



Cisco Secure ACS 5.1/5.2 用 Cisco Identity Services Engine Release 1.1.x 移行ガイド

2012 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 Secure ACS 5.1/5.2 用 Cisco Identity Services Engine Release 1.1.x 移行ガイド
Copyright ©2012 Cisco Systems, Inc.

All rights reserved.

Copyright © 2012, シスコシステムズ合同会社.

All rights reserved.



CONTENTS

このマニュアルの目的	vii
対象読者	viii
マニュアルの構成	ix
このマニュアルの使用方法	ix
表記法	x
マニュアルの最新情報	xi
関連資料	xi
リリース固有のマニュアル	xi
プラットフォーム固有のマニュアル	xii
通告	xii
OpenSSL/Open SSL Project	xii
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	xiv

CHAPTER 1

Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行概要 1-1

概要	1-1
Cisco Secure ACS から Cisco ISE へのサポートされている移行	1-2
ソフトウェア要件	1-2
機能説明	1-3
エクスポート	1-3
データの持続性	1-3
インポート	1-4
拡張性	1-4
ハイ アベイラビリティ	1-4
レポート	1-5
UTF-8 のサポート	1-8
ISE 802.1X サービスに対する FIPS サポート	1-9
Cisco Secure ACS/Cisco ISE バージョンの検証	1-10

CHAPTER 2

Cisco Secure ACS-Cisco ISE Migration Tool について 2-1

概要 : Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 へ	2-1
Cisco Secure ACS-Cisco ISE Migration Tool	2-2
移行ツールのコンポーネント	2-4

データ設定 2-4
 ステータス報告 2-4
 エクスポートおよびインポート 2-4
 データ構造マッピング 2-5

CHAPTER 3

Cisco Secure ACS-Cisco ISE Migration Tool のインストール 3-1

移行ツールのインストール ガイドライン 3-1
 システム要件 3-2
 セキュリティの考慮事項 3-2
 データの移行および展開のシナリオ 3-2
 シングル Cisco Secure ACS アプライアンスからのデータ移行のガイドライン 3-3
 分散環境におけるデータ移行のガイドライン 3-3
 Cisco Secure ACS-Cisco ISE Migration Tool のインストールおよび初期化 3-4

CHAPTER 4

Cisco Secure ACS-Cisco ISE Migration Tool の使用 4-1

ログインおよび移行ツールの使用 4-1
 インポート プロセスの検証 4-9
 レポート ファイルの提供 4-10

CHAPTER 5

Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行 5-1

概要 5-1
 Cisco Secure ACS の以前のリリースからの移行 5-2

APPENDIX A

Cisco Secure ACS 5.1/5.2 および Cisco ISE 1.1 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
 一般的な移行ルール A-3
 移行ポリシー A-3
 サポート対象属性およびデータ型 A-4
 データ情報マッピング A-6

APPENDIX B

Cisco Secure ACS-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

この移行マニュアルは、Cisco Identity Services Engine Releases 1.1 および 1.1.1 を対象としています。このマニュアルでは、Cisco Secure Access Control System (ACS) Release 5.1/5.2 データベースから Cisco Identity Services Engine (ISE) Release 1.1 アプライアンスへデータを移行するためのプロセスについて説明します。移行プロセスでは、Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への Migration Tool を使用します。移行マニュアルのこのセクションでは、マニュアルの目的、対象読者、および構成について説明し、以下のトピックについて取り上げます。

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

このマニュアルの目的

この移行マニュアルは、Cisco ISE 1.1 のマニュアルセットの一部であり、Cisco Secure ACS から Cisco ISE への Migration Tool を使用して既存のデータを Cisco Secure ACS Release 5.1/5.2 データベースから Cisco ISE 1.1 アプライアンスへ移行する方法について説明しています。この移行マニュアルには、以下の情報が含まれています。



(注)

これ以降、この移行マニュアルでは、Cisco Secure ACS から Cisco ISE への Migration Tool (およびその省略形である Cisco Secure ACS-Cisco ISE Migration Tool) は、Cisco Secure ACS 5.1/5.2 データベースから Cisco ISE 1.1 アプライアンスへのデータ移行で使用するツールを表します。

- Cisco Secure ACS-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 5.1/5.2 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 5.1/5.2 データベースから Cisco ISE 1.1 アプライアンスへデータを移行するための段階的な手順。
- シスコ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パスを定義しています。



(注)

Cisco Secure ACS-Cisco ISE Migration Tool は Cisco Secure ACS Release 5.1/5.2 のデータの移行のみサポートしています。

Cisco Secure ACS の以前のリリース（3.x や 4.x など）のデータを、Cisco ISE 1.1 アプライアンスへ移行可能な Cisco Secure ACS 5.1/5.2 のステートへ移行するには、以下の複数手順のプロセスが必要です。

1. シスコのマニュアルに記載されているプロセスを使用して、Cisco Secure ACS 3.x または 4.x のデータを Cisco Secure ACS Release 5.0 のステートへアップグレードします（「はじめに」の[関連資料](#)を参照してください）。
2. シスコのマニュアルに記載されているプロセスを使用して、Cisco Secure ACS 5.0 のデータを Cisco Secure ACS Release 5.1/5.2 のステートへアップグレードします（「はじめに」の[関連資料](#)を参照してください）。
3. この移行マニュアルの手順を使用して、Cisco Secure ACS-Cisco ISE Migration Tool で、Cisco Secure ACS 5.1/5.2 のデータを Cisco ISE 1.1 アプライアンスへ移行します（第 4 章「[Cisco Secure ACS-Cisco ISE Migration Tool の使用](#)」を参照してください）。

この移行マニュアルでは、Cisco Secure ACS-Cisco ISE Migration Tool を使用して既存の Cisco Secure ACS 5.1/5.2 データをエクスポートするためのプロセス、およびそのデータを Cisco ISE 1.1 アプライアンスへインポートするためのプロセスを説明することに重点をおいています。

既存の Cisco Secure ACS データを移行する前に、Cisco Secure ACS 5.1/5.2 システムと Cisco ISE 1.1 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。

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 5.1/5.2 データベース情報を Cisco ISE 1.1 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

この移行マニュアルは、以下のセクションで構成されています。

タイトル	説明
第 1 章「Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行概要」	Cisco Secure ACS-Cisco ISE の移行の概要、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 アーキテクチャについて説明します。
第 2 章「Cisco Secure ACS-Cisco ISE Migration Tool について」	Cisco Secure ACS-Cisco ISE Migration Tool の機能について説明します。このツールは、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-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 4 章「Cisco Secure ACS-Cisco ISE Migration Tool の使用」	Cisco Secure ACS-Cisco ISE Migration Tool を使用して、データベースから Cisco Secure ACS 5.1/5.2 データをエクスポートし、移行したデータを Cisco ISE 1.1 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。
第 5 章「Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行」	Cisco Secure ACS の以前のリリースのデータを Cisco Secure ACS Release 5.0 のステートへアップグレードする処理の概要、および必要なマニュアルへのリンクについて記載しています。Cisco Secure ACS の以前のリリースに対してサポートされている移行パスは、データを Cisco Secure ACS Release 5.0 のステートへアップグレードする方法のみです。Cisco Secure ACS Release 5.0 のステートになると、このデータを Cisco Secure ACS Release 5.1/5.2 へアップグレードするためにサポートされているパスを使用できます。
付録 A「Cisco Secure ACS 5.1/5.2 および Cisco ISE 1.1 のデータ構造マッピング」	Cisco Secure ACS Release 5.1/5.2 システムと Cisco ISE 1.1 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記載しているマッピング表を提供します。
付録 B「Cisco Secure ACS-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法

Cisco Secure ACS Release 5.1/5.2 のデータを Cisco ISE 1.1 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 5.1/5.2 および Cisco ISE 1.1 のデータ構造マッピング」](#)を参照してください。
- Cisco Secure ACS 5.1/5.2 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 1.1 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 5.1/5.2 から Cisco ISE 1.1 への移行概要」](#)を参照してください。

- Cisco Secure ACS 5.1/5.2 と Cisco ISE 1.1 間の機能と構成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-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 3 章「Cisco Secure ACS-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 5.1/5.2 のデータを Cisco ISE 1.1 へ移行するのに必要なプロセスを理解するには、第 4 章「Cisco Secure ACS-Cisco ISE Migration Tool の使用」を参照してください。

表記法

この移行マニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	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。
イタリック体フォント	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は、イタリック体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。
[x y z]	どれか 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。
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 フォント	システムが表示するターミナルセッションおよび情報は、courier 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。次に進む前に検討する必要がある重要情報、役に立つ情報、この移行マニュアル以外の参照資料などを紹介しています。

マニュアルの最新情報

表 1 『Cisco Secure ACS 5.1/5.2 用 Cisco Identity Services Engine Release 1.1.x 移行ガイド』の最新情報

日付	説明
2012年7月10日	Cisco Identity Services Engine, Release 1.1.1
2012年3月19日	Cisco Identity Services Engine, Release 1.1

関連資料

リリース固有のマニュアル

表 2 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 2 Cisco Identity Services Engine の製品マニュアル

マニュアル名	参照先
<ul style="list-style-type: none"> 『Release Notes for the Cisco Identity Services Engine, Release 1.1』 『Release Notes for the Cisco Identity Services Engine, Release 1.1.1』 	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
<ul style="list-style-type: none"> 『Cisco Identity Services Engine Network Component Compatibility, Release 1.1』 『Cisco Identity Services Engine Network Component Compatibility, Release 1.1.1』 	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
<ul style="list-style-type: none"> 『Cisco Identity Services Engine User Guide, Release 1.1』 『Cisco Identity Services Engine User Guide, Release 1.1.1』 	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
<ul style="list-style-type: none"> 『Cisco Identity Services Engine Hardware Installation Guide, Release 1.1』 『Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1』 	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Upgrade Guide, Release 1.1.1』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

表 2 Cisco Identity Services Engine の製品マニュアル (続き)

マニュアル名	参照先
『Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine API Reference Guide, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x』	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

プラットフォーム固有のマニュアル

Policy Management Business Unit マニュアルへのリンクは、以下のサイトの www.cisco.com を参照してください。

Cisco ISE

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

- Cisco Secure ACS
http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.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 Profiler
http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC ゲスト サーバ
http://www.cisco.com/en/US/products/ps10160/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 (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (ey@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。



CHAPTER 1

Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行概要

この章では、Cisco Identity Services Engine (ISE) および Cisco Secure Access Control System (ACS) の概要について説明します。この章の内容は、次のとおりです。

- 「概要」 (P.1-1)
- 「Cisco Secure ACS から Cisco ISE へのサポートされている移行」 (P.1-2)
- 「ソフトウェア要件」 (P.1-2)
- 「機能説明」 (P.1-3)

概要

Cisco ISE の展開モデルは、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、および 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、プライマリに定義する (Administration ペルソナとして稼働する) 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 や Monitoring などの他の 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。

1 つの 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) の展開モデルは、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が、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。

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することが可能で、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つことができます。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、移行ツールおよび手順を使用できます。この手順では、Cisco Secure ACS からデータを読み込み、Cisco ISE 内に対応するデータを作成します。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、この移行手順を使用できます。Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行プロセスでは、必要なユーザの介入は最小限で、Cisco Secure ACS から Cisco ISE へすべての設定データを移行できます。

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

Cisco ISE は、Cisco Secure ACS-ISE 1.1 Migration Tool を使用して Cisco Secure ACS 5.1 および 5.2 からのデータ移行をサポートしています。Cisco Secure ACS 3.x または Cisco Secure ACS 4.x を実行する場合、最初に Cisco Secure ACS 5.0 へアップグレードする必要があります。

Cisco Secure ACS 5.0 へのアップグレード後、Cisco Secure ACS 5.1 または 5.2 へアップグレードできます。この時点で、Cisco Secure ACS-ISE Migration Tool を使用して Cisco ISE 1.1 へ移行できます。



(注)

Cisco Secure ACS 5.0 から Cisco Secure ACS 5.1/5.2 へ直接アップグレードすることも可能です。Cisco Secure ACS から Cisco ISE への移行を試行する前に、Cisco Secure ACS の以前のリリースから Cisco Secure ACS 5.1/5.2 へのすべてのアップグレードを完了しておく必要があります。

Cisco Secure ACS 3.x または 4.x から Cisco Secure ACS 5.0 へのデータ移行については、[第 5 章「Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行」](#)を参照してください。

ソフトウェア要件

[表 1-1](#) に、Cisco ISE 1.1 で移行を行うための最小限のソフトウェア要件を記載しています。

表 1-1 Cisco ISE 1.1 で移行するため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.3-2) 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。

Cisco Secure ACS-Cisco ISE Migration Tool を実行する前に、Cisco ISE Release 1.1 へのアップグレードが完了していること、および ACS 5.1 と 5.2 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。

機能説明

移行ツールは、Cisco Secure ACS データを Cisco ISE へ転送します。ここでは主に次の 3 つの手順があります。

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. データを Cisco ISE 1.1 へインポートする。

Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行プロセスの主な機能は以下のとおりです。

- 「エクスポート」 (P.1-3)
- 「データの持続性」 (P.1-3)
- 「インポート」 (P.1-4)
- 「拡張性」 (P.1-4)
- 「ハイ アベイラビリティ」 (P.1-4)
- 「レポート」 (P.1-5)
- 「UTF-8 のサポート」 (P.1-8)
- 「ISE 802.1X サービスに対する FIPS サポート」 (P.1-9)
- 「Cisco Secure ACS/Cisco ISE バージョンの検証」 (P.1-10)

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 ACS データをエクスポートすることです。Cisco Secure ACS と接続し、Cisco Secure ACS データを移行アプリケーションへエクスポートするよう要求するには、クレデンシャルを提供する必要があります。この間に、エクスポートされたデータを Cisco ISE 1.1 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、検証する必要があります。データが不正な場合、このステータスは移行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 1.1 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 をアンインストールし、Cisco ISE 1.1 イメージでアプライアンスを再作成する必要があります。再作成が行われる前、および次のステージ (インポート) 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。

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 1.1 ヘ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 1.1 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何も設定されていないクリーンなマシンを使用しなければなりません。

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、移行レポートに記録されます。

拡張性

移行アプリケーションは、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 ISE 1.1 で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ictionary	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-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ステータスを保持します。これにより、インポートまたはエクスポートで障害が発生したために、いずれかのポイントでインポートまたはエクスポートのプロセスが失敗した場合でも、最初から開始するのではなく、障害の発生前で、発生したタイミングに一番近いチェックポイントから開始することができます。

インポートまたはエクスポートのフェーズで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。障害の後で移行を再開すると、ダイアログボックスが表示されます。

前のインポート/エクスポートを再開するか、前のプロセスを廃棄して新しいプロセスを開始するか、選択することができます。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オブジェクトタイプから再開されます。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

Cisco Secure ACS-Cisco ISE Migration Tool を使用して、Cisco Secure ACS 5.1/5.2 のデータを Cisco ISE アプライアンスへ移行する場合に、以下の3つのレポートを使用できます。

- **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。図 1-1 を参照してください。
エクスポート レポートには、エクスポートされるがインポートされないオブジェクトのエラー情報が含まれます。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 間のデータの機能ギャップ分析について記載されます。
- **インポート レポート** : Cisco ISE アプライアンスへ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。図 1-2 を参照してください。
- **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ます。図 1-3 を参照してください。

Cisco ISE 1.1 は、この新しいレポートを導入しています。このレポートはエクスポートが完了した後で使用できます。レポートを表示するには、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ます。

いずれかの認証ポリシーまたは許可ポリシーが移行されなかった場合は、ポリシーがこのレポートに記載されます。このレポートには、2つの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 の用語を使用して移行できるものがあります。たとえば、「Device Type In」は「Device Type Equals」として移行されます。このような場合には、条件は自動的に移行されます。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1つ以上の条件が検出された場合、ポリシー全体はインポートされずに、それらの条件がレポートに記載されます。

表 1-3 で、インポート レポートおよびエクスポート レポートのレポート タイプ、メッセージタイプ、メッセージの内容について説明します。

表 1-3 Cisco Secure ACS 5.1/5.2-Cisco ISE Migration Tool のレポート

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に基づいたエラー、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 1.1 でサポート対象外であるためにエクスポートが試行されなかったことによるエラーが示されます。

表 1-3 Cisco Secure ACS 5.1/5.2-Cisco ISE Migration Tool のレポート (続き)

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 オブジェクトがすでに存在 (重複) するためにインポートできないデータ オブジェクト エラーが示されます。
	エラー	名前の長さが Cisco ISE の文字数制限を超えているためにインポートできないデータ オブジェクト エラーが示されます。
	エラー	Cisco ISE でサポートしていない特殊文字が名前に含まれているために、インポートできないデータ オブジェクト エラーが示されます。
	エラー	Cisco ISE で使用できない、またはサポートされていないデータ文字がオブジェクトに含まれているために、インポートできないデータ オブジェクト エラーが示されます。

図 1-1 エクスポート レポートの例

```

1 2010-09-28 15:55:21,875 [INFO] main MigrationApplicationDriver.main:42: Starting Application, in the main method.....
2 2010-09-28 15:55:24,437 [INFO] main Refreshing org.springframework.context.support.ClassPathXmlApplicationContext@4d3d6f: startup date [Tue Sep
3 2010-09-28 15:55:24,484 [INFO] main Loading XML bean definitions from class path resource [conf/META-INF/beans.xml]
4 2010-09-28 15:55:29,047 [INFO] main Pre-instantiating singletons in org.springframework.beans.factory.support.DefaultListableBeanFactory@9a995
5 2010-09-28 15:55:29,109 [INFO] main Start parsing query XML file ...
6 2010-09-28 15:55:30,203 [INFO] main Start parsing procedure XML file .....
7 2010-09-28 16:46:02,953 [INFO] main MigrationApplicationDriver.main:42: Starting Application, in the main method.....
8 2010-09-28 16:46:08,010 [INFO] main Refreshing org.springframework.context.support.ClassPathXmlApplicationContext@1835282: startup date [Tue S
9 2010-09-28 16:46:08,057 [INFO] main Loading XML bean definitions from class path resource [conf/META-INF/beans.xml]
10 2010-09-28 16:46:10,557 [INFO] main Pre-instantiating singletons in org.springframework.beans.factory.support.DefaultListableBeanFactory@1b0bc
11 2010-09-28 16:46:10,619 [INFO] main Start parsing query XML file .....
12 2010-09-28 16:46:11,353 [INFO] main Start parsing procedure XML file .....
13 2010-09-28 16:50:15,105 [INFO] Thread-5 Start connecting to ACS5 PI
14 2010-09-28 16:50:15,277 [WARN] Thread-5 Unable to find required classes (javax.activation.DataHandler and javax.mail.internet.MimeMultipart).
15 2010-09-28 16:50:22,293 [INFO] Thread-5 connection to ACS5 PI succeed
16 2010-09-28 16:50:22,418 [INFO] Thread-4 Start Exporting .....
17 2010-09-28 16:50:22,527 [INFO] Thread-4 Start Exporting Predefined Reference Data Batch.
18 2010-09-28 16:50:22,668 [INFO] Thread-4 Start Exporting Generic Attributes
19 2010-09-28 16:50:22,668 [INFO] Thread-4 Start getting Generic Attributes PPOs from PI
20 2010-09-28 16:52:13,700 [INFO] Thread-4 # of Generic Attributes PPOs returned from PI is: 454
21 2010-09-28 16:52:13,700 [INFO] Thread-4 Start validating and wrapping Generic Attributes objects.
22 2010-09-28 16:52:13,732 [INFO] pool-1-thread-5 (ExportReportListenerImpl.addCurrentObjectInfo:181) - Predefined Reference Data-Generic Attribu
23 2010-09-28 16:52:13,732 [INFO] pool-1-thread-5 (ExportReportListenerImpl.addCurrentObjectInfo:181) - Predefined Reference Data-Generic Attribu
24 2010-09-28 16:52:13,732 [INFO] pool-1-thread-5 (ExportReportListenerImpl.addCurrentObjectInfo:181) - Predefined Reference Data-Generic Attribu
25 2010-09-28 16:52:13,732 [INFO] pool-1-thread-5 (ExportReportListenerImpl.addCurrentObjectInfo:181) - Predefined Reference Data-Generic Attribu
26 2010-09-28 16:52:13,732 [INFO] pool-1-thread-5 (ExportReportListenerImpl.addCurrentObjectInfo:181) - Predefined Reference Data-Generic Attribu
27 2010-09-28 16:52:13,732 [INFO] pool-1-thread-5 (ExportReportListenerImpl.addCurrentObjectInfo:181) - Predefined Reference Data-Generic Attribu
28 2010-09-28 16:52:13,732 [INFO] pool-1-thread-5 (ExportReportListenerImpl.addCurrentObjectInfo:181) - Predefined Reference Data-Generic Attribu

```

図 1-2 インポート レポートの例

```

=====
Migration Report
Migration Phase: Import into ISE
Date: Tue Sep 28 17:05:59 IST 2010
Machine: 10.56.13.190
=====

=====Object Group=====
Object Group: Predefined Reference Data
=====Object Group=====
Object Group: Dictionaries
=====Object Type=====
Object Type: VSA Vendors

Info Type: INFO
> 2010.09.28 17:06:07'055 : Added configuration: Cisco VPN 5000
> 2010.09.28 17:06:07'945 : Added configuration: US Robotics
> 2010.09.28 17:06:08'633 : Added configuration: Ascend
> 2010.09.28 17:06:09'367 : Added configuration: Nortel ( Bay )
> 2010.09.28 17:06:10'117 : Added configuration: RedCreek
> 2010.09.28 17:06:10'867 : Added configuration: Juniper
> 2010.09.28 17:06:11'586 : Added configuration: Cisco Aironet
> 2010.09.28 17:06:12'320 : Added configuration: Cisco Airespace

=====Object Type=====
Object Type: RADIUS VSAs

Info Type: INFO
> 2010.09.28 17:06:13'523 : Added configuration: Cisco
> 2010.09.28 17:06:14'148 : Added configuration: Cisco
> 2010.09.28 17:06:14'774 : Added configuration: Cisco
> 2010.09.28 17:06:15'477 : Added configuration: Cisco
> 2010.09.28 17:06:16'086 : Added configuration: Cisco
> 2010.09.28 17:06:16'680 : Added configuration: Cisco
> 2010.09.28 17:06:17'430 : Added configuration: Cisco
> 2010.09.28 17:06:18'242 : Added configuration: Cisco
> 2010.09.28 17:06:18'867 : Added configuration: Cisco
> 2010.09.28 17:06:19'477 : Added configuration: Cisco
> 2010.09.28 17:06:20'070 : Added configuration: Cisco
> 2010.09.28 17:06:20'664 : Added configuration: Cisco
> 2010.09.28 17:06:21'305 : Added configuration: Cisco
> 2010.09.28 17:06:21'914 : Added configuration: Cisco
> 2010.09.28 17:06:22'539 : Added configuration: Cisco
> 2010.09.28 17:06:23'180 : Added configuration: Cisco
> 2010.09.28 17:06:23'774 : Added configuration: Cisco
> 2010.09.28 17:06:24'383 : Added configuration: Cisco

```

282105

図 1-3 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 1.1 は、いくつかの管理設定に対して Universal Character Set Transformation Format 8 ビット (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せん。
 - [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-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 のバージョンを特定します。Cisco Secure ACS のバージョンが 5.1 よりも古い場合、または 5.2 よりも新しい場合、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 のバージョンが 1.1 であることを検証します。



CHAPTER 2

Cisco Secure ACS-Cisco ISE Migration Tool について

この章には、Cisco Secure Access Control System (ACS) -Cisco Identity Services Engine (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 5.1/5.2 データベースから Cisco ISE Release 1.1 アプライアンスヘデータを移行します。以下のトピックでは、Cisco Secure ACS-Cisco ISE Migration Tool を使用してデータを移行する前に、このツールについて理解しておく必要がある情報について説明します。

- 「概要 : Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 へ」 (P.2-1)
- 「Cisco Secure ACS-Cisco ISE Migration Tool」 (P.2-2)

概要 : Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 へ

Cisco Secure ACS-Cisco ISE Migration Tool は、Cisco Secure ACS 5.1/5.2 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 1.1 アプライアンスヘ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。Cisco Secure ACS-Cisco ISE Migration Tool を使用した移行プロセスには、以下の3つの手順があります。

- Cisco Secure ACS 5.1/5.2 のデータベースからデータをエクスポートする
- 移行ツールを使用してこのデータを保持する
- 保持しているデータを Cisco ISE 1.1 アプライアンスヘインポートする

Cisco Secure ACS-Cisco ISE Migration Tool は、Cisco Secure ACS 5.1/5.2 データから Cisco ISE 1.1 アプライアンスへのデータ移行のみをサポートしています。たとえば、Cisco Secure ACS-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 5.1/5.2 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である Cisco Secure ACS-1121 ハードウェア アプライアンスを、Cisco ISE 1.1 ソフトウェアで再作成します。
4. 変換した Cisco Secure ACS Release 5.1/5.2 のデータを、セキュアな外部サーバから Cisco ISE 1.1 アプライアンスヘインポートします。

Cisco Secure ACS-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 5.1/5.2 システムから Cisco ISE 1.1 アプライアンスへの移行のみです。ただし、表 2-1 に記載されているオプションを使用して、Cisco Secure ACS の古いバージョンのデータを Cisco Secure ACS 5.1/5.2 のステートへアップグレードすることが可能です。

Cisco Secure ACS-Cisco ISE Migration Tool は、Cisco Secure ACS 5.1/5.2 システムから Cisco ISE 1.1 アプライアンスへデータを移行します。これは、Cisco Secure ACS 3.x ~ 4.x の古いバージョンで 사용되는アップグレードとは別のプロセスです。

表 2-1 Cisco Secure ACS リリースのデータ アップグレード オプション

ACS リリース バージョン	アップグレード先の ACS リリース	ACS データ アップグレード リファレンス
Cisco Secure ACS Release 3.x	Cisco Secure ACS Release 5.0	• 第 5 章「Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行」
Cisco Secure ACS Release 4.x	Cisco Secure ACS Release 5.0	• 第 5 章「Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行」
Cisco Secure ACS Release 5.0	Cisco Secure ACS Release 5.1/5.2	• 第 5 章「Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行」



(注)

Cisco Secure ACS 3.x、4.x ~ 5.0 から Cisco Secure ACS 5.1/5.2 への移行に関する情報およびマニュアルのリンクについては、第 5 章「Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行」を参照してください。第 5 章には、Cisco Secure ACS 5.0 から Cisco Secure ACS 5.1/5.2 への移行に関する情報およびマニュアルのリンクも記載されています。

Cisco Secure ACS-Cisco ISE Migration Tool

この章の内容は次のとおりです。

- 「移行ツールのコンポーネント」(P.2-4)
- 「データ構造マッピング」(P.2-5)

Cisco Secure ACS-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 1.1 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 5.1/5.2 および Cisco ISE 1.1 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 ISE アプリケーションは、サポートされているすべてのハードウェア 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。

図 2-1 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 2-1 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

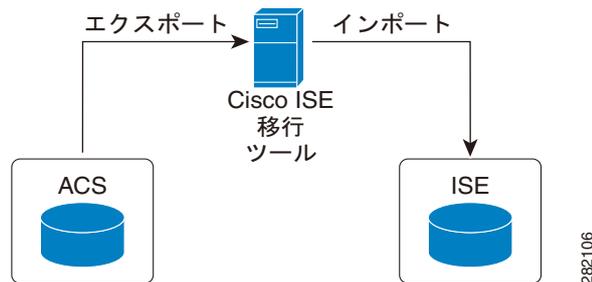


図 2-2 は、Cisco ISE ソフトウェアがインストールされるアプライアンスと同じアプライアンス上に、Cisco Secure ACS がインストールされている展開シナリオを示しています（シングルアプライアンス展開）。シングルアプライアンス展開では、以下の手順を完了します。

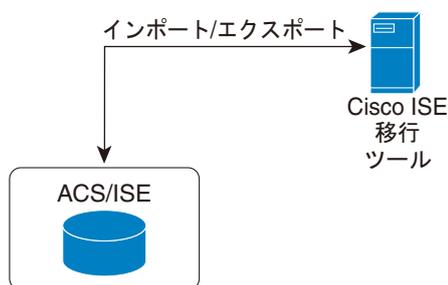
- ステップ 1 Cisco Secure ACS-Cisco ISE Migration Tool を、スタンドアロンの Windows マシンにインストールします。
- ステップ 2 Cisco Secure ACS アプライアンスから Cisco Secure ACS 5.1/5.2 データをエクスポートします。
- ステップ 3 Cisco Secure ACS のデータをバックアップします。
- ステップ 4 アプライアンスを Cisco ISE 1.1 ソフトウェアで再作成します。
- ステップ 5 Cisco Secure ACS 5.1/5.2 のデータを Cisco ISE 1.1 アプライアンスへインポートします。



(注)

Cisco Secure ACS 5.1/5.2 のデータを Cisco ISE 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場合のみ、その後で何らかの展開設定（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 1.1』を参照してください。

図 2-2 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



282107

移行ツールのコンポーネント

移行アプリケーション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.2-4)
- 「ステータス報告」 (P.2-4)
- 「エクスポートおよびインポート」 (P.2-4)

データ設定

移行プロセスの開始時には、入力として設定データの最小セットが必要です。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

インポートおよびエクスポートの処理は、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。これらの手順は、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。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。これらのチェックポイントにより、何らかの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。

エクスポートおよびデータの持続性

Cisco Secure ACS PI を使用して Cisco Secure ACS 5.1/5.2 データベースから Cisco Secure ACS データをエクスポートする場合、エクスポート コンポーネントは移行フェーズの間、アクティブになります。Cisco Secure ACS システムに接続し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、および認証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 5.1/5.2 ソフトウェアをアンインストールし、Cisco ISE 1.1 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-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-Cisco ISE Migration Tool は Cisco Secure ACS から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 ACS 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、問題およびデータ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 5.1/5.2 から Cisco ISE 1.1 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、Cisco Secure ACS-Cisco ISE Migration Tool によって各データ 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情報マッピングの完全なリストについては、[付録 A 「Cisco Secure ACS 5.1/5.2 および Cisco ISE 1.1 のデータ構造マッピング」](#)を参照してください。



CHAPTER 3

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

この章では、Cisco Secure Access Control System (ACS) -Cisco Identity Services Engine (ISE) Migration Tool のインストールに関する情報を提供します。また、重要な移行ツールのインストールに関する考慮事項、および移行プロセスについて以下のトピックで説明します。

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

移行ツールのインストール ガイドライン

インストールを開始する前に、次のガイドラインをよく読んでください。

- 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 5.1/5.2 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、およびターゲット システムとして、Cisco ISE 1.1 アプライアンスを展開する必要があります。
- Cisco Secure ACS 5.1/5.2 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。
- ACS から ISE への移行が同じアプライアンス上で実行される場合に備えて、ACS 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。
 - Cisco ISE 1.1 がターゲット マシン上にインストールされている (デュア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 1.1 のソフトウェアがある (シングルアプライアンスの移行の場合)。
 - Cisco Secure ACS 5.1/5.2 と Cisco ISE 1.1 の正しい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、データベースを備えている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ようにします。

システム要件

Cisco Secure ACS マシンは表 3-1 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 3-1 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 5.1/5.2 のソースマシン	『 Installation Guide for Cisco Secure ACS for Windows 5.1 』を参照してください。Cisco Secure ACS 5.1 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 1.1 ターゲットマシン	次のマニュアルを参照してください。 <ul style="list-style-type: none"> • Cisco Identity Services Engine Hardware Installation Guide, Release 1.1 • Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1 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 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 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 5.1/5.2 および Cisco ISE 1.1 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。

データの移行および展開のシナリオ

Cisco Secure ACS-ISE Migration Tool は、Cisco Secure ACS 5.1/5.2 のデータオブジェクトを Cisco ISE 1.1 へ移行する目的で設計されています。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移行のガイドライン](#)」 (P.3-3)
- 「[分散環境におけるデータ移行のガイドライン](#)」 (P.3-3)

シングル Cisco Secure ACS アプライアンスからのデータ移行のガイドライン

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、「[ログインおよび移行ツールの使用 \(P.4-1\)](#)」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。

分散環境におけるデータ移行のガイドライン

分散環境で Cisco Secure ACS を実行することができます。たとえば、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るとします。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-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。



(注) Cisco Secure ACS 5.1/5.2 のデータを Cisco ISE 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場合のみ、その後で何らかの展開設定 (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。

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



(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。

Cisco ISE ユーザ インターフェイスを使用して Cisco Secure ACS-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-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 バーで以下のコマンド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。

- ステップ 2** 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インストールされている場合、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、移行ツール ファイルの migTool.zip を以下の場所からダウンロードします。

<http://www.cisco.com/cisco/software/release.html?mdfid=283801620&flowid=26081&softwareid=283802505&release=1.1&reind=AVAILABLE&rellifecycle=&reltype=latest>

- ステップ 3** .zip ファイルを解凍します。図 3-1 は、Cisco Secure ACS-Cisco ISE Migration Tool ソフトウェアのディレクトリ構造を示しています。

図 3-1 Cisco ACS 5.1/5.2-Cisco ISE 1.1 Migration Tool のディレクトリ構造

Name	Size	Type	Date Modified
bin		File Folder	1/24/2011 4:00 PM
lib		File Folder	1/24/2011 4:00 PM
config.bat	1 KB	MS-DOS Batch File	1/23/2011 8:09 PM
migration.bat	1 KB	MS-DOS Batch File	1/23/2011 8:09 PM
migStart.sh	1 KB	SH File	1/23/2011 8:09 PM

282108

- ステップ 4** **config.bat** ファイルを編集して、移行プロセス用の Java ヒープ サイズに対してメモリの初期量を割り当てます (図 3-2 を参照してください)。メモリは、それぞれ 64 メガバイト、512 メガバイトにします。

図 3-2 Java ヒープ サイズの設定

```

1  @echo off
2  rem *****
3  rem          Copyright (c) 2010 Cisco Systems, Inc.
4  rem          All rights reserved.
5  rem *****
6
7  rem Setting java Heap Sizes
8  rem To set the initial amount of memory allocated for.
9  set Xms=64M
10 set Xmx=512M ]

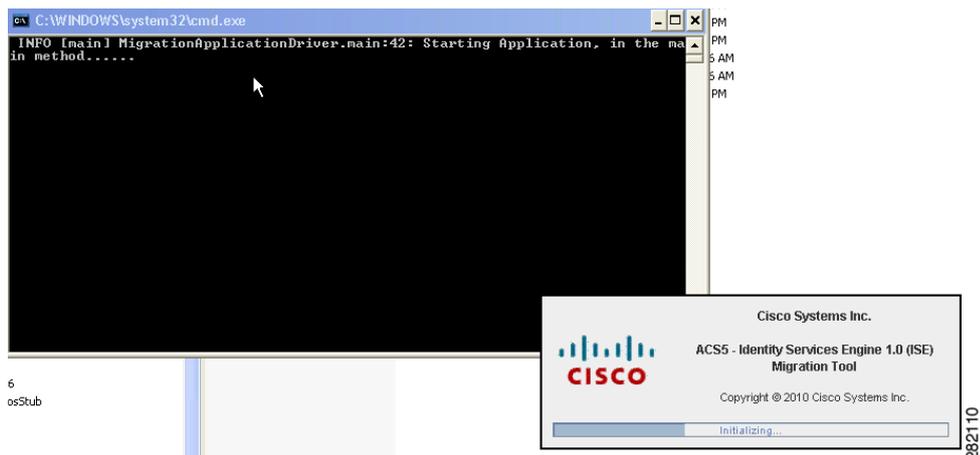
```

ステップ 5 [保存 (Save)] をクリックしてヒープ サイズの設定を保持します。

ステップ 6 **migration.bat** をクリックして移行プロセスを起動します。

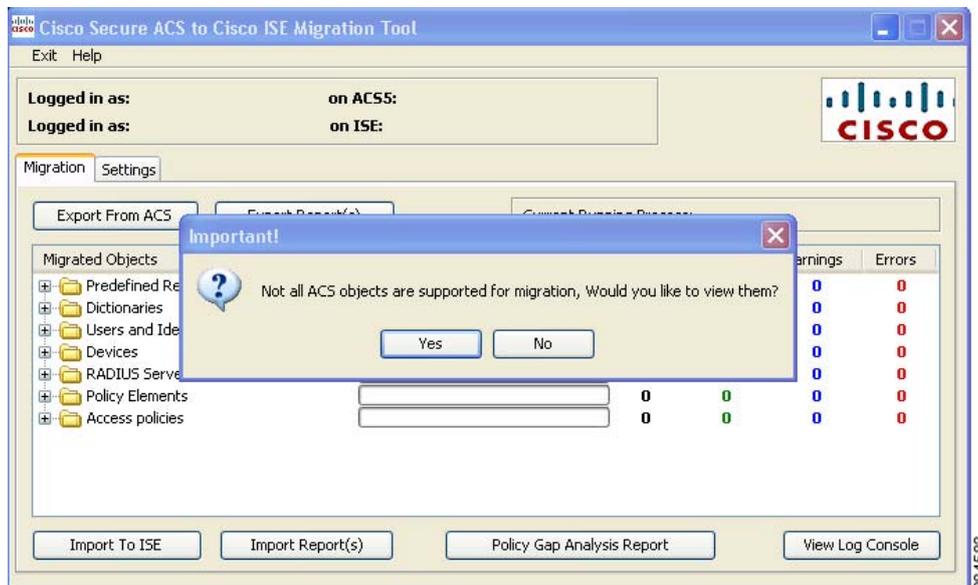
初期化画面が表示されます (図 3-3 を参照してください)。

図 3-3 初期化画面



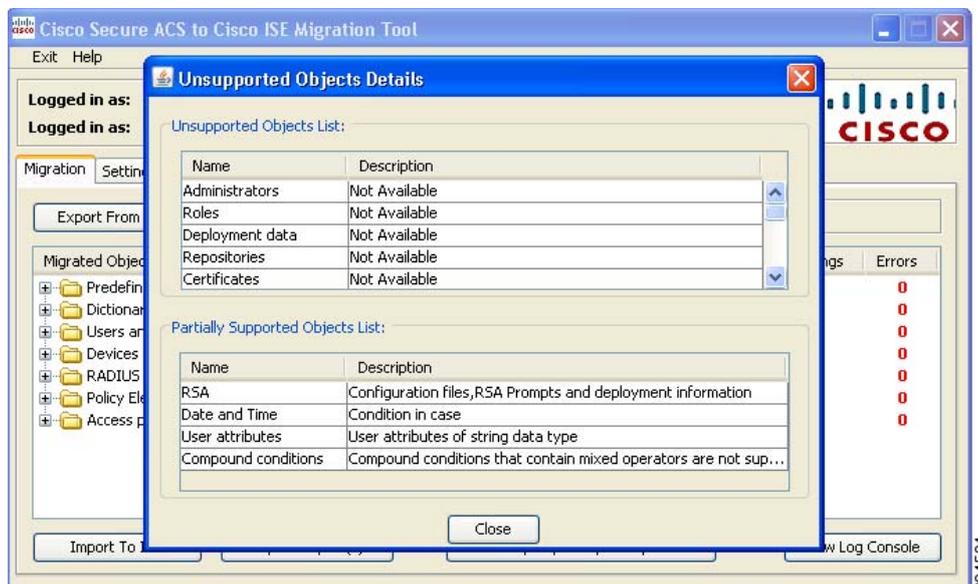
移行ツールが初期化された後でも、サポートされていない Cisco Secure ACS オブジェクトを引き続き移行する必要があります。以下のメッセージが表示されます (図 3-4 を参照してください)。

図 3-4 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 7 [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 3-5 を参照してください)。

図 3-5 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 8 [閉じる (Close)] をクリックします。

[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。

移行ツールを実行するには、[第4章「Cisco Secure ACS-Cisco ISE Migration Tool の使用」](#)を参照してください。



CHAPTER 4

Cisco Secure ACS-Cisco ISE Migration Tool の使用

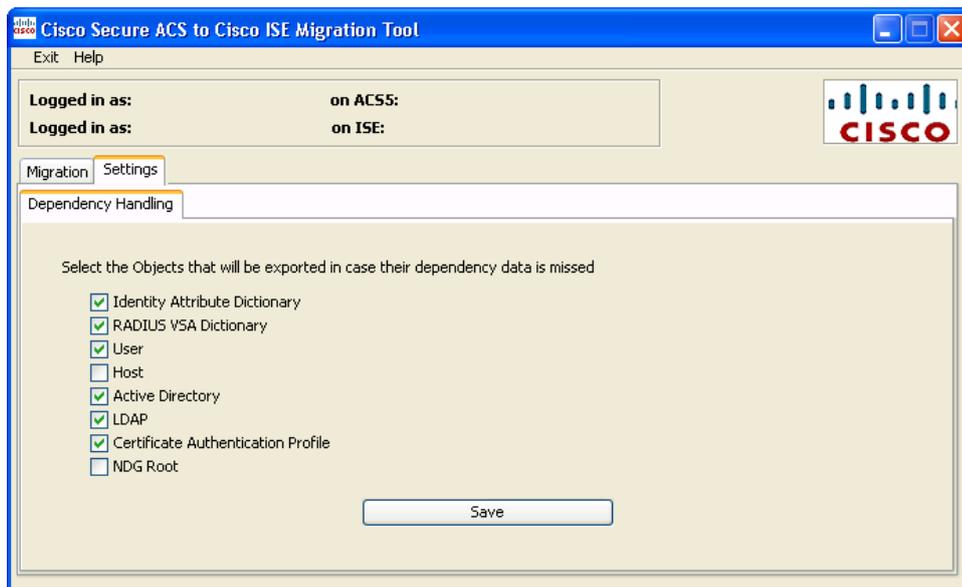
この章では、Cisco Secure Access Control System (ACS) -Cisco Identity Services Engine (ISE) Migration Tool を使用して、Cisco Secure ACS 5.1/5.2 のデータベースから Cisco ISE 1.1 アプリアンスヘデータを移行する方法について説明します。以下のトピックには、移行プロセスを実行する手順が含まれています。

- 「ログインおよび移行ツールの使用」(P.4-1)
- 「インポートプロセスの検証」(P.4-9)
- 「レポートファイルの提供」(P.4-10)

ログインおよび移行ツールの使用

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 5.1/5.2 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-Cisco ISE Migration Tool のメイン ウィンドウで [設定 (Settings)] をクリックして、移行するデータ オブジェクトのリストを表示します。

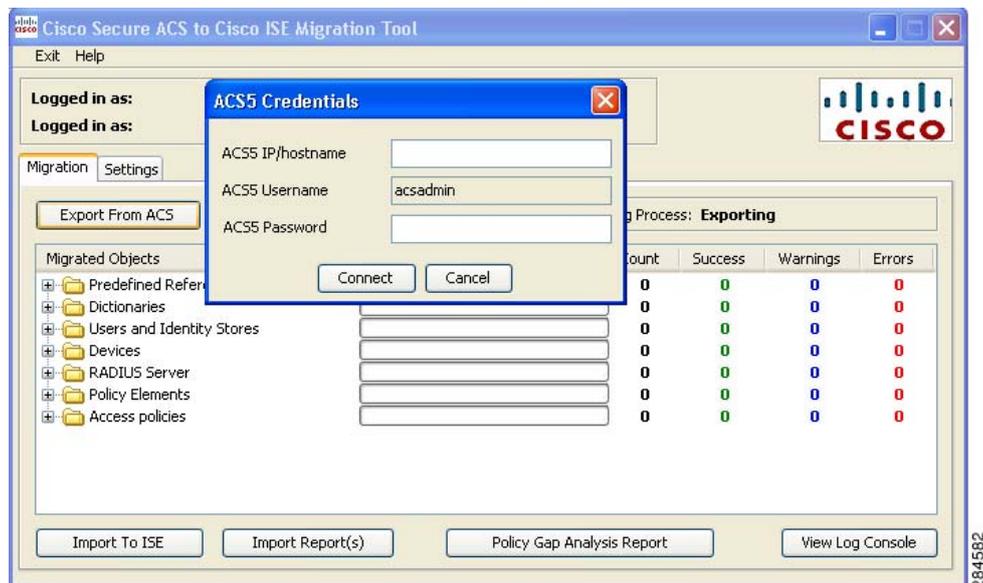


ログインおよび移行ツールの使用

ステップ 2 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 ボックスをクリックして選択し、[保存 (Save)] をクリックします。

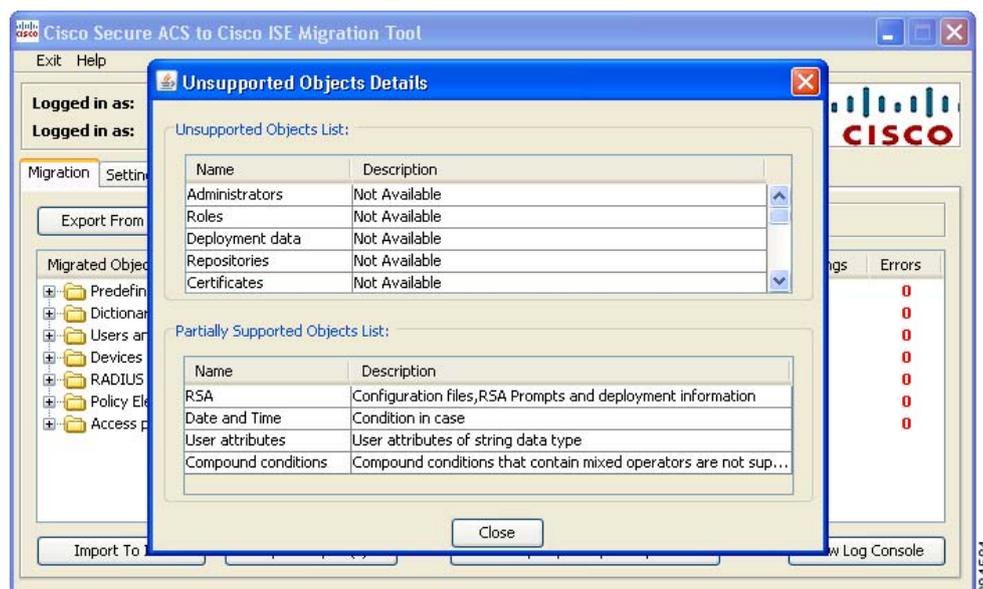
ステップ 3 Cisco Secure ACS-Cisco ISE Migration Tool のメイン ウィンドウで [移行 (Migration)]、および [ACS からのエクスポート (Export from ACS)] をクリックします。

Cisco Secure ACS 5.1/5.2 システムの [ログイン (Login)] ウィンドウが表示されます。

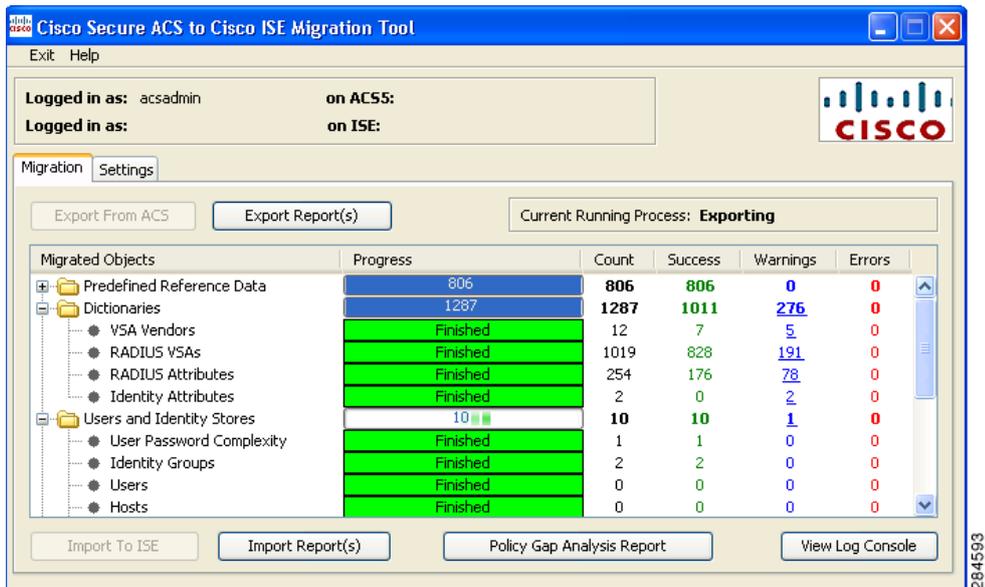
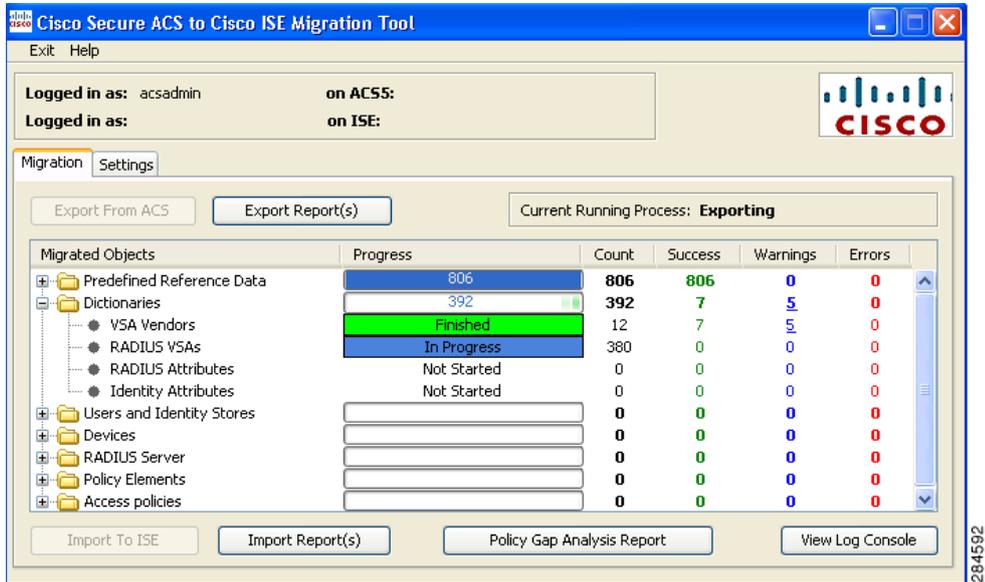


ステップ 4 [ACS クレデンシャル (ACS Credential)] ウィンドウに Cisco Secure ACS 5.1/5.2 システムの IP アドレス (またはホスト名) とパスワードを入力して [接続 (Connect)] をクリックします。

データの移行プロセスが開始されます。



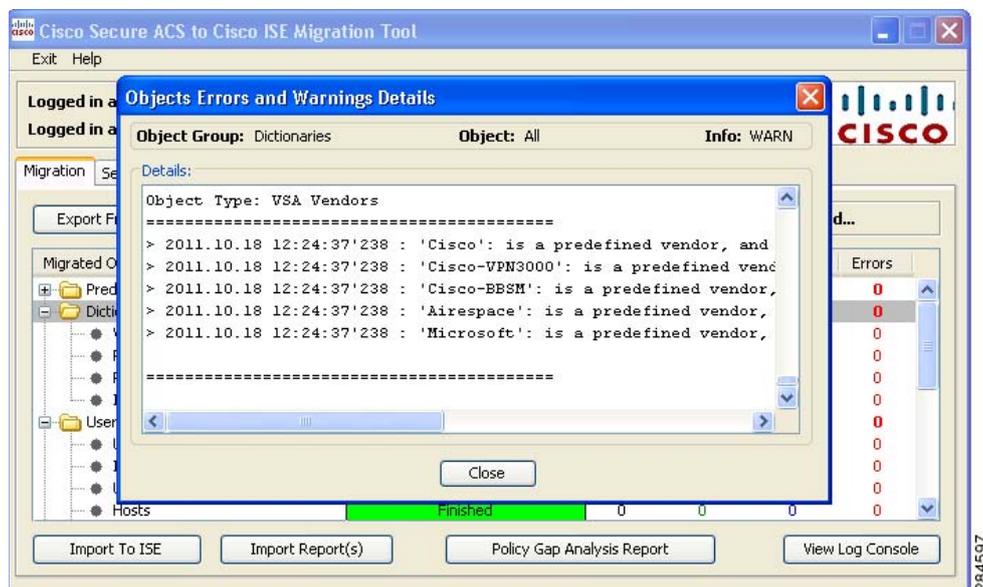
ステップ 5 Cisco Secure ACS-Cisco ISE Migration Tool のメイン ウィンドウを参照して、Cisco Secure ACS 5.1/5.2 のデータ移行の進捗を確認します。



Cisco Secure ACS-Cisco ISE Migration Tool のメイン ウィンドウに、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。

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詳しい情報を取得するには、表に記載されている [警告 (Warnings)] または [エラー (Errors)] をクリックします。以下の例は、表示されるエラーを選択して返される結果を示しています。

[オブジェクト エラーと警告の詳細 (Object Errors and Warnings Details)] ウィンドウが表示され、エラーが発生したオブジェクト グループ、タイプ、および日時が表示されます。

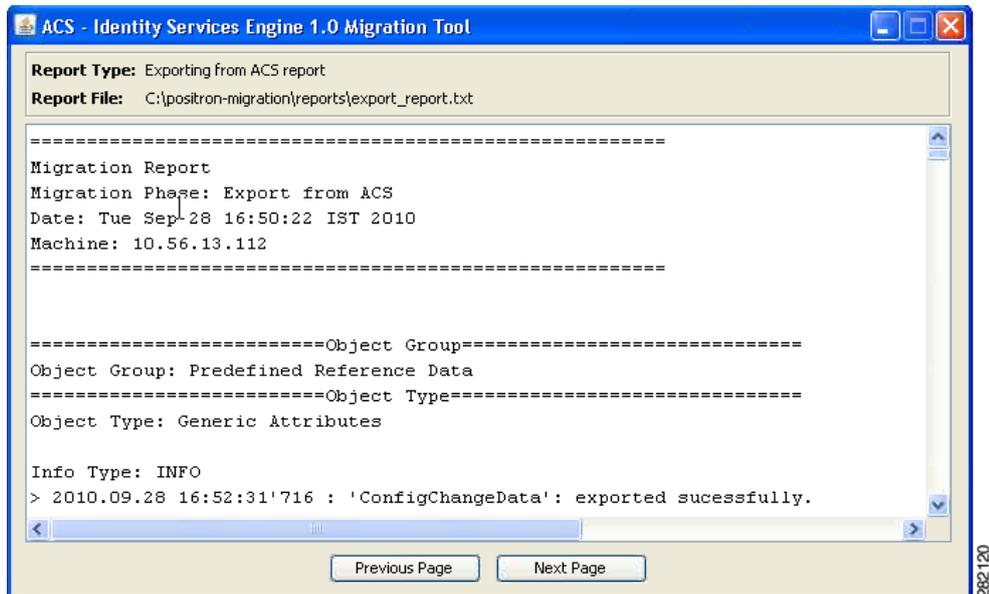


ステップ 7 詳細がすべて表示されるまで右へスクロールし、[閉じる (Close)] をクリックしてウィンドウを閉じます。

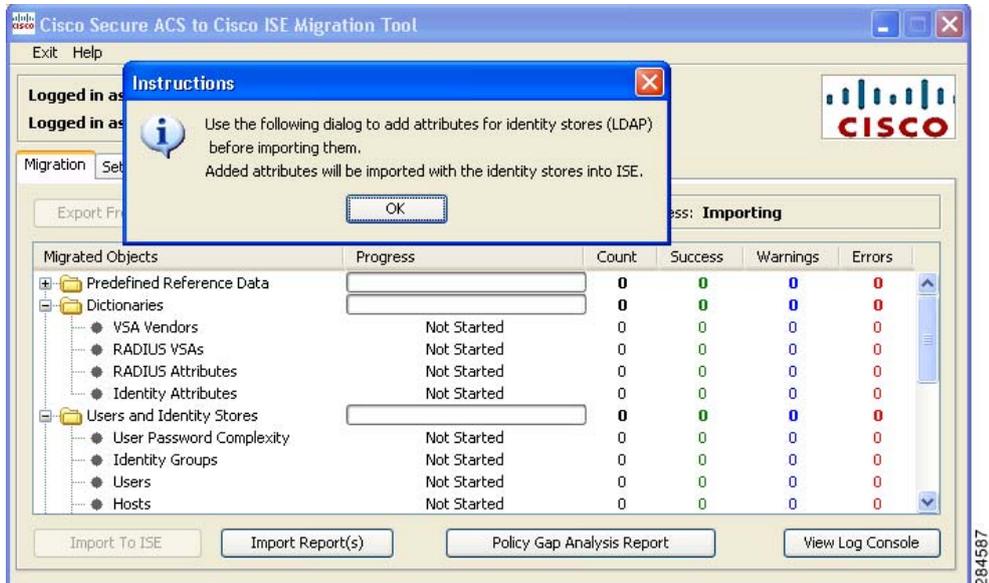
Cisco Secure ACS 5.1/5.2 システムからのデータ エクスポート プロセスが完了する ([エクスポート完了 (Exporting finished...)]) と、Cisco Secure ACS-Cisco ISE Migration Tool のメイン ウィンドウにこのステータスが表示されます。

ステップ 8 [エクスポート レポート (Export Report(s))] をクリックしてレポートの内容を表示します。これは、以下の例に示すようにエクスポート処理を要約しています。

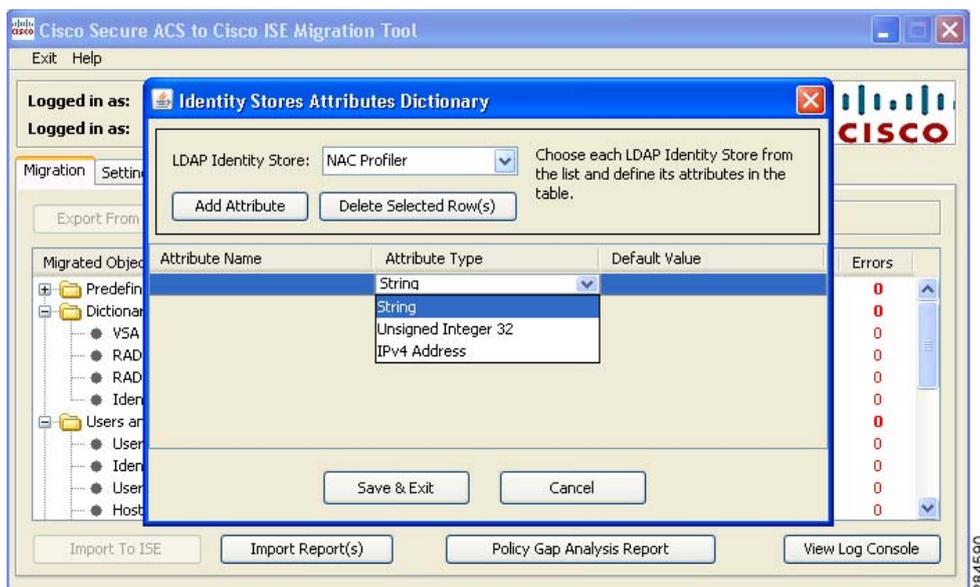
各エクスポート レポートには、ヘッダー情報、および処理のタイプ、日時、およびシステムの IP アドレスまたはホスト名が含まれています。各オブジェクト グループには、そのグループのオブジェクトのタイプ、および関連情報の詳細が記載されます。各レポートの最後には、開始と終了の日時、および処理の期間をまとめたレポートが付随しています。



- ステップ 9** Cisco ISE アプライアンスへ、このデータのインポートを開始するには、Cisco Secure ACS-Cisco ISE Migration Tool のメイン 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。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ます。

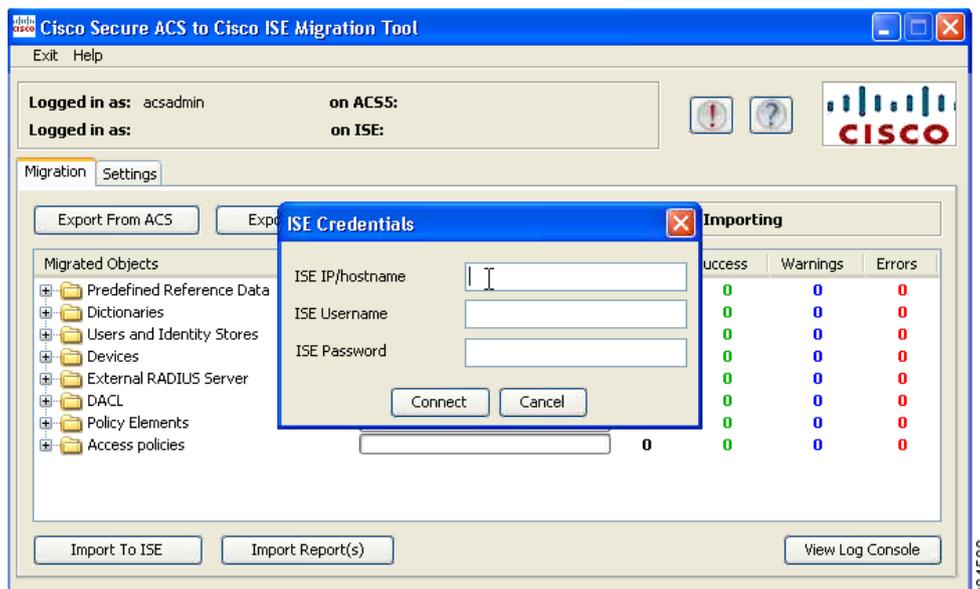


- ステップ 10** [OK] をクリックして、LDAP ID ストアへの属性追加プロセスを開始します。
- ステップ 11** [LDAP ID ストア (LDAP Identity Store)] ドロップダウンリストで、属性を追加する ID ストアを選択します。

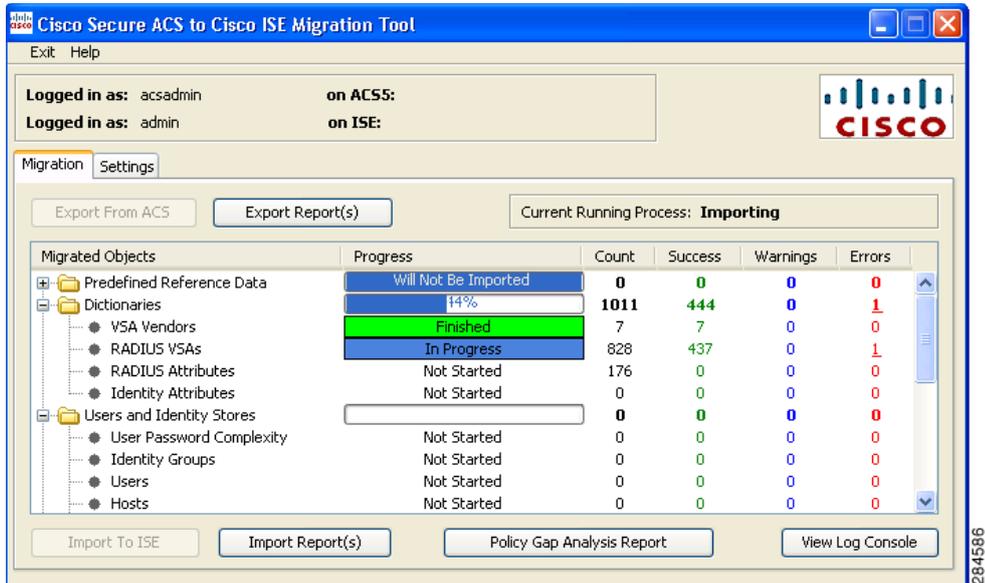


ステップ 12 [属性名 (Attribute Name)] フィールドに名前を入力し、[属性タイプ (Attribute Type)] ドロップダウンリストから属性タイプを選択します。[デフォルト値 (Default Value)] フィールドに値を入力して [保存して終了 (Save & Exit)] をクリックします。

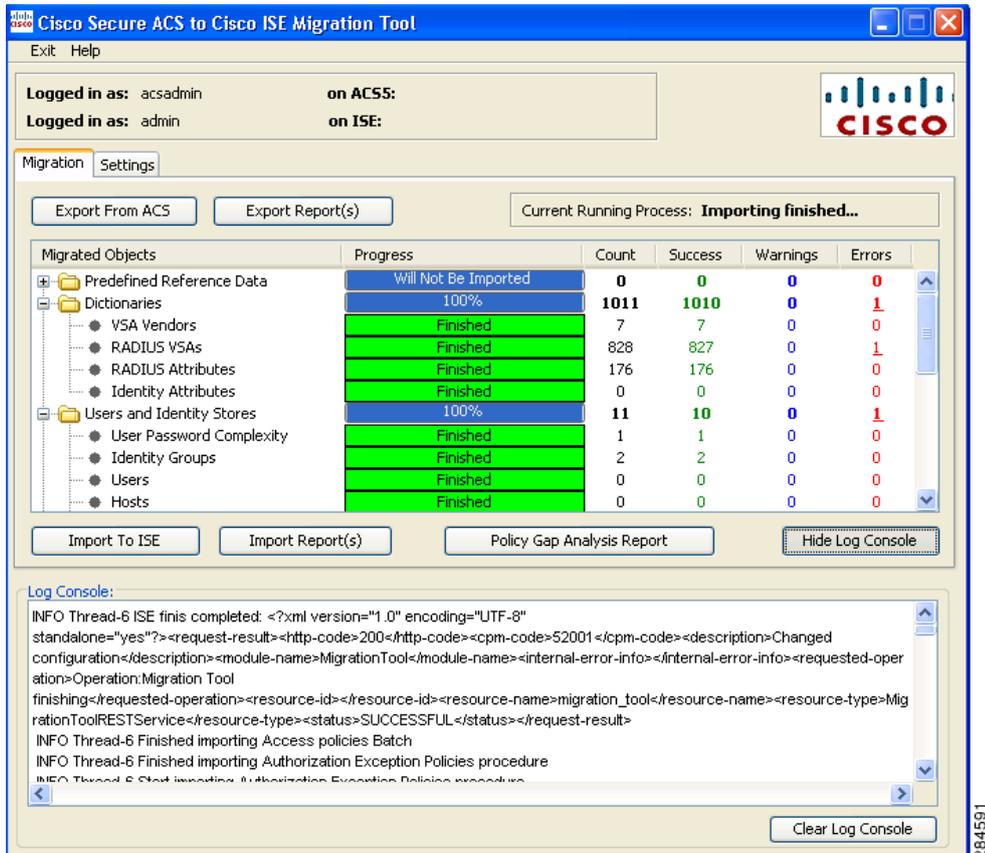
ステップ 13 属性の追加が終了したら、[ISE へのインポート (Import to ISE)] をクリックしてインポートプロセスを続行し、[ISE クレデンシアル (ISE Credentials)] ウィンドウを使用して Cisco ISE ヘログインします。



ステップ 14 必要に応じて ISE の IP アドレス (またはホスト名)、ISE のユーザ名、および ISE のパスワードを入力し、[接続 (Connect)] をクリックして、Cisco ISE アプライアンスヘデータのインポートを開始します。



ステップ 15 インポートまたはエクスポートのプロセスの任意のタイミングで [ログ コンソールの表示 (View Log Console)] をクリックすると、インポートまたはエクスポート処理の現在のステータスをリアルタイムで表示できます。

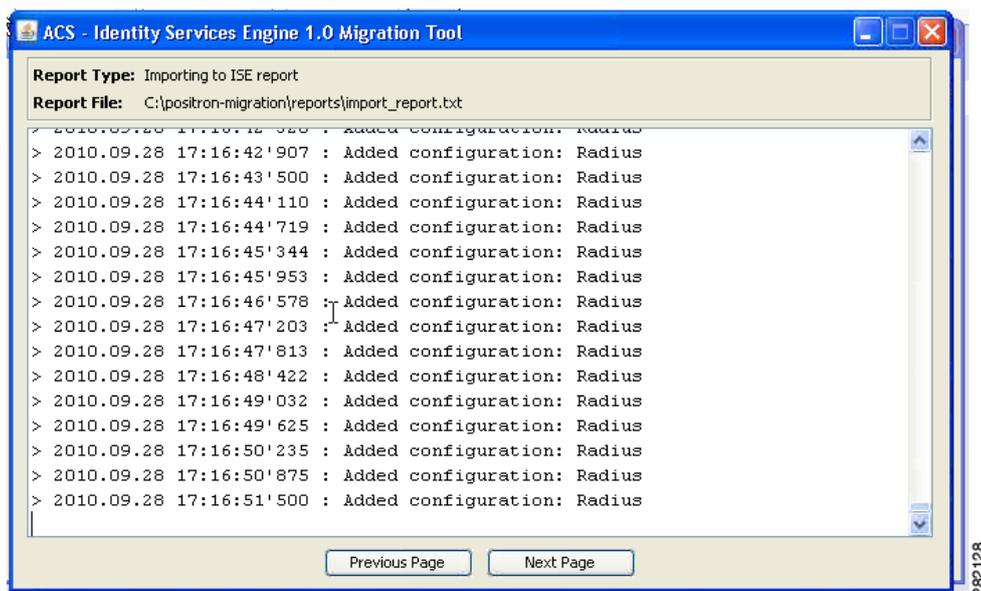


ログインおよび移行ツールの使用

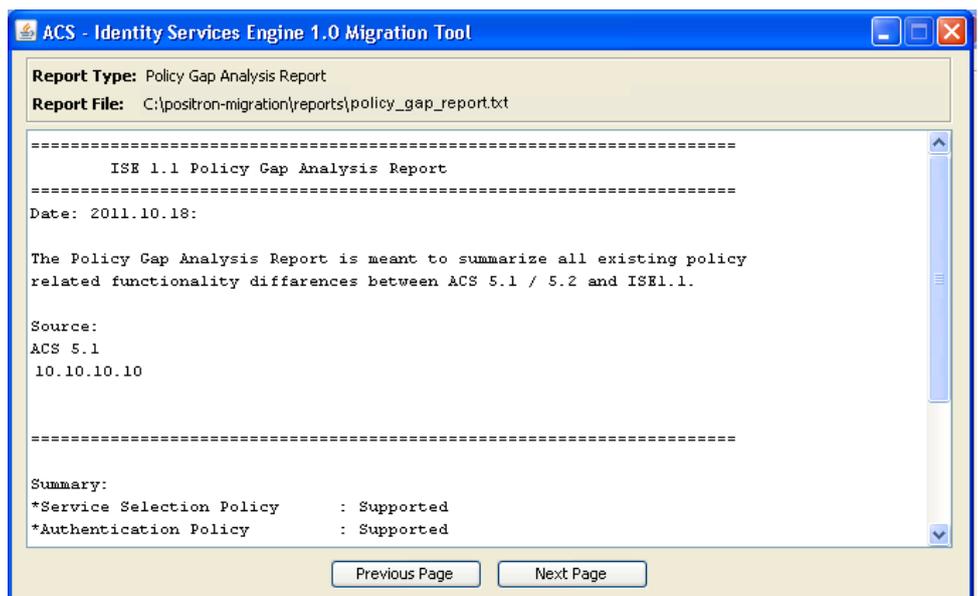
ステップ 16 インポート プロセスで発生した警告またはエラーについては、(手順 6 を参照して) 表に記載されている [警告 (Warnings)] または [エラー (Errors)] をクリックして詳細を表示します。

データのインポート処理が完了すると、Cisco Secure ACS-Cisco ISE Migration Tool のメイン ウィンドウにこのステータスが表示されます。

ステップ 17 Cisco ISE 1.1 アプライアンスへ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。レポートが表示されます。



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。レポートが表示されます。



インポート プロセスの検証

インポート プロセスが完了したことを検証するには、以下の手順を完了します。

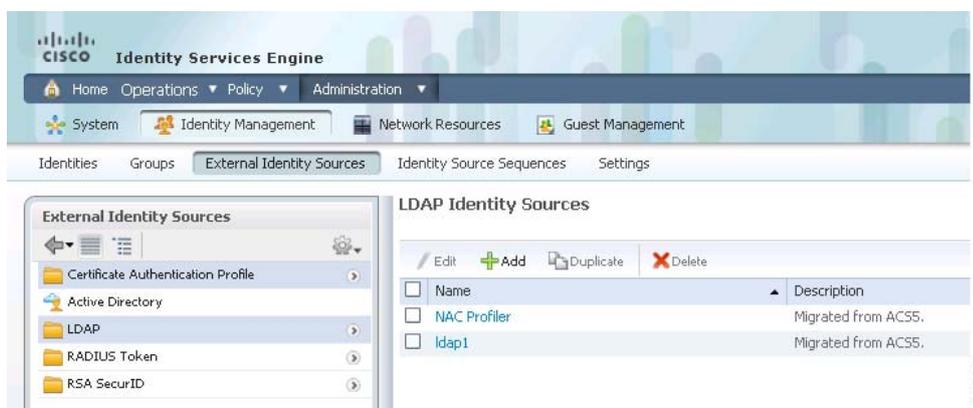
ステップ 1 Cisco ISE 1.1 アプライアンスへログインします。

- 正しいユーザ名とパスワードを入力します。
- [ログイン (Login)] をクリックします。



ステップ 2 たとえば、Cisco ISE のメイン ウィンドウで [管理 (Administration)] > [ID 管理 (Identity Management)] > [外部 ID ソース (External Identity Source)] > [LDAP] を選択し、[LDAP ID ソース (LDAP Identity source)] ウィンドウを表示して、何らかの ACS ベースの LDAP ID ソースがインポートされたかどうかを確認します。

ユーザ、またはその他の属性に対して同様の検証を実行し、インポートが正常に行われたかどうか確認することができます。



これで、Cisco Secure ACS-Cisco ISE Migration Tool の使用によるインポート/エクスポート処理は終了です。

レポート ファイルの提供

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 フォルダに以下のレポート ファイルがあります。

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



CHAPTER 5

Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行

この章では、以前の Cisco Secure Access Control System (ACS) 3.x release または 4.x release から Cisco Secure ACS 5.0 release のステートヘデータを移行する方法が記載されている Cisco のマニュアルへのリンクを提供します。Cisco Secure ACS 5.0 は、Cisco Secure ACS の以前のリリースのデータを Cisco Secure ACS 5.1/5.2 へ移行するために必要なステップです。

以前のリリースから Cisco Secure ACS 5.1/5.2 のステージへ、データの移行が正常に終了したら、Cisco Identity Services Engine (ISE) Release 1.1 アプライアンスヘデータを移行できます。以下のトピックでは、この情報について説明しています。

- [「概要」 \(P.5-1\)](#)
- [「Cisco Secure ACS の以前のリリースからの移行」 \(P.5-2\)](#)

概要

データを Cisco ISE 1.1 アプライアンスへ移行するための何らかの試行を開始する前に、[第 3 章「Cisco Secure ACS-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。

Cisco ISE 1.1 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-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。次に、例を示します。

- 移行前のステージが Cisco Secure ACS 3.x または 4.x の場合は、最初にデータを Cisco Secure ACS 5.0 へ移行する必要があります。
- Cisco Secure ACS 5.0 へのデータ移行が終了している場合、または最初に Cisco Secure ACS 5.0 から移行する場合は、データを Cisco Secure ACS Release 5.1/5.2 へ移行する必要があります。
- Cisco Secure ACS Release 5.1/5.2 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 5.1/5.2 から移行する場合は、Cisco Secure ACS-Cisco ISE Migration Tool を使用してデータを Cisco ISE 1.1 アプライアンスへ移行できます。

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 1.1 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 のマニュアルへのリンクが含まれています。

Cisco Secure ACS Release 3.x または 4.x のデータを Cisco Secure ACS 5.0 へ移行する

Cisco Secure ACS Release 3.x または 4.x から Cisco Secure ACS Release 5.0 へのデータ移行については、以下のリンクを参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/migration/guide/migrationguide.html

Cisco Secure ACS Release 5.0 から Cisco Secure ACS 5.1/5.2 へデータを移行する

Cisco Secure ACS Release 5.0 から Cisco Secure ACS Release 5.1/5.2 へのデータ移行については、以下のリンクを参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/migration/guide/Migration_Book.html



APPENDIX **A**

Cisco Secure ACS 5.1/5.2 および Cisco ISE 1.1 のデータ構造マッピング

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)
- 「一般的な移行ルール」 (P.A-3)
- 「移行ポリシー」 (P.A-3)
- 「サポート対象属性およびデータ型」 (P.A-4)
- 「データ情報マッピング」 (P.A-6)

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) 5.1/5.2 から Cisco Identity Services Engine (ISE) 1.1 へ移行されます。

- 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 Windows 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、移行ポリシーを参照)
- 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 (「一般的な移行ルール」(P.A-3) を参照)
- 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.1-8) を参照)

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 ACS 5.1/5.2 から Cisco ISE 1.1 へ移行されません。

- 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)
- Security Group (SG)
- サポートされている Security Group Access (SGA) デバイスの AAA サーバ
- SG マッピング
- Network Device Admission Control (NDAC) ポリシー
- SGA 出力マトリクス (SGA)
- 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)
- デバイス管理認証および許可ポリシー

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 ACS 5.1/5.2 から Cisco ISE 1.1 へ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）。

一般的な移行ルール

Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 へデータを移行する場合に、以下の移行ルールを考慮します。

- 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。
- 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。

移行ポリシー

認証および許可ポリシーは、Cisco Secure ACS から Cisco ISE へ移行されます。ACS と ISE には簡易認証およびルールベースの認証の両方のパラダイムがありますが、ACS と ISE は別のポリシー モデルに基づいています。ACS と ISE のポリシー モデルが異なるために、すべての ACS ポリシーおよびルールを移行することはできません。主な理由は以下のとおりです。

- 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（「begin with」など）

ルールを移行できない場合は、ポリシー全体は移行されず、その理由と詳細が Policy Gap Analysis レポートに記載されます。レポートを表示して、問題のあるルールを削除または修正することができます。Policy Gap Analysis レポートの詳細については、「[レポート](#)」(P.1-5) を参照してください。



(注) 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。

Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行ポリシーのガイドラインは以下のとおりです。

- 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。
- 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。
- 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。

- 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。
- 以下のオペランドは、条件内ではサポートされていません。
 - **String** : start with、end with、contains、not contains
 - **Date and time** : not in
 - **Identity group** : not in

条件内でこれらのオペランドを使用しているルールも移行されません。

- `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は移行されません。`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 사용할ことができます。
- 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。
- Cisco ISE は TACACS をサポートしていません。このため、TACACS 属性を使用しているすべての ACS ルールは移行されません。



(注)

エクスポート フェーズ中に、Cisco ACS 5.1/5.2-ISE 1.1 Migration Tool が、(このセクションに記載されている移行ガイドラインのいずれかと照合して) 認証ポリシーと許可ポリシー間の差異を認識した場合は、Policy Gap Analysis レポートに記載されます。差異が認識された場合、移行の実施管理者は、責任を持ってルールの修正または削除を行う必要があります。このようなルール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。

サポート対象属性およびデータ型

以下の表に、移行されるサポート対象の属性、およびそのターゲット データ型を記載しています。

表 A-1 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 へ移行されるユーザ属性

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
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 5.1/5.2	Cisco ISE 1.1
String	サポート
UI32	—
IPv4	—

表 A-2 ユーザ属性：ユーザとの関連（続き）

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
Boolean	—
Date	—

表 A-3 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 へ移行されるホスト属性

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
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 5.1/5.2	Cisco ISE 1.1
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 5.1/5.2 から Cisco ISE 1.1 へ移行される RADIUS 属性

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
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 5.1/5.2	Cisco ISE 1.1
UI32	サポート
UI64	サポート
IPv4	サポート

表 A-6 RADIUS 属性 : RADIUS サーバとの関連 (続き)

Cisco Secure ACS 5.1/5.2	Cisco ISE 1.1
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

このセクションでは、エクスポート中にマッピングされるデータ情報が記載されている一連の表を提供します。これらの表には、各オブジェクトについて Cisco Secure ACS 5.1/5.2 のカテゴリ、および Cisco ISE 1.1 におけるそれらと同等のカテゴリが含まれています。このセクションのデータ 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で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 \(P.A-7\)](#) (ネットワーク デバイス プロパティ マッピング)
- [表 A-8 \(P.A-7\)](#) (Active Directory プロパティ マッピング)
- [表 A-9 \(P.A-8\)](#) (外部 RADIUS サーバ プロパティ マッピング)
- [表 A-10 \(P.A-8\)](#) (ホスト/エンドポイント プロパティ マッピング)
- [表 A-11 \(P.A-9\)](#) (ID ディクショナリ プロパティ マッピング)
- [表 A-12 \(P.A-9\)](#) (ID グループ プロパティ マッピング)
- [表 A-13 \(P.A-9\)](#) (LDAP プロパティ マッピング)
- [表 A-14 \(P.A-11\)](#) (NDG タイプ マッピング)
- [表 A-15 \(P.A-11\)](#) (NDG 階層マッピング)
- [表 A-16 \(P.A-11\)](#) (RADIUS ディクショナリ ベンダー マッピング)
- [表 A-17 \(P.A-12\)](#) (RADIUS ディクショナリ属性マッピング)
- [表 A-18 \(P.A-12\)](#) (ユーザ マッピング)
- [表 A-19 \(P.A-12\)](#) (証明書認証プロファイル)
- [表 A-20 \(P.A-13\)](#) (許可プロファイル マッピング)
- [表 A-21 \(P.A-13\)](#) (DACL マッピング)
- [表 A-22 \(P.A-13\)](#) (外部 RADIUS サーバ マッピング)
- [表 A-23 \(P.A-13\)](#) (ID 属性ディクショナリ マッピング)
- [表 A-24 \(P.A-14\)](#) (RADIUS トークン マッピング)
- [表 A-25 \(P.A-15\)](#) (RSA マッピング)

- 表 A-26 (P.A-15) (RSA プロンプト)
- 表 A-27 (P.A-15) (ID ストア順序)
- 表 A-28 (P.A-16) (デフォルト ネットワーク デバイス)



(注) エクスポート レポートおよびインポート レポートには、情報、警告、エラー メッセージが含まれており、インポート プロセスとエクスポート プロセスの検証として機能します。

表 A-7 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 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	そのまま移行
TACACS information	TACACS は Cisco ISE 1.1 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 情報はありません。
Model name	これは Cisco ISE でのみ有効なプロパティです (値はデフォルトで「unknown」)。
Software version	これは Cisco ISE でのみ有効なプロパティです (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ていません。これらのデバイスは移行されないデバイスとして記載されます。

表 A-8 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 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

表 A-8 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への Active Directory マッピング (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
User attributes	そのまま移行
Groups	そのまま移行



(注)

Cisco Secure ACS-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「join」動作は失敗することがあります。また、Cisco ISE アプライアンスが AD のサーバ時間と正確に同期していることが重要です。同期していない場合は、「join」動作中に失敗することがあります。

表 A-9 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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」)。

表 A-10 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 へのホスト（エンドポイント）マッピング（続き）

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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 にはエンドポイント グループおよび ID グループが含まれています。Cisco Secure ACS 5.1/5.2 の ID グループは Cisco ISE へ、エンドポイント グループおよび ID グループとして移行されます。これは、ユーザを 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 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 5.1/5.2 から Cisco ISE 1.1 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-10） を参照）。

表 A-13 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への LDAP マッピング (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Directory organization information	そのまま移行 ([ディレクトリ構成 (Directory Organization)] タブ、図 A-2 (PA-10) 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

The screenshot shows the 'Server Connection' configuration page. It is divided into two main sections: 'Primary Server' and 'Secondary Server'.
Primary Server:
 Enable Secondary Server (checked)
 Always Access Primary Server First
 Failback To Primary Server After: 5 Minutes
 Hostname: sdfsdfff
 Port: 389
 Anonymous Access
 Authenticated Access
 Admin DN: [redacted]
 Password: [redacted]
 Use Secure Authentication
 Root CA: [dropdown]
 Server Timeout: 10 Seconds
 Max. Admin Connections: 20

Secondary Server:
 Hostname: [redacted]
 Port: [redacted]
 Anonymous Access
 Authenticated Access
 Admin DN: [redacted]
 Password: [redacted]
 Use Secure Authentication
 Root CA: [dropdown]
 Server Timeout: [redacted] Seconds
 Max. Admin Connections: [redacted]

282131

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

The screenshot shows the 'Directory Organization' configuration page.
Schema:
 Subject Objectclass: Person
 Group Objectclass: GroupOfUniqueNames
 Subject Name Attribute: uid
 Group Map Attribute: UniqueMember
 Certificate Attribute: usercertificate
 Subject Objects Contain Reference To Groups
 Group Objects Contain Reference To Subjects
 Subjects In Groups Are Stored In Member Attribute As: distinguished name
Directory Structure:
 Subject Search Base: sdfsdfff
 Group Search Base: sdfsdfff

Username Prefix/Suffix Stripping:
 Strip start of subject name up to the last occurrence of the separator: [redacted] (e.g. if separator set to '\', subject name 'acme\smith' becomes 'smith')
 Strip end of subject name from the first occurrence of the separator: [redacted] (e.g. if separator set to '@', subject name 'smith@acme.com' becomes 'smith')
MAC Address Format:
 Search for MAC Address in Format: xx-xx-xx-xx-xx-xx

282132

表 A-14 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への NDG タイプマッピング

Cisco Secure ACS 5.1/5.2 のプロパティ	Cisco ISE 1.1 のプロパティ
Name	Name
Description	Description



(注) Cisco Secure ACS 5.1/5.2 は、同じ名前の複数のネットワーク デバイス グループ (NDG) の所有をサポートすることができます。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 5.1/5.2 から Cisco ISE 1.1 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 1.1 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 5.1/5.2 から Cisco ISE 1.1 への RADIUS ディレクトリ (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 5.1/5.2 インストールの一部ではない、これらの 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 5.1/5.2 から Cisco ISE 1.1 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
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 5.1/5.2 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 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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)

表 A-19 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への証明書認証プロファイル マッピング (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Binary certificate comparison with certificate from LDAP or AD	Binary certificate comparison with certificate from LDAP or AD
AD - LDAP name for certificate fetching	AD - LDAP name for certificate fetching

表 A-20 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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

表 A-23 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 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
Name	そのまま移行
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 5.1/5.2 から Cisco ISE 1.1 RADIUS へのトークン 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
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

表 A-24 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 RADIUS へのトークン マッピング (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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 5.1/5.2 から Cisco ISE 1.1 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

表 A-27 Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への ID ストア順序 (続き)

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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 5.1/5.2 から Cisco ISE 1.1 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



APPENDIX **B**

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

この付録では、Cisco Secure Access Control System (ACS) -Cisco Identity Services Engine (ISE) Migration Tool の使用で発生する可能性のある一般的な問題、または状況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。
- 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.3-4) 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、技術的な問題の解決を最適に実現するための情報を入手します。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/tac/>

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。
- Cisco Secure ACS 4.x データベース（.dmp ファイル）のバックアップ
- 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 5.2 のログファイル
- Cisco Secure ACS 5.2 のビルド番号
- Cisco Secure ACS 4.x 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。



GLOSSARY

A

ACL

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

アクセス コントロール システム。規格準拠の認証、許可、アカウントिंग (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 Windows Active Directory。Microsoft で作成されたディレクトリ 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小規模なネットワーク インストールから、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へ、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、オブジェクトに割り当てられてい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。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。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。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。この意味における LDAP ディレクトリは、系統化されたレコード セットです。たとえば、電話帳は個人および組織のアルファベット順のリストであり、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。識別用に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、スイッチなどのデバイスを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。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、アカウントिंग (AAA) 集中管理を提供するネットワーク キング プロトコルです。

T

TACACS Terminal Access Controller Access-Control System。UNIX ネットワークで一般的に使用される認証サーバと通信するため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**

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。



INDEX

C

Cisco Secure ACS 5.1/5.2 から Cisco ISE への移行 [2-1](#)

い

移行方法 [2-1](#)

移行ユーティリティ [2-2](#)

移行ログ ファイル [B-3](#)

さ

サーバ要件 [3-2](#)

し

システム要件 [3-2](#)

サーバ [3-2](#)

ち

注意

説明 [x](#)

注、説明 [x](#)

て

データの移行および展開のシナリオ [3-2](#)

シングルまたはスタンドアロンの ACS アプライアンス [3-3](#)

データの移行と展開のシナリオ

分散環境の場合 [3-3](#)

と

トラブルシューティング [B-1](#)

よ

要件、サーバ [3-2](#)

