ACS와 Security Manager 통합

목차

소개

이 문서에서는 Cisco Security Manager를 Cisco ACS(Secure Access Control Server)와 통합하는 방법에 대해 설명합니다.

Cisco Secure ACS는 관리 네트워크 장치를 구성하기 위해 Cisco Security Manager와 같은 관리 애플리케이션을 활용하는 사용자에게 명령 권한 부여를 제공합니다.명령 권한 부여에 대한 지원은 Cisco Security Manager의 역할이라고 하는 고유한 명령 권한 부여 세트 유형에서 제공되며 권한 집합이 포함되어 있습니다.권한이라고도 하는 이러한 권한은 Cisco Security Manager 내에서 특정 역할을 가진 사용자가 수행할 수 있는 작업을 결정합니다.

Cisco Secure ACS는 TACACS+를 사용하여 관리 애플리케이션과 통신합니다.Cisco Security Manager가 Cisco Secure ACS와 통신하려면 Cisco Secure ACS의 CiscoWorks 서버를 TACACS+를 사용하는 AAA 클라이언트로 구성해야 합니다.또한 Cisco Secure ACS에 로그인하려면 CiscoWorks 서버에 사용하는 관리자 이름과 암호를 제공해야 합니다.이러한 요구 사항을 충족하면 Cisco Security Manager와 Cisco Secure ACS 간의 통신이 유효한지 확인합니다.

Cisco Security Manager가 Cisco Secure ACS와 처음 통신할 때 Cisco ACS에 기본 역할 생성을 지시합니다. 이 역할은 Cisco Secure ACS HTML 인터페이스의 Shared Profile Components 섹션에 표시됩니다.또한 TACACS+에서 인증하도록 사용자 지정 서비스를 지시합니다.이 맞춤형 서비스는 HTML 인터페이스의 Interface Configuration(인터페이스 컨피그레이션) 섹션에 있는 TACACS+(Cisco IOS®) 페이지에 나타납니다.그런 다음 각 Cisco Security Manager 역할에 포함된 권한을 수정하고 이러한 역할을 사용자 및 사용자 그룹에 적용할 수 있습니다.

참고: CSM은 지원되지 않으므로 ACS 5.2와 통합할 수 없습니다.

사전 요구 사항

요구 사항

Cisco Secure ACS를 사용하려면 다음을 확인하십시오.

- Cisco Security Manager에서 필요한 기능을 수행하는 데 필요한 명령을 포함하는 역할을 정의합니다.
- 프로파일에 NAR을 적용할 경우 NAR(Network Access Restriction)에는 관리할 디바이스 그룹(또는 디바이스)이 포함됩니다.
- 관리되는 디바이스 이름은 Cisco Secure ACS와 Cisco Security Manager에서 맞춤법이 동일하며 대문자로 지정됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Security Manager 버전 3.0
- Cisco Secure ACS 버전 3.3

참고: 네트워크 환경에 설치하기 전에 호환되는 CSM 및 ACS 버전을 선택해야 합니다.예를 들어, Cisco는 CSM 3.0만 사용하여 ACS 3.3을 테스트하고 이후 CSM 버전에 대해 중지했습니다.따라서 ACS 3.3과 함께 CSM 3.0을 사용하는 것이 좋습니다. 다양한 소프트웨어 버전에 대한 자세한 내용은 Compatible Matrix 표를 참조하십시오.

Cisco Security Manager 버전	테스트된 CS ACS 버전
3.0.0 3.0.0 SP1	Windows 3.3(3) 및 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Solutions Engine 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Solutions Engine 4.0(1) Windows 4.1(1) 및 4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	솔루션 엔진 v4.0(1) Windows 4.1(2), 4.1(3) 및 4.1(4)
3.1.1 SP1	Solutions Engine 4.0(1) Windows 4.1(4)
3.1.1 SP2	Solutions Engine 4.0(1) Windows 4.1(4) 및 4.2(0)
3.2.0	Solutions Engine 4.1(4) Windows 4.1(4) 및 4.2(0)

3.2.1	Solutions Engine 4.1(4) Windows 4.2(0)

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 규칙을 참조하십시오.

Cisco Security Manager와 Cisco Secure ACS 통합

이 섹션에서는 Cisco Security Manager를 Cisco Secure ACS와 통합하는 데 필요한 단계를 설명합니다.일부 단계에는 몇 가지 하위 단계가 포함되어 있습니다.이러한 단계와 하위 단계는 순서대로 수행해야 합니다.이 섹션에는 각 단계를 수행하기 위해 사용되는 특정 절차에 대한 참조도 포함되어 있습니다.

다음 단계를 완료하십시오.

1. **관리 인증 및 권한 부여 모델을 계획합니다.**Cisco Security Manager를 사용하려면 먼저 관리 모델을 결정해야 합니다.여기에는 사용할 관리 역할 및 계정의 정의가 포함됩니다.**팁:** 잠재적 관리자의 역할과 권한을 정의할 때 워크플로를 활성화할지 여부도 고려하십시오.이 선택은 액세스를 제한하는 방법에 영향을 줍니다.
2. **Cisco Secure ACS, Cisco Security Manager 및 CiscoWorks Common Services를 설치합니다.**Windows 2000/2003 서버에 Cisco Secure ACS 버전 3.3을 설치합니다.다른 Windows 2000/Windows 2003 서버에 CiscoWorks Common Services 및 Cisco Security Manager를 설치합니다.자세한 내용은 다음 문서를 참조하십시오.Cisco Security Manager 3.0 설치 설명서Windows 3.3용 Cisco Secure ACS 설치 설명서**참고:** CSM 및 ACS 소프트웨어 버전을 선택하기 전에 호환성 매트릭스 표를 참조하십시오.
3. **Cisco Secure ACS에서 통합 절차를 수행합니다.**Cisco Security Manager 사용자를 ACS 사용자로 정의하고, 계획된 역할에 따라 사용자 그룹에 할당하고, 모든 관리되는 디바이스(CiscoWorks/Security Manager 서버 및 CiscoWorks/Security Manager 서버)를 AAA 클라이언트로 추가하고, 관리 제어 사용자를 생성합니다.자세한 내용은 Cisco Secure ACS에서 수행되는 통합 절차를 참조하십시오.
4. **CiscoWorks Common Services에서 통합 절차를 수행합니다.**Cisco Secure ACS에 정의된 관리자와 일치하는 로컬 사용자를 구성하고, 시스템 ID 설정에 동일한 사용자를 정의하고, ACS를 AAA 설정 모드로 구성합니다.자세한 내용은 CiscoWorks에서 수행되는 통합 절차를 참조하십시오.
5. **Cisco Secure ACS에서 사용자 그룹에 역할 할당**Cisco Secure ACS에 구성된 각 사용자 그룹에 역할을 할당합니다.사용하는 절차는 NDG(Network Device Group)를 구성했는지에 따라 달라집니다.자세한 내용은 Cisco Secure ACS의 사용자 그룹에 역할 할당을 참조하십시오.

Cisco Secure ACS에서 수행되는 통합 절차

이 섹션에서는 Cisco Security Manager와 통합하기 위해 Cisco Secure ACS에서 완료해야 하는 단계에 대해 설명합니다.

1. Cisco Secure ACS에서 사용자 및 사용자 그룹 정의
2. Cisco Secure ACS에서 관리되는 디바이스를 AAA 클라이언트로 추가
3. Cisco Secure ACS에서 관리 제어 사용자 생성

Cisco Secure ACS에서 사용자 및 사용자 그룹 정의

Cisco Security Manager의 모든 사용자는 Cisco Secure ACS에서 정의되어야 하며 해당 직무 기능에 적합한 역할을 할당해야 합니다.가장 쉬운 방법은 ACS에서 사용할 수 있는 각 기본 역할에 따라 사용자를 다른 그룹으로 나누는 것입니다.예를 들어 모든 시스템 관리자를 한 그룹에 할당하고 모든 네트워크 운영자를 다른 그룹에 할당하는 등의 작업을 수행합니다.ACS의 기본 역할에 대한 자세한 내용은 Cisco Secure ACS 기본 역할을 참조하십시오.

또한 전체 권한을 가진 시스템 관리자 역할이 할당된 추가 사용자를 만들어야 합니다.이 사용자에 대해 설정된 자격 증명은 나중에 CiscoWorks의 시스템 ID 설정 페이지에서 사용됩니다.자세한 내용은 시스템 ID 사용자 정의를 참조하십시오.

이 단계에서는 사용자를 다른 그룹에 할당하기만 합니다.이러한 그룹에 대한 실제 역할 할당은 CiscoWorks, Cisco Security Manager 및 기타 모든 애플리케이션이 Cisco Secure ACS에 등록된 후에 수행됩니다.

팁: 계속하기 전에 Windows 2000/2003 서버 하나에 CiscoWorks Common Services 및 Cisco Security Manager를 설치하십시오.다른 Windows 2000/2003 서버에 Cisco Secure ACS를 설치합니다.

1. Cisco Secure ACS에 로그인합니다.
2. 전체 권한을 가진 사용자를 구성합니다.탐색 모음에서 User Setup을 클릭합니다.User Setup(사용자 설정) 페이지에서 새 사용자의 이름을 입력한 다음 **Add/Edit(추가/수정)를** 클릭합니다.User Setup(사용자 설정) 아래의 Password Authentication(비밀번호 인증) 목록에서 인증 방법을 선택합니다.새 사용자의 비밀번호를 입력하고 확인합니다.사용자**가** 할당된 그룹으로 그룹 **1**을 선택합니다.Submit(**제출**)을 클릭하여 사용자 계정을 생성합니다.
3. 각 Cisco Security Manager 사용자에 대해 2단계를 반복합니다.Cisco에서는 각 사용자에게 할당된 역할에 따라 사용자를 그룹으로 나누는 것이 좋습니다.그룹 1 - 시스템 관리자그룹 2 - 보안 관리자그룹 3 - 보안 승인자그룹 4 - 네트워크 관리자그룹 5 - 승인자그룹 6 - 네트워크 운영자그룹 7 - 헬프 데스크각 역할과 연결된 기본 권한에 대한 자세한 내용은 표를 참조하십시오.사용자 역할 사용자를 사용자 지정하는 방법에 대한 자세한 내용은 Cisco Secure ACS 역할 사용자 정의를 참조하십시오.**참고:** 이 단계에서는 그룹 자체가 역할 정의가 없는 사용자 모음입니다.통합 프로세스를 완료한 후 각 그룹에 역할을 할당합니다.자세한 내용은 Cisco Secure ACS의 사용자 그룹에 역할 할당을 참조하십시오.
4. 추가 사용자를 생성하고 이 사용자를 시스템 관리자 그룹에 할당합니다.이 사용자에 대해 설정된 자격 증명은 나중에 CiscoWorks의 시스템 ID 설정 페이지에서 사용됩니다.자세한 내용은 시스템 ID 사용자 정의를 참조하십시오.
5. Cisco Secure ACS에서 Add Managed Devices as AAA Clients(관리되는 디바이스를 AAA 클라이언트로 추가)를 계속 진행합니다.

Cisco Secure ACS에서 관리되는 디바이스를 AAA 클라이언트로 추가

Cisco Security Manager로 디바이스를 가져오기 시작하려면 먼저 Cisco Secure ACS에서 각 디바이스를 AAA 클라이언트로 구성해야 합니다.또한 CiscoWorks/Security Manager 서버를 AAA 클라이언트로 구성해야 합니다.

Cisco Security Manager가 Catalyst 6500/7600 디바이스의 FWSM에 구성된 보안 컨텍스트를 포함하는 방화벽 디바이스에 구성된 보안 컨텍스트를 관리하는 경우 각 컨텍스트를 Cisco Secure ACS에 개별적으로 추가해야 합니다.

관리되는 디바이스를 추가하기 위해 사용하는 방법은 사용자가 네트워크 디바이스 그룹(NDG)을 사용하여 특정 디바이스 세트를 관리하도록 제한할지 여부에 따라 달라집니다. 다음 섹션 중 하나를 참조하십시오.

- 사용자가 모든 디바이스에 액세스할 수 있도록 하려면 Add Devices as AAA Clients Without NDGs(디바이스를 AAA 클라이언트로 추가)에 설명된 대로 디바이스를 추가합니다.
- 사용자가 특정 NDG에만 액세스하도록 하려면 Configure Network Device Groups for Use in Security Manager(보안 관리자에서 사용할 네트워크 디바이스 그룹 구성)에 설명된 대로 디바이스를 추가합니다.

NDG가 없는 AAA 클라이언트로 디바이스 추가

이 절차에서는 Cisco Secure ACS의 AAA 클라이언트로 디바이스를 추가하는 방법에 대해 설명합니다.사용 가능한 모든 옵션에 대한 자세한 내용은 네트워크 컨피그레이션의 AAA 클라이언트 컨피그레이션 섹션을 참조하십시오.

참고: CiscoWorks/Security Manager 서버를 AAA 클라이언트로 추가해야 합니다.

1. Cisco Secure ACS 탐색 모음에서 Network Configuration(네트워크 컨피그레이션)을 클릭합니다.
2. AAA **Clients** 테이블 아래에서 Add Entry를 클릭합니다.
3. Add AAA Client(AAA 클라이언트 추가) 페이지에서 AAA 클라이언트 호스트 이름(최대 32자)을 입력합니다.AAA 클라이언트의 호스트 이름은 Cisco Security Manager에서 디바이스에 사용할 표시 이름과 일치해야 합니다.예를 들어 Cisco Security Manager의 디바이스 이름에 도메인 이름을 추가하려는 경우 ACS의 AAA 클라이언트 호스트 이름은 **<device_name>.<domain_name>**이어야 합니다.CiscoWorks 서버의 이름을 지정할 때 정규화된 호스트 이름을 사용하는 것이 좋습니다.호스트 이름의 철자가 올바른지 확인하십시오.호스트 이름은 대/소문자를 구분하지 않습니다.보안 컨텍스트의 이름을 지정할 때 컨텍스트 이름(**_<context_name>**)을 디바이스 이름에 추가합니다.FWSM의 경우 다음과 같은 명명 규칙이 있습니다.FWSM 블레이드 - **<chassis_name>_FW_<slot_number>**보안 컨텍스트 - **<chassis_name>_FW_<slot_number>_<context_name>**
4. AAA Client IP Address 필드에 네트워크 디바이스의 IP 주소를 입력합니다.
5. Key 필드에 공유 암호를 입력합니다.
6. Authenticate **Using** 목록에서 TACACS**+(Cisco IOS)**를 선택합니다.
7. 변경 사항을 저장하려면 **Submit**(제출)을 클릭합니다.추가한 디바이스가 AAA Clients 테이블에 나타납니다.
8. 추가 디바이스를 추가하려면 1~7단계를 반복합니다.
9. 모든 디바이스를 추가한 후 **Submit + Restart**를 클릭합니다.
10. Cisco Secure ACS에서 Create an Administration Control User(관리 제어 사용자 생성)를 계속 진행합니다.

보안 관리자에서 사용할 네트워크 장치 그룹 구성

Cisco Secure ACS를 사용하면 관리할 특정 디바이스가 포함된 NDG(네트워크 디바이스 그룹)를 구성할 수 있습니다.예를 들어, 조직 구조와 일치하는 각 지역 또는 NDG에 대해 NDG를 생성할 수

있습니다.Cisco Security Manager와 함께 사용할 경우 NDG를 사용하면 사용자가 관리해야 하는 디바이스에 따라 다양한 수준의 권한을 사용자에게 제공할 수 있습니다.예를 들어, NDG를 사용하면 유럽에 있는 장치에 사용자 A 시스템 관리자 권한을 할당하고 아시아에 있는 장치에 헬프 데스크 권한을 할당할 수 있습니다.그런 다음 사용자 B에 반대 권한을 할당할 수 있습니다.

NDG는 사용자에게 직접 할당되지 않습니다.대신 NDG는 각 사용자 그룹에 대해 정의하는 역할에 할당됩니다.각 NDG는 단일 역할에만 할당할 수 있지만 각 역할에는 여러 NDG를 포함할 수 있습니다.이러한 정의는 선택한 사용자 그룹에 대한 컨피그레이션의 일부로 저장됩니다.

다음 항목에서는 NDG를 구성하는 데 필요한 기본 단계를 간략하게 설명합니다.

NDG 기능 활성화

NDG를 생성하고 디바이스로 채우려면 먼저 NDG 기능을 활성화해야 합니다.

1. Cisco Secure ACS 탐색 모음에서 Interface Configuration을 클릭합니다.
2. 고급 **옵션을 클릭합니다**.
3. 아래로 스크롤한 다음 **Network Device Groups** 확인란을 선택합니다.
4. Submit(제출)**을 클릭합니다**.
5. Create NDGs(NDG 생성)를 계속 진행합니다.

NDG 생성

이 절차에서는 NDG를 생성하고 디바이스로 채우는 방법에 대해 설명합니다.각 디바이스는 하나의 NDG에만 속할 수 있습니다.

참고: Cisco는 CiscoWorks/Security Manager 서버를 포함하는 특별 NDG를 생성하는 것이 좋습니다.

1. 탐색 모음에서 Network Configuration을 클릭합니다.모든 디바이스는 처음에 NDG에 배치되지 않은 모든 디바이스를 포함하는 Not Assigned 아래에 배치됩니다.Not Assigned는 NDG가 아니라는 점에 유의하십시오.
2. NDG 생성:항목 **추가를 클릭합니다**.New Network Device Group 페이지에서 NDG의 이름을 입력합니다.최대 길이는 24자입니다.공백은 허용됩니다.**버전 4.0 이상의 경우 선택 사항**:NDG의 모든 디바이스에서 사용할 키를 입력합니다.NDG에 대한 키를 정의하는 경우 NDG의 개별 디바이스에 대해 정의된 모든 키를 재정의합니다.NDG를 저장하려면 Submit(제출)을 클릭합니다.추가 NDG를 생성하려면 a~d 단계를 반복합니다.
3. NDGs를 디바이스로 채웁니다.Network Device Groups 영역에서 NDG의 이름을 클릭합니다.AAA **Clients** 영역에서 Add Entry를 클릭합니다.NDG에 추가할 디바이스의 세부 정보를 정의한 다음 Submit(제출)을 **클릭합니다**.자세한 내용은 NDG가 없는 AAA 클라이언트로 디바이스 추가를 참조하십시오.디바이스의 나머지 부분을 NDGs에 추가하려면 b 및 c 단계를 반복합니다.Not Assigned(할당되지 않음) 카테고리에서 유지할 수 있는 유일한 디바이스는 기본 AAA 서버입니다.마지막 디바이스를 구성한 후 **Submit + Restart**를 클릭합니다.
4. Cisco Secure ACS에서 Create an Administration Control User(관리 제어 사용자 생성)를 계속 진행합니다.

Cisco Secure ACS에서 관리 제어 사용자 생성

Cisco Secure ACS의 관리 제어 페이지를 사용하여 CiscoWorks Common Services에서 AAA 설정 모드를 정의할 때 사용되는 관리자 계정을 정의합니다.자세한 내용은 CiscoWorks에서 AAA 설정 모드 구성을 참조하십시오.

1. Cisco Secure ACS 탐색 모음에서 Administration Control을 클릭합니다.
2. Add **Administrator를 클릭합니다**.
3. 관리자 추가 페이지에서 관리자의 이름과 비밀번호를 입력합니다.
4. 이 관리자**에게** 전체 관리 권한을 제공하려면 관리자 권한 영역에서 모두 부여를 누릅니다.
5. Submit(**제출**)을 클릭하여 관리자를 생성합니다.

참고: 관리자를 구성할 때 사용 가능한 옵션에 대한 자세한 내용은 관리자 및 관리 정책을 참조하십시오.

CiscoWorks에서 수행되는 통합 절차

이 섹션에서는 Cisco Security Manager와 통합하기 위해 CiscoWorks Common Services에서 완료하는 단계를 설명합니다.

- CiscoWorks에서 로컬 사용자 생성
- 시스템 ID 사용자 정의
- CiscoWorks에서 AAA 설정 모드 구성

Cisco Secure ACS에서 수행되는 통합 절차를 완료한 후 다음 단계를 완료합니다.Common Services는 Cisco Security Manager, Auto-Update Server, IPS Manager와 같은 설치된 모든 애플리케이션을 Cisco Secure ACS에 실제로 등록합니다.

CiscoWorks에서 로컬 사용자 생성

CiscoWorks Common Services의 Local User Setup(로컬 사용자 설정) 페이지를 사용하여 이전에 Cisco Secure ACS에서 생성한 관리자와 중복되는 로컬 사용자 계정을 생성합니다.이 로컬 사용자 계정은 나중에 시스템 ID 설정에 사용됩니다.자세한 내용은 을/를 참조하십시오.

참고: 계속하기 전에 Cisco Secure ACS에서 관리자를 만드십시오.자세한 내용은 Cisco Secure ACS에서 사용자 및 사용자 그룹 정의를 참조하십시오.

1. CiscoWorks에 기본 **관리자** 사용자 계정으로 로그인합니다.
2. Common **Services(공통 서비스)**에서 Server(서버) > Security(보안)를 선택한 다음 목차에서 **Local User Setup(로컬 사용자 설정)**을 선택합니다.
3. Add(**추가)를 클릭합니다**.
4. Cisco Secure ACS에서 관리자를 생성할 때 입력한 이름과 암호를 입력합니다.Cisco Secure ACS에서 사용자 및 사용자 그룹 정의의 4단계를 참조하십시오.
5. Roles except Data(데이터 내보내기 제외)에서 모든 확인란을 선택합니다.
6. 확인**을** 클릭하여 사용자를 생성합니다.

시스템 ID 사용자 정의

CiscoWorks Common Services의 System Identity Setup 페이지를 사용하여 동일한 도메인에 속한 서버와 동일한 서버에 있는 애플리케이션 프로세스 간의 통신을 가능하게 하는 System Identity 사용자로 알려진 트러스트 사용자를 생성합니다.애플리케이션은 로컬 또는 원격 CiscoWorks 서버에

서 프로세스를 인증하기 위해 시스템 ID 사용자를 사용합니다.이는 사용자가 로그인하기 전에 응용 프로그램을 동기화해야 하는 경우에 특히 유용합니다.

또한, 기본 작업이 이미 로그인한 사용자에 대해 권한이 부여된 경우 하위 작업을 수행하기 위해 시스템 ID 사용자가 자주 사용됩니다.예를 들어 Cisco Security Manager에서 디바이스를 편집하려면 Cisco Security Manager와 Common Services DCR 간에 애플리케이션 간 통신이 필요합니다.사용자가 편집 작업을 수행할 권한이 있는 후 DCR을 호출하기 위해 시스템 ID 사용자가 사용됩니다.

여기서 구성하는 시스템 ID 사용자는 ACS에서 구성한 관리(전체) 권한이 있는 사용자와 동일해야 합니다.이렇게 하지 않으면 Cisco Security Manager에 구성된 모든 디바이스 및 정책을 볼 수 없습니다.

참고: 계속하기 전에 CiscoWorks Common Services에서 이 관리자와 같은 이름과 암호를 가진 로컬 사용자를 생성합니다.자세한 내용은 CiscoWorks에서 로컬 사용자 생성을 참조하십시오.

1. Server(**서버) > Security(보안**)를 선택한 다음 TOC**에서 Multi-Server Trust Management(다중 서버 신뢰 관리) > System Identity Setup(시스템 ID 설정**)을 선택합니다.
2. Cisco Secure ACS에 대해 생성한 관리자의 이름을 입력합니다.Cisco Secure ACS에서 사용자 및 사용자 그룹 정의의 4단계를 참조하십시오.
3. 이 사용자의 비밀번호를 입력하고 확인합니다.
4. Apply를 **클릭합니다**.

CiscoWorks에서 AAA 설정 모드 구성

CiscoWorks Common Services의 AAA 설정 모드 페이지를 사용하여 Cisco Secure ACS를 필수 포트 및 공유 비밀 키를 포함하는 AAA 서버로 정의합니다.또한 최대 2개의 백업 서버를 정의할 수 있습니다.

이러한 단계는 Cisco Secure ACS에 CiscoWorks, Cisco Security Manager, IPS Manager(및 선택적으로 자동 업데이트 서버)를 실제로 등록합니다.

1. Server(**서버) > Security(보안**)를 선택한 다음 TOC에서 **AAA Mode Setup(AAA 모드 설정**)을 선택합니다.
2. Available Login Modules(사용 가능한 **로그인 모듈)** 아래에서 TACACS+ 확인란을 선택합니다.
3. AAA 유형으로 ACS를 선택합니다.
4. Server Details(서버 세부사항) 영역에 최대 3개의 Cisco Secure ACS 서버의 IP 주소를 입력합니다.보조 및 3차 서버는 기본 서버에 장애가 발생할 경우 백업 역할을 합니다.**참고:** 구성된 모든 TACACS+ 서버가 응답하지 않을 경우 관리자 CiscoWorks Local 계정으로 로그인한 다음 AAA 모드를 다시 Non-ACS/CiscoWorks Local로 변경해야 합니다.TACACS+ 서버를 서비스로 복원한 후 AAA 모드를 다시 ACS로 변경해야 합니다.
5. Login(로그인) 영역에서 Cisco Secure ACS의 Administration Control(관리 제어) 페이지에 정의한 관리자 이름을 입력합니다.자세한 내용은 Cisco Secure ACS에서 관리 제어 사용자 생성을 참조하십시오.
6. 이 관리자의 암호를 입력하고 확인합니다.
7. Security Manager 서버를 Cisco Secure ACS의 AAA 클라이언트로 추가할 때 입력한 공유 비밀 키를 입력하고 확인합니다.NDGs가 없는 AAA 클라이언트로 디바이스 추가에서 5단계를 참조하십시오.
8. Cisco Security **Manager** 및 설치된 다른 모든 애플리케이션을 Cisco Secure ACS에 등록하려면 **Register all installed applications with ACS(ACS에 설치된 모든 애플리케이션 등록**) 확인

란을 선택합니다.

9. 설정을 저장하려면 **Apply**(적용)를 클릭합니다.진행 표시줄에는 등록의 진행률이 표시됩니다.등록이 완료되면 메시지가 나타납니다.
10. Cisco Security Manager를 임의의 ACS 버전과 통합하는 경우 Cisco Security Manager Daemon Manager 서비스를 다시 시작합니다.자세한 내용은 데몬 관리자 다시 시작을 참조하십시오.**참고:** CSM 3.0.0 이후 Cisco는 더 이상 ACS 3.3(x)에 대해 테스트하지 않습니다.패치가 많이 적용되고 EOL(End-of-Life)이 발표되었기 때문입니다.따라서 CSM 버전 3.0.1 이상에 적합한 ACS 버전을 사용해야 합니다.자세한 내용은 호환성 매트릭스 테이블을 참조하십시오.
11. 각 사용자 그룹에 역할을 할당하려면 Cisco Secure ACS에 다시 로그인합니다.자세한 내용은 Cisco Secure ACS의 사용자 그룹에 역할 할당을 참조하십시오.**참고:** CiscoWorks Common Services 또는 Cisco Security Manager를 제거할 경우 여기에 구성된 AAA 설정은 유지되지 않습니다.또한 재설치 후에는 이 구성을 백업 및 복원할 수 없습니다.따라서 두 애플리케이션의 새 버전으로 업그레이드할 경우 AAA 설정 모드를 재구성하고 ACS에 Cisco Security Manager를 다시 등록해야 합니다.이 프로세스는 증분 업데이트에 필요하지 않습니다.CiscoWorks 위에 AUS와 같은 추가 애플리케이션을 설치하는 경우 새 애플리케이션과 Cisco Security Manager를 다시 등록해야 합니다.

데몬 관리자 다시 시작

이 절차에서는 Cisco Security Manager 서버의 데몬 관리자를 재시작하는 방법에 대해 설명합니다.구성한 AAA 설정을 적용하려면 이 작업을 수행해야 합니다.그런 다음 Cisco Secure ACS에 정의된 자격 증명을 사용하여 CiscoWorks에 다시 로그인할 수 있습니다.

1. Cisco Security Manager 서버가 설치된 시스템에 로그인합니다.
2. 서비스 창을 열려면 **시작 > 프로그램 > 관리 도구 > 서비스**를 선택합니다.
3. 오른쪽 창에 표시되는 서비스 목록에서 **Cisco Security Manager Daemon Manager**를 선택합니다.
4. 도구 모음에서 **Restart Service(서비스 재시작)** 버튼을 클릭합니다.
5. Cisco Secure ACS에서 사용자 그룹에 역할 할당을 계속 진행합니다.

Cisco Secure ACS에서 사용자 그룹에 역할 할당

CiscoWorks, Cisco Security Manager 및 기타 설치된 애플리케이션을 Cisco Secure ACS에 등록한 후 Cisco Secure ACS에서 이전에 구성한 각 사용자 그룹에 역할을 할당할 수 있습니다.이러한 역할은 각 그룹의 사용자가 Cisco Security Manager에서 수행할 수 있는 작업을 결정합니다.

사용자 그룹에 역할을 할당하기 위해 사용하는 절차는 NDGs 사용 여부에 따라 달라집니다.

- NDG 없이 사용자 그룹에 역할 할당
- NDG 및 역할을 사용자 그룹과 연결

NDG 없이 사용자 그룹에 역할 할당

이 절차에서는 NDG가 정의되지 않은 경우 사용자 그룹에 기본 역할을 할당하는 방법을 설명합니다.자세한 내용은 Cisco Secure ACS 기본 역할을 참조하십시오.

참고: 계속하기 전에

- 각 기본 역할에 대한 사용자 그룹을 만듭니다.자세한 내용은 Cisco Secure ACS에서 사용자 및 사용자 그룹 정의를 참조하십시오.
- Cisco Secure ACS에서 수행되는 통합 절차 및 CiscoWorks에서 수행되는 통합 절차에 설명된 절차를 완료합니다.

다음 단계를 완료하십시오.

1. Cisco Secure ACS에 로그인합니다.
2. 탐색 모음에서 Group Setup을 클릭합니다.
3. 목록에서 시스템 관리자의 사용자 그룹을 선택합니다.Cisco Secure ACS에서 사용자 및 사용자 그룹 정의의 2단계를 참조한 다음 **설정 편집**을 클릭합니다.

NDG 및 역할을 사용자 그룹과 연결

NDG를 Cisco Security Manager에서 사용할 역할과 연결할 때 Group Setup(그룹 설정) 페이지의 두 위치에서 정의를 생성해야 합니다.

- CiscoWorks 영역
- Cisco Security Manager 영역

각 영역의 정의는 가능한 한 일치해야 합니다.CiscoWorks Common Services에 없는 사용자 지정 역할 또는 ACS 역할을 연결할 때 해당 역할에 할당된 권한에 따라 가능한 한 가까운 역할을 정의해 보십시오.

Cisco Security Manager와 함께 사용할 각 사용자 그룹에 대한 연결을 생성해야 합니다.예를 들어, 서부 지역의 지원 인력이 포함된 사용자 그룹이 있는 경우 해당 사용자 그룹을 선택한 다음 해당 지역의 장치를 포함하는 NDG를 헬프 데스크 역할과 연결할 수 있습니다.

참고: 계속하기 전에 NDG 기능을 활성화하고 NDGs를 생성합니다.자세한 내용은 보안 관리자에서 사용할 네트워크 장치 그룹 구성을 참조하십시오.

1. 탐색 모음에서 Group Setup을 클릭합니다.
2. 그룹 목록에서 사용자 그룹을 선택한 다음 **설정 편집**을 클릭합니다.
3. CiscoWorks에서 사용할 NDG 및 역할 매핑:Group Setup(그룹 설정) 페이지에서 아래로 스크롤하여 TACACS+ Settings(TACACS+ 설정) 아래의 CiscoWorks 영역으로 이동합니다.**Assign a CiscoWorks on a Network Device Group Basis를 선택합니다**.Device Group 목록에서 NDG를 선택합니다.두 번째 목록에서 이 NDG를 연결할 역할을 선택합니다.연결 **추가를 클릭합니다**.연결이 Device Group(디바이스 그룹) 상자에 나타납니다.추가 연관을 생성하려면 c~e 단계를 반복합니다.**참고:** 연결을 제거하려면 장치 그룹에서 연결을 선택한 다음 연결 제거를 클릭합니다.
4. 아래로 스크롤하여 Cisco Security Manager 영역으로 이동하여 3단계에서 정의한 연관을 최대한 가깝게 일치하는 연관을 생성합니다.**참고:** Cisco Secure ACS에서 Security Approver 또는 Security Administrator 역할을 선택할 경우 Network Administrator를 가장 비슷한 CiscoWorks 역할로 선택하는 것이 좋습니다.
5. 설정을 저장하려면 **Submit**(제출)을 클릭합니다.
6. 사용자 그룹의 나머지 부분에 대해 NDGs를 정의하려면 2~5단계를 반복합니다.
7. NDG 및 역할을 각 사용자 그룹과 연결한 후 Submit **+ Restart**를 클릭합니다.

문제 해결

1. Cisco Security Manager로 디바이스를 가져오기 시작하려면 먼저 Cisco Secure ACS에서 각 디바이스를 AAA 클라이언트로 구성해야 합니다.또한 CiscoWorks/Security Manager 서버를 AAA 클라이언트로 구성해야 합니다.
2. 실패한 시도 로그를 수신하는 경우 Cisco Secure ACS에서 오류가 발생하여 만든 이가 실패했습니다.
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test
   Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches
   authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   이 문제를 해결하려면 ACS의 장치 이름이 정규화된 도메인 이름이어야 합니다.

관련 정보

- Windows용 Cisco Security Access Control Server 지원 페이지
- Cisco Security Manager 지원 페이지
- Windows용 Cisco Secure Access Control Server
- Cisco Secure ACS 4.1용 구성 설명서
- Cisco Secure ACS Online 문제 해결 가이드, 4.1
- 보안 제품 필드 알림(Windows용 CiscoSecure ACS 포함)
- 기술 지원 및 문서 – Cisco Systems