Cisco ACS 5.X와 RSA SecurID 토큰 서버 통합

목차

소개

이 문서에서는 Cisco ACS(Access Control System) 버전 5.x를 RSA SecurID 인증 기술과 통합하는 방법에 대해 설명합니다.

배경 정보

Cisco Secure ACS는 RSA SecurID 서버를 외부 데이터베이스로 지원합니다.

RSA SecurID 2단계 인증은 사용자의 PIN(Personal Identification Number)과 시간 코드 알고리즘을 기반으로 단일 사용 토큰 코드를 생성하는 개별적으로 등록된 RSA SecurID 토큰으로 구성됩니다.

다른 토큰 코드는 고정된 간격으로 생성되며, 대개 30초나 60초마다 생성됩니다.RSA SecurID 서버는 이 동적 인증 코드를 검증합니다.각 RSA SecurID 토큰은 고유하며, 이전 토큰을 기준으로 향후 토큰의 값을 예측할 수 없습니다.

따라서 올바른 토큰 코드가 PIN과 함께 제공되면 해당 사용자가 유효한 사용자임을 확신하는 수준이 높습니다.따라서 RSA SecurID 서버는 기존의 재사용 가능한 비밀번호보다 더 안정적인 인증 메커니즘을 제공합니다.

다음과 같은 방법으로 Cisco ACS 5.x를 RSA SecurID 인증 기술과 통합할 수 있습니다.

- RSA SecurID 에이전트 - 사용자는 기본 RSA 프로토콜을 통해 사용자 이름과 암호로 인증됩니다.
- RADIUS 프로토콜 - 사용자는 RADIUS 프로토콜을 통해 사용자 이름과 암호로 인증됩니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- RSA 보안
- Cisco ACS(Secure Access Control System)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ACS(Secure Access Control System) 버전 5.x
- RSA SecurID 토큰 서버

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.

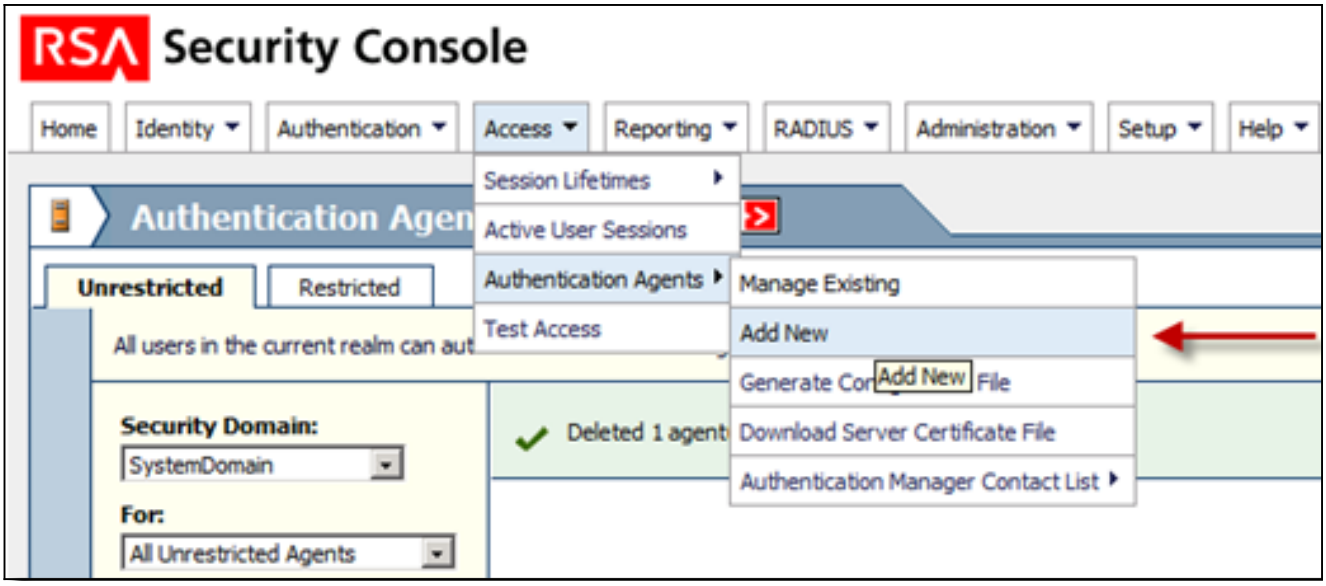
구성

RSA 서버

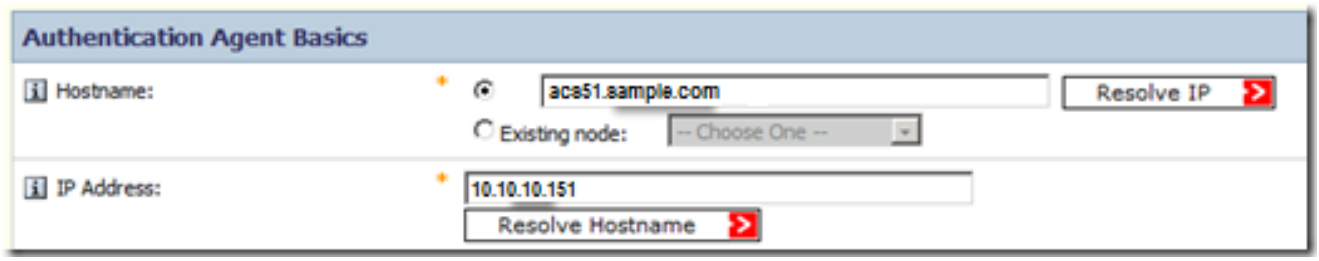
이 절차에서는 RSA SecurID 서버 관리자가 인증 에이전트 및 구성 파일을 생성하는 방법에 대해 설명합니다.인증 에이전트는 기본적으로 DNS(Domain Name Server) 이름 및 RSA 데이터베이스에 액세스할 수 있는 권한이 있는 디바이스, 소프트웨어 또는 서비스의 IP 주소입니다.구성 파일은 기본적으로 RSA 토폴로지 및 통신에 대해 설명합니다.

이 예에서는 RSA 관리자가 두 ACS 인스턴스에 대해 두 개의 에이전트를 생성해야 합니다.

1. RSA Security Console에서 **Access** > Authentication Agents > Add New(**인증 에이전트**) **Add New(새로 추가**:

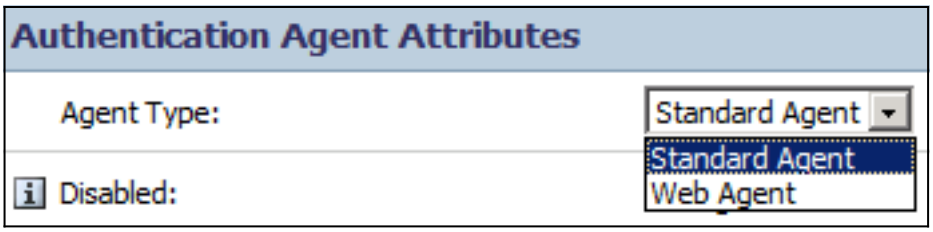


2. Add New Authentication Agent(새 인증 에이전트 추가) 창에서 두 에이전트 각각에 대해 호스트 이름 및 IP 주소를 정의합니다.

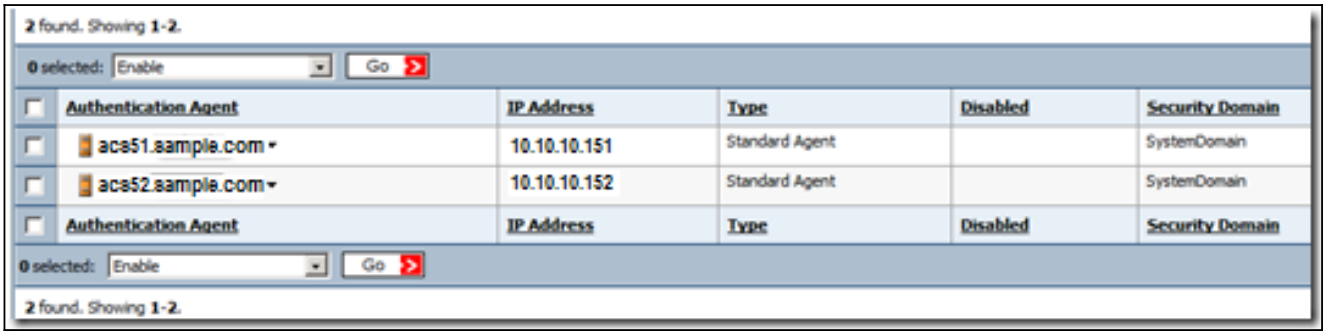


ACS 에이전트에 대한 DNS 정방향 및 역방향 조회가 모두 작동해야 합니다.

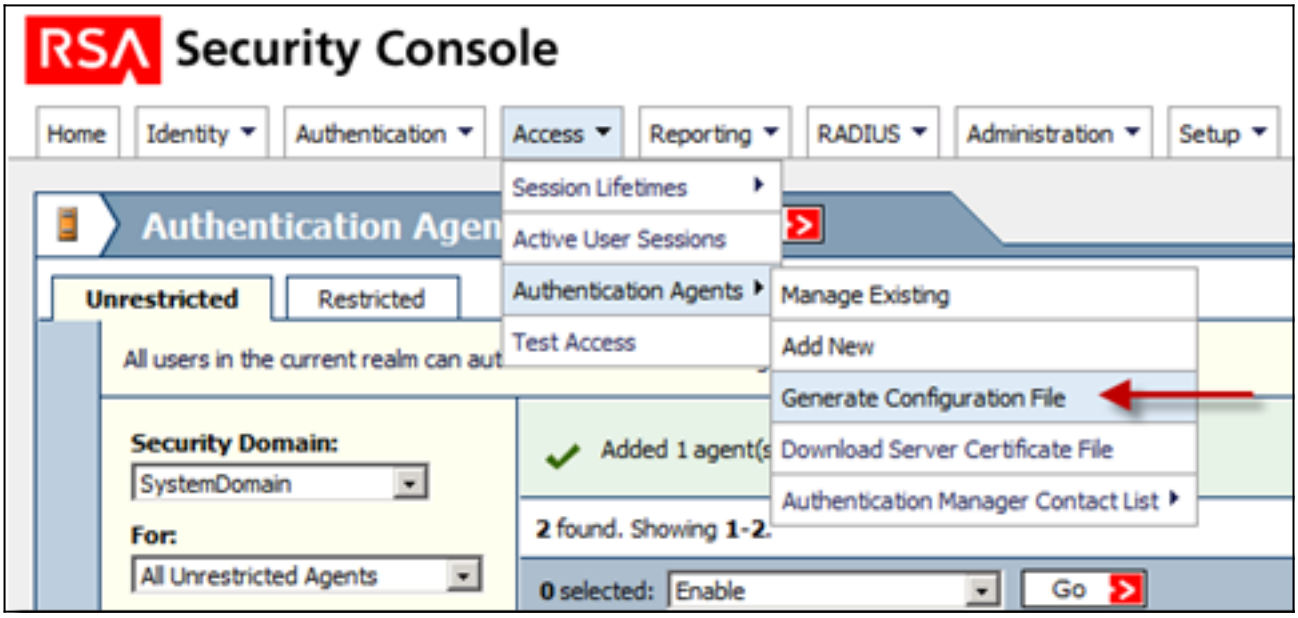
3. 상담원 유형을 표준 상담원으로 정의:



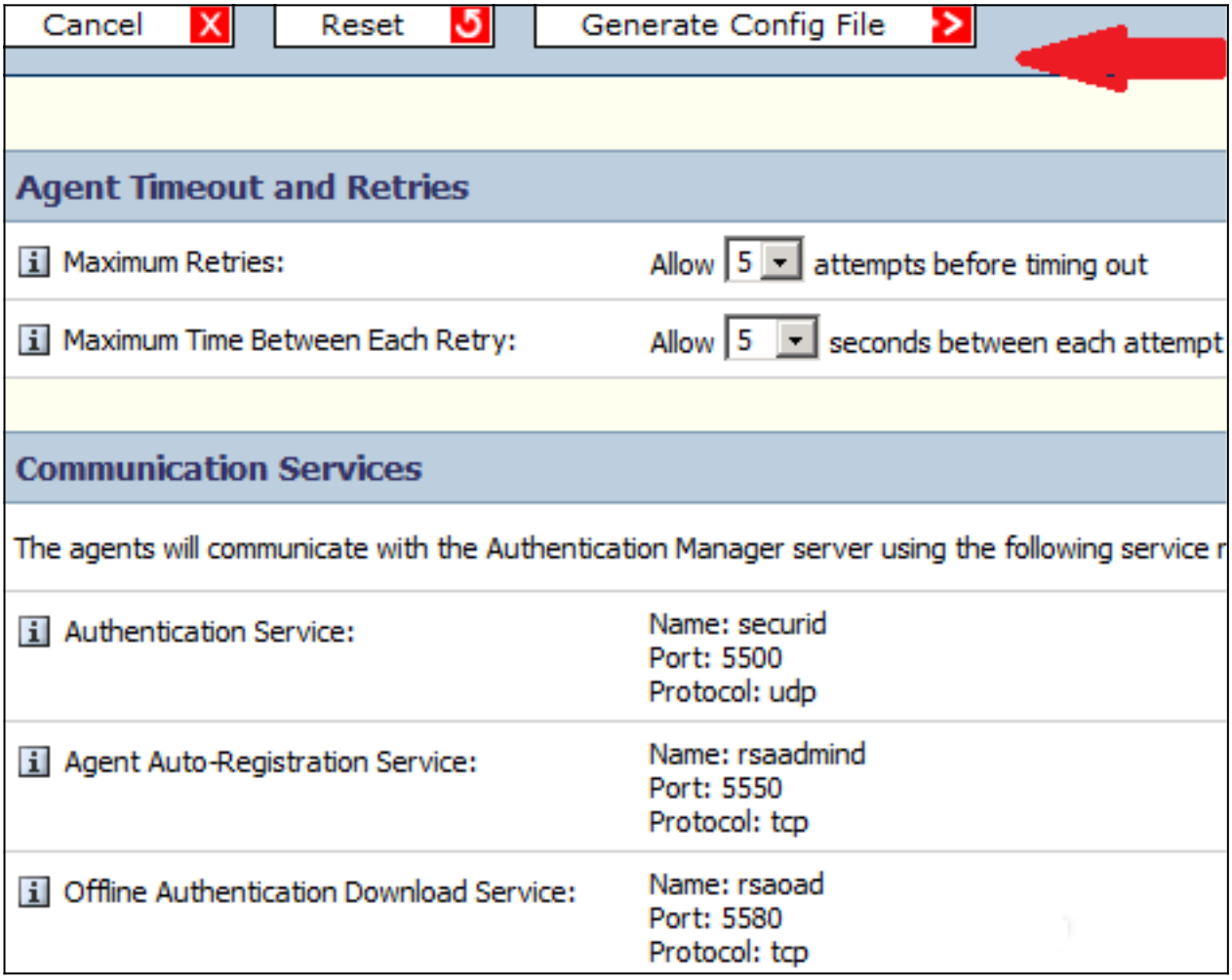
다음은 상담원이 추가되면 표시되는 정보의 예입니다.



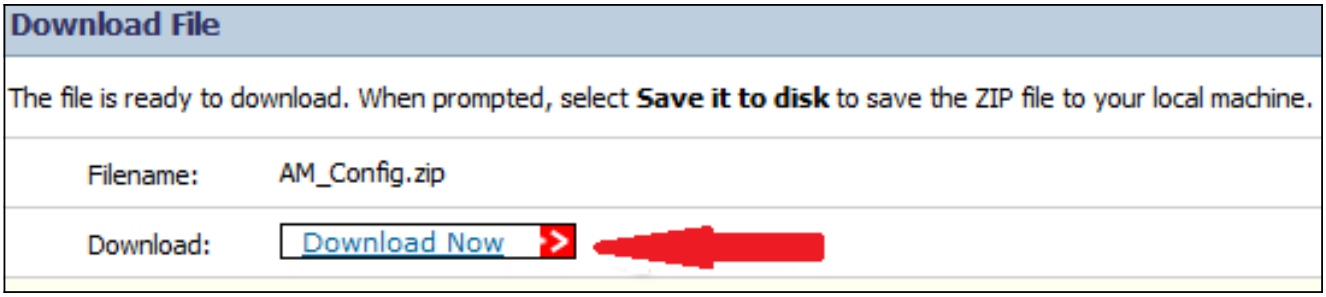
4. RSA Security Console에서 sdconf.rec 구성 파일을 생성하려면 **Access > Authentication Agents > Generate Configuration File**로 이동합니다.



5. 최대 재시도 횟수 및 각 재시도 사이의 최대 시간 기본값을 사용합니다.



6. 구성 파일을 다운로드합니다.

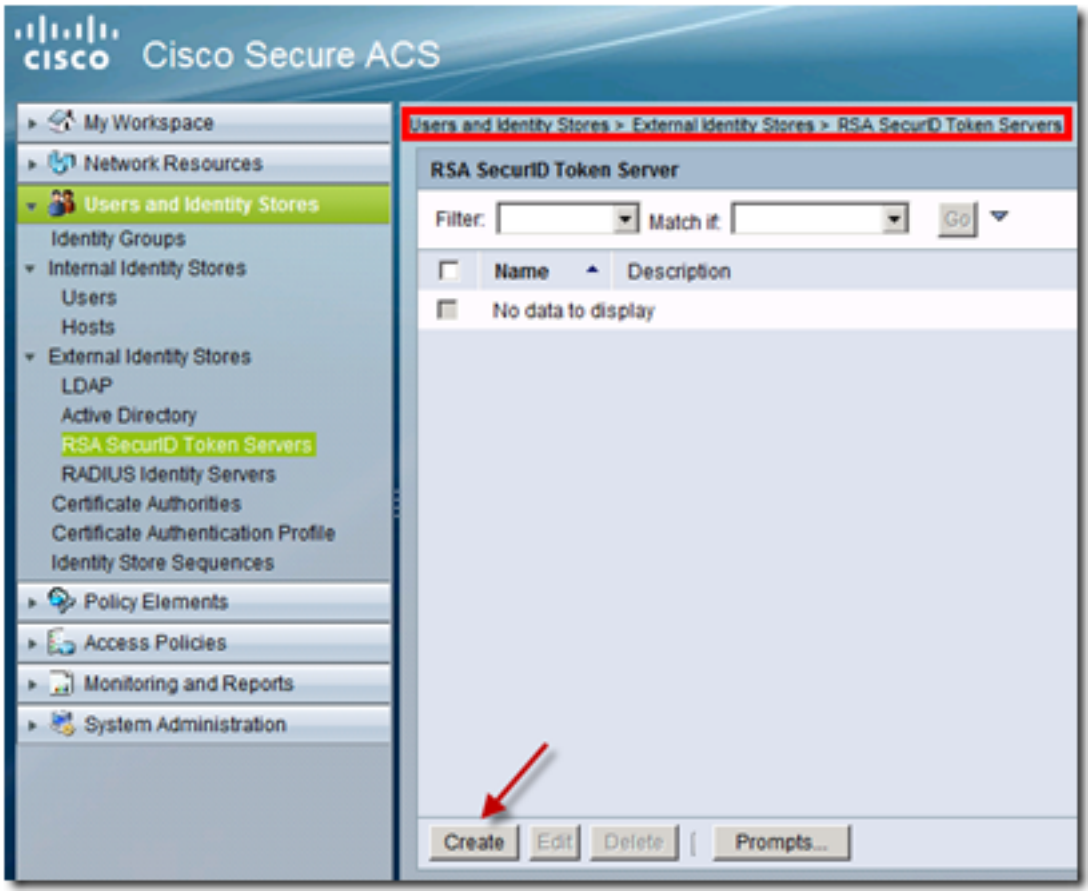


.zip 파일에는 실제 구성 sdconf.rec 파일이 포함되어 있습니다. 이 파일은 ACS 관리자가 구성 작업을 완료하기 위해 필요합니다.

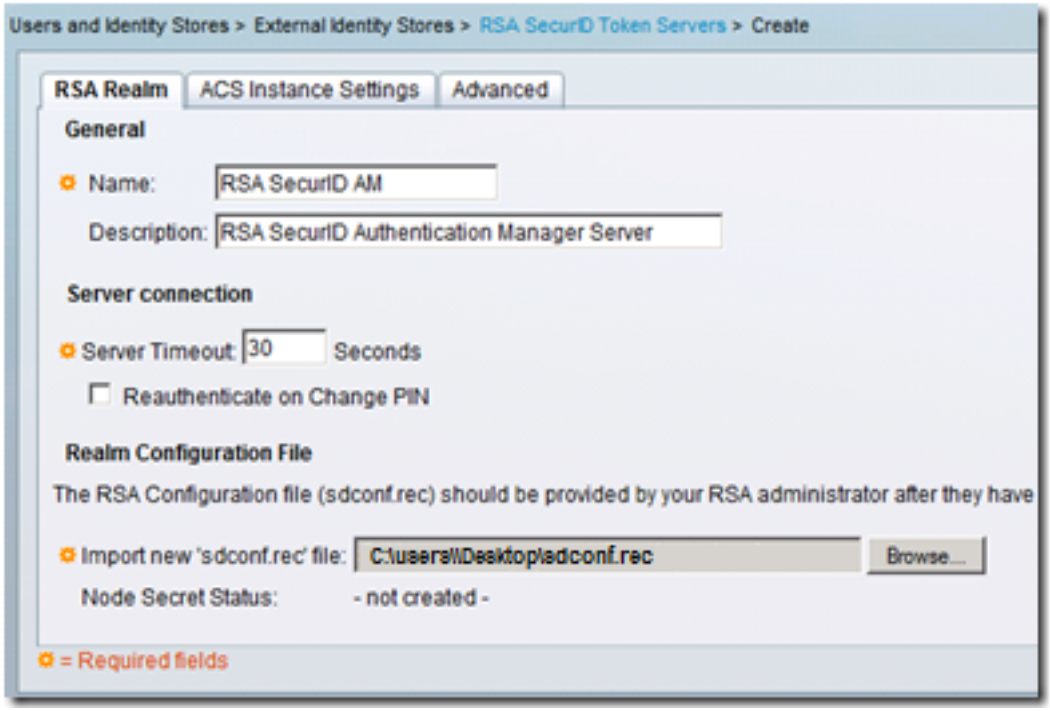
ACS 버전 5.X 서버

이 절차에서는 ACS 관리자가 구성 파일을 검색하고 전송하는 방법에 대해 설명합니다.

1. Cisco Secure ACS Version 5.x 콘솔에서 **Users and Identity Stores(사용자 및 ID 저장소) > External Identity Stores(외부 ID 저장소) > RSA SecurID Token Servers(RSA SecurID 토큰 서버)로 이동하고 Create**를 클릭합니다.



2. RSA 서버의 이름을 입력하고 RSA 서버에서 다운로드한 sdconf.rec 파일을 찾습니다.



3. 파일을 선택하고 Submit(제출)을 **클릭합니다**.

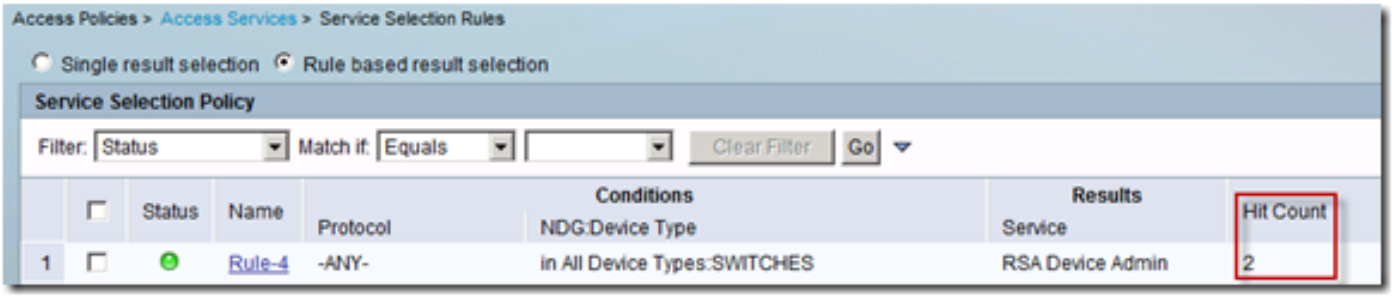
   참고:ACS가 토큰 서버에 처음 연결할 때 RSA Authentication Manager의 ACS 에이전트에 대해 노드 비밀 파일이라는 다른 파일이 생성되고 ACS에 다운로드됩니다.이 파일은 암호화된 통신에 사용됩니다.

다음을 확인합니다.

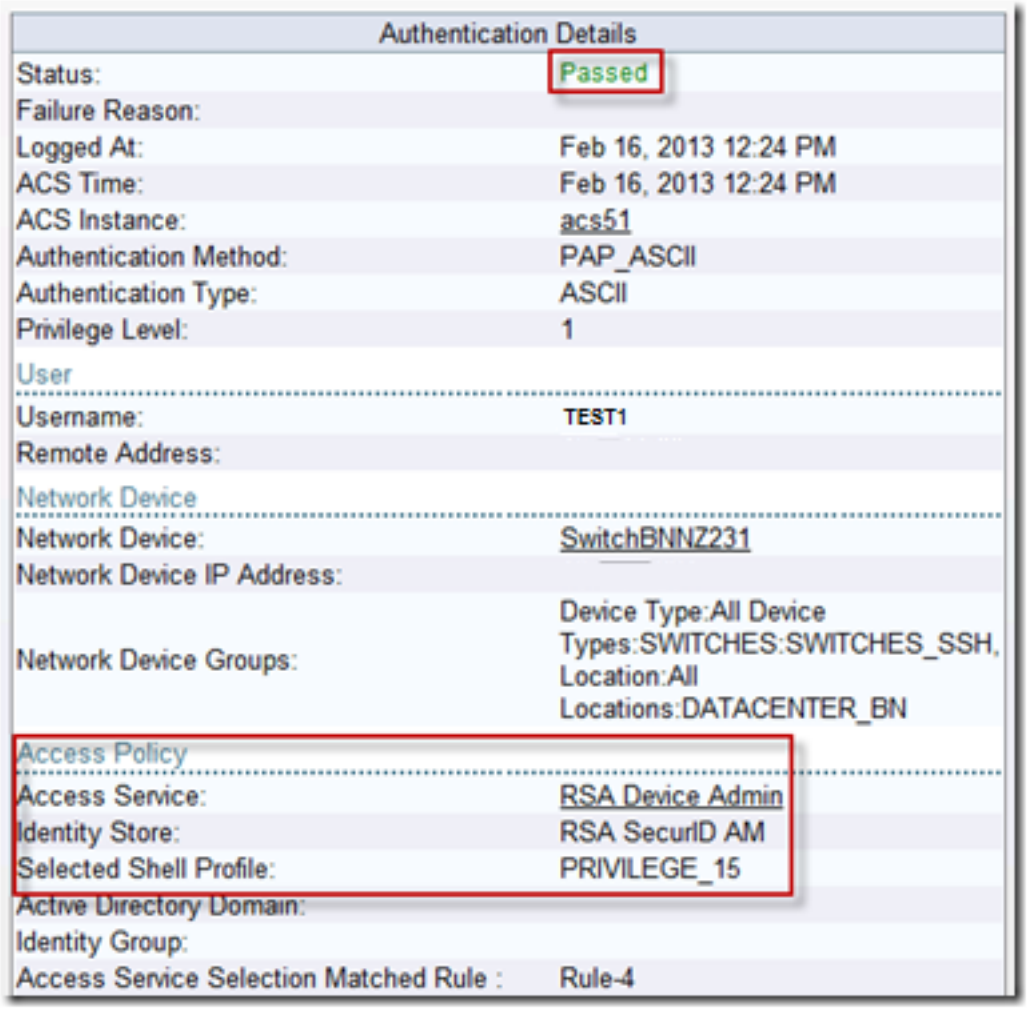
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

ACS 버전 5.X 서버

성공적으로 로그인했는지 확인하려면 ACS 콘솔로 이동하여 Hit Count(히트 수)를 검토합니다.



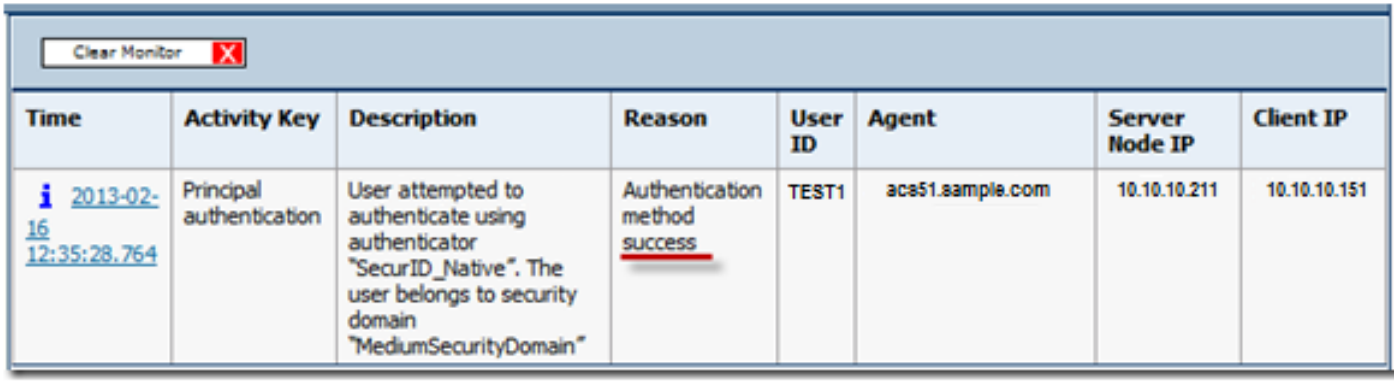
ACS 로그에서 인증 세부 정보를 검토할 수도 있습니다.



Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	acs51
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
User	
Username:	TEST1
Remote Address:	
Network Device	
Network Device:	SwitchBNNZ231
Network Device IP Address:	
Network Device Groups:	Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN
Access Policy	
Access Service:	RSA Device Admin
Identity Store:	RSA SecurID AM
Selected Shell Profile:	PRIVILEGE_15
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched Rule :	Rule-4

RSA 서버

성공적인 인증을 확인하려면 RSA 콘솔로 이동하여 로그를 검토합니다.



Clear Monitor

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
2013-02-16 12:35:28.764	Principal authentication	User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain"	Authentication method success	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

에이전트 레코드 만들기(sdconf.rec)

ACS 버전 5.3에서 RSA SecurID 토큰 서버를 구성하려면 ACS 관리자에게 sdconf.rec 파일이 있어야 합니다.sdconf.rec 파일은 RSA 에이전트가 RSA SecurID 서버 영역과 통신하는 방법을 지정하는 구성 레코드 파일입니다.

sdconf.rec 파일을 생성하려면 RSA 관리자가 ACS 호스트를 RSA SecurID 서버의 에이전트 호스트로 추가하고 이 에이전트 호스트에 대한 구성 파일을 생성해야 합니다.

노드 암호 재설정(securid)

에이전트가 처음에 RSA SecurID 서버와 통신하면 서버는 에이전트에 securid 라는 노드 비밀 파일을 제공합니다.서버와 에이전트 간의 후속 통신은 다른 노드의 신뢰성을 확인하기 위해 노드 비밀의 교환에 의존합니다.

관리자가 노드 암호를 재설정해야 하는 경우도 있습니다.

1. RSA 관리자는 RSA SecurID 서버의 에이전트 호스트 레코드에 있는 Node Secret Created 확인란을 선택 취소해야 합니다.
2. ACS 관리자는 ACS에서 securid 파일을 제거해야 합니다.

자동 로드 밸런싱 재정의

RSA SecurID 에이전트는 영역의 RSA SecurID 서버에서 요청된 로드 밸런싱을 자동으로 수행합니다.그러나 로드 밸런싱을 수동으로 수행할 수 있습니다.각 에이전트 호스트에서 사용하는 서버를 지정할 수 있습니다.에이전트 호스트가 다른 서버보다 더 자주 일부 서버에 인증 요청을 리디렉션하도록 각 서버에 우선순위를 할당할 수 있습니다.

텍스트 파일에서 우선 순위 설정을 지정하고 sdopts.rec로 저장한 다음 ACS에 업로드해야 합니다.

수동으로 개입하여 다운 RSA SecurID 서버 제거

RSA SecurID 서버가 다운되면 자동 제외 메커니즘이 항상 신속하게 작동하지 않습니다.이 프로세스를 가속화하기 위해 ACS에서 sdstatus.12 파일을 제거합니다.