AP 버전 1.01의 HTTP 관리자 인증

목차

소개

이 문서에서는 액세스 포인트(AP) 버전 1.01의 HTTP 관리자 인증을 위한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ACS(Access Control Server) 버전 2.6.4 이상

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.

배경 정보

GUI에서 EXEC 세션에 대한 TACACS+ 또는 RADIUS 어카운팅 또는 명령 권한 부여를 구성하는 옵션은 없습니다. 이러한 옵션은 CLI에서 구성할 수 있지만 권장하지 않습니다. 이러한 옵션을 구성할 경우 계정 관리 또는 권한 부여 요청이 있는 AP 및 ACS에서 심각하게 다운될 수 있습니다(각 페이지의 각 요소는 계정 관리 또는 권한 부여되어야 함).

ACS 컨피그레이션

인터페이스 컨피그레이션

인터페이스를 구성하려면 다음 단계를 완료하십시오.

1. TACACS+(Cisco IOS)에서 첫 번째 정의되지 않은 새 서비스 필드에 대한 그룹 상자를 선택합니다.
2. Service(서비스) 필드에 Aironet을 입력합니다.
3. Protocol 필드에 Shell을 입력합니다.
4. Advanced Configuration Options(고급 컨피그레이션 옵션)에서 Advanced TACACS+ Features(고급 TACACS+ 기능) > Display a window for each service selected(선택한 각 서비스에 대한 창 표시)를 선택합니다.
5. Submit(제출)을 클릭합니다.

사용자 구성

사용자를 구성하려면 다음 단계를 완료합니다.

1. Advanced TACACS+ Settings(고급 TACACS+ 설정)에서 Shell (exec)을 선택합니다.
2. Privilege level을 선택합니다.
3. 필드에 15를 입력합니다.
4. Submit(제출)을 클릭합니다.

그룹 컨피그레이션

그룹을 구성하려면 다음 단계를 완료합니다.

1. TACACS+를 선택합니다.

2. Aironet Shell > Custom attributes를 선택합니다.
3. Custom Attributes(맞춤형 특성) 필드에 aironet:admin-capability=write+ident+firmware+admin+snmp를 입력합니다.
4. Submit(제출)을 클릭합니다.
5. 다시 시작합니다.

네트워크 설정

네트워크를 구성하려면 다음 단계를 완료하십시오.

1. TACACS+를 프로토콜로 사용하여 AP용 NAS를 생성합니다.
2. 키는 AP의 공유 비밀입니다.
3. Submit(제출)을 클릭합니다.
4. 다시 시작합니다.

참고: 1회 비밀번호로 토큰 서버를 사용하는 경우 레벨 1 및 레벨 15 비밀번호를 묻는 메시지가 계속 표시되지 않도록 토큰 캐싱을 구성해야 합니다. 토큰 캐싱을 구성하려면 다음 단계를 완료하십시오.

1. 관리자 사용자가 속한 그룹에 대한 그룹 컨피그레이션을 입력합니다.
2. Token Card Settings(토큰 카드 설정)를 선택합니다.
3. 기간을 선택합니다.
4. 보안과 편의에 대한 요구 사항의 균형을 맞추는 기간을 선택합니다.

일반적인 관리 세션이 5분 이하로 지속되는 경우 지속 시간 값 5분이 가장 좋습니다. 세션이 5분 이상 실행되면 5분 간격으로 비밀번호를 입력하라는 메시지가 다시 표시됩니다. Session 옵션은 accounting을 활성화하지 않으면 작동하지 않습니다. 또한 토큰 캐싱은 그룹의 모든 사용자와 모든 디바이스에 대한 그룹의 모든 세션(AP에 대한 EXEC 세션뿐 아니라)에 적용됩니다.

VxWorks용 AP 컨피그레이션

사용자 구성

다음 단계를 완료하십시오.

1. Setup(설정) > Security(보안) > User Information(사용자 정보) > Add New User(새 사용자 추가)를 선택합니다.
2. 전체 관리 기능을 가진 새 사용자를 추가합니다(모든 기능 설정이 선택됨).
3. Back(뒤로)을 클릭합니다. Security Setup(보안 설정) 페이지로 돌아갑니다.

4. 사용자 관리자를 클릭합니다. User Manager Setup 페이지가 나타납니다.
5. 사용자 관리자를 활성화합니다.
6. OK(확인)를 클릭합니다.

서버 컨피그레이션

다음 단계를 완료하십시오.

1. 설정 > 보안 > 인증 서버를 선택 합니다.
2. TACACS+ 서버 IP 주소를 입력합니다.
3. TACACS 서버 유형을 선택합니다.
4. 필드에 포트 49를 입력합니다.
5. 필드에 공유 암호를 입력합니다.
6. User Authentication(사용자 인증) 상자를 선택합니다.

IOS용 AP 컨피그레이션

IOS용 AP를 구성하려면 다음 단계를 완료하십시오.

1. Security(보안) > Server Manager(서버 관리자)를 선택합니다.
2. 구성된 TACACS+ 서버를 선택하거나 새 서버를 구성합니다.
3. 적용을 클릭합니다.
4. Admin Authentication (TACACS+)(관리자 인증(TACACS+)) 드롭다운에서 TACACS+ 서버의 IP를 선택합니다.
5. 적용을 클릭합니다.
6. Security(보안) > Admin Access(관리자 액세스)를 선택합니다.
7. 읽기-쓰기 액세스 권한이 있는 로컬 사용자를 만듭니다(아직 만들지 않은 경우).
8. 적용을 클릭합니다.
9. Authentication Server Only(인증 서버만) 또는 Authentication Server(인증 서버)(Local List(로컬 목록)에 없는 경우)를 선택합니다.
10. 적용을 클릭합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Aironet 1200 Series 제품 지원
- TACACS+(Terminal Access Controller Access Control System) 기술 지원
- Cisco Secure Access Control Server for Windows 제품 지원
- Cisco Secure Access Control Server for Unix 제품 지원
- Technical Support - Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.