



Cisco Identity Services Engine는, 1.3 마이그레이션 툴 가이드 릴리스

초판: 2014년 10월 31일

최종 변경: 2014년 10월 31일

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

서문:

서론	ix
목적	ix
대상	x
문서 명명 규칙	x
관련 설명서	xi

장 1

Cisco Secure ACS-Cisco ISE 마이그레이션	1
Cisco Secure ACS에서 Cisco ISE로	1
지원 데이터 마이그레이션 경로	2
데이터 마이그레이션을 위한 지원 Cisco Secure ACS 릴리스	3
활성화 마이그레이션 인터페이스	3
마이그레이션이전 릴리스의 Cisco Secure ACS에서 Cisco ISE로	4
마이그레이션Cisco Secure ACS, 릴리스 3.x에서	4
마이그레이션Cisco Secure ACS, 릴리스 4.x에서	5
마이그레이션Cisco Secure ACS, 릴리스 5.x에서	5
정책 모델	5
Cisco Secure ACS 서비스 선택 정책 및 Cisco ISE 정책 설정	6
Cisco Secure ACS(Access Control System) 및 Cisco ISE 정책 집합	6
Cisco Secure ACS 분산 구축 모델	7
Cisco ISE 분산형 구축 모델	7
마이그레이션 기능	7
데이터 내보내기	8
실패한 데이터 마이그레이션 다시 시작	8
TACACS+ 기능을 Cisco ISE로 마이그레이션	8

외부 프록시 서버 마이그레이션 9

외부 프록시 서버 시퀀스 마이그레이션 10

마이그레이션 툴 보고서 10

 보고서 내보내기 11

 정책 간격 분석 보고서 11

 보고서 가져오기 12

UTF-8 지원 13

 네트워크 액세스 사용자 컨피그레이션 13

 RSA 14

 RADIUS 토큰 14

 정책 14

ISE 802.1X 서비스에 대한 FIPS 지원 14

Cisco Secure ACS/Cisco ISE 버전 검증 15

장 2

Cisco ISE에 대한 Cisco Secure ACS 17

Cisco Secure ACS에서 Cisco ISE로의 데이터 마이그레이션 17

 데이터 마이그레이션 시간 예상 17

Cisco Secure ACS-Cisco ISE 마이그레이션 툴 18

 마이그레이션을 시작하는 데 필요한 최소 데이터 컨피그레이션 19

 마이그레이션 툴로 데이터 마이그레이션 모니터링 19

 마이그레이션 툴에서 마이그레이션을 계속하기 위한 Checkpoint 19

 Cisco Secure ACS에서 컨피그레이션 데이터 내보내기 19

 구성 데이터 분석 19

 데이터 지속성 20

 Cisco ISE로 컨피그레이션 데이터 가져오기 20

 소프트웨어 요구 사항 20

장 3

데이터 마이그레이션 원칙 21

Data Migration and Deployment Scenarios 21

 마이그레이션단일 Cisco Secure ACS Appliance에서 데이터 21

 분산 환경에서 데이터 마이그레이션 22

Cisco Secure ACS 릴리스 5.5 또는 5.6 마이그레이션 준비 23
 정책 서비스 마이그레이션 지침 23
 정책별 서비스 마이그레이션 지침 24
 Cisco Secure ACS 정책 규칙 마이그레이션 지침 25
 지원되지 않는 규칙 요소 25

장 4 마이그레이션 툴 설치 29
 마이그레이션 툴 설치 지침 29
 시스템 요구 사항 30
 보안 문제 30
 다운로드Cisco ISE 관리자 포털에서 마이그레이션 툴 파일 31
 Cisco Secure ACS-Cisco ISE 마이그레이션 툴 초기화 31

장 5 영구 데이터 전송 절차 33
 내보내기 Cisco Secure ACS에서 데이터 33
 Cisco ISE와 Cisco Secure ACS 사이의 정책 차이 분석 36
 가져오기 Cisco ISE로 데이터 38
 Cisco ISE에서 마이그레이션된 데이터 확인 41

부록 A: 데이터 구조 매핑 43
 데이터 구조 매핑 43
 마이그레이션된 데이터 개체 43
 데이터 개체가 마이그레이션되지 않음 44
 부분적으로 마이그레이션된 데이터 개체 46
 지원되는 특성 및 데이터 유형 46
 사용자 속성이 Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE 1.4로 마이그레이션됨 46
 사용자 특성: 사용자와 연결 47
 Cisco Secure ACS, 릴리스 5.5 또는 5.6 1.4로 마이그레이션된 호스트 속성 47
 호스트 속성: 호스트에 연결 47
 RADIUS 속성이 Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4로 마이그레이션됨 48

RADIUS 속성: RADIUS 서버에 연결 48

데이터 정보 매핑 48

네트워크 디바이스 매핑 49

Active Directory 매핑 49

외부 TACACS 서버 매핑 50

호스트(엔드포인트) 매핑 50

ID 사전 매핑 51

ID 그룹 매핑 52

LDAP 매핑 52

NDG 유형 매핑 53

NDG 계층 구조 매핑 54

RADIUS 사전 (벤더) 매핑 54

RADIUS 사전 (속성) 매핑 55

사용자 매핑 55

인증서 인증 프로파일 매핑 56

권한 부여 프로파일 매핑 56

다운로드 가능한 ACL 매핑 56

외부 TACACS 서버 매핑 57

ID 속성 사전 매핑 57

RADIUS 토큰 매핑 58

RSA 매핑 59

RSA 프롬프트 매핑 60

ID 저장소 시퀀스 매핑 60

기본 네트워크 디바이스 매핑 60

부록 B:

문제 해결 마이그레이션 툴 문제 해결 63

마이그레이션 툴을 시작할 수 없음 63

로그에 표시되는 오류 메시지 63

연결 오류 63

I/O 예외 오류 64

메모리 부족 오류 64

기본 폴더, 파일 및 보고서 생성되지 않음 64

마이그레이션 내보내기 단계가 매우 느림 65

보고Cisco TAC에 문제 65



서론

이 가이드에서는 Cisco Secure ACS-Cisco ISE 마이그레이션 툴을 사용하여 데이터를 Cisco ACS(Secure Access Control Server), 릴리스 5.5 또는 5.6 Cisco ISE(Identity Services Engine), 릴리스 1.42.0로 마이그레이션하는 프로세스에 대해 설명합니다.



참고 각 Cisco Secure ACS 또는 Cisco ISE 릴리스에서 동적으로 변경되는 기능 상의 차이로 인해, 모든 Cisco Secure ACS 데이터를 Cisco ISE로 마이그레이션할 수 있는 것은 아닙니다. 마이그레이션 툴은 지원되지 않는 개체의 전체 목록을 제공합니다.

- 목적, ix 페이지
- 대상, x 페이지
- 문서 명명 규칙, x 페이지
- 관련 설명서, xi 페이지

목적

이 마이그레이션 가이드는 다음 정보가 포함된 Cisco ISE(Identity Services Engine), 릴리스 1.4 설명서 집합의 일부입니다.

- Cisco Secure ACS-Cisco ISE 마이그레이션 툴 설치 요구 사항, 전제 조건 및 데이터 마이그레이션 지침.
- 데이터를 Cisco Secure ACS, 릴리스 5.5/5.6 데이터베이스에서 Cisco ISE, 릴리스 1.4 어플라이언스로 마이그레이션하기 위한 단계별 절차.
- 마이그레이션할 수 있고 마이그레이션할 수 없는 Cisco Secure ACS, 릴리스 5.5/5.6 데이터 항목의 목록입니다.
- 이전 버전의 Cisco Secure ACS, 릴리스 3.x 및 릴리스 4.x에 필요한 업그레이드 및 마이그레이션 절차를 정의하는 Cisco Secure ACS 설명서에 대한 참조 링크.

대상

이 마이그레이션 가이드는 Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE 마이그레이션 툴)을 사용하여 기존 Cisco Secure ACS, 릴리스 5.5/5.6 데이터베이스 정보를 Cisco ISE, 릴리스 1.4 어플라이언스로 마이그레이션하는 네트워크 관리자를 대상으로 합니다.

문서 명명 규칙

이 설명서는 다음과 같은 명명 규칙을 사용합니다.

명명 규칙	설명
굵은 글꼴	명령과 키워드 및 사용자 입력 텍스트는 굵은 글꼴로 표시됩니다.
기울임꼴 글꼴	문서 제목, 새로운 용어 또는 강조된 용어 및 사용자가 값을 제공해야 하는 인수는 기울임꼴 글꼴로 표시합니다.
[x]	대괄호로 묶인 키워드 또는 인수는 선택적 요소입니다.
[]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에 표시됩니다.
	파이프라는 세로 선은 키워드나 인수 집합 내 선택을 나타냅니다.
[x y]	선택적 대체 키워드는 대괄호로 묶어 세로 선으로 구분합니다.
{x y}	필수 대체 키워드는 중괄호로 묶어 세로 선으로 구분합니다.
[x {y z}]	중첩된 대괄호 또는 중괄호 집합은 선택 요소 또는 필수 요소 내의 선택적 선택 항목 또는 필수 선택 항목을 나타냅니다. 대괄호 안의 중괄호 및 세로 막대는 선택 요소 내의 필수 선택 항목을 나타냅니다.
Courier 글꼴	고정 너비, 고정 폭 글꼴로 된 화면 표시, 프롬프트 및 스크립트의 예.
굵은 Courier 글꼴	입력하는 정보의 예.

명명 규칙	설명
<>	비인쇄 문자(예, 비밀번호)는 꺾쇠 괄호 안에 표시됩니다.
!#	코드 라인 시작 부분에 있는 느낌표(!) 또는 우물 정자(#)는 코멘트 행을 나타냅니다.

독자 알림 명명 규칙

이 문서에서는 독자 알림에 대한 다음의 명명 규칙을 사용합니다.



참고 독자가 주목해야 하는 내용을 의미합니다. 참고 사항에는 해당 설명서에서 다루지 않는 자료에 대한 유용한 제안이나 참조가 포함됩니다.



팁 다음 정보가 문제를 해결하는 데 도움이 되거나 유용한 정보가 될 수 있다는 것을 의미합니다.



주의 독자가 유의해야 한다는 것을 의미합니다. 이러한 상황에서는 장비가 손상되거나 데이터가 손실될 수 있다는 내용이 포함됩니다.



간편한 방법

설명한 작업이 시간을 절약한다는 것을 의미합니다. 단락에 설명된 작업을 수행하면, 시간을 절약할 수 있습니다.



경고!

독자에게 경고하는 것을 의미합니다. 이러한 상황에서는 신체 상해를 입을 수 있는 작업을 수행해야 할 수 있습니다.

관련 설명서

릴리스별 문서

Cisco ISE(Identity Services Engine)에 대한 일반 제품 정보는 <http://www.cisco.com/go/ise>에서 확인할 수 있습니다. 최종 사용자 설명서는 <http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html>의 Cisco.com에서 확인할 수 있습니다.

표 1: Cisco ISE(Identity Services Engine) 제품 설명서

Cisco ISE(Identity Services Engine), 릴리스 1.4의 릴리스 노트	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
Cisco ISE(Identity Services Engine) 네트워크 구성 요소 호환성, 릴리스 1.4	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
Cisco ISE(Identity Services Engine) 사용 설명서, 릴리스 1.4 Cisco ISE(Identity Services Engine) 후원 기관 포털 사용 설명서, 릴리스 1.4	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco ISE(Identity Services Engine) 하드웨어 설치 설명서, 릴리스 1.4 Cisco ISE(Identity Services Engine) 업그레이드 설명서, 릴리스 1.4 Cisco ISE(Identity Services Engine), 릴리스 1.4 마이그레이션 툴 설명서 Cisco ISE(Identity Services Engine) 3400 시리즈 어플라이언스 및 Cisco 3400 보안 액세스 제어 시스템에 대한 규정 준수 및 안전 정보	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco ISE(Identity Services Engine) CLI Reference Guide, 릴리스 1.4 Cisco ISE(Identity Services Engine) API Reference Guide, 릴리스 1.4	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco ISE(Identity Services Engine) In-Box 설명서 및 중국 RoHS 포인터 카드	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

플랫폼별 문서

다른 플랫폼별 문서에 대한 링크를 다음 위치에서 확인할 수 있습니다.

표 2: 특정 문서 플랫폼

Cisco ISE	http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html
Cisco NAC Appliance	http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
Cisco NAC Guest Server	http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
Cisco Secure Access Control System	http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
Cisco UCS C-Series Servers	http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html



1 장

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 1.3 의 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 1.4 의 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 3: 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 4: 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 5: 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 매핑](#)

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 툴은 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.



2 장

Cisco ISE에 대한 Cisco Secure ACS

이 장에서는 Cisco Secure ACS, 릴리스 5.5, 5.6, 데이터베이스에서 Cisco ISE, 릴리스 1.4 시스템으로의 데이터 마이그레이션에 사용되는 Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE로 마이그레이션 툴)에 대한 정보를 제공합니다.

- [Cisco Secure ACS에서 Cisco ISE로의 데이터 마이그레이션, 17 페이지](#)
- [Cisco Secure ACS-Cisco ISE 마이그레이션 툴, 18 페이지](#)
- [소프트웨어 요구 사항, 20 페이지](#)

Cisco Secure ACS에서 Cisco ISE로의 데이터 마이그레이션

Cisco Secure ACS-Cisco ISE 마이그레이션 툴을 사용하여 직접 마이그레이션하는 유일한 지원 프로세스는 Cisco Secure ACS, 릴리스 5.5 또는 5.6 Cisco ISE, 릴리스 1.4 시스템으로 업그레이드하는 것입니다.

마이그레이션 프로세스에는 3가지 단계가 있습니다.

1. 데이터베이스에서 Cisco Secure ACS, 릴리스 5.5 또는 5.6 데이터 내보내기
2. 마이그레이션 툴을 사용하여 데이터 유지
3. Cisco ISE, 릴리스 1.4 시스템으로 지속형 데이터 가져오기

데이터 마이그레이션 시간 예상

Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE 마이그레이션 툴)을 약 20시간 동안 실행하여 10,000개의 디바이스, 25,000명의 사용자, 100,000개의 호스트, 100개의 ID 그룹, 420개의 dACL(downloadable Access Control List), 320개의 권한 부여 프로파일, 6개의 디바이스 계층 구조 및 20개의 NDG(Network Device Group)를 마이그레이션할 수 있습니다. .

마이그레이션 툴을 약 52시간 동안 실행하여, 다음 컨피그레이션을 마이그레이션할 수 있습니다.

- 4개의 LDAP
- 1,000개의 ID 그룹
- 500개의 사용자 ID 그룹

- 20개의 네트워크 디바이스 위치
- 100개의 네트워크 디바이스 그룹
- 25개의 액세스 서비스
- 50개의 SSP
- 600개의 dACL(downloadable Access Control List)
- 320개의 권한 부여 규칙
- 600개의 권한 부여 프로파일(정책 집합 포함 또는 제외)
- 20 개 명령 집합 및 셸 프로파일(각 명령에 100개의 명령 포함)
- 40개의 정책 집합(최대 규칙으로 제한)
- 20개의 맞춤형 사용자 사전
- 100,000개의 네트워크 디바이스
- 300,000명의 사용자
- 150,000개의 호스트

Cisco Secure ACS-Cisco ISE 마이그레이션 툴

마이그레이션 툴을 실행하기 전에, Cisco ISE, 릴리스 1.4으로 업그레이드하고 Cisco Secure ACS, 릴리스 5.5 이상에 대한 최신 패치를 설치했는지 확인합니다.

마이그레이션 툴을 사용하면, Cisco Secure ACS 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4으로 데이터를 마이그레이션할 수 있습니다. 이 툴의 설계는 기본 하드웨어 플랫폼과 시스템, 데이터베이스 및 데이터 체계의 차이로 인해 발생하는 고유한 마이그레이션 문제를 해결합니다.

마이그레이션 툴은 Linux 기반 및 Windows 기반 시스템에서 실행됩니다. 마이그레이션 툴은 Cisco Secure ACS 데이터 파일을 내보내고, 데이터를 분석하며, 데이터를 Cisco ISE, 릴리스 1.4에서 사용할 수 있는 형식으로 가져오는 데 필요한 필수 데이터 수정 작업을 수행합니다.

- 마이그레이션 툴에는 최소한의 사용자 상호 작용 및 전체 컨피그레이션 데이터 집합이 필요합니다.
- 마이그레이션 툴은 지원되지 않는 개체의 전체 목록을 제공합니다.

Cisco Secure ACS, 릴리스 5.5 이상 및 Cisco ISE, 릴리스 1.4 애플리케이션은 동일한 유형의 물리적 하드웨어에서 실행되거나 실행되지 않을 수 있습니다. 마이그레이션 툴은 Cisco Secure ACS PI(Programmatic Interface) 및 Cisco ISE REST(Representational State Transfer) API(Application Programming Interface)를 사용합니다. Cisco Secure ACS PI 및 Cisco ISE REST API를 사용하면, Cisco Secure ACS 및 Cisco ISE 애플리케이션을 지원하는 하드웨어 플랫폼 또는 VMware 서버에서 실행할 수 있습니다. Cisco Secure ACS는 닫힌 어플라이언스로 간주되므로, Cisco ACS 어플라이언스에서 직접 마이그레이션 툴을 실행할 수 없습니다. 그 대신 Cisco Secure ACS PI가 표준화된 형식으로 컨피그레이션 데이터를 읽고 반환합니다. Cisco ISE REST API는 검증을 수행하고, 내보낸 Cisco Secure ACS 데이터를 표준화하여 Cisco ISE 소프트웨어가 사용할 수 있는 형식으로 유지합니다.



참고 AD 그룹의 SID 값은 마이그레이션 툴 프로세스의 일부이며, Cisco Secure ACS, 릴리스 5.x에서 Cisco ISE, 릴리스 2.0 이상으로 마이그레이션되지 않습니다. 외부 그룹 이름만 마이그레이션됩니다. 마이그레이션 프로세스가 완료되면, Cisco ISE에서 AD에 조인하고 AD 그룹 탭에서 사용 가능한 SID 값 업데이트 버튼을 클릭하여 그룹 SID를 업데이트해야 합니다. AD 그룹 SID를 수동으로 업데이트할 수 있을 때까지, 정책 조건이 AD 외부 그룹을 생성한 경우에 권한 부여 규칙이 일치하지 않음

마이그레이션을 시작하는 데 필요한 최소 데이터 컨피그레이션

애플리케이션이 전체 컨피그레이션 항목 집합을 마이그레이션하기 전에, 마이그레이션 프로세스를 시작할 때 최소한의 컨피그레이션 데이터가 필요합니다. 그러나 마이그레이션이 진행될 때, 일부 데이터는 두 애플리케이션 사이에서 자동으로 매핑되지 않을 수 있습니다. 마이그레이션을 처리하는 관리자에게 이 유형의 데이터를 알리며, 마이그레이션이 완료되기 전에 해결해야 합니다.

마이그레이션 툴로 데이터 마이그레이션 모니터링

마이그레이션이 진행되는 동안, 활동의 진행 상황과 함께 실시간 마이그레이션 상태를 모니터링할 수 있습니다. 문제 해결의 경우, 마이그레이션 툴에서 자세한 로그를 확인하여 액세스할 수 있습니다.

마이그레이션 툴에서 마이그레이션을 계속하기 위한 Checkpoint

내보내기 및 가져오기 작업을 개별적으로 또는 순서대로 수행할 수 있습니다. 내보내기 및 가져오기는 시간이 오래 걸릴 수 있으며, 마이그레이션되는 데이터의 양에 따라 달라집니다. 따라서 마이그레이션 툴은 수행 중인 활동의 상태와 함께 체크포인트를 주기적으로 표시합니다. 장애 발생 시 체크포인트에서 마이그레이션 프로세스를 재시작할 수 있습니다.

Cisco Secure ACS에서 컨피그레이션 데이터 내보내기

Cisco Secure ACS 시스템에 의해 인증되고 데이터 내보내기를 요청한 후, 내보내기 프로세스를 시작할 수 있습니다.

Cisco Secure ACS에서 Cisco ISE로 직접 업그레이드는 지원되지 않습니다. Cisco Secure ACS, 릴리스 5.5 또는 5.6 소프트웨어를 제거하고 Cisco ISE 릴리스 1.4 소프트웨어를 사용하여 물리적 하드웨어의 이미지를 재설치하려는 경우에는 마이그레이션 툴이 도움이 됩니다.

구성 데이터 분석

내보내기 단계 중에 마이그레이션 툴은 데이터를 읽고 분석하여 Cisco ISE 시스템에서 해당 데이터를 생성할 수 있는지 확인합니다. Cisco Secure ACS 및 Cisco ISE 정책 모델이 동일하지 않으므로, 일부 데이터가 Cisco ISE에서 지원되지 않을 수 있습니다. 마이그레이션 툴은 내보내기 단계가 끝날 때 관리자의 개입이 필요할 수 있는 데이터 문제를 보고합니다.

데이터 지속성

마이그레이션 툴은 재이미지 프로세스가 완료되는 동안 및 가져오기 단계가 시작되기 전에 Cisco Secure ACS 데이터를 유지합니다.

Cisco ISE로 컨피그레이션 데이터 가져오기

이 단계에서 마이그레이션 툴은 컨피그레이션 데이터를 Cisco ISE로 가져옵니다.

소프트웨어 요구 사항

표 6: Cisco Secure ACS-Cisco ISE로 마이그레이션 툴의 소프트웨어 요구 사항

운영 체제	마이그레이션 툴은 Windows 및 Linux 시스템에서 실행됩니다. 시스템에 JAVA가 설치되어 있어야 합니다.
최소 디스크 공간	필요한 최소 디스크 공간은 1GB입니다. 이 공간은 마이그레이션 툴을 설치하기 위해 또한 마이그레이션 툴이 마이그레이션 된 데이터를 저장하고 보고서와 로그를 생성하기 때문에 필요합니다.
최소 RAM	필요한 최소 RAM은 2GB입니다. 사용자 약 300,000명, 호스트 50,000개, 네트워크 디바이스 50,000개인 경우, 최소 2GB의 RAM을 사용하는 것이 좋습니다.



3 장

데이터 마이그레이션 원칙

이 장에서는 단일 어플라이언스에 구축하거나 Cisco ISE, 릴리스 1.3로 분산 구축할 때 Cisco Secure ACS, 릴리스 5.5, 5.6, 또는 5.8 데이터 마이그레이션을 설명합니다.

- [Data Migration and Deployment Scenarios, 21 페이지](#)
- [Cisco Secure ACS 릴리스 5.5 또는 5.6 마이그레이션 준비, 23 페이지](#)
- [정책 서비스 마이그레이션 지침, 23 페이지](#)
- [정책별 서비스 마이그레이션 지침, 24 페이지](#)
- [Cisco Secure ACS 정책 규칙 마이그레이션 지침, 25 페이지](#)
- [지원되지 않는 규칙 요소, 25 페이지](#)

Data Migration and Deployment Scenarios

Cisco Secure ACS 및 Cisco ISE는 서로 다른 하드웨어 플랫폼에 있으며, 운영 체제, 데이터베이스 및 정보 모델이 서로 다릅니다. 따라서 Cisco Secure ACS에서 Cisco ISE로 표준 업그레이드를 수행할 수 없습니다. 그 대신 마이그레이션 툴은 Cisco Secure ACS에서 데이터를 읽고 Cisco ISE에서 해당 데이터를 생성합니다.

마이그레이션 단일 **Cisco Secure ACS Appliance**에서 데이터

시작하기 전에

Cisco Secure ACS, 릴리스 5.5 이상의 데이터를 Cisco ISE, 릴리스 1.4으로 마이그레이션 할 준비가 되면, 독립형 Cisco ISE 노드에 대한 데이터인지 확인합니다. 마이그레이션이 성공적으로 완료되면, 모든 구축 컨피그레이션을 시작할 수 있습니다(예, 관리자 ISE 및 정책 서비스 ISE 페르소나 설정).

Cisco ISE 소프트웨어를 지원되는 하드웨어 어플라이언스에 "완전히" 새로 설치하는 경우, 마이그레이션 가져오기 단계를 수행해야 합니다. 지원되는 하드웨어 어플라이언스 목록은 *Cisco ISE(Identity Services Engine)* 하드웨어 설치 가이드, 릴리스 1.4을 참조하십시오.

사용자 환경에 단일 Cisco Secure ACS 어플라이언스가 있거나 분산된 설정이 아닌 여러 Cisco Secure ACS 어플라이언스가 있는 경우, Cisco Secure ACS 어플라이언스에 대해 마이그레이션 툴을 실행하십시오.

Cisco Secure ACS와 Cisco ISE가 CSACS-1121 어플라이언스라는 동일한 하드웨어를 사용하는 경우, 마이그레이션 툴과 다음 마이그레이션 절차를 사용할 수 있습니다.

- 단계 1 독립형 Windows 또는 Linux 컴퓨터에 마이그레이션 툴을 설치합니다.
- 단계 2 Cisco Secure ACS, 릴리스 5.5 이상의 데이터를 Cisco Secure ACS-1121 하드웨어 어플라이언스에서 데이터베이스가 있는 보안 외부 서버로 내보냅니다.
- 단계 3 Cisco Secure ACS 데이터를 백업합니다.
- 단계 4 Cisco ISE 릴리스 1.4 소프트웨어로 지원 Cisco ISE 어플라이언스와 동일한 물리적 하드웨어를 사용하는 Cisco Secure ACS-1121 하드웨어 어플라이언스를 다시 이미지화합니다.
- 단계 5 변환된 Cisco Secure ACS 데이터를 보안 외부 서버에서 Cisco ISE로 가져옵니다.

분산 환경에서 데이터 마이그레이션

시작하기 전에

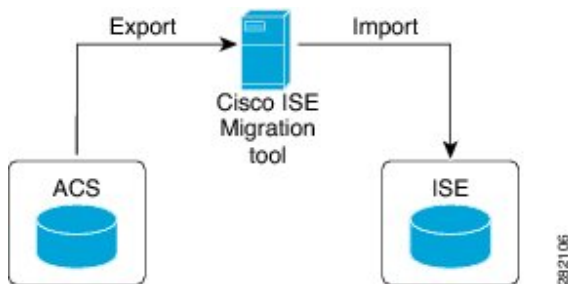
대규모 내부 데이터베이스가 있는 경우, 여러 보조 어플라이언스에 연결된 기본 어플라이언스가 아닌 독립형 기본 어플라이언스에서 마이그레이션을 실행하는 것이 좋습니다. 마이그레이션 프로세스가 완료되면 모든 보조 어플라이언스를 등록 할 수 있습니다.

분산 환경에는 기본 Cisco Secure ACS 어플라이언스 및 기본 어플라이언스와 상호 운용되는 하나 이상의 보조 Cisco Secure ACS 어플라이언스가 있습니다.

분산 환경에서 Cisco Secure ACS를 실행하는 경우, 다음을 수행해야 합니다.

- 단계 1 기본 Cisco Secure ACS 어플라이언스를 백업하고 마이그레이션 컴퓨터에서 복원합니다.
- 단계 2 기본 Cisco Secure ACS 어플라이언스에 대해 마이그레이션 툴을 실행합니다.

그림 2: 다른 어플라이언스에 설치된 **Cisco Secure ACS** 및 **Cisco ISE**



Cisco Secure ACS 릴리스 5.5 또는 5.6 마이그레이션 준비

Cisco Secure ACS에서 성공적으로 마이그레이션한 후에는 단순 모드로 변경하지 않는 것이 좋습니다. Cisco ISE에서 마이그레이션된 모든 정책이 손실될 수 있기 때문입니다. 마이그레이션된 정책은 검색할 수 없지만, Simple Mode(단순 모드)에서 Policy Set(정책 집합) 모드로 전환할 수 있습니다.

Cisco Secure ACS 데이터를 Cisco ISE로 마이그레이션하기 전에, 다음 사항을 고려해야 합니다.

- Cisco ISE, 릴리스 1.4의 정책 설정 모드에서만 Cisco Secure ACS, 릴리스 5.5 이상의 데이터를 마이그레이션하십시오.
- Cisco ISE 릴리스 1.4을 새로 설치하여 마이그레이션합니다. Cisco ISE에서 **Administration(관리)** > **System(시스템)** > **Settings(설정)** > **Policy Sets(정책 집합)**를 선택합니다.
- SSP(Service Selection Policy)에서 활성화된 규칙 당 하나의 정책 집합을 생성하고, SSP 규칙의 순서에 따라 순서를 지정합니다.



참고 SSP 기본 규칙의 결과인 서비스는 Cisco ISE 릴리스 1.4의 기본 정책 집합이 됩니다. 마이그레이션 프로세스에서 생성된 모든 정책 집합의 경우 첫 번째 일치 정책 집합은 일치 유형입니다.

정책 서비스 마이그레이션 지침

정책 서비스를 Cisco Secure ACS에서 Cisco ISE로 마이그레이션하는 동안, 다음 사항에 유의하십시오.

- SSP(Service Selection Policies)에 Cisco Secure ACS, 릴리스 5.5 이상에서 비활성화되거나 모니터링되는 SSP 규칙이 포함되어 있으면, Cisco ISE로 마이그레이션되지 않습니다.
- SSP(Service Selection Policy)에 Cisco Secure ACS, 릴리스 5.5 이상에서 활성화된 SSP 규칙이 포함된 경우:
 - 디바이스 관리 서비스를 요청합니다. Cisco ISE로 마이그레이션되지 않습니다. (Cisco ISE는 디바이스 관리를 지원하지 않습니다).
 - Group Mapping(그룹 매핑)정책이 포함된 서비스를 요청합니다. 이 서비스는 Cisco ISE로 마이그레이션되지 않습니다. Cisco ISE는 Group Mapping(그룹 매핑) 정책을 지원하지 않습니다.
 - 서비스를 요청하고 해당 ID 정책에 RADIUS ID 서버를 생성하는 규칙이 포함되어 있으면, Cisco ISE로 마이그레이션되지 않습니다(Cisco ISE는 RADIUS ID 서버를 인증에 사용하는 방식이 다릅니다).
 - Cisco ISE에서 지원되지 않는 특성 또는 정책 요소를 사용하는 정책이 있는 서비스를 요청합니다. 이 서비스는 Cisco ISE로 마이그레이션되지 않습니다.

정책별 서비스 마이그레이션 지침

Cisco ISE, 릴리스 1.32.1의 정책 집합 모드에서만 Cisco Secure ACS 데이터를 마이그레이션하므로, 이 섹션에서는 Cisco Secure ACS, 릴리스 5.5 또는 Cisco ISE 1.4로 마이그레이션하는 각 정책 서비스의 변경 사항에 대해 설명합니다.

Cisco Secure ACS 서비스 선택 정책 기본 규칙이 Cisco ISE 기본 정책 설정과 일치 함

Cisco ISE에서 서비스 이름으로 정책 집합을 생성할 수 있습니다. 정책 설정이 Cisco Secure ACS, 릴리스 5.5 또는 5.6 SSP 기본 규칙의 결과인 서비스와 일치하는 경우, 정책 집합은 Cisco ISE 릴리스 1.4의 기본 정책 집합이 됩니다. Cisco Secure ACS, 릴리스 5.5 또는 5.6 SSP 규칙의 조건은 Cisco ISE, 릴리스 1.4에서 정책 집합의 입력 조건이 됩니다. Cisco ISE, 릴리스 1.4 기본 정책 집합의 경우에는 입력 조건이 필요하지 않습니다.

Cisco Secure ACS DenyAccess Service-Cisco ISE 인증 및 권한 부여 정책 마이그레이션

Cisco Secure ACS, 릴리스 5.5 또는 5.6 DenyAccess 서비스를 Cisco ISE, 릴리스 1.4로 변환하면, 인증 및 권한 부여 정책이 다음으로 변경됩니다.

- 인증 정책에는 허용되는 프로토콜에 대한 기본 네트워크 액세스 및 ID 소스에 대한 DenyAccess로 설정된 기본 외부 규칙만 있습니다.
- 권한 부여 정책에는 DenyAccess(표준 권한)로 설정된 기본 규칙만 있습니다.

Cisco Secure ACS 서비스 ID 정책-정책 집합의 Cisco ISE 인증 정책 마이그레이션

Cisco Secure ACS, 릴리스 5.5 또는 5.6 서비스 ID 정책을 Cisco ISE, 릴리스 1.4에 설정된 정책의 인증 정책으로 변환하려면, 다음을 수행합니다.

- 활성화된 단일 외부 규칙이 있는 인증 정책을 생성합니다.
- Device:Location가 All Locations(모든 위치)로 시작하므로, 외부 규칙의 조건을 지정합니다(항상 일치하는 조건임).
- 기본 외부 규칙의 결과를 Allowed Protocol(허용되는 프로토콜)의 경우에는 Default Network Access(기본 네트워크 액세스)로 설정하고 ID 소스의 경우에는 DenyAccess로 설정합니다.

외부 규칙의 결과는 관련 서비스의 Allowed Protocol(허용되는 프로토콜)입니다. 인증 정책의 내부 규칙은 관련 ID 정책의 규칙입니다. 인증 정책의 내부 규칙 순서는 관련 ID 정책의 규칙 순서와 동일합니다. 인증 정책의 내부 규칙 상태(활성화됨, 비활성화됨 또는 모니터링됨)는 관련 ID 정책의 규칙 상태를 따릅니다.

Cisco Secure ACS Service Authorization Policy-정책 집합의 Cisco ISE 권한 부여 정책 마이그레이션

Cisco Secure ACS, 릴리스 5.5 또는 5.6 서비스의 권한 부여 정책을 Cisco ISE, 릴리스 1.4에서 정책 집합의 권한 부여 정책으로 변환하려는 경우:

- 정책 집합 Local Exception Authorization(로컬 예외 권한 부여) 정책의 규칙은 관련 서비스의 Exception Authorization(예외 권한 부여) 정책의 규칙입니다.

- 정책 집합 Authorization(권한 부여) 정책의 규칙은 관련 서비스의 Authorization(권한 부여) 정책의 규칙입니다.
- Local Exception Authorization(로컬 예외 권한 부여) 정책 및 Authorization(권한 부여) 정책에 설정된 정책의 규칙 순서는 관련 서비스의 Local Exception Authorization(로컬 예외 권한 부여) 정책 및 권한 부여 정책의 규칙 순서를 따릅니다.
- 정책 설정 Local Exception Authorization(로컬 예외 권한 부여) 정책 및 Authorization(권한 부여) 정책의 규칙 상태(활성화 됨, 비활성화 됨, 모니터링 됨)는 관련 서비스의 Local Exception Authorization(로컬 예외 권한 부여) 정책 및 Authorization(권한 부여) 정책의 규칙 상태를 따릅니다.

Cisco Secure ACS 정책 규칙 마이그레이션 지침

규칙을 마이그레이션할 수 없는 경우, 보안 측면과 데이터 무결성 때문에 정책 모델 전체를 마이그레이션할 수 없습니다. Policy Gap Analysis Report(정책 간격 분석 보고서)에서 문제가 있는 규칙의 상세 정보를 볼 수 있습니다. 지원되지 않는 규칙을 수정하거나 삭제하지 않으면, 정책이 Cisco ISE로 마이그레이션되지 않습니다.

일반적으로 Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4으로 데이터를 마이그레이션하는 동안 이러한 규칙을 고려해야 합니다.

- 특수 문자가 포함된 개체는 마이그레이션되지 않습니다.
- 열거형 유형의 속성(RADIUS, VSA, ID 및 호스트)은 허용되는 값을 가진 정수로 마이그레이션됩니다.
- (속성 데이터 유형과 관계없이) 모든 엔드포인트 속성은 문자열 데이터 유형으로 마이그레이션됩니다.
- RADIUS 속성 및 VSA 값은 필터링하여 Cisco ISE 로그에 추가할 수 없습니다.

지원되지 않는 규칙 요소

Cisco Secure ACS와 Cisco ISE는 서로 다른 정책 모델을 기반으로 하며, Cisco ISE로 마이그레이션할 때 Cisco Secure ACS 데이터 간에 차이가 있습니다. Cisco Secure ACS 및 Cisco ISE 릴리스 버전이 변경되면, 다음과 같은 이유로 모든 Cisco Secure ACS 정책 및 규칙을 마이그레이션할 수 있는 것은 아닙니다.

- 정책에서 사용되는 지원되지 않는 속성
- 지원되지 않는 AND/OR 조건 구조(주로 복잡한 조건이 구성되는 경우)
- 지원되지 않는 연산자

표 7: 지원되지 않는 규칙 요소

규칙 요소	지원 상태	설명
날짜 및 시간	지원되지 않음	매주 반복 설정이 있는 권한 부여 정책의 날짜 및 시간 조건은 Cisco ISE로 마이그레이션되지 않습니다. 따라서 규칙도 마이그레이션되지 않습니다.
Date and Time(날짜 및 시간)	지원되지 않음	인증 정책의 날짜 및 시간 조건은 Cisco ISE로 마이그레이션되지 않습니다. 따라서 규칙도 마이그레이션되지 않습니다.
In	부분적으로 지원됨	"In" 연산자는 계층 구조에 사용되며, "Is"는 문자열 유형에만 사용됩니다. 이는 "STARTS_WITH"를 사용하여 변환할 수 있습니다.
Not In	부분적으로 지원됨	"Not In" 연산자는 계층 구조에 사용되며, "Is"는 문자열 유형에만 사용됩니다. 이는 "Matches"를 사용하여 변환할 수 있습니다.
Contains Any	지원되지 않음	"Contains Any" 연산자는 Active Directory 및 LDAP(Lightweight Directory Access Protocol)와 같은 외부 그룹에 대해서만 사용됩니다.
Contains All	지원되지 않음	"Contains All" 연산자는 Active Directory 및 LDAP(Lightweight Directory Access Protocol)와 같은 외부 그룹 전용입니다.

규칙 요소	지원 상태	설명
논리식의 조합	지원되지 않음	<p>조건에서 이러한 연산자를 사용하는 규칙은 마이그레이션되지 않습니다.</p> <ul style="list-style-type: none"> • (a b) && c 같이 a b c ... 및/또는 a && b && c && ... 이외의 논리식이 있는 다른 복합 조건을 포함하는 인증 정책. • && b && c && 이외의 로컬식이 있는 다른 복합 조건을 포함하는 권한 부여 정책은 규칙 조건의 일부로 마이그레이션되지 않습니다. 이를 해결하기 위해, 일부 고급 논리식에 대해 라이브러리 복합 조건을 수동으로 사용할 수 있습니다.
네트워크 조건	지원되지 않음	<p>네트워크 조건만 포함하는 규칙은 마이그레이션되지 않습니다. 조건에 네트워크 조건 및 기타 지원되는 조건이 포함되는 경우, 네트워크 조건은 무시되며 규칙 조건의 일부로 마이그레이션되지 않습니다.</p>
사용자 속성	부분적으로 지원됨	<p>"String" 데이터 유형이 아닌 데이터 유형의 사용자 속성을 포함하는 조건이 포함된 규칙은 마이그레이션되지 않습니다.</p>
호스트 속성	지원되지 않음	<p>조건이 호스트 속성을 참조하는 경우, 인증이 실패합니다.</p> <p>호스트(엔드 포인트) 속성이 있는 조건을 포함하는 권한 부여 정책은 Cisco ISE 권한 부여 정책으로 마이그레이션되지 않습니다.</p>

규칙 요소	지원 상태	설명
TACACS+ 속성	지원되지 않음	Cisco ISE는 TACACS(Terminal Access Controller Access Control System)를 지원하지 않습니다. TACACS 속성을 사용하는 Cisco Secure SSP(Service Selection Policy) 규칙은 마이그레이션되지 않습니다.



4 장

마이그레이션 툴 설치

이 장에서는 Cisco Secure ACS-Cisco ISE 마이그레이션 툴을 설치하는 방법에 대한 지침을 제공합니다.

- [마이그레이션 툴 설치 지침, 29 페이지](#)
- [시스템 요구 사항, 30 페이지](#)
- [보안 문제, 30 페이지](#)
- [다운로드 Cisco ISE 관리자 포털에서 마이그레이션 툴 파일, 31 페이지](#)
- [Cisco Secure ACS-Cisco ISE 마이그레이션 툴 초기화, 31 페이지](#)

마이그레이션 툴 설치 지침

- 마이그레이션할 수 있는 환경인지 확인합니다. Cisco Secure ACS, 릴리스 5.5 이상 Windows 또는 Linux 소스 컴퓨터 외에, 이중 어플라이언스(분산형 구축에서 데이터 마이그레이션) 마이그레이션을 위한 데이터베이스가 있는 보안 외부 시스템을 구축해야 합니다.
- 단일 IP Address를 사용하여 Cisco Secure ACS, 릴리스 5.5 이상의 소스 컴퓨터를 설정했는지 확인합니다. 각 인터페이스에 여러 IP Address 별칭이 있는 경우, 마이그레이션 중에 마이그레이션 툴이 실패할 수 있습니다.
- Cisco Secure ACS에서 Cisco ISE로 마이그레이션이 동일한 어플라이언스에서 수행되는 경우 ACS 컨피그레이션 데이터를 백업해야 합니다.
- 다음 작업을 완료했는지 확인합니다.
 - 듀얼 어플라이언스 마이그레이션인 경우, 대상 컴퓨터에 Cisco ISE, 릴리스 1.4 소프트웨어를 설치한 것입니다.
 - 단일 어플라이언스 마이그레이션인 경우에는 Cisco ISE 릴리스 1.4 소프트웨어를 사용하여 어플라이언스 또는 가상 컴퓨터의 이미지를 재설치할 수 있습니다.
 - 적절한 모든 Cisco Secure ACS, 릴리스 5.5 이상과 Cisco ISE, 릴리스 1.4 자격 증명과 비밀번호가 있어야 합니다.
- 소스 컴퓨터와 보안 외부 시스템 사이에 네트워크 연결을 설정할 수 있는지 확인합니다.

시스템 요구 사항

표 8: 마이그레이션 컴퓨터의 시스템 요구 사항

플랫폼	요구 사항
Cisco Secure ACS, 릴리스 5.5 또는 5.6 소스 컴퓨터	Cisco Secure ACS 소스 컴퓨터가 단일 IP 주소를 갖도록 구성했는지 확인합니다.
Cisco ISE, 릴리스 1.4 대상 컴퓨터	Cisco ISE 대상 시스템에 2GB 이상의 RAM이 있는지 확인합니다.
Linux, Windows XP	Java JRE, 버전 1.6 이상 32비트를 설치합니다. 마이그레이션 시스템에 Java JRE를 설치하지 않으면, 마이그레이션 툴이 실행되지 않습니다.
64비트 Windows 7	Java JRE 버전 1.6 이상 64비트를 설치합니다. 마이그레이션 시스템에 Java JRE를 설치하지 않으면, 마이그레이션 툴이 실행되지 않습니다.
32비트 Windows:	Java JRE, 버전 1.6 이상 32비트를 설치합니다. 마이그레이션 시스템에 Java JRE를 설치하지 않으면, 마이그레이션 툴이 실행되지 않습니다.

보안 문제

마이그레이션 프로세스의 내보내기 단계에서는 가져오기 프로세스의 입력으로 사용되는 데이터 파일을 생성합니다. 데이터 파일의 내용은 비밀번호화되므로 직접 읽을 수 없습니다.

Cisco Secure ACS 데이터를 내보내고 Cisco ISE 어플라이언스로 성공적으로 가져오려면, Cisco Secure ACS, 릴리스 5.5 이상 및 Cisco ISE, 릴리스 1.4 관리자 사용자 이름 및 비밀번호를 알아야 합니다. 가져오기 유틸리티로 생성된 기록을 감사 로그에서 식별할 수 있도록 예약된 사용자 이름을 사용해야 합니다.

기본 Cisco Secure ACS 서버 및 Cisco ISE 서버의 IP 주소(또는 호스트네임) 및 관리자 자격 증명을 입력해야 합니다. 인증이 완료되면, 마이그레이션 툴이 업데이트와 유사한 형식으로 설정된 데이터 항목의 전체 집합을 마이그레이션합니다. 마이그레이션 툴을 실행하기 전에, ACS 서버에서 PI 인터페이스를 활성화하고 ISE 서버에서 ACS 마이그레이션 인터페이스를 활성화했는지 확인합니다.

다운로드 Cisco ISE 관리자 포털에서 마이그레이션 툴 파일

시작하기 전에

- config-bat 파일에서 마이그레이션 프로세스에 대한 Java Heap Size에 할당된 초기 메모리 양을 설정합니다. config.bat에서 힙 크기를 설정하기 위한 속성은 `_Xms = 64 and _Xmx = 1024`입니다(메모리는 각각 64 및 1024 메가 바이트).
- Cisco ISE 사용자 인터페이스 주소 표시 줄에서 최신 migTool.zip 파일을 다운로드 할 수 있습니다.
-

단계 1 Cisco Secure ACS 및 Cisco ISE 소프트웨어가 다른 어플라이언스에 설치되는 경우, Cisco ISE 사용자 인터페이스 주소 표시 줄에 다음 URL을 입력하여 마이그레이션 툴 파일을 다운로드합니다.

`https://<hostname-or-hostipaddress>/admin/migTool.zip`

단계 2 zip 파일의 콘텐츠를 풉니다. .zip 파일의 추출된 내용은 **config.bat** 및 **migration.bat** 파일을 포함하는 디렉토리 구조를 생성합니다.

단계 3 **config.bat** 파일을 편집하여 Java Heap Size에 할당된 초기 메모리 양을 설정합니다.

단계 4 **Save(저장)**를 클릭합니다.

Cisco Secure ACS-Cisco ISE 마이그레이션 툴 초기화

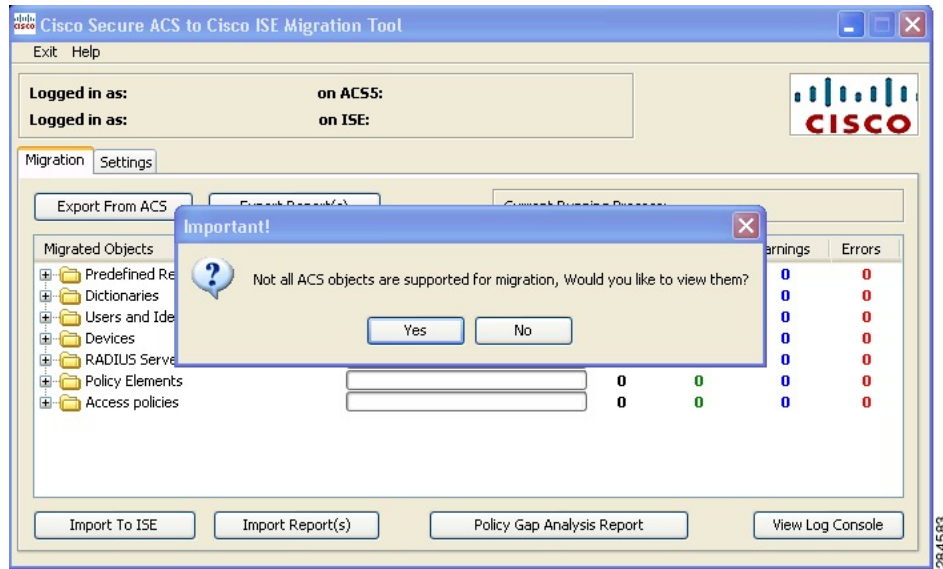
시작하기 전에

마이그레이션 툴은 반드시 Cisco ISE를 새로 설치한 후 또는 Cisco ISE 애플리케이션 컨피그레이션을 재설정하고 **application reset-config** 명령을 사용하여 Cisco ISE 데이터베이스를 지운 후에 실행해야 합니다. 따라서 마이그레이션 프로세스가 완료되기 전에 Cisco ISE FIPS 모드를 활성화해서는 안 됩니다.

마이그레이션 툴이 초기화되면 지원되지 않는 목록을 볼지 묻는 메시지 상자가 나타납니다. 마이그레이션 툴은 Cisco Secure ACS 개체의 하위 집합만 Cisco ISE로 마이그레이션할 수 있습니다. 이 도구는 마이그레이션할 수 없는 지원되지 않는 (또는 부분적으로 지원되는) 개체의 목록을 제공합니다. 또한 Cisco Secure ACS to Cisco ISE Migration Tool interface(Cisco Secure ACS-Cisco ISE 마이그레이션 툴 인터페이스)에서 **Help(도움말)> Unsupported Object Details(지원되지 않는 개체 상세정보)**를 선택하여 지원되지 않는 개체의 목록을 볼 수 있습니다.

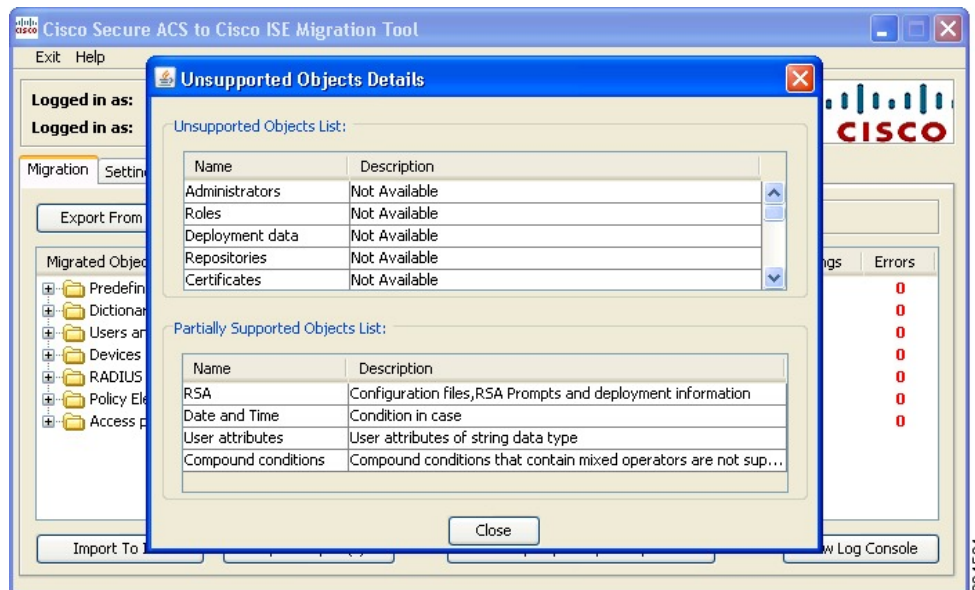
단계 1 마이그레이션 프로세스를 시작하려면, 마이그레이션을 클릭합니다.

그림 3: 지원되지 않는 개체에 대해 표시되는 메시지



단계 2 지원되지 않는 개체와 부분적으로 지원되는 개체의 목록을 표시하려면, **Yes(예)**를 클릭합니다.

그림 4: 지원되지 않는 개체 및 부분적으로 지원되는 개체 목록



단계 3 **Close(닫기)**를 클릭합니다.



5 장

영구 데이터 전송 절차

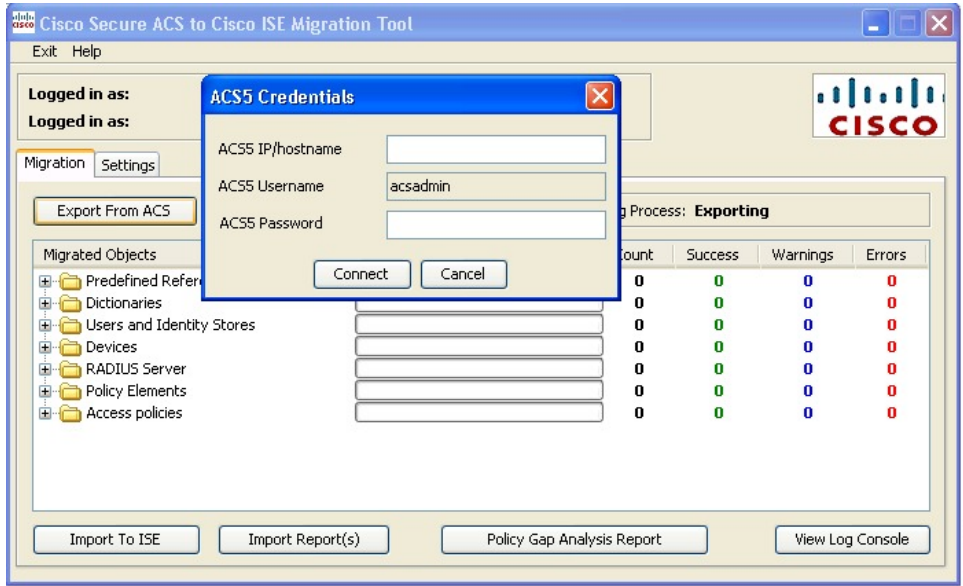
이 장에서는 마이그레이션 툴을 사용하여 Cisco Secure ACS, 릴리스 5.5, 5.6 데이터를 Cisco ISE, 릴리스 1.4으로 내보내고 가져오는 방법에 대해 설명합니다.

- 내보내기 Cisco Secure ACS에서 데이터, 33 페이지
- Cisco ISE와 Cisco Secure ACS 사이의 정책 차이 분석, 36 페이지
- 가져오기 Cisco ISE로 데이터, 38 페이지
- Cisco ISE에서 마이그레이션된 데이터 확인, 41 페이지

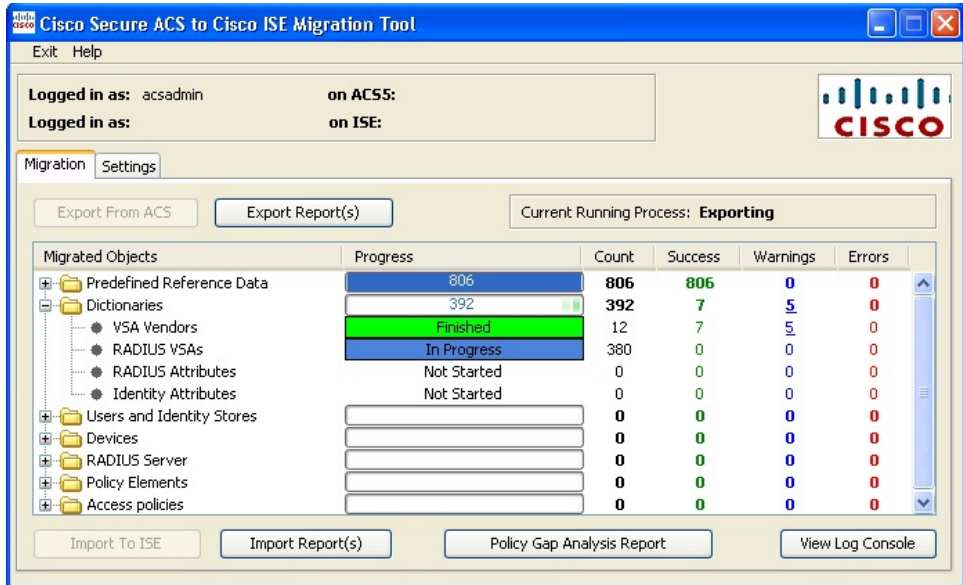
내보내기 Cisco Secure ACS에서 데이터

마이그레이션 툴을 시작한 후, 다음 단계를 완료하여 데이터를 Cisco Secure ACS에서 마이그레이션 툴로 내보냅니다.

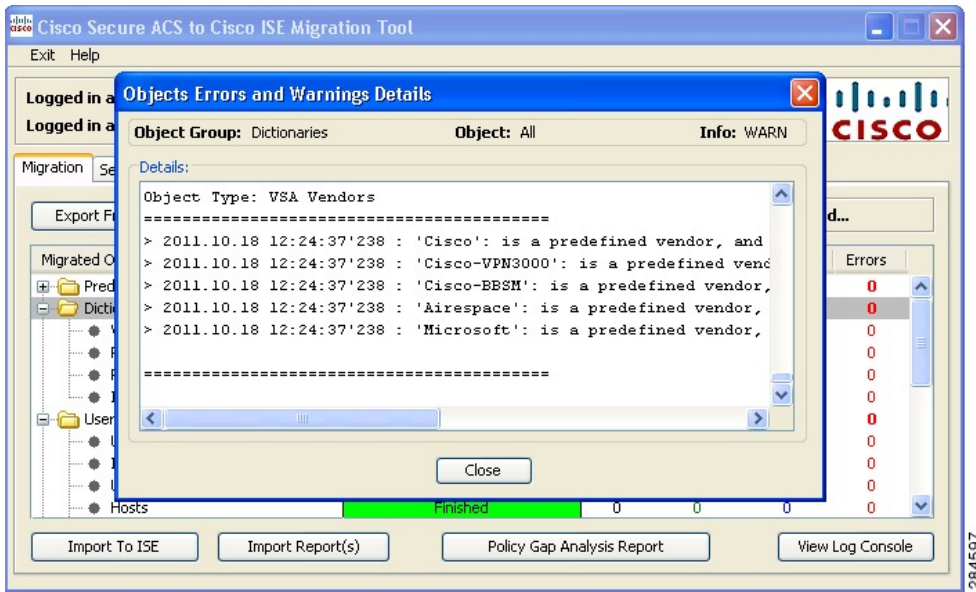
- 단계 1 Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE 마이그레이션 툴) 창에서 **Settings**(설정)를 클릭하여 마이그레이션에 사용할 수 있는 데이터 개체 목록을 표시합니다.
- 단계 2 (선택 사항) 마이그레이션을 수행하기 위해 종속성 처리를 설정할 필요가 없습니다. 종속성 데이터가 누락되는 경우, 내보낼 데이터 개체의 확인란을 선택하고 **Save**(저장)를 클릭합니다.
- 단계 3 Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE 마이그레이션 툴) 창에서 마이그레이션을 클릭한 다음 **Export From ACS**(ACS에서 내보내기)를 클릭합니다.
- 단계 4 IP 주소(또는 호스트네임)를 입력하고 비밀번호를 입력하고 ACS5 Credentials(ACS5 자격 증명)에서 **Connect**(연결)를 클릭합니다.



단계 5 Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE 마이그레이션 툴) 창에서 마이그레이션 프로세스를 모니터링하며, 이 창에는 성공한 개체 내보내기의 현재 수가 표시되고 경고 또는 오류를 트리거한 개체가 나열됩니다.

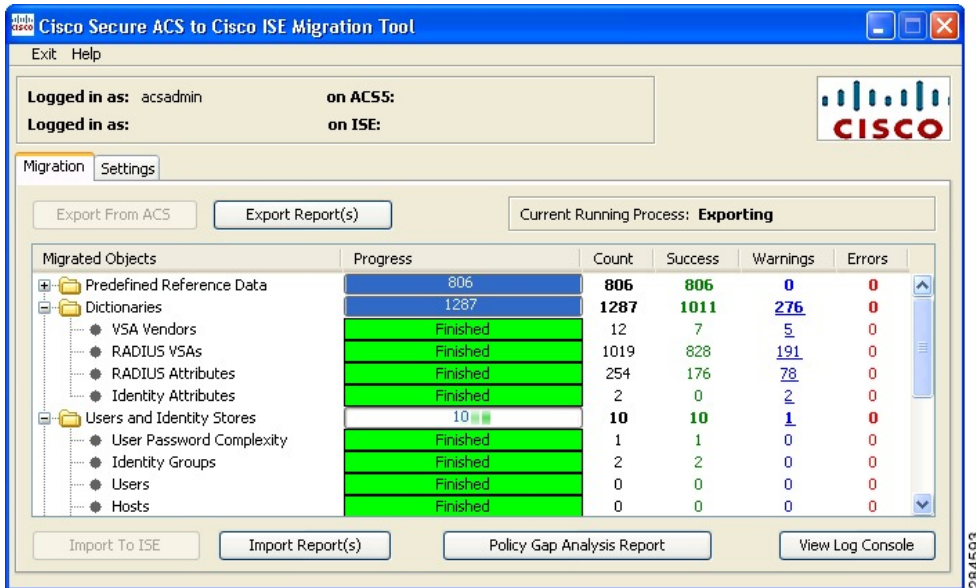


단계 6 내보내기 프로세스 중에 발생한 경고 또는 오류에 대한 자세한 정보를 얻으려면, 마이그레이션 탭의 경고 또는 오류 열에서 밑줄이 그어진 숫자를 클릭합니다. Object Errors and Warnings Details (개체 오류 및 경고 상세정보) 창에는 내보내기 중 경고 또는 오류 결과가 표시됩니다. 개체 그룹, 유형, 경고 또는 오류의 날짜와 시간을 제공합니다.

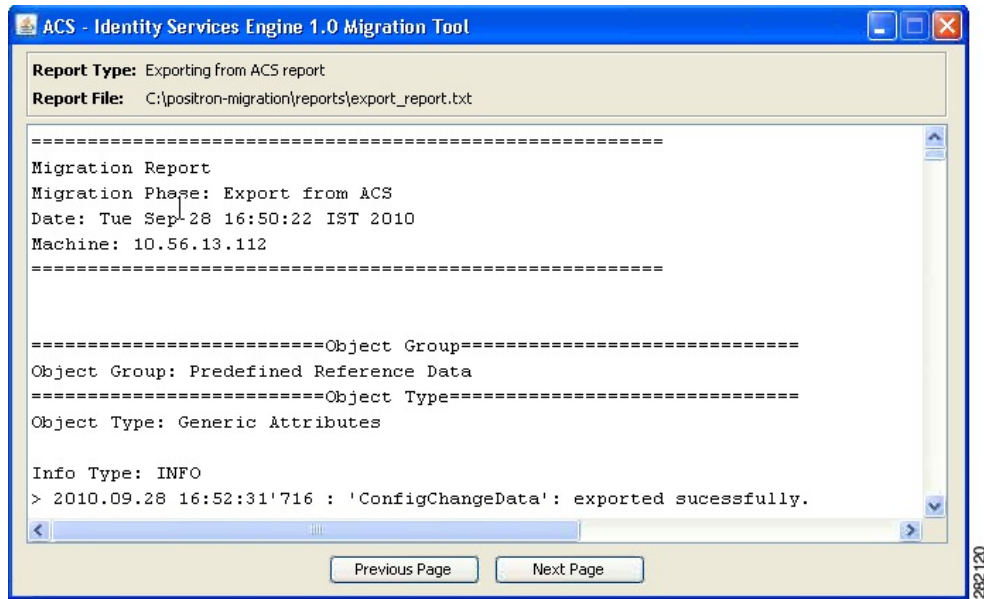


단계 7 스크롤하여 선택한 개체 오류의 상세정보를 표시한 다음, **Close**(닫기)를 클릭합니다.

단계 8 데이터 내보내기 프로세스가 완료되면, Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE 마이그레이션 툴) 창에 내보내기가 완료된 상태가 표시됩니다.



단계 9 **Export Reports**(보고서 내보내기)를 클릭하여 내보내기 보고서의 내용을 확인합니다.



단계 10 Cisco Secure ACS와 Cisco ISE 사이의 정책 격차를 분석하려면, **Policy Gap Analysis Report**(정책 간격 분석 보고서)를 클릭합니다.

Cisco ISE와 Cisco Secure ACS 사이의 정책 차이 분석

데이터를 내보낸 후에는 관리자가 내보내기 보고서 및 정책 격차 보고서를 분석하고, ACS 컨피그레이션에 나열된 오류를 수정하며, 경고 및 기타 문제를 해결해야 합니다.

Cisco Secure ACS 5.5 이상에서 Cisco ISE 로 마이그레이션되는 컨피그레이션 집합의 경우, 다음과 같은 차이가 있습니다. 이러한 차이 중 일부에 대해서는 조정이 가능합니다.

- **Identity Group(ID 그룹)**

- Internal Users(내부 사용자)

- Cisco Secure ACS와 Cisco ISE 사이의 패리티 격차

- 비밀번호 유형
 - 다음 로그인할 때 비밀번호 변경
 - 비밀번호 변경
 - 명명 제약 조건

- 외부 ID 저장소가 마이그레이션되었습니다. 이름을 확인해야 합니다.

- **Network Devices**(네트워크 디바이스) 또는 **Network Device Group**(네트워크 디바이스 그룹)

- Cisco ISE 2.1에 대한 네트워크 디바이스 마이그레이션 경고
 - Cisco ISE에서 지원되지 않는 IP 범위
 - IP 중복에 대한 제외
 - IPV4 전용
 - 기본 디바이스에는 RADIUS가 활성화되어 있어야 함
- 마이그레이션 툴의 조정 흐름
 - 디바이스가 Cisco ISE에 없는 경우(IP 컨피그레이션이 중복되지 않음으로 정의됨), 디바이스가 마이그레이션 중에 추가됩니다.
 - 디바이스가 있는 경우(IP 또는 서브넷이 정확히 일치하고, 이름이 정확하게 일치함), 마이그레이션 툴이 TACACS+ 요소를 추가합니다.
 - 디바이스가 있는 경우(IP/서브넷이 정확히 일치하거나 이름이 정확하게 일치함), 마이그레이션 툴에서 오류를 보고합니다.
- 권한 부여 결과

명령 집합(TACACS 명령 집합) 및 Shell Profiles(셸 프로파일)이 마이그레이션되었습니다. 개체 이름이 일치하지 않을 수 있습니다.

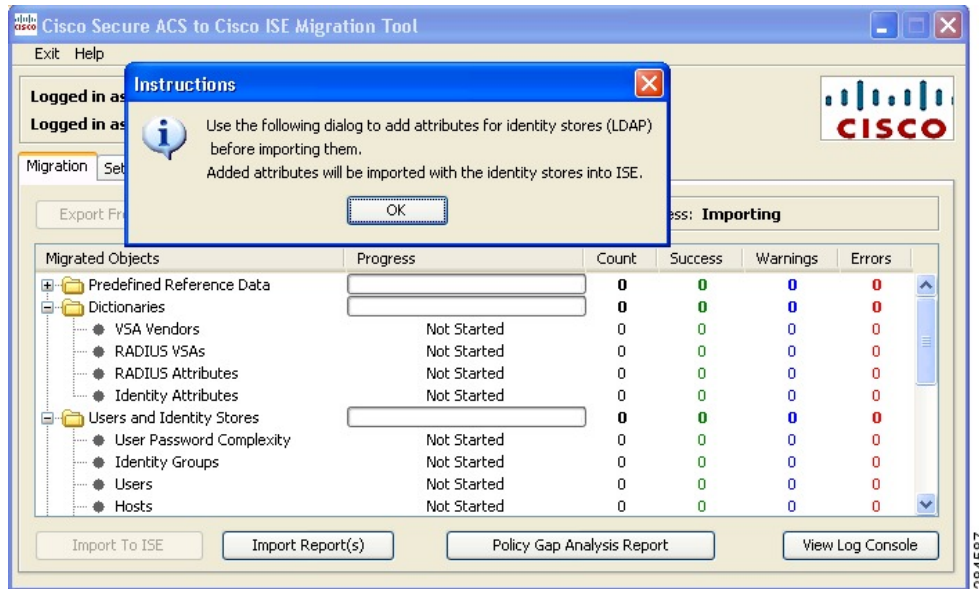
 - Cisco ISE는 이름을 엄격하게 준수합니다.
 - 정책 결과 네임스페이스가 네트워크 액세스 사용자와 공유됨
 - 디바이스 관리자 권한 부여 결과에 접두사를 사용하는 것이 좋음
- 정책
 - 선택 정책과 분리된 Cisco Secure ACS 5.x 액세스 서비스
 - 참여하지 않은 서비스를 보유할 수 있음
 - 다른 서비스 선택 규칙에 따라 서비스를 선택할 수 있음
 - Cisco Secure ACS 5.x 그룹 맵
 - Cisco Secure ACS 4.x에서 그룹 맵 전환
 - 그룹 맵 콘텐츠는 Cisco ISE의 권한 부여 정책으로 마이그레이션해야 합니다.
 - 인증 허용 프로토콜
 - Cisco Secure ACS 5.x의 서비스 컨피그레이션 부분
 - Cisco ISE 정책 결과의 일부

오류 또는 경고를 처리한 후, 내보내기 프로세스를 다시 수행합니다. Cisco Secure ACS에서 데이터를 내보내는 절차는 [내보내기 Cisco Secure ACS에서 데이터](#), 33 페이지를 참조하십시오.

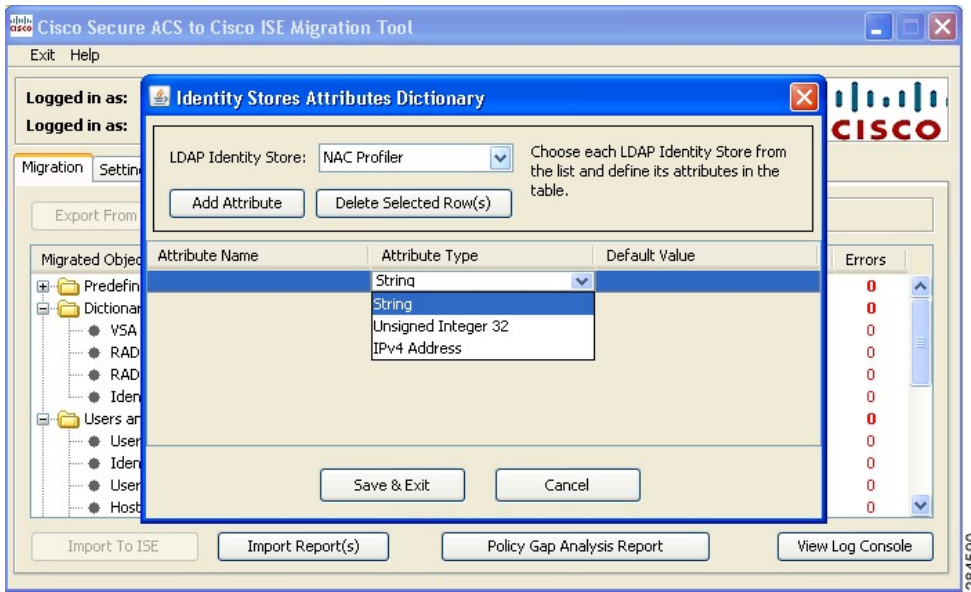
가져오기 Cisco ISE로 데이터

단계 1 Cisco Secure ACS to Cisco ISE Migration Tool 창에서 Import To ISE를 클릭합니다.

단계 2 Cisco ISE로 가져오기 전에, LDAP ID 저장소에 속성을 추가하라는 메시지가 표시되면 **OK**(확인)를 클릭합니다.



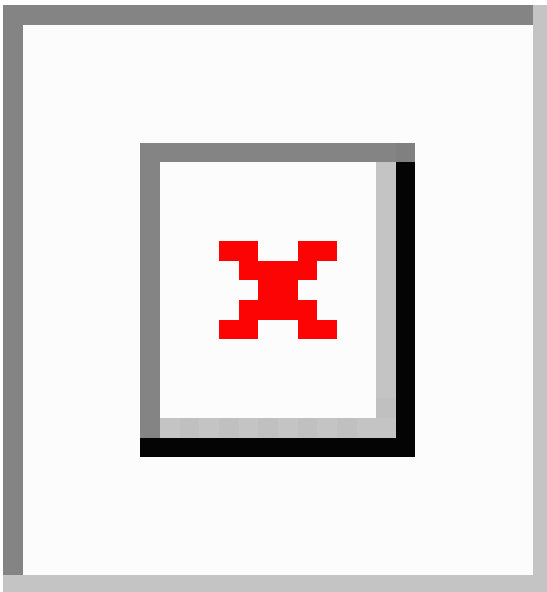
단계 3 **LDAP Identity Store**(LDAP ID 저장소) 드롭다운 목록에서, 속성을 추가할 ID 저장소를 선택하고 **Add Attribute**(속성 추가)를 클릭합니다.



단계 4 **Attribute Name**(속성 이름) 필드에 이름을 입력하고, **Attribute Type**(속성 유형) 드롭다운 목록에서 속성 유형을 선택한 다음 **Default Value**(기본값) 필드에 값을 입력하고 **Save & Exit**(저장 및 종료)를 클릭합니다.

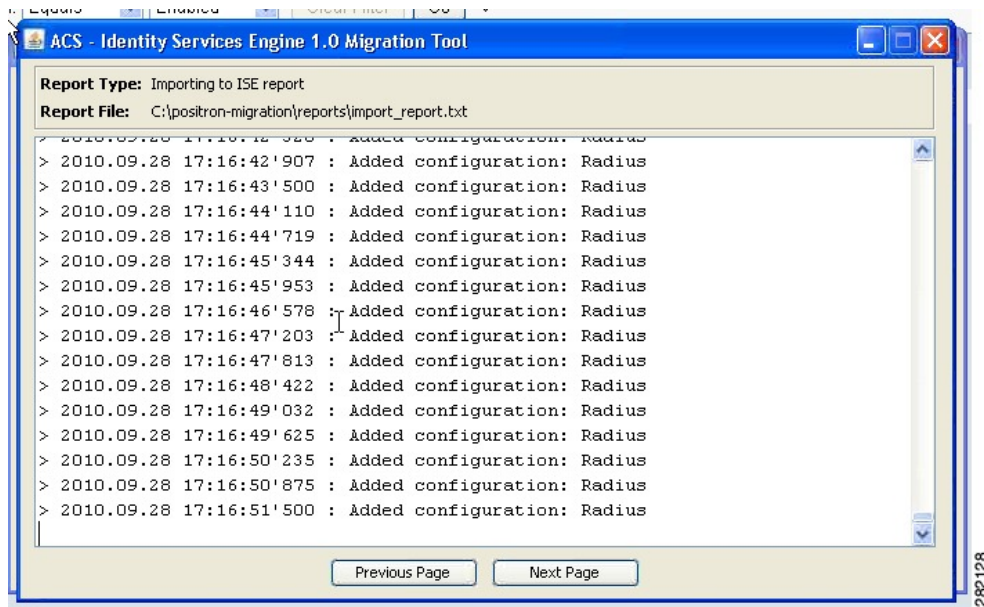
단계 5 속성을 추가한 후, **Import To ISE**(ISE로 가져오기)를 클릭하고 Cisco ISE FQDN(Fully Qualified Domain Name), 사용자 이름 및 비밀번호를 ISE Credentials(ISE 자격 증명) 창에 입력하고 **Connect**(연결)를 클릭합니다.

마이그레이션 툴은 SSL 인증서의 FQDN과 일치하는지 확인합니다.



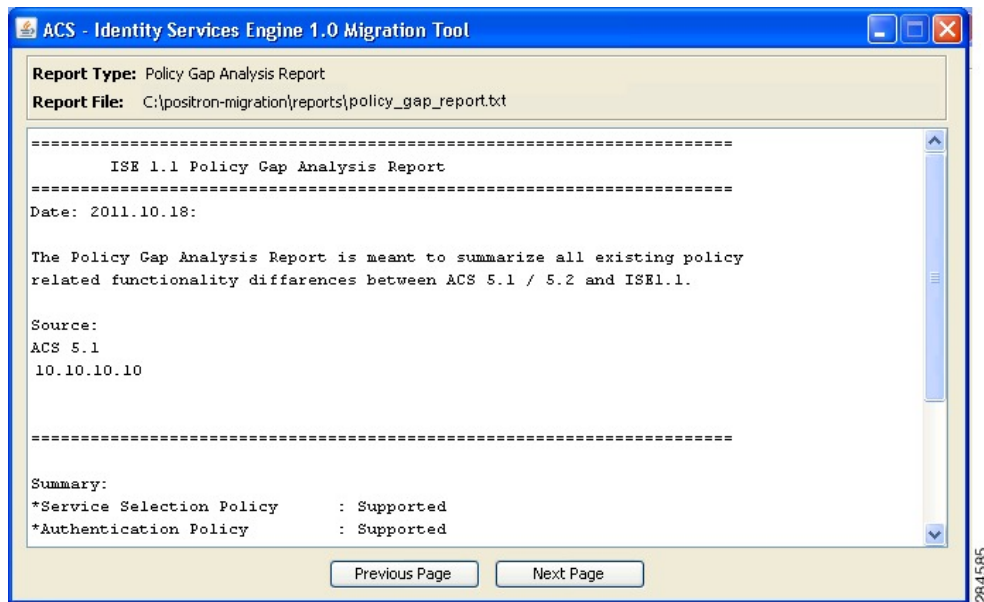
단계 6 데이터 가져오기 프로세스가 완료되면 Cisco Secure ACS to Cisco ISE Migration Tool(Cisco Secure ACS-Cisco ISE 마이그레이션 툴) 창에 가져오기의 상태가 가져오기 완료로 표시됩니다.

단계 7 가져온 데이터에 대한 전체 보고서를 보려면, **Import Report(s)**(보고서 가져오기)를 클릭합니다.

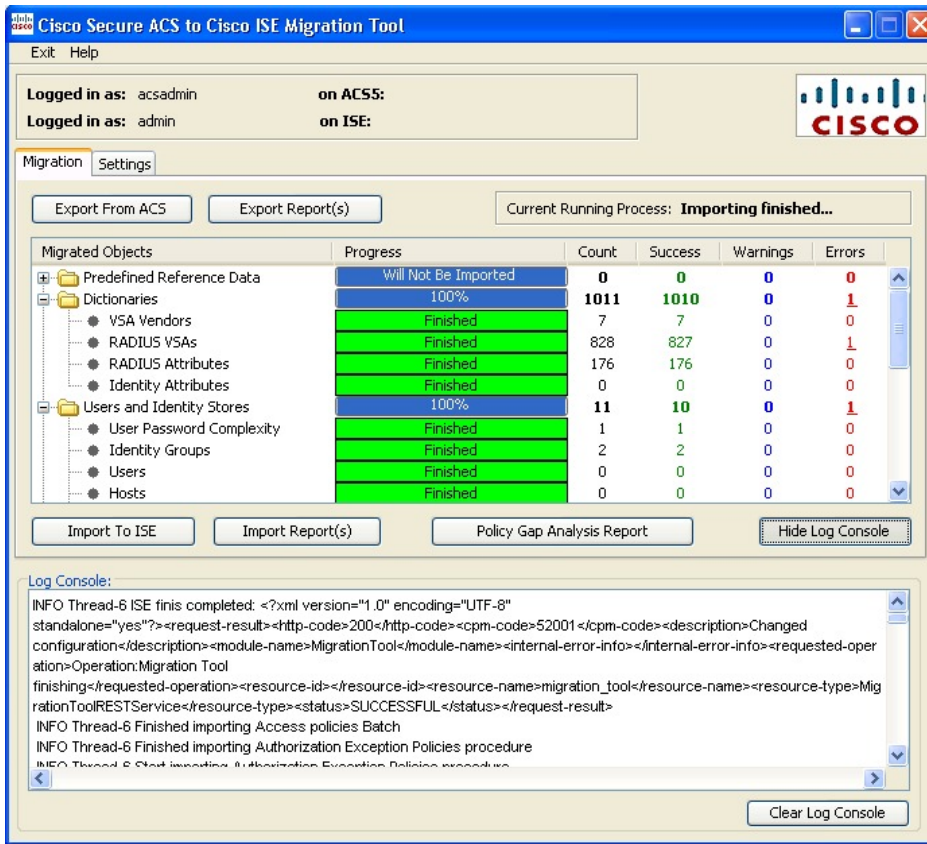


단계 8 가져오기 프로세스 중에 발생한 경고 또는 오류에 대한 자세한 정보를 얻으려면, **Migrations**(마이그레이션) 탭의 **Warnings or Errors**(경고 또는 오류) 열에서 밑줄이 그어진 숫자를 클릭합니다.

단계 9 Cisco Secure ACS와 Cisco ISE 사이의 정책 격차를 분석하려면, **Policy Gap Analysis Report**(정책 간격 분석 보고서)를 클릭합니다.



단계 10 **View Log Console**(로그 콘솔 보기)을 클릭하여, 내보내기 또는 가져오기 작업의 실시간 보기를 표시합니다.



284591

Cisco ISE에서 마이그레이션된 데이터 확인

Cisco Secure ACS 5.5 이상의 데이터가 Cisco ISE 으로 마이그레이션되었는지 확인하려면, Cisco ISE 에 로그인하여 다양한 Cisco Secure ACS 개체를 볼 수 있는지 확인합니다.



A 부록

데이터 구조 매핑

이 부록에서는 Cisco Secure ACS, 릴리스 5.5 또는 5.6 Cisco ISE 릴리스 1.4으로 마이그레이션, 부분 마이그레이션 및 마이그레이션되지 않는 데이터 개체에 대한 정보를 제공합니다.

- 데이터 구조 매핑, 43 페이지
- 마이그레이션된 데이터 개체, 43 페이지
- 데이터 개체가 마이그레이션되지 않음, 44 페이지
- 부분적으로 마이그레이션된 데이터 개체, 46 페이지
- 지원되는 특성 및 데이터 유형, 46 페이지
- 데이터 정보 매핑, 48 페이지

데이터 구조 매핑

Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4, 으로 데이터 구조를 매핑하는 것은 내 보내기 단계에서 마이그레이션 툴에서 데이터 개체를 분석하고 검증하는 프로세스입니다.

마이그레이션된 데이터 개체

다음 데이터 개체는 Cisco Secure ACS Cisco ISE,으로 마이그레이션됩니다.

- NDG(Network Device Group) 유형 및 계층 구조
- 네트워크 디바이스
- Default Network Device(기본 네트워크 디바이스)
- 외부 RADIUS 서버
- ID 그룹
- 내부 사용자
- 내부 엔드포인트(호스트)
- LDAP(Lightweight Directory Access Protocol)

- AD(Microsoft Active Directory)
- RSA (부분 지원, 표 A-19 참조)
- RADIUS 토큰(표 A-18 참조)
- 인증서 인증 프로파일
- 날짜 및 시간 조건(부분 지원, 지원되지 않는 규칙 요소 참조)
- RADIUS 속성 및 벤더별 속성(VSA) 값(표 A-5 및 표 A-6 참조)
- RADIUS 벤더 사전(표 A-5 및 표 A-6 참고 참조)
- 내부 사용자 속성(표 A-1 및 표 A-2 참조)
- 내부 엔드포인트 속성
- Authorization Profiles(권한 부여 프로파일)
- dACL(downloadable Access Control List)
- ID (인증) 정책
- 권한 부여 정책(네트워크 액세스용)
- TACACS+에 대한 인증, 권한 부여 및 권한 부여 예외 정책(정책 개체용)
- 권한 부여 정책(네트워크 액세스용)
- 서비스 선택 정책(네트워크 액세스용)
- RADIUS 프록시 서비스
- 사용자 비밀번호 복잡성
- ID 시퀀스 및 RSA 프롬프트
- UTF-8 데이터(UTF-8 지원 페이지 참조)
- EAP 인증 프로토콜-PEAP-TLS
- User check(사용자 확인) 속성
- ID 시퀀스 고급 옵션
- 정책 조건에서 사용 가능한 추가 속성-AuthenticationIdentityStore
- 추가 문자열 연산자-다음으로 시작, 끝, 포함, 포함 안 함
- RADIUS ID 서버 특성

데이터 개체가 마이그레이션되지 않음

다음 데이터 개체는 Cisco Secure ACS 않습니다.

- 보고서 모니터링
- 백업 예약
- 저장소
- 관리자, 역할 및 관리자 설정
- 고객/디버그 로그 컨피그레이션
- 구축 정보(보조 노트)
- 인증서(인증 기관 및 로컬 인증서)
인증서는 마이그레이션되지 않으므로, 수동으로 가져와야 합니다. 인증서를 사용하는 ID 저장소의 경우, 가져온 인증서를 ID 저장소에 매핑해야 합니다. ID 소스 시퀀스를 사용하는 경우, 원본을 복제하는 새 시퀀스를 생성해야 합니다.
- SGACL(Security Group Access Control List)
- SG(Security Group)
- 지원되는 SGA(Security Group Access) 디바이스용 AAA 서버
- Security Group(보안 그룹) 매핑
- NDAC(Network Device Admission Control) 정책
- SGA Egress 매트릭스
- 네트워크 디바이스 내의 SGA 데이터
- SGA 권한 부여 정책 결과의 SGT(Security Group Tag)
- 네트워크 조건(엔드 스테이션 필터, 디바이스 필터, 디바이스 포트 필터)
- 디바이스 AAA 정책
- 다이얼인(dial-in) 속성 지원
- TACACS + 프록시
- TACACS + CHAP 및 MSCHAP 인증
- TACACS + 셸 프로파일의 속성 대체
- RSA 노드 누락 비밀번호 표시
- 최대 사용자 세션 수
- 어카운트 비활성화
- 사용자 비밀번호 유형
- 비밀번호 유형을 외부 ID 저장소로 사용하여 설정된 내부 사용자
- 정책 조건에서 사용할 수 있는 추가 속성—NumberOfHoursSinceUserCreation

- 호스트용 와일드카드
- 네트워크 디바이스 범위
- OCSP 서비스
- SSL/TCP를 통한 Syslog 메시지
- 구성 가능한 저작권 배너
- 내부 사용자 만료일
- IP 주소 제외

부분적으로 마이그레이션된 데이터 개체

다음 데이터 개체는 Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4으로 부분적으로 마이그레이션됩니다.

- 날짜 유형의 ID 및 호스트 속성은 마이그레이션되지 않습니다.
- RSA sdopts.rec 파일 및 보조 정보는 마이그레이션되지 않습니다.
- 다중 Active Directory 도메인(기본에 가입한 Active Directory 도메인만 해당)이 마이그레이션됩니다.
- 기본 ACS 인스턴스에 대해 정의된 LDAP 컨피그레이션이 마이그레이션됩니다.

지원되는 특성 및 데이터 유형

사용자 속성이 **Cisco Secure ACS, 릴리스 5.5** 이상에서 **Cisco ISE 1.4**로 마이그레이션됨

Cisco Secure ACS, 릴리스 5.5 이상에서 지원되는 사용자 속성	Cisco ISE, 릴리스 1.4의 대상 데이터 유형
문자열	문자열
UI32	지원되지 않음
IPv4	지원되지 않음
부울	지원되지 않음
Date(날짜)	지원되지 않음
Enum	지원되지 않음

사용자 특성: 사용자와 연결

Cisco Secure ACS 릴리스 5.5 이상의 사용자와 연결된 특성	Cisco ISE, 릴리스 1.4
문자열	지원
UI32	지원되지 않음
IPv4	지원되지 않음
부울	지원되지 않음
Date(날짜)	지원되지 않음

Cisco Secure ACS, 릴리스 5.5 또는 5.6 1.4로 마이그레이션된 호스트 속성

Cisco Secure ACS, 릴리스 5.5 또는 5.6 지원되는 호스트 특성	Cisco ISE, 릴리스 1.4 의 대상 데이터 유형
문자열	문자열
UI32	UI32
IPv4	IPv4
부울	부울
Date(날짜)	지원되지 않음
Enum	허용되는 값이 있는 정수

호스트 속성: 호스트에 연결

Cisco Secure ACS, 릴리스 5.5 이상의 호스트에 연결된 속성	Cisco ISE, 릴리스 1.4
문자열	지원
UI32	지원됨(값이 문자열로 변환됨)
IPv4	지원됨(값이 문자열로 변환됨)
부울	지원됨(값이 문자열로 변환됨)
날짜	지원됨(값이 문자열로 변환됨)
Enum	지원됨(값이 문자열로 변환됨)

RADIUS 속성이 Cisco Secure ACS, 릴리스 5.5 이상에서 Cisco ISE, 릴리스 1.4로 마이그레이션됨

Cisco Secure ACS, 릴리스 5.5 이상에서 지원되는 RADIUS 속성	Cisco ISE 대상 데이터 유형, 릴리스 1.4
UI32	UI32
UI64	UI64
IPv4	IPv4
16진수 문자열	옥텟 문자열
문자열	문자열
Enum	허용되는 값이 있는 정수

RADIUS 속성: RADIUS 서버에 연결

Cisco Secure ACS, 릴리스 5.5 이상에서 RADIUS 서버와 연결된 속성	Cisco ISE, 릴리스 1.4
UI32	지원
UI64	지원
IPv4	지원
16진수 문자열	지원됨(16진수 문자열이 옥텟 문자열로 변환됨)
문자열	지원
Enum	지원됨(값은 허용되는 값의 정수임)

데이터 정보 매핑

이 섹션에는 내보내기 프로세스 중에 매핑되는 데이터가 나열됩니다. 이 테이블에는 Cisco Secure ACS, 릴리스 5.5 이상의 개체 범주 및 Cisco ISE, 릴리스 1.4의 해당 범주가 포함됩니다. 이 섹션의 데이터 매핑 테이블에는 마이그레이션 프로세스의 내보내기 단계에서 데이터를 마이그레이션할 때 매핑된 유효하거나 유효하지 않은 데이터 개체의 상태가 나열됩니다.

네트워크 디바이스 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	현재 상태로 마이그레이션
설명	현재 상태로 마이그레이션
Network Device Group(네트워크 디바이스 그룹)	현재 상태로 마이그레이션
단일 IP Address	현재 상태로 마이그레이션
단일 IP 및 서브넷 주소	현재 상태로 마이그레이션
IP 및 서브넷 주소 수집	지원되지 않음
IP Address 제외	지원되지 않음
TACACS 정보	TACACS가 Cisco ISE, 릴리스 1.4에서 지원되지 않으므로 마이그레이션되지 않습니다.
RADIUS 공유 비밀번호	현재 상태로 마이그레이션
CTS	현재 상태로 마이그레이션
SNMP	SNMP 데이터는 Cisco ISE에서만 사용 가능하기 때문에, 마이그레이션 된 디바이스에 대한 SNMP 정보가 없습니다.
Model Name(모델 이름)	이 속성은 Cisco ISE에서만 사용 가능하며, 기본 값은 "unknown"입니다.
소프트웨어 버전	이 속성은 Cisco ISE에서만 사용 가능하며, 기본 값은 "unknown"입니다.



참고 TACACS로만 설정된 네트워크 디바이스는 마이그레이션이 지원되지 않으며, 마이그레이션되지 않은 디바이스로 나열됩니다.

Active Directory 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
Domain name(도메인 이름)	현재 상태로 마이그레이션
User name(사용자 이름)	현재 상태로 마이그레이션
비밀번호	현재 상태로 마이그레이션

Cisco Secure ACS 속성	Cisco ISE Properties
Allow password change(비밀번호 변경 허용)	현재 상태로 마이그레이션
Allow machine access restrictions(MAR(Machine Access Restrictions) 허용)	현재 상태로 마이그레이션
Aging Time(유지 시간)	현재 상태로 마이그레이션
사용자 속성	현재 상태로 마이그레이션
Groups(그룹)	현재 상태로 마이그레이션
다중 도메인 지원	기본 ACS 인스턴스에 가입된 도메인만 마이그레이션됨

외부 TACACS 서버 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
서버 IP 주소	Hostname
공유 암호	공유 암호
Authentication Port(인증 포트)	Authentication Port(인증 포트)
Accounting Port(어카운팅 포트)	Accounting Port(계정 관리 포트)
Server timeout(서버 시간 초과)	Server timeout(서버 시간 초과)
Connection Attempts(연결 시도 횟수)	Connection Attempts(연결 시도 횟수)

호스트(엔드포인트) 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
MAC 주소	현재 상태로 마이그레이션
Status	Not migrated
설명	현재 상태로 마이그레이션
ID 그룹	엔드포인트 그룹에 대한 연결을 마이그레이션합니다.

Cisco Secure ACS 속성	Cisco ISE Properties
특성	엔드포인트 속성이 마이그레이션됩니다.
인증	이 속성은 Cisco ISE에서만 사용할 수 있는 속성입니다(값은 고정값 "Authenticated").
클래스 이름	이 속성은 Cisco ISE에서만 사용할 수 있는 속성입니다(값은 고정값 "TBD").
엔드포인트 정책	이 속성은 Cisco ISE에서만 사용할 수 있(으며, 습니다. 이 값은 고정 값인 "Unknown (알 수 없음)"입니다.
일치된 정책	이 속성은 Cisco ISE에서만 사용할 수 있(으며, 습니다. 이 값은 고정 값인 "Unknown (알 수 없음)"입니다.
일치된 값	이 속성은 Cisco ISE에서만 사용할 수 있는 속성입니다(값은 고정값 "0").
NAS IP Address(NAS IP 주소)	이 속성은 Cisco ISE에서만 사용할 수 있는 속성입니다(값은 고정값 "0.0.0.0").
OUI	이 속성은 Cisco ISE에서만 사용할 수 있는 속성입니다(값은 고정값 "TBD"임).
Posture Status(포스처 상태)	이 속성은 Cisco ISE에서만 사용할 수 있(으며, 습니다. 이 값은 고정 값인 "Unknown (알 수 없음)"입니다.
Static Assignment(정적 할당)	이 속성은 Cisco ISE에서만 사용할 수 있는 속성입니다(값은 고정값 "False").

ID 사전 매핑

Cisco Secure ACS 속성	Cisco ISE 속성
Attribute(속성)	Attribute Name(속성 이름)
설명	Description(설명)
Internal Name(내부 이름)	Internal Name(내부 이름)
Attribute Type(속성 유형)	Data Type(데이터 유형)
Maximum Length(최대 길이)	마이그레이션되지 않음
디폴트 값	마이그레이션되지 않음

Cisco Secure ACS 속성	Cisco ISE 속성
필수 필드	마이그레이션되지 않음
사용자	사전 속성이 이 값("user")을 수락합니다.

ID 그룹 매핑

Cisco Secure ACS 속성	Cisco ISE 속성
이름	이름
설명	Description(설명)
상위	이 속성은 계층 구조 상세정보의 일부로 마이그레이션됩니다.



참고 Cisco ISE, 릴리스 1.4에는 사용자 및 엔드포인트 ID 그룹이 포함되어 있습니다. 사용자는 사용자 ID 그룹에 할당되어야 하고 엔드포인트는 엔드포인트 ID 그룹에 할당되어야 하기 때문에, Cisco Secure ACS, 릴리스 5.5 이상의 ID 그룹은 사용자 및 엔드포인트 ID 그룹으로 Cisco ISE, 릴리스 1.4으로 마이그레이션됩니다.

LDAP 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
서버 연결 정보	현재 상태로 마이그레이션(Server Connection(서버 연결) 탭, A-10 페이지의 그림 A-1 참조)
디렉토리 조직 정보	현재 상태로 마이그레이션(Directory Organization(디렉토리 조직) 탭, A-10 페이지의 그림 A-2 참조)
디렉토리 그룹	현재 상태로 마이그레이션
디렉토리 속성	마이그레이션은 수동으로 수행됩니다(Cisco Secure ACS-Cisco ISE 마이그레이션 툴 사용).



참고 기본 ACS 인스턴스에 대해 정의된 LDAP 컨피그레이션만 마이그레이션됩니다.

그림 5: **Server Connection**(서버 연결) 탭

282131

그림 6: **Directory Organization**(디렉터리 조직) 탭

282132

NDG 유형 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)



참고 Cisco Secure ACS, 릴리스 5.5 이상에서는 동일한 이름의 네트워크 디바이스 그룹(NDG)을 두 개 이상 지원할 수 있습니다. Cisco ISE, 릴리스 1.3 1.4 2.0 2.1 2.2 2.3 2.4 2.6 2.7 3.0은 이 명명 체계를 지원하지 않습니다. 따라서 정의된 이름의 첫 번째 NDG 유형만 마이그레이션됩니다.

NDG 계층 구조 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
상위	이 값은 NDG 계층 이름의 일부로만 입력되므로, 이 속성과 관련된 특정 속성은 없습니다. 또한 NDG 유형은 이 개체 이름의 접두사입니다.



참고 Cisco ISE, 릴리스 1.4은 콜론을 유효한 문자로 인식하지 않기 때문에, 콜론(:)이 포함된 루트 이름을 포함하는 NDG는 마이그레이션되지 않습니다.

RADIUS 사전 (벤더) 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
벤더 ID	판매업체 ID
속성 접두사	이 속성을 마이그레이션할 필요가 없습니다.
벤더 길이 필드 크기	벤더 속성 유형 필드 길이입니다.
벤더 유형 필드 크기	벤더 특성 크기 필드 길이입니다.



참고 Cisco Secure ACS, 릴리스 5.5 이상의 설치에 포함되지 않은 RADIUS 벤더만 마이그레이션해야 합니다. 이는 사용자 정의 벤더에만 영향을 줍니다.

RADIUS 사전 (속성) 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
속성 ID	이 값은 NDG 계층 구조 이름의 일부로만 입력되므로, 이 속성과 연결된 특정 속성이 없습니다 (NDG 유형은 이 개체 이름의 접두사임).
방향	Cisco ISE에서 지원되지 않음
다중 허용	Cisco ISE에서 지원되지 않음
특성 유형	현재 상태로 마이그레이션
정책 조건 추가	Cisco ISE에서 지원되지 않음
정책 조건 표시 이름	Cisco ISE에서 지원되지 않음



참고 Cisco Secure ACS, 릴리스 5.5 이상 설치의 일부로 포함되지 않은 사용자 정의 RADIUS 특성만 마이그레이션하면 됩니다(사용자 정의 특성 만 마이그레이션하면 됨).

사용자 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
Status(상태)	이 속성을 마이그레이션할 필요가 없습니다. 이 속성이 Cisco ISE에 없습니다.
Identity Group(ID 그룹)	Cisco ISE에서 ID 그룹으로 마이그레이션
Password(비밀번호)	비밀번호
Enable Password(활성화 비밀번호)	이 속성을 마이그레이션할 필요가 없습니다. (이 속성이 Cisco ISE에 없음)
다음 로그인할 때 비밀번호 변경	이 속성을 마이그레이션할 필요가 없습니다.
사용자 속성 목록	사용자 속성은 Cisco ISE에서 가져오며, 사용자와 연결됩니다.

Cisco Secure ACS 속성	Cisco ISE Properties
만료일	지원되지 않음

인증서 인증 프로파일 매핑

Cisco Secure ACS 속성	Cisco ISE 속성
이름	이름
설명	Description(설명)
기본 사용자 이름(X.509 속성)	기본 사용자 이름(X.509 속성)
이진 인증서와 LDAP 또는 AD의 인증서의 비교	이진 인증서를 LDAP 또는 AD의 인증서와 비교합니다.
인증서 가져오기를 위한 AD 또는 LDAP 이름	인증서 가져오기를 위한 AD 또는 LDAP 이름입니다.

권한 부여 프로파일 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
DAACLID (다운로드 가능한 ACL ID)	현재 상태로 마이그레이션
속성 유형(정적 및 동적)	<ul style="list-style-type: none"> 정적 속성인 경우, 그대로 마이그레이션합니다. 동적 속성인 경우, 동적 VLAN을 제외한 상태로 마이그레이션됩니다.
속성(정적 유형에 대해서만 필터링됨)	RADIUS 속성

다운로드 가능한 ACL 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)

Cisco Secure ACS 속성	Cisco ISE Properties
DACL 콘텐츠	DACL 콘텐츠

외부 TACACS 서버 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
서버 IP 주소	Hostname
공유 암호	공유 암호
Authentication Port(인증 포트)	Authentication Port(인증 포트)
Accounting Port(어카운팅 포트)	Accounting Port(계정 관리 포트)
Server timeout(서버 시간 초과)	Server timeout(서버 시간 초과)
Connection Attempts(연결 시도 횟수)	Connection Attempts(연결 시도 횟수)

ID 속성 사전 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
특성	특성 이름
설명	Internal Name(내부 이름)
이름	현재 상태로 마이그레이션
특성 유형	데이터 유형
해당 속성 없음	사전(사용자 ID 속성인 경우에는 "InternalUser" 또는 호스트 ID 특성인 경우에는 "InternalEndpoint" 값으로 설정)
Cisco Secure ACS에서 아직 내보내거나 추출하지 않음	허용되는 값 = 표시 이름
Cisco Secure ACS에서 아직 내보내거나 추출하지 않음	허용되는 값 = 내부 이름
Cisco Secure ACS에서 아직 내보내거나 추출하지 않음	허용되는 값은 기본임

Cisco Secure ACS 속성	Cisco ISE Properties
Maximum Length(최대 길이)	None
디폴트 값	None
필수 필드	None
정책 조건 추가	None
정책 조건 표시 이름	None

RADIUS 토큰 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
SafeWord Server(SafeWord 서버)	SafeWord Server(SafeWord 서버)
보조 어플라이언스 활성화	보조 어플라이언스 활성화
Always Access Primary Server First(항상 기본 서버에 먼저 액세스)	Always Access Primary Server First(항상 기본 서버에 먼저 액세스)
몇 분 만에 기본 어플라이언스로 대체	몇 분 만에 기본 어플라이언스로 대체
Primary Appliance IP Address(기본 어플라이언스 IP 주소)	기본 어플라이언스 IP 주소
Primary Shared Secret(기본 공유 비밀번호)	기본 공유 암호
Primary Authentication Port(기본 인증 포트)	기본 인증 포트
Primary Appliance TO(기본 어플라이언스 TO)(시간 초과)	Primary Appliance TO(기본 어플라이언스 TO)
Primary Connection Attempts(기본 연결 시도 횟수)	Connection Attempts(연결 시도 횟수)
Secondary Appliance IP Address(보조 어플라이언스 IP 주소)	기본 어플라이언스 IP 주소
Secondary Shared Secret(보조 공유 비밀번호)	보조 공유 암호
Secondary Authentication Port(보조 인증 포트)	보조 인증 포트
Secondary Appliance TO(보조 어플라이언스 TO)	Secondary 보조 어플라이언스 TO

Cisco Secure ACS 속성	Cisco ISE Properties
Secondary Connection Attempts(보조 연결 시도 횟수)	Secondary Connection Attempts(보조 연결 시도 횟수)
Advanced(고급)> 거부를 인증 플래그 실패로 처리	Advanced(고급)> 거부를 인증 플래그 실패로 처리합니다.
Advanced(고급)> 거부를 사용자가 찾을 수 없는 플래그로 처리	Advanced(고급)> 거부를 사용자가 찾을 수 없는 플래그로 처리합니다.
Advanced(고급)> ID 캐싱 및 에이징 값 활성화	Advanced(고급)> ID 캐싱 및 에이징 값을 활성화합니다.
Shell(셸)> 프롬프트	Authentication(인증)> 프롬프트
디렉토리 속성	Authorization(권한 부여)> 속성 이름(In cases where the dictionary attribute lists in Cisco Secure ACS의 사전 속성 목록에 속성 “CiscoSecure-Group-Id”이 포함되는 경우에는 이 속성으로 마이그레이션되며, 그렇지 않으면 기본값이 “CiscoSecure-Group-Id”.)

RSA 매핑

Cisco Secure ACS 속성	Cisco ISE 속성
이름	이름은 항상 RSA
설명	마이그레이션되지 않음
영역 컨피그레이션 파일	영역 설정 필드
서버 대상	서버 대상
PIN 변경 시 재인증	PIN 변경 시 재인증
RSA 인스턴스 파일	Not migrated
인증 실패로 거부 처리	인증 실패로 거부 처리
사용자를 찾을 수 없으므로 거부 처리	사용자를 찾을 수 없으므로 거부 처리
ID 캐싱 활성화	ID 캐싱 활성화
ID 캐싱 에이징 시간	ID 캐싱 에이징 시간

RSA 프롬프트 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
Passcode Prompt(비밀번호 프롬프트)	Enter Passcode Prompt(암호 프롬프트 입력)
Next Token Prompt(다음 토큰 프롬프트)	Next Token Prompt(다음 토큰 프롬프트)
PIN Type Prompt(PIN 유형 프롬프트)	PIN Type PIN 유형 프롬프트
Accept System PIN(시스템 PIN 수락)	Accept System PIN(시스템 PIN 수락)
Alphanumeric PIN Prompt(영숫자 PIN 프롬프트)	Alphanumeric PIN 영숫자 PIN 프롬프트
Numeric PIN Prompt(숫자 PIN 프롬프트)	Numeric PIN Prompt(숫자 PIN 프롬프트)

ID 저장소 시퀀스 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
이름	이름
설명	Description(설명)
인증서 기반, 인증서 인증 프로파일	인증서 기반, 인증서 인증 프로파일
비밀번호 기반	인증 검색 목록
고급 옵션-현재 IDStore에 대한 액세스가 중단 시퀀스보다 실패하는 경우	시퀀스의 다른 저장소에 액세스하여 "AuthenticationStatus" 속성을 "ProcessError"로 설정하지 마십시오.
고급 옵션 > 현재 IDStore에 대한 액세스가 실패한 경우 다음으로 계속 진행	"User Not Found(사용자를 찾을 수 없음)"로 처리하고, 순서의 다음 저장소로 진행합니다.
특성 검색 전용 > 종료 시퀀스 및 "사용자를 찾을 수 없음"으로 처리	지원되지 않음(무시해야 함)

기본 네트워크 디바이스 매핑

Cisco Secure ACS 속성	Cisco ISE Properties
Default Network Device Status(기본 네트워크 디바이스 상태)	Default Network Device Status(기본 네트워크 디바이스 상태)
Network Device Group(네트워크 디바이스 그룹)	Not migrated

Cisco Secure ACS 속성	Cisco ISE Properties
인증 옵션-TACACS+	Not migrated
RADIUS 공유 비밀번호	Shared Secret(공유 암호)
RADIUS CoA 포트	Not migrated
RADIUS - Enable KeyWrap(KeyWrap 활성화)	Enable KeyWrap(KeyWrap 활성화)
RADIUS - Key Encryption Key(키 비밀번호화 키)	Key Encryption Key(키 비밀번호화 키)
RADIUS - Message Authenticator Code Key(메시지 인증자 코드 키)	Message Authenticator Code Key(메시지 인증자 코드 키)
RADIUS - Key Input Format(키 입력 형식)	Key Input Format(키 입력 형식)



B 부록

문제 해결 마이그레이션 툴 문제 해결

- 마이그레이션 툴을 시작할 수 없음, 63 페이지
- 로그에 표시되는 오류 메시지, 63 페이지
- 기본 폴더, 파일 및 보고서 생성되지 않음, 64 페이지
- 마이그레이션 내보내기 단계가 매우 느림, 65 페이지
- 보고Cisco TAC에 문제, 65 페이지

마이그레이션 툴을 시작할 수 없음

조건

마이그레이션 툴을 시작할 수 없습니다.

작업

마이그레이션 컴퓨터에 Java JRE, 버전 1.6 이상이 설치되어 있으며, 시스템 경로 및 클래스 경로에 올바르게 구성되어 있는지 확인합니다.

로그에 표시되는 오류 메시지

연결 오류

조건

다음 오류 메시지가 로그에 표시됩니다. “Hosts: Connection to https://hostname-or-ip refused: null” 또한 Cisco ISE로 마이그레이션하는 동안 개체가 보고됩니다.

작업

- 마이그레이션 애플리케이션 컴퓨터가 네트워크에 연결되어 있고 올바르게 설정되어 있는지 확인합니다.

- Cisco ISE 어플라이언스가 네트워크에 연결되어 있고 올바르게 설정되어 있는지 확인합니다.
- Cisco ISE 어플라이언스와 마이그레이션 컴퓨터가 네트워크를 통해 서로 연결할 수 있는지 확인합니다.
- 마이그레이션 툴이 Cisco ISE에 연결할 때, Cisco ISE 기본 노드에 사용된 호스트네임(있는 경우)이 DNS 내에서 해결 가능한지 확인합니다.
- Cisco ISE 어플라이언스가 작동 및 실행 중인지 확인합니다.
- Cisco ISE 애플리케이션 서버 서비스가 시작되어 실행 중인지 확인합니다.

I/O 예외 오류

조건

다음 오류 메시지가 로그에 표시됩니다.

“요청을 처리할 때 I/O 예외(org.apache.http.NoHttpResponseException)가 발생했습니다. 대상 서버가 응답하지 못했습니다.”

작업

- Cisco ISE 애플리케이션 서버 서비스가 시작되어 실행 중인지 확인합니다.
- Cisco ISE 웹 서버 임계값이 초과되지 않았거나 메모리 예외가 없는지 확인합니다.
- Cisco ISE 어플라이언스 CPU 사용량이 100%가 아니며 CPU가 활성 상태인지 확인합니다.

메모리 부족 오류

조건

다음 오류 메시지가 로그에 표시됩니다.

“OutOfMemory”.

작업

Java Heap Size를 1GB 이상으로 늘리십시오.

기본 폴더, 파일 및 보고서 생성되지 않음

조건

마이그레이션 툴이 기본 폴더, 로그 파일, 보고서 및 지속성 데이터 파일을 생성하지 못합니다.

작업

사용자에게 파일 시스템 쓰기 권한이 있고 디스크 공간이 충분한지 확인합니다.

마이그레이션 내보내기 단계가 매우 느림

조건

마이그레이션 프로세스의 내보내기 단계는 매우 느립니다.

작업

마이그레이션 프로세스를 시작하기 전에, Cisco Secure ACS 어플라이언스를 다시 시작하여 메모리 공간을 확보하십시오.

보고 Cisco TAC에 문제

기술 문제 또는 문제에 대한 소스 및 잠재적 해결 방법을 찾을 수 없는 경우, Cisco 고객 서비스 담당자에게 문의하여 문제 해결 방법에 대한 정보를 얻을 수 있습니다. Cisco TAC(Technical Assistance Center)에 대한 내용은 어플라이언스에 탑재된 Cisco Information Packet(Cisco 정보 패킷) 발행물을 참조하거나 다음 웹 사이트를 참조 하십시오.

<http://www.cisco.com/cisco/web/support/index.html>

Cisco TAC에 연락하기 전에, 다음 정보를 갖고 있는지 확인합니다.

- 어플라이언스 새시 및 일련 번호.
- 유지 관리 계약 또는 보증 정보(Cisco Information Packet(Cisco 정보 패킷) 참조).
- 소프트웨어의 이름, 유형 및 버전 또는 릴리스 번호(해당되는 경우).
- 새로운 어플라이언스 날짜를 받은 날짜.
- 경험한 문제 또는 조건에 대한 간략한 설명, 문제를 격리하거나 다시 만드는 단계 및 이 문제를 해결하기 위해 수행한 단계에 대한 기술.
- 마이그레이션 로그 파일(...migration/bin/migration.log).
- config 폴더의 모든 보고서(...migration/config).
- Cisco Secure ACS, 릴리스 5.5 이상 로그 파일.
- Cisco Secure ACS, 릴리스 5.5 이상의 빌드 번호.

**참고**

초기 설치 후 SNS 3300 Series 어플라이언스에서 수행된 모든 업그레이드 또는 유지 관리 정보를 고객 서비스 담당자에게 제공해야 합니다.

