보안 ACS - 사용자 및 사용자 그룹용 AAA 클라이언트가 있는 NAR

목차

소개

이 문서에서는 사용자 및 사용자 그룹을 위해 AAA 클라이언트(라우터, PIX, ASA, 무선 컨트롤러 포함)가 포함된 Cisco ACS(Secure Access Control Server) 4.x 버전에서 NAR(Network Access Restrictions)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서는 Cisco Secure ACS 및 AAA 클라이언트가 구성되고 제대로 작동한다는 가정 하에 작성되었습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Secure ACS 3.0 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

네트워크 액세스 제한

이 섹션에서는 NAR에 대해 설명하며 공유 NAR을 구성 및 관리하기 위한 자세한 지침을 제공합니다.

이 섹션에서는 다음 항목을 다룹니다.

- 네트워크 액세스 제한 정보
- 공유 NAR 추가
- 공유 NAR 편집
- 공유 NAR 삭제

네트워크 액세스 제한 정보

NAR은 사용자가 네트워크에 액세스하기 전에 충족해야 하는 추가 조건을 ACS에서 정의하는 정의입니다. ACS는 AAA 클라이언트가 전송하는 특성의 정보를 사용하여 이러한 조건을 적용합니다. 여러 가지 방법으로 NAR을 설정할 수 있지만 모두 AAA 클라이언트가 전송하는 일치하는 특성 정보를 기반으로 합니다. 따라서 유효한 NAR을 사용하려는 경우 AAA 클라이언트가 전송하는 특성의 형식과 내용을 이해해야 합니다.

NAR을 설정할 때 필터의 작동 여부를 양성으로 선택할 수 있습니다. 즉, NAR에서 NAR에 저장된 정보와 비교할 때 AAA 클라이언트에서 보낸 정보를 기반으로 네트워크 액세스를 허용할지 거부할지를 지정합니다. 그러나 NAR에 작동하기에 충분한 정보가 없으면 기본적으로 액세스가 거부됩니다. 이 표에서는 다음 조건을 보여 줍니다.

	IP 기반	비 IP 기반	정보 부족
허용	액세스 허가	액세스 거부됨	액세스 거부됨
거부	액세스 거부됨	액세스 허가	액세스 거부됨

ACS는 두 가지 유형의 NAR 필터를 지원합니다.

- **IP 기반 필터**—IP 기반 NAR 필터는 최종 사용자 클라이언트 및 AAA 클라이언트의 IP 주소를 기반으로 액세스를 제한합니다. 자세한 내용은 IP 기반 NAR 필터 정보 섹션을 참조하십시오.
- **비 IP 기반 필터**—비 IP 기반 NAR 필터는 AAA 클라이언트에서 전송된 값의 간단한 문자열 비교를 기반으로 액세스를 제한합니다. 값은 CLI(Calling Line Identification) 번호, DNIS(Dialed Number Identification Service) 번호, MAC 주소 또는 클라이언트에서 시작되는 다른 값일 수 있습니다. 이 유형의 NAR이 작동하려면 NAR 설명의 값이 클라이언트에서 전송되는 것과 정확히 일치해야 하며, 여기에는 어떤 형식이든 사용됩니다. 예를 들어 전화 번호(217) 555-4534가 217-555-4534와 일치하지 않습니다. 자세한 내용은 About Non-IP-based NAR Filters(비 IP 기반 NAR 필터 정보) 섹션을 참조하십시오.

특정 사용자 또는 사용자 그룹에 대해 NAR을 정의하고 적용할 수 있습니다. 자세한 내용은 Set Network Access Restrictions for a User(사용자에 대한 네트워크 액세스 제한 설정) 또는 Set Network Access Restrictions for a User Group(사용자 그룹에 대한 네트워크 액세스 제한 설정) 섹션을 참조하십시오. 그러나 ACS의 Shared Profile Components(공유 프로파일 구성 요소) 섹션에서 사용자 또는 사용자 그룹을 직접 언급하지 않고 공유 NAR을 생성하고 이름을 지정할 수 있습니다.

공유 NAR에 ACS 웹 인터페이스의 다른 부분에서 참조할 수 있는 이름을 지정합니다. 그런 다음 사용자 또는 사용자 그룹을 설정할 때 적용할 없음, 하나 또는 여러 공유 제한을 선택할 수 있습니다. 사용자 또는 사용자 그룹에 여러 공유 NAR의 애플리케이션을 지정할 때 다음 두 가지 액세스 기준 중 하나를 선택합니다.

- 선택한 모든 필터는 허용해야 합니다.
- 선택한 필터 중 하나를 허용해야 합니다.

서로 다른 유형의 NAR과 관련된 우선 순위를 이해해야 합니다. NAR 필터링 순서는 다음과 같습니다.

1. 사용자 레벨의 공유 NAR
2. 그룹 레벨의 공유 NAR
3. 사용자 레벨의 비공유 NAR
4. 그룹 레벨의 비공유 NAR

또한 **액세스 거부가 액세스를 거부하지 않는 다른 레벨의 설정에 우선합니다**. 사용자 수준 설정이 그룹 수준 설정을 재정의하는 규칙에 대한 ACS의 한 가지 예외입니다. 예를 들어, 특정 사용자는 적용되는 사용자 레벨에서 NAR 제한이 없을 수 있습니다. 그러나 해당 사용자가 공유 또는 비공유 NAR에 의해 제한된 그룹에 속할 경우 사용자는 액세스가 거부됩니다.

공유 NAR은 ACS 내부 데이터베이스에 보관됩니다. ACS 백업 및 복원 기능을 사용하여 백업 및 복원할 수 있습니다. 다른 컨피그레이션과 함께 공유 NAR을 보조 ACS에 복제할 수도 있습니다.

IP 기반 NAR 필터 정보

IP 기반 NAR 필터의 경우 ACS는 표시된 대로 특성을 사용합니다. 이는 인증 요청의 AAA 프로토콜에 따라 다릅니다.

- **TACACS+를 사용하는 경우**—TACACS+ 시작 패킷 본문의 rem_addr 필드가 사용됩니다.**참고:** 인증 요청이 프록시에 의해 ACS로 전달되면 TACACS+ 요청에 대한 모든 NAR은 원래 AAA 클라이언트의 IP 주소가 아니라 전달 AAA 서버의 IP 주소에 적용됩니다.
- **RADIUS IETF를 사용하는 경우** - calling-station-id(특성 31)를 사용해야 합니다.**참고:** IP 기반 NAR 필터는 ACS가 Radius Calling-Station-Id(31) 특성을 수신하는 경우에만 작동합니다. Calling-Station-Id(31)에는 유효한 IP 주소가 있어야 합니다. 그렇지 않으면 DNIS 규칙에 따라 넘어갑니다.

충분한 IP 주소 정보(예: 일부 방화벽 유형)를 제공하지 않는 AAA 클라이언트는 전체 NAR 기능을 지원하지 않습니다.

프로토콜별 **IP 기반** 제한에 대한 기타 특성은 다음과 같이 NAR 필드를 포함합니다.

- **TACACS+를 사용하는 경우**—ACS의 NAR 필드는 다음 값을 사용합니다.**AAA 클라이언트** - NAS-IP 주소는 ACS와 TACACS+ 클라이언트 사이의 소켓의 소스 주소에서 가져옵니다 .**Port**(포트) - 포트 필드는 TACACS+ 시작 패킷 본문에서 가져옵니다.

비 IP 기반 NAR 필터 정보

비 IP 기반 NAR 필터(즉, DNIS/CLI 기반 NAR 필터)는 설정된 IP 기반 연결이 없는 경우 AAA 클라이언트를 제한하는 데 사용할 수 있는 허용 또는 거부된 통화 또는 액세스 지점의 목록입니다. 비 IP 기반 NAR 기능은 일반적으로 CLI 번호와 DNIS 번호를 사용합니다.

그러나 CLI 대신 IP 주소를 입력하면 비 IP 기반 필터를 사용할 수 있습니다. AAA 클라이언트가 CLI 또는 DNIS를 지원하는 Cisco IOS® 소프트웨어 릴리스를 사용하지 않는 경우에도 마찬가지입니다. CLI를 입력하는 또 다른 예외에서는 액세스를 허용하거나 거부하기 위해 MAC 주소를 입력할 수 있습니다. 예를 들어 Cisco Aironet AAA 클라이언트를 사용하는 경우 마찬가지로 DNIS 대신 Cisco Aironet AP MAC 주소를 입력할 수 있습니다. CLI 상자에서 지정하는 형식(CLI, IP 주소 또는 MAC 주소)은 AAA 클라이언트에서 수신하는 것과 일치해야 합니다. RADIUS 계정 관리 로그에서 이 형식을 확인할 수 있습니다.

프로토콜별 DNIS/CLI 기반 제한에 대한 특성에는 다음과 같이 NAR 필드가 포함됩니다.

- **TACACS+를 사용하는 경우**—나열된 NAR 필드에는 다음 값이 적용됩니다.**AAA 클라이언트**—NAS-IP 는 ACS와 TACACS+ 클라이언트 사이의 소켓의 소스 주소에서 가져옵니다.**Port**(포트) - TACACS+ 시작 패킷 본문의 필드가 사용됩니다.**CLI**—TACACS+ 시작 패킷 본문의 rem-addr 필드가 사용됩니다.**DNIS** - TACACS+ 시작 패킷 본문에서 가져온 rem-addr 필드가 사용됩니다. rem-addr 데이터가 슬래시(/)로 시작되는 경우 DNIS 필드에는 슬래시(/)가 없는 rem-addr 데이터가 포함됩니다.**참고:** 인증 요청이 프록시에 의해 ACS로 전달되면 TACACS+ 요청에 대한 모든 NAR은 원래 AAA 클라이언트의 IP 주소가 아니라 전달 AAA 서버의 IP 주소에 적용됩니다.
- **RADIUS를 사용하는 경우** — 나열된 NAR 필드는 다음 값을 사용합니다.**AAA 클라이언트**—NAS-IP (특성 4) 또는 NAS-IP 주소가 없는 경우 NAS (RADIUS 특성 32)가 사용됩니다.**Port**—NAS (특성 5) 또는 NAS 포트가 없는 경우 NAS ID(특성 87)가 사용됩니다.**CLI**—calling-station-ID(특성 31)가 사용됩니다.**DNIS**—called-station-ID(특성 30)가 사용됩니다.

NAR을 지정할 때 임의의 값에 대한 와일드카드로 별표(*)를 사용하거나 임의의 값의 일부로 범위를 설정할 수 있습니다. NAR에서 액세스를 제한하려면 NAR 설명의 모든 값 또는 조건을 충족해야 합니다. 즉, 값은 부울 AND를 포함합니다.

공유 NAR 추가

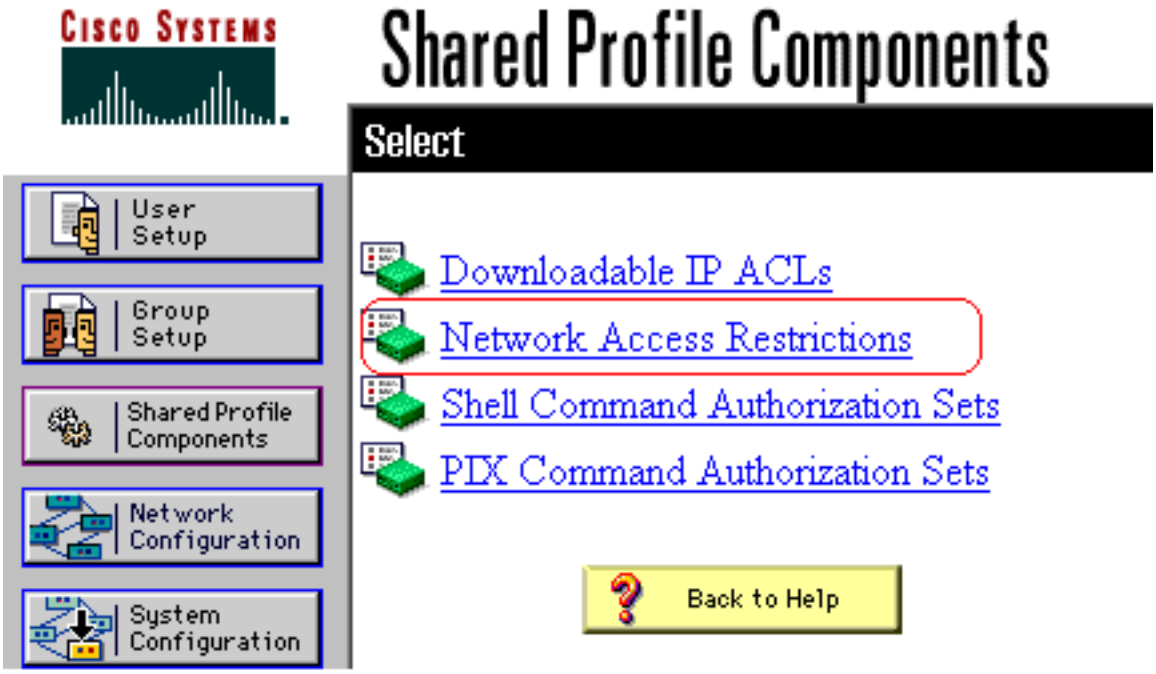
많은 액세스 제한을 포함하는 공유 NAR을 생성할 수 있습니다. ACS 웹 인터페이스는 공유 NAR의 액세스 제한 수 또는 각 액세스 제한 길이에 대한 제한을 적용하지 않지만 다음 제한을 준수해야 합니다.

- 각 행 항목에 대한 필드 조합은 1024자를 초과할 수 없습니다.
- 공유 NAR은 16KB를 초과할 수 없습니다. 지원되는 행 항목 수는 각 행 항목의 길이에 따라 달라집니다. 예를 들어, AAA 클라이언트 이름이 10자인 CLI/DNIS 기반 NAR를 생성하고 포트 번호는 5자, CLI 항목은 15자, DNIS 항목은 20자인 경우 16KB 제한에 도달하기 전에 450개의 라인 항목을 추가할 수 있습니다.

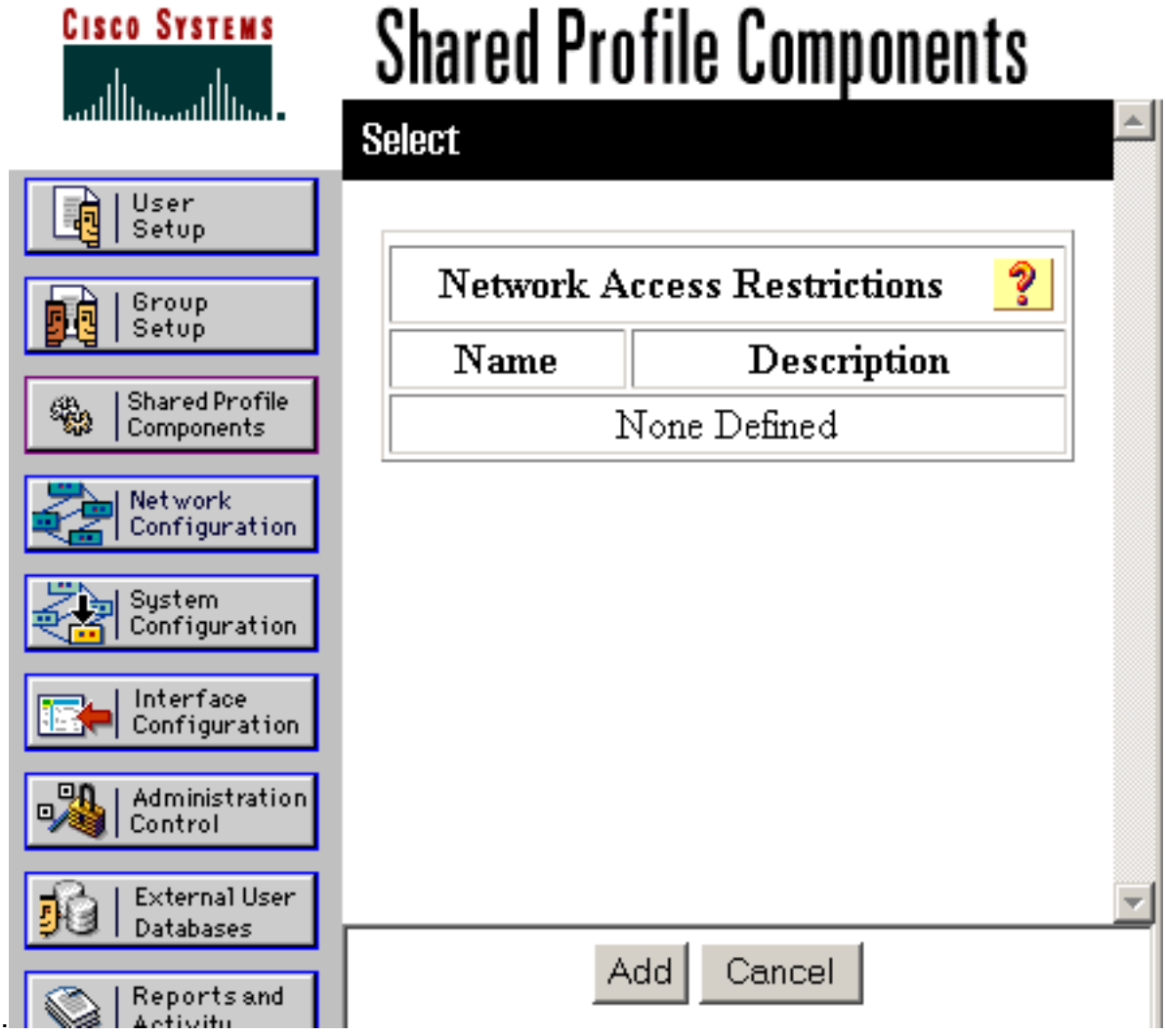
참고: NAR을 정의하기 전에 해당 NAR에서 사용할 요소를 설정했는지 확인합니다. 따라서 NAR 정의에 포함하기 전에 모든 NAC 및 NDG를 지정하고 모든 관련 AAA 클라이언트를 정의해야 합니다. 자세한 내용은 네트워크 액세스 제한 정보 섹션을 참조하십시오.

공유 NAR을 추가하려면 다음 단계를 완료하십시오.

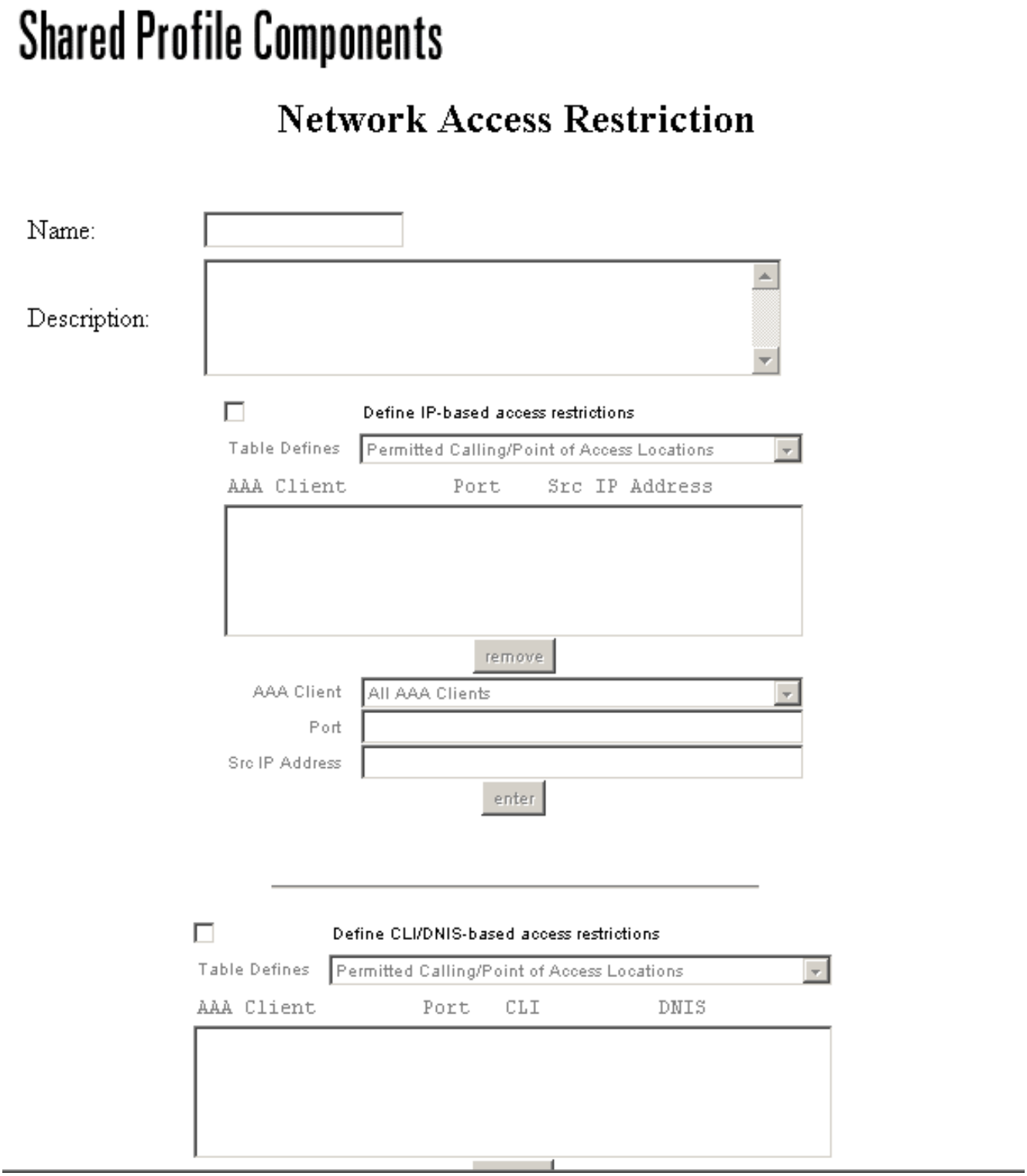
1. Navigation(탐색) 모음에서 Shared **Profile Components(공유 프로파일 구성 요소)를 클릭합니다**.Shared Profile Components 창이 나타납니다



2. Network **Access Restrictions(네트워크 액세스 제한)를 클릭합니다**



3. Add(**추가)를 클릭합니다**.네트워크 액세스 제한 창이 나타납니다



4. 이름 상자에 새 공유 NAR의 이름을 입력합니다.**참고:** 이름은 최대 31자까지 가능합니다. 선행 및 후행 공백은 허용되지 않습니다. 이름에는 다음 문자를 사용할 수 없습니다. 왼쪽 대괄호([), 오른쪽 대괄호(]), 쉼표(,) 또는 슬래시(/).
5. Description(설명) 상자에 새 공유 NAR에 대한 설명을 입력합니다. 설명은 최대 30,000자까지 입력할 수 있습니다.
6. IP 주소 지정을 기반으로 액세스를 허용하거나 거부하려면Define **IP-based access descriptions** 확인란을 선택합니다.허용 또는 거부된 주소를 나열할지 여부를 지정하려면 테이블 정의 목록에서 해당 값을 선택합니다.다음 각 상자에서 해당 정보를 선택하거나 입력합니다.**AAA Client**(AAA 클라이언트) - **모든 AAA 클라이언트**, 또는 액세스가 허용되거나 거부된 NDG, NAF 또는 개별 AAA 클라이언트의 이름을 선택합니다.**Port**(포트) - 액세스를 허용하거나 거부할 포트의 번호를 입력합니다. 별표(*)를 와일드카드로 사용하여 선택한 AAA 클라이언트의 모든 포트에 대한 액세스를 허용하거나 거부할 수 있습니다.**Src IP Address(소스 IP 주소**

) - 액세스 제한을 수행할 때 필터링할 IP 주소를 입력합니다. 모든 IP 주소를 지정하려면 별표(*)를 와일드카드로 사용할 수 있습니다.**참고:** AAA Client(AAA 클라이언트) 목록 및 Port(포트) 및 Src IP Address(소스 IP 주소) 상자의 총 문자 수는 1024를 초과해서는 안 됩니다. NAR을 추가할 때 ACS에서 1024자를 초과하는 문자를 허용하지만, NAR을 수정할 수 없으며 ACS는 사용자에게 정확하게 적용할 수 없습니다.Enter를 **클릭합니다**.AAA 클라이언트, 포트 및 주소 정보가 테이블에 행 항목으로 나타납니다.추가 IP 기반 라인 항목을 입력하려면 c 및 d 단계를 반복합니다.

7. 발신 위치 또는 IP 주소 이외의 값을 기준으로 액세스를 허용하거나 거부하려면Define **CLI/DNIS based access restrictions(CLI/DNIS 기반 액세스 제한 정의)** 확인란을 선택합니다.테이블 정의(Table Defines) 목록에서 허용 또는 거부된 위치를 나열할지 여부를 지정하려면 해당 값을 선택합니다.이 NAR이 적용되는 클라이언트를 지정하려면 AAA Client 목록에서 다음 값 중 하나를 선택합니다.NDG의 이름특정 AAA 클라이언트의 이름모든 AAA 클라이언트 **팁:** 이미 구성한 NDG만 나열됩니다.이 NAR에서 필터링할 정보를 지정하려면 다음 상자에 해당하는 값을 입력합니다.**팁:** 별표(*)를 와일드카드로 입력하여 **모두** 값으로 지정할 수 있습니다.**Port**(포트) - 필터링할 포트 번호를 입력합니다.**CLI** - 필터링할 CLI 번호를 입력합니다. IP 주소 또는 MAC 주소와 같은 CLI 이외의 값을 기준으로 액세스를 제한하려면 이 상자를 사용할 수도 있습니다. 자세한 내용은 네트워크 액세스 제한 정보 섹션을 참조하십시오.**DNIS** - 필터링할 번호를 입력합니다.**참고:** AAA Client 목록 및 Port, CLI, DNIS 상자의 총 문자 수는 1024를 초과할 수 없습니다. NAR을 추가할 때 ACS에서 1024자를 초과하는 문자를 허용하지만, NAR을 수정할 수 없으며 ACS는 사용자에게 정확하게 적용할 수 없습니다.Enter를 **클릭합니다**.NAR 행 항목을 지정하는 정보가 테이블에 나타납니다.IP가 아닌 NAR 라인 항목을 추가로 입력하려면 c~e 단계를 반복합니다.공유 NAR 정의를 저장하려면 **Submit**(제출)을 클릭합니다.ACS는 공유 NAR을 저장하고 **네트워크 액세스 제한** 테이블에 **나열합니다**.

공유 NAR 편집

공유 NAR을 수정하려면 다음 단계를 완료하십시오.

1. Navigation(탐색) 모음에서 Shared **Profile Components(공유 프로파일 구성 요소)를 클릭합니다**.Shared Profile Components 창이 나타납니다.
2. Network **Access Restrictions(네트워크 액세스 제한)를 클릭합니다**.네트워크 액세스 제한 테이블이 나타납니다.
3. Name(이름) 열에서 편집할 공유 NAR을 클릭합니다.Network Access Restriction(네트워크 액세스 제한) 창이 나타나고 선택한 NAR에 대한 정보가 표시됩니다.
4. 필요에 따라 NAR의 Name(이름) 또는 Description(설명)을 수정합니다. 설명은 최대 30,000자까지 입력할 수 있습니다.
5. IP 기반 액세스 제한 테이블에서 행 항목을 편집하려면 다음을 수행합니다.편집할 라인 항목을 두 번 클릭합니다.행 항목에 대한 정보가 테이블에서 제거되고 테이블 아래의 상자에 기록됩니다.필요에 따라 정보를 편집합니다.**참고:** AAA Client(AAA 클라이언트) 목록 및 Port(포트) 및 Src IP Address(소스 IP 주소) 상자의 총 문자 수는 1024를 초과할 수 없습니다. NAR을 추가할 때 ACS에서 1024자를 초과하는 문자를 허용할 수 있지만, 이러한 NAR을 수정할 수 없으며 ACS는 이를 사용자에게 정확하게 적용할 수 없습니다.Enter를 **클릭합니다**.이 항목에 대한 편집된 정보는 IP 기반 액세스 제한 테이블에 저장됩니다.
6. IP 기반 액세스 제한 테이블에서 라인 항목을 제거하려면 다음을 수행합니다.라인 항목을 선택합니다.테이블에서 제거를 **클릭합니다**.행 항목이 IP 기반 액세스 제한 테이블에서 제거됩니다.
7. CLI/DNIS access-restrictions 테이블에서 행 항목을 편집하려면 다음을 수행합니다.편집할 라인 항목을 두 번 클릭합니다.행 항목에 대한 정보가 테이블에서 제거되고 테이블 아래의 상자

에 기록됩니다.필요에 따라 정보를 편집합니다.**참고:** AAA Client 목록 및 Port, CLI, DNIS 상자의 총 문자 수는 1024를 초과할 수 없습니다. NAR을 추가할 때 ACS에서 1024자를 초과하는 문자를 허용할 수 있지만, 이러한 NAR을 수정할 수 없으며 ACS는 이를 사용자에게 정확하게 적용할 수 없습니다.Enter를 **클릭합니다.**이 항목에 대한 편집된 정보는 CLI/DNIS 액세스 제한 테이블에 저장됩니다.

8. CLI/DNIS 액세스 제한 테이블에서 행 항목을 제거하려면 다음을 수행합니다.라인 항목을 선택합니다.테이블에서 제거를 **클릭합니다**.행 항목이 CLI/DNIS 액세스 제한 테이블에서 제거됩니다.
9. **Submit(제출)**을 클릭하여 변경한 내용을 저장합니다.ACS가 새 정보로 필터를 다시 입력합니다. 이 정보는 즉시 적용됩니다.

공유 NAR 삭제

참고: 공유 NAR을 삭제하기 전에 모든 사용자 또는 그룹에 대한 연결을 제거해야 합니다.

공유 NAR을 삭제하려면 다음 단계를 완료하십시오.

1. Navigation(탐색) 모음에서 Shared **Profile Components(공유 프로파일 구성 요소)를 클릭합니다**.Shared Profile Components 창이 나타납니다.
2. Network **Access Restrictions(네트워크 액세스 제한)를 클릭합니다**.
3. 삭제할 공유 NAR의 이름을 클릭합니다.Network Access Restriction(네트워크 액세스 제한) 창이 나타나고 선택한 NAR에 대한 정보가 표시됩니다.
4. 창 하단에서 **삭제**를 클릭합니다.공유 NAR을 삭제하려 한다는 경고 대화 상자가 나타납니다.
5. OK(**확인)**를 클릭하여 공유 NAR을 삭제할 것임을 확인합니다.선택한 공유 NAR이 삭제됩니다.

사용자에 대한 네트워크 액세스 제한 설정

사용자 설정의 고급 설정 영역에서 네트워크 액세스 제한 테이블을 사용하여 NAR을 다음과 같은 세 가지 방법으로 설정합니다.

- 이름으로 기존 공유 NAR을 적용합니다.
- IP 연결이 설정되었을 때 지정된 AAA 클라이언트 또는 AAA 클라이언트의 지정된 포트에 대한 사용자 액세스를 허용하거나 거부하도록 IP 기반 액세스 제한을 정의합니다.
- CLI/DNIS 기반 액세스 제한을 정의하여 사용 중인 CLI/DNIS를 기반으로 사용자 액세스를 허용하거나 거부합니다.**참고:** CLI/DNIS 기반 액세스 제한 영역을 사용하여 다른 값을 지정할 수도 있습니다. 자세한 내용은 네트워크 액세스 제한 섹션을 참조하십시오.

일반적으로 공유 구성 요소 섹션에서 NAR을 정의하여 둘 이상의 그룹 또는 사용자에게 이러한 제한을 적용할 수 있습니다. 자세한 내용은 공유 NAR 추가 섹션을 참조하십시오. 웹 인터페이스에 이 옵션 집합이 나타나도록 하려면 Interface Configuration 섹션**의 Advanced** Options 페이지에서 User-Level Network Access Restrictions 확인란을 선택해야 합니다.

그러나 User Setup(사용자 설정) 섹션에서 ACS를 사용하여 단일 사용자에 대한 NAR을 정의하고 적용할 수도 있습니다. 단일 사용자 IP 기반 필터 옵션 및 단일 사용자 CLI/DNIS 기반 필터 옵션이 웹 인터페이스**에** 나타나게 하려면 Interface Configuration 섹션의 Advanced Options 페이지에서 User-Level Network Access Restrictions 설정을 활성화해야 합니다.

참고: 인증 요청이 프록시에 의해 ACS로 전달되면 TACACS+(Terminal Access Controller Access Control System) 요청의 모든 NAR은 원래 AAA 클라이언트의 IP 주소가 아니라 포워딩 AAA 서버의

IP 주소에 적용됩니다.

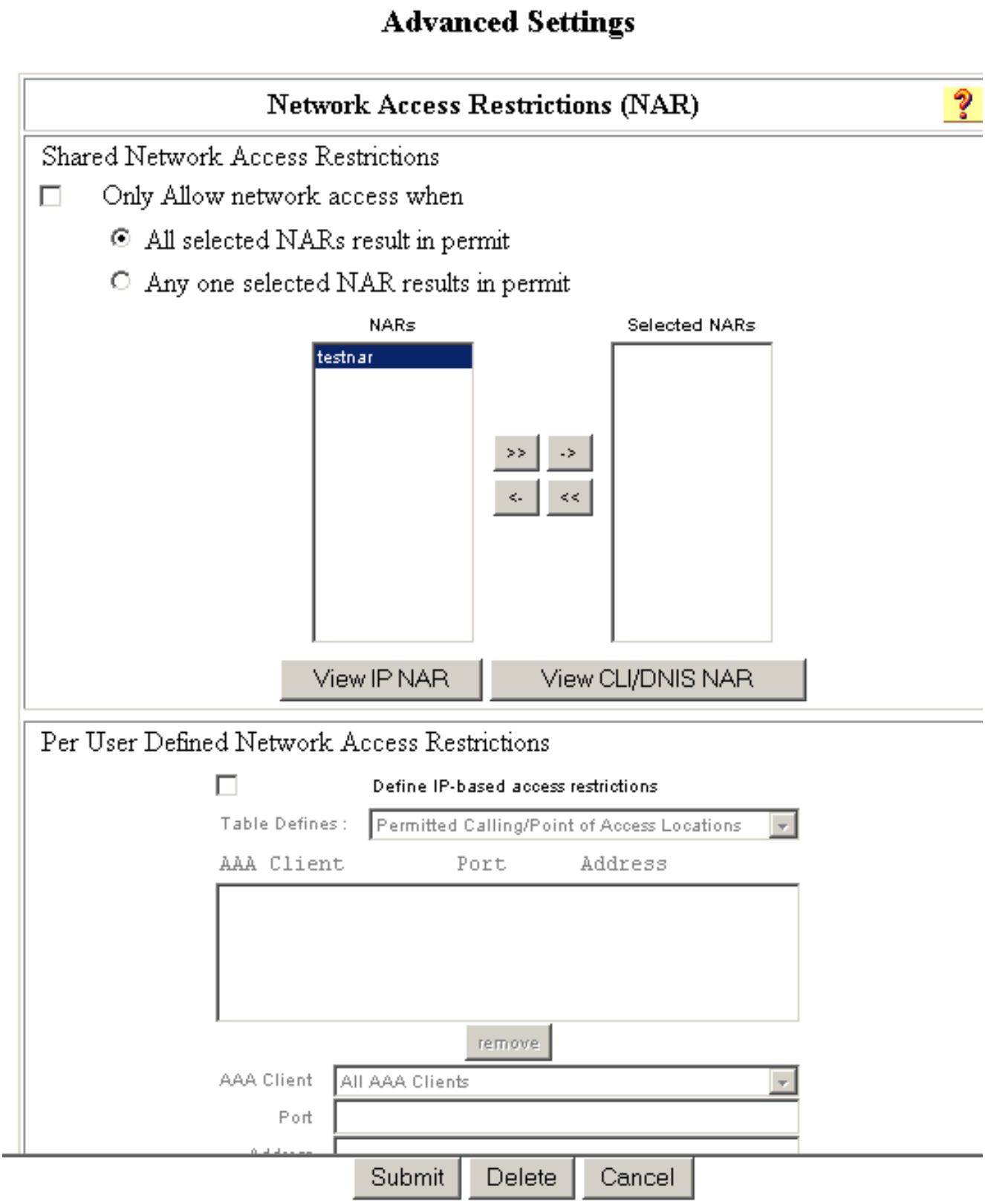
사용자별로 액세스 제한을 생성할 때 ACS는 액세스 제한 수에 제한을 적용하지 않으며 각 액세스 제한 길이에 대한 제한을 시행하지 않습니다. 그러나 여기에는 엄격한 제한이 있습니다.

- 각 행 항목의 필드 조합은 길이가 1024자를 초과할 수 없습니다.
- 공유 NAR은 16KB를 초과할 수 없습니다. 지원되는 행 항목 수는 각 행 항목의 길이에 따라 달라집니다. 예를 들어, AAA 클라이언트 이름이 10자인 CLI/DNIS 기반 NAR를 생성하고 포트 번호는 5자, CLI 항목은 15자, DNIS 항목은 20자인 경우 16KB 제한에 도달하기 전에 450개의 라인 항목을 추가할 수 있습니다.

사용자에 대한 NAR을 설정하려면 다음 단계를 완료합니다.

1. 기본 사용자 계정 추가 단계 1~3단계를 수행합니다.사용자 설정 편집 창이 열립니다. 추가 또는 수정하는 사용자 이름이 창 상단에 나타납니다
   .

User Setup



2. 이전에 구성한 공유 NAR을 이 사용자에게 적용하려면**참고:** 공유 NAR을 적용하려면 Shared Profile Components(공유 프로필 구성 요소) 섹션의 Network Access Restrictions(네트워크 액세스 제한)에서 공유 NAR을 구성해야 합니다. 자세한 내용은 공유 NAR 추가 섹션을 참조하십시오.Only **Allow network access when** 확인란을 선택합니다.사용자가 액세스를 허용하기 위해 하나 또는 모든 공유 NAR을 적용해야 하는지 여부를 지정하려면 필요에 따라 하나를 선택합니다.선택한 모든 NARS가 허용됩니다.선택한 NAR을 하나만 허용하면 됩니다.NAR 목록에

서 공유 NAR 이름을 선택한 다음 —> (오른쪽 화살표 버튼)을 클릭하여 이름을 Selected NARs 목록으로 이동합니다.**팁:** 적용하려고 선택한 공유 NAR의 서버 세부사항을 보려면 **View IP NAR** 또는 **View CLID/DNIS NAR(IP NAR 보기)**을 클릭합니다.

3. 이 특정 사용자에 대해 NAR을 정의하고 적용하려면 IP 주소 또는 IP 주소 및 포트를 기준으로 이 사용자 액세스를 허용하거나 거부합니다.**참고:** 공유 구성 요소 섹션에서 대부분의 NAR을 정의하여 둘 이상의 그룹 또는 사용자에게 적용할 수 있습니다. 자세한 내용은 공유 NAR 추가 섹션을 참조하십시오.Network Access Restrictions(네트워크 액세스 제한) 테이블의 Per User Defined Network Access Restrictions(사용자 정의 네트워크 액세스 제한당)에서 **Define IP-based access restrictions(IP 기반 액세스 제한 정의)** 확인란을 선택합니다.후속 목록에서 허용 또는 거부된 IP 주소를 지정할지 지정하려면 Table Defines 목록에서 다음 중 하나를 선택합니다.**허용된 발신/액세스 지점 위치**거부된 **발신/액세스 지점 위치**다음 상자에 정보를 선택하거나 입력합니다.**AAA Client**(AAA 클라이언트) - **모든 AAA 클라이언트**, 또는 액세스를 허용하거나 거부할 개별 AAA 클라이언트의 이름(NDG)을 선택합니다.**Port**(포트) - 액세스를 허용하거나 거부할 포트의 번호를 입력합니다. 별표(*)를 와일드카드로 사용하여 선택한 AAA 클라이언트의 모든 포트에 대한 액세스를 허용하거나 거부할 수 있습니다.**Address**(주소) - 액세스 제한을 수행할 때 사용할 IP 주소를 입력합니다. 별표(*)를 와일드카드로 사용할 수 있습니다.**참고:** AAA Client(AAA 클라이언트) 목록의 총 문자 수와 Port(포트) 및 Src IP Address(소스 IP 주소) 상자는 1024를 초과해서는 안 됩니다. NAR을 추가할 때 ACS에서 1024자를 초과하는 문자를 허용하지만, NAR을 수정할 수 없으며 ACS는 사용자에게 정확하게 적용할 수 없습니다.Enter를 **클릭합니다**.지정된 AAA 클라이언트, 포트 및 주소 정보가 AAA Client 목록 위의 테이블에 나타납니다.
4. 설정된 IP 주소 이외의 발신 위치 또는 값을 기반으로 이 사용자 액세스를 허용하거나 거부하려면Define **CLI/DNIS based access restrictions(CLI/DNIS 기반 액세스 제한 정의)** 확인란을 선택합니다.다음 목록에서 허용 또는 거부 값을 지정할지 여부를 지정하려면 테이블 정의 목록에서 다음 중 하나를 선택합니다.**허용된 발신/액세스 지점 위치**거부된 **발신/액세스 지점 위치**다음과 같이 상자를 완료합니다.**참고:** 각 상자에 입력해야 합니다. 별표(*)를 값의 전체 또는 일부에 대한 와일드카드로 사용할 수 있습니다. 사용하는 형식은 AAA 클라이언트에서 수신하는 문자열의 형식과 일치해야 합니다. RADIUS 계정 관리 로그에서 이 형식을 확인할 수 있습니다.**AAA Client**(AAA 클라이언트) - **모든 AAA 클라이언트** 또는 NDG의 이름 또는 액세스를 허용하거나 거부할 개별 AAA 클라이언트의 이름을 선택합니다.**PORT** - 액세스를 허용하거나 거부할 포트의 번호를 입력합니다. 모든 포트에 대한 액세스를 허용하거나 거부하려면 별표(*)를 와일드카드로 사용할 수 있습니다.**CLI**—액세스를 허용하거나 거부할 CLI 번호를 입력합니다. 별표(*)를 와일드카드로 사용하여 번호의 일부를 기준으로 액세스를 허용하거나 거부할 수 있습니다.**팁:** Cisco Aironet Client MAC 주소와 같은 다른 값을 기준으로 액세스를 제한하려면 CLI 항목을 사용합니다. 자세한 내용은 네트워크 액세스 제한 정보 섹션을 참조하십시오.**DNIS** - 액세스를 허용하거나 거부할 DNIS 번호를 입력합니다. 사용자가 전화를 걸 번호를 기준으로 액세스를 제한하려면 이 항목을 사용합니다. 별표(*)를 와일드카드로 사용하여 번호의 일부를 기준으로 액세스를 허용하거나 거부할 수 있습니다.**팁:** Cisco Aironet AP MAC 주소와 같은 다른 값을 기준으로 액세스를 제한하려면 DNIS 선택을 사용합니다. 자세한 내용은 네트워크 액세스 제한 정보 섹션을 참조하십시오.**참고:** AAA Client 목록 및 **Port**, **CLI** 및 **DNIS** 상자의 총 문자 수는 1024를 초과할 수 없습니다. NAR을 추가할 때 ACS에서 1024자를 초과하는 문자를 허용하지만, NAR을 수정할 수 없으며 ACS는 사용자에게 정확하게 적용할 수 없습니다.Enter를 **클릭합니다**.AAA 클라이언트, 포트, CLI 및 DNIS를 지정하는 정보는 AAA Client 목록 위의 테이블에 나타납니다.
5. 사용자 계정 옵션 구성을 마쳤으면 **Submit**(제출)을 클릭하여 옵션을 기록합니다.

사용자 그룹에 대한 네트워크 액세스 제한 설정

Group Setup(그룹 설정)에서 Network Access Restrictions(네트워크 액세스 제한) 테이블을 사용하여 다음과 같은 세 가지 방법으로 NAR을 적용합니다.

- 이름으로 기존 공유 NAR을 적용합니다.
- IP 연결이 설정된 경우 지정된 AAA 클라이언트 또는 AAA 클라이언트의 지정된 포트에 대한 액세스를 허용 또는 거부하도록 IP 기반 그룹 액세스 제한을 정의합니다.
- CLI/DNIS 기반 그룹 NAR을 정의하여 사용된 CLI 번호 또는 DNIS 번호에 대한 액세스를 허용하거나 거부합니다.**참고:** CLI/DNIS 기반 액세스 제한 영역을 사용하여 다른 값을 지정할 수도 있습니다. 자세한 내용은 네트워크 액세스 제한 정보 섹션을 참조하십시오.

일반적으로 공유 구성 요소 섹션에서 NAR을 정의하여 둘 이상의 그룹 또는 사용자에게 이러한 제한을 적용할 수 있습니다. 자세한 내용은 공유 NAR 추가 섹션을 참조하십시오. 이러한 옵션이 ACS 웹 인터페이스에 나타나려면 Interface Configuration 섹션의 **Advanced Options** 페이지에서 **Group-Level Shared Network Access Restriction** 확인란을 선택해야 합니다.

그러나 ACS를 사용하여 **Group Setup** 섹션 내에서 단일 그룹에 대한 NAR을 정의하고 적용할 수도 있습니다. 단일 그룹 IP 기반 필터 옵션 및 단일 그룹 CLI/DNIS 기반 필터 옵션이 ACS 웹 인터페이스에 나타날 경우 Interface Configuration 섹션의 Advanced Options 페이지 아래에서 **Group-Level Network Access Restriction** 설정을 확인해야 합니다.

참고: 인증 요청이 프록시에 의해 ACS 서버로 전달되면 RADIUS 요청에 대한 모든 NAR은 원래 AAA 클라이언트의 IP 주소가 아니라 전달 AAA 서버의 IP 주소에 적용됩니다.

사용자 그룹에 대한 NAR을 설정하려면 다음 단계를 완료합니다.

1. 탐색 모음에서 **그룹 설정**을 클릭합니다.그룹 설정 선택 창이 열립니다.
2. 그룹 목록에서 그룹을 선택한 다음 **설정 편집**을 클릭합니다.그룹 이름이 그룹 설정 창 상단에 나타납니다
   .