UNIX용 CSU 구성(Solaris)

목차

소개

Cisco Secure ACS for UNIX(CSU) 소프트웨어는 네트워크의 보안을 보장하고 네트워크에 성공적으로 연결된 사용자의 활동을 추적하는 데 도움이 됩니다.CSU는 TACACS+ 또는 RADIUS 서버 역할을 하며 AAA(Authentication, Authorization, and Accounting)를 사용하여 네트워크 보안을 제공합니다.

CSU는 다음과 같은 데이터베이스 옵션을 지원하여 그룹 및 사용자 프로필과 계정 정보를 저장합니다.

- SQLAnywhere(CSU에 포함).이 버전의 Sybase SQLAnywhere에는 클라이언트/서버 지원이 없습니다.그러나 CSU를 사용하여 필수 AAA 서비스를 수행하도록 최적화되었습니다.**주의:** SQLAnywhere 데이터베이스 옵션은 사용자 5,000명을 초과하는 프로필 데이터베이스, 데이터베이스 사이트 간 프로필 정보 복제 또는 Cisco DSM(Secure Distribute Session Manager) 기능을 지원하지 않습니다.
- Oracle 또는 Sybase RDBMS(Relational Database Management System).5,000명 이상의 사용자, 데이터베이스 복제 또는 Cisco Secure DSM 기능으로 구성된 Cisco Secure 프로파일 데이터베이스를 지원하려면 Cisco Secure 프로파일 정보를 보관할 Oracle(버전 7.3.2, 7.3.3 또는 8.0.3) 또는 Sybase SQL Server(버전 11) RDBMS를 미리 설치해야 합니다.Cisco Secure 설치가 완료된 후 데이터베이스 복제를 수행하려면 추가 RDBMS 구성이 필요합니다.

- 기존 데이터베이스를 이전(2.x) 버전의 CSU에서 업그레이드합니다.이전 2.x 버전의 Cisco Secure에서 업그레이드할 경우 Cisco Secure 설치 프로그램은 프로파일 데이터베이스를 UNIX용 CSU 2.3과 호환되도록 자동으로 업그레이드합니다.
- 기존 프로파일 데이터베이스를 가져오는 중입니다.기존 프리웨어 TACACS+ 또는 RADIUS 프로파일 데이터베이스 또는 플랫 파일을 이 버전의 CSU와 함께 사용하도록 변환할 수 있습니다 .

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 UNIX용 Cisco Secure ACS 2.3을 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 참조하십시오.

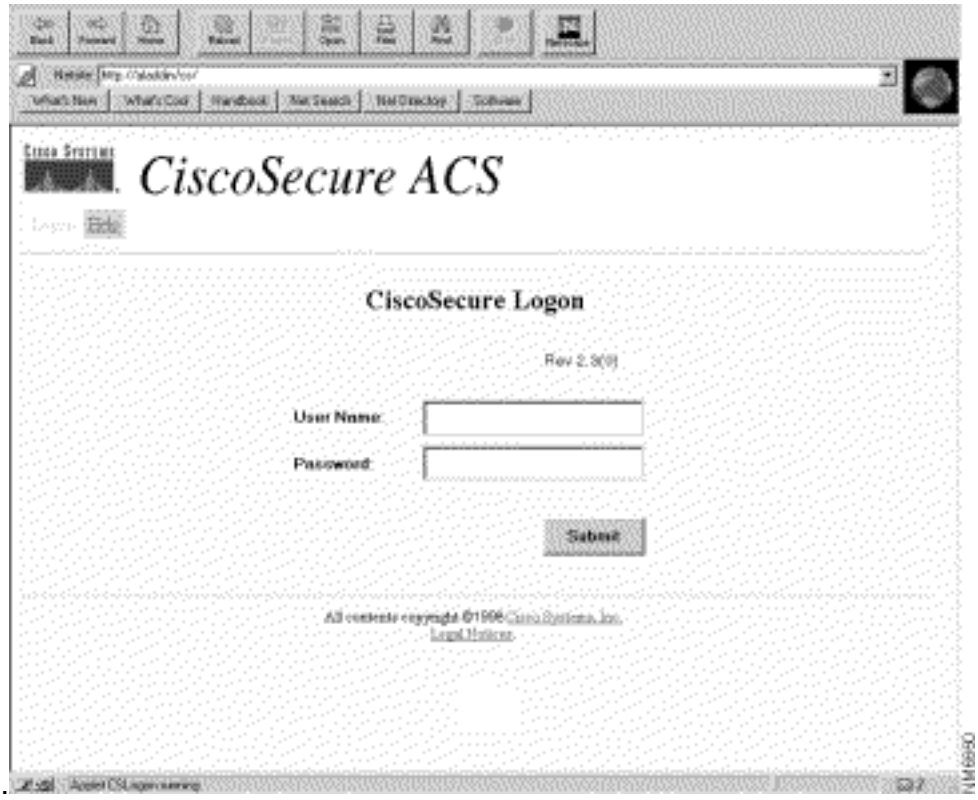
CSU 컨피그레이션

다음 절차에 따라 CSU를 구성합니다.

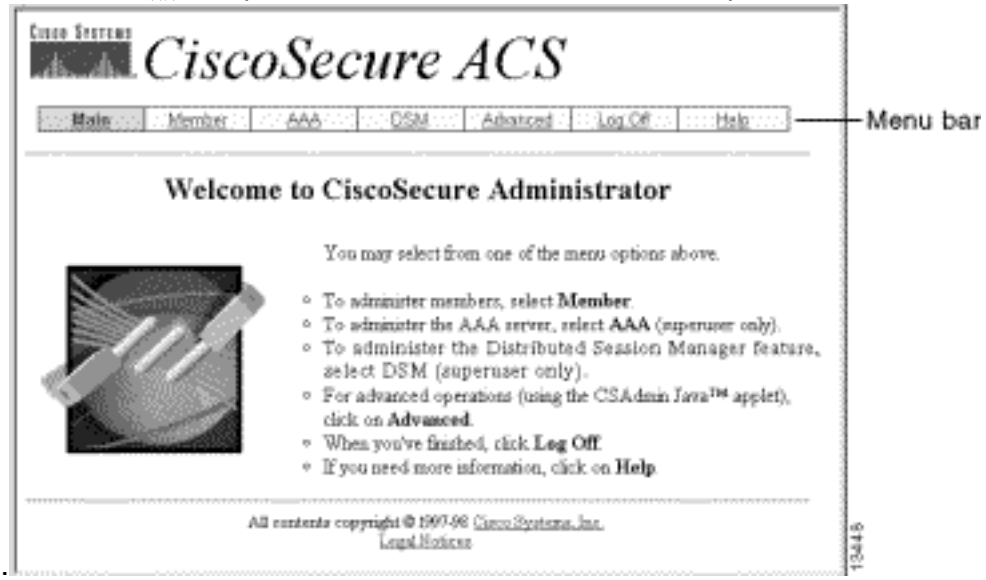
Cisco Secure Administrator 인터페이스 시작

이 절차를 사용하여 Cisco Secure Administrator에 로그인합니다.

1. ACS에 대한 웹 연결이 있는 워크스테이션에서 웹 브라우저를 시작합니다.
2. Cisco Secure Administrator 웹 사이트의 다음 URL 중 하나를 입력합니다.브라우저에서 보안 소켓 레이어 기능이 활성화되지 않은 경우 다음을 입력합니다.
   ```
   http://your_server/cs
   ```
   여기서 your_server는 CSU를 설치한 SPARCstation의 호스트 이름(또는 호스트 이름과 FQDN이 다른 경우 FQDN)입니다.SPARCstation의 IP 주소를 your_server로 대체할 수도 있습니다.브라우저에서 보안 소켓 레이어 기능이 활성화된 경우 하이퍼텍스트 전송 프로토콜로 "http"가 아닌 "https"를 지정합니다.다음을 입력합니다.
   ```
   https://your_server/cs
   ```
   여기서 your_server는 CSU를 설치한 SPARCstation의 호스트 이름(또는 호스트 이름과 FQDN이 다른 경우 FQDN)입니다.SPARCstation의 IP 주소를 your_server로 대체할 수도 있습니다.**참고:** URL 및 서버 이름은 대/소문자를 구분합니다.표시된 대로 정확하게 대문자와 소문자로 입력해야 합니다.CSU 로그온 페이지가 표시됩니다



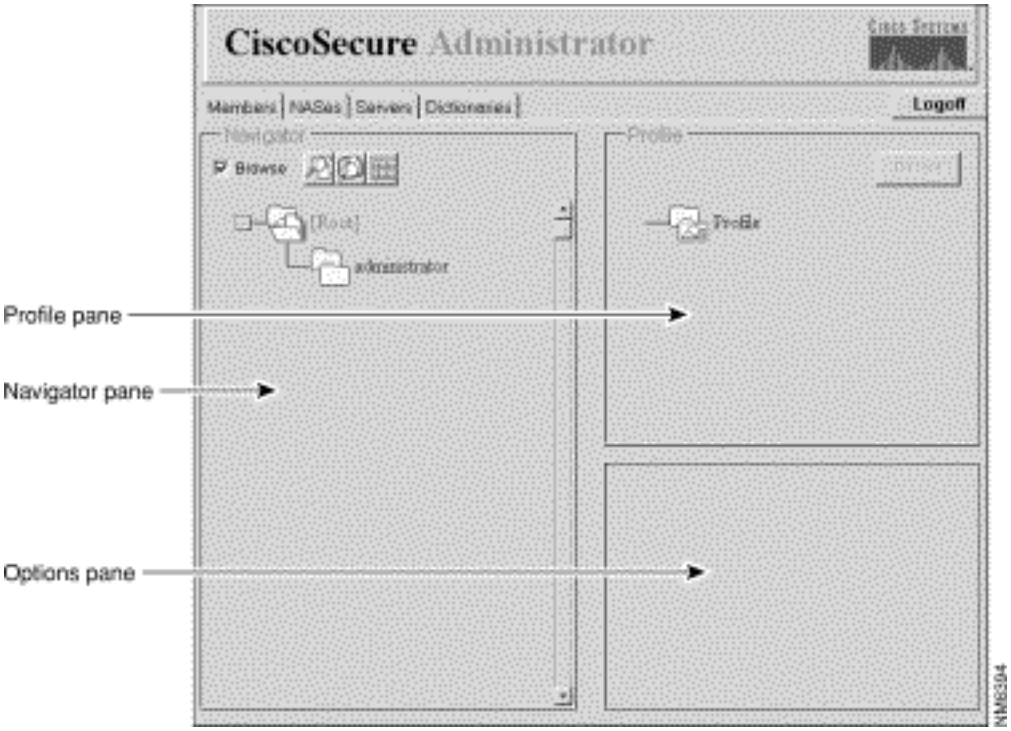
3. 사용자 이름과 비밀번호를 입력합니다.Submit(제출)**을 클릭합니다.참고:** 초기 기본 사용자 이름은 "수퍼유저"입니다. 초기 기본 비밀번호는 "changeme"입니다. 최초 로그인 후 보안을 극대화하려면 즉시 사용자 이름과 비밀번호를 변경해야 합니다.로그인한 후 CSU 주 페이지가 맨 위에 기본 메뉴 모음과 함께 표시됩니다.CSU Main(CSU 기본) 메뉴 페이지는 사용자가 관리자 레벨 권한을 가진 이름과 비밀번호를 제공하는 경우에만 표시됩니다.사용자가 사용자 수준 권한만 있는 이름과 암호를 제공하면 다른 화면이 표시됩니다



고급 구성 프로그램 시작

CSU 관리자 웹 페이지에서 Java 기반 Cisco Secure Administrator Advanced Configuration 프로그램을 시작합니다.CSU 웹 인터페이스의 메뉴 모음에서 **Advanced(고급)**를 클릭한 다음 **Advanced(고급)를** 다시 클릭합니다.

Cisco Secure Administrator Advanced Configuration 프로그램이 표시됩니다.로드하는 데 몇 분 정도 걸릴 수 있습니다.

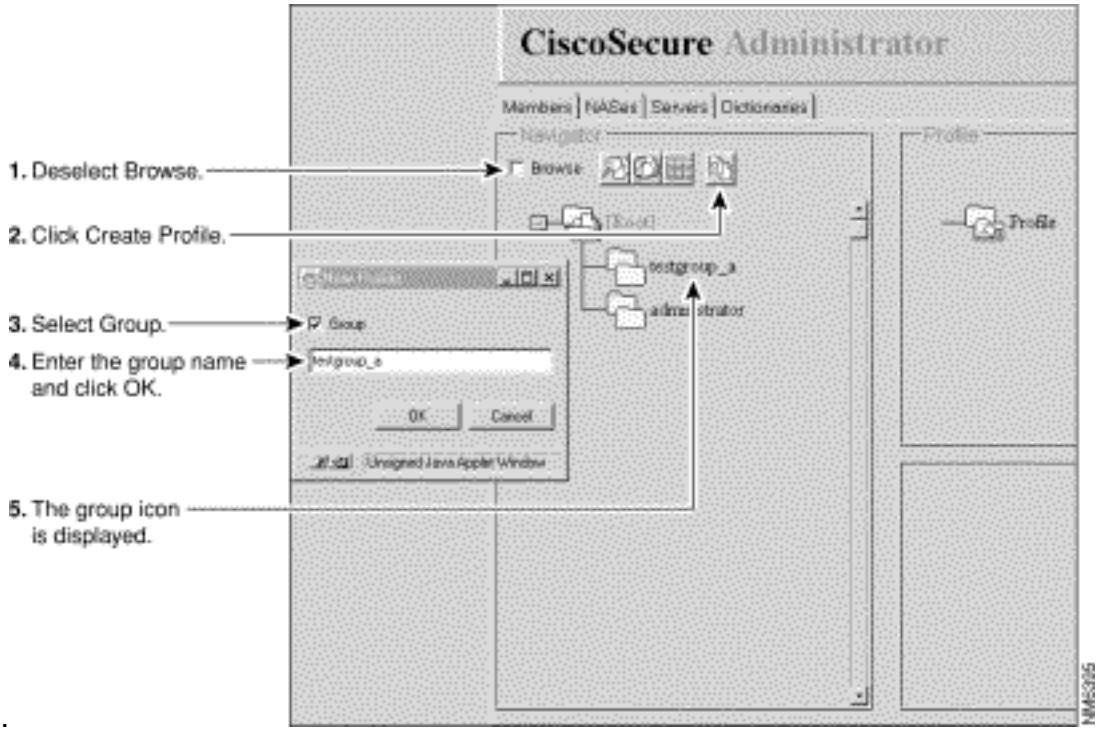


그룹 프로필 생성

Cisco Secure Administrator Advanced Configuration 프로그램을 사용하여 그룹 프로필을 생성하고 구성합니다.다수의 유사 사용자에 대한 자세한 AAA 요구 사항을 구성하기 위해 그룹 프로필을 생성하는 것이 좋습니다.그룹 프로필을 정의한 후 CSU Add a User(사용자 추가) 웹 페이지를 사용하여 그룹 프로필에 사용자 프로필을 빠르게 추가합니다.그룹에 대해 구성된 고급 요구 사항은 각 구성원 사용자에게 적용됩니다.

이 절차를 사용하여 그룹 프로필을 생성합니다.

1. Cisco Secure Administrator Advanced Configuration 프로그램에서 **Members** 탭을 선택합니다.네비게이터 창에서 **찾아보기** 확인란을 선택 취소합니다.새 프로필 생성 아이콘이 표시됩니다.
2. 네비게이터 창에서 다음 중 하나를 수행합니다.상위 항목이 없는 그룹 프로필을 생성하려면 **[Root]** 폴더 아이콘을 찾아 클릭합니다.그룹 프로필을 다른 그룹 프로필의 자식으로 만들려면 상위 그룹 프로필을 찾아 클릭합니다.상위 그룹이 하위 그룹인 경우 해당 상위 그룹의 폴더를 눌러 해당 그룹을 표시합니다.
3. Create **New Profile을 클릭합니다**.New Profile 대화 상자가 표시됩니다.
4. **그룹** 확인란을 선택하고 생성할 그룹의 이름을 입력한 다음 **확인**을 클릭합니다.트리에 새 그룹이 표시됩니다.
5. 그룹 프로필을 생성한 후 TACACS+ 또는 RADIUS 특성을 할당하여 특정 AAA 속성을 구성합



니다.

고급 구성 모드에서 사용자 프로필 생성

Cisco Secure Administrator Advanced Configuration 모드를 사용하여 사용자 프로필을 생성하고 구성합니다.Add a User(사용자 추가) 페이지에서 가능한 것보다 더 세부적으로 사용자 프로필의 권한 부여 및 회계 관련 속성을 사용자 정의할 수 있습니다.

다음 절차에 따라 사용자 프로필을 생성합니다.

1. Cisco Secure Administrator Advanced Configuration 프로그램에서 **Members** 탭을 선택합니다.네비게이터 창에서 찾아보기를 찾아 선택 **취소합니다**.새 프로필 생성 아이콘이 표시됩니다.
2. 네비게이터 창에서 다음 중 하나를 수행합니다.사용자가 속한 그룹을 찾아 클릭합니다.사용자가 그룹에 속하지 않게 하려면 [**Root**] 폴더 아이콘을 클릭합니다.
3. Create **Profile을 클릭합니다**.New Profile 대화 상자가 표시됩니다.
4. **그룹** 확인란이 선택 취소되었는지 확인합니다.
5. 생성할 사용자의 이름을 입력하고 **확인**을 클릭합니다.새 사용자가 트리에 표시됩니다.
6. 사용자 프로필을 생성한 후 특정 TACACS+ 또는 RADIUS 특성을 할당하여 특정 AAA 속성을 구성합니다.사용자 프로필에 TACACS+ 프로파일을 할당하려면 그룹 또는 사용자 프로필에 TACACS+ 특성 할당을 참조하십시오.사용자 프로필에 RADIUS 프로파일을 할당하려면 그룹 또는 사용자 프로필에 RADIUS 특성 할당을 참조하십시오.

특성 적용 전략

CSU를 통해 네트워크 사용자에 대한 인증 및 권한 부여를 구현하려면 CSU 그룹 프로필 기능 및 TACACS+ 및 RADIUS 특성을 사용합니다.

그룹 및 사용자에 대한 계획 속성

CSU의 그룹 프로필 기능을 사용하면 다수의 사용자에 대한 공통 AAA 요구 사항 집합을 정의할 수 있습니다.

그룹 프로필에 TACACS+ 또는 RADIUS 특성 값 집합을 할당할 수 있습니다.그룹에 할당된 이러한 속성 값은 멤버이거나 해당 그룹의 구성원으로 추가된 모든 사용자에게 적용됩니다.

효과적으로 그룹 프로필 기능 사용

복잡한 AAA 요구 사항을 가진 다수의 사용자 및 다양한 유형의 사용자를 관리하도록 CSU를 구성하려면 Cisco Secure Administrator Advanced Configuration 프로그램의 기능을 사용하여 그룹 프로파일을 생성하고 구성하는 것이 좋습니다.

그룹 프로필은 사용자에 특정하지 않은 모든 특성을 포함해야 합니다.이는 일반적으로 비밀번호를 제외한 모든 속성을 의미합니다.그런 다음 Cisco Secure Administrator의 Add a User(사용자 추가) 페이지를 사용하여 비밀번호 속성을 가진 간단한 사용자 프로파일을 생성하고 이러한 사용자 프로파일을 적절한 그룹 프로파일에 할당할 수 있습니다.특정 그룹에 대해 정의된 기능 및 속성 값이 해당 멤버 사용자에게 적용됩니다.

상위 그룹 및 하위 그룹

그룹 계층을 생성할 수 있습니다.그룹 프로필 내에서 하위 그룹 프로필을 생성할 수 있습니다.상위 그룹 프로필에 지정된 속성 값은 하위 그룹 프로필의 기본값입니다.

그룹 수준 관리

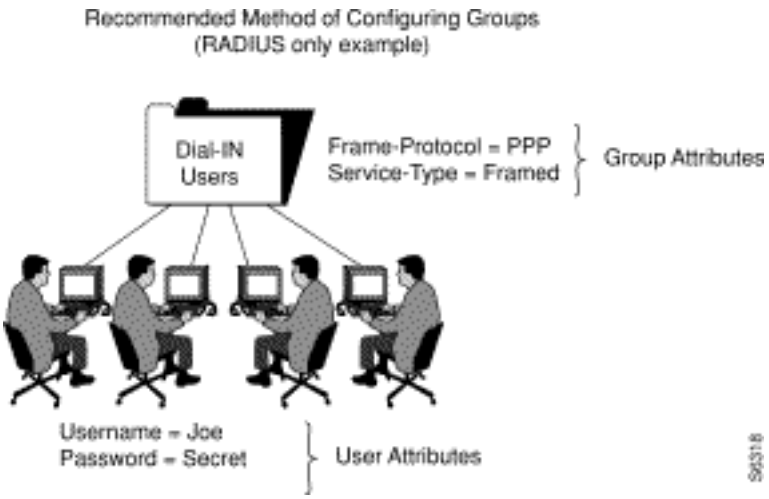
Cisco Secure 시스템 관리자는 개별 Cisco Secure 사용자 그룹 관리자 상태를 할당할 수 있습니다.그룹 관리자 상태를 사용하면 개별 사용자가 하위 그룹 프로필 및 그룹에 종속된 사용자 프로필을 관리할 수 있습니다.그러나 그룹 계층 구조를 벗어나는 그룹 또는 사용자를 관리할 수는 없습니다.따라서 시스템 관리자는 각 개인에게 동등한 권한을 부여하지 않고 대규모 네트워크를 관리하는 임무를 수행하게 됩니다.

개별 사용자에 대해 어떤 특성을 정의합니까?

사용자 이름, 비밀번호, 비밀번호 유형 및 웹 권한을 정의하는 속성 등 사용자에게 고유한 기본 인증 속성 값을 개별 사용자에게 할당할 것을 권장합니다.CSU의 사용자 편집 또는 사용자 추가 페이지를 통해 기본 인증 속성 값을 사용자에게 할당합니다.

그룹 프로파일에 대해 어떤 특성을 정의합니까?

그룹 레벨에서 자격, 권한 부여 및 회계 관련 특성을 정의할 것을 권장합니다.



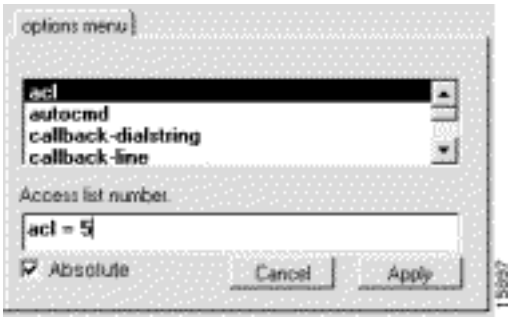
이 예에서 "Dial-In Users"라는 그룹 프로필에는 특성-값 쌍 Frame-Protocol=PPP 및 Service-Type=Framed가 할당됩니다.

절대 특성이란?

CSU의 TACACS+ 및 RADIUS 특성의 하위 집합은 그룹 프로파일 레벨에서 절대 상태를 할당할 수 있습니다.그룹 프로파일 레벨에서 절대 상태에 대해 활성화된 속성 값은 하위 그룹 프로파일 또는 멤버 사용자 프로파일 레벨의 모든 컨텐트 속성 값을 재정의합니다.

여러 레벨의 그룹 관리자가 있는 다중 레벨 네트워크 내에서 절대 속성을 사용하면 시스템 관리자가 하위 레벨의 그룹 관리자가 재정의할 수 없는 선택된 그룹 속성 값을 설정할 수 있습니다.

절대 상태를 지정할 수 있는 속성은 Cisco Secure Administrator Advanced Configuration 프로그램의 Attributes(특성) 상자에 Absolute(절대) 확인란을 표시합니다.절대 상태를 활성화하려면 확인란을 선택합니다.



속성 값과 사용자 속성 값이 충돌할 수 있습니까?

상위 그룹 프로파일, 하위 그룹 프로파일 및 멤버 사용자 프로파일에 할당된 특성 값 간의 충돌 해결은 특성 값이 절대인지, 그리고 TACACS+ 또는 RADIUS 특성인지 여부에 따라 달라집니다.

- 절대 상태의 그룹 프로파일에 할당된 TACACS+ 또는 RADIUS 특성 값은 하위 그룹 또는 사용자 프로필 레벨에서 설정된 모든 컨텍스트 속성 값을 재정의합니다.
- TACACS+ 특성 값의 절대 상태가 그룹 프로파일 레벨에서 활성화되지 않은 경우 하위 그룹 또는 사용자 프로파일 레벨에서 설정된 모든 컨텍스트 속성 값에 의해 재정의됩니다.
- 상위 그룹 레벨에서 RADIUS 특성 값의 절대 상태를 활성화하지 않으면 하위 그룹에 설정된 모든 컨텍스트 속성 값이 예측할 수 없는 결과를 생성합니다.그룹 및 해당 멤버 사용자에 대해 RADIUS 특성 값을 정의할 때 사용자 및 그룹 프로파일 모두에 동일한 특성을 할당하지 마십시

오.

금지 및 허용 옵션 사용

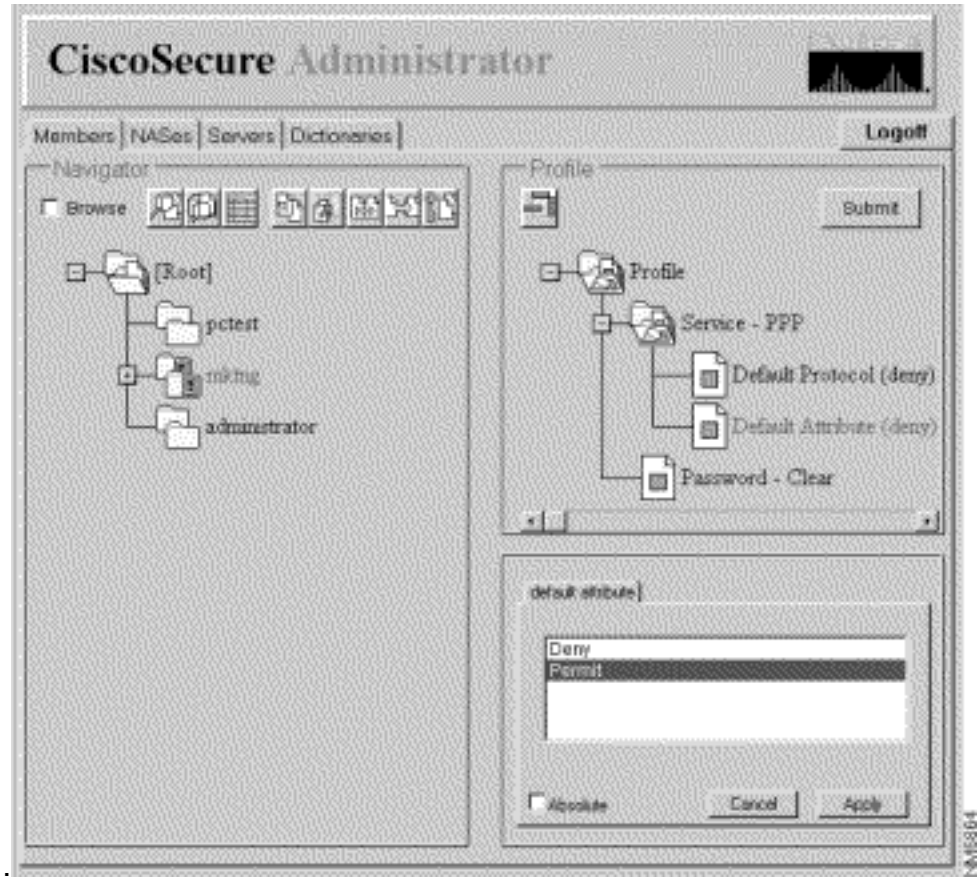
TACACS+의 경우 서비스 사양에 대해 키워드 **금지** 또는 **허용**을 미리 수정하여 상속된 서비스 값의 가용성을 재정의합니다.permit 키워드는 지정된 서비스를 허용합니다.prohibit 키워드는 지정된 서비스를 허용하지 않습니다.이러한 키워드를 함께 사용하면 "everything except" 컨피그레이션을 구성할 수 있습니다.예를 들어 이 컨피그레이션에서는 X.25를 제외한 모든 서비스에서 액세스할 수 있습니다.

```
default service = permit
prohibit service = x25
```

그룹 또는 사용자 프로필에 TACACS+ 특성 할당

그룹 또는 사용자 프로필에 특정 TACACS+ 서비스 및 특성을 할당하려면 다음 단계를 수행합니다.

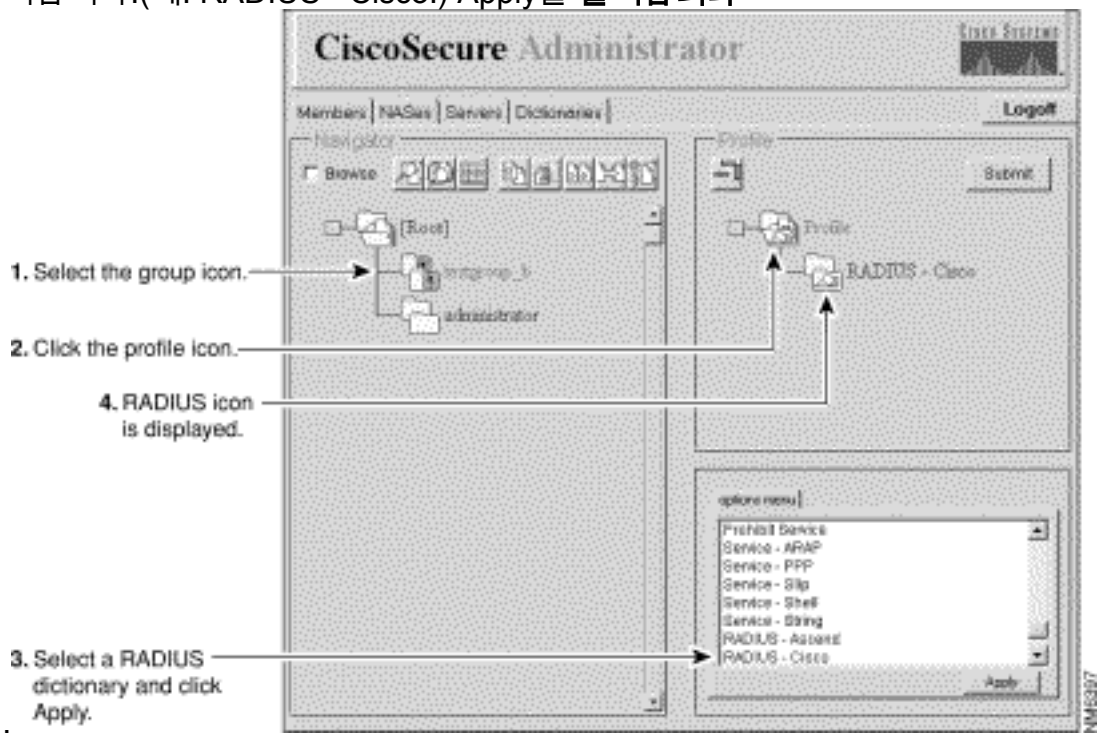
1. Cisco Secure Administrator Advanced Configuration 프로그램에서 **Members** 탭을 선택합니다.Navigator 창에서 TACACS+ 특성이 할당된 그룹 또는 사용자 프로필의 아이콘을 클릭합니다.
2. 필요한 경우 Profile(프로필) 창에서 Profile(**프로필**) 아이콘을 클릭하여 확장합니다.선택한 프로필 또는 서비스에 적용할 수 있는 특성이 포함된 목록 또는 대화 상자가 화면 오른쪽 하단에 있는 창에 표시됩니다.이 창의 정보는 프로필 창에서 선택한 프로필 또는 서비스에 따라 변경됩니다.
3. 추가할 서비스 또는 프로토콜을 클릭하고 Apply(적용)를 **클릭합니다**.서비스가 프로파일에 추가됩니다.
4. 속성 창에서 필요한 텍스트를 입력하거나 선택합니다.유효한 항목은 UNIX용 CSU 2.3 참조 설명서의 Strategies for Apply Attributes 섹션에서 설명합니다.**주:** 그룹 프로파일 레벨에서 속성 값을 지정하고 지정하는 속성에 **절대** 체크박스가 표시되면 해당 체크박스를 선택하여 값 절대 상태를 지정합니다.하위 그룹 프로필 또는 사용자 프로필 수준에서 할당된 모든 컨텍스트 값으로 값이 할당된 절대 상태를 재정의할 수 없습니다.
5. 추가해야 하는 추가 서비스 또는 프로토콜마다 1단계부터 1단계까지 반복합니다.
6. 모든 변경 사항이 발생하면 Submit(제출)을 **클릭합니다**



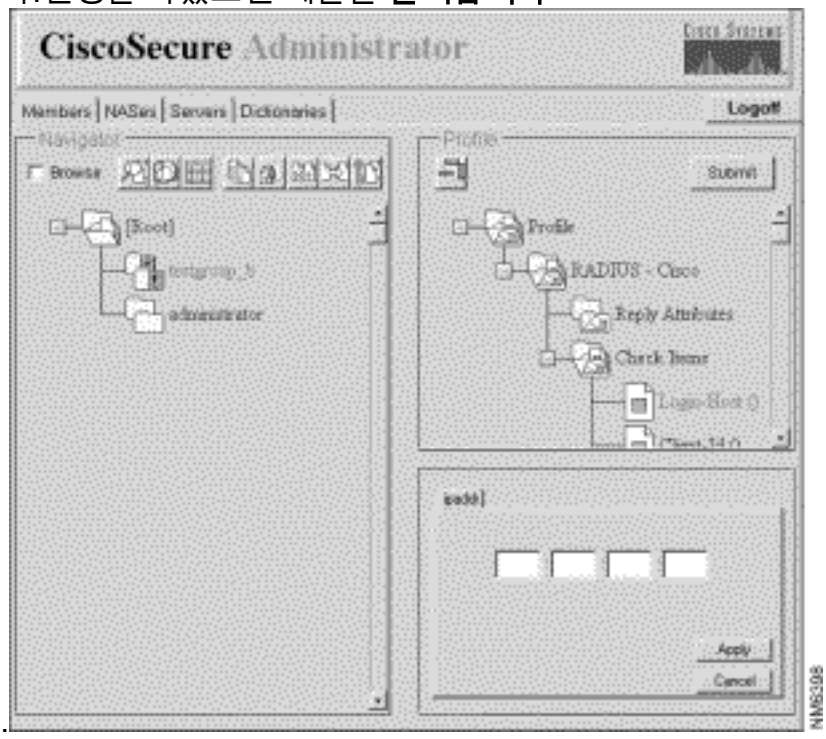
그룹 또는 사용자 프로필에 RADIUS 특성 할당

그룹 또는 사용자 프로필에 특정 RADIUS 특성을 할당하려면

1. 그룹 프로필에 RADIUS 사전을 할당합니다.Cisco Secure Administrator Advanced Configuration 프로그램의 Members(구성원) 페이지에서 **Group(그룹)** 또는 **User(사용자)** 아이콘을 클릭한 다음 Profiles(프로파일) 창에서 Profile(**프로필**) 아이콘을 클릭합니다.속성 창에 옵션 메뉴가 표시됩니다.**옵션** 메뉴에서 그룹 또는 사용자가 사용할 RADIUS 사전의 이름을 클릭합니다.(예: RADIUS - Cisco.) Apply를 **클릭합니다**



2. RADIUS 프로필에 필요한 확인 항목 및 회신 특성을 추가합니다.**참고:** 확인 항목은 사용자 ID 및 암호와 같은 인증에 필요한 특성입니다.Reply Attributes(회신 특성)는 프로파일이 Framed-Protocol과 같은 인증 절차를 통과한 후 NAS(Network Access Server)로 전송되는 특성입니다.Check Items(확인 항목) 및 Reply Attributes(회신 특성)에 대한 목록 및 설명은 CSU 2.3 for UNIX Reference Guide의 RADIUS Attribute-Value Pairs and Dictionary Management(RADIUS 특성-값 쌍 및 사전 관리)를 참조하십시오.프로파일 창에서 RADIUS - 사전 이름 폴더 아이콘을 클릭합니다.RADIUS 폴더를 확장하려면 프로필의 + 기호를 클릭해야 할 수 있습니다. 항목 확인 및 회신 속성 옵션이 속성 그룹 창에 표시됩니다.이러한 특성 중 하나 이상을 사용하려면 사용할 특성을 클릭한 다음 **적용**을 클릭합니다.한 번에 둘 이상의 특성을 추가할 수 있습니다.RADIUS - dictionaryname의 **+**기호를 클릭하여 폴더를 확장합니다.**참고:** RADIUS-Cisco11.3 옵션을 선택한 경우 Cisco IOS® 소프트웨어 릴리스 11.3.3(T) 이상이 연결 NAS에 설치되어 있는지 확인하고 NAS 구성에 새 명령줄을 추가합니다.UNIX용 CSU 2.3 참조 설명서의 RADIUS-Cisco11.3 사전 완전 활성화 를 참조하십시오.
3. 추가된 확인 항목 및 회신 속성 값을 지정합니다.**주의:** RADIUS 프로토콜의 경우 상속은 계층적 프로토콜과 반대로 가산됩니다.(TACACS+ 프로토콜은 계층 상속을 사용합니다.) 예를 들어, 사용자 및 그룹 프로필에 동일한 회신 속성을 할당하면 NAS에서 두 배의 특성 수를 수신하므로 권한 부여가 실패합니다.회신 특성을 이해할 수 없습니다.동일한 확인 항목 또는 회신 특성을 그룹 및 사용자 프로필 모두에 할당하지 마십시오.항목 **확인** 또는 **회신 속성**을 클릭하거나 둘 다 클릭합니다.적용 가능한 확인 항목 및 회신 속성 값 목록이 오른쪽 아래 창에 나타납니다.**+** 기호를 클릭하여 폴더를 확장합니다.할당할 값을 클릭한 다음 적용을 **클릭합니다**.값에 대한 자세한 내용은 UNIX용 CSU 2.3 참조 설명서의 RADIUS 특성-값 쌍 및 사전 관리를 참조하십시오.**주:** 그룹 프로파일 레벨에서 속성 값을 지정하고 지정하는 속성에 절대 확인란이 표시되면 해당 체크박스를 선택하여 값 절대 상태를 지정합니다.하위 그룹 프로필 또는 사용자 프로필 수준에서 할당된 모든 컨텍스트 값으로 절대 상태가 할당된 값을 재정의할 수 없습니다.변경을 마쳤으면 제출을 **클릭합니다**



4. 이러한 특성 중 하나 이상을 사용하려면 사용할 특성을 클릭한 다음 **적용**을 클릭합니다.한 번에 둘 이상의 특성을 적용할 수 있습니다.

액세스 제어 권한 레벨 할당

수퍼유저 관리자는 웹 권한 특성을 사용하여 Cisco Secure 사용자에게 액세스 제어 권한 수준을 할당합니다.

1. Cisco Secure Administrator Advanced Configuration 프로그램에서 액세스 제어 권한을 할당할 사용자를 클릭한 다음 Profiles 창에서 Profile 아이콘을 클릭합니다.
2. 옵션 메뉴에서 **웹 권한**을 클릭하고 다음 값 중 하나를 선택합니다.**0** - 사용자의 Cisco Secure 비밀번호를 변경할 수 있는 기능이 포함된 액세스 제어 권한을 사용자에게 거부합니다.**1** - CSUser 웹 페이지에 대한 사용자 액세스 권한을 부여합니다.이를 통해 Cisco Secure 사용자는 Cisco Secure 비밀번호를 변경할 수 있습니다.비밀번호 변경 방법에 대한 자세한 내용은 단순 사용자 및 ACS 관리의 사용자 레벨 기능(비밀번호 변경)을 참조하십시오.**12** - 사용자 그룹 관리자 권한을 부여합니다.**15** - 사용자 시스템 관리자 권한을 부여합니다.**참고:** 0 이외의 웹 권한 옵션을 선택하는 경우 비밀번호도 지정해야 합니다.웹 권한 암호 요구 사항을 충족하기 위해 빈 공간 하나가 최소한으로 허용됩니다.

CSU 시작 및 중지

일반적으로 CSU는 설치된 SPARCstation을 시작하거나 다시 시작하면 자동으로 시작됩니다.그러나 CSU를 수동으로 시작하거나 전체 SPARCSotion을 종료하지 않고 종료할 수 있습니다.

CSU를 설치한 SPARCStation에 [Root]로 로그인합니다.

CSU를 수동으로 시작하려면 다음을 입력합니다.

```
# /etc/rc2.d/S80CiscoSecure
```

CSU를 수동으로 중지하려면 다음을 입력합니다.

```
# /etc/rc0.d/K80CiscoSecure
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- UNIX용 Cisco Secure ACS 지원 페이지
- TACACS+ 지원 페이지
- RADIUS 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems