

Secure ACS - NAR met AAA-clients voor gebruikers en gebruikersgroepen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Netwerktoegangsbeperkingen](#)

[Over toegangsbeperkingen voor netwerken](#)

[Een gedeelde NAR toevoegen](#)

[Een gedeelde NAR bewerken](#)

[Een gedeelde NAR verwijderen](#)

[Netwerktoegangsbeperkingen voor een gebruiker instellen](#)

[Netwerktoegangsbeperkingen voor een gebruikersgroep instellen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u de Netwerktoegangsbeperkingen (NAR) kunt configureren in Cisco Secure Access Control Server (ACS) 4.x-versie met AAA-clients (inclusief routers, PIX, ASA, draadloze controllers) voor gebruikers en gebruikersgroepen.

[Voorwaarden](#)

[Vereisten](#)

Dit document wordt gemaakt met de aanname dat Cisco Secure ACS en AAA-clients zijn geconfigureerd en correct werken.

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op Cisco Secure ACS 3.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

[Conventies](#)

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\)](#) voor meer informatie over documentconventies.

Netwerktogangsbeperkingen

In deze sectie worden NAR's beschreven en worden gedetailleerde instructies gegeven om gedeelde NAR's te configureren en te beheren.

Deze sectie bevat deze onderwerpen:

- [Over toegangsbeperkingen voor netwerken](#)
- [Een gedeelde NAR toevoegen](#)
- [Een gedeelde NAR bewerken](#)
- [Een gedeelde NAR verwijderen](#)

Over toegangsbeperkingen voor netwerken

Een NAR is een definitie, die u in ACS maakt, van extra voorwaarden waaraan u moet voldoen alvorens een gebruiker tot het netwerk kan toegang hebben. ACS past deze voorwaarden toe door informatie van eigenschappen te gebruiken die uw AAA cliënten verzenden. Hoewel u op verschillende manieren NAR's kunt instellen, zijn alle gebaseerd op matchingstoewijzingsinformatie die een AAA-client verstuurt. Daarom moet u het formaat en de inhoud van de eigenschappen begrijpen die uw AAA cliënten verzenden als u effectieve NARs wilt gebruiken.

Wanneer u een NAR instelt, kunt u kiezen of het filter positief of negatief werkt. In de NAR specificeert u of u netwerktoegang wilt toestaan of weigeren, gebaseerd op informatie die van AAA-klanten is verstuurd in vergelijking met de informatie die in de NAR is opgeslagen. Echter, als een NAR niet genoeg informatie om te opereren tegenkomt, blijft het standaard toegang ontzegd. In deze tabel worden deze voorwaarden weergegeven:

	IP-gebaseerd	Niet-IP gebaseerd	Onvoldoende informatie
vergunning	Toegelaten toegang	Toegang geweigerd	Toegang geweigerd
ontkennen	Toegang geweigerd	Toegelaten toegang	Toegang geweigerd

ACS ondersteunt twee soorten NAR-filters:

- **IP-gebaseerde filters**-IP-gebaseerde NAR filters beperken de toegang op basis van de IP-adressen van de eindgebruiker client en de AAA-client. Zie het [gedeelte About IP-gebaseerde NAR filters](#) voor meer informatie.
- **Niet-IP-gebaseerde filters** - Niet-IP-gebaseerde NAR filters beperken toegang gebaseerd op eenvoudige string vergelijking van een waarde verzonden van de AAA client. De waarde kan het CLI-nummer (Call Line Identification Service), het DNIS-nummer (Dited Number Identification Service), het MAC-adres of een andere waarde zijn die afkomstig is van de client. Om dit type van NAR in werking te kunnen stellen moet de waarde in de NAR beschrijving precies overeenkomen wat van de cliënt wordt verzonden, die welke formaat ook

wordt gebruikt omvat. Het telefoonnummer (217) 555-4534 komt bijvoorbeeld niet overeen met 217-555-4534. Zie het gedeelte [Over niet-IP-gebaseerde NAR-filters](#) voor meer informatie.

U kunt een NAR definiëren voor een specifieke gebruiker of gebruikersgroep en deze toepassen op een bepaalde gebruiker of gebruikersgroep. Zie de [beperkingen voor netwerktoegang voor een gebruiker instellen](#) of [Netwerktoegangsbeperkingen instellen voor een gebruikersgroep](#) voor meer informatie. In het gedeelte Shared Profile Componenten van ACS kunt u echter een gedeelde NAR maken en benoemen zonder direct een gebruiker of gebruikersgroep te bellen. U geeft de gedeelde NAR een naam die in andere delen van de ACS web interface kan worden vermeld. Wanneer u gebruikers of gebruikersgroepen instelt, kunt u vervolgens geen, één of meerdere gedeelde beperkingen selecteren die moeten worden toegepast. Wanneer u de toepassing van meerdere gedeelde NAR's op een gebruiker of gebruikersgroep specificeert, kiest u een van de twee toegangscriteria:

- Alle geselecteerde filters moeten dit toestaan.
- Een geselecteerd filter moet toestemming geven.

U moet de volgorde van voorrang begrijpen die gerelateerd is aan de verschillende typen NAR's. Dit is de volgorde van NAR-filtering:

1. Gedeeld NAR op gebruikersniveau
2. Gedeeld NAR op groepsniveau
3. Niet-gedeelde NAR op gebruikersniveau
4. Niet-gedeelde NAR op groepsniveau

U zou ook moeten begrijpen dat **het weigeren van toegang op om het even welk niveau voorrang heeft op instellingen op een ander niveau die de toegang niet ontzeggen**. Dit is de enige uitzondering in ACS op de regel dat de instellingen van het gebruikersniveau de instellingen van het groepsniveau overschrijven. Een bepaalde gebruiker kan bijvoorbeeld geen NAR-beperkingen op het gebruikersniveau hebben die van toepassing zijn. Als die gebruiker echter behoort tot een groep die is beperkt door een gedeeld of niet-gedeeld NAR, wordt de gebruiker de toegang geweigerd.

Gedeelde NAR's worden in de ACS-interne gegevensbank bewaard. U kunt de ACS back-up gebruiken en de functies herstellen om een back-up te maken en ze te herstellen. U kunt de gedeelde NARs, samen met andere configuraties, ook repliceren naar secundaire ACSs.

[Over IP-gebaseerde NAR-filters](#)

Voor IP-gebaseerde NAR-filters gebruikt ACS de eigenschappen zoals weergegeven, die afhankelijk zijn van het AAA-protocol van de verificatieaanvraag:

- **Als u TACACS+**—het `rem_addr` veld van het TACACS+ startpakket gebruikt wordt gebruikt. **Opmerking:** Wanneer een verificatieaanvraag bij volmacht aan een ACS wordt doorgestuurd, worden alle NAR's voor TACACS+-verzoeken toegepast op het IP-adres van de verzendende AAA-server, niet op het IP-adres van de oorspronkelijke AAA-client.
- **Als u RADIUS IETF gebruikt**, moet de `roeping-station-id` (eigenschap 31) worden gebruikt. **Opmerking:** IP-gebaseerde NAR-filters werken alleen als ACS de eigenschap Radius Calling-ID (31) ontvangt. De geroepen-Station-ID (31) moet een geldig IP-adres bevatten. Indien dit niet het geval is, valt het onder de DNIS - regels.

AAA-klienten die niet voldoende IP-adresinformatie leveren (bijvoorbeeld bepaalde typen firewall) ondersteunen geen volledige NAR-functionaliteit.

Andere eigenschappen voor **IP-gebaseerde** beperkingen, per protocol, omvatten de NAR velden zoals aangegeven:

- **Als u TACACS+**—de NAR-velden in ACS gebruikt, gebruiken u deze waarden:**AAA client**—Het NAS-IP-adres is afkomstig van het bronadres in de socket tussen ACS en de TACACS+ client.**Port**—Het poortveld wordt van de TACACS+ beginpakketentiteit gehaald.

[Over niet-IP-gebaseerde NAR-filters](#)

Een niet-IP-gebaseerd NAR-filter (dwz, een op DNIS/CLI gebaseerd NAR-filter) is een lijst van toegestane of ontkende aanroep of punt van toegangslocaties die u kunt gebruiken om een AAA-client te beperken wanneer u geen gevestigde IP-gebaseerde verbinding hebt. De niet-IP-gebaseerde NAR optie gebruikt over het algemeen het CLI-nummer en het DNIS-nummer.

Wanneer u echter een IP-adres invoert in plaats van de CLI, kunt u het niet-IP-gebaseerde filter gebruiken; zelfs wanneer de AAA-client geen Cisco IOS® software release gebruikt die CLI of DNIS ondersteunt. In een andere uitzondering om een CLI in te voeren, kunt u een MAC adres in gaan om toegang toe te staan of te ontkennen. Bijvoorbeeld, wanneer u een Cisco Aironet AAA client gebruikt. Evenzo kunt u het Cisco Aironet AP MAC-adres in plaats van de DNIS invoeren. Het formaat van wat u in het CLI vakje—CLI, IP adres of MAC adres opgeeft moet overeenkomen met het formaat van wat u van uw AAA-client ontvangt. U kunt deze indeling bepalen aan de hand van uw RADIUS-accounting logboek.

Eigenschappen voor op DNIS/CLI gebaseerde beperkingen, per protocol, omvatten de NAR velden zoals aangegeven:

- **Als u TACACS+**—de vermelde NAR-velden gebruiken deze waarden:**AAA client**—Het `NAS-IP-adres` is afkomstig van het bronadres in de socket tussen ACS en de TACACS+ client.**Port**—het poortveld in het TACACS+ startpakket wordt gebruikt.**CLI**—Het veld `rem-adres` in het pakketvak TACACS+ wordt gebruikt.**DNIS**—Het `rem-adres` veld `dat` van de TACACS+ startpakketinstelling is genomen, wordt gebruikt. In gevallen waarin de zakelijke gegevens met de slash (/) beginnen, bevat het DNIS - veld de zakelijke gegevens zonder de slash (/).**Opmerking:** Wanneer een verificatieaanvraag bij volmacht aan een ACS wordt doorgestuurd, worden alle NAR's voor TACACS+-verzoeken toegepast op het IP-adres van de verzendende AAA-server, niet op het IP-adres van de oorspronkelijke AAA-client.
- **Als u RADIUS gebruikt:** in de lijst NAR-velden worden deze waarden gebruikt:**AAA client**—Het `NAS-IP-adres` (eigenschap 4) of, indien `NAS-IP-adres` niet bestaat, `NAS-identificer` (RADIUS-kenmerk 32) wordt gebruikt.**Port**—De `NAS-poort` (eigenschap 5) of, als `NAS-poort` niet bestaat, `NAS-Port-ID` (eigenschap 87) wordt gebruikt.**CLI**—De `call-station-ID` (eigenschap 31) wordt gebruikt.**DNIS**—De `naam-station-ID` (eigenschap 30) wordt gebruikt.

Wanneer u een NAR specificeert, kunt u een sterretje (*) gebruiken als een jokerteken voor elke waarde, of als onderdeel van een waarde om een bereik in te stellen. Aan alle waarden of voorwaarden in een NAR beschrijving moet zijn voldaan opdat de NAR de toegang beperkt. Dit betekent dat de waarden een Booleaans EN bevatten.

[Een gedeelde NAR toevoegen](#)

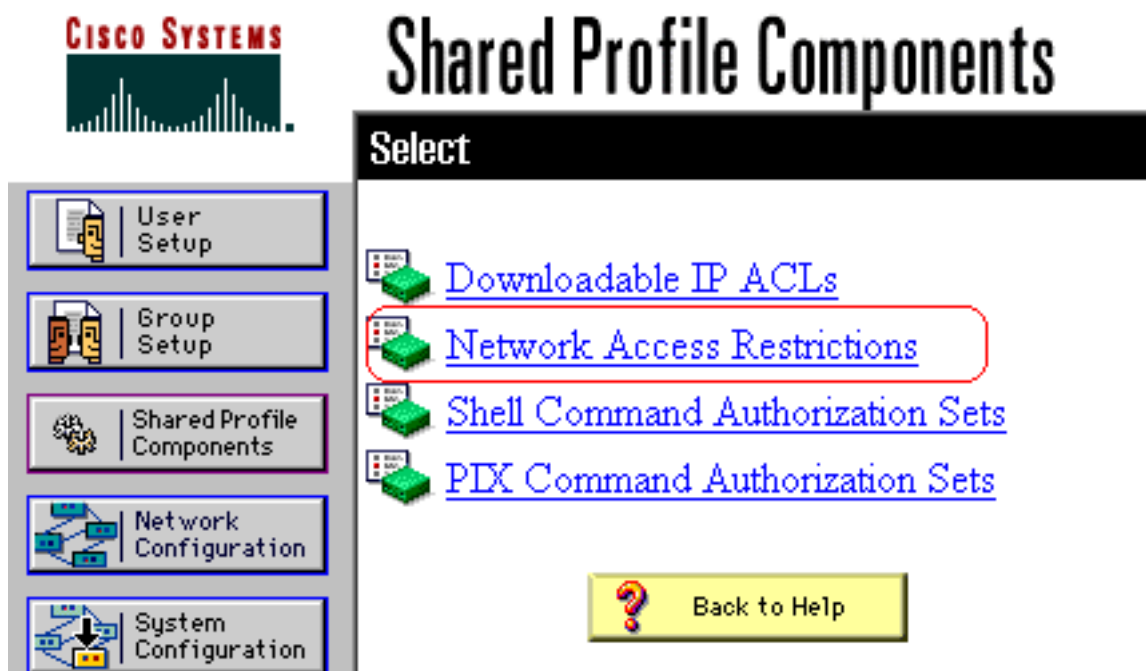
U kunt een gedeelde NAR maken die veel toegangsbeperkingen bevat. Hoewel de ACS web interface geen beperkingen van het aantal toegangsbeperkingen in een gedeelde NAR of de lengte van elke toegangsbeperking afdwingt, moet u deze beperkingen in acht nemen:

- De combinatie van velden voor elk lijnitem kan niet meer dan 1024 tekens bevatten.
- De gedeelde NAR kan niet meer dan 16 KB tekens hebben. Het aantal ondersteunde lijnitems is afhankelijk van de lengte van elk lijnitem. Als u bijvoorbeeld een op CLI/DNIS gebaseerde NAR maakt waar de AAA-clientnamen 10 tekens zijn, zijn de poortnummers 5 tekens, zijn de CLI-waarden 15 tekens en zijn de DNIS-waarden 20 tekens, dan kunt u 450 lijnitems toevoegen voordat u de 16 KB-limiet bereikt.

Opmerking: Voordat u een NAR definieert, moet u ervoor zorgen dat u de elementen hebt vastgesteld die u in die NAR wilt gebruiken. Daarom moet u alle NAF's en NDG's hebben opgegeven en alle relevante AAA-klienten hebben gedefinieerd, voordat u ze deel uitmaakt van de NAR-definitie. Zie het gedeelte [Over netwerktoegangsbeperkingen](#) voor meer informatie.

Voltooi deze stappen om een gedeelde NAR toe te voegen:

1. Klik in de navigatiebalk op **Gedeelde profielen**. Het venster Shared Profile Componenten




verschijnt.

2. Klik op **Netwerktoegangsbeperkingen**.



Shared Profile Components

Select

Network Access Restrictions 

Name	Description
None Defined	

Add Cancel

3. Klik op **Add** (Toevoegen). Het venster Network Access Bepertion verschijnt.

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. Typ in het vak Naam een naam voor de nieuwe gedeelde NAR. **Opmerking:** de naam kan maximaal 31 tekens bevatten. Leden en verplaatsen zijn niet toegestaan. De namen kunnen deze tekens niet bevatten: linkerbeugel (()), rechterbeugel (]), komma (,) of slash (/).
5. Typ in het vak Description een beschrijving van de nieuwe gedeelde NAR. De beschrijving kan maximaal 30.000 tekens bevatten.
6. Als u toegang wilt toestaan of ontkennen op basis van IP-adressering: Schakel het vakje **voor IP-gebaseerde toegangsbeschrijvingen** in. Om te specificeren of u adressen opslaat die zijn toegestaan of geweigerd, selecteert u in de lijst Tabeldefinities de toepasbare waarde. Selecteer de gewenste informatie in elk van deze vakjes of voer deze in: **AAA-client**—Selecteer **Alle AAA-clients**, of de naam van de NDG, of de NAF, of de individuele AAA-client, waartoe de toegang is toegestaan of geweigerd. **Port**—Voer het nummer in van de poort waar u de toegang wilt toestaan of weigeren. U kunt het sterretje (*) gebruiken als een

jokerteken om toegang tot alle poorten op de geselecteerde AAA-client mogelijk te maken of te weigeren. **SRC IP-adres**—Voer het IP-adres in om te filteren bij het uitvoeren van toegangsbeperkingen. U kunt de asterisk (*) gebruiken als een jokerteken om alle IP adressen te specificeren. **Opmerking:** het totale aantal tekens in de AAA-clientlijst en de selectievakjes in Port- en SRC-IP mogen niet hoger zijn dan 1024. Alhoewel ACS meer dan 1024 tekens accepteert wanneer u een NAR toevoegt, kunt u NAR niet bewerken en ACS kan het niet accuraat op gebruikers toepassen. Klik op **ENTER**. De AAA-client, poort en adresinformatie verschijnen als een lijnitem in de tabel. Herhaal stappen c en d om extra IP-gebaseerde lijnpunten in te voeren.

- Als u toegang wilt toestaan of ontkennen gebaseerd op het roepen van plaats of waarden anders dan IP adressen: Controleer het aanvinkvakje op **CLI/DNIS gebaseerde toegangsbeperkingen**. Om te specificeren of u locaties opslaat die al dan niet zijn toegestaan in de lijst Tabeldefinities, selecteert u de toepasbare waarde. Om de klanten te specificeren waarop deze NAR van toepassing is, selecteert u een van deze waarden in de AAA-clientlijst: De naam van de NDG De naam van de specifieke AAA-client Alle AAA-klanten **Tip:** Alleen NDG's die u al hebt ingesteld, worden in de lijst opgenomen. Om de informatie te specificeren waarop deze NAR moet filteren, moet u waarden in deze vakjes invoeren, zoals van toepassing: **Tip:** U kunt een sterretje (*) als een jokerteken invoeren om **alle** als waarde te specificeren. **Port**-Voer het aantal poorten in waarop u wilt filteren. **CLI** - Voer het CLI-nummer in waarop u wilt filteren. U kunt dit vakje ook gebruiken om toegang te beperken op basis van waarden anders dan CLIs, zoals een IP-adres of MAC-adres. Zie het gedeelte [Over netwerktoegangsbeperkingen](#) voor meer informatie. **DNIS**-Voer het nummer in dat wordt ingedrukt om naar te filteren. **Opmerking:** het totale aantal tekens in de AAA-clientlijst en de dozen Port, CLI en DNIS mogen niet groter zijn dan 1024. Alhoewel ACS meer dan 1024 tekens accepteert wanneer u een NAR toevoegt, kunt u NAR niet bewerken en ACS kan het niet accuraat op gebruikers toepassen. Klik op **ENTER**. De informatie die de NAR lijnoptie specificeert verschijnt in de tabel. Herhaal stappen c tot en met e om extra niet op IP gebaseerde NAR lijnpunten in te voeren. Klik op **Inzenden** om de gedeelde NAR-definitie op te slaan. ACS slaat de gedeelde NAR op en maakt deze op in de tabel **Netwerktoegangsbeperkingen**.

Een gedeelde NAR bewerken

Voltooi deze stappen om een gedeeld NAR te bewerken:

- Klik in de navigatiebalk op **Gedeelde profielen**. Het venster Shared Profile Componenten verschijnt.
- Klik op **Netwerktoegangsbeperkingen**. De tabel met netwerktoegangsbeperkingen verschijnt.
- Klik in de kolom Naam op het gedeelde NAR dat u wilt bewerken. Het venster Network Access Beperktion verschijnt en geeft informatie voor de geselecteerde NAR weer.
- Bewerk de naam of beschrijving van de NAR, naar gelang van toepassing. De beschrijving kan maximaal 30.000 tekens bevatten.
- Zo bewerkt u een regelitem in de tabel met IP-gebaseerde toegangsbeperkingen: Dubbelklik op het lijnitem dat u wilt bewerken. Informatie voor het lijnitem wordt uit de tabel verwijderd en naar de vakjes onder de tabel geschreven. Bewerk de informatie indien nodig. **Opmerking:** het totale aantal tekens in de AAA-clientlijst en de dialoogvensters Port- en SRC-IP-adres mogen niet hoger zijn dan 1024. Alhoewel ACS meer dan 1024 tekens kan accepteren wanneer u een NAR toevoegt, kunt u dergelijke NAR niet bewerken en ACS kan het niet accuraat op

gebruikers toepassen. Klik op **ENTER**. De bewerkte informatie voor dit lijnitem wordt geschreven naar de op IP gebaseerde access-beperkingen tabel.

6. Zo verwijdert u een lijnitem uit de op IP gebaseerde tabel met toegangsbeperkingen: Selecteer de optie Lijn. Klik onder de tabel op **Verwijderen**. Het lijnitem wordt verwijderd uit de tabel met IP-gebaseerde toegangsbeperkingen.
7. Zo bewerkt u een regelitem in de tabel met CLI/DNIS-toegangsbeperkingen: Dubbelklik op het lijnitem dat u wilt bewerken. Informatie voor het lijnitem wordt uit de tabel verwijderd en naar de vakjes onder de tabel geschreven. Bewerk de informatie indien nodig. **Opmerking:** het totale aantal tekens in de AAA-clientlijst en de dozen Port, CLI en DNIS mogen niet groter zijn dan 1024. Alhoewel ACS meer dan 1024 tekens kan accepteren wanneer u een NAR toevoegt, kunt u dergelijke NAR niet bewerken en ACS kan het niet accuraat op gebruikers toepassen. Klik op **ENTER**. De bewerkte informatie voor dit lijnitem wordt geschreven naar de CLI/DNIS-toegangslijst.
8. Zo verwijdert u een regelitem uit de tabel met CLI/DNIS-toegangsbeperkingen: Selecteer de optie Lijn. Klik onder de tabel op **Verwijderen**. Het lijnitem wordt verwijderd uit de tabel CLI/DNIS-toegangsbeperkingen.
9. Klik op **Inzenden** om de door u aangebrachte wijzigingen op te slaan. ACS voert het filter opnieuw in met de nieuwe informatie, die onmiddellijk van kracht wordt.

Een gedeelde NAR verwijderen

Opmerking: Zorg ervoor dat u de associatie van een gedeeld NAR naar een gebruiker of groep verwijdert voordat u de NAR verwijdert.

Voltooi deze stappen om een gedeelde NAR te verwijderen:

1. Klik in de navigatiebalk op **Gedeelde profielen**. Het venster Shared Profile Componenten verschijnt.
2. Klik op **Netwerktoegangsbeperkingen**.
3. Klik op de naam van de gedeelde NAR die u wilt verwijderen. Het venster Network Access Beperkingen verschijnt en geeft informatie voor de geselecteerde NAR weer.
4. Klik onder in het venster op **Verwijderen**. Een dialoogvenster waarschuwt u dat u een gedeeld NAR wilt verwijderen.
5. Klik op **OK** om te bevestigen dat u de gedeelde NAR wilt verwijderen. De geselecteerde gedeelde NAR wordt verwijderd.

Netwerktoegangsbeperkingen voor een gebruiker instellen

U gebruikt de tabel Netwerktoegangsbeperkingen in het gebied Geavanceerde instellingen van Gebruiker Setup om NAR's op drie manieren in te stellen:

- Pas bestaande gedeelde NARs door naam toe.
- Definieer IP-gebaseerde toegangsbeperkingen om gebruikerstoegang tot een gespecificeerde AAA-client of tot gespecificeerde poorten op een AAA-client toe te staan of te weigeren wanneer een IP-verbinding is gerealiseerd.
- Definieer op CLI/DNIS gebaseerde toegangsbeperkingen om gebruikerstoegang toe te staan of te weigeren op basis van de CLI/DNIS die wordt gebruikt. **Opmerking:** U kunt het op CLI/DNIS gebaseerde toegangsbeperkingsgebied ook gebruiken om andere waarden te

specificeren. Zie het gedeelte [Netwerktoegangsbeperkingen](#) voor meer informatie.

Meestal definieert u (gedeelde) NAR's vanuit het gedeelte Gedeelde componenten, zodat u deze beperkingen op meer dan één groep of gebruiker kunt toepassen. Zie de [sectie Gedeeld NAR toevoegen](#) voor meer informatie. U moet het dialoogvenster **Netwerktoegangsbeperkingen op gebruikersniveau** hebben geselecteerd op de pagina Geavanceerde opties van het gedeelte Interface Configuration voor deze reeks opties die in de webinterface moeten worden weergegeven.

U kunt echter ook ACS gebruiken om een NAR te definiëren en toe te passen voor één gebruiker vanuit de sectie Gebruikersinstelling. U moet de instelling **Netwerktoegangsbeperkingen op gebruikersniveau** hebben ingeschakeld op de pagina Geavanceerde opties van het vak Interfaceconfiguratie voor één gebruiker met IP-gebaseerde filteropties en in de webinterface worden één gebruiker met op CLI/DNIS gebaseerde filteropties weergegeven.

Opmerking: Wanneer een verificatieaanvraag bij volmacht naar een ACS wordt doorgestuurd, worden alle NAR's voor terminaltoegangscontroleregeling (TACACS+)-verzoeken op het IP-adres van de verzendende AAA-server toegepast, niet op het IP-adres van de oorspronkelijke AAA-client.

Wanneer u toegangsbeperkingen per gebruiker creëert, worden ACS geen beperkingen van het aantal toegangsbeperkingen opgelegd en wordt geen limiet van de lengte van elke toegangsbeperking afgedwongen. Er zijn echter strikte grenzen:

- De combinatie van velden voor elk lijnitem kan niet langer zijn dan 1024 tekens.
- De gedeelde NAR kan niet meer dan 16 KB tekens hebben. Het aantal ondersteunde lijnitems is afhankelijk van de lengte van elk lijnitem. Als u bijvoorbeeld een op CLI/DNIS gebaseerde NAR maakt waar de AAA-clientnamen 10 tekens zijn, zijn de poortnummers 5 tekens, zijn de CLI-waarden 15 tekens en zijn de DNIS-waarden 20 tekens, dan kunt u 450 lijnitems toevoegen voordat u de 16 KB-limiet bereikt.

Voltooi deze stappen om NAR's voor een gebruiker in te stellen:

1. Voer stap 1 t/m 3 uit van [een basisgebruikersaccount toevoegen](#). Het venster Gebruikersinstellingen bewerken wordt geopend. De gebruikersnaam die u toevoegt of bewerkt, verschijnt boven in het venster.

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. Zo past u een eerder ingesteld gedeeld NAR op deze gebruiker toe:**Opmerking:** om een gedeelde NAR toe te passen, moet u het onder Netwerktogangsbeperkingen in het gedeelte Gedeelde Profile Componenten hebben geconfigureerd. Zie de [sectie Gedeeld NAR toevoegen](#) voor meer informatie. Controleer het vakje **Alleen netwerk toegang verlenen**. Om te specificeren of één of alle gedeelde NAR's een aanvraag moeten indienen voor de gebruiker om toegang te krijgen, selecteert u één, zoals van toepassing: Alle

geselecteerde NARS resulteren in een licentie. Elke geselecteerde NAR levert een vergunning op. Selecteer een gedeelde NAR naam in de lijst van NAR's en klik vervolgens op -> (rechterpijlknoop) om de naam in de lijst van Geselecteerde NAR's te verplaatsen. **Tip:** u kunt de serverdetails van de gedeelde NAR's bekijken die u hebt geselecteerd om toe te passen, u kunt **IP NAR bekijken** of **CLID/DNIS NAR bekijken**, zoals van toepassing.

- Om een NAR, voor deze specifieke gebruiker te definiëren en toe te passen, die deze gebruikerstoegang op basis van IP adres, of IP adres en poort toestaat of ontkent: **Opmerking:** U dient de meeste NAR's te definiëren vanuit het gedeelte Gedeelde componenten, zodat u ze op meer dan één groep of gebruiker kunt toepassen. Zie de [sectie Gedeeld NAR toevoegen](#) voor meer informatie. In de tabel Netwerktoegangsbeperkingen, onder Beperkingen van netwerktoegang per gebruiker, controleert u het vakje **gedefinieerde IP-gebaseerde toegangsbeperkingen**. Om te specificeren of de daaropvolgende lijst toegestane of ontkende IP adressen specificeert, kiest u in de lijst Tabelgedefinieerde adressen één: **Verboden oproepen/point of access points Denied Calling/Point of Access Locaties**. Selecteer de informatie in deze vakjes of voer deze in: **AAA-client**-Selecteer **Alle AAA-clients**, of de naam van een netwerkapparaatgroep (NDG) of de naam van de afzonderlijke AAA-client, waar u toegang toe kunt geven of weigeren. **Port**-Voer het nummer in van de poort waar u de toegang kunt toestaan of weigeren. U kunt het sterretje (*) gebruiken als een jokerteken om toegang tot alle poorten op de geselecteerde AAA-client mogelijk te maken of te weigeren. **Adres**-Voer het IP adres of de adressen in om te gebruiken wanneer het uitvoeren van toegangsbeperkingen. U kunt de sterretje (*) gebruiken als een jokerteken. **Opmerking:** het totale aantal tekens in de lijst AAA-client en de selectievakjes in Port- en SRC-IP mogen niet hoger zijn dan 1024. Alhoewel ACS meer dan 1024 tekens accepteert wanneer u een NAR toevoegt, kunt u NAR niet bewerken en ACS kan het niet accuraat op gebruikers toepassen. Klik op **ENTER**. De gespecificeerde AAA-client, poort en adresinformatie verschijnt in de tabel boven de AAA-clientlijst.
- Zo verleent of ontkent u deze gebruikerstoegang op basis van een oproepende locatie of waarden anders dan een vastgesteld IP-adres: Controleer het aanvinkvakje **op CLI/DNIS gebaseerde toegangsbeperkingen**. Om te specificeren of de daaropvolgende lijst toegestane of ontkende waarden specificeert, kiest u een van de volgende waarden in de lijst Tabeldefinities: **Verboden oproepen/point of access points Denied Calling/Point of Access Locaties**. Vul de vakjes in zoals aangegeven: **Opmerking:** U moet in elk vak een aantekening maken. U kunt de asterisk (*) gebruiken als een jokerteken voor de gehele waarde of een deel daarvan. Het formaat dat u gebruikt moet overeenkomen met het formaat van de string die u van uw AAA-client ontvangt. U kunt deze indeling bepalen aan de hand van uw RADIUS-accounting logboek. **AAA-client**-Selecteer **Alle AAA-clients** of de naam van de NDG, of de naam van de afzonderlijke AAA-client, waar u de toegang kunt toestaan of weigeren. **POORT**-Voer het nummer van de poort in waar u toegang kunt toestaan of weigeren. U kunt het sterretje (*) gebruiken als een jokerteken om toegang tot alle poorten toe te staan of te weigeren. **CLI**—Voer het CLI-nummer in waarop u toegang wilt toestaan of weigeren. U kunt de asterisk (*) gebruiken als een jokerteken om toegang toe te staan of te weigeren op basis van een deel van het nummer. **Tip:** Gebruik de CLI-ingang als u de toegang wilt beperken op basis van andere waarden zoals een MAC-adres van de Cisco Aironet-client. Zie het gedeelte [Over netwerktoegangsbeperkingen](#) voor meer informatie. **DNIS**—Voer het DNIS-nummer in waar u toegang kunt toestaan of ontkennen. Gebruik deze ingang om de toegang te beperken gebaseerd op het aantal waar de gebruiker zal bellen. U kunt de asterisk (*) gebruiken als een jokerteken om toegang toe te staan of te weigeren op basis van een deel van het nummer. **Tip:** Gebruik de DNIS-selectie als u

toegang wilt beperken op basis van andere waarden zoals een Cisco Aironet AP MAC-adres. Zie het gedeelte [Over netwerktoegangsbeperkingen](#) voor meer informatie. **Opmerking:** het totale aantal tekens in de AAA-clientlijst en de boxen **Port**, **CLI** en **DNIS** mogen niet groter zijn dan 1024. Alhoewel ACS meer dan 1024 tekens accepteert wanneer u een NAR toevoegt, kunt u NAR niet bewerken en ACS kan het niet accuraat op gebruikers toepassen. Klik op **ENTER**. De informatie die de AAA-client, poort, CLI en DNIS specificieert, verschijnt in de tabel boven de AAA-clientlijst.

5. Als u klaar bent met het configureren van de gebruikersaccountopties, klikt u op **Indienen** om de opties op te nemen.

[Netwerktoegangsbeperkingen voor een gebruikersgroep instellen](#)

U gebruikt de tabel Netwerktoegangsbeperkingen in de groepsinstellingen om NAR's op drie verschillende manieren toe te passen:

- Pas bestaande gedeelde NARs door naam toe.
- Definieer IP-gebaseerde groepstoegangsbeperkingen om toegang tot een gespecificeerde AAA-client of tot gespecificeerde poorten op een AAA-client toe te staan of te weigeren wanneer een IP-verbinding is gerealiseerd.
- Definieer op CLI/DNIS gebaseerde groep NAR's om toegang te verlenen of te weigeren tot het CLI-nummer of het DNIS-nummer dat wordt gebruikt. **Opmerking:** U kunt het op CLI/DNIS gebaseerde toegangsbeperkingengebied ook gebruiken om andere waarden te specificeren. Zie het gedeelte [Over netwerktoegangsbeperkingen](#) voor meer informatie.

Meestal definieert u (gedeelde) NAR's vanuit het gedeelte Gedeelde componenten, zodat deze beperkingen op meer dan één groep of gebruiker van toepassing kunnen zijn. Zie de [sectie Gedeeld NAR toevoegen](#) voor meer informatie. U moet het aanvinkvakje **Toegang tot gedeeld netwerk op groepsniveau** controleren op de pagina **Geavanceerde opties** van het gedeelte Interface Configuration voor deze opties in de ACS-webinterface.

U kunt echter ook ACS gebruiken om een NAR te definiëren en toe te passen voor één groep vanuit de sectie **Groepsinstallatie**. U moet de instelling **Netwerktoegangsbeperking op groepsniveau** controleren onder de pagina Geavanceerde opties van de interfaceconfiguratie voor één groep IP-gebaseerde filteropties en één groep CLI/DNIS-gebaseerde filteropties die in de ACS-webinterface moeten worden weergegeven.

Opmerking: Wanneer een verificatieaanvraag bij volmacht naar een ACS-server wordt doorgestuurd, worden alle NAR's voor RADIUS-verzoeken toegepast op het IP-adres van de verzendende AAA-server, niet op het IP-adres van de oorspronkelijke AAA-client.

Voltooi deze stappen om NAR's voor een gebruikersgroep in te stellen:

1. Klik in de navigatiebalk op **Groepsinstelling**. Het venster Selectiegereedschap groepsinstellingen wordt geopend.
2. Selecteer een groep in de lijst Groep en klik vervolgens op **Instellingen bewerken**. De naam van de groep verschijnt boven in het venster Instellingen groep.

