

ACS seguro: NAR con clientes AAA para usuarios y grupos de usuarios

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Restricciones de acceso a la red](#)

[Acerca de las restricciones de acceso a la red](#)

[Agregar un NAR compartido](#)

[Editar un NAR compartido](#)

[Eliminar un NAR compartido](#)

[Establecer restricciones de acceso a la red para un usuario](#)

[Establecer restricciones de acceso a la red para un grupo de usuarios](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar las Restricciones del acceso a la red (NAR) en la versión 4.x de Cisco Secure Access Control Server (ACS) con los clientes AAA (incluidos los routers, PIX, ASA, controladores inalámbricos) para los usuarios y grupos de usuarios.

[Prerequisites](#)

[Requirements](#)

Este documento se crea suponiendo que los clientes Cisco Secure ACS y AAA están configurados y funcionan correctamente.

[Componentes Utilizados](#)

La información de este documento se basa en Cisco Secure ACS 3.0 y posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Convenciones](#)

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

Restricciones de acceso a la red

Esta sección describe los NAR y proporciona instrucciones detalladas para configurar y administrar los NAR compartidos.

Esta sección contiene los siguientes temas:

- [Acerca de las restricciones de acceso a la red](#)
- [Agregar un NAR compartido](#)
- [Editar un NAR compartido](#)
- [Eliminar un NAR compartido](#)

Acerca de las restricciones de acceso a la red

Un NAR es una definición, que se hace en ACS, de condiciones adicionales que debe cumplir antes de que un usuario pueda acceder a la red. ACS aplica estas condiciones mediante el uso de la información de los atributos que envían sus clientes AAA. Aunque puede configurar los NAR de varias maneras, todos se basan en la información de atributo coincidente que envía un cliente AAA. Por lo tanto, debe entender el formato y el contenido de los atributos que envían sus clientes AAA si desea emplear NAR efectivos.

Al configurar un NAR, puede elegir si el filtro funciona positiva o negativamente. Es decir, en el NAR usted especifica si se permite o deniega el acceso a la red, en base a la información enviada por los clientes AAA cuando se compara con la información almacenada en el NAR. Sin embargo, si un NAR no encuentra información suficiente para funcionar, de forma predeterminada se deniega el acceso. Esta tabla muestra estas condiciones:

	Basado en IP	No basado en IP	Información insuficiente
Permiso	Acceso concedido	Access Denied	Access Denied
Denegar	Access Denied	Acceso concedido	Access Denied

ACS admite dos tipos de filtros NAR:

- **Filtros basados en IP:** los filtros NAR basados en IP limitan el acceso basándose en las direcciones IP del cliente de usuario final y el cliente AAA. Vea la sección [Acerca de los Filtros NAR basados en IP](#) para obtener más información.
- **Filtros no basados en IP:** los filtros NAR no basados en IP limitan el acceso basándose en la comparación de cadenas simple de un valor enviado desde el cliente AAA. El valor puede ser el número de identificación de línea de llamada (CLI), el número de servicio de identificación de número marcado (DNIS), la dirección MAC u otro valor que se origine en el cliente. Para que este tipo de NAR funcione, el valor en la descripción de NAR debe coincidir exactamente con lo que se envía desde el cliente, que incluye el formato que se utilice. Por ejemplo, el número de teléfono (217) 555-4534 no coincide con 217-555-4534. Vea la sección [Acerca de](#)

[los Filtros NAR No Basados en IP](#) para obtener más información.

Puede definir un NAR para un usuario o grupo de usuarios específico y aplicarlo a él. Consulte las secciones [Establecer restricciones de acceso a la red para un usuario](#) o [Establecer restricciones de acceso a la red para un grupo de usuarios](#) para obtener más información. Sin embargo, en la sección Componentes de Perfil Compartidos de ACS puede crear y nombrar un NAR compartido sin citar directamente a ningún usuario o grupo de usuarios. Usted le da al NAR compartido un nombre al que se puede hacer referencia en otras partes de la interfaz web ACS. A continuación, al configurar usuarios o grupos de usuarios, puede seleccionar ninguna, una o varias restricciones compartidas para aplicar. Cuando especifica la aplicación de varios NAR compartidos a un usuario o grupo de usuarios, elige uno de dos criterios de acceso:

- Todos los filtros seleccionados deben permitirse.
- Cualquier filtro seleccionado debe permitirlo.

Debe comprender el orden de precedencia que está relacionado con los diferentes tipos de NAR. Este es el orden del filtrado de NAR:

1. NAR compartido a nivel de usuario
2. NAR compartido a nivel de grupo
3. NAR no compartido a nivel de usuario
4. NAR no compartido a nivel de grupo

También debe comprender que **la denegación de acceso en cualquier nivel tiene prioridad sobre las configuraciones en otro nivel que no niegan el acceso**. Esta es la única excepción en ACS a la regla que la configuración de nivel de usuario invalida la configuración de nivel de grupo. Por ejemplo, un usuario determinado podría no tener restricciones NAR en el nivel de usuario que se apliquen. Sin embargo, si ese usuario pertenece a un grupo que está restringido por un NAR compartido o no compartido, se deniega el acceso al usuario.

Los NAR compartidos se mantienen en la base de datos interna ACS. Puede utilizar las funciones ACS backup y restore para realizar copias de seguridad y restaurarlas. También puede replicar los NAR compartidos, junto con otras configuraciones, a los ACS secundarios.

[Acerca de los filtros NAR basados en IP](#)

Para los filtros NAR basados en IP, ACS utiliza los atributos como se muestra, que depende del protocolo AAA de la solicitud de autenticación:

- **Si utiliza TACACS+**—Se utiliza el campo `rem_addr` del cuerpo del paquete de inicio TACACS+. **Nota:** Cuando un proxy reenvía una solicitud de autenticación a un ACS, cualquier NAR para solicitudes TACACS+ se aplica a la dirección IP del servidor AAA de reenvío, no a la dirección IP del cliente AAA de origen.
- **Si utiliza RADIUS IETF:** se debe utilizar `call-station-id` (atributo 31). **Nota:** Los filtros NAR basados en IP funcionan sólo si ACS recibe el atributo Radius Calling-Station-Id (31). El ID de estación de llamada (31) debe contener una dirección IP válida. Si no lo hace, caerá en las reglas DNIS.

Los clientes AAA que no proporcionan suficiente información de dirección IP (por ejemplo, algunos tipos de firewall) no admiten la funcionalidad NAR completa.

Otros atributos para las restricciones **basadas en IP**, por protocolo, incluyen los campos NAR como se muestra:

- **Si utiliza TACACS+**—Los campos NAR en ACS utilizan estos valores:**Ciente AAA:** la dirección IP de NAS se toma de la dirección de origen en el socket entre ACS y el cliente TACACS+.**Puerto:** el campo de puerto se toma del cuerpo del paquete de inicio TACACS+.

[Acerca de los filtros NAR no basados en IP](#)

Un filtro NAR no basado en IP (es decir, un filtro NAR basado en DNIS/CLI) es una lista de ubicaciones de punto de acceso o llamada permitidas o denegadas que puede utilizar para restringir un cliente AAA cuando no tiene una conexión basada en IP establecida. La función NAR no basada en IP generalmente utiliza el número CLI y el número DNIS.

Sin embargo, cuando ingresa una dirección IP en lugar de la CLI, puede utilizar el filtro no basado en IP; incluso cuando el cliente AAA no utiliza una versión de software del IOS® de Cisco que soporte CLI o DNIS. En otra excepción para ingresar una CLI, puede ingresar una dirección MAC para permitir o denegar el acceso. Por ejemplo, cuando utiliza un cliente AAA Cisco Aironet. De la misma manera, podría ingresar la dirección MAC del punto de acceso Cisco Aironet en lugar del DNIS. El formato de lo que especifica en el cuadro CLI (CLI, dirección IP o dirección MAC) debe coincidir con el formato de lo que recibe de su cliente AAA. Puede determinar este formato desde el registro de cuentas RADIUS.

Los atributos para las restricciones basadas en DNIS/CLI, por protocolo, incluyen los campos NAR como se muestra:

- **Si utiliza TACACS+**—Los campos NAR enumerados emplean estos valores:**Ciente AAA:** la dirección IP NAS se toma de la dirección de origen en el socket entre ACS y el cliente TACACS+.**Puerto:** se utiliza el campo `port` en el cuerpo del paquete de inicio TACACS+.**CLI:** se utiliza el campo `rem-addr` en el cuerpo del paquete de inicio TACACS+.**DNIS:** se utiliza el campo `rem-addr` tomado del cuerpo del paquete de inicio TACACS+. En los casos en los que los datos `rem-addr` comienzan con la barra (/), el campo DNIS contiene los datos `rem-addr` sin la barra (/).**Nota:** Cuando un proxy reenvía una solicitud de autenticación a un ACS, cualquier NAR para solicitudes TACACS+ se aplica a la dirección IP del servidor AAA de reenvío, no a la dirección IP del cliente AAA de origen.
- **Si utiliza RADIUS:** los campos NAR enumerados utilizan estos valores:**Ciente AAA:** se utiliza `NAS-IP-address` (atributo 4) o, si no existe `NAS-IP-address`, `NAS-identificador` (atributo RADIUS 32).**Puerto:** se utiliza el `puerto NAS` (atributo 5) o, si no existe el puerto NAS, `NAS-port-ID` (atributo 87).**CLI:** se utiliza el `call-station-ID` (atributo 31).**DNIS:** se utiliza el `identificador de estación` (atributo 30).

Cuando se especifica un NAR, se puede utilizar un asterisco (*) como comodín para cualquier valor o como parte de cualquier valor para establecer un rango. Todos los valores o condiciones de una descripción NAR deben cumplirse para que el NAR restrinja el acceso. Esto significa que los valores contienen un valor Boolean AND.

[Agregar un NAR compartido](#)

Puede crear un NAR compartido que contenga muchas restricciones de acceso. Aunque la interfaz web ACS no aplica límites al número de restricciones de acceso en un NAR compartido o a la longitud de cada restricción de acceso, debe cumplir estos límites:

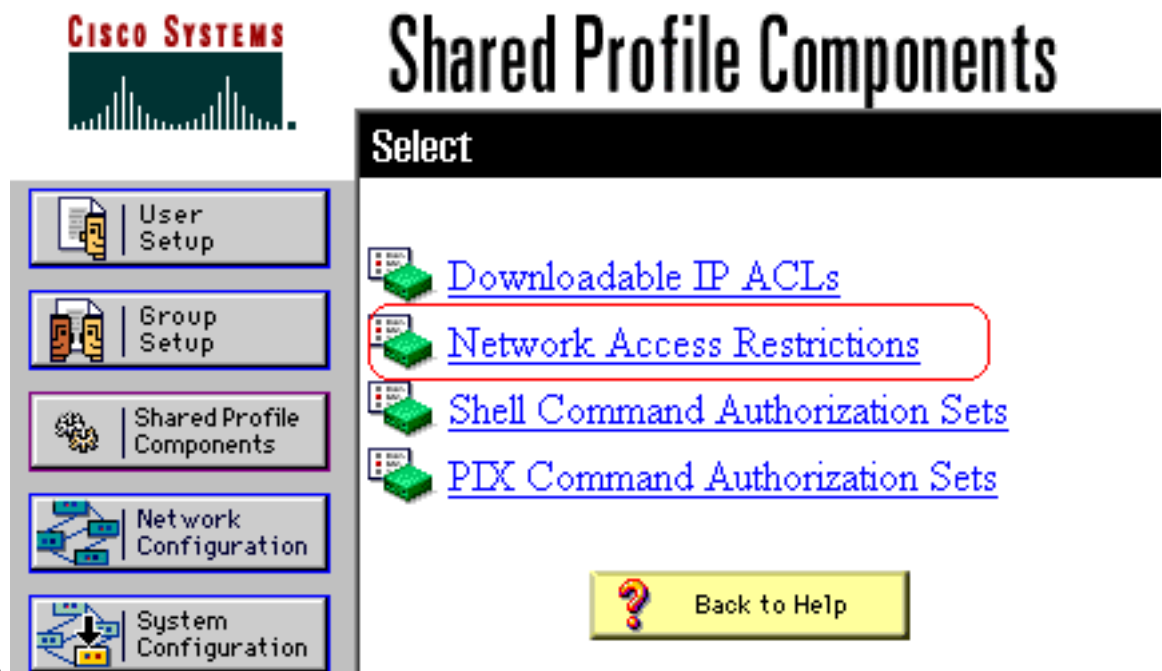
- La combinación de campos para cada elemento de línea no puede superar los 1024 caracteres.

- El NAR compartido no puede tener más de 16 KB de caracteres. El número de elementos de línea admitidos depende de la longitud de cada elemento de línea. Por ejemplo, si crea un NAR basado en CLI/DNIS donde los nombres de cliente AAA son 10 caracteres, los números de puerto son 5 caracteres, las entradas de CLI son 15 caracteres y las entradas DNIS son 20 caracteres, puede agregar 450 elementos de línea antes de alcanzar el límite de 16 KB.

Nota: Antes de definir un NAR, asegúrese de que ha establecido los elementos que pretende utilizar en ese NAR. Por lo tanto, debe haber especificado todos los NAF y NDG, y definido todos los clientes AAA relevantes, antes de convertirlos en parte de la definición NAR. Consulte la sección [Acerca de las Restricciones de Acceso a la Red](#) para obtener más información.

Complete estos pasos para agregar un NAR compartido:

1. En la barra de navegación, haga clic en **Componentes del perfil compartido**. Aparecerá la ventana Componentes del perfil



compartido.

2. Haga clic en **Restricciones de acceso a la**



Shared Profile Components

Select

User Setup

Group Setup

Shared Profile Components

Network Configuration


System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Network Access Restrictions 

Name	Description
None Defined	

Add Cancel

red.

3. Haga clic en Add (Agregar). Aparecerá la ventana Network Access Restriction (Restricción de acceso a la red).

Shared Profile Components

Network Access Restriction

Name:

Description:

Define IP-based access restrictions

Table Defines:

AAA Client	Port	Src IP Address
<input type="text"/>		

AAA Client:

Port:

Src IP Address:

Define CLI/DNIS-based access restrictions

Table Defines:

AAA Client	Port	CLI	DNIS
<input type="text"/>			

4. En el cuadro Nombre, introduzca un nombre para el nuevo NAR compartido. **Nota:** El nombre puede contener hasta 31 caracteres. No se permiten los espacios finales ni los espacios finales. Los nombres no pueden contener estos caracteres: soporte izquierdo ([), soporte derecho (]), coma (,) o barra diagonal (/).
5. En el cuadro Descripción, introduzca una descripción del nuevo NAR compartido. La descripción puede tener hasta 30 000 caracteres.
6. Si desea permitir o denegar el acceso en función del direccionamiento IP: Marque la casilla de verificación **Definir descripciones de acceso basadas en IP**. Para especificar si está enumerando direcciones que están permitidas o denegadas, en la lista Define Table, seleccione el valor aplicable. Seleccione o introduzca la información correspondiente en cada uno de estos cuadros: **Cliente AAA:** seleccione **Todos los clientes AAA**, o el nombre del NDG, o el NAF, o el cliente AAA individual, al que se permite o se niega el acceso. **Puerto:**

introduzca el número del puerto al que desea permitir o denegar el acceso. Puede utilizar el asterisco (*) como comodín para permitir o denegar el acceso a todos los puertos del cliente AAA seleccionado.**Dirección IP Src:** introduzca la dirección IP sobre la que se filtrará al aplicar restricciones de acceso. Puede utilizar el asterisco (*) como comodín para especificar todas las direcciones IP.**Nota:** El número total de caracteres de la lista de clientes AAA y los cuadros Dirección IP de puerto y servidor no debe exceder 1024. Aunque ACS acepta más de 1024 caracteres cuando agrega un NAR, no puede editar el NAR y ACS no puede aplicarlo con precisión a los usuarios.Haga clic en **Enter**.La información de cliente, puerto y dirección AAA aparece como un elemento de línea en la tabla.Repita los pasos c y d para introducir elementos de línea adicionales basados en IP.

7. Si desea permitir o denegar el acceso en función de la ubicación de la llamada o de valores distintos de las direcciones IP: Marque la casilla de verificación **Definir restricciones de acceso basadas en CLI/DNIS**. Para especificar si está enumerando las ubicaciones permitidas o denegadas en la lista de definiciones de tabla, seleccione el valor aplicable. Para especificar los clientes a los que se aplica este NAR, seleccione uno de estos valores de la lista de clientes AAA: El nombre de la DGEI nombre del cliente AAA particular Todos los clientes AAASugerencia: Solo se muestran los NDG que ya ha configurado. Para especificar la información sobre la que debe filtrarse este NAR, introduzca los valores en estos cuadros, según proceda: Sugerencia: Puede introducir un asterisco (*) como comodín para especificar **todo** como valor. Puerto: introduzca el número del puerto en el que desea filtrar. CLI: introduzca el número de CLI en el que desea filtrar. También puede utilizar este cuadro para restringir el acceso basándose en valores distintos de CLI, como una dirección IP o una dirección MAC. Consulte la sección [Acerca de las Restricciones de Acceso a la Red](#) para obtener más información. DNIS: introduzca el número al que se va a llamar para filtrar. Nota: El número total de caracteres en la lista de clientes AAA y en los cuadros Puerto, CLI y DNIS no debe exceder 1024. Aunque ACS acepta más de 1024 caracteres cuando agrega un NAR, no puede editar el NAR y ACS no puede aplicarlo con precisión a los usuarios. Haga clic en **Enter**. La información que especifica el elemento de línea NAR aparece en la tabla. Repita los pasos c a e para introducir elementos de línea NAR adicionales no basados en IP. Haga clic en **Enviar** para guardar la definición NAR compartida. ACS guarda el NAR compartido y lo enumera en la tabla **Restricciones de Acceso a la Red**.

[Editar un NAR compartido](#)

Complete estos pasos para editar un NAR compartido:

1. En la barra de navegación, haga clic en **Componentes del perfil compartido**. Aparecerá la ventana Componentes del perfil compartido.
2. Haga clic en **Restricciones de acceso a la red**. Aparece la tabla Restricciones de acceso a la red.
3. En la columna Nombre, haga clic en la NAR compartida que desee editar. Aparece la ventana Network Access Restriction (Restricción de acceso a la red), que muestra información para el NAR seleccionado.
4. Edite el nombre o la descripción del NAR, según corresponda. La descripción puede tener hasta 30 000 caracteres.
5. Para editar un elemento de línea en la tabla de restricciones de acceso basada en IP: Haga doble clic en el elemento de línea que desee editar. La información del elemento de línea se

quita de la tabla y se escribe en los cuadros de la tabla. Edite la información, según sea necesario. **Nota:** El número total de caracteres de la lista de clientes AAA y de las casillas Dirección IP de puerto y servidor no debe exceder 1024. Aunque ACS puede aceptar más de 1024 caracteres cuando agrega un NAR, no puede editar un NAR y ACS no puede aplicarlo con precisión a los usuarios. Haga clic en **Enter**. La información editada de este elemento de línea se escribe en la tabla de restricciones de acceso basadas en IP.

6. Para quitar un elemento de línea de la tabla de restricciones de acceso basada en IP: Seleccione el elemento de línea. En la tabla, haga clic en **Eliminar**. El elemento de línea se elimina de la tabla de restricciones de acceso basadas en IP.
7. Para editar un elemento de línea en la tabla de restricciones de acceso CLI/DNIS: Haga doble clic en el elemento de línea que desee editar. La información del elemento de línea se quita de la tabla y se escribe en los cuadros de la tabla. Edite la información, según sea necesario. **Nota:** El número total de caracteres en la lista de clientes AAA y en los cuadros Puerto, CLI y DNIS no debe exceder 1024. Aunque ACS puede aceptar más de 1024 caracteres cuando agrega un NAR, no puede editar un NAR y ACS no puede aplicarlo con precisión a los usuarios. Haga clic en **Enter**. La información editada para este elemento de línea se escribe en la tabla de restricciones de acceso CLI/DNIS.
8. Para quitar un elemento de línea de la tabla de restricciones de acceso CLI/DNIS: Seleccione el elemento de línea. En la tabla, haga clic en **Eliminar**. El elemento de línea se elimina de la tabla de restricciones de acceso CLI/DNIS.
9. Haga clic en **Enviar** para guardar los cambios que ha realizado. ACS vuelve a ingresar el filtro con la nueva información, que entra en efecto inmediatamente.

[Eliminar un NAR compartido](#)

Nota: Asegúrese de quitar la asociación de un NAR compartido a cualquier usuario o grupo antes de eliminar dicho NAR.

Complete estos pasos para eliminar un NAR compartido:

1. En la barra de navegación, haga clic en **Componentes del perfil compartido**. Aparecerá la ventana Componentes del perfil compartido.
2. Haga clic en **Restricciones de acceso a la red**.
3. Haga clic en el nombre del NAR compartido que desea eliminar. Aparece la ventana Network Access Restriction (Restricción de acceso a la red), que muestra información para el NAR seleccionado.
4. En la parte inferior de la ventana, haga clic en **Eliminar**. Un cuadro de diálogo le advierte de que va a eliminar un NAR compartido.
5. Haga clic en **Aceptar** para confirmar que desea eliminar el NAR compartido. Se elimina el NAR compartido seleccionado.

[Establecer restricciones de acceso a la red para un usuario](#)

La tabla Restricciones de acceso a la red del área Configuración avanzada de la configuración de usuario se utiliza para establecer los NAR de tres maneras:

- Aplique los NAR compartidos existentes por nombre.
- Defina restricciones de acceso basadas en IP para permitir o denegar el acceso del usuario a

un cliente AAA especificado o a puertos especificados en un cliente AAA cuando se haya establecido una conexión IP.

- Defina las restricciones de acceso basadas en CLI/DNIS para permitir o denegar el acceso del usuario en función de la CLI/DNIS que se utilice. **Nota:** También puede utilizar el área de restricciones de acceso basadas en CLI/DNIS para especificar otros valores. Consulte la sección [Restricciones de Acceso a la Red](#) para obtener más información.

Normalmente, los NARs definidos (compartidos) desde la sección Componentes compartidos permiten aplicar estas restricciones a más de un grupo o usuario. Consulte la sección [Agregar un NAR compartido](#) para obtener más información. Debe haber seleccionado la casilla de verificación **Restricciones de acceso a la red de nivel de usuario** en la página Opciones avanzadas de la sección Configuración de la interfaz para que este conjunto de opciones aparezca en la interfaz web.

Sin embargo, también puede utilizar ACS para definir y aplicar un NAR para un único usuario desde la sección User Setup (Configuración de usuario). Debe haber habilitado la configuración **Restricciones de acceso a la red de nivel de usuario** en la página Opciones avanzadas de la sección Configuración de la interfaz para que aparezcan las opciones de filtro basadas en IP de un solo usuario y las opciones de filtro basadas en CLI/DNIS de un solo usuario para que aparezcan en la interfaz web.

Nota: Cuando un proxy reenvía una solicitud de autenticación a un ACS, cualquier NAR para solicitudes del sistema de control de acceso del controlador de acceso de terminal (TACACS+) se aplica a la dirección IP del servidor AAA de reenvío, no a la dirección IP del cliente AAA de origen.

Cuando crea restricciones de acceso por usuario, ACS no aplica límites al número de restricciones de acceso y no aplica un límite a la longitud de cada restricción de acceso. Sin embargo, hay límites estrictos:

- La combinación de campos para cada elemento de línea no puede superar los 1024 caracteres de longitud.
- El NAR compartido no puede tener más de 16 KB de caracteres. El número de elementos de línea admitidos depende de la longitud de cada elemento de línea. Por ejemplo, si crea un NAR basado en CLI/DNIS donde los nombres de cliente AAA son 10 caracteres, los números de puerto son 5 caracteres, las entradas de CLI son 15 caracteres y las entradas DNIS son 20 caracteres, puede agregar 450 elementos de línea antes de alcanzar el límite de 16 KB.

Complete estos pasos para configurar los NAR para un usuario:

1. Realice los pasos 1 a 3 de [Adición de una Cuenta de Usuario Básica](#). Se abre la ventana User Setup Edit (Editar configuración de usuario). El nombre de usuario que agrega o edita aparece en la parte superior de la ventana.

User Setup

Advanced Settings

Network Access Restrictions (NAR)

Shared Network Access Restrictions

Only Allow network access when

- All selected NARs result in permit
- Any one selected NAR results in permit

NARs

testnar

Selected NARs

--

>> <>

<< >>

View IP NAR

View CLI/DNIS NAR

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client: All AAA Clients

Port:

Address:

Submit

Delete

Cancel

2. Para aplicar un NAR compartido previamente configurado a este usuario:**Nota:** Para aplicar un NAR compartido, debe haberlo configurado en Restricciones de acceso a la red en la sección Componentes del perfil compartido. Consulte la sección [Agregar un NAR compartido](#) para obtener más información. Marque la **casilla de verificación Permitir acceso a la red solamente cuando**. Para especificar si uno o todos los NAR compartidos deben solicitar el acceso del usuario, seleccione uno, según corresponda: Todos los NARS seleccionados dan

como resultado permiso. Cualquier NAR seleccionado da como resultado el permiso. Seleccione un nombre NAR compartido en la lista NAR y, a continuación, haga clic en → (botón de flecha derecha) para mover el nombre a la lista NAR seleccionados. **Sugerencia:** Para ver los detalles del servidor de los NAR compartidos que ha seleccionado aplicar, puede hacer clic en **Ver NAR IP** o **Ver CLID/DNIS NAR**, según corresponda.

3. Para definir y aplicar un NAR, para este usuario en particular, que permita o deniegue este acceso de usuario basado en la dirección IP, o dirección IP y puerto: **Nota:** Debe definir la mayoría de los NAR desde la sección Componentes compartidos para poder aplicarlos a más de un grupo o usuario. Consulte la sección [Agregar un NAR compartido](#) para obtener más información. En la tabla Restricciones de acceso a la red, en Restricciones de acceso a la red definidas por el usuario, marque la casilla de verificación **Definir restricciones de acceso basadas en IP**. Para especificar si el listado posterior especifica direcciones IP permitidas o denegadas, en la lista de definiciones de tabla, elija una: **Llamadas permitidas/ubicaciones de punto de acceso** **Ubicaciones de punto de acceso/llamadas denegadas**. Seleccione o introduzca la información en estos cuadros: **Cliente AAA:** seleccione **Todos los clientes AAA**, o el nombre de un grupo de dispositivos de red (NDG), o el nombre del cliente AAA individual, al que permitir o denegar el acceso. **Puerto:** introduzca el número del puerto al que desea permitir o denegar el acceso. Puede utilizar el asterisco (*) como comodín para permitir o denegar el acceso a todos los puertos del cliente AAA seleccionado. **Dirección:** introduzca la dirección IP o las direcciones que desea utilizar al realizar las restricciones de acceso. Puede utilizar el asterisco (*) como comodín. **Nota:** El número total de caracteres en la lista de clientes AAA y las casillas Dirección IP de puerto y servidor no debe exceder de 1024. Aunque ACS acepta más de 1024 caracteres cuando agrega un NAR, no puede editar el NAR y ACS no puede aplicarlo con precisión a los usuarios. Haga clic en **Enter**. La información de cliente, puerto y dirección AAA especificada aparece en la tabla sobre la lista de clientes AAA.
4. Para permitir o denegar este acceso de usuario en función de la ubicación de la llamada o de valores distintos de una dirección IP establecida: Marque la casilla de verificación **Definir restricciones de acceso basadas en CLI/DNIS**. Para especificar si el listado posterior especifica los valores permitidos o denegados, en la lista Defina la tabla, elija uno: **Llamadas permitidas/ubicaciones de punto de acceso** **Ubicaciones de punto de acceso/llamadas denegadas**. Complete los cuadros como se muestra: **Nota:** Debe introducir una entrada en cada cuadro. Puede utilizar el asterisco (*) como comodín para todo o parte de un valor. El formato que utilice debe coincidir con el formato de la cadena que recibe de su cliente AAA. Puede determinar este formato desde el registro de cuentas RADIUS. **Cliente AAA:** seleccione **Todos los Clientes AAA**, o el nombre del NDG, o el nombre del cliente AAA individual, al que se permite o se deniega el acceso. **PORT:** introduzca el número del puerto al que desea permitir o denegar el acceso. Puede utilizar el asterisco (*) como comodín para permitir o denegar el acceso a todos los puertos. **CLI:** introduzca el número de CLI al que desea permitir o denegar el acceso. Puede utilizar el asterisco (*) como comodín para permitir o denegar el acceso en función de parte del número. **Sugerencia:** Utilice la entrada CLI si desea restringir el acceso basándose en otros valores como una dirección MAC de Cisco Aironet Client. Consulte la sección [Acerca de las Restricciones de Acceso a la Red](#) para obtener más información. **DNIS:** introduzca el número DNIS al que desea permitir o denegar el acceso. Utilice esta entrada para restringir el acceso en función del número al que el usuario marcará. Puede utilizar el asterisco (*) como comodín para permitir o denegar el acceso en función de parte del número. **Sugerencia:** Use la selección DNIS si desea

restringir el acceso basándose en otros valores como una dirección MAC de Cisco Aironet AP. Consulte la sección [Acerca de las Restricciones de Acceso a la Red](#) para obtener más información. **Nota:** El número total de caracteres en la lista AAA Client y en las casillas **Port**, **CLI** y **DNIS** no debe exceder de 1024. Aunque ACS acepta más de 1024 caracteres cuando agrega un NAR, no puede editar el NAR y ACS no puede aplicarlo con precisión a los usuarios. Haga clic en **Enter**. La información que especifica el cliente AAA, puerto, CLI y DNIS aparece en la tabla sobre la lista de clientes AAA.

5. Si ha terminado de configurar las opciones de cuenta de usuario, haga clic en **Enviar** para registrar las opciones.

[Establecer restricciones de acceso a la red para un grupo de usuarios](#)

La tabla Restricciones de acceso a la red de la Configuración de grupo se utiliza para aplicar NAR de tres maneras distintas:

- Aplique los NAR compartidos existentes por nombre.
- Defina restricciones de acceso de grupo basadas en IP para permitir o denegar el acceso a un cliente AAA especificado o a puertos especificados en un cliente AAA cuando se haya establecido una conexión IP.
- Defina los NAR de grupo basados en CLI/DNIS para permitir o denegar el acceso al número CLI o al número DNIS utilizado. **Nota:** También puede utilizar el área de restricciones de acceso basadas en CLI/DNIS para especificar otros valores. Consulte la sección [Acerca de las Restricciones de Acceso a la Red](#) para obtener más información.

Normalmente, los NARs definidos (compartidos) desde la sección Componentes compartidos se pueden aplicar a más de un grupo o usuario. Consulte la sección [Agregar un NAR compartido](#) para obtener más información. Debe marcar la casilla de verificación **Group-Level Shared Network Access Restriction** en la página **Opciones Avanzadas** de la sección Configuración de la Interfaz para que estas opciones aparezcan en la interfaz web ACS.

Sin embargo, también puede utilizar ACS para definir y aplicar un NAR para un único grupo desde la sección **Configuración de grupo**. Debe verificar la configuración de **Restricción de Acceso a la Red de Nivel de Grupo** en la página Opciones Avanzadas de la sección Configuración de la Interfaz para que aparezcan las opciones de filtro basadas en IP de un solo grupo y las opciones de filtro basadas en CLI/DNIS de un solo grupo en la interfaz web ACS.

Nota: Cuando un proxy reenvía una solicitud de autenticación a un servidor ACS, cualquier NAR para solicitudes RADIUS se aplica a la dirección IP del servidor AAA de reenvío, no a la dirección IP del cliente AAA de origen.

Complete estos pasos para configurar los NAR para un grupo de usuarios:

1. En la barra de navegación, haga clic en **Group Setup**. Se abre la ventana Selección de configuración de grupo.
2. En la lista Grupo, seleccione un grupo y, a continuación, haga clic en **Editar configuración**. El nombre del grupo aparece en la parte superior de la ventana Configuración de grupo.

