관리 계정에 대한 TACACS+ 인증을 지원하도록 Cisco VPN 3000 Concentrator를 구성하는 방법

목차

소개

이 문서에서는 관리 어카운트를 위한 TACACS+ 인증을 지원하도록 Cisco VPN 3000 Series Concentrator를 구성하기 위한 단계별 지침을 제공합니다.

VPN 3000 Concentrator에 TACACS+ 서버가 구성되면 admin, config, isp 등과 같이 로컬로 구성된 계정 이름과 비밀번호가 더 이상 사용되지 않습니다. VPN 3000 Concentrator에 대한 모든 로그인은 사용자 및 비밀번호 확인을 위해 구성된 외부 TACACS+ 서버로 전송됩니다.

TACACS+ 서버의 각 사용자에 대한 권한 레벨 정의는 각 TACACS+ 사용자 이름에 대한 VPN 3000 Concentrator에 대한 권한을 결정합니다. 그런 다음 VPN 3000 Concentrator에서 로컬로 구성된 사용자 이름 아래에 정의된 AAA 액세스 레벨과 일치시킵니다. TACACS+ 서버가 정의되면 VPN 3000 Concentrator에서 로컬로 구성된 사용자 이름이 더 이상 유효하지 않기 때문에 이 점이 중요합니다. 그러나 TACACS+ 서버에서 반환된 권한 수준을 해당 로컬 사용자 아래의 AAA Access Level과 일치시키기 위해서만 사용됩니다. 그런 다음 TACACS+ 사용자 이름에는 로컬로 구성된 VPN 3000 Concentrator 사용자가 자신의 프로필에 정의한 권한이 할당됩니다.

예를 들어, 구성 섹션에서 자세히 설명하면 TACACS+ 사용자/그룹이 TACACS+ 권한 레벨 15를 반환하도록 구성됩니다. VPN 3000 Concentrator의 Administrators(관리자) 섹션에서 관리 사용자는 AAA 액세스 레벨도 15로 설정됩니다. 이 사용자는 모든 섹션에서 구성을 수정하고 파일을 읽기/쓰도록 허용됩니다. TACACS+ 권한 레벨 및 AAA 액세스 레벨이 일치하므로 TACACS+ 사용자에게 VPN 3000 Concentrator에 대한 권한이 부여됩니다.

예를 들어 사용자가 컨피그레이션을 수정할 수는 있지만 읽기/쓰기 파일은 *수정할 수 없다고* 결정하면 TACACS+ 서버에 권한 레벨 12를 할당합니다. 1에서 15 사이의 숫자를 선택할 수 있습니다. 그런 다음 VPN 3000 Concentrator에서 로컬로 구성된 다른 관리자 중 하나를 선택합니다. 그런 다음 AAA Access Level(AAA 액세스 레벨)을 12로 설정하고, 이 사용자에 대한 권한을 설정하여 컨피그레이션을 수정할 수 있지만 파일을 읽고 쓸 수는 없습니다. 일치하는 권한/액세스 수준 때문에 사용자가 로그인할 때 해당 권한을 가져옵니다.

VPN 3000 Concentrator에서 로컬로 구성된 사용자 이름은 더 이상 사용되지 않습니다. 그러나 각 사용자 아래의 액세스 권한 및 AAA 액세스 레벨은 로그인 시 특정 TACACS+ 사용자가 얻을 수 있는 권한을 정의하기 위해 사용됩니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- VPN 3000 Concentrator에서 TACACS+ 서버에 대한 IP 연결이 있는지 확인합니다. TACACS+ 서버가 공용 인터페이스를 향하는 경우 공용 필터에서 TACACS+(TCP 포트 49)를 여는 것을 잊지 마십시오.
- 콘솔을 통한 백업 액세스가 작동 가능한지 확인합니다. 이 설정을 처음 설정할 때 모든 사용자를 컨피그레이션에서 실수로 잠그는 것이 쉽습니다. 액세스를 복구하는 유일한 방법은 로컬 구성 사용자 이름 및 비밀번호를 사용하는 콘솔을 통해서입니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco VPN 3000 Concentrator Software 릴리스 4.7.2.B(또는 3.0 이상 OS 소프트웨어의 모든 릴리스가 작동합니다.)
- Cisco Secure Access Control Server for Windows Servers 릴리스 4.0(또는 2.4 이상 소프트웨어의 모든 릴리스가 작동합니다.)

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.

TACACS+ 서버 구성

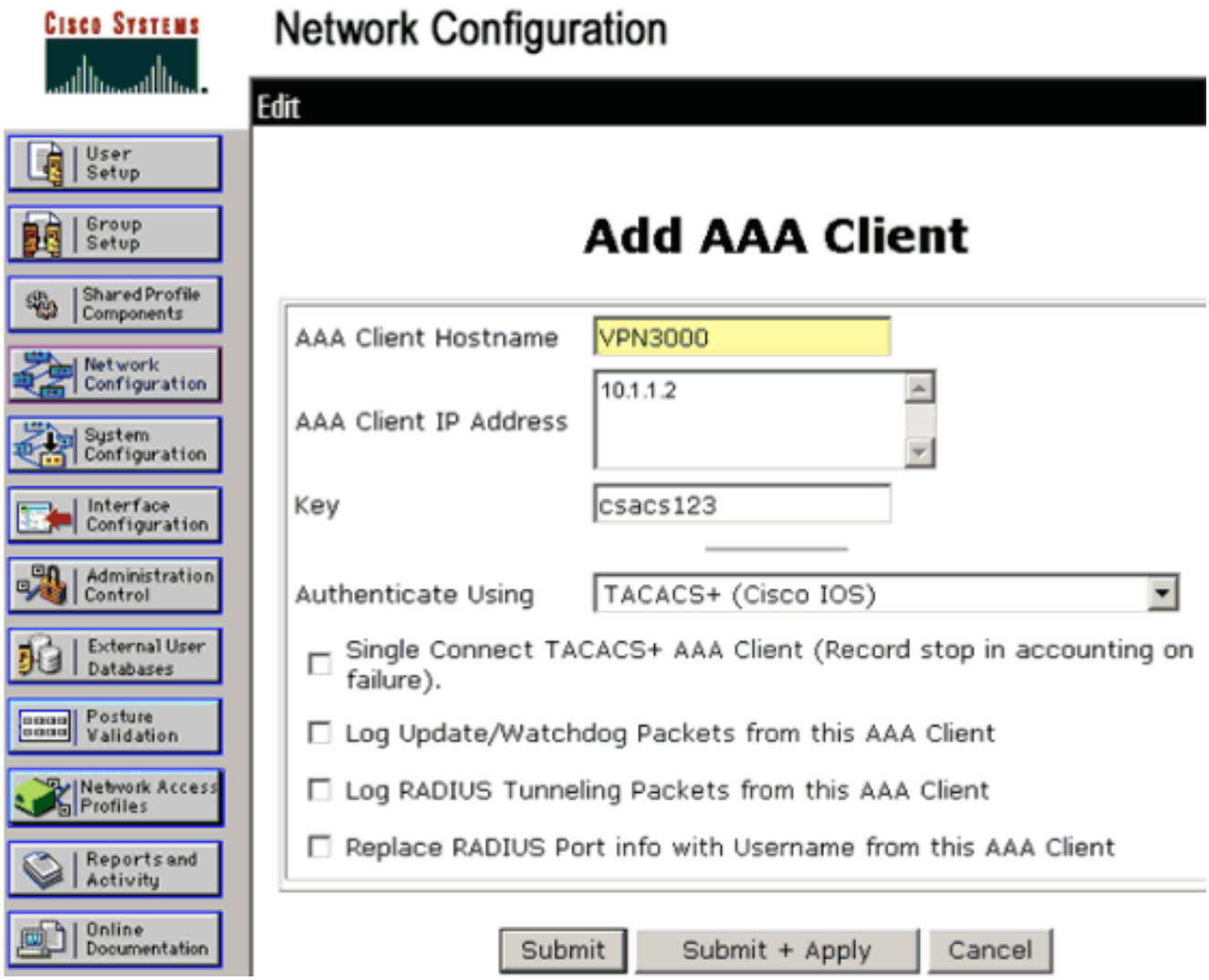
TACACS+ 서버에서 VPN 3000 Concentrator 항목 추가

TACACS+ 서버에서 VPN 3000 Concentrator에 대한 항목을 추가하려면 다음 단계를 완료합니다.

1. 왼쪽 패널**에서 Network Configuration(네트워크 컨피그레이션**)을 클릭합니다. AAA Clients(AAA 클라이언트)에서 Add **Entry(항목 추가)를** 클릭합니다.

2. 다음 창에서 양식을 입력하여 VPN Concentrator를 TACACS+ 클라이언트로 추가합니다. 이 예에서는 다음을 사용합니다.AAA 클라이언트 호스트 이름 = **VPN3000**AAA 클라이언트 IP 주소 = **10.1.1.2**키 = **csacs123**TACACS**+(Cisco IOS)를** 사용하여 **인증**Submit **+Restart를 클릭합니다**

.



TACACS+ 서버에서 사용자 계정 추가

TACACS+ 서버에 사용자 계정을 추가하려면 다음 단계를 완료합니다.

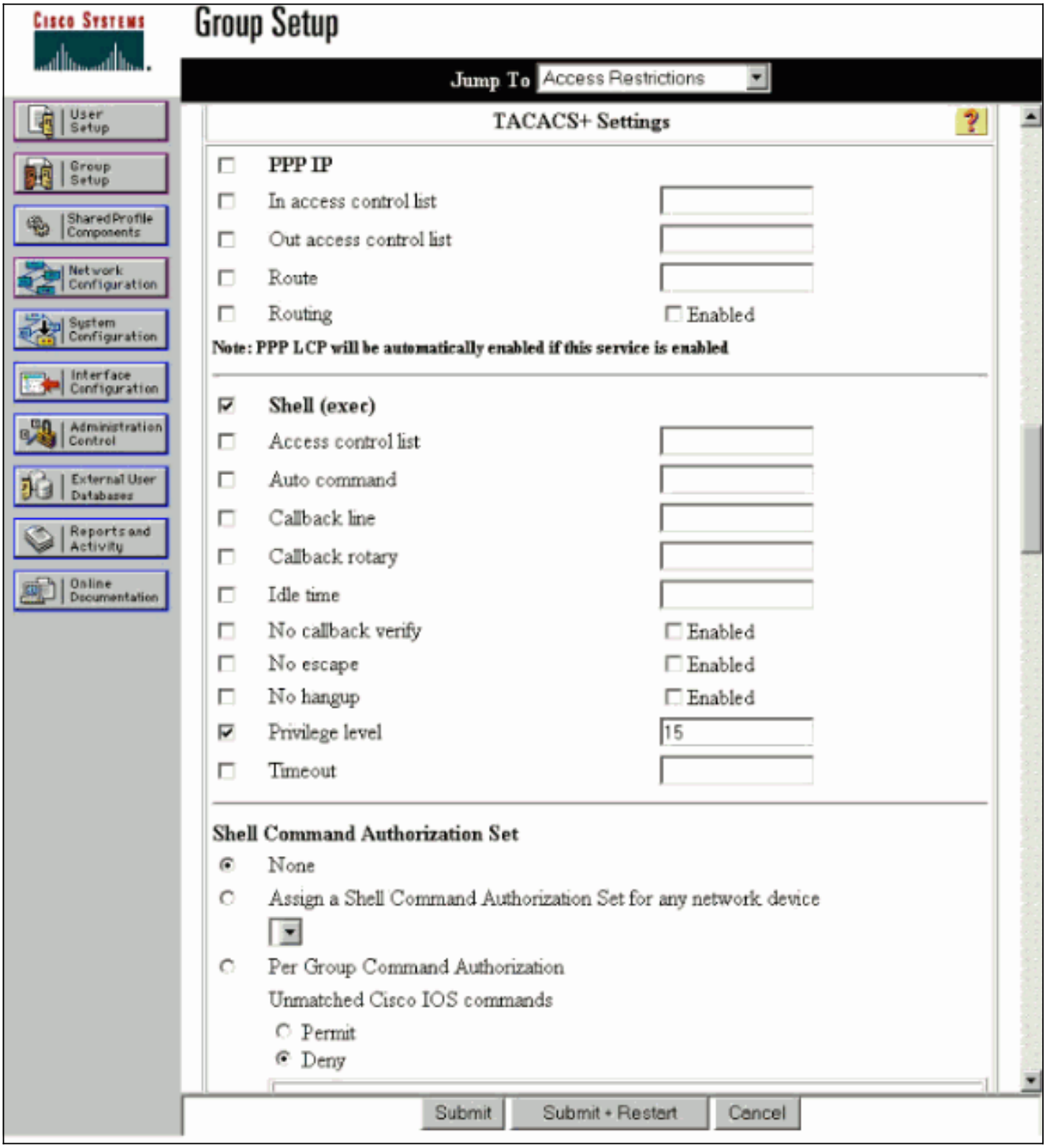
1. 나중에 TACACS+ 인증에 사용할 수 있는 사용자 계정을 TACACS+ 서버에서 생성합니다. 왼쪽 패널에서 **User Setup(사용자 설정)**을 클릭하고 "johnsmith" 사용자를 추가한 다음 Add/**Edit(추가/편집)**를 클릭하여 이 작업을 수행합니다.
2. 이 사용자의 비밀번호를 추가하고 다른 VPN 3000 Concentrator 관리자가 포함된 ACS 그룹에 사용자를 할당합니다.**참고:** 이 예에서는 이 특정 사용자 ACS 그룹 프로필에서 권한 레벨을 정의합니다. 사용자 단위로 이를 수행하려면 Interface Configuration(**인터페이스 컨피그레이션) > TACACS+(Cisco IOS)를** 선택하고 Shell(exec) 서비스의 **User**(사용자) 상자를 선택합니다. 이 문서에 설명된 TACACS+ 옵션만 각 사용자 프로필에서 사용할 수 있습니다.

TACACS+ 서버에서 그룹 편집

TACACS+ 서버에서 그룹을 수정하려면 다음 단계를 완료합니다.

1. 왼쪽 패널에서 Group Setup을 클릭합니다.
2. 드롭다운 메뉴에서 사용자가 추가된 그룹을 TACACS+ Server 섹션의 Add a User Account(사용자 계정 추가)에서 선택합니다(이 예에서는 Group 1). 그런 다음 **Edit Settings(설정 편집)**를 클릭합니다.
3. 다음 창의 TACACS+ Settings(TACACS+ 설정) 아래에서 이러한 특성이 선택되었는지 확인합니다.**셸(exec)권한 수준 = 15**완료되면 **Submit + Restart**를 클릭합니다

.

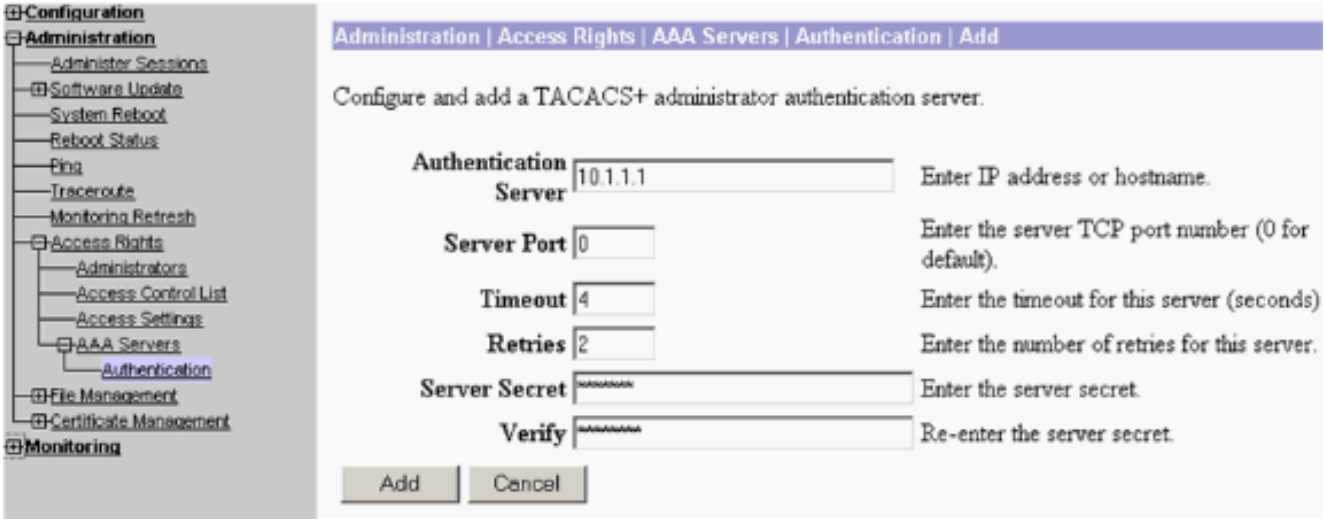


VPN 3000 Concentrator 구성

VPN 3000 Concentrator에서 TACACS+ 서버에 대한 항목 추가

VPN 3000 Concentrator에서 TACACS+ 서버에 대한 항목을 추가하려면 다음 단계를 완료합니다.

1. 왼쪽 패널의 탐색 트리에서 **Administration(관리) > Access Rights(액세스 권한) > AAA Servers(AAA 서버)** > Authentication(인증)을 선택한 다음 오른쪽 패널에서 **Add(추가)**를 클릭합니다.이 서버를 추가하기 위해 **Add**(추가)를 클릭하는 즉시 VPN 3000 Concentrator에서 로컬로 구성된 사용자 이름/비밀번호는 더 이상 사용되지 않습니다. 잠금이 발생할 경우 콘솔을 통한 백업 액세스가 제대로 작동하는지 확인합니다.
2. 다음 창에서 다음과 같이 양식을 작성합니다.인증 서버 = **10.1.1.1**(TACACS+ 서버의 IP 주소)서버 포트 = **0**(기본값)시간 초과 = **4**재시도 = **2**서버 암호 = **csacs123**확인 = **csacs123**

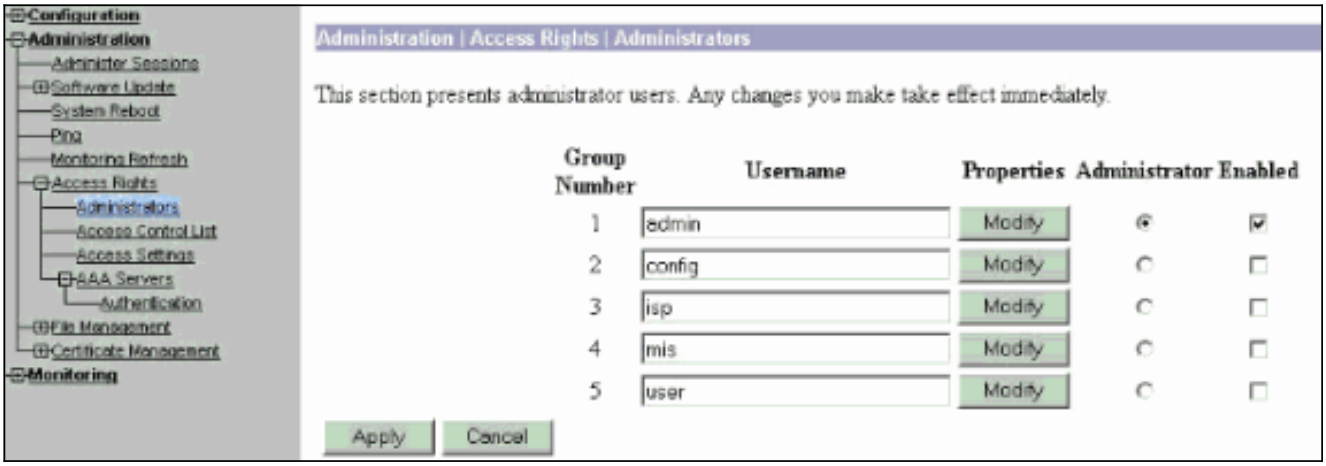


TACACS+ 인증을 위한 VPN Concentrator에서 관리 계정 수정

TACACS+ 인증을 위한 VPN Concentrator에서 관리자 계정을 수정하려면 다음 단계를 완료합니다.

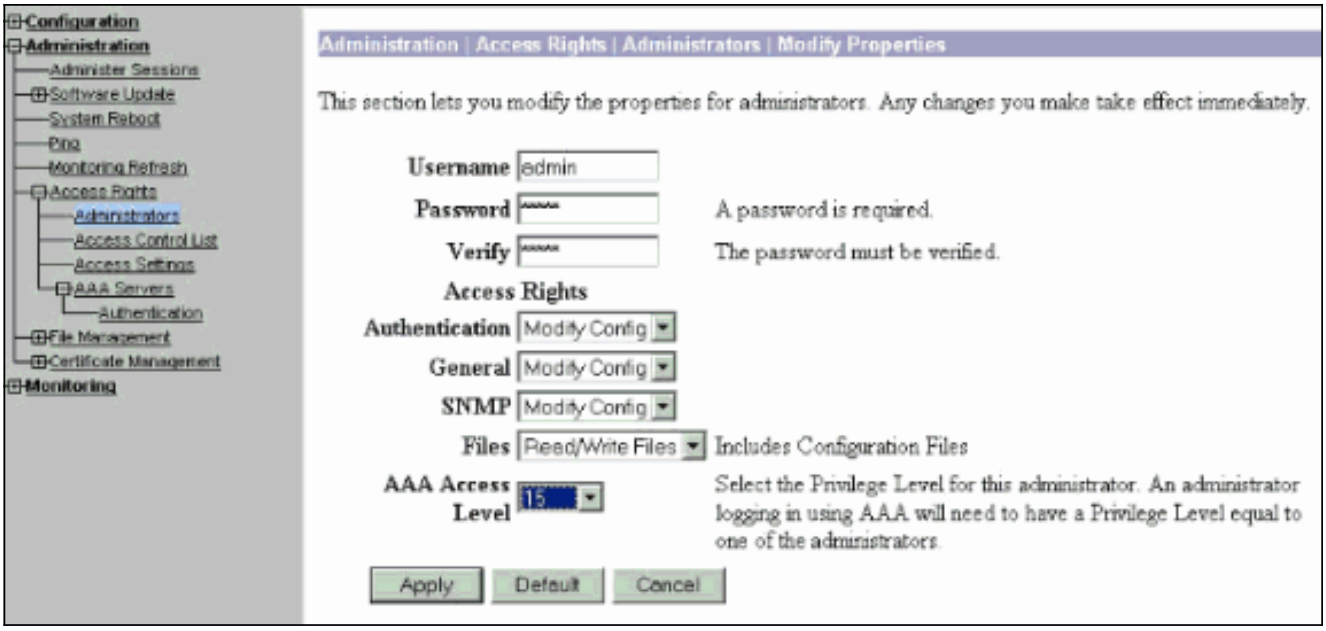
1. 이 사용자의 속성을 수정하려면 사용자 관리자에 대한 수정을 클릭합니다

.



2. AAA Access Level(AAA 액세스 레벨)을 **15**로 **선택합니다**.이 값은 1에서 15 사이의 숫자일 수 있습니다. TACACS+ 서버의 사용자/그룹 프로필에 정의된 TACACS+ 권한 레벨과 일치해야 합니다. 그런 다음 TACACS+ 사용자는 컨피그레이션 수정, 파일 읽기/쓰기 등에 대해 이 VPN 3000 Concentrator 사용자 아래에 정의된 권한을 선택합니다

.



다음을 확인합니다.

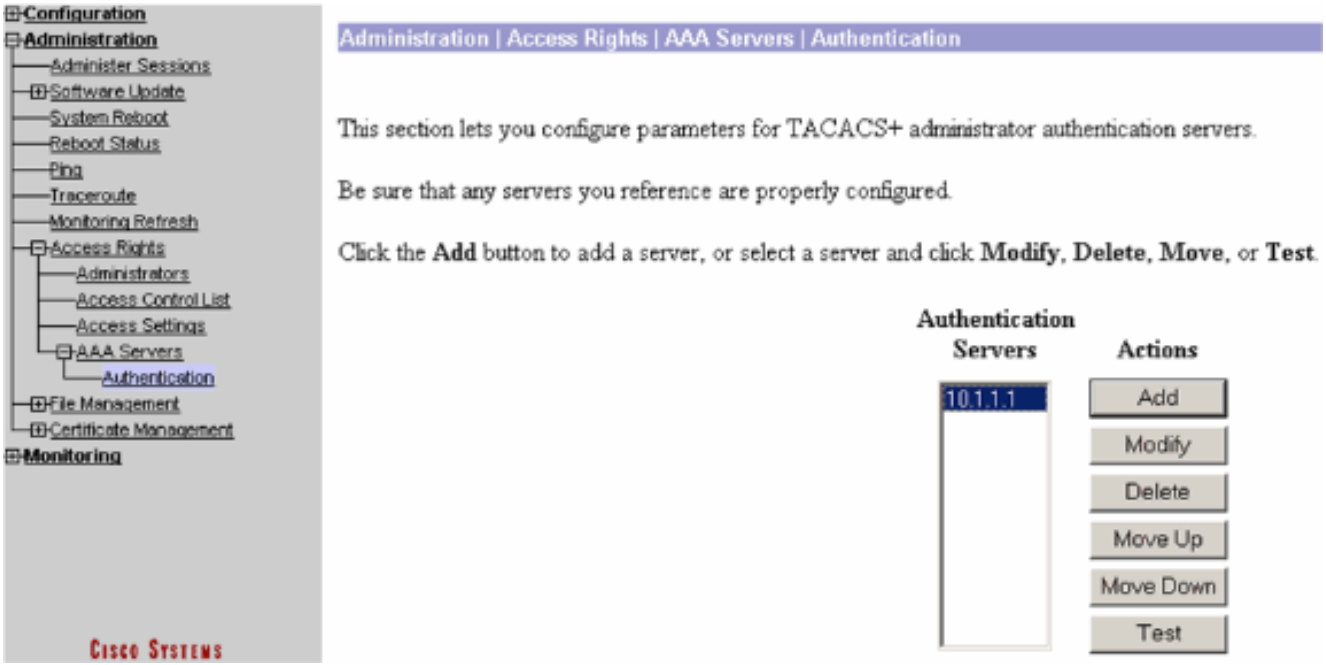
현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

컨피그레이션을 트러블슈팅하려면 이 지침의 단계를 완료합니다.

1. 인증을 테스트하려면TACACS+ 서버의 경우Administration(**관리) > Access Rights(액세스 권한) > AAA Servers(AAA 서버) > Authentication(인증)을 선택합니다**.서버를 선택한 다음 **테스트**를 클릭합니다

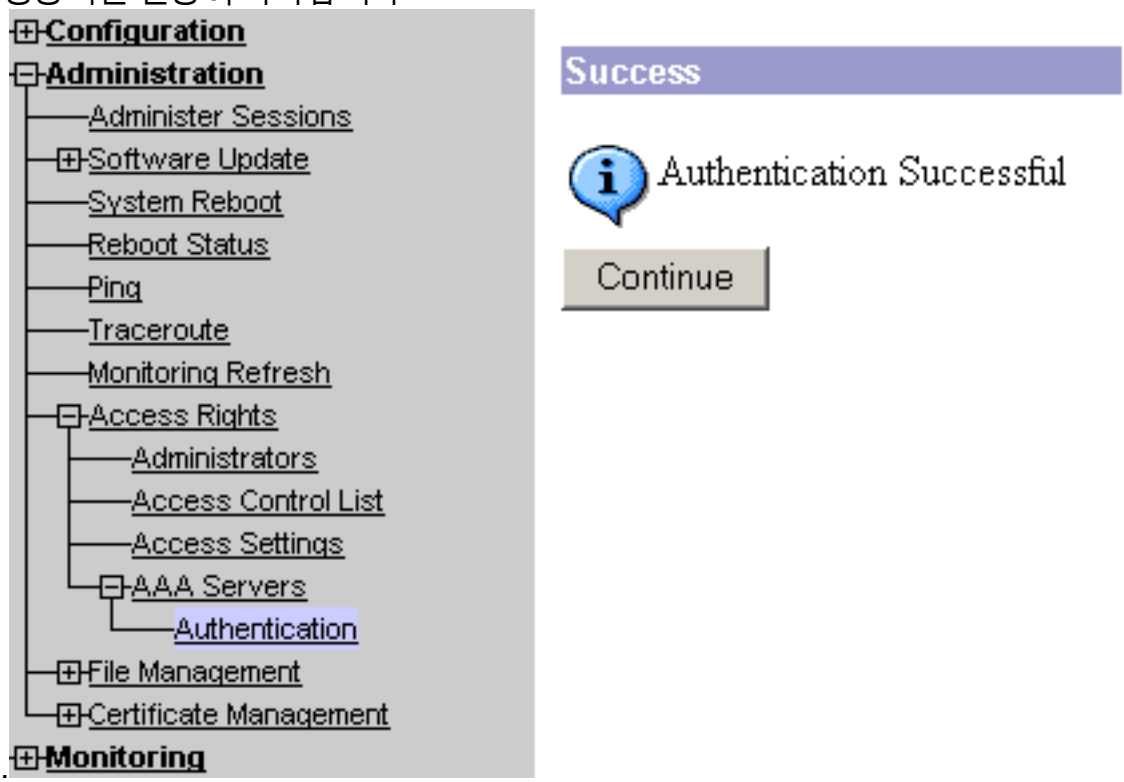
.



참고: Administration(관리) 탭에서 TACACS+ 서버가 구성된 경우 VPN 3000 로컬 데이터베이스에서 인증하도록 사용자를 설정할 방법이 없습니다. 다른 외부 데이터베이스 또는 TACACS 서버를 사용해서만 대체를 수행할 수 있습니다.TACACS+ 사용자 이름 및 비밀번호를 입력하고 **OK**(확인)를 클릭합니다

.

성공적인 인증이 나타납니다



.

2. 장애가 발생하면 구성 문제 또는 IP 연결 문제가 발생합니다. ACS 서버의 Failed Attempts Log에서 실패와 관련된 메시지를 확인합니다.이 로그에 메시지가 표시되지 않으면 IP 연결 문제가 발생할 수 있습니다. TACACS+ 요청이 TACACS+ 서버에 도달하지 않습니다. 적절한 VPN 3000 Concentrator 인터페이스에 적용된 필터가 TACACS+(TCP 포트 49) 패킷이 들어오고 나가는 것을 허용하는지 확인합니다.로그에 서비스 거부로 표시되는 오류가 TACACS+ 서버의 사용자 또는 그룹 프로필에서 셸(exec) 서비스가 올바르게 활성화되지 않은 경우
3. 테스트 인증이 성공했지만 VPN 3000 Concentrator에 대한 로그인이 계속 실패하면 콘솔 포트를 통해 Filterable Event Log(필터링 가능한 이벤트 로그)를 확인합니다.유사한 메시지가 표시되면

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.
Status: <REFUSED> authorization failure. NO Admin Rights
```

이 메시지는 TACACS+ 서버에 할당된 권한 수준이 VPN 3000 Concentrator 사용자 아래에 일치하는 AAA 액세스 레벨이 없음을 나타냅니다. 예를 들어 사용자 johnsmith는 TACACS+ 서버에 TACACS+ 권한 레벨이 7이지만 VPN 3000 Concentrator 관리자 5명 중 AAA 액세스 레벨이 7인 것은 없습니다.

관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 협상/IKE 프로토콜 지원 페이지
- TACACS/TACACS+ 지원 페이지
- IOS 설명서의 TACACS+
- 기술 지원 및 문서 – Cisco Systems