Cisco Secure ACS to Cisco ISE Migration Tool リリース 3.0 ユーザーガイド

初版：2023 年 6 月 11 日

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/

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

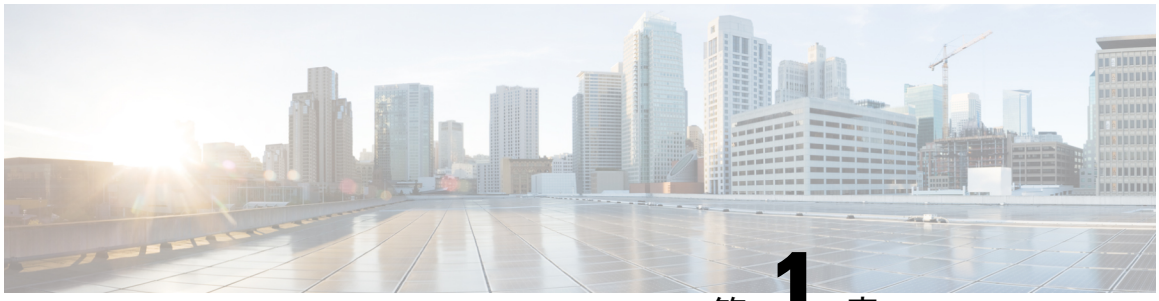
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

使用する前に

この章では、Cisco Secure Access Control Server（ACS）からCisco Identity Services Engine（ISE）へのデータ移行に使用される Cisco Secure ACS to Cisco ISE Migration Tool について説明します。

この移行ツールは、設定データを次の Cisco Secure ACS バージョンから Cisco ISE 3.0 に移行します。

- Cisco Secure ACS 5.5 以降：すべてのデータ オブジェクトを移行するには、移行ツールで [ACS 5.x サポート対象オブジェクト（ACS 5.x Supported Objects）] オプションを選択します。

  Cisco Secure ACS 5.5 以降からデータ オブジェクトを移行する場合、移行ツールは最初にデータ オブジェクトをCisco ISE に移行し、その後、対応するポリシー設定に移行します。

移行の概要

Cisco Secure ACS 5.x と Cisco ISE プラットフォーム、オペレーティング システム、データベース、および情報モデル間の相違のため、Cisco Secure ACS からデータを読み取り、対応するデータをCisco ISE に作成する移行アプリケーションが必須となります。移行アプリケーションは、Cisco Secure ACS から設定を抽出して Cisco ISE にインポートするためにシスコが提供するユーティリティです。移行管理者はトラブルシューティングのために、全移行プロセスの間、ACS 設定に関連する詳細ログだけでなく、現在の進行状況も表示できます。エラー メッセージは、移行されないオブジェクト、属性、およびポリシーに対して表示されます。移行後、移行された構成の正確性を確認することを**強く**お勧めします。Cisco ISE のポリシーセットのセマンティクスと構造を理解し、Cisco Secure ACS のアクセス ポリシーと照合してください。

（注） Cisco ISE をインストールする前でも、移行アプリケーションを活用して Cisco Secure ACS からデータを抽出することは可能です。このようにして、移行アプリケーションを活用して、Cisco Secure ACS から Cisco ISE への移行の準備ができているかどうかを判断できます。

ISE コミュニティ リソース

ACS 5.x から ISE 2.x への移行方法

ACS と ISE の比較

ACS から ISE への移行

（注） ISE コミュニティ リソースで提供される例やスクリーンショットは、以前のリリースの Cisco ISE のものである可能性があります。新しい機能、追加機能、更新については、GUI を確認してください。

Cisco Secure ACS から Cisco ISE へのデータ移行

データを Cisco ISE リリース 3.0 に移行するには、まず Cisco Secure ACS リリース 5.5、5.6、5.7、または 5.8 パッチ 3 から Cisco Secure ACS リリース 5.8 パッチ 4 にアップグレードする必要があります。Cisco Secure ACS リリース 5.8 パッチ 4 および TLS 1.2 の互換性の詳細については、『Release Notes for Cisco Secure Access Control System 5.8』の「TLS 1.2 Settings」を参照してください。

既存の Cisco Secure ACS リリース 5.5 以降のデータを Cisco ISE リリース 3.0、VM またはアプライアンスに移行する前に、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手順を読み、理解する必要があります。

既存の Cisco Secure ACS リリース 5.5 以降のデータを移行する前に、Cisco Secure ACS リリース 5.5 以降のシステムと Cisco ISE リリース 3.0 との間の関連するデータ構造とスキーマの違いを十分に理解することを推奨します。

（注） 命名規則、ポリシー階層、あらかじめ定義されたオブジェクトなどに関する Cisco ISE および Cisco Secure ACS データの相違により、移行ツールがすべてのオブジェクトをサポートしていない可能性があります。ただし、修正措置を促進するために、移行されていないオブジェクトには警告とエラーが表示されます。

Cisco Secure ACS to Cisco ISE Migration Tool の概要

移行ツールを使用すると、Cisco Secure ACS リリース 5.5 以降のデータを Cisco ISE リリース 3.0 に簡単に移行できます。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。

移行ツールは、Linux と Windows ベースのシステムで実行されます。移行ツールは、Cisco Secure ACS データファイルをエクスポートし、データを分析し、Cisco ISE リリース 3.0 で使用可能な形式にデータをインポートするために必要なデータ変更を行うことによって機能します。

- 移行ツールには、最小限のユーザー操作とフルセットの設定データが必要です。
- 移行ツールにより、サポートされていないオブジェクトの完全なリストが提供されます。

Cisco Secure ACS リリース 5.5 以降、および Cisco ISE リリース 3.0 アプリケーションは、同じタイプの物理ハードウェアで動作する場合と動作しない場合があります。移行ツールは 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 サーバー上で稼働することが可能です。Cisco Secure ACS アプライアンスで直接移行ツールを実行することはできません。Cisco Secure ACS PI は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） Cisco Secure ACS の以前のリリースから Cisco ISE 3.0 への移行プロセスについては、Cisco Secure ACS の以前のリリースから Cisco ISE への移行 （25 ページ）を参照してください。

データを Cisco ISE リリース 3.0 に移行するには、まず Cisco Secure ACS リリース 5.5、5.6、5.7、または 5.8 パッチ 3 から Cisco Secure ACS リリース 5.8 パッチ 4 にアップグレードする必要があります。Cisco Secure ACS リリース 5.8 パッチ 4 および TLS 1.2 の互換性の詳細については、『Release Notes for Cisco Secure Access Control System 5.8』の「TLS 1.2 Settings」を参照してください。

（注） Cisco Secure ACS リリース 5.x から Cisco ISE リリース 2.0 以降、AD グループの SID 値は移行ツールプロセスの一部として移行されません。外部グループ名のみが移行されます。移行プロセスの完了後、Cisco ISE で AD に参加し、[ADグループ（AD Groups）] タブにある [SID値の更新（Update SID values）] ボタンをクリックして、グループ SID を更新する必要があります。ポリシー条件で AD 外部グループが作成された場合は、AD グループ SID が手動で更新されるまで、承認ルールは一致しません。

システム要件

表 *1:* 移行ツールのシステム要件

オペレーティング システム	移行ツールは、WindowsおよびLinuxマシン上で動作します。マシンには、Java バージョン 1.8 以降がインストールされている必要があります。
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だけでなく、移行されたデータの保存、レポートおよびログの生成にも使用されます。
最小構成の RAM	必要な最小 RAM は 2 GB です。 約 300,000 人のユーザー、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。

表 *2:* ソースおよびターゲットの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 リリース 5.5 以降	Cisco Secure ACS 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 リリース 3.0	Cisco ISE ターゲット マシンに少なくとも 2 GB の RAM があることを確認します。
移行マシン：移行マシンには少なくとも 2 GB の RAM が搭載されていることを確認してください。	
64 ビットの Windows および Linux	Java JRE バージョン 1.8 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、移行ツールは機能しません。
32 ビットの Windows および Linux	Java JRE バージョン 1.8 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、移行ツールは機能しません。

移行ツールの向上

移行ツールには、ACS 5.x でサポートされているオブジェクトを移行するためのオプションが用意されています。移行ツールには、選択したバージョンに基づいてデータ オブジェクトが一覧表示されます。

移行ツールは以下をサポートしています。

- RADIUS または TACACS ベースの設定の移行：移行ツールを使用すると、RADIUS または TACACS に固有のオブジェクトの移行を選択できます。Cisco Secure ACS の展開に TACACS または RADIUS の設定のみが含まれている場合は、次のオプションを選択できます。
  - [RADIUS 設定（RADIUS Configuration）]：TACACS 固有の設定（シェル プロファイル、コマンド セット、アクセス サービス（デバイス管理）など）を除くすべての設定を移行します。
  - [TACACS 設定（TACACS Configuration）]：RADIUS 固有の設定（許可プロファイルやアクセス サービス（ネットワーク アクセス）など）を除くすべての設定を移行します。

（注） 選択された TACACS または RADIUS の移行オプションに関係なく、移行ツールは一部の TACACS および RADIUS オブジェクトを Cisco ISE に移行します。

既存の Cisco ISE インストールで、または同じ Cisco ISE サーバーへの Cisco Secure ACS の異なる展開から移行を実行する場合は、次のようになります。

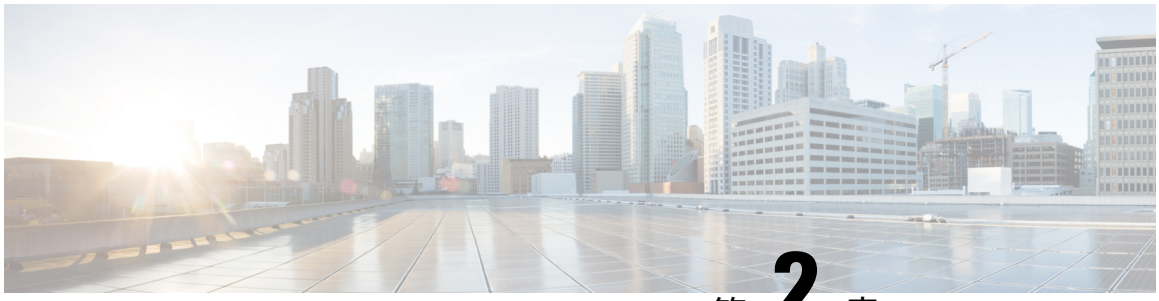
- 同じ名前のオブジェクトが Cisco ISE に存在しない場合は、オブジェクトが作成されます。
- 同じ名前のデータ オブジェクトが Cisco ISE に存在する場合、移行ツールはオブジェクト名の詳細を示す警告メッセージ「オブジェクトはすでに存在しています/リソースはすでに存在しています（object already exists/resource already exists）」を表示します。
- TACACS または RADIUS ベースの移行の場合、Cisco ISE に同じ名前のネットワーク デバイスが存在する場合は、プロトコル設定が更新されます。

- 選択的オブジェクトの移行：移行ツールを使用すると、事前定義された参照データ、グローバル操作、ディクショナリ、外部サーバー、ユーザーと ID ストア、デバイス、ポリシー要素、アクセスポリシーなどの高レベルの設定コンポーネントを Cisco Secure ACS 5.5 以降から Cisco ISE 3.0 に移行するように選択できます。選択的オブジェクトの移行を実行する前に、オブジェクト レベルの依存関係リストを参照することをお勧めします。要件に基づいて、サポートされているすべての構成コンポーネントを移行するか、または構成コンポーネントのリストから高レベルの設定コンポーネントの一部を選択できます。この選

択的オブジェクトの移行は、エクスポートおよびポリシーギャップ分析レポートに基づいて実行できます。

（注） アクセスポリシーの移行が正常に行われるようにするには、移行されたオブジェクトリストからすべてのオブジェクトを選択する必要があります。

- オブジェクト名の特殊文字：Cisco Secure ACS のデータ オブジェクトの名前に Cisco ISE でサポートされていない特殊文字が含まれている場合、移行ツールはサポートされていない特殊文字をアンダースコア（_）に変換し、データ オブジェクトを Cisco ISE に移行します。自動変換されたデータ オブジェクトは、エクスポート レポートに警告として表示されます。ただし、LDAP および AD 属性、RSA、RSA レルム プロンプト、内部ユーザー、およびすべての事前定義された参照データに Cisco ISE でサポートされていない特殊文字が含まれている場合、エクスポート プロセスは失敗します。
- すべてのオクテットの IP アドレス範囲を持つネットワーク デバイスの移行：移行ツールを使用すると、IP アドレス範囲を対応するサブネットまたは単一の IP アドレスに変換することによって、すべてのオクテット。移行では、すべてのオクテットの IP アドレス範囲の重複を報告します。
- 複合条件付きポリシー ルールの移行：移行ツールを使用すると、AND 演算子および OR 演算子を持つ複合条件付きの認証および許可（標準および例外）ルールを移行できます。
- 日時条件の移行：移行ツールは、ACS の曜日と時間グリッドが異なる曜日と時間で設定されている場合、データ オブジェクトを複数のデータ オブジェクトに分割することで、日時条件の移行を実行します。
- 拡張ヘルプ：移行ツールの UI で、[ヘルプ（Help）] > [移行ツールの使用法（Migration Tool Usage）] に移動して、移行ツールで使用可能なオプションの詳細を表示できます。



第 2 章

移行ツールのインストール

この章では、Cisco Secure ACS to Cisco ISE Migration Tool をインストールする方法のガイドラインを提供します。

移行ツールのインストール ガイドライン

- 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 リリース 5.5 以降の Windows または Linux のソース マシン以外に、デュアルアプライアンスの移行（分散展開のデータ移行）用に 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する必要があります。
- Cisco Secure ACS リリース 5.5 以降のソース 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、ACS 設定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 リリース 3.0 ソフトウェアをインストールしている。
  - 単一アプライアンスの移行の場合、アプライアンスまたは仮想マシンの再作成に使用可能な Cisco ISE リリース 3.0 ソフトウェアがある。
  - すべての適切な Cisco Secure ACS リリース 4.2 または 5.5 以降および Cisco ISE リリース 5.5 and above and Cisco ISE, Release 3.0 のクレデンシャルとパスワードがある。
- 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。

セキュリティに関する注意事項

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。

ユーザーは、Cisco Secure ACS データをエクスポートし、それを Cisco ISE アプライアンスに正常にインポートするために、Cisco Secure ACS リリース 5.5 以降および Cisco ISE リリース 3.0 の管理者のユーザー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、予約済みユーザー名を使用する必要があります。

プライマリ Cisco Secure ACS サーバーおよび Cisco ISE サーバーの 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。ユーザーが認証されると、移行ツールは、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。移行ツールを実行する前に、ACS サーバーの PI インターフェイスと ISE サーバーの ACS 移行インターフェイスが有効になっていることを確認します。

移行ツール ファイルのダウンロード

始める前に

- 移行プロセス用に Java ヒープ サイズに割り当てる初期メモリ量を config.bat ファイルに設定します。config.bat でヒープ サイズを設定する属性は次のとおりです。_Xms = 64（メモリ = 64 MB）および _Xmx = 1024（メモリ = 1024 MB）。

ステップ 1 ソフトウェアのダウンロード Web ページに移動します。場合によってはログイン クレデンシャルを提供する必要があります。

ステップ 2 [製品（Products）] > [セキュリティ（Security）] > [アクセス制御とポリシー（Access Control and Policy）] > [Cisco Identity Services Engine] > [Cisco Identity Services Engine ソフトウェア（Cisco Identity Services Engine Software）] に移動します。

ステップ 3 左側のペインで、バージョンを選択します。
[ソフトウェアのダウンロード（Download Software）] ページに、選択したバージョンで使用可能なソフトウェアの一覧が表示されます。

ステップ 4 移行ツールのソフトウェアパッケージに対応する [ダウンロード（Download）] をクリックして、ACS-MigrationApplication-3.0.zip ファイルをダウンロードします。

ステップ 5 .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で、config.bat および migration.bat ファイルを保持するディレクトリ構造が作成されます。

ステップ 6 **config.bat** ファイルを編集して、Java ヒープ サイズに割り当てる初期メモリ量を設定します。

ステップ 7 [Save] をクリックします。

移行ツールの初期化

始める前に

移行ツールが初期化されると、サポートされているすべてのオブジェクトの設定、または認証プロファイル、タイプ ネットワーク アクセスのアクセス サービスなどの RADIUS 設定、あるいはコマンドセット、シェル プロファイル、タイプ デバイス管理のアクセス サービスなどの TACACS 設定を移行するオプションを提供するメッセージ ボックスが表示されます。ツールは、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（移行できません）と、オブジェクトレベルの依存関係リストを提供します。Cisco Secure ACS to Cisco ISE Migration Tool のインターフェイスから [ヘルプ（Help）] > [サポートされていないオブジェクトの詳細およびオブジェクトレベルの依存関係リスト（Unsupported Object Details & Object-level dependencies list）] 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。

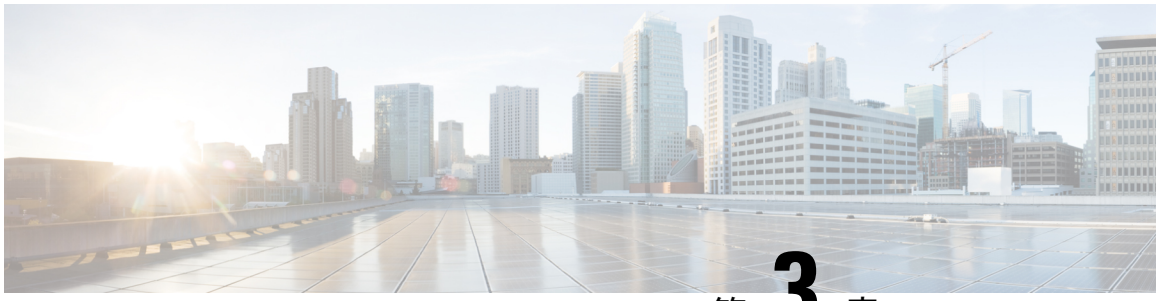
（注） 移行は、Cisco ISE の新規設定または既存の Cisco ISE 設定で実行できます。オブジェクトがすでに Cisco ISE に存在する場合は、警告メッセージが表示され、オブジェクトの移行はスキップされます。それ以外の場合は、オブジェクトが Cisco ISE に作成されます。

ステップ 1 **migration.bat** バッチ ファイルをクリックして、移行ツールを起動します。
[移行選択オプション（Migration selection options）] ウィンドウが表示されます。

ステップ 2 移行オプションのリストから、選択する移行オプションに対応するオプション ボタンをクリックします。

- サポートされているすべてのオブジェクトの設定：サポートされているすべてのオブジェクトが表示されます。
- 認証プロファイル、タイプ ネットワーク アクセスのアクセス サービスなどの RADIUS 設定：RADIUS 関連オブジェクトと共通オブジェクトのみ表示されます。
- コマンドセット、シェル プロファイル、タイプ デバイス管理のアクセス サービスなどの TACACS 設定：TACACS に関連するオブジェクトおよび共通オブジェクトのみ表示されます。

ステップ 3 ポップアップ ウィンドウで、[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と部分的にサポートされているオブジェクトおよびオブジェクトレベルの移行依存関係のリストを表示します。



第 3 章

移行計画

この章では、移行計画に必要な情報を提供します。移行を注意深く計画することで、移行がスムーズに行われ、移行が失敗するリスクが軽減されます。

前提条件

ここでは、移行プロセスを実行するための前提条件について説明します。

移行インターフェイスの有効化

移行プロセスを開始する前に、Cisco Secure ACS および Cisco ISE サーバーでデータ移行に使用するインターフェイスを有効にする必要があります。移行プロセスが完了した後、両方のサーバーの移行インターフェイスを無効にすることをお勧めします。

ステップ 1 Cisco Secure ACS CLI で次のコマンドを入力して、Cisco Secure ACS マシンの移行インターフェイスを有効にします。

acs config-web-interface migration enable

ステップ 2 Cisco ISE サーバーで移行インターフェイスを有効にします。

a) Cisco ISE CLI で、**application configure ise** と入力します。

b) ACS の移行を有効または無効にするには、**11** と入力します。

c) **Y** と入力します。

（注） 移行プロセスが完了した後で、コマンド **acs config-web-interface migration disable** を使用して、Cisco Secure ACS マシン上の移行インターフェイスを無効にします。

（注） 移行プロセスが完了したら、Cisco ISE サーバー上の移行インターフェイスを無効にします。

移行ツールでの信頼できる証明書の有効化

始める前に

Cisco Secure ACS サーバーから移行ツールにデータをエクスポートできるようにするために、Cisco Secure ACS CA 証明書または Cisco Secure ACS 管理証明書を信頼することができます。

移行ツールから Cisco ISE サーバーへのデータのインポートを有効にするために、Cisco ISE CA 証明書または Cisco ISE 管理証明書を信頼することができます。

移行ツールで信頼できる証明書を有効にするには、次の手順を実行します。

- Cisco Secure ACS で、サーバー証明書が **[システム管理（System Administration）] > [設定（Configuration）] > [ローカル サーバー証明書（Local Server Certificates）] > [ローカル証明書（Local Certificates）]** ページにあることを確認します。証明書内の共通名（[サブジェクト（Subject）] フィールドの CN 属性）または DNS 名（[サブジェクト代替名（Subject Alternative Name）] フィールド内）は、接続の確立と Cisco Secure ACS からのデータのエクスポートのために [ACS5 クレデンシャル（ACS5 Credentials）] ダイアログボックスで使用されます。
- Cisco ISE で、サーバー証明書が **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [システム証明書（System Certificates）]** ページにあることを確認します。共通名（[サブジェクト（Subject）] フィールドの CN 属性）または DNS 名（[サブジェクト代替名（Subject Alternative Name）] フィールド内）は、接続の確立と移行ツールから Cisco ISE へのデータのインポートのために [ISE クレデンシャル（ISE Credentials）] ダイアログボックスで使用されます。

ステップ 1 [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで、**[設定（Settings）] > [信頼できる証明書（Trusted Certificates）] > [追加（Add）]** を選択して、信頼できる通信を有効にする Cisco Secure ACS および Cisco ISE 証明書を追加します。

移行ツールで証明書を表示または削除できます。

ステップ 2 [開く（Open）] ダイアログボックスで、信頼できるルート証明書が格納されているフォルダを選択し、[開く（Open）] をクリックして、選択した Cisco ISE 証明書を移行ツールに追加します。

ステップ 3 前の手順を繰り返して、Cisco Secure ACS 証明書を追加します。

（注） Cisco Secure ACS および Cisco ISE のホスト名が IP アドレスに解決可能であることを確認します。

データ移行の推定時間

移行ツールは、次の構成を移行するのに約 5 時間稼働する可能性があります。

- 10,000 の内部ユーザー
- 4 個の ID グループ
- 16,000 台のネットワーク デバイス
- 512 個のネットワーク デバイス グループ
- 2 個の許可プロファイル（ポリシー セットの有無にかかわらず）
- 1 個のコマンド セット
- 42 個のシェル プロファイル
- 9 個のアクセス サービス（25 個の許可ルールを含む）

Cisco Secure ACS リリース 5.5 または 以降からの移行の準備

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 Secure ACS リリース 5.5 以降のデータは、Cisco ISE リリース 3.0 のポリシーセット モードでのみ移行します。
- サービス選択ポリシー（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 ルールの順序に従って順序付けします。

（注） SSP のデフォルトルールの結果であるサービスは、Cisco ISE リリース 3.0 のデフォルトポリシーセットになります。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 サービスの移行中、次の点を確認してください。

- サービス選択ポリシー（SSP）に、Cisco Secure ACS リリース 5.5 以降で無効になっているか、またはモニターされている SSP ルールが含まれている場合、それらは Cisco ISE に移行されません。
- サービス選択ポリシー（SSP）に、Cisco Secure ACS リリース 5.5 以降で有効な SSP ルールが含まれている場合は、次のようになります。
  - サービスを要求していて、そこにグループ マッピング ポリシーが含まれている場合、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。

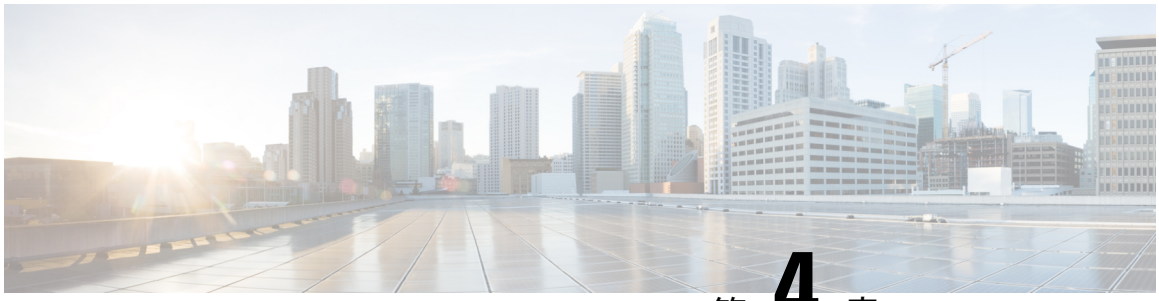
    特定のアクセス サービスにグループ マッピングが含まれている場合、移行ツールはそれをポリシー ギャップ分析レポートに警告として表示し、そのアクセス サービスに関連する許可ルールを移行します。
  - サービスを要求し、その ID ポリシーにルールが含まれ、それが RADIUS ID サーバーになる場合、Cisco ISE に移行されません（Cisco ISE はこれとは異なり、認証に RADIUS ID サーバーを使用します）。
  - サービスを要求し、そこに Cisco ISE でサポートされていない属性またはポリシー要素を使用するポリシーが含まれている場合、Cisco ISE に移行されません。

Cisco Secure ACS ポリシー ルールの移行ガイドライン

ルールを移行できない場合、データ整合性だけでなくセキュリティ面からも、ポリシーモデル全体を移行できません。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かった場合、ポリシーは Cisco ISE へ移行されません。

一般に、Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 3.0 にデータを移行する際は、次のルールを考慮する必要があります。

- 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。



第 4 章

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

この章では、移行ツールを使用して、Cisco Secure ACS リリース 以降のデータを Cisco ISE リリース 3.0 システム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。

Cisco Secure ACS からのデータのエクスポート

移行ツールの起動後、次の手順を実行して、Cisco Secure ACS から移行ツールにデータをエクスポートします。

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）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 Cisco Secure ACS リリース 5.5 以降のシステムの場合は Cisco Secure ACS のホスト名、ユーザー名、およびパスワード、[ACS5クレデンシャル（ACS5 Credentials）] ウィンドウで [接続（Connect）] をクリックします。

[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで移行プロセスをモニターできます。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。

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、[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。警告またはエラーのオブジェクト グループ、タイプ、および日時が示されます。

ステップ 5 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）] をクリックします。

ステップ 6 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 7 [エクスポート レポート（Export Report(s)）] をクリックして、エクスポート レポートの内容を表示します。

ステップ 8 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。

（注） 移行ツールは、エクスポートされたオブジェクトのキャッシュを保持し、その後のエクスポートのためにキャッシュを取得します。

エクスポート時のパスワードのコンプライアンス

移行ツールは、エクスポート プロセス中にパスワードのコンプライアンスを遵守します。

- **パスワードの複雑度**

  次に、ユーザーのパスワードがパスワードの複雑度要件を満たしていない場合にエクスポート プロセス中に発生するエラー メッセージの一覧を示します。

  「ユーザー：パスワードがパスワードの複雑度と一致しないためエクスポートできませんでした（*user: Failed to Export because its password does not match with the password Complexity*）」

  「パスワードの長さは *5* 文字以上にしてください。（*Password length should be minimum of '5' characters.*）」

  「パスワードには、「*cisco*」またはその文字の逆順は使用できません。（*Password should not contain 'cisco' or its characters in reverse.*）」

  「パスワードには、「*hello*」またはその文字の逆順は使用できません。（*Password should not contain 'hello' or its characters in reverse.*）」

  「パスワードには、*4* 回以上連続する繰り返し文字は使用できません。（*Password should not contain repeated characters four or more times consecutively.*）」

  「パスワードには、小文字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one Lower case character.*）」

「パスワードには、大文字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one Upper case character.*）」

「パスワードには、数字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one Numeric Character.*）」

「パスワードには、英数字以外の文字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one non alphanumeric characters.*）」

- **パスワード ハッシュ**

  Cisco Secure ACS で内部ユーザーのパスワード ハッシュを有効にして内部ユーザーをエクスポートしようとすると、移行ツールに次のエラー メッセージが表示されます。

  「ユーザー：*ISE* でサポートされていないパスワード ハッシュで設定されているためエクスポートできませんでした。この設定を *ACS* で無効にしてから、再度エクスポートしてください。（*user: Failed to Export because its configured with Password Hash which is not supported by ISE, disable this configuration in ACS and export again.*）」

Cisco ISE へのデータのインポート

ステップ 1 [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 2 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。

ステップ 3 [LDAP IDストア（LDAP Identity Store）] ドロップダウン リストから、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。

ステップ 4 [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 5 属性を追加したら、[ISE へのインポート（Import To ISE）] をクリックし、[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）、ユーザー名、およびパスワードを入力して [接続（Connect）] をクリックします。

ステップ 6 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。

ステップ 7 インポートされたデータの詳細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 8 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詳しい情報を取得するには、[移行（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 9 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。

ステップ 10 [ログ コンソールの表示（View Log Console）] をクリックすると、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。

Cisco ISE での移行されたデータの検証

Cisco Secure ACS 5.5 以降のデータが Cisco ISE 3.0 に移行されたことを確認するには、Cisco ISE にログインし、さまざまな Cisco Secure ACS オブジェクトを表示できることを確認します。

失敗したデータ移行の再開

移行ツールは、インポート操作またはエクスポート操作の各段階で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。

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

始める前に

Cisco Secure ACS リリース 5.5 移行のデータを Cisco ISE リリース 3.0 に移行する準備ができたら、それ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 のペルソナの設定など）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。サポートされるハードウェアアプライアンスの一覧については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 3.0*』を参照してください。

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、分散した設定内にない場合）は、移行ツールを Cisco Secure ACS アプライアンスに対して実行します。

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は、移行ツールと次の移行手順を使用できます。

ステップ 1 スタンドアロンの Windows または Linux マシンに移行ツールをインストールします。

ステップ 2 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ーへ Cisco Secure ACS リリース 5.5 以降の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 サポートされている Cisco ISE 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のイメージを、Cisco ISE リリース 3.0 ソフトウェアで再適用します。

ステップ 5 変換された Cisco Secure ACS のデータを、セキュアな外部サーバーから Cisco ISE にインポートします。

分散環境からのデータの移行

始める前に

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に接続されているプライマリアプライアンスから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。

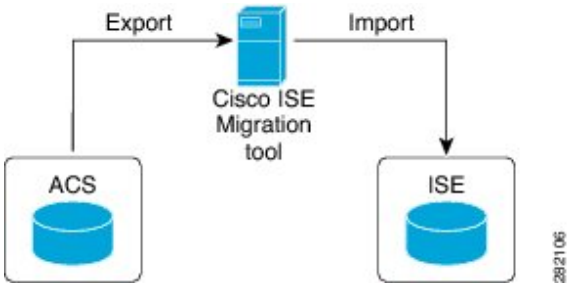
分散環境では、1 つのプライマリ Cisco Secure ACS アプライアンス、およびこのプライマリ アプライアンスと相互運用する 1 つ以上のセカンダリ Cisco Secure ACS アプライアンスがあります。

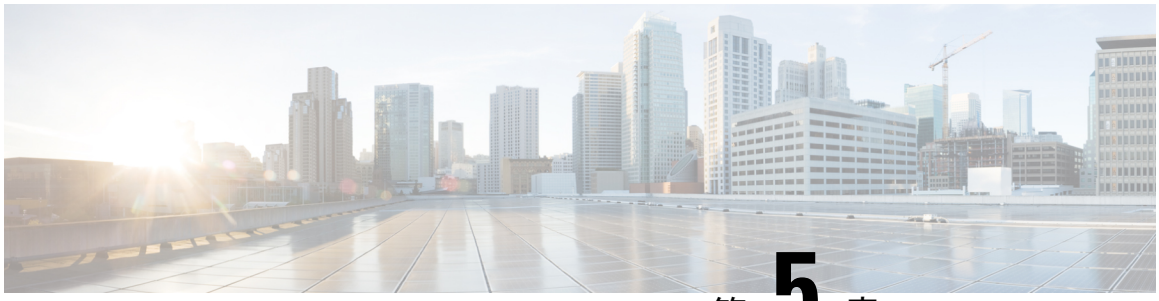
分散環境で Cisco Secure ACS を実行する場合は、以下のようにする必要があります。

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移行ツールを実行します。

図 *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*





第 5 章

レポート

移行ツールは、データ移行中のエクスポート、インポート、およびポリシーギャップ分析のレポートを生成します。移行ツール ディレクトリのレポート フォルダには、次のファイルが格納されています。

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

エクスポート レポート

このレポートは、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を示します。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、エクスポートされた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。

表 *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（Export）	Success	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。
	情報	Cisco ISE で事前定義されているためエクスポートされないデータ オブジェクトが示されます。
	警告	エクスポートされたデータ オブジェクトが示されますが、移行後に Cisco ISE で追加の設定が必要な場合があります。 移行ツールによって命名変換が行われたデータ オブジェクトが示されます。
	エラー（Error）	Cisco ISE でサポートされていない設定済みの名前または属性タイプの制限のためにエクスポートされないデータ オブジェクトが示されます。 Cisco ISE でサポートされていないためエクスポートされないデータ オブジェクトが示されます。

ポリシー ギャップ分析レポート

このレポートには、Cisco Secure ACS と Cisco ISE 間のポリシー ギャップに関する情報が一覧されます。このレポートは、エクスポート プロセスの完了後に、移行ツールのユーザー 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）] ボタンをクリックすることで利用できます。

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、その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、ポリシーに関連する矛盾した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、または自動変換可能な場合、その条件はレポートには記載されません。条件が「Not Supported」または「Partially supported」として検出された場合、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。

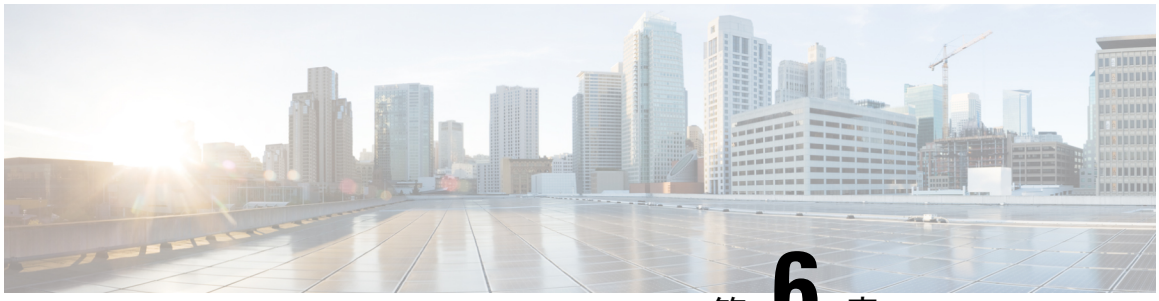
（注） データをエクスポートした後、エクスポート レポートとポリシーギャップ レポートを分析し、ACS 設定にリストされたエラーを修正し、警告およびその他の問題に対処する必要があります。エラーまたは警告に対処した後、再度エクスポート プロセスを実行します。Cisco Secure ACS からのデータのエクスポートについては、Cisco Secure ACS からのデータのエクスポート（15 ページ） を参照してください。

インポート レポート

このレポートは、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を示します。

表 *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（Import）	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。
	警告	インポートされたデータ オブジェクトが示されますが、移行後に Cisco ISE で追加の設定が必要な場合があります。 既存の Cisco ISE インストールで移行が実行された場合、Cisco ISE にすでに存在するデータ オブジェクトが示されます。
	エラー（Error）	以下の理由により、データオブジェクトはインポートされません。 • Cisco ISE にデータ オブジェクトをインポートする際に予期しないエラーが発生した



第 6 章

Cisco Secure ACS の以前のリリースから Cisco ISE への移行

この章では、Cisco Secure ACS の以前のリリースから Cisco ISE へのデータ移行に関する詳細情報を提供します。

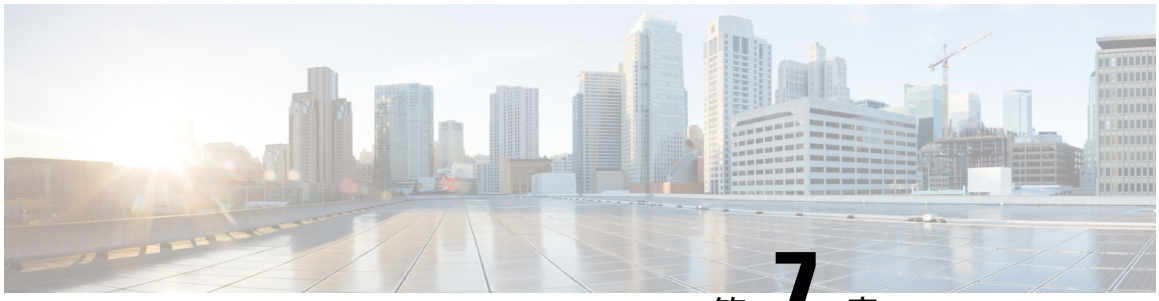
Cisco Secure ACS の以前のリリースから Cisco ISE への移行

以前のリリースの Cisco Secure ACS データを Cisco Secure ACS リリース 5.5 以降の状態に移行することで、移行ツールを使用して Cisco ISE リリース 3.0 に移行できるようになります。

Cisco Secure ACS リリース 5.x からの移行

ご使用の環境で Cisco Secure ACS リリース 5.x を実行している場合は、Cisco Secure ACS リリース 5.5 以降にアップグレードする必要があります。

内部ユーザーを Cisco Secure ACS 5.x から Cisco ISE に移行するには、Cisco Secure ACS 5.5 パッチ 4 以降または ACS 5.6 または ACS 5.7 パッチ 1 以降あるいは ACS 5.8 をインストールしてから移行を開始する必要があります。



第 7 章

ポリシー要素

この章では、Cisco ISE および Cisco Secure ACS のポリシー要素について説明します。

Cisco ISE および Cisco Secure ACS パリティ

Cisco ISE には、Cisco Secure ACS とのパリティを実現するための次の機能が導入されています。

- 個々のユーザーに設定された日付が特定の期間を超えている場合、ユーザーアカウントを無効にします
- すべてのユーザーにグローバルに設定された日付が特定の期間を超えている場合、ユーザー アカウントを無効にします
- n 日間の設定後にユーザー アカウントをグローバルに無効にします
- n 日間の非アクティブ後にユーザー アカウントを無効にします
- ネットワーク デバイスのすべてのオクテットにおける IP アドレス範囲のサポート
- IPv4 または IPv6 アドレスを持つネットワーク デバイスの設定
- IPv4 または IPv6 アドレスを持つ外部プロキシ サーバーの設定
- 最大長のネットワーク デバイス グループ（NDG）名のサポート
- 時間と日付の条件のサポート
- AND 演算子および OR 演算子を持つ複合条件によるサービス選択ルール、認証ルール、および許可（標準および例外）ルールのサポート
- Active Directory での MAR 構成
- Dial-In 属性のサポート

- LDAP のパスワード変更を有効にします
- 各 PSN のプライマリおよびバックアップ LDAP サーバーの構成
- RADIUS ポートの構成
- 動的属性で構成される許可プロファイル
- service-type RADIUS 属性の 2 つの新しい値
- 300,000 のユーザーに対する内部ユーザー サポートの向上
- 内部ユーザー認証キャッシュ
- 外部 ID ストア パスワードに対する内部ユーザーの認証
- 管理ユーザーおよび内部ユーザーのパスワードのディクショナリ チェック
- 許可されたプロトコルに対する Crytobinding TLV 属性のサポート
- 端末ワイヤレス LAN ユニット（TWLU）クライアントに対する EAP-TLS 認証実行時に長さを含むフラグを使用
- LDAP ID ストアのグループ名属性に対する共通名と識別名のサポート

ポリシー モデル

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 5.5 以降から Cisco ISE への移行ポリシーが少し複雑になっています。

Cisco Secure ACS のポリシー階層は、認証要求をアクセス サービスにリダイレクトするサービス選択ルールで始まります。アクセス サービスは、内部または外部の ID ストアに対してユーザーを認証し、定義された条件に基づいてユーザーを承認する ID ポリシーと許可ポリシーで構成されます。

認証ポリシーおよび許可ポリシーは、Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 3.0 に移行されます。Cisco ISE は、Cisco Secure ACS のサービス選択ポリシー（SSP）と同様のポリシー セットとをサポートしているため、

Cisco Secure ACS サービス セレクション ポリシーと Cisco ISE ポリシー セット

Cisco Secure ACS サービス選択ポリシー（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 セットのエントリ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トリ ルールと同じ順序で、SSP ルールの順序に類似しています。

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トリ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 で SSP ルールを無効またはモニター対象として定義でき、ポリシー セットの同等のエントリ 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ー対象になっている場合、SSP 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。

Cisco Secure ACS ポリシー アクセス サービスと Cisco ISE ポリシー セット

サービスを要求せずにポリシー サービスを定義できます。つまり、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して定義できます。Cisco Secure ACS リリース 5.5 以降には、既成の DenyAccess サービスがあり、そのサービスには Cisco Secure ACS のデフォルトの SSP ルールに対するポリシーも許可されるプロトコルもなく、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。しかし、Cisco ISE のポリシーセットを参照するエントリ ルールのないポリシーセットを持つことはできません。

許可されるプロトコルは、（特定のポリシーではなく）Cisco Secure ACS リリース 5.5 以降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。

ID ポリシーは、Cisco Secure ACS Release 5.5 以降の 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。

Cisco Secure ACS リリース 5.5 以降および Cisco ISE リリース 3.0 には、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ています。Cisco ISE リリース 3.0 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 リリース 5.5 以降には、グローバル例外ポリシーに相当するポリシーがありません。認証時には、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。

ISE 802.1X サービスに対する FIPS サポート

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。

連邦処理標準（FIPS）をサポートするために、移行ツール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。

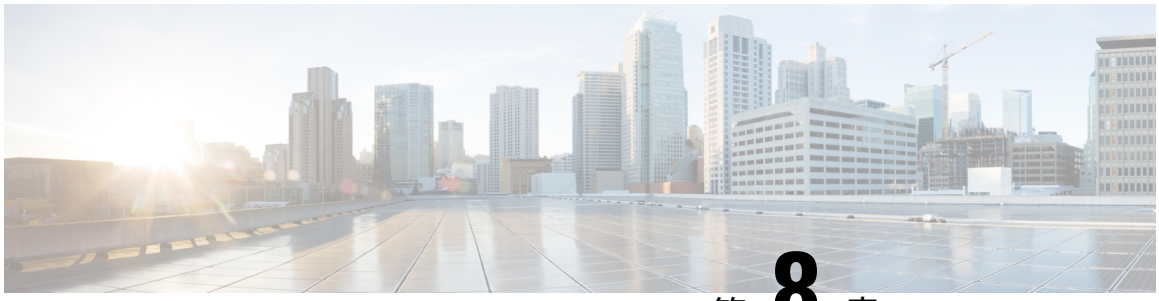
FIPS 準拠およびサポートされているプロトコル：

- ホスト ルックアップの処理（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）



第 8 章

Migration Toolトラブルシューティング

移行ツールを開始できない

条件

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 1.8 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。

トラブルシューティング移行ツールの接続の問題

移行ツールを Cisco Secure ACS または ISE に接続できない場合は、migration.log ファイルを調べて問題を特定します。

エラー メッセージ

Cisco Secure ACS または ISE ホスト名が解決できない場合は、エラー メッセージ「UnknownHostException：ホスト名（UnknownHostException: hostname）」が表示されます。

アクション

- 移行ツールを実行するクライアント マシンから Cisco Secure ACS または ISE ホスト名を解決できることを確認します。
- DNS の設定と接続性を確認します。

エラー メッセージ

移行ツールに入力された Cisco Secure ACS または Cisco ISE のホスト名が証明書の名前と一致しない場合は、エラー メッセージ「証明書のホスト名が一致しません：<hostname> != </hostname_in_certificate>（hostname in certificate didn't match: <hostname> != </hostname_in_certificate>）」が表示されます。

アクション

Cisco Secure ACS および Cisco ISE の [サブジェクト（Subject）] フィールドの証明書の共通名または [サブジェクト代替名（Subject Alternate Name）] フィールドの DNS 名が、移行ツールに提供されたホスト名と一致することを確認します。

エラー メッセージ

Cisco Secure ACS および ISE 証明書が移行ツールによって信頼されていない場合は、エラー メッセージ「SSLHandshakeException：要求されたターゲットへの有効な認証パスを見つけることができません（SSLHandshakeException: unable to find valid certification path to requested target）」が表示されます。

操作

Cisco Secure ACS to Cisco ISE Migration Tool の **[設定（Settings）]** > **[信頼できる証明書（Trusted Certificates）]** ページで必要な証明書を追加して、Cisco Secure ACS および Cisco ISE の証明書が信頼できるものであ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

接続エラー

条件

次のエラー メッセージがログに表示されます。「ホスト：https://hostname-or-ip への接続が拒否されました：null（Hosts: Connection to https://hostname-or-ip refused: null）」。さらに、Cisco ISE への移行時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 サーバー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。

I/O 例外エラー

条件

ログに以下のエラー メッセージが表示されます。

「要求の処理中に、I/O 例外（org.apache.http.NoHttpResponseException）がキャッチされました。ターゲット サーバーが応答に失敗しました。（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 サーバー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 サーバー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。

メモリ不足エラー

条件

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

Java のヒープ サイズを 1 GB 以上に増やします。

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

条件

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

ユーザーが、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

条件

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

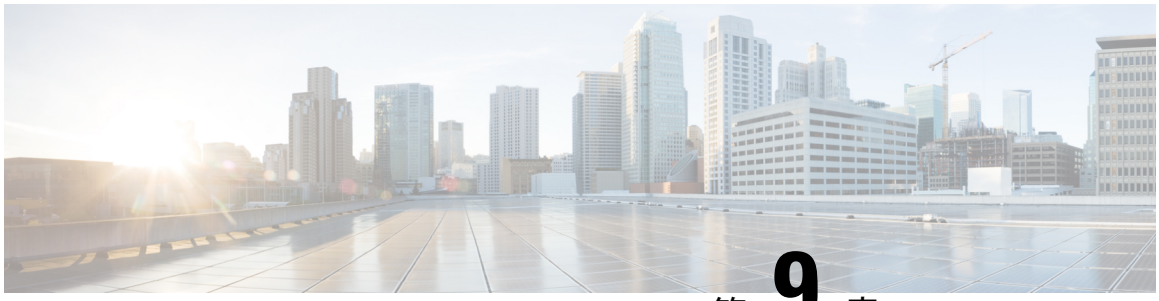
技術的な問題に対して、原因および考えられる解決方法を見つけられない場合は、Cisco カスタマー サービスの担当者に連絡して、問題の解決方法を入手します。Cisco Technical Assistance Center（TAC）に関する情報については、アプライアンスに付随している『Cisco Information Packet』の資料を参照するか、または以下の Web サイトにアクセスしてください。

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 リリース 5.5 以降のログファイル。
- Cisco Secure ACS Release 5.5 以降のビルド番号。



第 9 章

よく寄せられる質問

よく寄せられる質問

移行しないとどうなりますか。

Cisco Secure ACS では、すべてのリリースに対し サポートを終了することが発表されました。Cisco ISE をアップグレードすることで、シスコは今後の Cisco ISE リリースにおいて Cisco Secure ACS とのより近いパリティを実現します。新しい開発努力ではすべて、Cisco ISE に重点が置かれています。Cisco ISE は、TACACS+ と RADIUS の両方の将来のプラットフォームになります。高度な TACACS+ および RADIUS プロトコルをサポートするセキュリティ製品を使用する場合は、Cisco ISE に移行する必要があります。

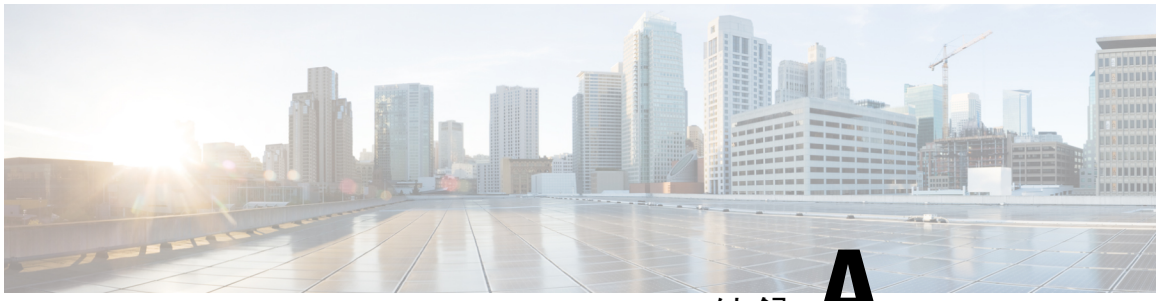
移行中にシスコによって提供されるサポートは何ですか。

移行ツールのユーザー ガイドには、移行プロセスに関する情報が記載されています。アドバンスドサービスおよびパートナーにお問い合わせいただいて移行を実行することもできます。移行中に問題が発生した場合は、TAC チームに連絡することができます。

Cisco ISE は、移行中にセキュリティ サポートをどのように提供しますか。

Cisco Secure ACS to Cisco ISE Migration Tool は、Cisco ISE と Cisco Secure ACS 間のセキュアな接続を使用して、エクスポート後および Cisco ISE にインポートする前にデータを暗号化して保管します。

よく寄せられる質問



付録 A

データ構造マッピング

この付録では、Cisco Secure ACS リリース 5.5 または 以降から Cisco ISE リリース 3.0 に移行されるデータオブジェクト、一部が移行されるデータオブジェクト、および移行されないデータオブジェクトについて説明します。

データ構造マッピング

へのデータ構造マッピングは、エクスポートフェーズの実行時に移行ツールでデータオブジェクトを分析および検証するプロセスです。

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 リリース 5.5 以降から Cisco ISE、リリース 3.0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
- IPv4 または IPv6 アドレスを持つネットワーク デバイス
- デフォルト ネットワーク デバイス
- ネットワーク デバイスの範囲（すべてのオクテット内）
- 外部 RADIUS サーバー
- 外部 TACACS+ サーバー
- TACACS+ サーバーの順序

- TACACS+ 設定
- ステートレス セッション再開機能の設定
- ID グループ
- 内部ユーザー
- 内部ユーザー認証キャッシュ
- イネーブル パスワードの変更がある内部ユーザー
- パスワード タイプが外部 ID ストアとして設定された内部ユーザー
- 日付が超過している場合のユーザー アカウントの無効化
- n 日間の非アクティブ後にユーザー アカウントを無効にするためのグローバル オプション
- 内部エンドポイント（ホスト）
- Lightweight Directory Access Protocol（LDAP）
- LDAP ID ストアのグループ名属性に対する共通名と識別名
- Microsoft Active Directory（AD）
- RSA
- RADIUS トークン
- 証明書認証プロファイル
- 日時条件（部分的にサポート。「サポートされていないルール要素」を参照）
- 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）
- 最大ユーザー セッション数
- RADIUS 属性およびベンダー固有属性（VSA）の値
- RADIUS ベンダー ディクショナリ
- 内部ユーザー属性
- 内部エンドポイント属性
- TACACS+ 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
- TACACS+ の認証、認可、承認の例外ポリシー（ポリシー オブジェクトの場合）
- 日時条件
- TACACS+ コマンド セット

- 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
- TACACS+ プロキシ サービス
- ユーザー 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
- EAP 認証プロトコル：PEAP-TLS
- ユーザー チェック属性
- ダイヤルイン属性
- 暗号バインディング属性
- 許可されているプロトコルに対する脆弱な暗号サポート
- 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
- RADIUS ID サーバー属性
- EAP-MD5、EAP-TLS、LEAP、PEAP および EAP-FAST 認証における長さを含むフラグ（L ビット）

一部が移行されるデータ オブジェクト

次のデータオブジェクトは、Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 3.0 に部分的に移行されます。

- IP アドレスと日付型の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。
- マルチ Active Directory ドメイン（プライマリに結合された Active Directory ドメインのみ）は移行される。
- プライマリ ACS インスタンスに定義された LDAP 設定は移行される。セカンダリ ACS インスタンス固有の設定は移行されない。

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 リリース 5.5 以降から Cisco ISE 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）

  証明書は移行されないため、手動でインポートする必要があります。証明書を使用する ID ストアの場合、インポートした証明書を ID ストアにマッピングする必要があります。ID ソース シーケンスを使用している場合は、証明書が重複している新しいシーケンスを作成する必要があります。
- Trustsec 関連の設定
- RSA ノード欠落の秘密の表示
- 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
- OCSP サービス
- SSL/TCP 経由の syslog メッセージ
- 設定可能な著作権バナー

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が一覧表示されています。これらの表には、Cisco Secure ACS リリース 5.5 以降からのオブジェクトカテゴリと、Cisco ISE リリース 3.0 における対応カテゴリが含まれています。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。

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
名前	そのまま移行
Description	そのまま移行
ネットワーク デバイス グループ	そのまま移行
単一の IP アドレス	そのまま移行
Single IP and subnet address	そのまま移行
IP 範囲	[IP の除外（Exclude IP）] オプションがあるすべてのオクテットの IP 範囲が移行されます
TACACS information	そのまま移行
RADIUS shared secret	そのまま移行
TACACS+ 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」）。

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
名前	名前
説明	説明

（注） Cisco Secure ACS Release 5.5 以降は、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 リリース 3.0 は、この命名方式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。

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
名前	名前
説明	説明
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。

デフォルト ネットワーク デバイスのマッピング

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
TACACS+ 共有秘密	共有秘密鍵（Shared Secret）
TACACS+ Single Connect デバイス	シングル接続モードを有効にする（Enable Single Connect Mode）
レガシー TACACS+ Single Connect サポート	レガシー シスコ デバイス
TACACS+ ドラフト準拠 Single Connect サポート	TACACS+ ドラフト コンプライアンス Single Connect サポート
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

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
名前	名前
説明	説明
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 リリース 3.0 には、ユーザー ID グループとエンドポイント ID グループが含まれています。Cisco Secure ACS リリース 5.5 以降の ID グループは Cisco ISE リリース 3.0 に、ユーザー 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、ユーザーをユーザー 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。

ユーザー マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	名前
説明	説明
ステータス	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	パスワード
Change password on next login	移行されない
User attributes list	ユーザー属性は Cisco ISE からインポートされ、ユーザーに関連付けられます
Expiry days	対応

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 でのみ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」）。

LDAP マッピング

Cisco Secure ACS のプロパティ	**Cisco ISE** のプロパティ
名前	名前
説明	説明
Server connection information	そのまま移行。
Directory organization information	そのまま移行。

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Directory groups	そのまま移行
Directory attributes	移行は（Cisco Secure ACS to Cisco ISE Migration Tool を使用して）手動で行われます。

（注） プライマリ ACS インスタンスに定義された LDAP 設定のみ移行されます。

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
Multiple domain support	プライマリ ACS インスタンスに結合されているドメインのみ移行

証明書認証プロファイルのマッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	名前
説明	説明
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。

ID ストア順序マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	名前
説明	説明
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）

許可プロファイルのマッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	名前
説明	説明
DACLID（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）	• 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 属性

シェル プロファイル属性マッピング

Cisco Secure ACS	Cisco ISE
共通タスク属性	
名前	名前
説明	説明

Cisco Secure ACS	Cisco ISE
デフォルト権限（静的および動的）	デフォルト権限（0 ～ 15）
最大権限（静的）	最大権限（0 ～ 15）
アクセス コントロール リスト（静的および動的）	アクセス コントロール リスト（静的および動的）
自動コマンド（静的および動的）	自動コマンド（静的および動的）
コールバック確認なし（静的および動的）	—
エスケープなし（静的および動的）	エスケープなし（True または False）
ハングアップなし（静的および動的）	—
タイムアウト（静的および動的）	タイムアウト（静的および動的）
アイドル時間（静的および動的）	アイドル時間（静的および動的）
コールバック回線（静的および動的）	—
コールバック ロータリー（静的および動的）	—
カスタム属性（Custom Attributes）	
属性（Attribute）	名前
要件（必須およびオプション）	タイプ（必須およびオプション）
値（静的および動的）	値（静的および動的）

コマンド セット属性マッピング

Cisco Secure ACS	Cisco ISE
名前	名前
説明	説明
次の表にないコマンドを許可します	次にリストされていないコマンドを許可します
付与（許可、拒否、常に拒否）	付与（許可、拒否、常に拒否）
コマンド（Command）	コマンド（Command）
引数	引数

ダウンロード可能な ACL マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	名前
説明	説明
DACL content	DACL content

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
名前	名前
説明	説明
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） 移行ツールは、ベンダーの ID と属性に基づいて、ベンダーとその属性の移行をサポートします。

ベンダー名が Cisco Secure ACS でユーザー定義され、Cisco ISE で事前定義されていて、それらの ID が異なる場合、エクスポート プロセスは成功しますがインポート プロセスは失敗します。ベンダー名が Cisco Secure ACS および Cisco ISE で事前定義されていて、それらの ID が同じ場合は、警告メッセージが表示されます。ベンダー名が Cisco Secure ACS でユーザー定義され、Cisco ISE で事前定義されていて、それらの ID が同じ場合、エクスポート プロセスは失敗します。

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
名前	名前
説明	説明

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Attribute ID	この値は NDG 階層名の一部としてのみ入力されるため（NDG タイプはこのオブジェクト名のプレフィックスです）、これに関連する特定のプロパティはありません。
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 リリース 5.5 以降のインストールの一部ではない、ユーザー定義の RADIUS 属性のみ移行する必要があります。

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
説明	説明
Internal name	Internal name
Attribute type	データ型
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。

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

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
説明（Description）	Internal name
名前	そのまま移行
Attribute type	データ型
該当プロパティなし	Dictionary（ユーザー 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

外部 RADIUS サーバー マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	名前
説明	説明
サーバの IP アドレス	ホストネーム
Shared secret	Shared secret
Authentication port	Authentication port
Accounting port	Accounting port
Server timeout	Server timeout

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Connection attempts	Connection attempts

外部 TACACS+ サーバー マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	名前
説明	説明
IP アドレス	ホスト名/アドレス（Host IP）
接続ポート（Connection Port）	接続ポート（Connection Port）
ネットワーク タイムアウト（Network Timeout）	Timeout
Shared secret	Shared secret

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
名前	名前
説明	説明
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

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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
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）。

RSA マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
名前	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

RSA プロンプト マッピング

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

翻訳について
このドキュメントは、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。