



Cisco Identity Services Engine、Release 1.2 Migration Tool ガイド

2013 年 7 月

【注意】シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/)をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Identity Services Engine, Release 1.2 Migration Tool ガイド
Copyright ©2013 Cisco Systems, Inc. All rights reserved.



- このマニュアルの目的 vii
- Cisco Secure ACS の以前のリリースからの移行 viii
- 対象読者 ix
- マニュアルの構成 x
- このマニュアルの使用方法 x
- 表記法 xi
- 関連資料 xii
 - リリース固有のマニュアル xii
 - プラットフォーム固有のマニュアル xii
- 通告 xiii
 - OpenSSL/Open SSL Project xiii
 - License Issues xiii
- マニュアルの入手方法およびテクニカル サポート xv

CHAPTER 1

- Cisco Secure ACS から Cisco ISE へのデータ移行 1-1**
 - Cisco Secure ACS から Cisco ISE へのサポートされているデータ移行 1-1
 - Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のポリシー モデル 1-2
 - Cisco Secure ACS 5.3 と Cisco ISE のポリシー モデルの違い 1-2
 - Cisco ISE および Cisco Secure ACS の導入モデル 1-3
 - 移行機能 1-3
 - データのエクスポート 1-4
 - データの持続性 1-4
 - データのインポート 1-4
 - オブジェクトの拡張性 1-4
 - ハイ アベイラビリティ 1-5
 - レポート 1-5
 - UTF-8 のサポート 1-7
 - ISE 802.1X サービスに対する FIPS サポート 1-8
 - Cisco Secure ACS/Cisco ISE バージョンの検証 1-9

CHAPTER 2

- Cisco Secure ACS to Cisco ISE Migration Tool について 2-1**
 - Cisco Secure ACS to Cisco ISE Migration Tool 2-1
 - ソフトウェア要件 2-2

移行ツールのコンポーネント 2-3
 データ設定 2-3
 ステータス報告 2-3
 エクスポートおよびインポート 2-3
 データ構造マッピング 2-4

CHAPTER 3

Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 へのデータの移行 3-1
 データの移行および導入のシナリオ 3-1
 シングル Cisco Secure ACS アプライアンスからのデータの移行 3-1
 分散環境におけるデータの移行 3-2
 Cisco Secure ACS データの Cisco ISE への移行 3-3
 ポリシー規則の検証 3-3
 Cisco Secure ACS Release 5.3 からの移行の準備 3-5
 ポリシー サービスの移行のガイドライン 3-5
 ポリシー サービスごとの移行のガイドライン 3-6

CHAPTER 4

Cisco Secure ACS to Cisco ISE Migration Tool のインストール 4-1
 移行ツールのインストール ガイドライン 4-1
 システム要件 4-2
 セキュリティの考慮事項 4-2
 Cisco Secure ACS-Cisco ISE Migration Tool のインストールおよび初期化 4-3

CHAPTER 5

Cisco Secure ACS to Cisco ISE Migration Tool の使用方法 5-1
 Cisco Secure ACS データをエクスポートおよびインポートするための移行ツールの使用方法 5-1
 Cisco ISE に移行されたデータの確認 5-8

APPENDIX A

Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のデータ構造マッピング A-1
 移行されるデータ オブジェクト A-1
 移行されないデータ オブジェクト A-2
 一部が移行されるデータ オブジェクト A-3
 サポート対象属性およびデータ型 A-3
 データ情報マッピング A-5

APPENDIX B

Cisco Secure ACS to Cisco ISE Migration Tool のトラブルシューティング B-1
 移行ツールを開始できない B-1
 ログにエラー メッセージが表示される B-1
 デフォルトのフォルダ、ファイル、およびレポートが作成されない B-3

移行のエクスポート フェーズが非常に遅い B-3

Cisco TAC への問題の報告 B-3

GLOSSARY

INDEX



はじめに

このマニュアルでは、Cisco Secure ACS to Cisco ISE Migration Tool を使用して Cisco Secure Access Control System (ACS) のリリース 5.3 データベースから Cisco Identity Services Engine (ISE) のリリース 1.2 アプライアンスヘデータを移行するプロセスについて説明します。



(注)

各 Cisco Secure ACS または Cisco ISE リリースで動的に変化している機能ギャップのために、すべての Cisco Secure ACS データを Cisco ISE に移行できるわけではありません。Cisco Secure ACS to Cisco ISE Migration Tool には、サポートされていないオブジェクトの完全なリストが含まれています。詳細については、[図 4-1](#) を参照してください。

具体的な内容は、次のとおりです。

- 「このマニュアルの目的」 (P.vii)
- 「対象読者」 (P.ix)
- 「マニュアルの構成」 (P.x)
- 「このマニュアルの使用法」 (P.x)
- 「表記法」 (P.xi)
- 「マニュアルの入手方法およびテクニカル サポート」 (P.xv)
- 「関連資料」 (P.xii)
- 「通告」 (P.xiii)
- 「マニュアルの入手方法およびテクニカル サポート」 (P.xv)

このマニュアルの目的

この移行マニュアルは、Cisco ISE Release 1.2 のマニュアルセットの一部です。

この移行マニュアルには、以下の情報が含まれています。

- Cisco Secure ACS to Cisco ISE Migration Tool のインストール要件、前提条件、および移行のガイドライン。
- Cisco Secure ACS Release 5.3 の移行可能なデータ項目、および移行不可能なデータ項目の一覧。
- Cisco Secure ACS Release 5.3 データベースから Cisco ISE Release 1.2 アプライアンスヘデータを移行するための段階的な手順。

- Cisco Secure ACS のマニュアルへの参照リンク。これらのリンクでは、Cisco Secure ACS の以前のリリース（リリース 3.x および 4.x）のデータを移行できるようにするためのアップグレードおよび移行手順を定義しています。

Cisco Secure ACS の以前のリリースからの移行

このセクションには、Cisco Secure ACS ソフトウェアの以前のリリースから Cisco ISE Release 1.2 アプライアンスへ、（移行が可能なポイントへの）データ移行を完了させるうえで有用な Cisco Secure ACS のマニュアルへのリンクが含まれています。

はじめる前に

既存の Cisco Secure ACS Release 5.3 のデータを Cisco ISE Release 1.2 アプライアンスへ移行しようとする前に、第 4 章「Cisco Secure ACS to Cisco ISE Migration Tool のインストール」に記載されているすべてのセットアップ、バックアップ、およびインストールの指示について読んで、理解しておく必要があります。

既存の Cisco Secure ACS Release 5.3 のデータを移行する前に、Cisco Secure ACS Release 5.3 システムと Cisco ISE Release 1.2 システムにおける関連データ構造およびスキーマの違いについて、十分に理解しておくことをお勧めします。



(注)

Cisco Secure ACS to Cisco ISE Migration Tool は Cisco Secure ACS Release 5.3 のデータの Cisco ISE Release 1.2 への移行のみサポートしています。

Cisco ISE Release 1.2 アプライアンスへ移行する Cisco Secure ACS データの移行前のリリースによっては、Cisco Secure ACS to Cisco ISE Migration Tool を使用する前に、いくつかの移行ステージが必要な場合があります。

Cisco ISE Release 1.2 アプライアンスへ移行できるように、Cisco Secure ACS の以前のリリースのデータを Cisco Secure ACS Release 5.3 のステートへ移行するには、次の手順を実行する必要があります。

1. 使用環境に Cisco Secure ACS Release 3.x を配置している場合、次の手順を実行する必要があります。
 - a. Cisco Secure ACS Release 3.x のアップグレードパスをチェックします。

Cisco Secure ACS Solution Engine については、次を参照してください：
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.1/installation/guide/solution_engine/upgap.html#wp1120037

Cisco Secure ACS for Windows については、次を参照してください：
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/install.html#wp1102849
 - b. 使用している Cisco Secure ACS Release 3.x サーバを Cisco Secure ACS Release 4.x の移行サポートバージョンアップグレードします。

Cisco Secure ACS Release 4.x の移行サポートバージョンは次のとおりです。

 - Cisco Secure ACS 4.1.1.24
 - Cisco Secure ACS 4.1.4
 - Cisco Secure ACS 4.2.0.124
 - Cisco Secure ACS 4.2.1.

- c. アップグレード後、Cisco Secure ACS Release 4.x から Cisco Secure ACS Release 5.3 への移行方法を示した手順を実行します。(詳細については、『[Migration Guide for the Cisco Secure Access Control System 5.3](#)』を参照してください)。
2. 使用環境に Cisco Secure ACS Release 4.x を配置している場合、次の手順を実行する必要があります。
 - a. Cisco Secure ACS Release 4.x サーバで、現在、移行サポート バージョンのいずれも稼働していない場合は、Cisco Secure ACS Release 4.x バージョンを移行サポート バージョンにアップグレードします。
 - b. 移行マシン (Windows サーバ) に同じ移行サポート バージョンの Cisco Secure ACS をインストールします。
 - c. Cisco Secure ACS Release 4.x データをバックアップして、移行マシンで復元します。
 - d. 移行マシンに移行ユーティリティを保存します。移行ユーティリティは、Installation and Recovery DVD から取得できます。
 - e. 移行マシンで、移行ユーティリティの分析およびエクスポート フェーズを実行します。
 - f. 分析およびエクスポート フェーズで発生した問題を解決します。
 - g. 移行ユーティリティのインポート フェーズを移行マシンで実行し、このフェーズ中にデータを Cisco Secure ACS 5.3 サーバにインポートします。
3. 環境に Cisco Secure ACS Release 5.3 より前の Cisco Secure ACS Release 5.x が配置されている場合は、Cisco Secure ACS Release 5.3 にアップグレードする必要があります。次の URL を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/installation/guide/csacs_upg.html#wp1194843
4. Cisco Secure ACS Release 5.3 へのデータ移行が終了している場合、または最初にデータを Cisco Secure ACS Release 5.3 から移行する場合は、Cisco Secure ACS to Cisco ISE Migration Tool を使用してデータを Cisco ISE Release 1.2 アプライアンスへ移行できます。

対象読者

この移行マニュアルは、Cisco Secure ACS-Cisco ISE Migration Tool を使用して、既存の Cisco Secure ACS Release 5.3 データベース情報を Cisco ISE Release 1.2 アプライアンスへ移行するネットワーク管理者を対象としています。

マニュアルの構成

セクション	説明
第 1 章「Cisco Secure ACS から Cisco ISE へのデータ移行」	Cisco Secure ACS-Cisco ISE の移行の概要について説明し、ソフトウェアの要件、サポートされているリリース、アプリケーション コンポーネント、移行可能なデータ項目、およびソフトウェア アーキテクチャに関する情報を提供します。
第 2 章「Cisco Secure ACS to Cisco ISE Migration Tool について」	Cisco Secure ACS to Cisco ISE Migration Tool の機能について説明します。このツールは、Cisco Secure ACS データのエクスポートおよびインポート、データの持続性、拡張性、ハイ アベイラビリティ、およびレポート機能をサポートしています。
第 3 章「Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 へのデータの移行」	さまざまな導入シナリオ、移行ガイドライン、およびポリシーを移行する方法の詳細を説明します。
第 4 章「Cisco Secure ACS to Cisco ISE Migration Tool のインストール」	Cisco Secure ACS-Cisco ISE Migration Tool の要件、インストールの前提条件、インストールおよびセットアップするためのガイドラインと方法について説明します。
第 5 章「Cisco Secure ACS to Cisco ISE Migration Tool の使用方法」	Cisco Secure ACS-Cisco ISE Migration Tool を使用して、データベースから Cisco Secure ACS Release 5.3 データをエクスポートし、Cisco ISE Release 1.2 アプライアンスへインポートするための方法について説明します。
付録 A「Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のデータ構造マッピング」	Cisco Secure ACS Release 5.3 システムと Cisco ISE Release 1.2 システムの間でデータ オブジェクトをマップする方法について説明します。
付録 B「Cisco Secure ACS to Cisco ISE Migration Tool のトラブルシューティング」	Cisco Secure ACS-Cisco ISE Migration Tool の使用時に発生する可能性のある問題をトラブルシューティングする方法について説明します。

このマニュアルの使用方法

Cisco Secure ACS Release 5.3 のデータを Cisco ISE Release 1.2 アプライアンスへ移行する前に、以下のセクションを読み、参考にしてください。

- 移行する前に Cisco Secure ACS と Cisco ISE 間のデータ オブジェクト、スキーマ、および属性の違いについて理解するには、[付録 A「Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のデータ構造マッピング」](#)を参照してください。
- 異なる展開シナリオで移行を実行する方法、移行ガイドライン、および Cisco ACS から Cisco ISE へポリシーを移行する方法を理解するには、[第 3 章「Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 へのデータの移行」](#)を参照してください。
- Cisco Secure ACS 5.3 のデータベース、データ オブジェクト、アーキテクチャ、およびデータを Cisco ISE Release 1.2 アプライアンスへ移行するプロセスの概要については、[第 1 章「Cisco Secure ACS から Cisco ISE へのデータ移行」](#)を参照してください。
- Cisco Secure ACS Release 5.3 と Cisco ISE Release 1.2 間の違いおよび類似点、特別な設定の推奨事項について理解するには、[第 2 章「Cisco Secure ACS to Cisco ISE Migration Tool について」](#)を参照してください。

- Cisco Secure ACS-Cisco ISE Migration Tool のインストール方法について理解するには、第 4 章「Cisco Secure ACS to Cisco ISE Migration Tool のインストール」を参照してください。
- Cisco Secure ACS-Cisco ISE Migration Tool を使用して、既存の Cisco Secure ACS 5.3 のデータを Cisco ISE Release 1.2 へ移行するのに必要なプロセスを理解するには、第 5 章「Cisco Secure ACS to Cisco ISE Migration Tool の使用方法」を参照してください。

表記法

表記法	説明
bold	コマンド、キーワード、ユーザ入力テキストは 太字 で表示しています。
<i>italic</i>	ドキュメント名、新規用語または強調する用語、値を指定するための引数と変数は、 <i>italic</i> フォントで示しています。
[]	角カッコは次のいずれかを示します。 <ul style="list-style-type: none"> • オプションの要素 • システム プロンプトへのデフォルトの応答
{ x y z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。いずれか 1 つを選択する必要があります。
[x y z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。該当する場合、1 つを選択できます。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier	画面表示、プロンプト、およびスクリプトは、モノスペースの固定幅フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
!#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



注意

「**要注意**」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



(注)

「**注釈**」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

関連資料

リリース固有のマニュアル

表 1 に、Cisco ISE Release で利用可能な製品マニュアルを示します。Cisco ISE の一般的な製品情報については、<http://www.cisco.com/go/ise> から入手できます。エンドユーザー向けマニュアルは、http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html の Cisco.com から入手できます。

表 1 Cisco Identity Services Engine の製品マニュアル

マニュアル名	参照先
『Release Notes for the Cisco Identity Services Engine, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
『Cisco Identity Services Engine Network Component Compatibility, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
『Cisco Identity Services Engine User Guide, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine Hardware Installation Guide, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Upgrade Guide, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine, Release 1.2 Migration Tool ガイド	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine CLI Reference Guide, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine API Reference Guide, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine Troubleshooting Guide, Release 1.2』	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
『Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card』	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html
『My Devices Portal に関する FAQ リリース 1.2』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

プラットフォーム固有のマニュアル

その他のプラットフォーム固有のマニュアルへのリンクは、次の場所で利用できます。

- Cisco ISE
http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html

- Cisco NAC アプライアンス
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 Server
http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html

通告

本ソフトウェア ライセンスに関連する通知内容を以下に示します。

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".
The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed.i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。





Cisco Secure ACS から Cisco ISE へのデータ移行

Cisco Secure Access Control System (ACS) のリリース 5.3 から Cisco Identity Services Engine (ISE) リリース 1.2 へのデータ移行には、最小限のユーザの介入とすべての設定データが必要です。

この章では、次のトピックについて取り上げます。

- 「Cisco Secure ACS から Cisco ISE へのサポートされているデータ移行」 (P.1-1)
- 「Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のポリシー モデル」 (P.1-2)
- 「Cisco ISE および Cisco Secure ACS の導入モデル」 (P.1-3)
- 「移行機能」 (P.1-3)

Cisco Secure ACS から Cisco ISE へのサポートされているデータ移行

Cisco Secure ACS to Cisco ISE Migration Tool を使用した、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのデータ移行がサポートされます。Cisco Secure ACS の以前のリリース (3.x または 4.x) を実行している場合は、を参照してください [「Cisco Secure ACS の以前のリリースからの移行」 \(P.-viii\)](#)。



(注)

各 Cisco Secure ACS または Cisco ISE リリースで動的に変化している機能ギャップのために、すべての Cisco Secure ACS データを Cisco ISE に移行できるわけではありません。Cisco Secure ACS to Cisco ISE Migration Tool には、サポートされていないオブジェクトの完全なリストが含まれています。詳細については、[図 4-1](#) を参照してください。

Cisco Secure ACS Release 5.3 データベースから Cisco ISE Release 1.2 に移行すると、データ移行で次がサポートされます。

- Cisco ISE Release 1.2 で Cisco Secure ACS Release 5.3 の新機能をサポートします。
- データを Cisco Secure ACS Release 5.3 から移行すると、Cisco ISE Release 1.2 の新機能がサポートされます。
- Cisco Secure ACS Release 5.3 と Cisco ISE Release 1.2 の間の設定のギャップを最小します。つまり、データ移行は、Cisco ISE で以前にサポートされていなかった Cisco Secure ACS 機能をサポートします。

表 1-1 Cisco Secure ACS Release から Cisco ISE Release へのサポートされている移行

	Cisco Secure ACS 3.x、4.x、および 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3
Cisco ISE 1.0	非サポート	サポート対象	非サポート	非サポート
Cisco ISE 1.1	非サポート	サポート対象	サポート対象	非サポート
Cisco ISE 1.2	非サポート	非サポート	非サポート	サポート対象

関連項目

Cisco Secure ACS Release 5.3 からのデータの移行については、第 3 章「Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 へのデータの移行」を参照してください。

Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のポリシー モデル

認証ポリシーおよび許可ポリシーは、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へ移行されます。Cisco Secure ACS と Cisco ISE の両方にはシンプルなルール ベースの認証パラダイムがありますが、Cisco Secure ACS と Cisco ISE は異なるポリシー モデルに基づいており、そのため Cisco Secure ACS ポリシーから Cisco ISE への移行が少し複雑になります。

ただし、Cisco ISE Release 1.2 は、Cisco Secure ACS Release 5.3 のサービス セレクション ポリシー (SSP) に類似した、ポリシー セットと呼ばれる新しいポリシー モデルをサポートし、ポリシー移行プロセスの簡素化に役立っています。

Cisco Secure ACS 5.3 と Cisco ISE のポリシー モデルの違い

- Cisco Secure ACS Release 5.3 サービス セレクション ポリシー (SSP) は、SSP のルールに基づいて適切なサービスに要求を配信しますが、Cisco ISE ポリシー セットは、ポリシー セットのエン트리基準を含むルールを保持します。ポリシー セットの順序はエン트리 ルールと同じ順序で、SSP ルールの順序に類似しています。
- サービスを要求せずにポリシー サービスを定義でき、それは、Cisco Secure ACS の SSP ルールによってポリシー サービスを非アクティブと定義できることを意味します。しかし、Cisco ISE のポリシー セットを参照するエン트리 ルールのないポリシー セットを持つことはできません。
- Cisco Secure ACS で SSP ルールを無効またはモニタ対象と定義でき、ポリシー セットの同等のエン트리 ルールは Cisco ISE で常に有効です。SSP ルールが Cisco Secure ACS で無効またはモニタ対象になっている場合、SSP のルールによって要求されたポリシー サービスは Cisco ISE に移行できません。
- 複数の SSP ルールが Cisco Secure ACS で同じサービスまたはサービスの再利用を要求する場合があります。しかし、各ポリシー セットは独自のエン트리条件を持っているので、Cisco ISE でポリシー セットを再利用することはできません。複数の SSP ルールによって要求された 1 つのサービスを移行する場合、そのサービスのコピーである複数のポリシー セットを作成する必要があります。つまり、Cisco Secure ACS で同じサービスを要求する SSP ルールごとに Cisco ISE のポリシー セットを作成する必要があります。

- Cisco Secure ACS Release 5.3 には、既成の DenyAccess サービスがあり、そのサービスは Cisco Secure ACS のデフォルトの SSP ルールの、ポリシーも許可されるプロトコルも持たず、自動的にすべての要求を拒否します。Cisco ISE には同等のポリシー セットはありません。
- ID ポリシーは、Cisco Secure ACS Release 5.3 の ID ソース (ID ソースおよび ID ストア順序) になるルールのフラットなリストです。認証ポリシーは、2 レベルのルール、外部ポリシー ルール、内部ポリシー ルールを保持します。外部ポリシーは許可されるプロトコルになり、内部ポリシー ルールのセットへのエントリ基準です。内部ポリシー ルールは ID ソースになります。
- 許可されるプロトコルは、(特定のポリシーに接続されるのではなく) Cisco Secure ACS Release 5.3 で条件付けられていない (サービス全体を指す SSP の条件を除く) サービス全体に接続されます。許可されるプロトコルは、Cisco ISE で条件付けられた外部ルールの結果としての認証ポリシーだけに適用されます。
- Cisco Secure ACS Release 5.3 および Cisco ISE Release 1.2 の両方に、各許可ポリシーに接続されるオプションの例外ポリシーが含まれます。Cisco ISE Release 1.2 には、例外ポリシーに加えて、すべての許可ポリシーに影響を与えるオプションのグローバル例外ポリシーがあります。Cisco Secure ACS Release 5.3 には、グローバル例外ポリシーに相当するものはありません。許可のために、ローカル例外ポリシーが最初に処理され、続いてグローバル例外ポリシーおよび許可ポリシーが処理されます。

Cisco ISE および Cisco Secure ACS の導入モデル

Cisco Identity Services Engine (ISE) の導入モデルは、1 つのプライマリ ノードと複数のセカンダリ ノードで構成されます。展開内の各 Cisco ISE ノードには、Administration、Policy Service、Monitoring のペルソナいずれか 1 つ以上を設定することができます。Cisco ISE をインストールした後は、すべてのノードがスタンドアロンの状態になります。Cisco ISE ノードのいずれか 1 つを、Administration ペルソナとして稼働するプライマリに定義する必要があります。プライマリ ノードを定義すると、ネットワークに対して、Policy Service ペルソナや Monitoring ペルソナで他の Cisco ISE ノードのペルソナを設定できます。次に、プライマリ ノードに他のセカンダリ ノードを登録し、相互に特定のロールを定義できます。Cisco ISE ノードをセカンダリ ノードとして登録すると、Cisco ISE はプライマリ ノードからセカンダリ ノードへのデータベース リンクをすぐに作成し、複製のプロセスを開始します。すべての設定変更はプライマリの Administration ISE ノード上で行われ、セカンダリ ノードへ複製されます。Monitoring ISE ノードはログ コレクタとして機能します。

Cisco Secure Access Control System (ACS) の導入モデルは、1 つのプライマリ、および複数のセカンダリ Cisco Secure ACS サーバで構成されます。ここで設定の変更は、プライマリ Cisco Secure ACS サーバ上で行われます。これらの設定はセカンダリ Cisco Secure ACS サーバへ複製されます。すべてのプライマリおよびセカンダリ Cisco Secure ACS サーバで AAA 要求を処理できます。プライマリ Cisco Secure ACS サーバは Monitoring Viewer および Report Viewer のデフォルトのログ コレクタでもあります。任意の Cisco Secure ACS サーバをログ コレクタに設定することができます。

移行機能

移行ツールは、Cisco Secure ACS データを Cisco ISE へ転送し、主要な 3 つの手順を実行します。

1. Cisco Secure ACS からデータをエクスポートする。
2. 移行ツール内でデータを保持する。
3. Cisco ISE にデータをインポートする。

Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 への移行プロセスの主な機能は以下のとおりです。

- 「データのエクスポート」 (P.1-4)
- 「データの持続性」 (P.1-4)
- 「データのインポート」 (P.1-4)
- 「オブジェクトの拡張性」 (P.1-4)
- 「ハイ アベイラビリティ」 (P.1-5)
- 「レポート」 (P.1-5)
- 「UTF-8 のサポート」 (P.1-7)
- 「ISE 802.1X サービスに対する FIPS サポート」 (P.1-8)
- 「Cisco Secure ACS/Cisco ISE バージョンの検証」 (P.1-9)

データのエクスポート

移行プロセスの最初のステージは、Cisco Secure ACS の Programmatic Interface (PI) を使用して Cisco Secure ACS データをエクスポートすることです。データのエクスポート元である Cisco Secure ACS Release 5.3 システムへログインし、データを移行アプリケーションにエクスポートするように要求します。エクスポートされたデータを Cisco ISE Release 1.2 アプライアンスへ正常にインポートできるかどうかを確認するために、検証します。データが不正な場合、ステータスがエクスポートレポートに記録されます。

データの持続性

Cisco ISE は、Cisco Secure ACS から Cisco ISE へのアップグレードをサポートしていません。このため、Cisco Secure ACS アプライアンスから Cisco ISE へアップグレードする場合は、Cisco Secure ACS Release 5.3 をアンインストールし、Cisco ISE Release 1.2 メージでアプライアンスを再作成する必要があります。再作成が行われ、インポート ステージが始まる前に、移行ツールは Cisco Secure ACS データを保持します。保持されているデータは、暗号化形式になっています。

データのインポート

インポート ステージでは、移行ツールに Cisco Secure ACS からの情報が含まれており、Cisco ISE へデータをインポートする準備ができています。Cisco ISE をインストールするのに同じマシンを使用する場合は、Cisco ISE Release 1.2 イメージで Cisco Secure ACS マシンを再作成し、インポート操作を開始する必要があります。Cisco ISE に対して別のマシンを使用する場合は、インストール直後でも何も設定されていないクリーンなマシンを使用します。

インポートの進捗を表示するには、Cisco Secure ACS-Cisco ISE Migration Tool のユーザ インターフェイスを使用します。転送中のオブジェクト タイプ、および配信に対して保留中になっているオブジェクトの数を参照できます。このプロセス中のすべてのエラーは、インポート レポートに記録されます。

オブジェクトの拡張性

移行ツールは、表 1-2 に記載されているオブジェクトのスケールをサポートしています。

表 1-2 Cisco Secure ACS から Cisco ISE Release 1.2 への移行に対するオブジェクトの拡張性

オブジェクト	小規模な展開	中規模な展開	大規模な展開
1 つの展開あたりのユーザ (AD ¹ /LDAP ² /内部)	1,000	10,000	25,000
ホスト/エンドポイント	1,000	10,000	100,000
ネットワーク デバイス	500	1,000	10,000
ID グループ	1	5	20
許可プロファイル	5	10	30
ユーザ ディクショナリ	2	5	20
ユーザ属性	1	5	8
ユーザ グループ	2	10	100
DAACL ³ (それぞれ 1,600 エントリ が含まれている)	5	20	50

1. AD は Microsoft Windows Active Directory の頭文字です (Glossary の [Active Directory](#) を参照してください)。
2. LDAP は Lightweight Directory Access Protocol の頭文字です (Glossary の [LDAP](#) を参照してください)。
3. DAACL はダウンロード可能アクセス コントロール リストの頭文字です (Glossary の [DAACL](#) を参照してください)。

ハイ アベイラビリティ

Cisco Secure ACS to Cisco ISE Migration Tool は、インポートまたはエクスポート操作の各ステージのチェックポイントを保持します。これは、インポートまたはエクスポート プロセスが失敗しても、プロセスを最初から再起動する必要がないことを意味します。障害発生前の最後のチェックポイントから開始できます。

移行プロセスが失敗すると、移行ツールはプロセスを終了します。障害の後で移行ツールを再起動すると、ダイアログボックスが表示され、以前のインポートまたはエクスポートを再開するか、または、以前のプロセスを破棄し、新しい移行プロセスを開始するか選択できます。前のプロセスを再開することを選択した場合、移行プロセスは最後のチェックポイントから再開されます。障害が発生した時点から再開する場合、前のプロセスから実行するためにレポートも再開されます。

レポート

3 つの Cisco ISE レポートは、Cisco Secure ACS 5.3 データの移行中に生成されます。レポート ファイルを他のユーザと共有する場合、または他の場所に保存する場合は、移行ツールのディレクトリの Reports フォルダにレポート ファイルがあります。

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

エクスポート レポート : Cisco Secure ACS データベースのデータをエクスポートするときに発生した特定の情報またはエラーについて示します。レポートの最後にはデータ分析のセクションがあり、Cisco Secure ACS と Cisco ISE 間の機能ギャップについて記載されます。エクスポート レポートには、インポートされないエクスポートされたオブジェクトのエラー情報が含まれます。表 1-3 を参照してください。

表 1-3 Cisco Secure ACS to Cisco ISE Migration Tool のエクスポート レポート

レポート タイプ	メッセージタイプ	メッセージの説明
エクスポート	情報	正常にエクスポートされたデータ オブジェクトの名前が示されます。
	警告	エクスポートの障害、または (TACACS ベースのデバイスなど) データ オブジェクトが Cisco ISE Release 1.2 でサポート対象外であるため試行されなかったにエクスポートが示されます。

インポート レポート : Cisco ISE アプライアンスヘデータをインポートするときに発生した特定の情報またはエラーについて示します。表 1-4 を参照してください。

表 1-4 Cisco Secure ACS to Cisco ISE Migration Tool のインポート レポート

レポート タイプ	メッセージタイプ	メッセージの説明
インポート	情報	正常にインポートされたデータ オブジェクトの名前が示されます。
	エラー	データ オブジェクトのエラーの原因を次のように識別します。 <ul style="list-style-type: none"> オブジェクトがすでに存在します オブジェクト名が文字数制限を超えています オブジェクト名にサポートされていない特殊文字が含まれています オブジェクトにサポートされていないデータ文字が含まれています

ポリシー ギャップ分析レポート : Cisco Secure ACS と Cisco ISE 間のポリシー ギャップに関連する特定の情報について示し、エクスポートの完了後に移行ツールのユーザ インターフェイスで [ポリシー ギャップ分析レポート (Policy Gap Analysis Report)] ボタンをクリックして使用できます。図 1-1 を参照してください。

エクスポート フェーズ中に、移行ツールは、認証および許可ポリシーのギャップを識別します。いずれかのポリシーが移行されなかった場合は、ポリシーがポリシー ギャップ分析レポートに記載されます。レポートには、ポリシーに関連して、矛盾するルールおよび条件がすべて記載されます。また、移行できなかったデータ、および手動で対応した理由についても記載されます。

条件の中には、Cisco ISE の用語を使用して自動的に移行できるものがあります。たとえば、「Device Type In」と名付けられた条件は「Device Type Equals」として移行されます。条件がサポートされている場合、または自動的に変換可能な場合は、その条件はレポートには記載されません。「Not Supported」または「Partially supported」として条件が検出された場合、ポリシーはインポートされずに、条件がレポートに記載されます。移行の実施管理者は、責任を持って条件の修正または削除を行う必要があります。それらが修正または削除されない場合、ポリシーは Cisco ISE へ移行されません。

図 1-1 ポリシーギャップ分析レポートの例

```

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

```

UTF-8 のサポート

Cisco ISE Release 1.2 は、いくつかの管理設定に対して 8 ビットの Unicode Transformation Format (UTF-8) をサポートしています。以下の設定項目は、UTF-8 エンコーディングでエクスポートおよびインポートされます。

- ネットワーク アクセスのユーザ設定
 - ユーザ名
 - パスワードおよびパスワードの再入力
 - 名
 - 姓
 - E メール
- RSA : RSA プロンプトおよびメッセージは、サブリカントによってエンドユーザに示されます。
 - メッセージ
 - プロンプト

- **RADIUS トークン** : RADIUS トークン プロンプトは、エンド ユーザのサブリカントに示されま
す。
 - [認証 (Authentication)] タブ > [プロンプト (Prompts)]
 - 管理設定
 - 管理者のユーザ名およびパスワード
 - UTF-8 を使用した管理者の設定
- **ポリシー** :
 - [認証 (Authentication)] > [AV 式の値 (Value for AV expression)]
 - [許可 (Authorization)] > [その他の条件 (Other Conditions)] > [AV 式の値 (Value for AV expression)]
 - 属性 - 値の条件
 - [認証 (Authentication)] > [単純条件 / 複合条件 (Simple Condition/compound Condition)] > [AV 式の値 (Value for AV expression)]
 - [許可 (Authorization)] > [単純条件 / 複合条件 (Simple Condition/compound Condition)] > [AV 式の値 (Value for AV expression)]

ISE 802.1X サービスに対する FIPS サポート

連邦処理標準 (FIPS) をサポートするために、Cisco Secure ACS-Cisco ISE Migration Tool はデフォルトのネットワーク デバイス キーラップ データを移行します。



(注) 移行プロセスを完了する前に、Cisco ISE FIPS モードは有効にしないでください。

FIPS 準拠およびサポートされているプロトコル :

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

FIPS 非準拠およびサポート対象外のプロトコル :

- EAP- メッセージ ダイジェスト 5 (MD5)
- Password Authentication Protocol および ASCII
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)
- Lightweight Extensible Authentication Protocol (LEAP)

Cisco Secure ACS/Cisco ISE バージョンの検証

Cisco Secure ACS to Cisco ISE Migration Tool はエクスポート フェーズを開始する前に、Cisco Secure ACS release のバージョンを特定します。Cisco Secure ACS のバージョンが 5.3 よりも古いかまたは新しい場合、移行プロセスは開始されません。また、Cisco ISE ヘデータをインポートする前に、この移行ツールで Cisco ISE release のバージョンが 1.2 であることを検証します。



Cisco Secure ACS to Cisco ISE Migration Tool について

この章には、Cisco Secure ACS to Cisco ISE Migration Tool に関する情報が記載されています。このツールを使用して、Cisco Secure ACS Release 5.3 データベースから Cisco ISE Release 1.2 アプライアンスへデータを移行します。

この章は、次の章で構成されています。

- [「Cisco Secure ACS to Cisco ISE Migration Tool」 \(P.2-1\)](#)
- [「ソフトウェア要件」 \(P.2-2\)](#)
- [「移行ツールのコンポーネント」 \(P.2-3\)](#)
- [「データ構造マッピング」 \(P.2-4\)](#)

Cisco Secure ACS to Cisco ISE Migration Tool

Cisco Secure ACS to Cisco ISE Migration Tool は、Cisco Secure ACS Release 5.3 データベースがすでにインストールされているユーザに対して、Cisco ISE Release 1.2 アプライアンスへデータを転送するための方法を提供する目的で設計されています。このツールの設計では、ベースとなるハードウェアプラットフォームとシステム、データベース、およびデータスキーマにおける違いによって生じる、特有の移行問題について対処しています。

移行プロセスには、3つの手順があります。

1. Cisco Secure ACS Release 5.3 のデータベースからデータをエクスポートする
2. 移行ツールを使用してデータを保持する
3. 保持しているデータを Cisco ISE Release 1.2 アプライアンスへインポートする

Cisco Secure ACS to Cisco ISE Migration Tool を使用する直接移行プロセスでサポートされているのは、Cisco Secure ACS Release 5.3 システムから Cisco ISE Release 1.2 アプライアンスへの移行のみです。たとえば、Cisco Secure ACS to Cisco ISE Migration Tool を使用して以下のデータ移行手順を実行できます。

1. Cisco Secure ACS-1121 ハードウェア アプライアンスから、データベースを持つセキュアな外部サーバへ Cisco Secure ACS Release 5.3 のデータをエクスポートします。
2. Cisco Secure ACS のデータをバックアップします。
3. Cisco ISE 3315 アプライアンスと同じ物理ハードウェアを持つ Cisco Secure ACS-1121 ハードウェア アプライアンスを、Cisco ISE Release 1.2 ソフトウェアで再作成します。

4. 変換した Cisco Secure ACS 5.3 のデータを、セキュアな外部サーバから Cisco ISE Release 1.2 アプライアンスへインポートします。

Cisco Secure ACS to Cisco ISE Migration Tool は Windows ベースのシステム上で稼働します。このツールは、Cisco Secure ACS のデータ ファイルをインポートし、そのデータを分析して、Cisco ISE Release 1.2 システムで使用可能な形式へデータをインポートするのに必要なデータ修正を行うことによって機能します。

Cisco Secure ACS Release 5.3 および Cisco ISE Release 1.2 のアプリケーションは、同じタイプの物理ハードウェア上で稼働する場合も、稼働しない場合もあります。Cisco Secure ACS-Cisco ISE Migration Tool は、Cisco Secure ACS Programmatic Interface (PI) および Cisco ISE representational state transfer (REST) アプリケーション プログラミング インターフェイス (API) を使用します。Cisco Secure ACS PI および Cisco ISE REST API により、Cisco Secure ACS および Cisco ISE アプリケーションは、サポートされているハードウェア プラットフォームまたは VMware サーバ上で稼働することが可能です。

Cisco Secure ACS はクローズ アプライアンスと見なされているため、Cisco Secure ACS-1121 アプライアンス上で移行ツールを直接稼働させることはできません。代わりに、Cisco Secure ACS PI は ACS 設定データを読み込み、正規化された形式で返します。Cisco ISE REST API は検証を実行し、エクスポートされた Cisco Secure ACS データを正規化して、Cisco ISE ソフトウェアで使用できる形式で保持します。



(注)

移行ツールは、Cisco ISE のフレッシュ インストール後、または **application reset-config** コマンドを使用して Cisco ISE アプリケーションの設定をリセットし、Cisco ISE データベースをクリアした後で実行する必要があります。このため、移行プロセスの完了前は、Cisco ISE FIPS モードを有効にすることはできません。

ソフトウェア要件

Cisco Secure ACS to Cisco ISE Migration Tool を実行する前に、Cisco ISE Release 1.2 へのアップグレードが完了していること、および Cisco Secure ACS Release 5.3 の最新パッチをインストールしていることを確認してください。

表 2-1 は、移行ツールの最小ソフトウェア要件を示します。

表 2-1 Cisco Secure ACS to Cisco ISE Migration Tool のソフトウェア要件

オペレーティング システム	Cisco Secure ACS-Cisco ISE Migration Tool は Windows および Linux マシン上で稼働します。マシンには、Java をインストールしておく必要があります。詳細については、「システム要件」(P.4-2) を参照してください。
最小ディスク領域	必要な最小ディスク領域は 1 GB です。 この領域は、移行ツールのインストールでのみ必要なわけではありません。移行ツールで、移行したデータを保存し、レポートやログを生成する目的でも領域を使用します。
最小構成の RAM	必要な最小 RAM は 2 GB です。 約 300,000 人のユーザ、50,000 個のホスト、50,000 個のネットワーク デバイスを備えている場合、最小 RAM として 2 GB を推奨しています。

移行ツールのコンポーネント

移行ツールは以下のコンポーネントで構成されています。

- 「データ設定」(P.2-3)
- 「ステータス報告」(P.2-3)
- 「エクスポートおよびインポート」(P.2-3)

データ設定

移行プロセスの開始時には、設定データの最小量が必要です。次にアプリケーションは設定項目のフルセットの移行を処理します。プライマリ Cisco Secure ACS サーバおよび Cisco ISE サーバの IP アドレス（またはホスト名）と、管理者のクレデンシャルを入力する必要があります。ユーザが認証されると、Cisco Secure ACS-Cisco ISE Migration Tool は、アップグレードに似た形式で、設定されているデータ項目のフルセットの移行を処理します。

いったん移行プロセスが開始すると、通常それ以降はオペレータは介入する必要はありません。ただし、移行が進捗すると、2つのアプリケーション間でいくつかのデータが自動的にマップされない場合があります。移行を処理する管理者には、このデータのタイプが通知されます。この問題は移行が完了する前に解決する必要があります。

ステータス報告

移行が進捗すると、移行のリアルタイムのステータス、およびアクティビティの進捗をモニタリングできます。トラブルシューティングの場合は、詳細なログを使用することができます。このログには、移行ツール内でアクセスできます。

エクスポートおよびインポート

エクスポートおよびインポートの処理は、個別の処理として実行することも、順番に実行することもできます。エクスポートおよびインポートは、移行されるデータの量によって時間がかかることがあります。そのため、移行ツールは、チェックポイント、および実行中のアクティビティのステータスを定期的に表示します。障害があった場合でも、チェックポイントから移行プロセスを再開できます。

Cisco Secure ACS にコマンドライン インターフェイスにログインし、次のコマンドを入力する必要があります。

```
<acsmachine>/admin# acs config-web-interface migration enable
```

エクスポートおよびデータの持続性

Cisco Secure ACS システムによって認証された後でエクスポート プロセスを開始し、データのエクスポートを要求することができます。

Cisco Secure ACS から Cisco ISE への直接アップグレードはサポートされていません。Cisco Secure ACS Release 5.3 ソフトウェアをアンインストールし、Cisco ISE Release 1.2 ソフトウェアで物理ハードウェアを再作成する場合、Cisco Secure ACS to Cisco ISE Migration Tool が有用です。移行ツールにより、再作成のプロセスが完了してからインポートのステージが開始するまでの間、Cisco Secure ACS のデータが保持されます。

データ分析およびインポート

エクスポート フェーズの間、Cisco Secure ACS to Cisco ISE Migration Tool はデータを読み込んで分析し、これらのデータが Cisco ISE アプライアンス上に正しく作成できることを確認します。Cisco Secure ACS および Cisco ISE Policy のモデルは同じではないため、いくつかのデータは ISE でサポートされない可能性があります。ツールにより、問題がレポートされます。エクスポート フェーズの最後に管理者が介入しなければならない場合があります。

データ構造マッピング

Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのデータ構造マッピングは、エクスポート フェーズ中に、移行ツール内で Cisco Secure ACS to Cisco ISE Migration Tool によってデータ オブジェクトが分析および検証されるプロセスです。エクスポート中に生じるデータ構造マッピングの完全なリストについては、[付録 A 「Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のデータ構造マッピング」](#)を参照してください。



Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 へのデータの移行

データの移行および導入のシナリオ

Cisco Secure ACS と Cisco ISE は別のハードウェア プラットフォーム上に配置され、異なるオペレーティング システム、データベース、および情報モデルを持ちます。このため、Cisco Secure ACS から Cisco ISE へ標準のアップグレードを実行することはできません。代わりに、Cisco Secure ACS to Cisco ISE Migration Tool が Cisco Secure ACS からのデータを読み取り、Cisco ISE に対応するデータを作成します。

シングル アプライアンスにおけるデータ移行プロセスは、分散環境におけるアプライアンスのデータ移行プロセスとは異なります。以降のセクションでは、これらのトピックについてとりあげます。

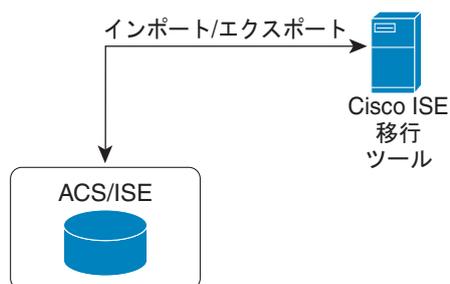
- 「[シングル Cisco Secure ACS アプライアンスからのデータの移行](#)」 (P.3-1)
- 「[分散環境におけるデータの移行](#)」 (P.3-2)

シングル Cisco Secure ACS アプライアンスからのデータの移行

ご使用の環境内にシングル Cisco Secure ACS アプライアンスがある場合（または複数の Cisco Secure ACS アプライアンスがあるが、分散した配置内でない場合）は、「[Cisco Secure ACS データをエクスポートおよびインポートするための移行ツールの使用方法](#)」 (P.5-1) に記載されているように、Cisco Secure ACS-Cisco ISE Migration Tool を Cisco Secure ACS アプライアンスに対して実行します。

図 3-1 は、Cisco ISE Release 1.0 ソフトウェアがインストールされるアプライアンスと同じアプライアンス上に、Cisco Secure ACS 5.1 がインストールされている展開シナリオを示しています（シングルアプライアンス展開）。他の Cisco Secure ACS Release から Cisco ISE リリースへのサポートされている移行については、表 1-1 を参照してください。

図 3-1 シングル アプライアンスにインストールされる Cisco Secure ACS および Cisco ISE



また、Cisco Secure ACS および Cisco ISE が同じハードウェア（CSACS-1121 アプライアンス）を使用している場合も、次の移行手順を使用できます。

-
- ステップ 1** Cisco Secure ACS to Cisco ISE Migration Tool を、スタンドアロンの Windows マシンにインストールします。
 - ステップ 2** Cisco Secure ACS アプライアンスから Cisco Secure ACS Release 5.3 データをエクスポートします。
 - ステップ 3** Cisco Secure ACS のデータをバックアップします。
 - ステップ 4** アプライアンスを Cisco ISE Release 1.2 ソフトウェアで再作成します。
 - ステップ 5** Cisco Secure ACS Release 5.3 のデータを Cisco ISE Release 1.2 アプライアンスへインポートします。
-



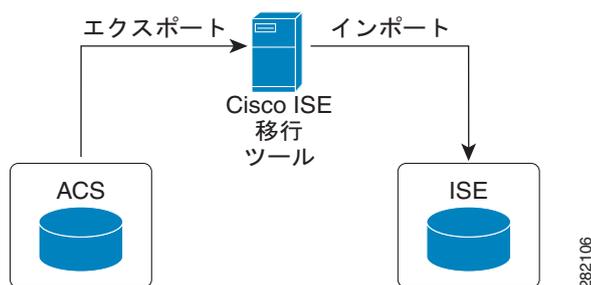
(注) Cisco Secure ACS Release 5.3 のデータを Cisco ISE Release 1.2 アプライアンスへ移行開始する準備ができた場合は、移行先がスタンドアロンの Cisco ISE ノードであることを確認します。移行が正常に終了した後に、何らかの展開設定（Administrator ISE や Policy Service ISE のペルソナなど）を開始することができます。移行のインポート フェーズは、サポートされているハードウェア アプライアンス上で、Cisco ISE ソフトウェアの新しい「クリーンな」インストールにおいて実行する必要があります。サポートされているハードウェア アプライアンスのリストについては、『Cisco Identity Services Engine Hardware Installation Guide, Release 1.2』を参照してください。

分散環境におけるデータの移行

分散環境では、1 つのプライマリ Cisco Secure ACS アプライアンス、およびこのプライマリ アプライアンスと相互運用する 1 つ以上のセカンダリ Cisco Secure ACS アプライアンスがあります。

図 3-2 は、Cisco Secure ACS および Cisco ISE が異なるアプライアンスにインストールされている場合の展開シナリオについて説明しています（デュアルアプライアンス展開）。

図 3-2 異なるアプライアンスにインストールされている Cisco Secure ACS および Cisco ISE



分散環境で Cisco Secure ACS を実行する場合は、以下のようにする必要があります。

-
- ステップ 1** プライマリ Cisco Secure ACS アプライアンスをバックアップし、それを移行マシン上で復元します。
 - ステップ 2** プライマリ Cisco Secure ACS アプライアンスに対して Cisco Secure ACS to Cisco ISE Migration Tool を実行します。
-



(注) 大規模な内部データベースがある場合、シスコではスタンドアロンのプライマリ アプライアンスから移行を実行し、複数のセカンダリ アプライアンスへ接続されているプライマリ アプライアンスへの移行は実行しないことを推奨しています。移行プロセスの完了後、セカンダリ アプライアンスを登録できます。



(注) Cisco Secure ACS-Cisco ISE Migration Tool は約 20 時間稼働して、10,000 個のデバイス、25,000 人のユーザ、100,000 個のホスト、100 個の ID グループ、420 個のダウンロード可能アクセス コントロール リスト (DACL)、320 個の許可プロファイル、6 個のデバイス階層、および 20 個のネットワーク デバイス グループ (NDG) を移行することができます。

Cisco Secure ACS データの Cisco ISE への移行

Cisco Secure ACS と Cisco ISE は異なるポリシー モデルに基づいています。Cisco Secure ACS データが Cisco ISE に移行されると、その部分の間にギャップが常に存在します。

一般的に、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へデータを移行する場合に、以下の移行ルールを考慮する必要があります。

- 特殊文字は移行されない。
- enum 型の属性 (RADIUS、VSA、ID、およびホスト) は、使用可能な値を持つ整数として移行される。
- (属性のデータ型に関係なく) すべてのエンドポイント属性は String データ型として移行される。
- Cisco ISE ログに追加される RADIUS 属性および VSA 値をフィルタすることはできない。

ポリシー規則の検証

Cisco Secure ACS と Cisco ISE のポリシー モデルは異なるので、バージョンが変わると、次の理由のためにすべての Cisco Secure ACS ポリシーおよび規則を移行できるとは限りません。

- ポリシーで使用されている属性がサポートされていない
- 構造がサポートされていない、または条件付きである (大半は、以前に複雑な条件が設定されている)
- 演算子がサポートされていない

ルールが移行できない場合、データ整合性だけでなく、セキュリティ面のために、全体としてのポリシー モデルは移行できませんでした。ポリシーのギャップ分析レポートで問題のあるルールの詳細情報を表示できます。サポート対象外のルールを修正または削除しない場合、ポリシーは Cisco ISE へ移行されません。

表 3-1 サポートされていない規則要素

規則要素	サポート対象	説明
日時	非サポート	反復的な週次設定を持つ許可ポリシー内の日時条件は、Cisco ISE へ移行されません。結果として、ルールも移行されません。
日時	非サポート	認証ポリシー内の日時条件は Cisco ISE へ移行されません。結果として、ルールも移行されません。
In	一部サポートあり	「In」オペランドは階層に使用され、「Is」は文字列タイプのみで使用されます。これは「Matches」を使用して変換することができます。
Not In	一部サポートあり	「Not in」オペランドは階層に使用され、「Is」は文字列タイプのみで使用されます。これは「Matches」を使用して変換することができます。
Contains Any	一部サポートあり	「Contains Any」オペランドは、Active Directory および Lightweight Directory Access Protocol などの外部グループにのみ使用されます。
Contains All	非サポート	「Contains All」オペランドは、Active Directory および Lightweight Directory Access Protocol などの外部グループにのみ使用されます。
論理式の組み合わせ	非サポート	条件内でこれらのオペランドを使用しているルールは移行されません。 <ul style="list-style-type: none"> • a b c ... や a && b && c && ... 以外の論理式 ((a b) && c など) を持つ複合条件が含まれている認証ポリシー。 • a && b && c && 以外のローカル式を持つ複合条件が含まれている許可ポリシーは、ルール条件の一部として移行されません。代わりに、いくつかの高度な論理式に対してライブラリ複合条件を手動で使用することができます。
ネットワーク条件	非サポート	ネットワーク条件のみが含まれているルールは移行されません。条件にネットワーク条件、およびサポート対象の他の条件が含まれている場合、ネットワーク条件は無視され、ルール条件の一部として移行されません。
ユーザ属性	一部サポートあり	データ型が「String」以外のユーザ属性を含む条件付きルールは移行されません。

表 3-1 サポートされていない規則要素 (続き)

規則要素	サポート対象	説明
ホスト属性	非サポート	条件でホスト属性を参照している場合、認証は失敗します。 ホスト (エンドポイント) 属性を持つ条件が含まれている許可ポリシーは、Cisco ISE 許可ポリシーへ移行されません。
TACACS 属性	非サポート	Cisco ISE は、Terminal Access Controller Access-Control System (TACACS) をサポートしません。TACACS 属性を使用する Cisco Secure ACS サービス セレクション ポリシー ルールは移行されません。

Cisco Secure ACS Release 5.3 からの移行の準備

Cisco ISE Release 1.2 のポリシー セット モードでのみ Cisco Secure ACS Release 5.3 データを移行する必要があります。

Cisco Secure ACS から正常に移行した後に簡易モードに変更しないことを推奨します。Cisco ISE に移行されたすべてのポリシーが失われる可能性があるからです。それらの移行されたポリシーを取得することはできませんが、簡易モードからポリシー セット モードに切替えることができます。

Cisco Secure ACS データを Cisco ISE に移行し始める前に、次のことを考慮してください。

- Cisco ISE Release 1.2 の新規インストール上に移行します。
- サービス セレクション ポリシー (SSP) の有効なルールごとに 1 つのポリシー セットを生成し、SSP のルール順序に従って順序付けします。



(注) SSP のデフォルト規則の結果であるサービスは、Cisco ISE Release 1.2 で設定されたデフォルトポリシーになります。移行プロセスで作成されたすべてのポリシー セットで、最初の一一致ポリシー セットが一致タイプになります。

ポリシー サービスの移行のガイドライン

Cisco Secure ACS から Cisco ISE へのポリシー サービスの移行を確実にするには、次を確認する必要があります。

- Cisco Secure ACS Release 5.3 で無効またはモニタになっている SSP ルールを持つサービス セレクション ポリシー (SSP) がある場合、それらは Cisco ISE に移行されません。
- Cisco Secure ACS Release 5.3 のデバイス管理サービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。Cisco ISE は、デバイス管理をサポートしていません。
- Cisco Secure ACS Release 5.3 のプロキシサービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。プロキシ サービスを実装する Cisco ISE は異なります。
- Cisco Secure ACS Release 5.3 のグループ マッピング ポリシーを含むネットワーク アクセス サービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。Cisco ISE は、グループ マッピング ポリシーをサポートしません。

- ID ポリシーに Cisco Secure ACS Release 5.3 の RADIUS ID サーバになるルールが含まれるサービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。認証に RADIUS ID サーバを使用する Cisco ISE は異なります。
- Cisco Secure ACS Release 5.3 の属性またはポリシー要素を使用するポリシーを含むサービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。

ポリシー サービスごとの移行のガイドライン

はじめる前に

「Cisco Secure ACS Release 5.3 からの移行の準備」(P3-5) を参照してください。

- Cisco ISE のサービスの名前を使用してポリシー セットを作成できます。ポリシー セットが Cisco Secure ACS Release 5.3 の SSP デフォルト規則の結果であるサービスに一致する場合、ポリシー セットは Cisco ISE Release 1.2 のデフォルトのポリシー セットになります。
- Cisco Secure ACS Release 5.3 の SSP ルールの条件は、Cisco ISE Release 1.2 のポリシー セットのエン트리条件になります。Cisco ISE Release 1.2 のデフォルトのポリシー セットの場合、必要なエン트리条件はありません。
- Cisco Secure ACS Release 5.3 の DenyAccess サービスを Cisco ISE Release 1.2 に変換すると、認証および許可ポリシーが次のように変更されます。
 - 許可ポリシーでのみ、結果を持つデフォルトの外部ルールが、許可されるプロトコルに対して Default Network Access に設定され、ID ソースに対して DenyAccess に設定されます。
 - 許可ポリシーでのみ、デフォルトのルール セットが DenyAccess に設定されます (標準権限)。
- Cisco Secure ACS Release 5.3 のサービスの ID ポリシーを、Cisco ISE Release 1.2 のポリシー セットの許可ポリシーに変換する場合、次の手順を実行します。
 - 単一で有効な外部ルールを持つ許可ポリシーを作成します。
 - 外部ルールの条件をデバイスとして指定します。場所はすべての場所で開始します (これは常に一致した条件です)。
 - デフォルトの外部ルールの結果を、許可されるプロトコルに対して Default Network Access に設定し、ID ソースに対して DenyAccess に設定します。

外部ルールの結果は、関連するサービスの許可されたプロトコルです。認証ポリシーの内部ルールは、関連する ID ポリシーのルールです。認証ポリシーの内部ルールの順序は、関連する ID ポリシーのルールと同じ順序に従います。認証ポリシーの内部ルールの状態 (有効、無効、またはモニタ) は、関連する ID ポリシー規則の状態に従います。

- Cisco Secure ACS Release 5.3 のサービスの許可ポリシーを、Cisco ISE Release 1.2 のポリシー セットの許可ポリシーに変換する場合、
 - ローカル例外許可ポリシーのポリシー セットのルールは、関連するサービスの例外許可ポリシーのルールです。
 - 許可ポリシーのポリシー セットのルールは、関連するサービスの許可ポリシーのルールです。
 - ローカル例外許可ポリシーおよび許可ポリシーのポリシー セットのルールの順序は、関連するサービスのローカル例外許可ポリシーおよび許可ポリシーのルールの順序に従います。
 - ローカル例外許可ポリシーおよび許可ポリシーのポリシー セットのルールの状態 (有効、無効、モニタ) は、関連するサービスのローカル例外許可ポリシーおよび許可ポリシーのルールの状態に従います。



Cisco Secure ACS to Cisco ISE Migration Tool のインストール

この章では、Cisco Secure ACS to Cisco ISE Migration Tool をインストールする方法について説明します。

この章では、次のトピックについて取り上げます。

- 「移行ツールのインストール ガイドライン」 (P.4-1)
- 「システム要件」 (P.4-2)
- 「セキュリティの考慮事項」 (P.4-2)
- 「Cisco Secure ACS-Cisco ISE Migration Tool のインストールおよび初期化」 (P.4-3)

移行ツールのインストール ガイドライン

はじめる前に

- ご使用の環境で、移行する準備ができていることを確認してください。Cisco Secure ACS Release 5.3 Windows または Linux のソース マシン以外に、シングルアプライアンスまたはデュアルアプライアンスの移行用の 1 つのデータベースを備えたセキュアな外部システムを展開し、ターゲットシステムとして、Cisco ISE Release 1.2 アプライアンスを持つ必要があります。
- Cisco Secure ACS Release 5.3 のソース マシンにシングル IP アドレスが設定されていることを確認してください。各インターフェイスが複数の IP アドレス エイリアスを持つ場合、移行のときに移行ツールは失敗します。
- Cisco Secure ACS から Cisco ISE への移行が同じアプライアンス上で実行される場合は、データのバックアップが作成されていることを確認してください。
- 以下のタスクが完了していることを確認してください。
 - デュアルアプライアンスの移行の場合、ターゲット マシンに Cisco ISE Release 1.2 ソフトウェアをインストールしている。
 - シングルアプライアンスの移行の場合、CSACS-1121 アプライアンスを再作成するのに使用できる Cisco ISE Release 1.2 のソフトウェアがある。
 - Cisco Secure ACS Release 5.3 と Cisco ISE Release 1.2 の適切なクレデンシャルおよびパスワードをすべて保持している。
- ソース マシンと、セキュアな外部システム間でネットワーク接続を確立できることを確認します。

関連項目

次を参照してください。第 5 章「Cisco Secure ACS to Cisco ISE Migration Tool の使用方法」

システム要件

Cisco Secure ACS マシンは表 4-1 に説明するシステム要件を満たしている必要があります。すべてのマニュアルは Cisco.com で入手できます。

表 4-1 移行マシンのシステム 要件

プラットフォーム	要件
Cisco Secure ACS Release 5.3 ソース マシン	『 Installation and Upgrade Guide for the Cisco Secure Access Control System 5.3 』を参照してください。Cisco Secure ACS Release 5.3 のソース マシンにシングル IP アドレスが設定されていることを確認します。
Cisco ISE Release 1.2 ターゲット マシン	『 Cisco Identity Services Engine Hardware Installation Guide, Release 1.2 』を参照してください。このアプライアンスでは、最低 2 GB の RAM が必要です。
Linux、Windows XP	Java JRE バージョン 1.6 以降の 32 ビットをインストールします。移行マシン上に Java JRE がインストールされていない場合は、移行ツールは機能しません。
64 ビット版 Windows 7	Java JRE バージョン 1.6 以降の 64 ビットをインストールします。移行マシン上に Java JRE がインストールされていない場合は、移行ツールは機能しません。
32 ビット版 Windows 7	Java JRE バージョン 1.6 以降の 32 ビットをインストールします。移行マシン上に Java JRE がインストールされていない場合は、移行ツールは機能しません。

セキュリティの考慮事項

移行プロセスのエクスポート フェーズでは、インポート プロセスの入力として使用されるデータ ファイルが作成されます。データ ファイルの内容は暗号化され、直接読み取ることはできません。

ユーザは、Cisco Secure ACS データをエクスポートし、それを Cisco ISE アプライアンスへ正常にインポートするために、Cisco Secure ACS Release 5.3 および Cisco ISE Release 1.2 の管理者のユーザ名およびパスワードを知っている必要があります。インポート ユーティリティによって作成されたレコードを監査ログ内で識別できるように、予約済みユーザ名を使用する必要があります。

Cisco Secure ACS-Cisco ISE Migration Tool のインストールおよび初期化



(注)

Cisco Secure ACS to Cisco ISE Migration Tool は、Cisco ISE のフレッシュインストール後、または **application reset-config** コマンドを使用して Cisco ISE アプリケーションの設定をリセットし、Cisco ISE データベースをクリアした後で実行する必要があります。このため、移行プロセスの完了前は、Cisco ISE FIPS モードを有効にすることはできません。

Cisco ISE ユーザ インターフェイスを使用して Cisco Secure ACS to Cisco ISE Migration Tool ファイルをダウンロードすることができます。

Cisco Secure ACS to Cisco ISE Migration Tool ソフトウェアをダウンロードして実行するには、以下の手順を完了します。

- ステップ 1** Cisco Secure ACS ソフトウェアおよび Cisco ISE ソフトウェアが複数のアプライアンスにインストールされている場合は、Cisco ISE ユーザ インターフェイスのアドレス バーで以下の URL を入力して移行ツールをダウンロードします。

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



(注)

移行ツール ファイルのダウンロードで現在サポートされているブラウザは、Mozilla Firefox バージョン 3.6、6、7、8、9、および 10 のみです。Microsoft Windows Internet Explorer (IE8 および IE7) ブラウザは、このリリースでは現在サポートされていません。

Cisco Secure ACS ソフトウェアおよび Cisco ISE ソフトウェアが同じアプライアンスに存在する場合、または新しい Cisco ISE ハードウェア アプライアンスを使用している場合は、Cisco ISE Release 1.2 の最新の migTool.zip を以下の場所からダウンロードします。

<http://software.cisco.com/download/release.html?mdfid=283801620&flowid=26081&softwareid=283802505&release=1.2>

- ステップ 2** .zip ファイルを解凍します。.zip ファイルから解凍された内容は、config.bat および migration.bat ファイルを保持するディレクトリ構造を作成します。

- ステップ 3** config.bat ファイルを編集して、移行プロセス用の Java ヒープ サイズに割り当てるメモリの初期量を設定します。メモリは、それぞれ 64 メガバイト、512 メガバイトにします。config.bat でヒープ サイズを設定する属性と値は次のとおりです。_Xms = 64 および _Xmx = 512。

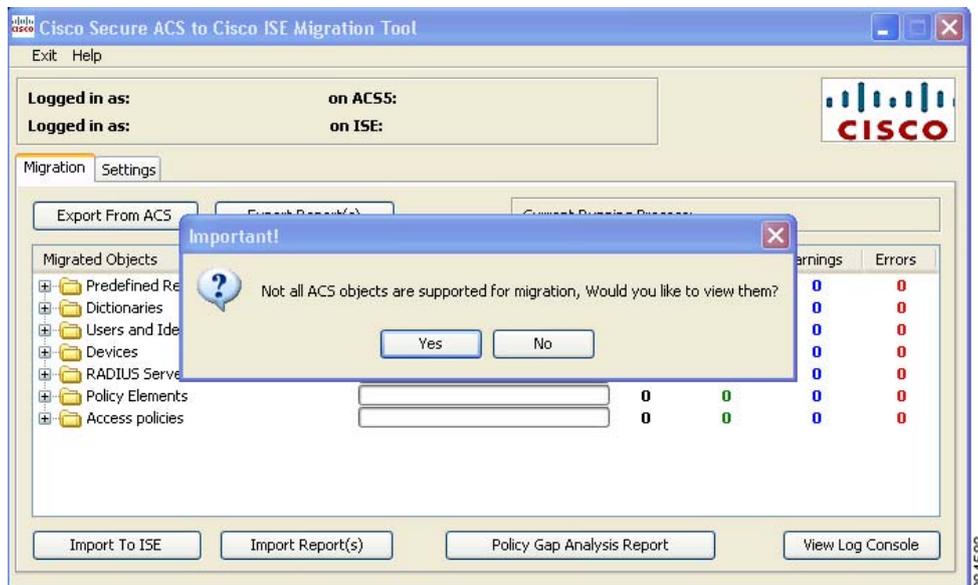
- ステップ 4** [保存 (Save)] をクリックします。

- ステップ 5** migration.bat をクリックして移行プロセスを起動します。

初期化画面が表示されます。

移行ツールは、Cisco Secure ACS オブジェクトのサブセットのみを Cisco ISE に移行できます。ツールは、移行できない、サポートされていない（または一部しかサポートされていない）オブジェクトのリストを提供します。移行ツールが初期化されるときに、この未サポートのリストを表示するかどうかを確認するメッセージボックスが表示されます。図 4-1 を参照してください。

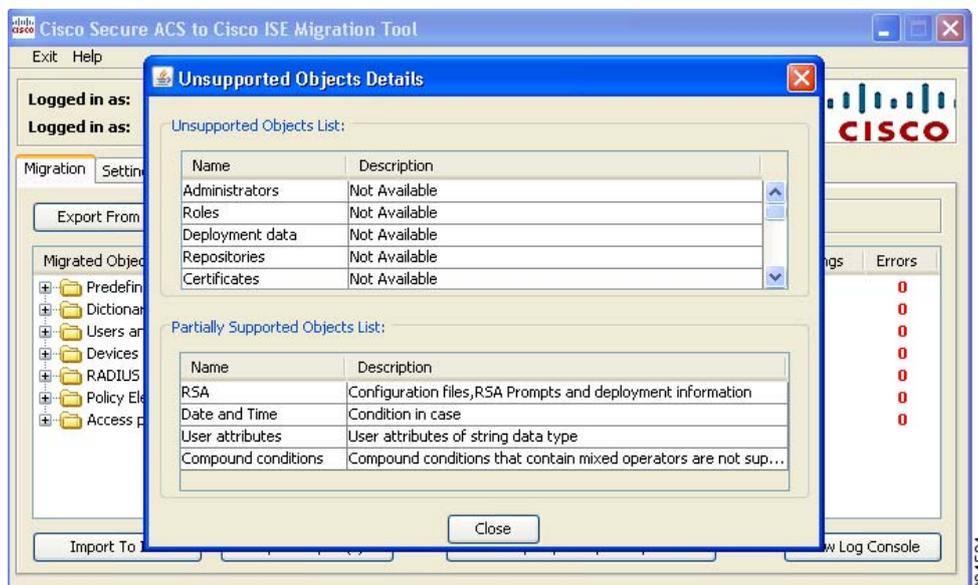
図 4-1 サポートされていないオブジェクトで表示されるメッセージ



ステップ 6 [はい (Yes)] をクリックして、サポートされていないオブジェクト、および一部しかサポートされていないオブジェクトのリストを表示します。図 4-2 を参照してください。

Cisco Secure ACS to Cisco ISE Migration Tool で [ヘルプ (Help)] > [未サポート オブジェクトの詳細 (Unsupported Object Details)] を選択して、サポートされていないオブジェクトのリストを表示することもできます。

図 4-2 未サポートおよび一部サポートのオブジェクトのリスト



ステップ 7 [閉じる (Close)] をクリックします。



Cisco Secure ACS to Cisco ISE Migration Tool の使用方法

この章では、Cisco Secure ACS to Cisco ISE Migration Tool を使用して、Cisco Secure ACS 5.3 のデータを Cisco ISE Release 1.2 アプライアンスにエクスポートおよびインポートする方法について説明します。

この章では、次の事項について説明します。

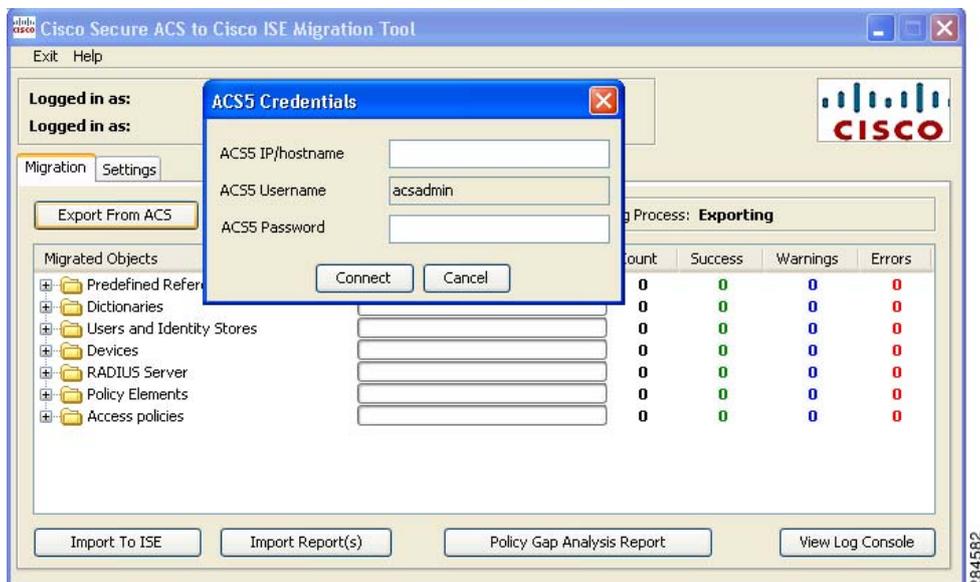
- 「Cisco Secure ACS データをエクスポートおよびインポートするための移行ツールの使用方法」 (P.5-1)
- 「Cisco ISE に移行されたデータの確認」 (P.5-8)

Cisco Secure ACS データをエクスポートおよびインポートするための移行ツールの使用方法

移行ツールを開始した後で、データのエクスポート元である Cisco Secure ACS Release 5.3 システムへログインします。移行ツールの使用を開始するには、以下の手順を完了します。

- ステップ 1** [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで [設定 (Settings)] をクリックして、移行に使用できるデータ オブジェクトのリストを表示します。
- ステップ 2** (任意) データの移行を実行するために、依存関係処理を設定する必要はありません。従属データがない場合は、エクスポートするデータ オブジェクトのチェック ボックスをオンにして、[保存 (Save)] をクリックします。
- ステップ 3** [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで [移行 (Migration)] をクリックし、[ACS からのエクスポート (Export from ACS)] をクリックします。
- ステップ 4** [ACS5 クレデンシヤル (ACS5 Credential)] ウィンドウに Cisco Secure ACS Release 5.3 システムの IP アドレス (またはホスト名) とパスワードを入力して [接続 (Connect)] をクリックします。

図 5-1 Cisco Secure ACS への接続



ステップ 5 [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで移行プロセスをモニタします。ウィンドウには、正常にエクスポートされた現在のオブジェクト数、およびデータの移行プロセスの開始後警告やエラーの原因となったオブジェクトが表示されます。

図 5-2 Cisco Secure ACS オブジェクトのエクスポート

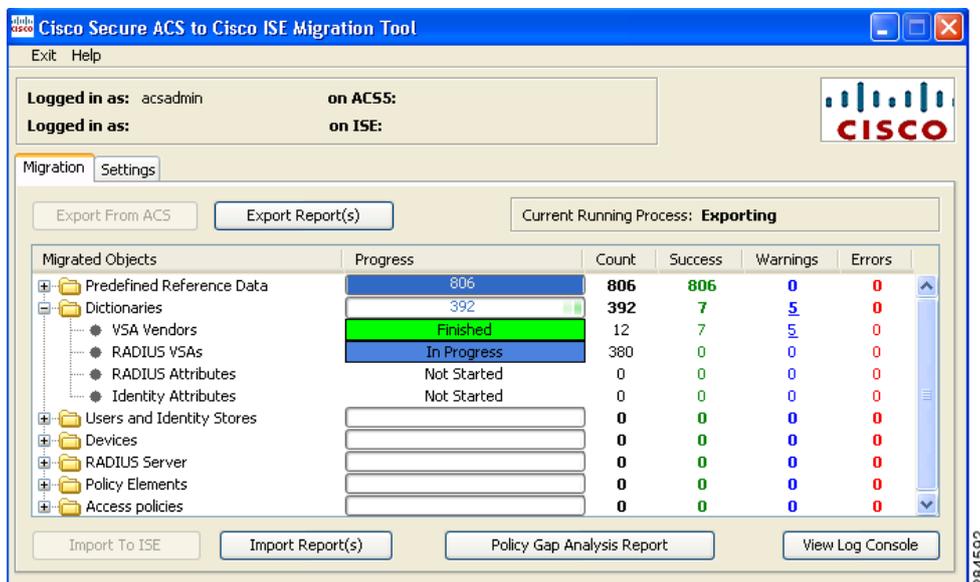
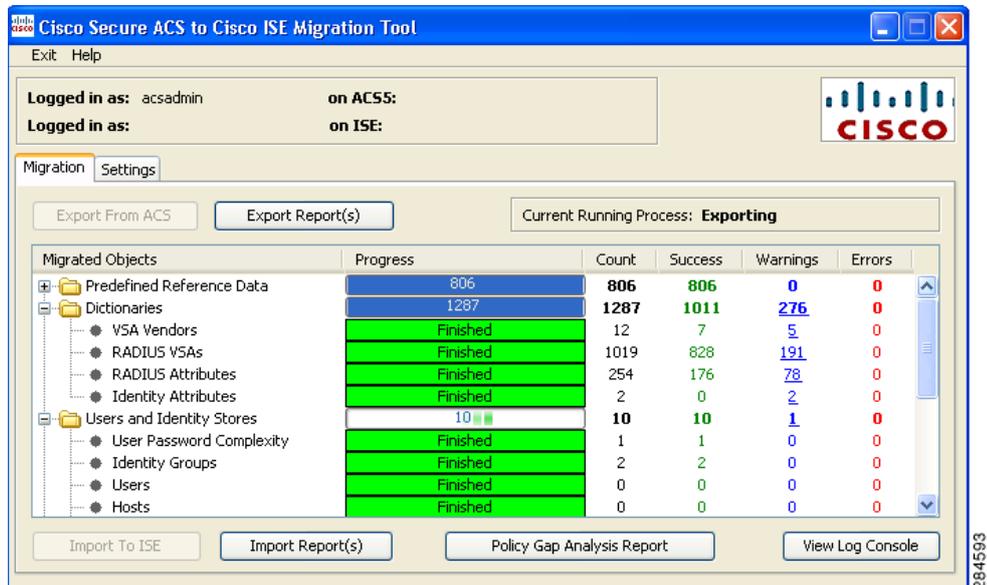


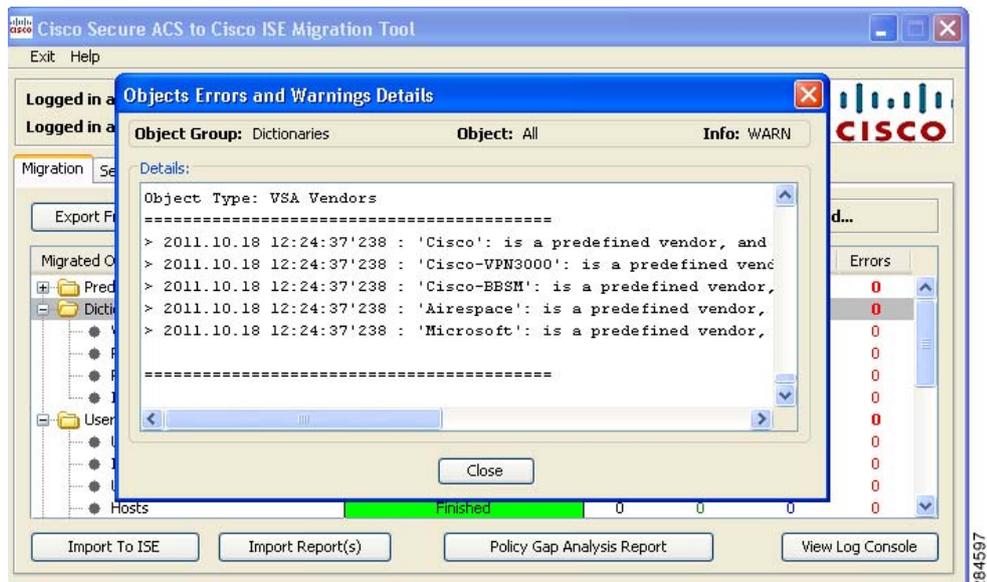
図 5-3 Cisco Secure ACS オブジェクトのエクスポートの終了



ステップ 6 エクスポートプロセスで発生した警告またはエラーについては、[移動 (Migrations)] タブの [警告 (Warnings)] または [エラー (Errors)] カラムで下線の付いた数字をクリックします。

[オブジェクトエラーと警告の詳細 (Object Errors and Warnings Details)] ウィンドウに、エクスポート中に発生した警告またはエラーの結果が表示されます。つまり、警告またはエラーのオブジェクトグループ、タイプ、および日時が表示されます。

図 5-4 オブジェクトエラーと警告の詳細の表示

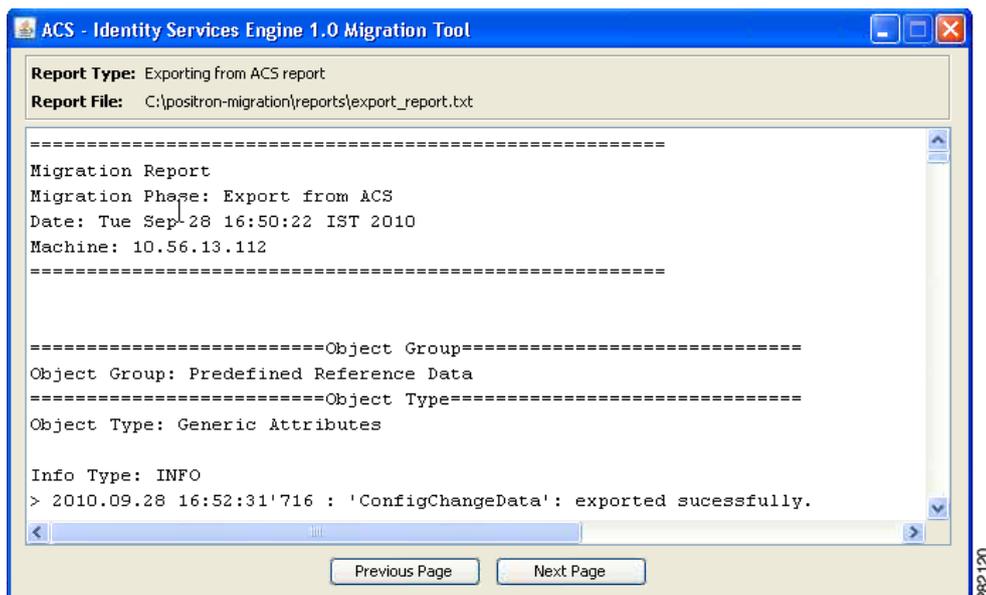


ステップ 7 スクロールして、選択したオブジェクトのエラーの詳細を表示し、[閉じる (Close)] をクリックしてします。

Cisco Secure ACS データをエクスポートおよびインポートするための移行ツールの使用方法

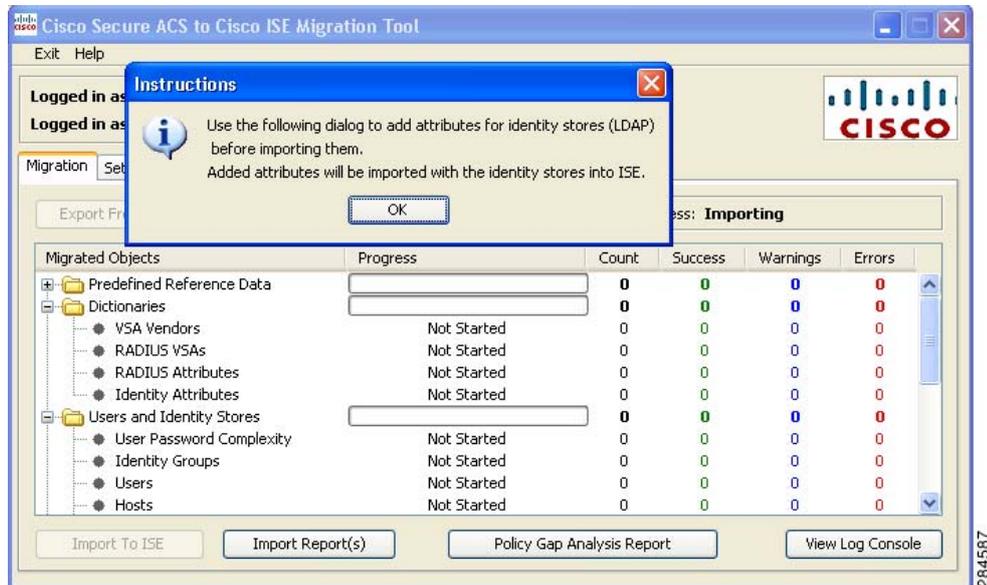
- ステップ 8** データ エクスポート プロセスが完了したら、[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウに、エクスポートが終了したときのエクスポートのステータスが表示されます。
- ステップ 9** エクスポートされたデータの完全なレポートを表示するには、[エクスポート レポート (Export Report(s))] をクリックします。

各エクスポート レポートには、ヘッダー情報、および処理のタイプ、日時、およびシステムの IP アドレスまたはホスト名が含まれています。各オブジェクト グループは、タイプおよび関連情報を詳しく説明します。レポートの最後には、開始と終了の日時、および処理の期間のサマリーが付随しています。



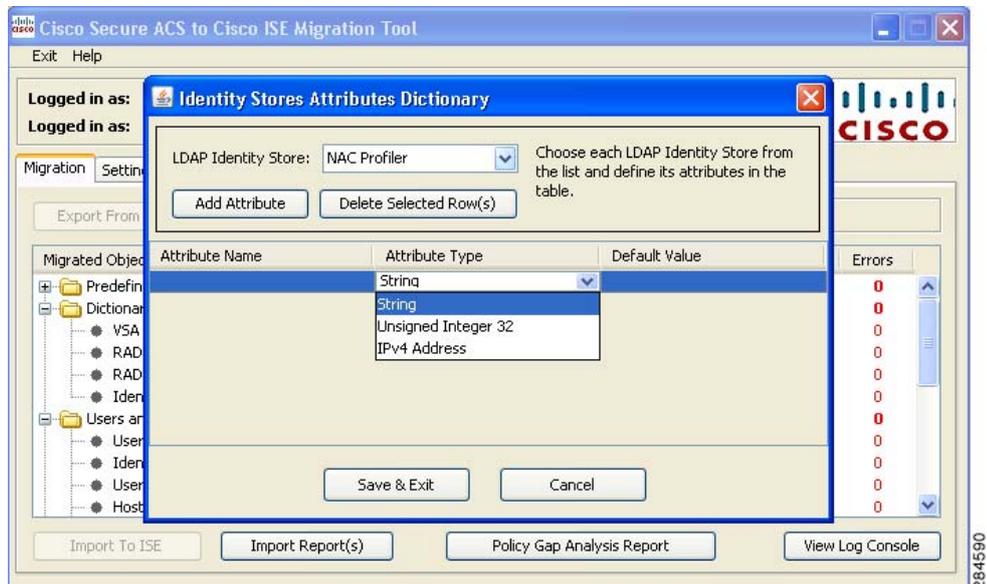
- ステップ 10** Cisco ISE にデータのインポートを開始するには、[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで [ISE へのインポート (Import to ISE)] をクリックします。
- ステップ 11** データを Cisco ISE へインポートする前に、LDAP ID ストアに属性を追加するようプロンプトが表示されたら、[OK] をクリックします。

図 5-5 ID ストアへの属性の追加



ステップ 12 [LDAP ID ストア (LDAP Identity Store)] ドロップダウン リストで、属性を追加する ID ストアを選択し、[属性の追加 (Add Attribute)] をクリックします。

図 5-6 ID ストア属性ディクショナリ



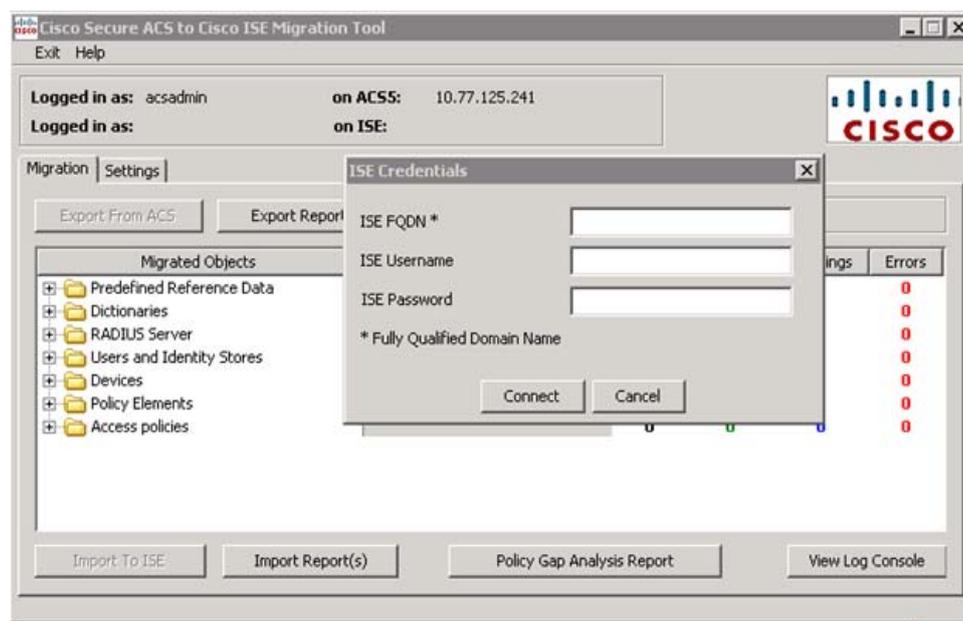
ステップ 13 [属性名 (Attribute Name)] フィールドに名前を入力し、[属性タイプ (Attribute Type)] ドロップダウン リストから属性タイプを選択します。[デフォルト値 (Default Value)] フィールドに値を入力して [保存して終了 (Save & Exit)] をクリックします。

ステップ 14 属性の追加が終了したら、[ISE へのインポート (Import To ISE)] をクリックします。

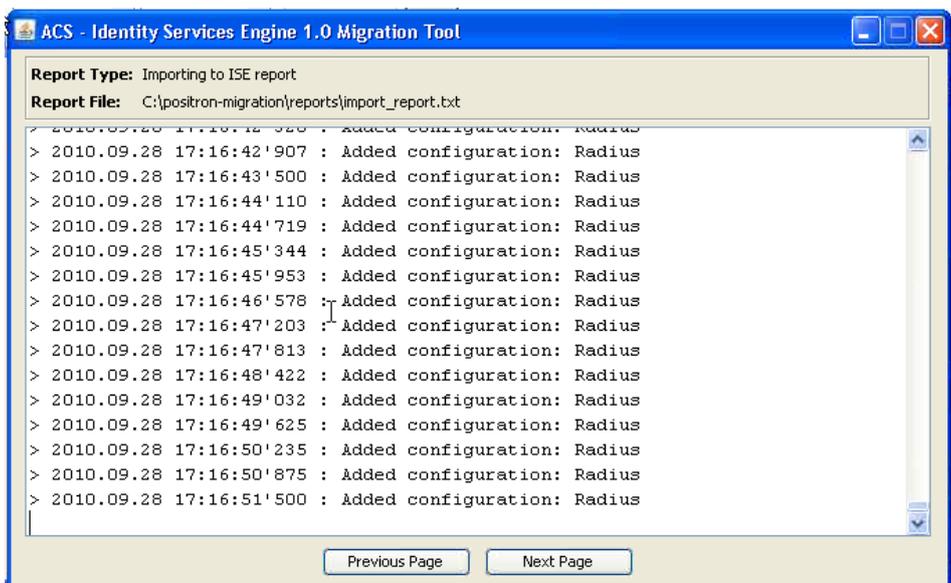
ステップ 15 [ISE クレデンシャル (ISE Credentials)] ウィンドウに、Cisco ISE の完全修飾ドメイン名 (FQDN)、ユーザ名、およびパスワードを入力し、[接続 (Connect)] をクリックします。移行ツールは FQDN をチェックし、SSL 証明書に書き込まれた FQDN と一致することを確認します。

データ インポート プロセスが完了したら、[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウに、インポートが終了したときのインポートのステータスが表示されます。

図 5-7 Cisco ISE への接続



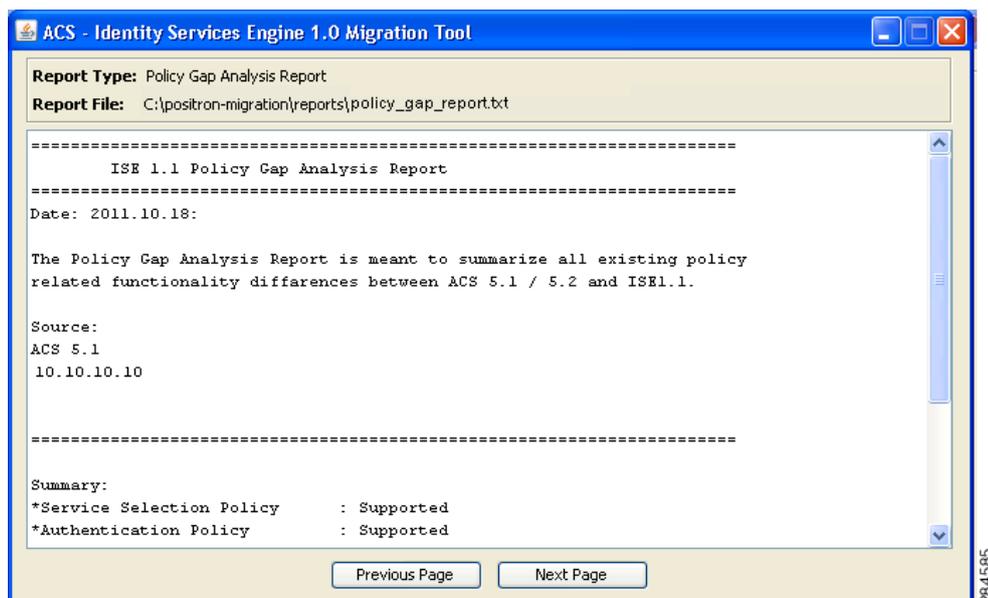
ステップ 16 インポートされたデータの完全なレポートを表示するには、[インポート レポート (Import Report(s))] をクリックします。



ステップ 17 インポートプロセスで発生した警告またはエラーについては、[移動 (Migrations)] タブの [警告 (Warnings)] または [エラー (Errors)] カラムで下線の付いた数字をクリックします。ステップ 6 を参照してください。

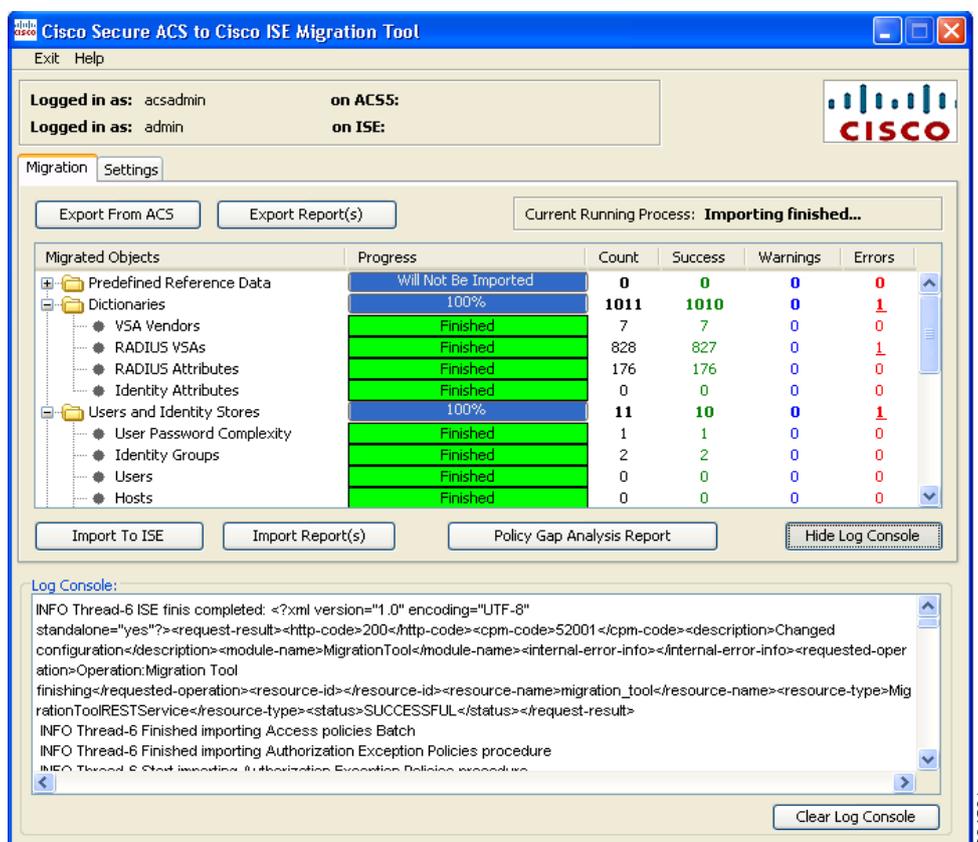
ステップ 18 Cisco Secure ACS と Cisco ISE 間のポリシー ギャップを分析するには、[ポリシー ギャップ分析レポート (Policy Gap Analysis Report)] をクリックします。

図 5-8 ポリシー ギャップ分析レポート



ステップ 19 [ログ コンソールの表示 (View Log Console)] をクリックすると、いつでもエクスポートまたはインポート処理のリアルタイム ビューを表示できます。

図 5-9 ログ コンソールの表示



Cisco ISE に移行されたデータの確認

Cisco ISE にログインし、さまざまな Cisco Secure ACS オブジェクトが Cisco ISE に移行されたことを確認できます。



Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のデータ構造マッピング

この付録では、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 に移行される、一部が移行される、および移行されないデータ オブジェクトが含まれる機能ギャップについて説明します。

この付録では、以下の移行関連のトピックについて説明します。

- 「移行されるデータ オブジェクト」 (P.A-1)
- 「移行されないデータ オブジェクト」 (P.A-2)
- 「一部が移行されるデータ オブジェクト」 (P.A-3)
- 「サポート対象属性およびデータ型」 (P.A-3)
- 「データ情報マッピング」 (P.A-5)

移行されるデータ オブジェクト

以下のデータ オブジェクトは、Cisco Secure Access Control System (ACS) から Cisco Identity Services Engine (ISE) に移行されます。

- ネットワーク デバイス グループ (NDG) タイプと階層
- ネットワーク デバイス
- デフォルト ネットワーク デバイス
- 外部 RADIUS サーバ
- ID グループ
- 内部ユーザ
- 内部エンドポイント (ホスト)
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory (AD)
- RSA (一部サポート、表 A-25 を参照)
- RADIUS トークン (表 A-24 を参照)
- 証明書認証プロファイル
- 日付と時間の条件 (一部サポート、「ポリシー規則の検証」 (P.3-3) を参照)
- RADIUS 属性およびベンダー固有属性 (VSA) の値 (表 A-5 および 表 A-6 を参照)

■ 移行されないデータ オブジェクト

- RADIUS ベンダー ディクショナリ (表 A-5 および 表 A-6 の注釈を参照)
- 内部ユーザ属性 (表 A-1 および 表 A-2 を参照)
- 内部エンドポイント属性
- 許可プロファイル
- ダウンロード可能アクセス コントロール リスト (DACL)
- ID (認証) ポリシー
- ネットワーク アクセスの許可ポリシー
- ネットワーク アクセスの許可例外ポリシー
- ネットワーク アクセスのサービス選択ポリシー
- RADIUS プロキシ サービス
- ユーザ パスワードの複雑度
- ID 順序および RSA プロンプト
- UTF-8 データ (「UTF-8 のサポート」(P.1-7) を参照)
- EAP 認証プロトコル : PEAP-TLS
- ユーザ チェック属性
- ID 順序の高度なオプション
- ポリシー条件で使用可能な追加属性 : AuthenticationIdentityStore
- 追加の文字列演算子 : Start with、Ends with、Contains、Not contains

移行されないデータ オブジェクト

以下のデータ オブジェクトは、Cisco Secure Access Control System (ACS) から Cisco ISE Release 1.2 に移行されません。

- モニタリング レポート
- スケジュール バックアップ
- リポジトリ
- 管理者、ロール、および管理者の設定
- カスタマー/デバッグ ログ設定
- 展開情報 (セカンダリ ノード)
- 証明書 (認証局およびローカル証明書)
- Security Group Access Control List (SGACL)
- セキュリティ グループ (SG)
- サポートされている Security Group Access (SGA) デバイスの AAA サーバ
- セキュリティ グループ マッピング
- Network Device Admission Control (NDAC) ポリシー
- SGA 出力マトリクス
- ネットワーク デバイス内の SGA データ
- SGA 許可ポリシー結果のセキュリティ グループ タグ (SGT)

- ネットワーク条件（エンドステーションフィルタ、デバイスフィルタ、デバイスポートフィルタ）
- デバイスの AAA ポリシー
- Dial-In 属性のサポート
- TACACS+ プロキシ
- TACACS+ CHAP と MSCHAP 認証
- TACACS+ シェルプロファイルの属性置換
- RSA ノード欠落の秘密の表示
- 最大ユーザセッション数
- アカウントのディセーブル化
- ユーザパスワードタイプ
- ポリシー条件で使用可能な追加属性：NumberOfHoursSinceUserCreation
- ホストのワイルドカード
- ネットワーク デバイスの範囲

一部が移行されるデータ オブジェクト

以下のデータ オブジェクトは、Cisco Secure Access Control System (ACS) から Cisco ISE Release 1.2 に一部が移行されます。

- 日付型の ID およびホスト属性は移行されない。
- RSA sdopts.rec ファイルおよびセカンダリ情報は移行されない。
- RADIUS ID サーバ属性（属性 CiscoSecure-Group-Id のみ移行される）。

サポート対象属性およびデータ型

表 A-1 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へ移行されるユーザ属性

Cisco Secure ACS Release 5.3 でサポートされるユーザ属性	Cisco ISE Release 1.2 のターゲット データ型
String	String
UI32	未サポート
IPv4	未サポート
Boolean	未サポート
Date	未サポート
Enum	未サポート

表 A-2 ユーザ属性：ユーザとの関連

Cisco Secure ACS Release 5.3 のユーザに関連付けられている属性	Cisco ISE Release 1.2
String	サポート
UI32	—
IPv4	—
Boolean	—
Date	—

表 A-3 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 に移行されるホスト属性

Cisco Secure ACS Release 5.3 でサポートされるホスト属性	Cisco ISE Release 1.2 のターゲット データ型
String	String
UI32	UI32
IPv4	IPv4
Boolean	Boolean
Date	未サポート
Enum	使用可能な値の整数

表 A-4 ホスト属性：ホストとの関連

Cisco Secure ACS Release 5.3 のホストに関連付けられている属性	Cisco ISE Release 1.2
String	サポート
UI32	サポート (値は String に変換される)
IPv4	サポート (値は String に変換される)
Boolean	サポート (値は String に変換される)
Date	サポート (値は String に変換される)
Enum	サポート (値は String に変換される)

表 A-5 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へ移行される RADIUS 属性

Cisco Secure でサポートされる RADIUS 属性 ACS 5.3	Cisco ISE Release 1.2 のターゲット データ型
UI32	UI32
UI64	UI64
IPv4	IPv4
Hex String	Octect String
String	String
Enum	使用可能な値の整数

表 A-6 RADIUS 属性 : RADIUS サーバとの関連

Cisco Secure ACS Release 5.3 の RADIUS サーバに関連付けられている属性	Cisco ISE Release 1.2
UI32	サポート
UI64	サポート
IPv4	サポート
Hex String	サポート (Hex string は Octet String に変換される)
String	サポート
Enum	サポート (Enum は使用可能な値の整数)

データ情報マッピング

この項には、エクスポート プロセス中にマッピングされるデータ情報を一覧表示する表が記載されています。表には、Cisco Secure ACS Release 5.3 のオブジェクト カテゴリと、Cisco ISE Release 1.2 の相当するカテゴリが記載されています。この項のデータマッピング表には、移行プロセスのエクスポート ステージ中のデータ移行時にマップされるデータ オブジェクトのステータス (有効または無効) が記載されています。

- [表 A-7](#) (ネットワーク デバイス プロパティ マッピング)
- [表 A-8](#) (Active Directory プロパティ マッピング)
- [表 A-9](#) (外部 RADIUS サーバ プロパティ マッピング)
- [表 A-10](#) (ホスト/エンドポイント プロパティ マッピング)
- [表 A-11](#) (ID ディクショナリ プロパティ マッピング)
- [表 A-12](#) (ID グループ プロパティ マッピング)
- [表 A-13](#) (LDAP プロパティ マッピング)
- [表 A-14](#) (NDG タイプ マッピング)
- [表 A-15](#) (NDG 階層マッピング)
- [表 A-16](#) (RADIUS ディクショナリ ベンダー マッピング)
- [表 A-17](#) (RADIUS ディクショナリ属性マッピング)
- [表 A-18](#) (ユーザ マッピング)
- [表 A-19](#) (証明書認証プロファイル)
- [表 A-20](#) (許可プロファイル マッピング)
- [表 A-21](#) (DAACL マッピング)
- [表 A-22](#) (外部 RADIUS サーバ マッピング)
- [表 A-23](#) (ID 属性ディクショナリ マッピング)
- [表 A-24](#) (RADIUS トークン マッピング)
- [表 A-25](#) (RSA マッピング)
- [表 A-26](#) (RSA プロンプト)
- [表 A-27](#) (ID ストア順序)

- 表 A-28 (デフォルトのネットワーク デバイス)

表 A-7 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのネットワーク デバイス マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	そのまま移行
Description	そのまま移行
Network device group	そのまま移行
Single IP address	そのまま移行
Single IP and subnet address	そのまま移行
Collection of IP and subnet addresses	非サポート
TACACS information	TACACS は Cisco ISE Release 1.2 でサポート対象外のため移行されません。
RADIUS shared secret	そのまま移行
CTS	そのまま移行
SNMP	SNMP データは Cisco ISE でのみ使用できるため、移行されたデバイス用の SNMP 情報はありませぬ。
Model name	このプロパティは Cisco ISE でのみ有効です (値はデフォルトで「unknown」)。
Software version	このプロパティは Cisco ISE でのみ有効です (値はデフォルトで「unknown」)。



(注)

TACACS としてのみ設定されているネットワーク デバイスは、移行に対してサポートされず、移行されないデバイスとして記載されています。

表 A-8 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への Active Directory マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Domain name	そのまま移行
User name	そのまま移行
Password	そのまま移行
Allow password change	そのまま移行
Allow machine access restrictions	そのまま移行
Aging time	そのまま移行
User attributes	そのまま移行
Groups	そのまま移行



(注) Cisco Secure ACS to Cisco ISE Migration Tool は、Active Directory データが移行された後で **join** コマンドを発行します。ドメイン名、ユーザ名、およびパスワードが不正な場合、この動作は失敗することがあります。また、「join」操作中の失敗を避けるには、Cisco ISE アプライアンスが Active Directory のサーバ時間と同期していることが重要です。

表 A-9 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への外部 RADIUS サーバ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	そのまま移行
Description	そのまま移行
Server IP address	そのまま移行
Shared secret	そのまま移行
Authentication port	そのまま移行
Accounting port	そのまま移行
Server timeout	そのまま移行
Connection attempts	そのまま移行

表 A-10 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのホスト (エンドポイント) マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
MAC address	そのまま移行
Status	移行されない
Description	そのまま移行
Identity group	エンドポイント グループとの関連を移行します。
Attribute	エンドポイント属性が移行されます。
Authentication state	これは Cisco ISE で有効なプロパティです (値は固定値「Authenticated」)。
Class name	これは Cisco ISE でのみ有効なプロパティです (値は固定値「TBD」)。
Endpoint policy	これは Cisco ISE でのみ有効なプロパティです (値は固定値「Unknown」)。
Matched policy	これは Cisco ISE でのみ有効なプロパティです (値は固定値「Unknown」)。
Matched value	これは Cisco ISE でのみ有効なプロパティです (値は固定値「0」)。
NAS IP address	これは Cisco ISE でのみ有効なプロパティです (値は固定値「0.0.0.0」)。
OUI	これは Cisco ISE でのみ有効なプロパティです (値は固定値「TBD」)。
Posture status	これは Cisco ISE でのみ有効なプロパティです (値は固定値「Unknown」)。
Static assignment	これは Cisco ISE でのみ有効なプロパティです (値は固定値「False」)。

表 A-11 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への ID ディクショナリ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Attribute	Attribute name
Description	Description
Internal name	Internal name
Attribute type	Data type
Maximum length	移行されない
Default value	移行されない
Mandatory fields	移行されない
User	ディクショナリ プロパティはこの値（「user」）を承認します。

表 A-12 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への ID グループ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Parent	このプロパティは、階層の詳細の一部として移行されます。



(注)

Cisco ISE にはユーザ ID グループおよびエンドポイント ID グループが含まれています。Cisco Secure ACS Release 5.3 の ID グループは Cisco ISE へ、ユーザ ID グループおよびエンドポイント ID グループとして移行されます。これは、ユーザをユーザ ID グループに割り当て、エンドポイントをエンドポイント ID グループに割り当てる必要があるためです。

表 A-13 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への LDAP マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Server connection information	そのまま移行。([サーバ接続 (Server Connection)] タブ、 図 A-1 (P.A-9) を参照)。
Directory organization information	そのまま移行。([ディレクトリ構成 (Directory Organization)] タブ、 図 A-2 (P.A-9) を参照)
Directory groups	そのまま移行
Directory attributes	移行は (Cisco Secure ACS-Cisco ISE Migration Tool を使用して) 手動で行われます。

図 A-1 [サーバ接続 (Server Connection)] タブ



図 A-2 [ディレクトリ構成 (Directory Organization)] タブ

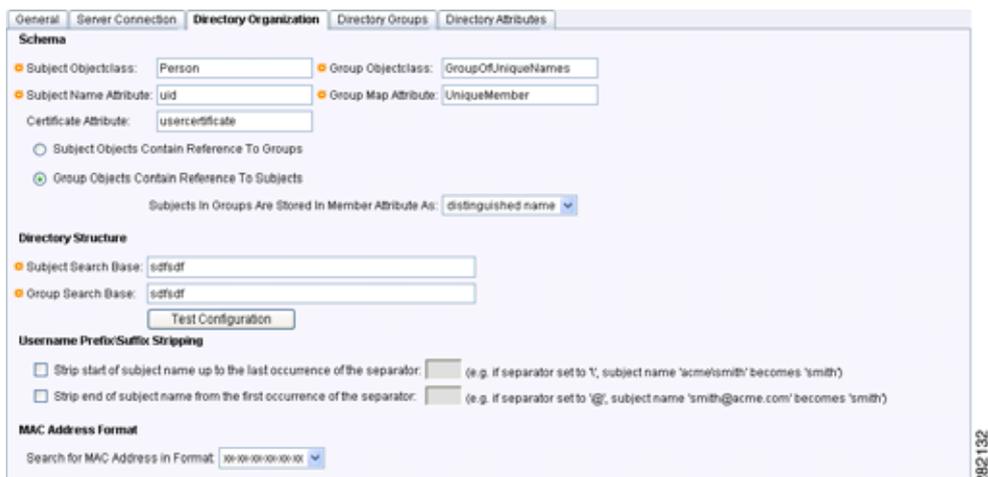


表 A-14 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への NDG タイプ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description

 (注)

Cisco Secure ACS Release 5.3 は、同じ名前の複数のネットワーク デバイス グループ (NDG) をサポートできます。Cisco ISE は、この命名規則をサポートしていません。したがって、定義されている名前の最初の NDG タイプのみが移行されます。

表 A-15 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への NDG 階層マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Parent	このプロパティには特別なプロパティは関連付けられません。この値は、NDG 階層名の一部としてのみ入力されるためです (NDG タイプはこのオブジェクト名のプレフィックスです)。



(注)

コロン (:) を持つルート名が含まれている NDG は移行されません。これは、Cisco ISE Release 1.2 で、コロンを有効な文字として認識しないためです。

表 A-16 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RADIUS ディクショナリ (ベンダー) マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Vendor ID	Vendor ID
Attribute prefix	このプロパティは移行する必要ありません。
Vendor length field size	Vendor attribute type field length.
Vendor type field size	Vendor attribute size field length.



(注)

Cisco Secure ACS Release 5.3 インストールの一部ではない、RADIUS ベンダーのみ移行する必要があります。これはユーザ定義ベンダーにのみ影響します。

表 A-17 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RADIUS ディクショナリ (属性) マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Attribute ID	この値には特定のプロパティを関連付けられません。この値は、NDG 階層名の一部としてのみ入力されるためです。(NDG タイプはこのオブジェクト名のプレフィックスです)。
Direction	Cisco ISE ではサポート対象外
Multiple allowed	Cisco ISE ではサポート対象外

表 A-17 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RADIUS ディクショナリ (属性) マッピング (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Attribute type	そのまま移行
Add policy condition	Cisco ISE ではサポート対象外
Policy condition display name	Cisco ISE ではサポート対象外



(注) Cisco Secure ACS Release 5.3 インストールの一部ではない、これらの RADIUS 属性のみ移行する必要があります (ユーザ定義属性のみ移行する必要があります)。

表 A-18 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのユーザ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Status	このプロパティは移行する必要ありません。(このプロパティは Cisco ISE には存在しません)。
Identity group	Cisco ISE の ID グループへ移行します。
Password	Password
Enable password	このプロパティは移行する必要ありません。(このプロパティは Cisco ISE には存在しません)。
Change password on next login	このプロパティは移行する必要ありません。
User attributes list	ユーザ属性は Cisco ISE からインポートされ、ユーザに関連付けられます。

表 A-19 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への証明書認証プロファイル マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Principle user name (X.509 属性)	Principle user name (X.509 属性)
Binary certificate comparison with certificate from LDAP or AD	Binary certificate comparison with certificate from LDAP or AD
AD or LDAP name for certificate fetching	AD or LDAP name for certificate fetching.

表 A-20 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への許可プロファイル マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
DAACLID (ダウンロード可能 ACL ID)	そのまま移行
Attribute type (静的および動的)	<ul style="list-style-type: none"> 静的属性の場合はそのまま移行されます。 動的属性の場合は、Dynamic VLAN は除き、そのまま移行されます。
Attributes (静的タイプに対してのみフィルタされる)	RADIUS attributes

表 A-21 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのダウンロード可能 ACL マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
DAACL content	DAACL content

表 A-22 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への外部 RADIUS サーバ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Server IP address	Hostname
Shared secret	Shared secret
Authentication port	Authentication port
Accounting port	Accounting port
Server timeout	Server timeout
Connection attempts	Connection attempts

表 A-23 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への ID 属性ディクショナリ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Attribute	Attribute name
Description	Internal name
Name	そのまま移行

表 A-23 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への ID 属性ディクショナリマッピング (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Attribute type	Data type
該当プロパティなし	Dictionary (ユーザ ID 属性の場合は値「InternalUser」で設定し、ホスト ID 属性の場合は「InternalEndpoint」で設定します)。
Cisco Secure ACS からまだエクスポートまたは抽出されていない	使用可能な値 = display name
Cisco Secure ACS からまだエクスポートまたは抽出されていない	使用可能な値 = internal name
Cisco Secure ACS からまだエクスポートまたは抽出されていない	使用可能な値はデフォルトです。
Maximum length	なし
Default value	なし
Mandatory field	なし
Add policy condition	なし
Policy condition display name	なし

表 A-24 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RADIUS トークン マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Safeword server	Safeword server
Enable secondary appliance	Enable secondary appliance
Always access primary appliance first	Always access primary appliance first
Fallback to primary appliance in minutes	Fallback to primary appliance in minutes
Primary appliance IP address	Primary appliance IP address
Primary shared secret	Primary shared secret
Primary authentication port	Primary authentication port
Primary appliance TO (timeout)	Primary appliance TO
Primary connection attempts	Primary connection attempts
Secondary appliance IP address	Secondary appliance IP address
Secondary shared secret	Secondary shared secret
Secondary authentication port	Secondary authentication port
Secondary appliance TO	Secondary appliance TO
Secondary connection attempts	Secondary connection attempts

表 A-24 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RADIUS トークン マッピング (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Advanced > treat reject as authentication flag fail	Advanced > treat reject as authentication flag fail
Advanced > treat rejects as user not found flag	Advanced > treat rejects as user not found flag
Advanced > enable identity caching and aging value	Advanced > enable identity caching and aging value
Shell > prompt	Authentication > prompt
Directory attributes	Authorization > attribute name (Cisco Secure ACS のディクショナリ属性リストに属性「CiscoSecure-Group-Id」が含まれている場合は、この属性に移行されます。それ以外の場合はデフォルト値は「CiscoSecure-Group-Id」になります)。

表 A-25 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RSA マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name は常に RSA
Description	移行されない
Realm configuration file	Realm configuration file
Server TO	Server TO
Reauthenticate on change to PIN	Reauthenticate on change to PIN
RSA instance file	移行されない
Treat rejects as authentication fail	Treat rejects as authentication fail
Treat rejects as user not found	Treat rejects as user not found
Enable identity caching	Enable identity caching
Identity caching aging time	Identity caching aging time

表 A-26 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RSA プロンプト

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Passcode prompt	Passcode prompt
Next Token prompt	Next Token prompt
PIN Type prompt	PIN Type prompt
Accept System PIN prompt	Accept System PIN prompt
Alphanumeric PIN prompt	Alphanumeric PIN prompt
Numeric PIN prompt	Numeric PIN prompt

表 A-27 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への ID ストア順序

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Certificate based, certificate authentication profile	Certificate based, certificate authentication profile
Password based	Authentication search list
Advanced options > if access on current IDStore fails than break sequence	Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError."
Advanced options > if access on current IDStore fails then continue to next	Treated as "User Not Found" and proceed to the next store in the sequence.
Attribute retrieval only > exit sequence and treat as "User Not Found"	未サポート（無視される）

表 A-28 Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのデフォルト ネットワーク デバイス

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Default network device status	Default network device status
Network device group	移行されない
Authentication Options - TACACS+	移行されない
RADIUS - shared secret	Shared Secret
RADIUS - CoA port	移行されない
RADIUS - Enable keywrap	Enable keyWrap
RADIUS - Key encryption key	Key encryption key
RADIUS - Message authenticator code key	Message authenticator code key
RADIUS - Key input format	Key input format

■ データ情報マッピング



Cisco Secure ACS to Cisco ISE Migration Tool のトラブルシューティング

この付録では、Cisco Secure ACS to Cisco ISE Migration Tool の使用時に問題をトラブルシューティングする方法について説明します。

ここでは、次の内容について説明します。

- 「移行ツールを開始できない」(P.B-1)
- 「ログにエラー メッセージが表示される」(P.B-1)
- 「デフォルトのフォルダ、ファイル、およびレポートが作成されない」(P.B-3)
- 「移行のエクスポート フェーズが非常に遅い」(P.B-3)
- 「Cisco TAC への問題の報告」(P.B-3)

移行ツールを開始できない

状況

移行ツールを開始できません。

アクション

Java JRE バージョン 1.6 以降が移行マシンにインストールされており、システム パスおよびクラスパスで正しく設定されていることを確認します。

ログにエラー メッセージが表示される

状況

ログに以下のエラー メッセージが表示されます。

```
"Hosts: Connection to https://hostname-or-ip refused: null".
```

Cisco ISE へ移行するときにオブジェクトがレポートされます。

アクション

- 移行のアプリケーション マシンがネットワークに接続されており、正しく設定されていることを確認します。

■ ログにエラーメッセージが表示される

- Cisco ISE アプライアンスがネットワークに接続されており、正しく設定されていることを確認します。
- Cisco ISE アプライアンスおよび移行マシンが、ネットワークを介して相互に接続可能であることを確認します。
- 移行ツールが Cisco ISE に接続している場合は、Cisco ISE プライマリ ノードで使用されているホスト名が（もしあれば）、DNS で解決可能であることを確認します。
- Cisco ISE アプライアンスがアクティブで、稼働中であることを確認します。
- Cisco ISE アプリケーション サーバのサービスがアクティブで、稼働中であることを確認します。

状況

ログに以下のエラーメッセージが表示されます。

```
"I/O exception (org.apache.http.NoHttpResponseException) caught when processing request: The target server failed to respond".
```

アクション

- Cisco ISE アプリケーション サーバのサービスがアクティブで、稼働中であることを確認します。
- Cisco ISE の Web サーバのしきい値を超過していないこと、またはメモリの例外がないことを確認します。
- Cisco ISE アプライアンスで CPU 消費が 100 % でないこと、および CPU がアクティブであることを確認します。

状況

ログに以下のエラーメッセージが表示されます。

```
"OutOfMemory".
```

アクション

[「Cisco Secure ACS-Cisco ISE Migration Tool のインストールおよび初期化」\(P.4-3\)](#)に記載されているとおりに、Java ヒープ サイズを 1 GB 以上に増やします。

状況

ログに以下のエラーメッセージが表示されます。

```
Caused by: java.sql.SQLException: [Sybase][ODBC Driver][SQL Anywhere]Temporary space limit exceeded.
```

アクション

累積パッチ ACS 5.1.0.44.4 をインストールします。このパッチには、一時的なデータベース領域の制限に関する問題の修正が含まれています。

デフォルトのフォルダ、ファイル、およびレポートが作成されない

状況

移行ツールで、デフォルトのフォルダ、ログ ファイル、レポート、および永続的なデータ ファイルを作成できません。

アクション

ユーザが、ファイルシステムの書き込み権限を持っていること、および十分なディスク領域があることを確認します。

移行のエクスポート フェーズが非常に遅い

状況

移行プロセスのエクスポート フェーズで処理が非常に遅くなっています。

アクション

移行プロセスを開始する前に、Cisco Secure ACS アプライアンスを再起動してメモリ領域を解放します。

Cisco TAC への問題の報告

技術的な問題に対して、原因および考えられる解決方法を見つけれない場合は、Cisco カスタマーサービスの担当者に連絡して、問題の解決方法を入手します。Cisco Technical Assistance Center (TAC) に関する情報については、アプライアンスに付随している『Cisco Information Packet』の資料を参照するか、または以下の Web サイトにアクセスしてください。

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

Cisco TAC に連絡する前に、以下の情報を用意しておいてください。

- アプライアンスのシャーシタイプおよびシリアル番号。
- 保守契約または保証書 (『Cisco Information Packet』を参照)。
- ソフトウェアの名前とタイプ、バージョンまたはリリースの番号 (該当する場合)。
- 新しいアプライアンスを入手した日付。
- 問題または状況が発生したときの簡単な説明、問題を切り分けまたは再現するための手順、問題を解決するために実行する手順の説明。
- 移行のログファイル (...migration/bin/migration.log)。
- config フォルダのすべてのレポート (...migration/config)。
- Cisco Secure ACS Release 5.3 のログ ファイル。
- Cisco Secure ACS Release 5.3 のビルド番号。



(注)

カスタマー サービス担当者には、必ず Cisco ISE 3300 シリーズ アプライアンスの初期インストール後に行ったアップグレードまたは保守の情報をすべてお伝えください。



A

ACL

Access Control List (アクセス コントロール リスト)。オブジェクトに割り当てられているアクセス権のリスト。このリストにより、どのユーザまたはプロセスが、どのオブジェクトに対してアクセス権を付与されているか、また特定のオブジェクトについてどのような操作が許可されているかが指定されています。ACL のエントリは、ユーザ、操作、ポート、またはホスト名に対して権限を指定できます。

ACS

Cisco Secure Access Control Server。規格準拠の認証、許可、アカウンティング (AAA) サービスをネットワークに提供するポリシーベースのセキュリティ サーバです。ACS を使用すると、シスコおよびシスコ以外のデバイスとアプリケーションを簡単に管理できます。

Active Directory

Microsoft Active Directory はディレクトリ サービスで、中央のデータベースにおける展開の情報および設定がすべて格納されています。管理者は **Active Directory** を使用してポリシーを割り当て、少数のコンピュータ、ユーザ、およびプリンタを持つネットワークから、複数のドメインおよび複数の場所に及ぶ大規模なネットワーク環境まで、さまざまなネットワーク上でソフトウェアを展開および更新することができます。

D

DAACL

ダウンロード可能アクセス コントロール リスト。Cisco ISE は、オブジェクトに対するダウンロード可能なアクセス権のリストをサポートしています。DAACL のエントリは、ユーザ、操作、ポート、またはホスト名に対して権限を指定できます。

H

HTTPS

Hypertext Transfer Protocol Secure。Hypertext Transfer Protocol (HTTP) と SSL/TLS プロトコルの組み合わせにより、セキュアで暗号化された通信、およびネットワークやインターネット トラフィックに対してセキュアな識別を提供します。HTTPS 接続は、企業システム、金融システム、または商用システム内の機密トランザクションで、よく使用されます。HTTPS は、別のポートを使用して、HTTP と TCP 間の暗号化および認証の追加レイヤを提供します。

L

LDAP

Lightweight Directory Access Protocol は、TCP/IP で実行するディレクトリ サービスを使用してディレクトリ内のデータを問い合わせ、変更するためのアプリケーション プロトコルです。LDAP ディレクトリは、系統化されたレコードセットで、それぞれの住所と電話番号によって「レコード」が構成されています。セキュアな LDAP 通信を実現するためには、一般的には SSL トンネルを使用します。

M**MAC アドレス**

メディア アクセス コントロール アドレス。ほとんどのネットワーク アダプタやネットワーク インターフェイス カードにメーカーによって割り当てられる疑似固有識別子。

N**NDG**

ネットワーク デバイス グループ。Cisco ISE では、デバイス グループは階層的な構造でネットワーク デバイス グループ (NDG) が含まれています。NDG は、場所やデバイス タイプなどの基準に基づいて類似のデバイスを論理的にグループ化したものです。たとえば、デバイスを、大陸、地域、または国などの場所ごとにグループ化することも、ファイアウォール、ルータ、スイッチなどのタイプごとにグループ化することもできます。Cisco ISE では、ポリシー条件で NDG を使用することもできます。

P**PI**

プログラマチック インターフェイス。外部アプリケーションが Cisco Secure ACS とやりとりするためのメカニズム。

R**RADIUS**

Remote Authentication Dial-In User Service (リモート認証ダイヤルイン ユーザ サービス)。コンピュータがネットワーク サービスに接続してこのサービスを使用するための認証、許可、アカウントリング (AAA) 集中管理を提供するネットワークング プロトコルです。

T**TACACS**

Terminal Access Controller Access Control System は、UNIX ネットワークで一般的に使用される認証サーバとの通信に使用されるリモート認証プロトコルです。リモート アクセス サーバは、ユーザがネットワークへのアクセス権を持つかどうかを判断するために、TACACS を使用して、認証サーバと通信します。

V**VSA**

Vendor-Specific Attribute (ベンダー固有属性)。標準 RADIUS 属性セットによって提供されない独自のプロパティまたは特性。VSA は、リモート アクセス サーバのベンダーによって、RADIUS をベンダー サーバ用にカスタマイズするために定義されます。



C

Cisco Secure ACS 5.3 から Cisco ISE への移行 [2-1](#)

い

移行ツール [2-1](#)

移行方法

移行コンポーネント [2-3](#)

移行ログ ファイル [B-3](#)

し

システム要件 [4-2](#)

て

データの移行および展開のシナリオ [3-1](#)

シングルまたはスタンドアロンの ACS アプライアンス [3-1](#)

データの移行と展開のシナリオ

分散環境の場合 [3-2](#)

と

トラブルシューティング [B-1](#)

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>