

Secure ACS - NAR con client AAA per utenti e gruppi di utenti

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Restrizioni accesso alla rete](#)

[Informazioni sulle restrizioni di accesso alla rete](#)

[Aggiungi NAR condiviso](#)

[Modifica NAR condiviso](#)

[Eliminazione di un NAR condiviso](#)

[Impostazione delle restrizioni di accesso alla rete per un utente](#)

[Impostazione delle restrizioni di accesso alla rete per un gruppo di utenti](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare le restrizioni di accesso alla rete (NAR) in Cisco Secure Access Control Server (ACS) versione 4.x con client AAA (include router, PIX, ASA, controller wireless) per utenti e gruppi di utenti.

[Prerequisiti](#)

[Requisiti](#)

Per creare questo documento, si presume che i client Cisco Secure ACS e AAA siano configurati e funzionino correttamente.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano su Cisco Secure ACS 3.0 e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Restrizioni accesso alla rete

In questa sezione vengono descritti i NAR e vengono fornite istruzioni dettagliate per la configurazione e la gestione dei NAR condivisi.

In questa sezione vengono trattati questi argomenti:

- [Informazioni sulle restrizioni di accesso alla rete](#)
- [Aggiungi NAR condiviso](#)
- [Modifica NAR condiviso](#)
- [Eliminazione di un NAR condiviso](#)

Informazioni sulle restrizioni di accesso alla rete

Un NAR è una definizione, creata in ACS, di condizioni aggiuntive che è necessario soddisfare prima che un utente possa accedere alla rete. ACS applica queste condizioni utilizzando le informazioni provenienti dagli attributi inviati dai client AAA. Sebbene sia possibile impostare i NAR in diversi modi, tutti i NAR sono basati sulle informazioni sugli attributi corrispondenti inviate da un client AAA. Per utilizzare NAR efficaci, è quindi necessario comprendere il formato e il contenuto degli attributi inviati dai client AAA.

Quando si imposta un NAR, è possibile scegliere se il filtro deve funzionare in modo positivo o negativo. In altre parole, nel NAR si specifica se autorizzare o negare l'accesso alla rete, in base alle informazioni inviate dai client AAA rispetto alle informazioni memorizzate nel NAR. Tuttavia, se un NAR non rileva informazioni sufficienti per funzionare, per impostazione predefinita viene negato l'accesso. Nella tabella seguente vengono illustrate le seguenti condizioni:

	Basato su IP	Non basato su IP	Informazioni insufficienti
Permetti	Accesso concesso	Accesso negato	Accesso negato
Nega	Accesso negato	Accesso concesso	Accesso negato

ACS supporta due tipi di filtri NAR:

- **Filtri basati su IP:** i filtri NAR basati su IP limitano l'accesso in base agli indirizzi IP del client dell'utente finale e del client AAA. Per ulteriori informazioni, vedere la sezione [Informazioni sui filtri NAR basati su IP](#).
- **Filtri non basati su IP:** i filtri NAR non basati su IP limitano l'accesso in base al semplice confronto tra stringhe di un valore inviato dal client AAA. Il valore può essere il numero di identificazione della linea chiamante (CLI), il numero DNIS (Dialed Number Identification Service), l'indirizzo MAC o un altro valore proveniente dal client. Affinché questo tipo di NAR funzioni, il valore nella descrizione NAR deve corrispondere esattamente a quello inviato dal

client, incluso il formato utilizzato. Ad esempio, il numero di telefono (217) 555-4534 non corrisponde a 217-555-4534. Per ulteriori informazioni, vedere la sezione [Informazioni sui filtri NAR non basati su IP](#).

È possibile definire un NAR e applicarlo a un utente o gruppo di utenti specifico. Per ulteriori informazioni, vedere le sezioni [Imposta restrizioni di accesso alla rete per un utente](#) o [Imposta restrizioni di accesso alla rete per un gruppo di utenti](#). Tuttavia, nella sezione Componenti profilo condiviso di ACS è possibile creare e denominare un NAR condiviso senza citare direttamente alcun utente o gruppo di utenti. È possibile assegnare al server NAR condiviso un nome a cui è possibile fare riferimento in altre parti dell'interfaccia Web di ACS. Quando si impostano utenti o gruppi di utenti, è quindi possibile selezionare nessuna, una o più restrizioni condivise da applicare. Quando si specifica l'applicazione di più NAR condivisi a un utente o a un gruppo di utenti, è possibile scegliere uno dei due criteri di accesso riportati di seguito.

- Tutti i filtri selezionati devono consentire.
- Tutti i filtri selezionati devono consentire.

È necessario comprendere l'ordine di precedenza relativo ai diversi tipi di NAR. Questo è l'ordine del filtro NAR:

1. NAR condiviso a livello utente
2. NAR condiviso a livello di gruppo
3. NAR non condiviso a livello utente
4. NAR non condiviso a livello di gruppo

È inoltre necessario comprendere che la **negazione dell'accesso a qualsiasi livello ha la precedenza sulle impostazioni a un altro livello che non la negano**. Si tratta dell'unica eccezione in ACS alla regola per cui le impostazioni a livello utente sostituiscono le impostazioni a livello di gruppo. Ad esempio, un determinato utente potrebbe non avere restrizioni NAR a livello utente applicabili. Tuttavia, se l'utente appartiene a un gruppo limitato da un NAR condiviso o non condiviso, all'utente viene negato l'accesso.

I NAR condivisi vengono conservati nel database interno di ACS. È possibile utilizzare le funzionalità di backup e ripristino di ACS per eseguire il backup e il ripristino. È inoltre possibile replicare i NAR condivisi, insieme ad altre configurazioni, negli ACS secondari.

[Informazioni sui filtri NAR basati su IP](#)

Per i filtri NAR basati su IP, ACS utilizza gli attributi mostrati, che dipendono dal protocollo AAA della richiesta di autenticazione:

- **Se si utilizza TACACS+**— viene utilizzato il campo `rem_addr` del corpo del pacchetto iniziale TACACS+. **Nota:** quando una richiesta di autenticazione viene inoltrata da un proxy ad un ACS, tutte le NAR per le richieste TACACS+ vengono applicate all'indirizzo IP del server AAA di inoltro, non all'indirizzo IP del client AAA di origine.
- **Se si utilizza RADIUS IETF**, è necessario utilizzare `Calling-Station-id` (attributo 31). **Nota:** i filtri NAR basati su IP funzionano solo se ACS riceve l'attributo Radius Calling-Station-Id (31). Calling-Station-Id (31) deve contenere un indirizzo IP valido. In caso contrario, verrà applicata la regola DNIS.

I client AAA che non forniscono informazioni sufficienti sull'indirizzo IP (ad esempio, alcuni tipi di firewall) non supportano la funzionalità NAR completa.

Altri attributi per le restrizioni **basate su IP**, per protocollo, includono i campi NAR come mostrato:

- **Se si utilizza TACACS+**—I campi NAR in ACS utilizzano i seguenti valori:**Client AAA:** l'indirizzo IP-NAS viene ricavato dall'indirizzo di origine nel socket tra ACS e il client TACACS+.**Porta:** il campo port (porta) viene preso dal corpo del pacchetto iniziale TACACS+.

[Informazioni sui filtri NAR non basati su IP](#)

Un filtro NAR non basato su IP, ovvero un filtro NAR basato su DNIS/CLI, è un elenco di posizioni di chiamata o di punto di accesso consentite o negate che è possibile utilizzare per limitare un client AAA quando non si dispone di una connessione basata su IP stabilita. La funzione NAR non basata su IP utilizza in genere il numero CLI e il numero DNIS.

Tuttavia, quando si immette un indirizzo IP al posto della CLI, è possibile usare il filtro non basato su IP; anche quando il client AAA non usa una versione software Cisco IOS® che supporta CLI o DNIS. In un'altra eccezione all'immissione di una CLI, è possibile immettere un indirizzo MAC per autorizzare o negare l'accesso. Ad esempio, quando si usa un client Cisco Aironet AAA. Analogamente, è possibile immettere l'indirizzo MAC del Cisco Aironet AP al posto di DNIS. Il formato specificato nella casella CLI (CLI, indirizzo IP o indirizzo MAC) deve corrispondere al formato ricevuto dal client AAA. È possibile determinare questo formato dal registro di accounting RADIUS.

Gli attributi per le restrizioni basate su DNIS/CLI, per protocollo, includono i campi NAR come mostrato:

- **Se si utilizza TACACS+**—I campi NAR elencati utilizzano i seguenti valori:**Client AAA:** l'indirizzo IP-NAS viene ricavato dall'indirizzo di origine nel socket tra ACS e il client TACACS+.**Porta:** viene utilizzato il campo port nel corpo del pacchetto iniziale TACACS+.**CLI:** viene utilizzato il campo rem-addr nel corpo del pacchetto iniziale TACACS+.**DNIS**—Viene utilizzato il campo rem-addr preso dal corpo del pacchetto iniziale TACACS+. Se i dati rem-addr iniziano con la barra (/), il campo DNIS conterrà i dati rem-addr senza la barra (/).**Nota:** quando una richiesta di autenticazione viene inoltrata da un proxy ad un ACS, tutte le NAR per le richieste TACACS+ vengono applicate all'indirizzo IP del server AAA di inoltro, non all'indirizzo IP del client AAA di origine.
- **Se si utilizza RADIUS**—I campi NAR elencati utilizzano i seguenti valori:**Client AAA:** viene utilizzato l'indirizzo IP-NAS (attributo 4) o, se l'indirizzo IP-NAS non esiste, l'identificatore NAS (attributo RADIUS 32).**Porta:** la porta NAS (attributo 5) o, se la porta NAS non esiste, viene utilizzato NAS-port-ID (attributo 87).**CLI:** viene utilizzato il valore calling-station-ID (attributo 31).**DNIS** - Viene utilizzato l>ID stazione (attributo 30).

Quando si specifica un valore NAR, è possibile utilizzare un asterisco (*) come carattere jolly per qualsiasi valore o come parte di qualsiasi valore per definire un intervallo. Per limitare l'accesso, NAR deve soddisfare tutti i valori o le condizioni della descrizione NAR. Ciò significa che i valori contengono un AND booleano.

[Aggiungi NAR condiviso](#)

È possibile creare un NAR condiviso che contenga molte limitazioni di accesso. Anche se l'interfaccia Web di ACS non impone limiti al numero di restrizioni di accesso in un NAR condiviso o alla lunghezza di ciascuna restrizione di accesso, è necessario rispettare questi limiti:

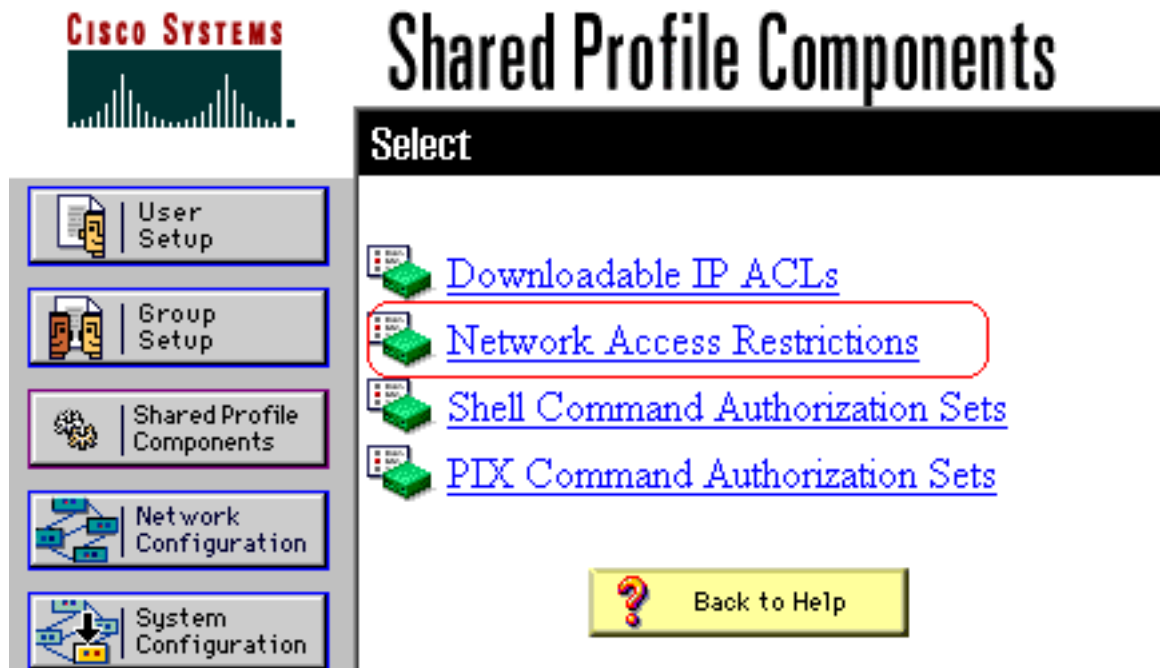
- La combinazione di campi per ogni voce non può superare i 1024 caratteri.
- Il NAR condiviso non può contenere più di 16 KB di caratteri. Il numero di righe supportate

dipende dalla lunghezza di ogni riga. Ad esempio, se si crea un NAR basato su CLI/DNIS in cui i nomi dei client AAA sono costituiti da 10 caratteri, i numeri di porta sono 5 caratteri, le voci CLI sono 15 caratteri e le voci DNIS sono 20 caratteri, è possibile aggiungere 450 righe prima di raggiungere il limite di 16 KB.

Nota: prima di definire un NAR, accertarsi di aver definito gli elementi che si desidera utilizzare in tale NAR. Pertanto, è necessario aver specificato tutti i NAF e gli NDG e aver definito tutti i client AAA rilevanti prima di renderli parte della definizione NAR. Per ulteriori informazioni, vedere la sezione [Informazioni sulle restrizioni di accesso alla rete](#).

Per aggiungere un NAR condiviso, completare i seguenti passaggi:

1. Nella barra di spostamento fare clic su **Componenti profilo condiviso**. Viene visualizzata la finestra Componenti profilo




condiviso.

2. Fare clic su **Restrizioni accesso alla**



Shared Profile Components

Select

Network Access Restrictions 

Name	Description
None Defined	

Add Cancel

rete.

3. Fare clic su **Add**.Viene visualizzata la finestra Limitazione accesso alla rete.

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"/>			

- Nella casella Nome immettere un nome per il nuovo NAR condiviso. **Nota:** il nome può contenere un massimo di 31 caratteri. Gli spazi iniziali e finali non sono consentiti. I nomi non possono contenere i caratteri seguenti: parentesi quadra aperta ([), parentesi quadra chiusa (]), virgola (,) o barra (/).
- Nella casella Descrizione immettere una descrizione del nuovo NAR condiviso. La descrizione può contenere un massimo di 30.000 caratteri.
- Per autorizzare o negare l'accesso in base all'indirizzo IP: Selezionare la casella di controllo **Definisci descrizioni accesso basato su IP**. Per specificare se elencare gli indirizzi consentiti o negati, selezionare il valore applicabile nell'elenco Definizioni tabella. Selezionare o immettere le informazioni applicabili in ciascuna di queste caselle: **Client AAA:** selezionare **Tutti i client AAA**, oppure il nome del NDG, del NAF o del singolo client AAA a cui è consentito o negato l'accesso. **Porta:** immettere il numero della porta per la quale si desidera

autorizzare o negare l'accesso. È possibile utilizzare l'asterisco (*) come carattere jolly per consentire o negare l'accesso a tutte le porte sul client AAA selezionato.**Src IP Address:** immettere l'indirizzo IP da utilizzare come filtro quando si applicano le restrizioni di accesso. È possibile utilizzare l'asterisco (*) come carattere jolly per specificare tutti gli indirizzi IP.**Nota:** il numero totale di caratteri nell'elenco dei client AAA e nelle caselle Porta e Indirizzo IP origine non deve essere superiore a 1024. Sebbene ACS accetti più di 1024 caratteri quando si aggiunge un NAR, non è possibile modificare il NAR e ACS non è in grado di applicarlo correttamente agli utenti.Fare clic su **Invio**.Le informazioni su client, porta e indirizzo AAA vengono visualizzate come voce nella tabella.Ripetere i passaggi c e d per inserire altre voci basate su IP.

7. Se si desidera autorizzare o negare l'accesso in base alla località di chiamata o a valori diversi dagli indirizzi IP:Selezionare la casella di controllo **Definisci restrizioni di accesso basate su CLI/DNIS**.Per specificare se elencare le posizioni consentite o negate dall'elenco Definizioni tabella, selezionare il valore applicabile.Per specificare i client a cui applicare il NAR, selezionare uno dei seguenti valori dall'elenco Client AAA:Il nome della DG NDGNome del client AAA specificoTutti i client AAASuggerimento: sono elencati solo i gruppi di criteri di rete già configurati.Per specificare le informazioni su cui il NAR deve filtrare, immettere i valori in queste caselle, come applicabile:**Suggerimento:** è possibile immettere un asterisco (*) come carattere jolly per specificare **tutti** come valore.**Porta (Port)** - Consente di immettere il numero della porta su cui applicare il filtro.**CLI:** immettere il numero CLI su cui filtrare. È possibile utilizzare questa casella anche per limitare l'accesso in base a valori diversi da CLI, come un indirizzo IP o un indirizzo MAC. Per ulteriori informazioni, vedere la sezione [Informazioni sulle restrizioni di accesso alla rete](#).**DNIS** - Immettere il numero da comporre per filtrare.**Nota:** il numero totale di caratteri nell'elenco dei client AAA e nelle caselle Porta, CLI e DNIS non deve essere superiore a 1024. Sebbene ACS accetti più di 1024 caratteri quando si aggiunge un NAR, non è possibile modificare il NAR e ACS non è in grado di applicarlo correttamente agli utenti.Fare clic su **Invio**.Le informazioni che specificano la voce NAR vengono visualizzate nella tabella.Ripetere i passaggi da c a e per inserire altre righe NAR non basate su IP.Per salvare la definizione NAR condivisa, fare clic su **Submit** (Invia).ACS salva l'NAR condiviso e lo elenca nella tabella **Limitazioni di accesso alla rete**.

[Modifica NAR condiviso](#)

Per modificare un NAR condiviso, completare i seguenti passaggi:

1. Nella barra di spostamento fare clic su **Componenti profilo condiviso**.Viene visualizzata la finestra Componenti profilo condiviso.
2. Fare clic su **Restrizioni accesso alla rete**.Viene visualizzata la tabella Limitazioni di accesso alla rete.
3. Nella colonna Nome fare clic sul NAR condiviso che si desidera modificare.Viene visualizzata la finestra Limitazione accesso alla rete che contiene le informazioni relative al NAR selezionato.
4. Modificare il Nome o la Descrizione del NAR, a seconda dei casi. La descrizione può contenere un massimo di 30.000 caratteri.
5. Per modificare una voce nella tabella delle restrizioni di accesso basate su IP:Fare doppio clic sull'elemento riga che si desidera modificare.Le informazioni relative alla voce vengono rimosse dalla tabella e scritte nelle caselle sottostanti.Modificare le informazioni, se necessario.**Nota:** il numero totale di caratteri nell'elenco dei client AAA e nelle caselle Porta e

Indirizzo IP origine non deve essere superiore a 1024. Sebbene ACS possa accettare più di 1024 caratteri quando si aggiunge un NAR, non è possibile modificare tale NAR e ACS non può applicarlo in modo accurato agli utenti. Fare clic su **Invio**. Le informazioni modificate per questa riga vengono scritte nella tabella delle restrizioni di accesso basate su IP.

6. Per rimuovere una voce dalla tabella delle restrizioni di accesso basate su IP: Selezionare la voce. Nella tabella fare clic su **Rimuovi**. La voce viene rimossa dalla tabella delle restrizioni di accesso basate su IP.
7. Per modificare una voce nella tabella delle restrizioni di accesso di CLI/DNIS: Fare doppio clic sull'elemento riga che si desidera modificare. Le informazioni relative alla voce vengono rimosse dalla tabella e scritte nelle caselle sottostanti. Modificare le informazioni, se necessario. **Nota:** il numero totale di caratteri nell'elenco dei client AAA e nelle caselle Porta, CLI e DNIS non deve essere superiore a 1024. Sebbene ACS possa accettare più di 1024 caratteri quando si aggiunge un NAR, non è possibile modificare tale NAR e ACS non può applicarlo in modo accurato agli utenti. Fare clic su **Invio**. Le informazioni modificate per questa riga vengono scritte nella tabella delle restrizioni di accesso CLI/DNIS.
8. Per rimuovere una voce dalla tabella delle restrizioni di accesso di CLI/DNIS: Selezionare la voce. Nella tabella fare clic su **Rimuovi**. La voce viene rimossa dalla tabella delle restrizioni di accesso di CLI/DNIS.
9. Per salvare le modifiche apportate, fare clic su **Submit** (Invia). ACS inserisce nuovamente il filtro con le nuove informazioni, che diventano effettive immediatamente.

[Eliminazione di un NAR condiviso](#)

Nota: assicurarsi di rimuovere l'associazione di un NAR condiviso da qualsiasi utente o gruppo prima di eliminare tale NAR.

Per eliminare un NAR condiviso, completare i seguenti passaggi:

1. Nella barra di spostamento fare clic su **Componenti profilo condiviso**. Viene visualizzata la finestra Componenti profilo condiviso.
2. Fare clic su **Restrizioni accesso alla rete**.
3. Fare clic sul nome del NAR condiviso che si desidera eliminare. Viene visualizzata la finestra Limitazione accesso alla rete che contiene le informazioni relative al NAR selezionato.
4. Nella parte inferiore della finestra fare clic su **Elimina**. Viene visualizzata una finestra di dialogo in cui si avvisa che si sta per eliminare un NAR condiviso.
5. Fare clic su **OK** per confermare l'eliminazione del NAR condiviso. Il NAR condiviso selezionato viene eliminato.

[Impostazione delle restrizioni di accesso alla rete per un utente](#)

La tabella Limitazioni di accesso alla rete dell'area Impostazioni avanzate di Configurazione utente consente di impostare le NAR in tre modi:

- Applica NAR condivisi esistenti per nome.
- Definire le restrizioni di accesso basate sull'indirizzo IP per consentire o negare l'accesso degli utenti a un client AAA specificato o a porte specifiche su un client AAA quando è stata stabilita una connessione IP.
- Definire le restrizioni di accesso basate su CLI/DNIS per autorizzare o negare l'accesso degli

utenti in base alla CLI/DNIS utilizzata. **Nota:** per specificare altri valori, è possibile usare anche l'area delle restrizioni di accesso basata su CLI/DNIS. Per ulteriori informazioni, vedere la sezione [Restrizioni di accesso alla rete](#).

In genere, le NAR (condivise) vengono definite dall'interno della sezione Componenti condivisi in modo che sia possibile applicare queste restrizioni a più gruppi o utenti. Per ulteriori informazioni, vedere la sezione [Aggiunta di un NAR condiviso](#). Affinché questo gruppo di opzioni venga visualizzato nell'interfaccia Web, è necessario che sia stata selezionata la casella di controllo **Restrizioni di accesso alla rete a livello utente** nella pagina Opzioni avanzate della sezione Configurazione interfaccia.

Tuttavia, è anche possibile utilizzare ACS per definire e applicare un NAR per un singolo utente dalla sezione Impostazione utente. Per visualizzare nell'interfaccia Web le opzioni di filtro basate su IP per utente singolo e le opzioni di filtro basate su CLI/DNIS per utente singolo, è necessario aver attivato l'impostazione **Restrizioni accesso alla rete a livello utente** nella pagina Opzioni avanzate della sezione Configurazione interfaccia.

Nota: quando una richiesta di autenticazione viene inoltrata da un proxy ad un ACS, qualsiasi NAR per le richieste TACACS+ (Terminal Access Controller Access Control System) viene applicato all'indirizzo IP del server AAA di inoltro e non all'indirizzo IP del client AAA di origine.

Quando si creano restrizioni di accesso per singoli utenti, ACS non impone limiti al numero di restrizioni di accesso e non impone un limite alla lunghezza di ciascuna restrizione di accesso. Esistono tuttavia dei limiti rigorosi:

- La combinazione di campi per ogni voce non può superare i 1024 caratteri.
- Il NAR condiviso non può contenere più di 16 KB di caratteri. Il numero di righe supportate dipende dalla lunghezza di ogni riga. Ad esempio, se si crea un NAR basato su CLI/DNIS in cui i nomi dei client AAA sono costituiti da 10 caratteri, i numeri di porta sono 5 caratteri, le voci CLI sono 15 caratteri e le voci DNIS sono 20 caratteri, è possibile aggiungere 450 righe prima di raggiungere il limite di 16 KB.

Per impostare i NAR per un utente, completare i seguenti passaggi:

1. Eseguire i passaggi da 1 a 3 di [Aggiunta di un account utente di base](#). Viene visualizzata la finestra Modifica impostazione utente. Il nome utente aggiunto o modificato viene visualizzato nella parte superiore della finestra.

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 NARView 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

SubmitDeleteCancel

2. Per applicare un NAR condiviso configurato in precedenza a questo utente:**Nota:** per applicare un NAR condiviso, è necessario configurarlo in Restrizioni di accesso alla rete nella sezione Componenti profilo condiviso. Per ulteriori informazioni, vedere la sezione [Aggiunta di un NAR condiviso](#). Selezionare la casella di controllo **Consenti accesso alla rete solo quando**. Per specificare se una o tutte le NAR condivise devono richiedere all'utente l'accesso, selezionarne una, a seconda del caso: Tutti i NAR selezionati restituiscono il

permesso. Una qualsiasi delle NAR selezionate genera un permesso. Selezionare un nome NAR condiviso nell'elenco NAR, quindi fare clic su → (pulsante freccia destra) per spostare il nome nell'elenco NAR selezionati. **Suggerimento:** per visualizzare i dettagli del server dei NAR condivisi selezionati per l'applicazione, è possibile fare clic su **Visualizza NAR IP** o **Visualizza NAR CLID/DNIS**, a seconda dei casi.

3. Per definire e applicare un NAR, per questo particolare utente, che consenta o neghi a questo utente l'accesso in base all'indirizzo IP o all'indirizzo IP e alla porta: **Nota:** è necessario definire la maggior parte dei NAR dalla sezione Componenti condivisi in modo da poterli applicare a più gruppi o utenti. Per ulteriori informazioni, vedere la sezione [Aggiunta di un NAR condiviso](#). Nella tabella Limitazioni di accesso alla rete, in Restrizioni di accesso alla rete definite dall'utente, selezionare la casella di controllo **Definisci restrizioni di accesso basate su IP**. Per specificare se nell'elenco che segue vengono specificati gli indirizzi IP consentiti o non consentiti, sceglierne uno dall'elenco Definizioni tabella: **Percorsi di chiamata/punto di accesso consentiti** **Percorsi chiamate/punti di accesso negati** Selezionare o immettere le informazioni nelle seguenti caselle: **Client AAA:** selezionare **Tutti i client AAA**, il nome di un gruppo di dispositivi di rete (NDG) o il nome del singolo client AAA a cui consentire o negare l'accesso. **Porta:** immettere il numero della porta a cui consentire o negare l'accesso. È possibile utilizzare l'asterisco (*) come carattere jolly per consentire o negare l'accesso a tutte le porte sul client AAA selezionato. **Indirizzo:** immettere l'indirizzo o gli indirizzi IP da utilizzare quando si applicano le restrizioni di accesso. È possibile utilizzare l'asterisco (*) come carattere jolly. **Nota:** il numero totale di caratteri nell'elenco dei client AAA e nelle caselle Porta e Indirizzo IP origine non deve essere superiore a 1024. Sebbene ACS accetti più di 1024 caratteri quando si aggiunge un NAR, non è possibile modificare il NAR e ACS non è in grado di applicarlo correttamente agli utenti. Fare clic su **Invio**. Le informazioni specificate su client, porta e indirizzo AAA vengono visualizzate nella tabella sopra l'elenco dei client AAA.
4. Per autorizzare o negare l'accesso di questo utente in base alla località di chiamata o a valori diversi da un indirizzo IP stabilito: Selezionare la casella di controllo **Definisci restrizioni di accesso basate su CLI/DNIS**. Per specificare se nell'elenco successivo vengono specificati valori consentiti o non consentiti, scegliere una delle opzioni seguenti dall'elenco Definizioni tabella: **Percorsi di chiamata/punto di accesso consentiti** **Percorsi chiamate/punti di accesso negati** Completate le caselle come mostrato: **Nota:** è necessario inserire una voce in ciascuna casella. È possibile utilizzare l'asterisco (*) come carattere jolly per un valore intero o parziale. Il formato utilizzato deve corrispondere al formato della stringa ricevuta dal client AAA. È possibile determinare questo formato dal registro di accounting RADIUS. **Client AAA:** selezionare **Tutti i client AAA**, o il nome del gruppo di distribuzione di rete, o il nome del singolo client AAA, a cui consentire o negare l'accesso. **PORT:** immettere il numero della porta a cui consentire o negare l'accesso. È possibile utilizzare l'asterisco (*) come carattere jolly per consentire o negare l'accesso a tutte le porte. **CLI:** immettere il numero CLI a cui consentire o negare l'accesso. È possibile utilizzare l'asterisco (*) come carattere jolly per autorizzare o negare l'accesso in base a parte del numero. **Suggerimento:** utilizzare la voce CLI per limitare l'accesso in base ad altri valori, ad esempio l'indirizzo MAC di un client Cisco Aironet. Per ulteriori informazioni, vedere la sezione [Informazioni sulle restrizioni di accesso alla rete](#). **DNIS:** immettere il numero DNIS a cui consentire o negare l'accesso. Utilizzare questa voce per limitare l'accesso in base al numero composto dall'utente. È possibile utilizzare l'asterisco (*) come carattere jolly per autorizzare o negare l'accesso in base a parte del numero. **Suggerimento:** utilizzare la selezione DNIS per limitare l'accesso in base ad altri valori, ad esempio un indirizzo MAC Cisco Aironet AP. Per ulteriori informazioni,

vedere la sezione [Informazioni sulle restrizioni di accesso alla rete](#). **Nota:** il numero totale di caratteri nell'elenco dei client AAA e nelle caselle **Porta**, **CLI** e **DNIS** non deve essere superiore a 1024. Sebbene ACS accetti più di 1024 caratteri quando si aggiunge un NAR, non è possibile modificare il NAR e ACS non è in grado di applicarlo correttamente agli utenti. Fare clic su **Invio**. Le informazioni che specificano il client AAA, la porta, CLI e DNIS vengono visualizzate nella tabella sopra l'elenco dei client AAA.

5. Dopo aver configurato le opzioni dell'account utente, fare clic su **Submit** (Invia) per registrarle.

[Impostazione delle restrizioni di accesso alla rete per un gruppo di utenti](#)

La tabella Limitazioni di accesso alla rete in Impostazione gruppo consente di applicare i NAR in tre modi distinti:

- Applica NAR condivisi esistenti per nome.
- Definire le restrizioni di accesso ai gruppi basate sull'IP per autorizzare o negare l'accesso a un client AAA specificato o a porte specifiche su un client AAA quando è stata stabilita una connessione IP.
- Definire i NAR di gruppo basati su CLI/DNIS per consentire o negare l'accesso a uno dei due numeri CLI o a entrambi. **Nota:** per specificare altri valori, è possibile usare anche l'area delle restrizioni di accesso basata su CLI/DNIS. Per ulteriori informazioni, vedere la sezione [Informazioni sulle restrizioni di accesso alla rete](#).

In genere, le NAR (condivise) vengono definite dall'interno della sezione Componenti condivisi in modo che queste restrizioni possano essere applicate a più gruppi o utenti. Per ulteriori informazioni, vedere la sezione [Aggiunta di un NAR condiviso](#). Affinché queste opzioni vengano visualizzate nell'interfaccia Web di ACS, è necessario selezionare la casella di controllo **Restrizione accesso alla rete condiviso a livello di gruppo** nella pagina **Opzioni avanzate** della sezione Configurazione interfaccia.

Tuttavia, è possibile utilizzare ACS anche per definire e applicare un NAR per un singolo gruppo dalla sezione **Impostazione gruppo**. È necessario controllare l'impostazione **Limitazione dell'accesso alla rete a livello di gruppo** nella pagina Opzioni avanzate della sezione Configurazione interfaccia per visualizzare nell'interfaccia Web ACS le opzioni di filtro basate su IP per gruppo singolo e le opzioni di filtro basate su CLI/DNIS per gruppo singolo.

Nota: quando una richiesta di autenticazione viene inoltrata da un proxy a un server ACS, qualsiasi NAR per le richieste RADIUS viene applicato all'indirizzo IP del server AAA di inoltro e non all'indirizzo IP del client AAA di origine.

Per impostare i NAR per un gruppo di utenti, completare i seguenti passaggi:

1. Nella barra di spostamento fare clic su **Imposta gruppo**. Viene visualizzata la finestra Selezione impostazione gruppo.
2. Nell'elenco Gruppo selezionare un gruppo e quindi fare clic su **Modifica impostazioni**. Il nome del gruppo viene visualizzato nella parte superiore della finestra Impostazioni gruppo.

