



Cisco Secure ACS-Cisco ISE 마이그레이션

이 장에서는 데이터를 Cisco ACS(Secure Access Control System), 릴리스 5.5, 5.6, 에서 Cisco ISE(Identity Services Engine), 릴리스 1.4로 마이그레이션하는 것과 관련된 정보를 설명합니다.

- Cisco Secure ACS에서 Cisco ISE로 , 1 페이지
- 마이그레이션이전 릴리스의 Cisco Secure ACS에서 Cisco ISE로 , 4 페이지
- 정책 모델, 5 페이지
- Cisco Secure ACS 분산 구축 모델, 7 페이지
- Cisco ISE 분산형 구축 모델, 7 페이지
- 마이그레이션 기능, 7 페이지
- 마이그레이션 툴 보고서, 10 페이지
- UTF-8 지원, 13 페이지
- ISE 802.1X 서비스에 대한 FIPS 지원, 14 페이지
- Cisco Secure ACS/Cisco ISE 버전 검증, 15 페이지

Cisco Secure ACS에서 Cisco ISE로

기존 Cisco Secure ACS, 릴리스 5.5 이상 데이터를 Cisco ISE, 릴리스 1.4, VM 또는 어플라이언스로 마이그레이션하기 전에, 모든 설정, 백업 및 설치 지침을 읽고 이해해야 합니다.

기존 Cisco Secure ACS, 릴리스 5.5 이상 데이터를 마이그레이션하기 전에, Cisco Secure ACS, 릴리스 5.5 이상과 Cisco ISE, 릴리스 1.3의 관련 데이터 구조 및 스키마 차이를 완전히 파악하는 것이 좋습니다.

Cisco Secure ACS, 릴리스 5.5 이상 데이터베이스에서 Cisco ISE, 릴리스 1.4으로 마이그레이션하는 경우, 데이터 마이그레이션은 다음을 지원합니다.

- Cisco ISE 릴리스 1.4에서 Cisco Secure ACS 릴리스 5.5 이상의 기능을 지원합니다.
- Cisco Secure ACS, 릴리스 5.5 이상에서 데이터를 마이그레이션 할 때, Cisco ISE, 릴리스 1.4의 새로운 기능을 지원합니다.



참고 각 Cisco Secure ACS 또는 Cisco ISE 릴리스에서 동적으로 변경되는 기능상의 차이로 인해, 모든 Cisco Secure ACS 데이터를 Cisco ISE로 마이그레이션할 수 있는 것은 아닙니다. Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4 으로 데이터를 마이그레이션하면, 컨피그레이션 차이가 최소화되므로 Cisco ISE에서 이전에 지원되지 않았던 Cisco Secure ACS 기능을 지원합니다.



참고 명명 규칙, 정책 계층 구조, 사전 정의된 개체 등과 관련된 Cisco ISE 및 Cisco Secure ACS 데이터의 차이로 인해, 마이그레이션 툴이 모든 개체를 지원하지는 않을 수 있습니다. 그러나 용이하게 수정 조치를 취할 수 있도록, 마이그레이션되지 않은 개체에 대한 경고 및 오류를 표시합니다.

관련 항목

[지원 데이터 마이그레이션 경로](#), 2 페이지

[활성화 마이그레이션 인터페이스](#), 3 페이지

[데이터 마이그레이션을 위한 지원 Cisco Secure ACS 릴리스](#), 3 페이지

지원 데이터 마이그레이션 경로

표 1: Cisco Secure ACS 릴리스-Cisco ISE 릴리스 지원 마이그레이션

Cisco ISE	Cisco Secure ACS 3.x, 4.x 및 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3	Cisco Secure ACS 5.5	Cisco Secure ACS 5.6 이상
1.0	지원되지 않음	지원됨 (RADIUS만 해당)	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음
1.1	지원되지 않음	지원됨 (RADIUS 만)	지원됨 (RADIUS 만)	지원되지 않음	지원되지 않음	지원되지 않음
1.2	지원되지 않음	지원되지 않음	지원되지 않음	지원됨 (RADIUS만 해당)	지원되지 않음	지원되지 않음
1.3	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원	지원
1.4	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원	지원
2.0	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원	지원

Cisco ISE	Cisco Secure ACS 3.x, 4.x 및 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3	Cisco Secure ACS 5.5	Cisco Secure ACS 5.6 이상
2.1	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원	지원
2.2	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원	지원
2.3	지원됨(Cisco Secure ACS 4.2만 해당)	지원되지 않음	지원되지 않음	지원되지 않음	지원	지원
2.4	지원됨(Cisco Secure ACS 4.2만 해당)	지원되지 않음	지원되지 않음	지원되지 않음	지원	지원

관련 항목

[Cisco Secure ACS에서 Cisco ISE로](#), 1 페이지

데이터 마이그레이션을 위한 지원 Cisco Secure ACS 릴리스

Cisco Secure ACS 소프트웨어의 이전 릴리스에서 Cisco ISE, 릴리스 1.4로 마이그레이션할 수 있는 지점으로 데이터를 마이그레이션할 수 있습니다.

Cisco ISE, 릴리스 1.4 어플라이언스로 마이그레이션하려는 Cisco Secure ACS 데이터의 시작 릴리스 단계에 따라, 마이그레이션 툴을 사용하기 전에 몇 가지 마이그레이션 단계가 필요할 수 있습니다.

관련 항목

[Cisco Secure ACS에서 Cisco ISE로](#), 1 페이지

활성화 마이그레이션 인터페이스

마이그레이션 프로세스를 시작하기 전에, Cisco Secure ACS 및 Cisco ISE 서버에서 데이터 마이그레이션에 사용되는 인터페이스를 활성화해야 합니다. 마이그레이션 프로세스가 완료된 후, 두 서버에서 마이그레이션 인터페이스를 비활성화하는 것이 좋습니다.

단계 1 Cisco Secure ACS CLI에서 다음 명령을 입력하여 Cisco Secure ACS 시스템에서 마이그레이션 인터페이스를 활성화합니다.

acs config-web-interface 마이그레이션 활성화

단계 2 Cisco ISE 서버에서 마이그레이션 인터페이스를 활성화합니다.

a) Cisco ISE CLI에서 **application configure ise** 명령을 입력합니다.

b) **11**을 enable/disable ACS Migration에 입력합니다.

c) **Y**를 입력합니다.



참고 마이그레이션 프로세스가 완료된 후, 다음의 **acs config-web-interface migration disable** 명령을 사용하여 Cisco Secure ACS 컴퓨터에서 마이그레이션 인터페이스를 비활성화합니다.



참고 마이그레이션 프로세스가 완료된 후, Cisco ISE 서버에서 마이그레이션 인터페이스를 비활성화합니다.

관련 항목

[Cisco Secure ACS에서 Cisco ISE로](#), 1 페이지

마이그레이션이전 릴리스의 Cisco Secure ACS에서 Cisco ISE로

마이그레이션 툴을 사용하여 Cisco ISE 릴리스 1.4으로 마이그레이션 할 수 있도록 Cisco Secure ACS 데이터의 이전 릴리스를 Cisco Secure ACS, 릴리스 5.5 이상으로 마이그레이션할 수 있습니다.

관련 항목

[마이그레이션Cisco Secure ACS, 릴리스 3.x에서](#), 4 페이지

[마이그레이션Cisco Secure ACS, 릴리스 4.x에서](#), 5 페이지

[마이그레이션Cisco Secure ACS, 릴리스 5.x에서](#), 5 페이지

마이그레이션Cisco Secure ACS, 릴리스 3.x에서

사용자 환경에서 Cisco Secure ACS, 릴리스 3.x를 실행 중인 경우 마이그레이션 지원 버전의 Cisco Secure ACS, 릴리스 4.x로 업그레이드한 다음, Cisco Secure ACS, 릴리스 5.5 이상으로 업그레이드하십시오.

단계 1 [Cisco Secure ACS Solution Engine 4.1 설치 설명서](#) 또는 [Cisco Secure ACS Solution Engine 4.2 설치 설명서](#)에 설명된 대로, Cisco Secure ACS, 릴리스 3.x의 업그레이드 경로를 확인합니다.

단계 2 Cisco Secure ACS, 릴리스 3.x 서버를 마이그레이션 지원 Cisco Secure ACS, 릴리스 4.x 버전으로 업그레이드합니다. 예를 들어 다음 Cisco Secure ACS 4.1.1.24, Cisco Secure ACS 4.1.4, Cisco Secure ACS 4.2.0.124 또는 Cisco Secure ACS 4.2.1 릴리스 중 하나로 업그레이드합니다.

단계 3 업그레이드한 후, Cisco Secure ACS, 릴리스 4.x에서 Cisco Secure ACS, 릴리스 5.5 이상으로 마이그레이션을 설명하는 단계를 수행합니다.

관련 항목

[마이그레이션이전 릴리스의 Cisco Secure ACS에서 Cisco ISE로](#) , 4 페이지

마이그레이션 Cisco Secure ACS, 릴리스 4.x에서

사용자 환경에서 마이그레이션 지원 버전의 Cisco Secure ACS, 릴리스 4.x를 실행하고 있지 않은 경우, Cisco Secure ACS, 릴리스 4.x에서 Cisco Secure ACS, 릴리스 5.5 이상으로 마이그레이션할 수 있는 지점으로 업그레이드합니다.

-
- 단계 1 Cisco Secure ACS, 릴리스 4.x 서버가 현재 마이그레이션 지원 버전 중 하나를 실행하지 않는 경우, Cisco Secure ACS 릴리스 4.x 버전을 마이그레이션 지원 버전으로 업그레이드합니다.
 - 단계 2 마이그레이션 컴퓨터(Windows 서버)에 동일한 마이그레이션 지원 버전의 Cisco Secure ACS를 설치합니다.
 - 단계 3 Cisco Secure ACS, 릴리스 4.x 데이터를 백업하고, 마이그레이션 컴퓨터에서 복원합니다.
 - 단계 4 마이그레이션 유틸리티를 마이그레이션 컴퓨터에 놓습니다. 설치 및 복구 DVD에서 마이그레이션 유틸리티를 가져올 수 있습니다.
 - 단계 5 마이그레이션 컴퓨터에서 마이그레이션 유틸리티의 Analyze and Export(분석 및 내보내기) 단계를 실행합니다.
 - 단계 6 Analyze and Export(분석 및 내보내기) 단계에서 문제를 해결합니다.
 - 단계 7 마이그레이션 컴퓨터에서 마이그레이션 유틸리티의 Import(가져오기) 단계를 실행하며, 이 단계에서 마이그레이션 유틸리티는 데이터를 Cisco Secure ACS, 릴리스 5.5 이상의 서버로 가져옵니다.
-

관련 항목

[마이그레이션이전 릴리스의 Cisco Secure ACS에서 Cisco ISE로](#) , 4 페이지

마이그레이션 Cisco Secure ACS, 릴리스 5.x에서

사용자 환경에서 Cisco Secure ACS, 릴리스 5.x를 실행 중인 경우, Cisco Secure ACS, 릴리스 5.5 이상으로 업그레이드해야 합니다.

관련 항목

[마이그레이션이전 릴리스의 Cisco Secure ACS에서 Cisco ISE로](#) , 4 페이지

정책 모델

Cisco Secure ACS 및 Cisco ISE에는 단순 및 규칙 기반 인증 패러다임이 모두 포함되어 있지만, Cisco Secure ACS 및 Cisco ISE는 여러 정책 모델을 기반으로 하므로 정책을 Cisco Secure ACS 5.5 이상에서 Cisco ISE로 마이그레이션하는 것이 약간 복잡합니다.

Cisco Secure ACS 정책 계층 구조는 인증 요청을 액세스 서비스로 리디렉션하는 서비스 선택 규칙으로 시작합니다. 액세스 서비스는 내부 또는 외부 ID 저장소에 대해 사용자를 인증하고 정의된 조건에 따라 사용자에게 권한을 부여하는 ID 및 권한 부여 정책으로 구성됩니다.

인증 및 권한 부여 정책은 Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4으로 마이그레이션됩니다. Cisco ISE 릴리스 1.4은 Cisco Secure ACS, 릴리스 5.5/5.6의 SSP(Service Selection Policy)와 유사한 정책 집합이라는 새로운 정책 모델을 지원하므로, 정책 마이그레이션 프로세스가 간소화됩니다.

관련 항목

[Cisco Secure ACS 서비스 선택 정책 및 Cisco ISE 정책 설정, 6 페이지](#)

[Cisco Secure ACS\(Access Control System\) 및 Cisco ISE 정책 집합, 6 페이지](#)

Cisco Secure ACS 서비스 선택 정책 및 Cisco ISE 정책 설정

Cisco Secure ACS, 릴리스 5.5/5.6 SSP(Service Selection Policy)는 SSP 규칙을 기반으로 적절한 서비스에 요청을 배포하는 반면, Cisco ISE 정책 집합은 정책 집합에 대한 항목 기준을 포함하는 규칙을 보유합니다. 정책 집합의 순서는 SSP 규칙의 순서와 유사한 입력 규칙의 순서와 동일합니다.

여러 SSP 규칙이 Cisco Secure ACS에서 동일한 서비스 또는 서비스 재사용을 요청할 수 있습니다. 그러나 각 정책 집합에는 고유한 입력 조건이 있으므로, Cisco ISE의 정책 집합을 재사용할 수 없습니다. 여러 SSP 규칙에서 요청한 단일 서비스를 마이그레이션하려는 경우, 해당 서비스의 복사본인 여러 정책 집합을 생성해야 합니다. Cisco Secure ACS에서 동일한 서비스를 요청하는 각 SSP 규칙에 대해 Cisco ISE에서 정책 집합을 생성해야 하는 것입니다.

Cisco Secure ACS에서 SSP 규칙을 비활성화되거나 모니터링되는 것으로 정의할 수 있으며, 정책 집합의 동등한 항목 규칙은 Cisco ISE에서 항상 활성화됩니다. Cisco Secure ACS에서 SSP 규칙이 비활성화되거나 모니터링되는 경우, SSP 규칙에서 요청하는 정책 서비스를 Cisco ISE로 마이그레이션할 수 없습니다.

관련 항목

[정책 모델, 5 페이지](#)

Cisco Secure ACS(Access Control System) 및 Cisco ISE 정책 집합

해당 서비스를 요청하지 않고 정책 서비스를 정의할 수 있어, Cisco Secure ACS의 SSP에서 규칙에 따라 비활성 상태인 정책 서비스를 정의할 수 있습니다. Cisco Secure ACS 릴리스 5.5 이상에는 즉시 사용 가능한 DenyAccess 서비스가 있으며, 이 서비스에는 모든 요청을 자동으로 거부하는 Cisco Secure ACS의 기본 SSP 규칙에 대한 정책이나 허용되는 프로토콜이 없습니다. Cisco ISE에 대한 동일한 정책 집합이 없습니다. 그러나 항목 규칙이 없이 Cisco ISE의 정책 집합을 참조하는 정책 집합은 가질 수 없습니다.

허용되는 프로토콜은 Cisco Secure ACS, 릴리스 5.5 이상에서 (SSP에서 전체 서비스를 가리키는 조건 제외하고) 조건이 지정되지 않은 전체 서비스(특정 정책 아님)에 연결됩니다. 허용되는 프로토콜은 인증 정책을 Cisco ISE에서 조건이 지정된 외부 규칙의 결과로서 참조합니다.

ID 정책은 Cisco Secure ACS, 릴리스 5.5 이상에서 ID 소스(ID 소스 및 ID 저장소 시퀀스)를 생성하는 규칙의 단순한 목록입니다. 인증 정책에는 두 가지 레벨의 규칙, 즉 외부 정책 규칙과 내부 정책 규칙이 있습니다. 외부 정책 규칙은 허용되는 프로토콜이 되며, 내부 정책 규칙 집합의 항목 기준입니다. 내부 정책 규칙으로 인해 ID 소스가 생성됩니다.

Cisco Secure ACS, 릴리스 5.5 이상 및 Cisco ISE, 릴리스 1.4에는 각 권한 부여 정책에 첨부된 선택적 예외 정책이 포함되어 있습니다. Cisco ISE, 릴리스 1.4은 모든 권한 부여 정책에 영향을 주는 예외 정책 외에 선택적인 Global Exception Policy(전역 예외 정책)를 제공합니다. Cisco Secure ACS 릴리스 5.5 이상의 Global Exception Policy(전역 예외 정책)에 해당하는 정책은 없습니다. 로컬 예외 정책을 먼저 처리한 다음 Global Exception Policy(전역 예외 정책) 및 권한 부여 정책을 부여합니다.

관련 항목

[정책 모델, 5 페이지](#)

Cisco Secure ACS 분산 구축 모델

Cisco Secure ACS 구축 모델은 기본 Cisco Secure ACS 서버에서 구성을 변경하는 하나의 기본 및 여러 보조 Cisco Secure ACS 서버로 구성됩니다. 이러한 구성은 보조 Cisco Secure ACS 서버에 복제됩니다. 모든 기본 및 보조 Cisco Secure ACS 서버는 AAA 요청을 처리할 수 있습니다. 모든 Cisco Secure ACS 서버를 로그 컬렉터로 설정할 수 있지만, 기본 Cisco Secure ACS 서버는 모니터링 및 보고서 뷰어의 기본 로그 컬렉터이기도 합니다.

Cisco ISE 분산형 구축 모델

Cisco ISE 구축 모델은 하나의 기본 노드와 여러 보조 노드로 구성됩니다. 구축의 각 Cisco ISE 노드는 관리, 정책 서비스 및 모니터링 페르소나 중에서 하나 이상을 선택할 수 있습니다. Cisco ISE를 설치 하면, 모든 노드가 독립형 상태가 됩니다. Cisco ISE 노드 중 하나를 관리 페르소나로 실행되는 기본 노드로 정의해야 합니다. 기본 노드를 정의한 후에는 정책 서비스 및 모니터링 페르소나를 사용하여 다른 Cisco ISE 노드를 설정할 수 있습니다. 그런 다음 기본 노드로 다른 보조 노드를 등록하고, 각 노드에 대해 특정 역할을 정의할 수 있습니다. Cisco ISE 노드를 보조 노드로 등록하는 경우, Cisco ISE에서는 즉시 기본 노드에서 보조 노드로 연결되는 데이터베이스 링크를 생성하고 복제 프로세스를 시작합니다. 모든 컨피그레이션은 기본 관리 ISE 노드에서 변경되며, 보조 노드에 복제됩니다. 모니터링 ISE 노드는 로그 컬렉터 역할을 합니다.

마이그레이션 기능

마이그레이션 툴은 Cisco Secure ACS 데이터를 Cisco ISE로 전송하는 기능을 담당하여, 다음과 같은 3가지 주요 단계를 수행합니다.

1. 데이터를 Cisco Secure ACS에서 내보냅니다.
2. 데이터를 마이그레이션 툴에 유지합니다.
3. 데이터를 Cisco ISE로 가져옵니다.

관련 항목

[데이터 내보내기, 8 페이지](#)

[데이터 가져오기](#)

[개체 확장성](#)[실패한 데이터 마이그레이션 다시 시작](#), 8 페이지

데이터 내보내기

마이그레이션 프로세스의 첫 번째 단계는 Cisco Secure ACS PI(Programmatic Interface)를 사용하여 Cisco Secure ACS 데이터를 내보내는 것입니다. 데이터를 내보내고 마이그레이션 애플리케이션으로 내보내도록 요청하는 Cisco Secure ACS, 릴리스 5.5 또는 5.6 시스템에 로그인해야 합니다. 내보낸 데이터는 Cisco ISE, 릴리스 1.4 어플라이언스로 가져올 수 있는지 확인하기 위해 검증됩니다. 데이터가 유효하지 않은 경우, 내보내기 보고서에 상태가 기록됩니다.

[관련 항목](#)[마이그레이션 기능](#), 7 페이지

실패한 데이터 마이그레이션 다시 시작

마이그레이션 툴은 가져오기 또는 내보내기 작업의 각 단계에서 체크포인트를 유지 관리합니다. 가져오기 또는 내보내기 프로세스가 실패하는 경우, 프로세스를 처음부터 다시 시작할 필요가 없습니다. 장애가 발생하기 전에, 마지막 체크포인트에서 시작할 수 있습니다.

마이그레이션 프로세스가 실패하면, 마이그레이션 툴이 프로세스를 종료합니다. 실패 후 마이그레이션 툴을 재시작하면, 이전 가져오기/내보내기를 재개하거나 이전 프로세스를 취소하고 새 마이그레이션 프로세스를 시작할 수 있는 대화 상자가 표시됩니다. 이전 프로세스를 재개하도록 선택하면, 마이그레이션 프로세스가 마지막 체크포인트에서 재개됩니다. 장애에서 다시 시작하면, 이전 프로세스에서 실행되도록 보고서가 다시 시작됩니다.

[관련 항목](#)[마이그레이션 기능](#), 7 페이지

TACACS+ 기능을 Cisco ISE로 마이그레이션

아래에는 Cisco ISE로 마이그레이션되는 TACACS+ 설정이 나와 있습니다.

- 비밀번호 활성화: 내부 사용자는 비밀번호 사용 속성과 함께 Cisco Secure ACS에서 Cisco ISE로 마이그레이션됩니다.
- 네트워크 디바이스: TACACS+ 설정으로 설정된 네트워크 디바이스(예, Cisco Secure ACS의 공유 비밀번호 및 단일 연결 모드)를 마이그레이션 툴로 내보냅니다.
 - 기본 네트워크 디바이스: TACACS+ 설정으로 구성된 기본 네트워크 디바이스 개체를 Cisco Secure ACS에서 내보내고 마이그레이션하는 동안에 Cisco ISE 릴리스 2.0을 새로 설치할 때 ISE로 가져옵니다. 기존 Cisco ISE 컨피그레이션에서는 기본 네트워크 디바이스(RADIUS 및 TACACS+ 설정 사용)가 업데이트됩니다.
- 셸 프로파일: Cisco Secure ACS의 셸 프로파일 개체를 마이그레이션 툴로 내보냅니다. Cisco ISE로 가져오고 **Work Centers**(작업 센터) > **Device Administration**(디바이스 관리) > **Policy Results**(정책 결과) > **TACACS Profiles**(TACACS 프로파일) 페이지에 표시됩니다. 이 페이지에는 ISE로 식

별되는 사전 정의된 속성이 포함되어 있으며, 나머지 특성은 사용자 지정 속성으로 표시됩니다. 마이그레이션된 속성에는 Cisco Secure ACS에서 마이그레이션되었음을 나타내는 설명이 있습니다. 정적 특성과 동적 특성이 모두 지원됩니다.

- 명령 집합: Cisco Secure ACS의 명령 집합 개체를 마이그레이션 도구로 내보냅니다. Cisco ISE로 가져와서 **Work Centers**(작업 센터) > **Device Administration**(디바이스 관리) > **Policy Results**(정책 결과) > **TACACS Command Sets**(TACACS 명령 집합) 페이지에 표시됩니다. Cisco Secure ACS에서는 마이그레이션된 개체에 대한 설명을 추가합니다. 이미 설명이 있는 마이그레이션된 개체의 경우, Cisco Secure ACS가 동일하게 유지됩니다.
- TACACS 전역 설정: Cisco Secure ACS의 TACACS+ 전역 설정 개체를 마이그레이션 툴로 내보내고 검증 오류 또는 경고가 보고됩니다. 마이그레이션 툴에서 사전 정의된 데이터 개체의 일부로 데이터를 가져올 수 있습니다.
- TACACS 정책: 디바이스 관리 서비스에 대한 TACACS+ 인증, 권한 부여 및 권한 부여 예외 정책을 Cisco ISE로 가져옵니다. 권한 부여 정책 규칙의 결과는 명령 집합 및 셸 프로파일일 수 있습니다. 오류로 인해 명령 집합 또는 셸 프로파일을 내보내지 않으면, 정책을 마이그레이션 툴로 내보낼 수 없습니다.

마이그레이션 중에는 마이그레이션 툴이 네트워크 액세스 및 디바이스 관리 서비스에 대한 두 가지 정책 집합을 유지 관리합니다. ISE로 가져오는 동안 마이그레이션 툴은 서비스 유형을 확인하고 서비스 유형을 가져와야 하는 정책을 결정합니다.



참고 마이그레이션 후, Cisco ISE에서 정책 컨피그레이션을 확인하십시오.

외부 프록시 서버 마이그레이션

마이그레이션 툴은 다음 외부 프록시 서버에서 프록시 개체를 내보낼 수 있습니다.

- TACACS+ 외부 프록시 서버:
외부 프록시 서버가 TACACS+로 설정된 경우, TACACS+ 개체는 **Work Centers**(작업 센터) > **Device Administration**(디바이스 관리) > **Network Resources**(네트워크 리소스) > **TACACS External Servers**(TACACS 외부 서버) 페이지로 마이그레이션됩니다.
- RADIUS 외부 프록시 서버:
외부 프록시 서버가 RADIUS로 설정된 경우, RADIUS 개체는 **Administration**(관리) > **Network Resources**(네트워크 리소스) > **External TACACS Servers**(TACACS 외부 서버) 페이지로 마이그레이션됩니다.
- Cisco Secure ACS 외부 프록시 서버:
외부 프록시 서버가 Cisco Secure ACS(TACACS + 및 RADIUS 모두 지원) 옵션으로 설정된 경우, TACACS 및 RADIUS 개체가 다른 위치로 마이그레이션됩니다. TACACS+ 개체는 개체 이름 앞에 "TACACS_"라는 접두사가 붙은 **Work Centers**(작업 센터) > **Device Administration**(디바이스 관리) > **Network Resources**(네트워크 리소스) > **External TACACS Servers**(외부 TACACS 서버)

페이지로 마이그레이션됩니다. RADIUS 개체는 개체 이름 앞에 "RADIUS_"라는 접두사가 붙은 **Administration(관리) > Network Resources(네트워크 리소스) > External TACACS Servers(외부 TACACS 서버)** 페이지로 마이그레이션됩니다.

Cisco Secure ACS는 단일 연결 컨피그레이션을 지원하지 않으므로, 가져오기를 수행하는 동안 마이그레이션 애플리케이션은 이 속성에 대해 Cisco ISE에서 지원하는 기본값으로 프록시 개체를 생성합니다.

외부 프록시 서버 시퀀스 마이그레이션

마이그레이션 툴은 다음 외부 프록시 서버에서 외부 서버 집합을 내보낼 수 있습니다.

- TACACS+ 외부 프록시 서버:

외부 프록시 서버가 TACACS+ 서버 시퀀스로 설정되면, TACACS+ 개체는 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > TACACS Server Sequence(TACACS 서버 시퀀스)** 페이지로 마이그레이션됩니다.

- RADIUS 외부 프록시 서버:

외부 프록시 서버가 RADIUS 서버 시퀀스로 설정되면, RADIUS 개체는 **Administration(관리) > Network Resources(네트워크 리소스) > RADIUS Server Sequence(RADIUS 서버 시퀀스)** 페이지로 마이그레이션됩니다.

- Cisco Secure ACS 외부 프록시 서버:

외부 프록시 서버가 Cisco Secure ACS(TACACS 및 RADIUS 모두 지원) 옵션으로 설정되면, TACACS 및 RADIUS 개체가 다른 위치로 마이그레이션됩니다. TACACS+ 개체는 개체 이름 앞에 "TACACS_"라는 접두사가 포함된 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > TACACS Server Sequence(TACACS 서버 시퀀스)** 페이지로 마이그레이션됩니다. RADIUS 개체는 개체 이름 앞에 "RADIUS_"라는 단어가 포함된 **Administration(관리) > Network Resources(네트워크 리소스) > RADIUS Server Sequence(RADIUS 서버 시퀀스)** 페이지로 마이그레이션됩니다.

마이그레이션 툴 보고서

Cisco ISE는 Cisco Secure ACS, 릴리스 5.5/5.6 데이터 마이그레이션 중에 가져오기, 내보내기 및 정책 차이 분석을 위한 보고서를 생성합니다.

보고서 파일을 다른 사람과 공유하거나 다른 위치에 저장하려는 경우, 마이그레이션 툴 디렉토리의 Reports(보고서) 폴더에서 다음 파일을 찾을 수 있습니다.

- import_report.txt
- export_report.txt
- policy_gap_report.txt

관련 항목

[보고서 내보내기](#), 11 페이지[보고서 가져오기](#), 12 페이지[정책 간격 분석 보고서](#), 11 페이지

보고서 내보내기

이 보고서는 데이터를 Cisco Secure ACS 데이터베이스에서 내보내는 동안 발생하는 특정 정보 또는 오류를 나타냅니다. 보고서 끝 부분에는 Cisco Secure ACS와 Cisco ISE 사이의 기능적 차이에 대해 설명하는 데이터 분석 섹션이 포함되어 있습니다. 내보내기 보고서에는 가져오지 않을 개체에 대한 오류 정보도 포함됩니다.

표 2: Cisco Secure ACS-Cisco ISE 마이그레이션 툴 내보내기 보고서

보고서 유형	메시지 유형	메시지 설명 5:
Export(내보내기)	정보	성공적으로 내보낸 데이터 개체의 이름을 나열합니다.
	경고	Cisco ISE, 릴리스 1.4에서는 데이터 개체가 지원되지 않으므로, 내보내기 실패 또는 시도하지 않은 내보내기를 나열합니다(예, TACACS 기반 디바이스인 경우).

관련 항목

[마이그레이션 툴 보고서](#), 10 페이지

정책 간격 분석 보고서

이 보고서에는 Cisco Secure ACS와 Cisco ISE 사이의 정책 격차와 관련된 특정 정보가 나열되어 있으며, 마이그레이션 툴 사용자 인터페이스에서 Policy Gap Analysis Report(정책 간격 분석 보고서) 버튼을 클릭하여 내보내기 프로세스를 완료한 후에 사용할 수 있습니다.

내보내기 단계에서 마이그레이션 툴은 인증 및 권한 부여 정책의 차이를 식별합니다. 마이그레이션되지 않은 정책은 Policy Gap Analysis Report(정책 간격 분석 보고서)에 나열됩니다. 보고서에는 정책과 관련된 모든 호환되지 않는 규칙 및 조건이 나열됩니다. 수작업으로 마이그레이션 할 수 없는 데이터 및 이유를 설명합니다.

일부 조건은 적절한 Cisco ISE 용어를 사용하여 자동으로 마이그레이션할 수 있습니다. 예를 들어, Device Type In(디바이스 유형 입력)이라는 조건은 Device Type Equals(디바이스 유형이 같음)로 마이그레이션됩니다. 조건이 지원되거나 자동으로 변환 될 수 있는 경우, 보고서에 표시되지 않습니다. 조건이 "Not Supported" 또는 "Partially supported"로 확인되면, 정책을 가져오지 않으며 보고서에 조건이 표시됩니다. 마이그레이션을 수행하는 관리자는 그러한 조건을 수정하거나 삭제할 책임이 있습니다. 정책이 수정되거나 삭제되지 않으면, 정책이 Cisco ISE로 마이그레이션되지 않습니다.

그림 1: **Policy Gap Analysis Report**(정책 간격 분석 보고서)의 예

```

policy_gap_report.txt - Notepad
File Edit Format View Help
=====
ISE 1.1 Policy Gap Analysis Report
Date: 2012.01.11:

The Policy Gap Analysis Report is meant to summarize all existing policy
related functionality differences between ACS 5.1 / 5.2 and ISE1.1.

Source:
ACS 5.2
10.56.13.106

=====
Service Selection Policy
=====

All Policy Rules found to be compatible with ISE.

=====
Service: Default Network Access
Policy Type: Authentication Policy
=====

Rule: Rule-1
Description: This rule cannot be migrated because Compound conditions
which have different logical expressing is currently not supported by
ISE policy engine.

=====
Service: Default Network Access
Policy Type: Authorization Policy
=====

All Policy Rules found to be compatible with ISE.

=====
Summary:
*Service Selection Policy      : Supported
*Authentication Policy        : Unsupported
*Authorization Policy          : Supported

Not all policies are compatible with ISE 1.1. out of security concerns,
the migration application will not migrate any of your ACS policies.

=====
End of Report
=====
284608

```

관련 항목

[마이그레이션 툴 보고서](#), 10 페이지

보고서 가져오기

이 보고서는 Cisco ISE 어플라이언스로 데이터를 가져오는 동안 발생하는 특정 정보 또는 오류를 나타냅니다.

표 3: Cisco Secure ACS-Cisco ISE 마이그레이션 툴 가져오기 보고서

보고서 유형	메시지 유형	메시지 설명:
가져오기	정보	성공적으로 가져온 데이터 개체의 이름을 나열합니다.
	오류	다음으로 인한 데이터 개체 오류를 식별합니다. <ul style="list-style-type: none"> • 개체가 이미 있음 • 개체 이름이 문자 제한을 초과함 • 백업 파일에 지원되지 않는 특수 문자가 포함되어 있음 • 개체에 지원되지 않는 데이터 문자가 포함되어 있음

관련 항목

[마이그레이션 툴 보고서](#), 10 페이지

UTF-8 지원

Cisco ISE, 릴리스 1.4는 일부 관리 컨피그레이션에 대해 UTF-8(8 bit Unicode Transformation Format)을 지원합니다. 다음의 컨피그레이션 항목은 UTF-8 인코딩으로 내보내고 가져옵니다.

- [네트워크 액세스 사용자 컨피그레이션](#)
- [RSA](#)
- [RADIUS 토큰](#)
- [정책](#)
- [ID 그룹 이름](#)

네트워크 액세스 사용자 컨피그레이션

- Username(사용자 이름)
- 비밀번호 및 비밀번호 재입력
- 이름
- 성
- 이메일

RSA

RSA 프롬프트 및 메시지는 신청자가 최종 사용자에게 표시합니다.

- Messages(메시지)
- Prompts(프롬프트)

RADIUS 토큰

RADIUS 토큰 프롬프트는 최종 사용자 신청자에게 표시됩니다.

- Authentication(인증) 탭 > Prompt(프롬프트)
- Administrator Configuration(관리자 컨피그레이션)
- 시스템 관리자 사용자 이름과 비밀번호
- UTF-8을 사용하여 관리자 설정

정책

- Authentication(인증) > AV 식의 값
- Authorization(권한 부여) > Other Conditions(기타 조건) > AV 식의 값
- Attribute Value(속성 값)
- Authentication(인증) > simple condition/compound condition(단순 조건/복합 조건) > AV 식의 값
- Authorization(권한 부여) > simple condition/compound condition(단순 조건/복합 조건) > AV 식의 값

ISE 802.1X 서비스에 대한 FIPS 지원

마이그레이션 프로세스가 완료되기 전에 Cisco ISE FIPS 모드를 활성화해서는 안됩니다.

FIPS(Federal Information Processing Standard)를 지원하기 위해, 마이그레이션 톨은 기본 네트워크 디바이스 키랩 데이터를 마이그레이션합니다.

FIPS 준수 및 지원 프로토콜:

- Process Host Lookup(프로세스 호스트 조회)
- EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)
- PEAP(Protected Extensible Authentication Protocol)
- EAP-FAST(Flexible Authentication via Secure Tunneling)

FIPS 비준수 및 미지원 프로토콜:

- EAP-MD5(Message Digest 5)
- PAP(Password Authentication Protocol) 및 ASCII
- CHAP(Challenge Handshake Authentication Protocol)
- MS-CHAPv1(Microsoft Challenge Handshake Authentication Protocol Version 1)
- MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2)
- LEAP(Lightweight Extensible Authentication Protocol)

Cisco Secure ACS/Cisco ISE 버전 검증

내보내기 단계가 시작되기 전에, 마이그레이션 툴이 Cisco Secure ACS 릴리스 버전을 식별합니다. Cisco Secure ACS 버전이 5.5/5.6/5.7/5.8보다 낮거나 높으면, 마이그레이션 프로세스가 시작되지 않습니다. 또한 데이터를 Cisco ISE로 가져오기 전에, Cisco ISE 릴리스 버전이 1.4인지 확인합니다.

