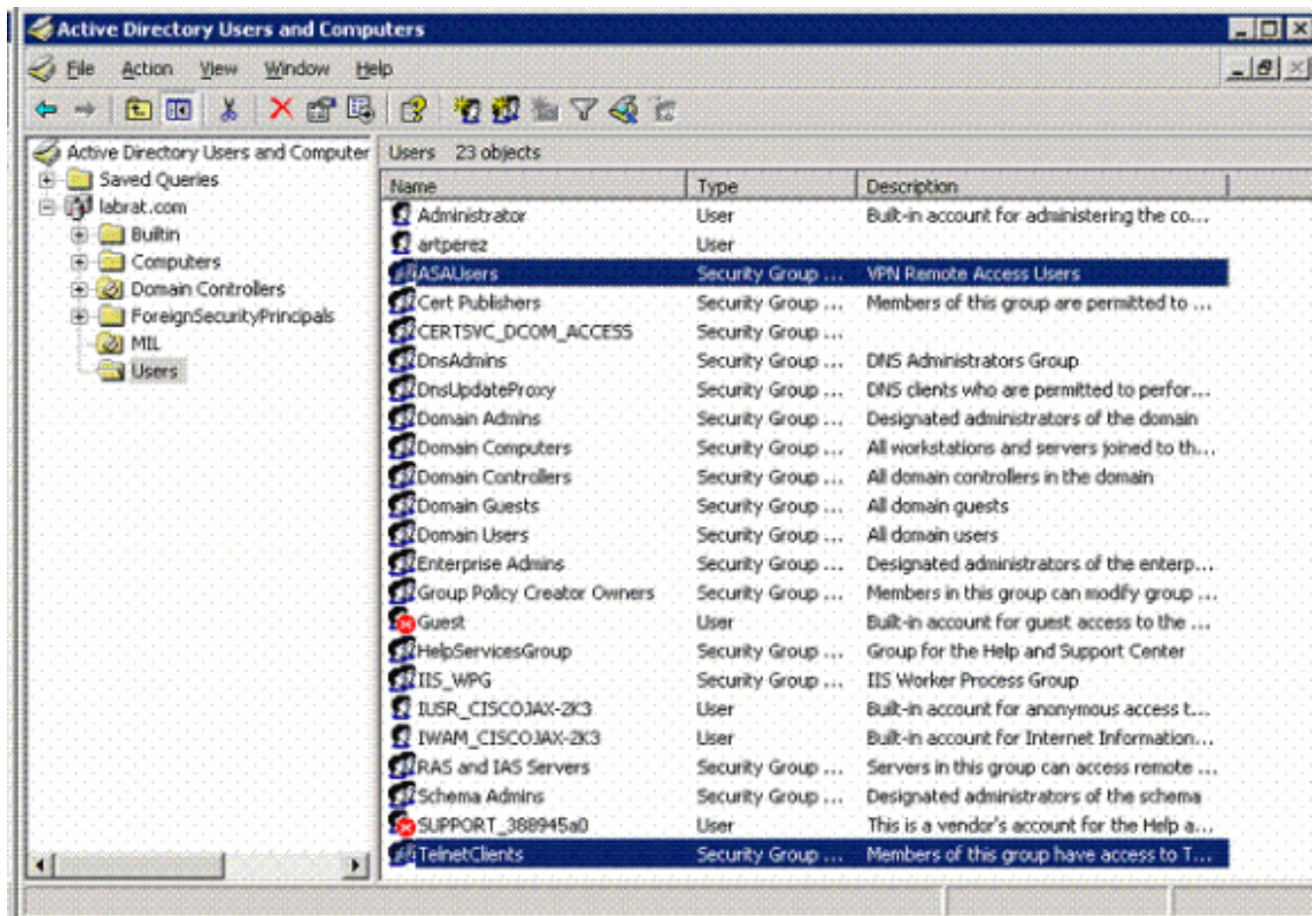
Para la condición **DENY**, usted asocia:

- memberOf CN=TelnetClients, cn=Users, DC=gsgseclab, DC=org = 1

Nota: En la futura versión, hay un atributo de Cisco para permitir y negar la conexión. Refiera a [configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad](#) para más información sobre los atributos de Cisco.

Configuración del Active Directory

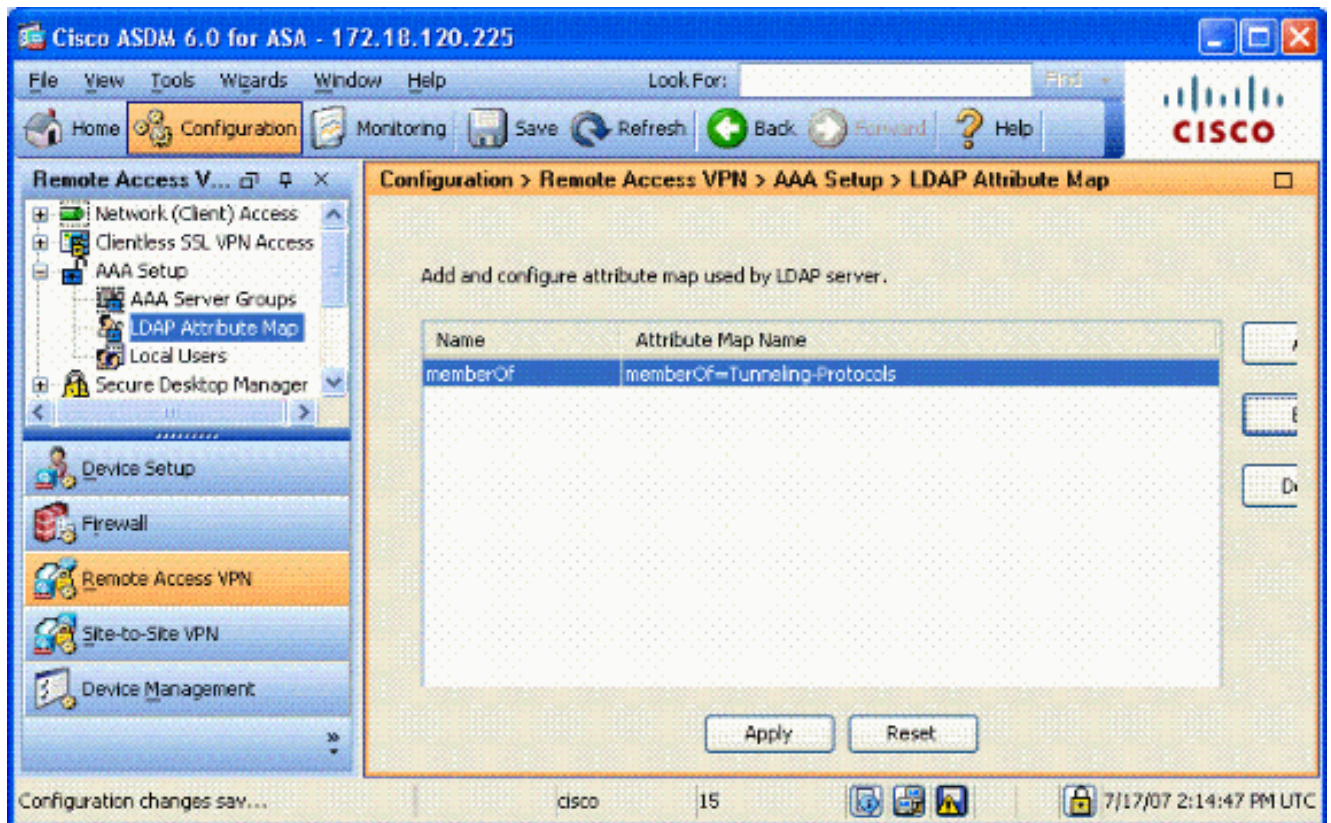
1. En el servidor Active Directory, elija el **Start (Inicio) > Run (Ejecutar)**.
2. En el cuadro de texto abierto, teclee **dsa.msc**, y después haga clic la autorización. **Esto** enciende la consola de administración del Active Directory.
3. En la consola de administración del Active Directory, haga clic el signo más para ampliar a los usuarios de directorio activo y computadora. Vea la figura A8 **Figura A8: Grupos del Active Directory**



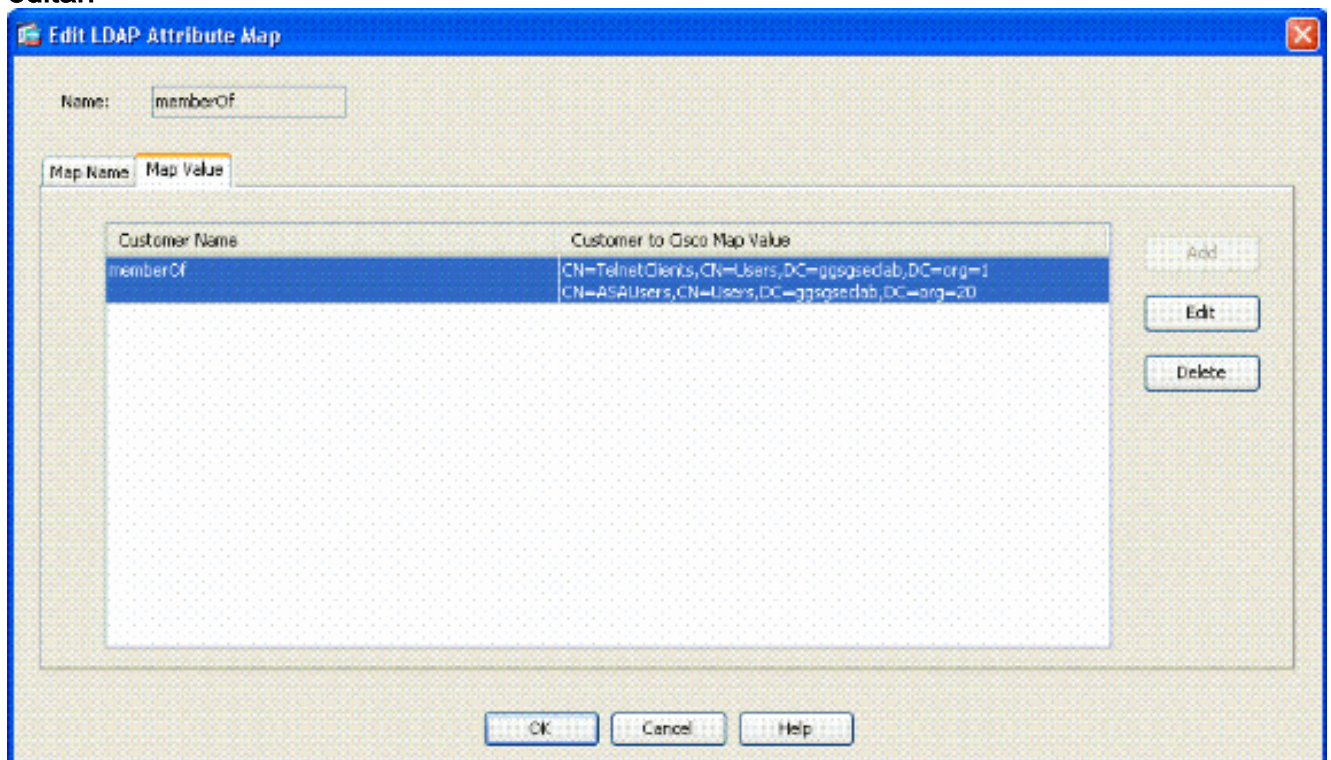
4. Haga clic el signo más para ampliar el Domain Name.
5. Haga clic con el botón derecho del ratón en la **carpeta del usuario** y elija **nuevo > grupo**.
6. Ingrese un nombre del grupo. Por ejemplo: **ASAUsers**.
7. **Autorización del teclado**.
8. Haga clic en la **carpeta del usuario**, y entonces el clic doble en el grupo que usted acaba de crear.
9. Elija la lengüeta de los **miembros**, y entonces el haga click en Add
10. Teclee el nombre del usuario que usted quiere agregar, y después haga clic la **autorización**.

Configuración ASA

1. En el ASDM, elija el **VPN de acceso remoto > AAA ponen > mapa del atributo LDAP**.
2. Haga clic en Add (Agregar).
3. En la ventana del mapa del atributo del agregar LDAP, complete estos pasos. Vea la figura A3. Ingrese un nombre en el textbox del nombre. En la lengüeta del nombre de asignación, teclee el **memberOf** en el cuadro de texto C. del nombre del cliente. En la lengüeta del nombre de asignación, elija los **protocolos de túneles** en la opción del descenso-abajo en el nombre de Cisco. Elija **agregan**. Haga clic la lengüeta del **valor del mapa**. Elija **agregan**. En la ventana del valor del mapa del atributo LDAP del agregar, teclee **CN=ASAUsers, cn=Users, DC=gsgseclab, DC=org** en el cuadro de texto y el tipo **20** del nombre del cliente en el cuadro de texto del valor de Cisco. Haga clic en Add (Agregar). Teclee **CN=TelnetClients, cn=Users, DC=gsgseclab, DC=org** en el cuadro de texto y el tipo **1** del nombre del cliente en el cuadro de texto del valor de Cisco. Vea la figura A4. Haga clic la **autorización**. Haga clic la **autorización**. Haga clic en Apply (Aplicar). La configuración debe parecer la figura A9. **Figura mapa del atributo A9 LDAP**



4. Elija a los **grupos de servidores puestos AAA del Acceso Remoto VPN> >AAA**.
5. Haga clic en al grupo de servidores que usted quiere editar. En los servidores en la sección de grupo seleccionada, seleccione el dirección IP del servidor o el nombre de host, y después haga clic **editan**



6. En edite la ventana del servidor de AAA, en el cuadro de texto del mapa del atributo LDAP, seleccionan la correspondencia del atributo LDAP creada en el menú desplegable.
7. Haga clic la **autorización**.

Nota: Gire el debugging LDAP mientras que usted prueba para verificar el atascamiento LDAP y atribuir las asignaciones trabaje correctamente. Vea el C del apéndice para los comandos de Troubleshooting.

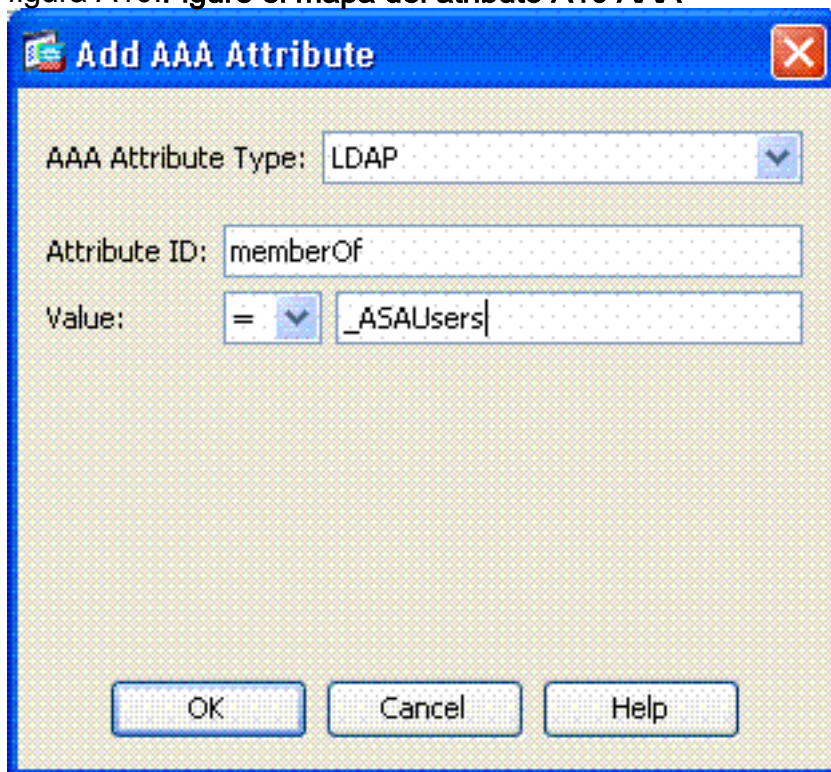
Escenario 3: Directivas del acceso dinámico para los atributos múltiples del memberOf

Este ejemplo utiliza el DAP para mirar los atributos múltiples del memberOf para permitir el acceso basado apagado de la membresía del grupo del Active Directory. Antes de 8.x, el ASA leyó solamente el primer atributo del memberOf. Con 8.x y posterior, el ASA puede mirar todos los atributos del memberOf.

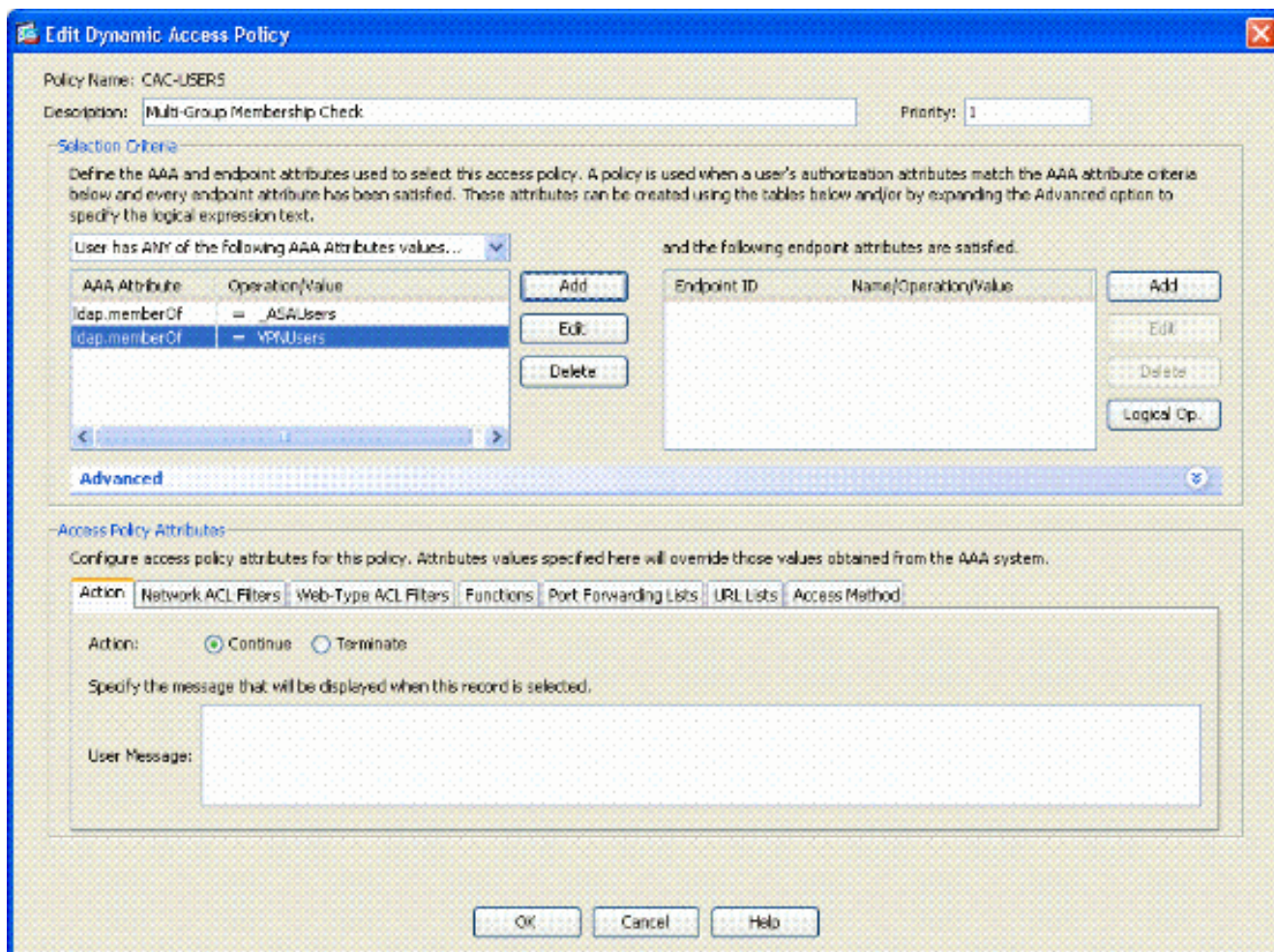
- Utilice a un grupo que exista ya o cree un nuevo grupo (o a los múltiples grupos) para que los usuarios de VPN ASA sean un miembro para de las condiciones ALLOW.
- Utilice a un grupo que exista ya o cree a un nuevo grupo para que no los usuarios ASA sean un miembro para de las condiciones DENY.
- Asegurese al incorporar el Visualizador LDAP que usted tiene el DN derecho para el grupo. Ver Apéndice D. Si el DN es incorrecto, la asignación no trabaja correctamente.

Configuración ASA

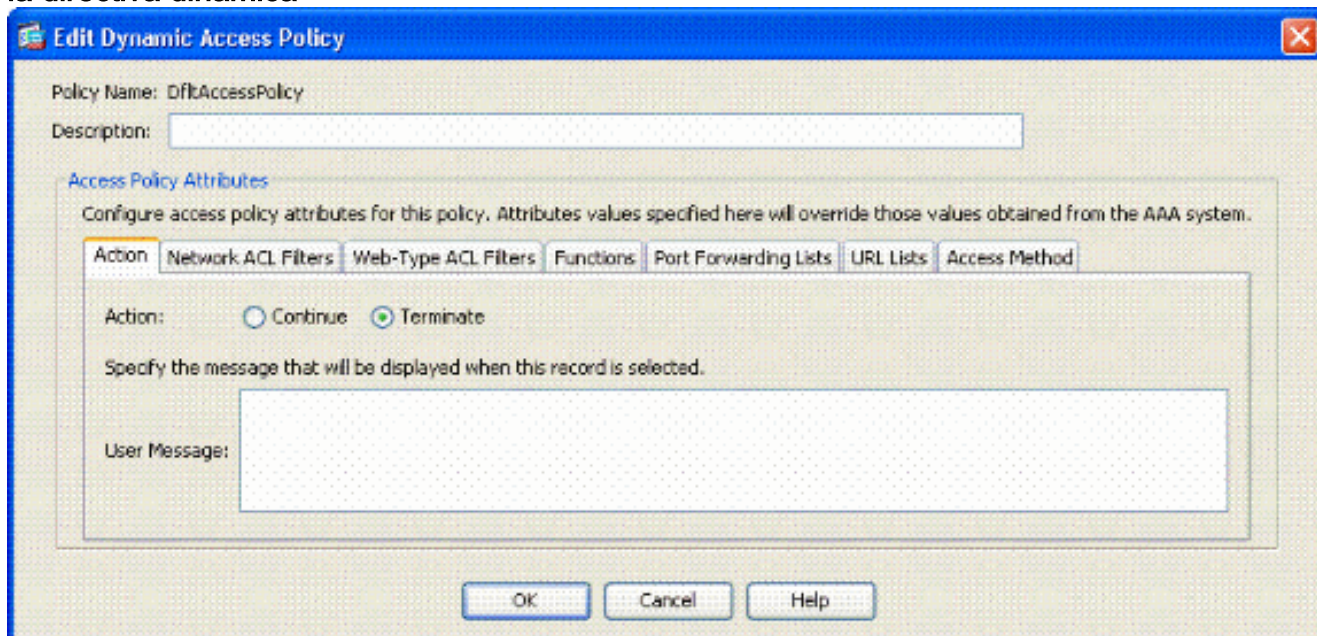
1. En el ASDM, elija las **directivas del acceso > del acceso dinámico de la red del Acceso Remoto VPN> (cliente)**.
2. Haga clic en Add (Agregar).
3. En la directiva del acceso dinámico del agregar, complete estos pasos: Ingrese un nombre en el textbox B. del nombre. En la sección de prioridad, ingrese 1, o un número mayor de 0. En el Criterio de selección, haga click en Add. En el atributo del agregar AAA, elija el **LDAP**. En la sección del atributo ID, ingrese el **memberOf**. En la sección del valor, elija = y ingrese el nombre del grupo AD. Relance este paso para cada grupo que usted quiere referirse. Vea la figura A10. **Figure el mapa del atributo A10 AAA**



Haga clic en OK. En la política de acceso atribuye la sección, choose Continue. Vea la figura A11. **La figura A11 agrega la directiva dinámica**



4. En el ASDM, elija las directivas del acceso > del acceso dinámico de la red del Acceso Remoto VPN> (cliente).
5. Elija la política de acceso predeterminada y elija editar.
6. La acción predeterminada se debe fijar para terminar. Vea la figura A12.La figura A12 edita la directiva dinámica



7. Autorización del teclado.

Nota: Si **Terminate** no se selecciona, adentro a le se permite incluso si no en cualquier grupo porque el valor por defecto es continuar.

Apéndice B – Configuración CLI ASA

ASA 5510

```
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=gsgseclab,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=gsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn
CN=Administrator,CN=Users,DC=gsgseclab,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-----
-----
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-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-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

```

[Troubleshooting del apéndice c](#)

[Resolver problemas el AAA y el LDAP](#)

- **ldap 255 del debug** — Intercambios de las visualizaciones LDAP
- **campo común 10 aaa del debug** — Intercambios de las visualizaciones AAA

[Ejemplo 1: Conexión permitida con la asignación correcta del atributo](#)

Este ejemplo muestra la salida del **ldap** y del **debug aaa del debug comunes** durante una conexión satisfactoria con el escenario 2 mostrado en el Apéndice A.

Figura c1: haga el debug del LDAP y haga el debug de la salida común 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=gsgseclab,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=gsgseclab,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 la asignación mis configurada del atributo de Cisco](#)

Este ejemplo muestra la salida del **ldap** y del **debug aaa** del **debug comunes** durante una conexión permitida con el escenario 2 mostrado en el Apéndice A.

Figura C2: haga el debug del LDAP y haga el debug de la salida común aaa – mapeo incorrecto

```
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=gsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=gsgseclab,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=gsgseclab,DC=or
g
[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
```

[Resolver problemas el DAP](#)

- **errores del dap del debug** — Errores de las visualizaciones DAP
- **traza del dap del debug** — Traza de la función de las visualizaciones DAP

Ejemplo 1: Conexión permitida con el DAP

Este ejemplo muestra la salida de los **errores del dap del debug** y la **traza del dap del debug** durante una conexión satisfactoria con el escenario 3 mostrado en el Apéndice A. Atributos múltiples del memberOf del aviso. Usted puede pertenecer a los _ASAUsers y VPNUsers o tp cualquier grupo, que depende de los config ASA.

Figura c3: debug DAP

```
#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=gsgseclab,DC=or
g
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=gsgsecclab,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=gsgseclab,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 negada con el DAP

El ejemplo de Thia muestra la salida de los **errores del dap del debug** y la **traza del dap del debug** durante una conexión fracasada con el escenario 3 mostrado en el Apéndice A.

Figura C4: debug DAP

```

#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=gsgseclab,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=gsgseclab,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=gsgseclab,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
```

[Resolver problemas el Certificate Authority/OCSP](#)

- **debug crypto ca 3**

- En el modo de configuración — **debugging de la consola de la clase Ca del registro (o buffer)**

Estos ejemplos muestran una validación de certificado acertada con el respondedor OCSP y una directiva que corresponde con fallada del grupo del certificado.

La figura c3 muestra la salida de los debugs que tiene un certificado validado y una directiva que corresponde con de trabajo del grupo del certificado.

La figura C4 muestra la salida de los debugs de una directiva que corresponde con del grupo mis configurado del certificado.

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

Figura C5: Debugging OCSP – validación de certificado acertada

```
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 directiva que corresponde con fallada del grupo del certificado

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,validid cor
=noct
oamuthorized.
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.

```

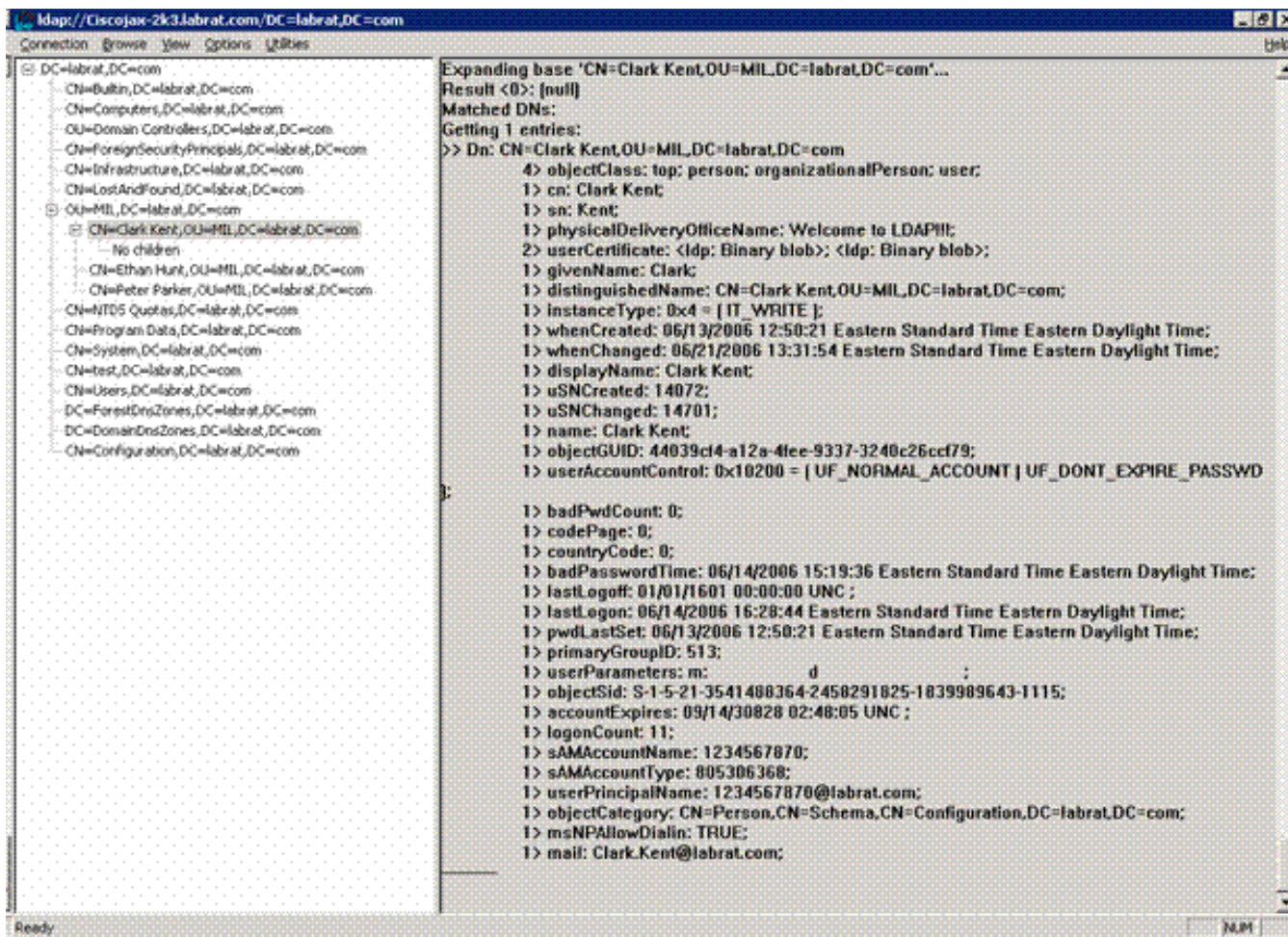
```
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org, issuer_name:
cn=gsgseclab,dc=gsgseclab,dc=org.
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=gsgseclab,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=gsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

[Apéndice D – Verifique los objetos LDAP en el MS](#)

En el CD del servidor de Microsoft 2003, hay las herramientas adicionales que se pueden instalar para ver la estructura LDAP así como los objetos LDAP/los atributos. Para instalar estas herramientas, vaya al directorio del **soporte** en el CD y entonces las **herramientas**. Instale **SUPTOOLS.MSI**.

[Visualizador LDAP](#)

- Después de la instalación, elija el **Start (Inicio) > Run (Ejecutar)**.
- Teclee el **ldp**, después haga clic la **autorización**. Esto enciende el Visualizador LDAP.
- Elija la **conexión > conectan**.
- Ingrese Nombre del servidor y después haga clic la **autorización**.
- Elija la **conexión > el lazo**.
- Ingrese un nombre de usuario y contraseña. **Nota:** Usted necesita las derechas del administrador.
- Haga clic en OK.
- Objetos de la visión LDAP. Vea la figura D1. **Figura D1: Visualizador LDAP**

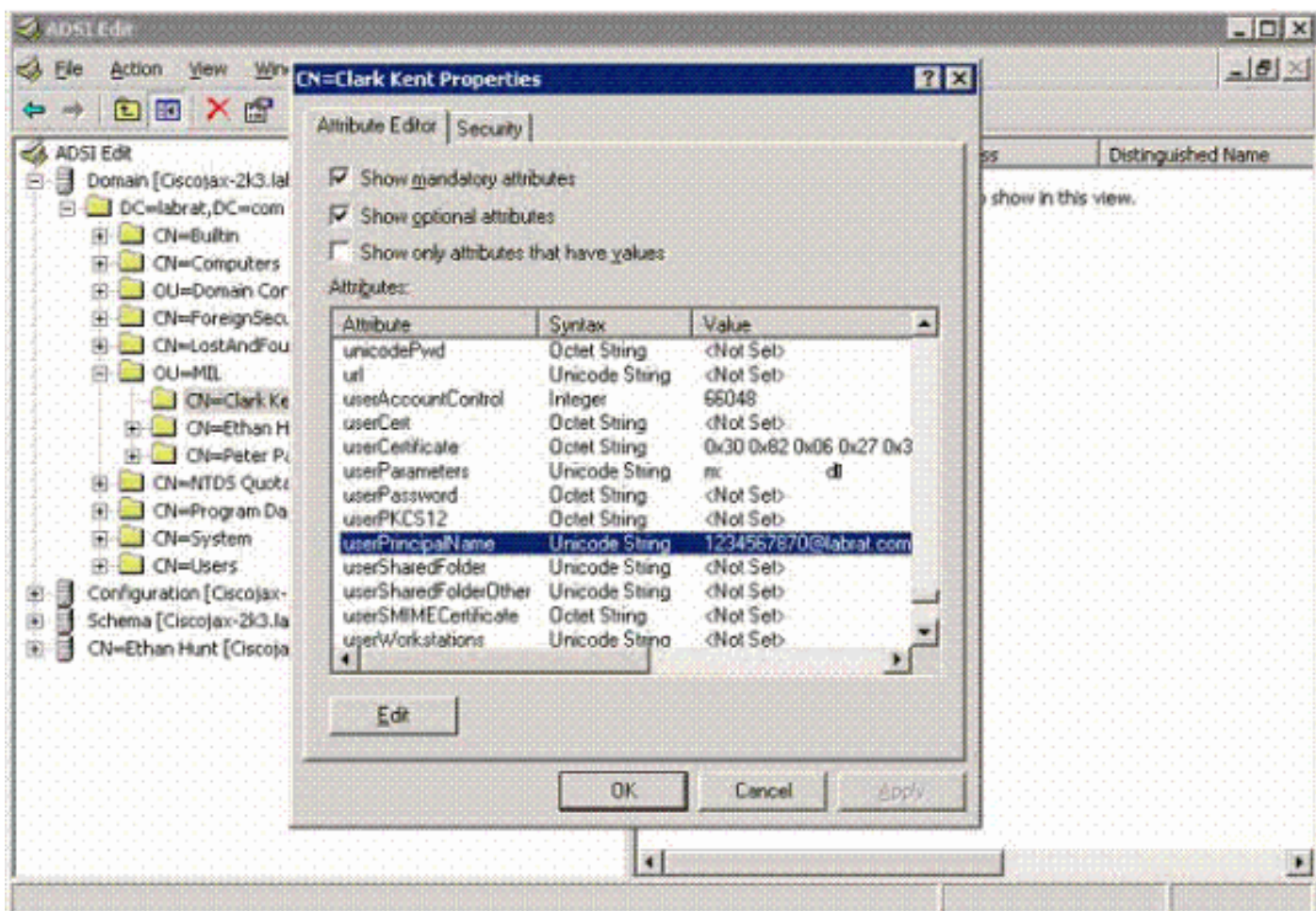


Editor de la interfaz de los servicios de Active Directory

- En el servidor Active Directory, elija el **Start (Inicio) > Run (Ejecutar)**.
- Teclee **adsiedit.msc**. Esto comienza el editor.
- Click derecho en un objeto y las **propiedades del teclado**.

Esta herramienta muestra todos los atributos para los objetos específicos. Vea la figura D2.

Figura D2: El ADSI edita



Apéndice E

Un perfil de AnyConnect se puede crear y agregar a un puesto de trabajo. El perfil puede referirse a los diversos valores tales como host ASA o certificar los parámetros que corresponden con tales como nombre distintivo o emisor. El perfil se salva como archivo del .xml y se puede editar con la libreta. El archivo se puede agregar a cada cliente manualmente o avanzar del ASA con una directiva del grupo. El archivo se salva en:

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

Complete estos pasos:

1. Elija el AnyConnectProfile.tmpl y abra el archivo con la libreta.
2. Haga las modificaciones apropiadas al archivo tal como emisor o IP del host. Vea la figura F1 por ejemplo.
3. Cuando está acabado, salve el archivo como .xml.

Esto es una muestra de un archivo XML del perfil del Cliente Cisco AnyConnect VPN.

Refiera a la documentación de Cisco AnyConnect con respecto a la Administración del perfil. En el cortocircuito:

- Un perfil se debe nombrar únicamente para su compañía. Se presenta un ejemplo a continuación: CiscoProfile.xml
- El nombre del perfil debe ser lo mismo incluso si es diferente para el grupo individual dentro de la compañía.

Este archivo se piensa para ser mantenido por un administrador seguro del gateway y después para ser distribuido con el software de cliente. El perfil basado en este XML se puede distribuir a los clientes en cualquier momento. Los mecanismos de distribución soportados son como un archivo unido con la distribución de software o como parte del mecanismo automático de la descarga. El mecanismo automático de la descarga solamente disponible con cierto Cisco asegura los Productos del gateway.

Nota: Animan a los administradores fuertemente a validar el perfil XML que crean con el uso de una herramienta en línea de la validación o con las funciones de la importación del perfil en el ASDM. La validación se puede lograr con el AnyConnectProfile.xsd encontrado en este directorio. AnyConnectProfile es el elemento raíz que representa el perfil del cliente de AnyConnect.

```
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, for
example, BackupServerList, host specific !--- overrides
are possible. !-- --> - <ClientInitialization>
!-- The Start Before Logon feature can be used to
activate !--- the VPN as part of the logon sequence. !--
- UserControllable: Does the administrator of this
profile allow the user !--- to control this attribute
for their own use. Any user setting !--- associated with
this attribute is stored elsewhere. -->
<UseStartBeforeLogon
UserControllable="false">>false</UseStartBeforeLogon>
!-- This control enables an administrator to have a one
time !--- message displayed prior to a users first
connection attempt. As an !--- example, the message can
be used to remind a user to insert their smart !--- card
into its reader. !--- The message to be used with this
control is localizable and can be !--- found in the
AnyConnect message catalog. !--- (default: "This is a
pre-connect reminder message.")
<ShowPreConnectMessage>>false</ShowPreConnectMessage>
!-- This section enables the definition of various
attributes !--- that can be used to refine client
certificate selection. --> - <CertificateMatch>
!-- Certificate Distinguished Name matching allows for
exact !--- match criteria in the choosing of acceptable
client !--- certificates. - <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 el X.509 y el RFC 3280](#)
- [OCSP especificado por el RFC 2560](#)
- [Introducción del Public Key Infrastructure](#)
- ["OCSP ligero" perfilado por el estándar de borrador](#)
- [SSL/TLS especificado por RFC2246](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)