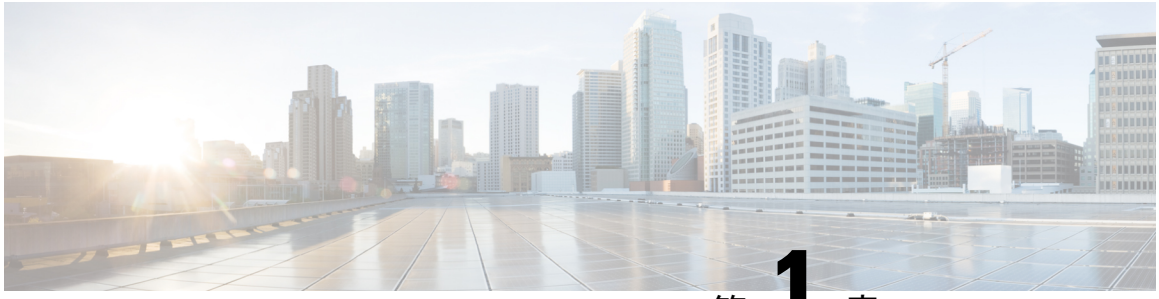
Cisco Secure ACS to Cisco ISE Migration Tool リリース 2.4 ユーザ ガイド

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/

目 次



第 1 章

使用する前に

この章では、Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 2.4 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。

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 ISE をインストールした後に実行できます。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。警告 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（特にポリシー セット）が適切であることを確認するよう**強く**お勧めします。

Cisco Secure ACS から データ移行

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 2.4、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 2.4 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。

Cisco Secure ACS リリース 5.5 以降のデータベースから Cisco ISE リリース 2.4 に移行する場合、データ移行で次がサポートされます。

- Cisco ISE リリース 2.4 で Cisco Secure ACS リリース 5.5 以降の機能がサポートされます。
- データが Cisco Secure ACS リリース 5.5 以降から移行される場合は、Cisco ISE リリース 2.4 の新機能がサポートされます。

（注） 各 Cisco Secure ACS または Cisco ISE リリースで動的に変化している機能ギャップのために、すべての Cisco Secure ACS データを Cisco ISE に移行できるわけではありません。Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 2.4 へのデータ移行では設定のギャップが最小限に抑えられています。つまり、以前は Cisco ISE でサポートされていなかった Cisco Secure ACS 機能がサポートされるようになっています。

（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。

サポートされているデータ移行パス

表 *1 : Cisco Secure ACS* リリースから *Cisco ISE* リリースへのサポートされている移行

Cisco ISE	Cisco Secure ACS 3.x、4.x、および 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3	Cisco Secure ACS 5.5	Cisco Secure ACS 5.6 以降
1.0	未サポート	サポート対象（Radius のみ）	未サポート	未サポート	未サポート	未サポート
1.1	未サポート	サポート対象（Radius のみ）	サポート対象（Radius のみ）	未サポート	未サポート	未サポート
1.2	未サポート	未サポート	未サポート	サポート対象（Radius のみ）	未サポート	未サポート
1.3	未サポート	未サポート	未サポート	未サポート	サポート対象	サポート対象

Cisco ISE	Cisco Secure ACS 3.x、4.x、および 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3	Cisco Secure ACS 5.5	Cisco Secure ACS 5.6 以降
2.0	未サポート	未サポート	未サポート	未サポート	サポート対象	サポート対象
2.1	未サポート	未サポート	未サポート	未サポート	サポート対象	サポート対象
2.2	未サポート	未サポート	未サポート	未サポート	サポート対象	サポート対象
2.3	未サポート	未サポート	未サポート	未サポート	サポート対象	サポート対象
2.4	未サポート	未サポート	未サポート	未サポート	サポート対象	サポート対象

Cisco Secure ACS to Cisco ISE Migration Tool

移行ツールを実行する前に、Cisco ISE リリース 2.4 にアップグレードし、Cisco Secure ACS リリース 5.5 以降の最新の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。

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 2.4 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 2.4 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 2.4 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 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。

システム要件

表 *2:* 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 1.7 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、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 *3:* 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 2.4	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 1.7 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。

プラットフォーム	要件
32 ビットの Windows および Linux	Java JRE バージョン 1.7 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。

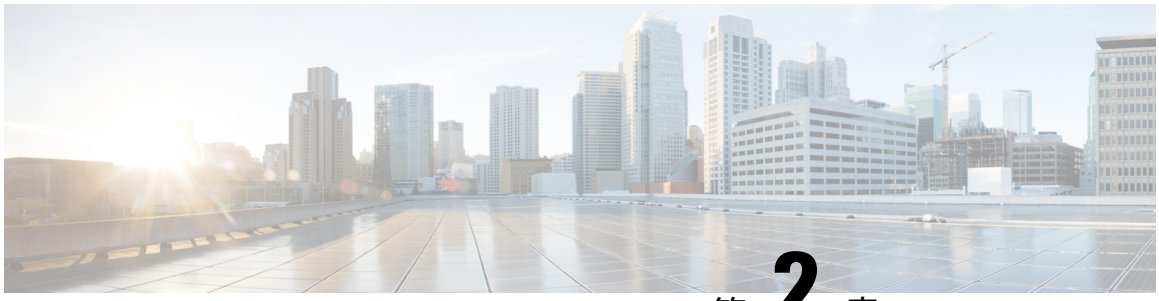
移行ツールの向上

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。

  既存の Cisco ISE インストールで、または同じ Cisco ISE サーバへの 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、ディクショナリ、外部サーバ、ユーザと 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 2.4 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。

- 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、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。
- 最後のオクテットの 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、最後のオクテットの IP アドレス範囲で設定されたネットワーク デバイスを移行できます。たとえば、10.197.64.40-50 は 10.197.64.40/29、10.197.64.48/32、10.197.64.49/32、10.197.64.50/32 に変換されます。
- 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 2.4 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 2.4 ソフトウェアがある。
  - すべての適切な Cisco Secure ACS リリース 5.5 以降および Cisco ISE リリース 2.4 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 リリース 5.5 以降および Cisco ISE リリース 2.4 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。

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、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 サーバの PI インターフェイスと ISE サーバの 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。

移行ツールの初期化

始める前に

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。

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。

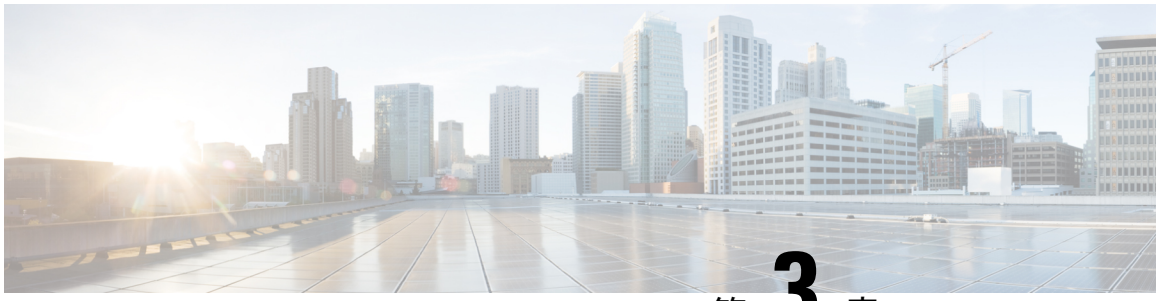
（注） 移行は、Cisco ISE の新規設定または既存の Cisco ISE 設定で実行できます。オブジェクトがすでに Cisco ISE に存在する場合は、警告メッセージが表示され、オブジェクトの移行はスキップされます。それ以外の場合は、オブジェクトが Cisco ISE に作成されます。

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 ISE からクライアント マシンに移行ツールをダウンロードします。Cisco Secure ACS サーバから移行ツール（クライアント マシン上）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、サーバ証明書が **[システム管理（System Administration）] > [設定（Configuration）] > [ローカル サーバ証明書（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。

データ移行の推定時間

Cisco Secure ACS to 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。

移行ツールは、次の構成を移行するのに約 52 時間稼働する可能性があります。

- 4 個の LDAP
- 1,000 個の ID グループ
- 500 個のユーザ ID グループ
- 20 個のネットワーク デバイス ロケーション
- 100 個のネットワーク デバイス グループ
- 25 個のアクセス サービス
- 50 個の SSP
- 600 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 個の許可ルール
- 600 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）
- 20 個のコマンド セットとシェル プロファイル（各コマンドには 100 個のコマンドが含まれています）
- 40 個のポリシー セット（最大ルール数によって制限されます）
- 20 個のカスタム ユーザ ディクショナリ
- 100,000 台のネットワーク デバイス
- 300,000 ユーザ
- 150,000 のホスト

Cisco Secure ACS リリース 5.5 または 5.6 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 2.4 のポリシー セット モードでのみ移行します。

- Cisco ISE リリース 2.4 の新規インストール時に移行します。Cisco ISE で、[管理（Administration）]>[システム（System）]>[設定（Settings）]>[ポリシー セット（Policy Sets）] の順に選択して、ポリシー セットを有効にします。
- 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 2.4 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。

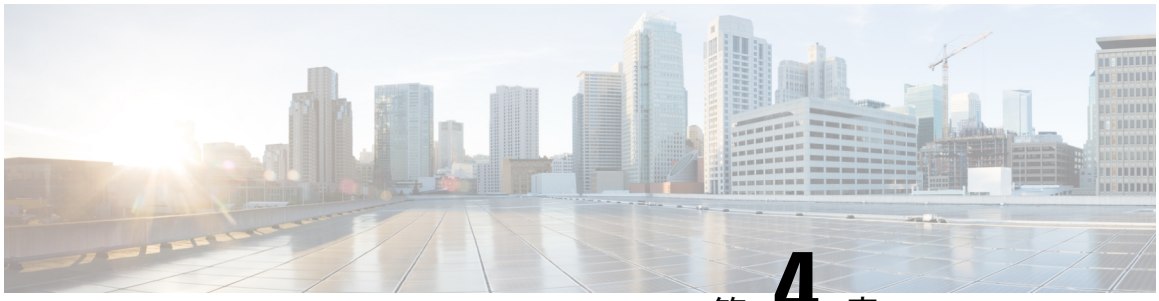
- サービス選択ポリシー（SSP）に、Cisco Secure ACS リリース 5.5 以降で無効になっているか、またはモニタされている SSP ルールが含まれている場合、それらは Cisco ISE に移行されません。
- サービス選択ポリシー（SSP）に、Cisco Secure ACS リリース 5.5 以降で有効な SSP ルールが含まれている場合は、次のようになります。
  - デバイス管理サービスを要求している場合は、Cisco ISE に移行されません。（Cisco ISE はデバイス管理をサポートしていません）。
  - サービスを要求していて、そこにグループマッピングポリシ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。
  - 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 2.4 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。

- 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。
- RADIUS 属性および VSA の値をフィルタ処理して Cisco ISE ログに追加することはできない。



第 4 章

永続的なデータの転送手順

この章では、移行ツールを使用して、Cisco Secure ACS リリース 5.5、5.6、 のデータを Cisco ISE リリース 2.4 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

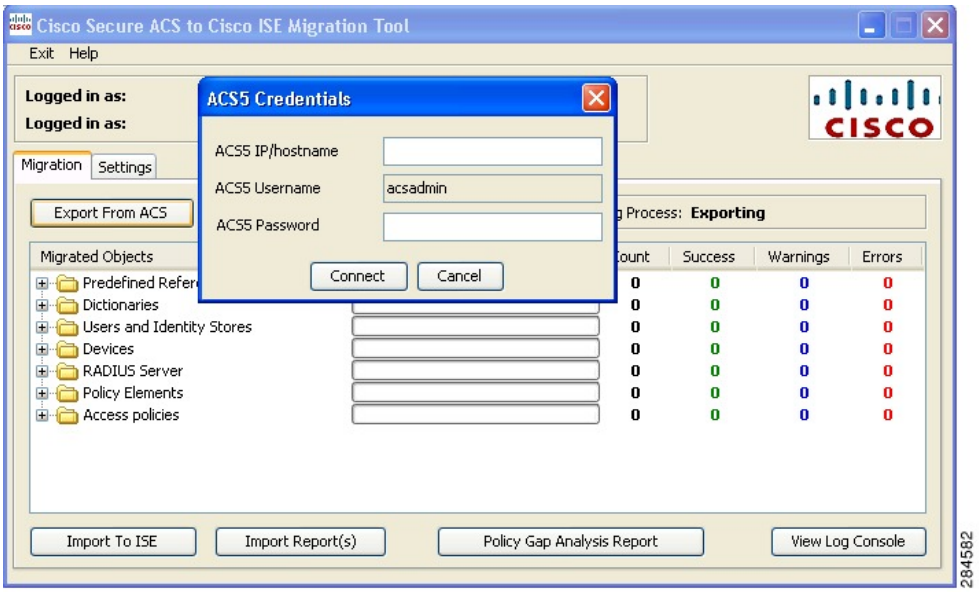
移行ツールの起動後、次の手順を実行して、Cisco Secure ACS から移行ツールにデータをエクスポートします。

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。

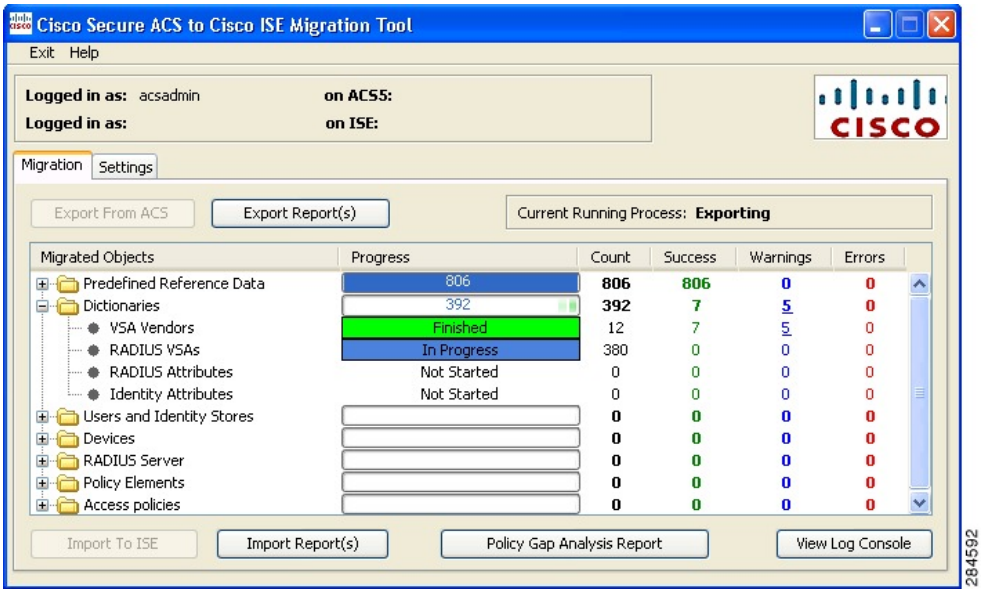
ステップ 2 （任意）移行を実行するために、依存関係処理を設定する必要はありません。従属データがない場合は、エクスポートするデータ オブジェクトのチェック ボックスをオンにして、[保存（Save）] をクリックします。

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。

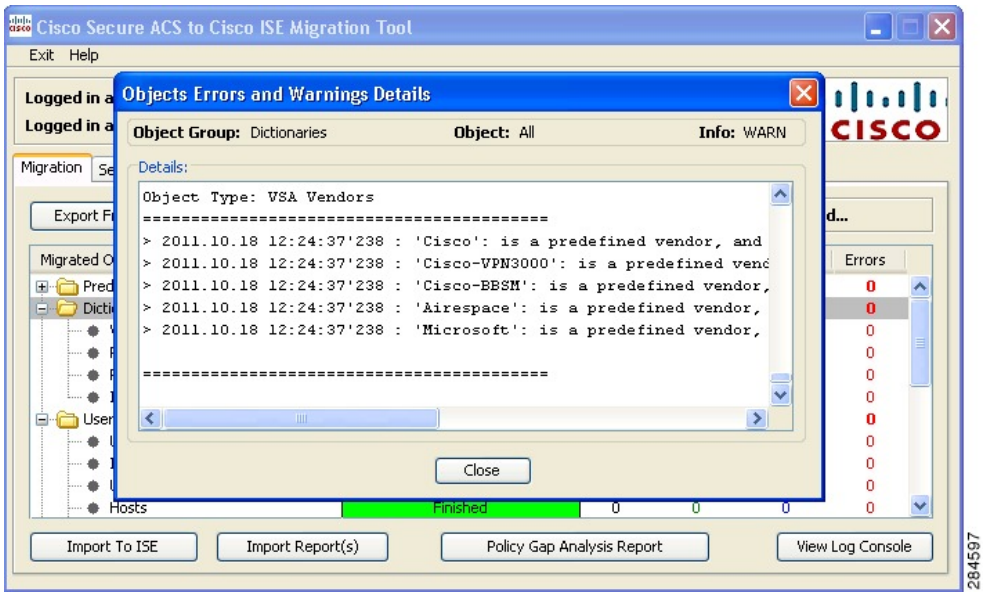
ステップ 4 パスワードを入力し、[ACS5クレデンシャル（ACS5 Credentials）] ウィンドウで [接続（Connect）] をクリックします。



ステップ 5 [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで移行プロセスをモニタします。ウィンドウには、正常にエクスポートされた現在のオブジェクト数、および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。

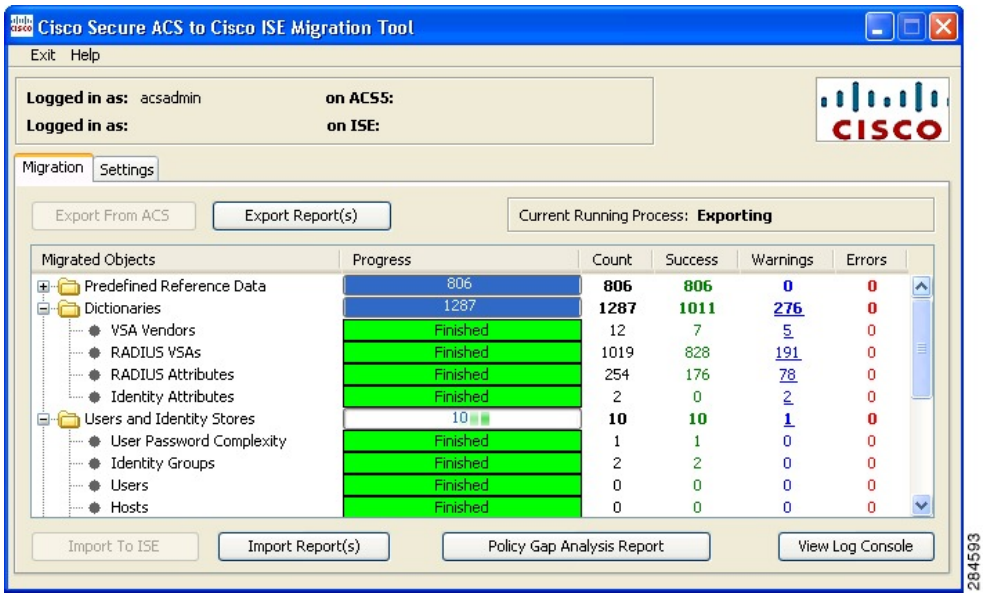


ステップ 6 エクスポート プロセスで発生した警告またはエラーについて詳しい情報を取得するには、[移動（Migrations）] タブの [警告（Warnings）] または [エラー（Errors）] カラムで下線の付いた数字をクリックします。[オブジェクト エラーと警告の詳細（Object Errors and Warnings Details）] ウィンドウに、エクスポート中に発生した警告またはエラーの結果が表示されます。警告またはエラーのオブジェクト グループ、タイプ、および日時が示されます。

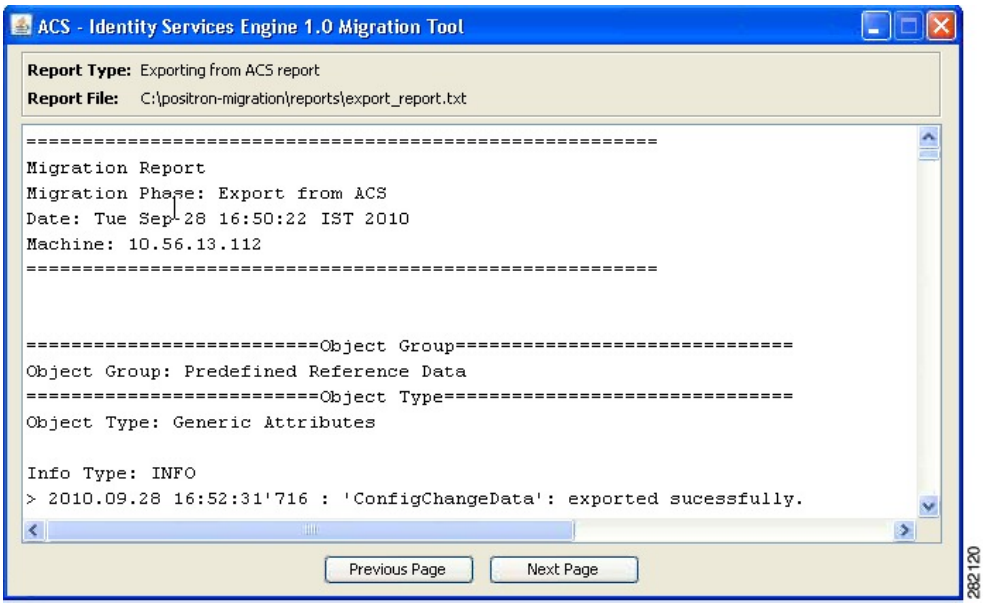


ステップ 7 スクロールして、選択したオブジェクトのエラーの詳細を表示し、[閉じる（Close）]をクリックします。

ステップ 8 データ エクスポート プロセスが完了したら、[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウに、エクスポートが終了したときのエクスポートのステータスが表示されます。



ステップ 9 [エクスポート 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 10 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。

Cisco ISE と Cisco Secure ACS 間のポリシー ギャップの分析

データをエクスポートした後、管理者はエクスポート レポートとポリシー ギャップ レポートを分析し、ACS設定でリストされたエラーを修正して、警告およびその他の問題に対処する必要があります。

Cisco Secure ACS 5.5 以降から Cisco ISE 2.4 に移行された構成セットには、次のようなギャップが見られます。これらのギャップの一部は調整可能です。

- **ID グループ**
  - 内部ユーザの問題
    - Cisco Secure ACS と Cisco ISE 間のパリティ ギャップ
      - パスワード タイプ
      - 次のログイン時にパスワードを変更
      - パスワードの変更
      - 名前の制約
  - 外部の ID ストアは正常に移行されます。名前を検証する必要があります。

- **ネットワーク デバイスまたはネットワーク デバイス グループ**
  - Cisco ISE 2.1 のネットワーク デバイスの移行に関する警告
    - Cisco ISE でサポートされていない IP 範囲
      - 重複する IP には除外が適用されます
    - IPV4 のみ
    - デフォルトのデバイスでは RADIUS を有効にする必要があります
  - 移行ツールの調整フロー
    - デバイスが Cisco ISE に存在しない（IP 設定の重複なしで定義される）場合は、デバイスは移行時に追加されます。
    - デバイスが存在する（IP またはサブネットが正確に一致し、名前が正確に一致する）場合は、移行ツールによって TACACS+ 要素が追加されます
    - デバイスが存在する（IP またはサブネットが正確に一致する、または名前が正確に一致する）場合は、移行ツールによってエラーが報告されます
- **認証結果**

  コマンド セットとシェル プロファイルは正常に移行されます。オブジェクト名では不整合が生じます。
  - Cisco ISE は厳密に名前に準拠します
  - ネットワーク アクセス ユーザと共有されるポリシー結果の名前空間
    - デバイス管理の認証結果にプレフィックスを使用することを推奨します
- **ポリシー**
  - 選択ポリシーから分離された Cisco Secure ACS 5.x アクセス サービス
    - 関与していないサービスを持つことができます
    - 異なるサービス選択ルールによって選択されたサービスを持つことができます
  - Cisco Secure ACS 5.x グループ マップ
    - Cisco Secure ACS 4.x からのグループ マップの移行
    - グループ マップのコンテンツは、Cisco ISE の認証ポリシーに移行する必要があります
  - 認証が許可されたプロトコル

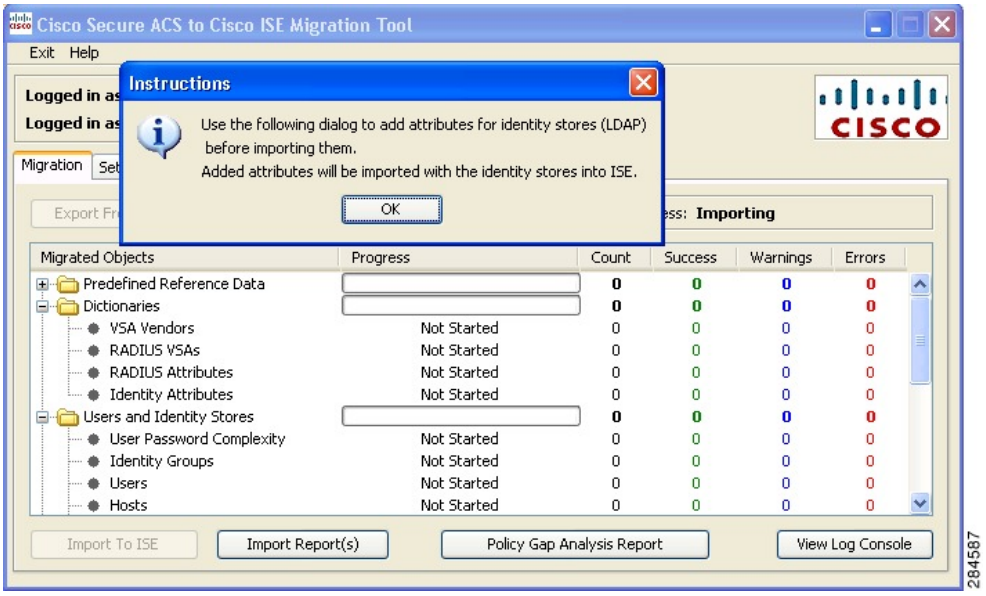
- Cisco Secure ACS 5.x のサービス設定の一部
- Cisco ISE のポリシー結果の一部

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 からデータをエクスポートする手順については、Cisco Secure ACS からのデータのエクスポート （17 ページ）を参照してください。

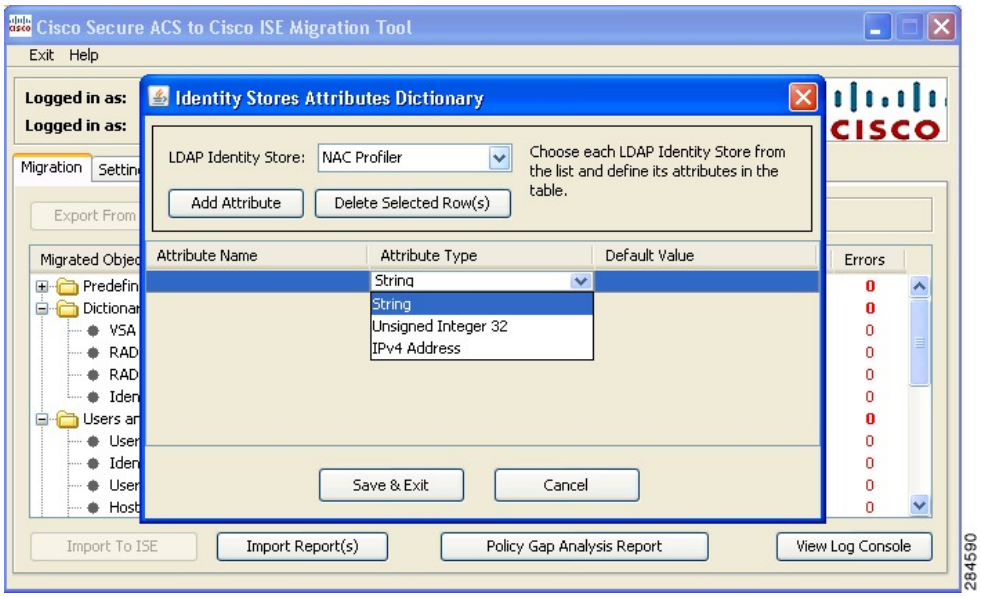
Cisco ISE へのデータのインポート

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。



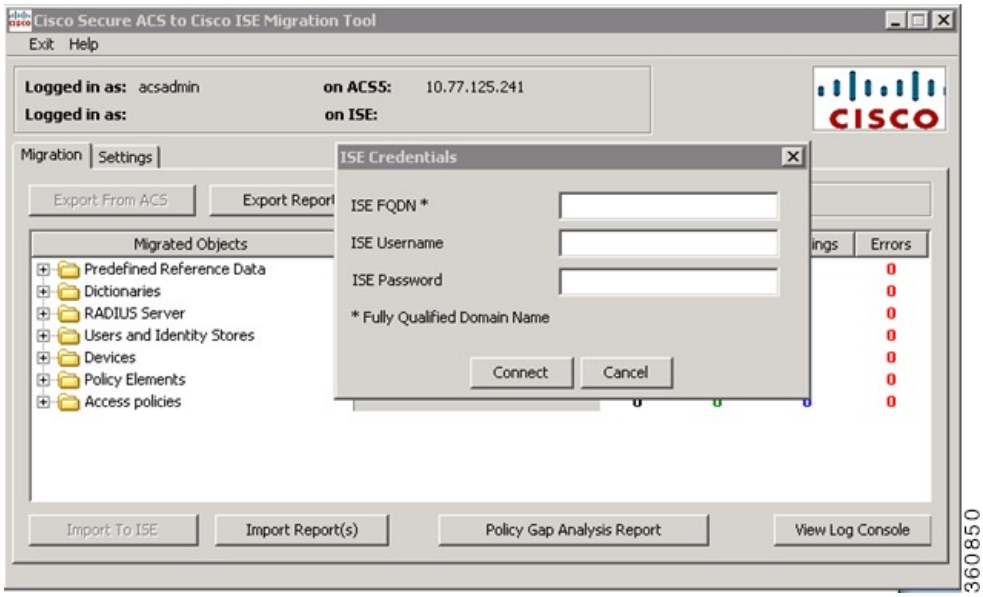
ステップ 3 [LDAP IDストア（LDAP Identity Store）] ドロップダウン リストから、属性を追加する ID ストアを選択し、[属性の追加（Add Attribute）] をクリックします。



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。

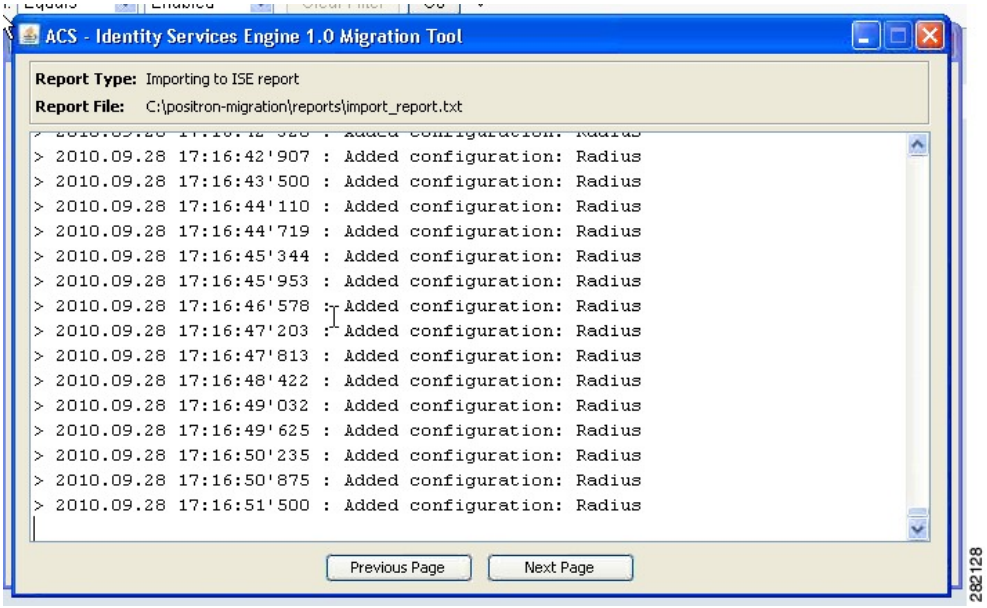
ステップ 5 属性を追加したら、[ISE へのインポート（Import To ISE）] をクリックし、[ISE クレデンシャル（ISE Credentials）] ウィンドウに Cisco ISE の完全修飾ドメイン名（FQDN）、ユーザ名、およびパスワードを入力して [接続（Connect）] をクリックします。

移行ツールは、これが SSL 証明書の FQDN と一致することを確認します。



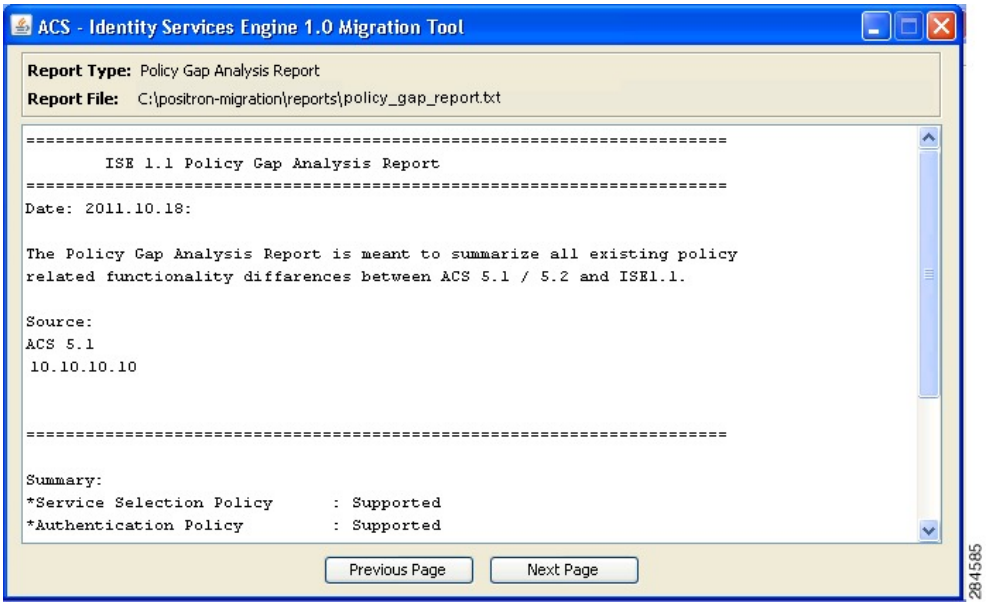
ステップ 6 データ インポート プロセスが完了したら、[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウに、**インポートが終了**したときのインポートのステータスが表示されます。

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。

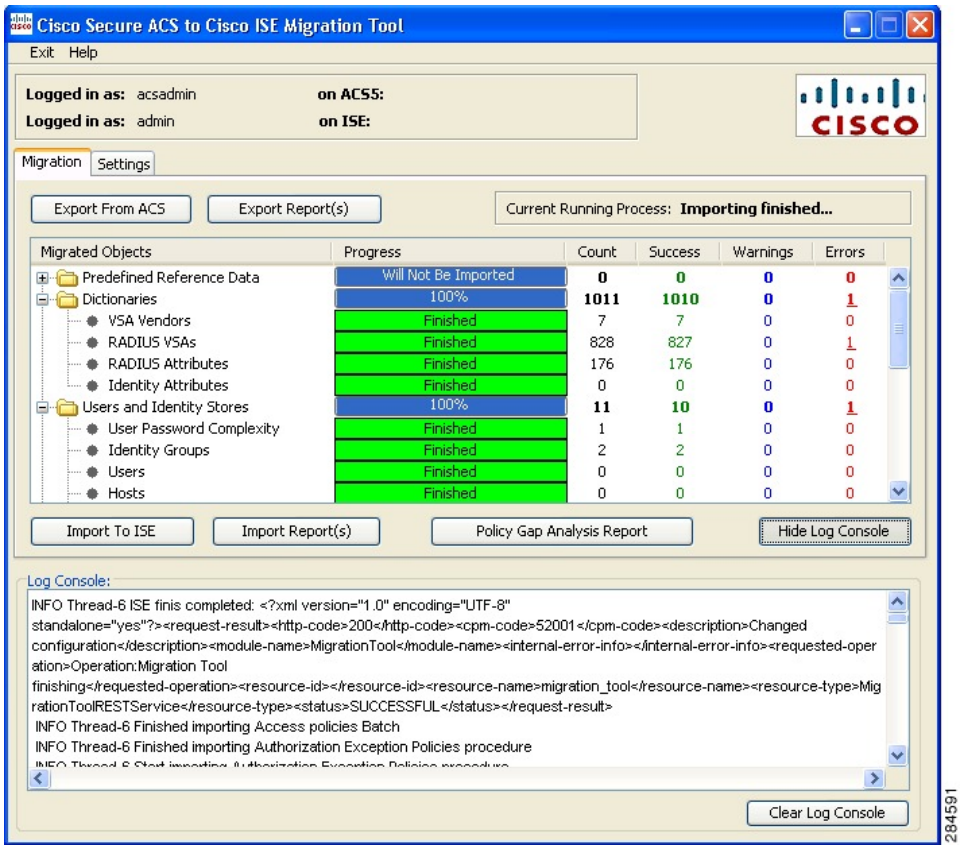


ステップ 8 インポートプロセスで発生した警告またはエラーについて詳しい情報を取得するには、[移行（Migrations）] タブの [警告（Warnings）] または [エラー（Errors）] カラムで下線の付いた数字をクリックします。

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。

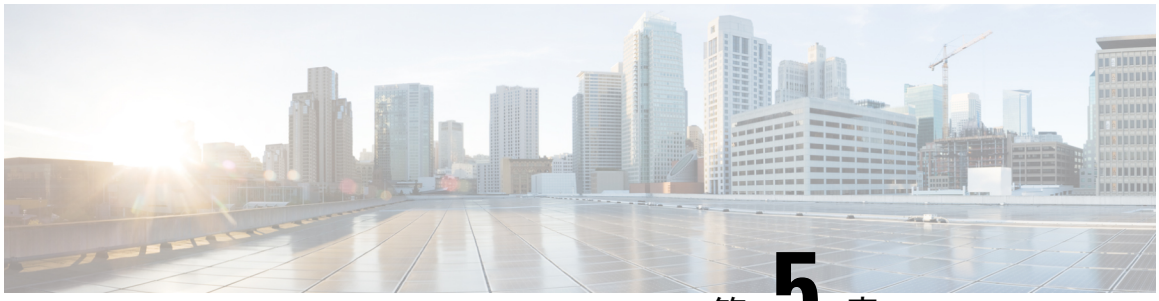


ステップ 10 [ログ コンソールの表示（View Log Console）] をクリックすると、エクスポートまたはインポート処理のリアルタイム ビューを表示できます。



Cisco ISE での移行されたデータの検証

Cisco Secure ACS 5.5 以降データが Cisco ISE 2.4 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。



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 *4 : 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）	情報	正常にエクスポートされたデータ オブジェクトの名前が示されます。
	警告	エクスポートの障害、またはデータ オブジェクトが Cisco ISE リリース 1.4 でサポート対象外であるために試行されなかったエクスポートが示されます。

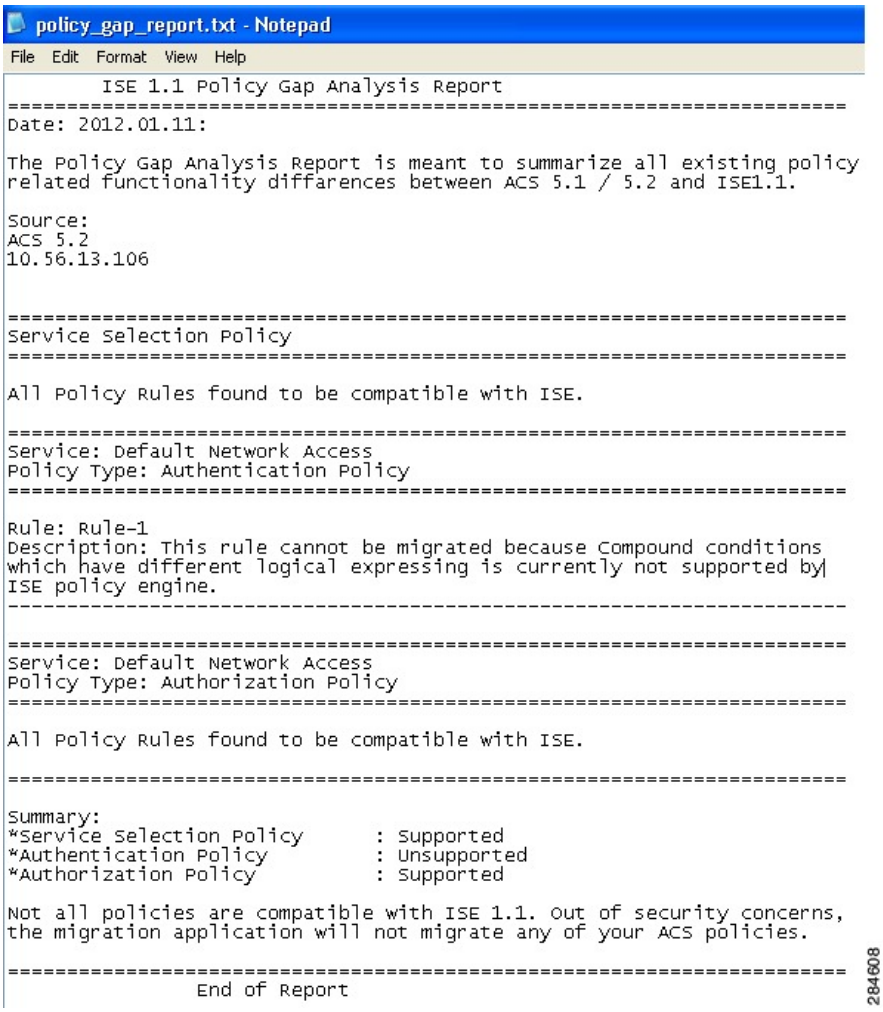
ポリシー ギャップ分析レポート

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。

図 *1*:ポリシー ギャップ分析レポートの例

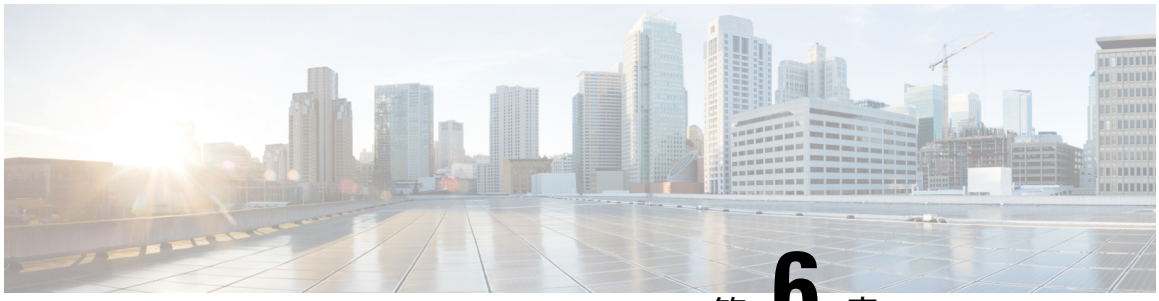


インポート レポート

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 *5 : 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。
	エラー	データ オブジェクトのエラーの原因を次のように識別します。 • オブジェクトがすでに存在します • オブジェクト名が文字数制限を超えています • オブジェクト名にサポートされていない特殊文字が含まれています • オブジェクトにサポートされていないデータ文字が含まれています



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 2.4 に移行できるようになります。

Cisco Secure ACS リリース 3.x からの移行

お使いの環境で Cisco Secure ACS Release 3.x を実行している場合は、Cisco Secure ACS Release 4.x の移行サポート バージョンにアップグレードしてから、Cisco Secure ACS Release 5.5 以降にアップグレードします。

ステップ 1 『Installation Guide for Cisco Secure ACS Solution Engine 4.1』または『Installation Guide for Cisco Secure ACS Solution Engine 4.2』の説明に従って、Cisco Secure ACS リリース 3.x のアップグレード パスを確認します。

ステップ 2 使用している Cisco Secure ACS Release 3.x サーバを Cisco Secure ACS Release 4.x の移行サポート バージョンにアップグレードします。たとえば、Cisco Secure ACS 4.1.1.24、Cisco Secure ACS 4.1.4、Cisco Secure ACS 4.2.0.124、または Cisco Secure ACS 4.2.1 リリースのいずれかにアップグレードします。

ステップ 3 アップグレード後、Cisco Secure ACS Release 4.x から Cisco Secure ACS Release 5.5 以降への移行方法を示した手順を実行します。

Cisco Secure ACS リリース 4.x からの移行

お使いの環境で Cisco Secure ACS Release 4.x の移行サポート バージョンのいずれも実行していない場合は、Cisco Secure ACS Release 4.x から Cisco Secure ACS Release 5.5 以降に移行可能なポイントまでアップグレードします。

ステップ 1 Cisco Secure ACS Release 4.x サーバで、現在、移行サポート バージョンのいずれも稼働していない場合は、Cisco Secure ACS Release 4.x バージョンを移行サポート バージョンにアップグレードします。

ステップ 2 移行マシン（Windows サーバ）に同じ移行サポート バージョンの Cisco Secure ACS をインストールします。

ステップ 3 Cisco Secure ACS Release 4.x データをバックアップして、移行マシンで復元します。

ステップ 4 移行マシンに移行ユーティリティを保存します。移行ユーティリティは、Installation and Recovery DVD から取得できます。

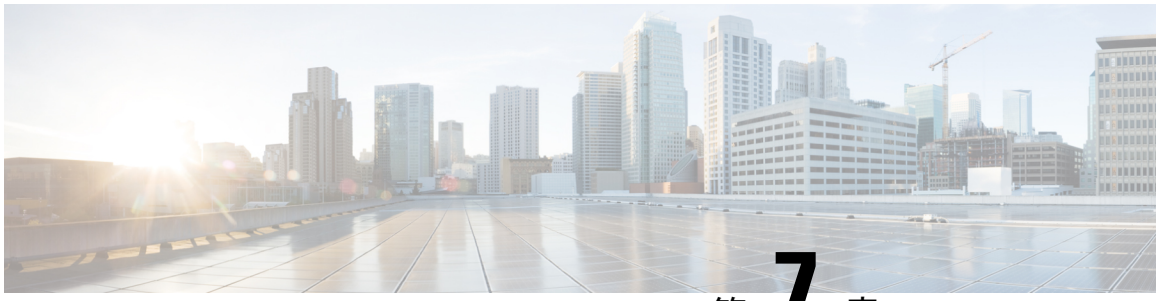
ステップ 5 移行マシンで、移行ユーティリティの分析およびエクスポート フェーズを実行します。

ステップ 6 分析およびエクスポート フェーズで問題が発生した場合はその問題を解決します。

ステップ 7 移行マシンで移行ユーティリティのインポート フェーズを実行します。このフェーズで移行ユーティリティは Cisco Secure ACS Release 5.5 以降サーバへデータをインポートします。

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。



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、ユーザアカウントを無効にします
- すべてのユーザ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、ユーザアカウントを無効にします
- n 日間の設定後にユーザ 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 アカウントを無効にします
- Active Directory での MAR 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 のユーザに対する内部ユーザ サポートの向上
- 外部 ID ストア パスワードに対する内部ユーザの認証
- 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

Cisco ISE および Cisco Secure ACS のパリティ機能の詳細については、『Cisco Identity Services Engine 2.1 Administration Guide』を参照してください。

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を認証し、定義された条件に基づいてユーザを承認する 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 2.4 に移行されます。Cisco ISE リリース は、Cisco Secure ACS リリース 5.5/5.6 のサービス選択ポリシー（SSP）と同様のポリシーセットと呼ばれる新しいポリシーモデルをサポートしているため、ポリシー移行プロセスが簡素化されます。

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 リリース 5.5/5.6 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。認証ポリシーは、外部ポリシー ルールと内部ポリシー ルールの 2 レベルのルールを保持します。外部ポリシー ルールは許可されるプロトコルになり、内部ポリシー ルールのセットへのエントリ基準になります。内部ポリシー ルールは ID ソースになります。

Cisco Secure ACS リリース 5.5 以降および Cisco ISE リリース 2.4 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 2.4 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。

UTF-8 のサポート

Cisco ISE リリース 2.4 は、いくつかの管理設定に対して 8 ビットの Unicode Transformation Format（UTF-8）をサポートしています。以下の設定項目は、UTF-8 エンコーディングでエクスポートおよびインポートされます。

- ネットワーク アクセスのユーザ設定
- RSA
- RADIUS トークン
- ポリシー
- ID グループ マッピング

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、サプ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、エンドユーザのサプリカントに示されます。

- [認証（Authentication）] タブ > [プロンプト（Prompts）]
- 管理設定
- 管理者のユーザ名およびパスワード
- UTF-8 を使用した管理者の設定

ポリシー

- [認証（Authentication）] > [AV 式の値（Value for AV expression）]
- [許可（Authorization）] > [その他の条件（Other Conditions）] > [AV 式の値（Value for AV expression）]
- 属性-値の条件
- [認証（Authentication）] > [単純条件/複合条件（Simple Condition/compound Condition）] > [AV 式の値（Value for AV expression）]
- [許可（Authorization）] > [単純条件/複合条件（Simple Condition/compound Condition）] > [AV 式の値（Value for AV expression）]

ISE 802.1X サービスに対する FIPS サポート

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。

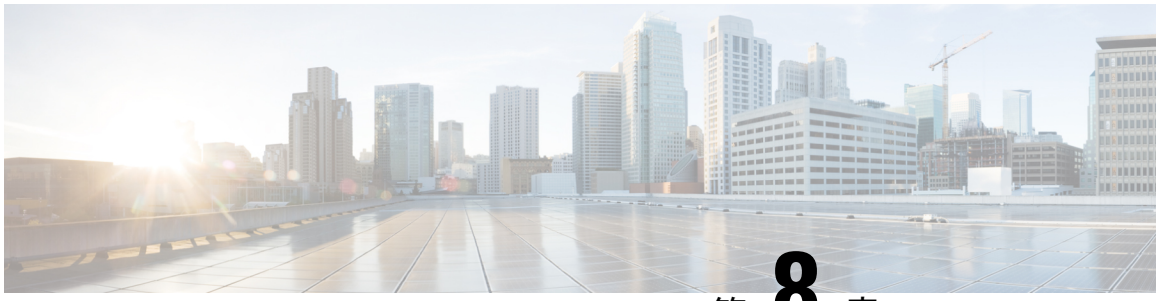
FIPS 準拠およびサポートされているプロトコル：

- 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

Cisco Secure ACS to Cisco ISE 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 1.6 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

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。

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。

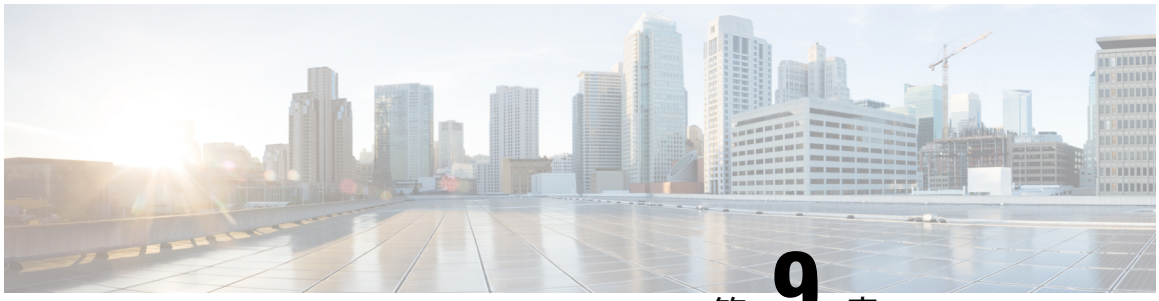
http://www.cisco.com/cisco/web/support/index.html

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。

（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。



第 9 章

FAQ

FAQ

移行しないとどうなりますか。

Cisco Secure ACS では、5.7 リリースをもって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。Cisco Secure ACS 5.8 の EOL は、Cisco ISE が Cisco Secure ACS との完全なパリティを実現した後に発表されます。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。

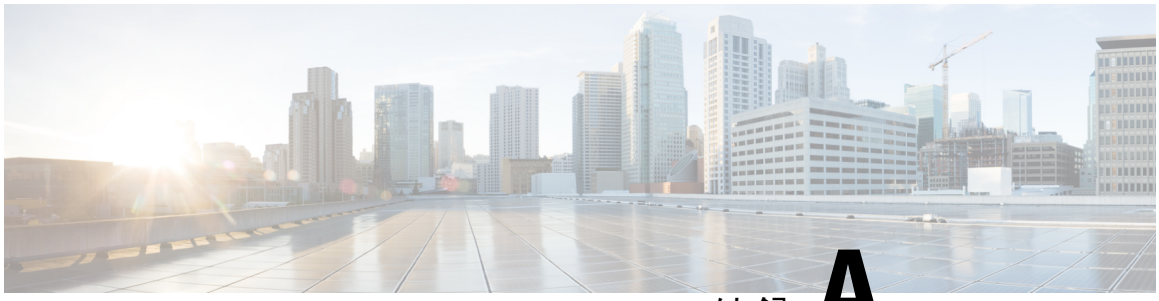
移行中にシスコによって提供されるサポートは何ですか。

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。

FAQ



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 5.6 から Cisco ISE リリース 2.4 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

Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 2.4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から Cisco ISE 、リリース 2.4 に移行されます。

- ネットワーク デバイス グループ（NDG）タイプと階層
- ネットワーク デバイス
- デフォルト ネットワーク デバイス
- 外部 RADIUS サーバ
- ID グループ

- 内部ユーザ
- 内部エンドポイント（ホスト）
- Lightweight Directory Access Protocol（LDAP）
- Microsoft Active Directory（AD）
- RSA（部分的にサポート。表 A-19 を参照）
- RADIUS トークン（表 A-18 を参照）
- 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）
- RADIUS 属性およびベンダー固有属性（VSA）の値（表 A-5 および A-6 を参照）
- RADIUS ベンダー ディクショナリ（表 A-5 および A-6 の注記を参照）
- 内部ユーザ属性（表 A-1 および A-2 を参照）
- 内部エンドポイント属性
- 許可プロファイル
- ダウンロード可能アクセス コントロール リスト（DACL）
- ID（認証）ポリシー
- ネットワーク アクセスの許可ポリシー
- 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）
- 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」ページを参照）
- EAP 認証プロトコル：PEAP-TLS
- ユーザ チェック属性
- ID 順序の高度なオプション
- ポリシー条件で使用可能な追加属性：AuthenticationIdentityStore
- 追加の文字列演算子：Start with、Ends with、Contains、Not contains
- RADIUS ID サーバ属性

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 2.4 に部分的に移行されます。

- 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。
- 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。

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。
- セキュリティ グループ アクセス コントロール リスト（SGACL）
- セキュリティ グループ（SG）
- サポートされているセキュリティ グループ アクセス（SGA）デバイスの AAA サーバ
- セキュリティ グループ マッピング
- ネットワーク デバイス アドミッション コントロール（NDAC）ポリシー
- SGA 出力マトリクス
- ネットワーク デバイス内の SGA データ

- SGA 許可ポリシー結果のセキュリティ グループ タグ（SGT）
- ネットワーク条件（エンド ステーション フィルタ、デバイス フィルタ、デバイス ポート フィルタ）
- デバイスの AAA ポリシー
- Dial-In 属性のサポート
- TACACS+ プロキシ
- TACACS+ CHAP と MSCHAP 認証
- TACACS+ シェル プロファイルの属性置換
- RSA ノード欠落の秘密の表示
- 最大ユーザ セッション数
- アカウントの無効化
- ユーザ パスワード タイプ
- 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
- ポリシー条件で使用可能な追加属性：NumberOfHoursSinceUserCreation
- ホストのワイルドカード
- ネットワーク デバイスの範囲
- 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
- 内部ユーザの有効期限日
- IP アドレスの除外

サポートされていないルール要素

Cisco Secure ACS と Cisco ISE は異なるポリシー モデルに基づいているため、Cisco ISE に移行した場合に、Cisco Secure ACS のデータ間でギャップが発生します。Cisco Secure ACS と Cisco ISE のリリース バージョンが変わった場合、次の理由のためにすべての Cisco Secure ACS ポリシーおよびルールを移行できるわけではありません。

- ポリシーで使用されている属性がサポートされていない
- AND/OR 条件構造がサポートされていない（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

表 *6* : サポートされていないルール要素

ルール要素	サポート状況	説明
日付および時刻（Date and Time）	未サポート	反復的な週次設定を持つ許可ポリシー内の日時条件は、Cisco ISE へ移行されません。結果として、ルールも移行されません。
日付および時刻（Date and Time）	未サポート	認証ポリシー内の日時条件は Cisco ISE へ移行されません。結果として、ルールも移行されません。
In	一部サポートあり	「In」演算子は階層に使用され、「Is」は文字列タイプのみに使用されます。これは「STARTS_WITH」を使用して変換することができます。
Not In	一部サポートあり	「Not in」演算子は階層に使用され、「Is」は文字列タイプのみに使用されます。これは「Matches」を使用して変換することができます。
Contains Any	未サポート	「Contains Any」演算子は、Active Directory および Lightweight Directory Access Protocol などの外部グループにのみ使用されます。
Contains All	未サポート	「Contains All」演算子は、Active Directory および Lightweight Directory Access Protocol などの外部グループにのみ使用されます。

ルール要素	サポート状況	説明
論理式の組み合わせ	未サポート	条件内でこれらの演算子を使用しているルールは移行されません。 • 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。 • a && b && c && 以外のローカル式を持つ複合条件が含まれている許可ポリシーは、ルール条件の一部として移行されません。代わりに、いくつかの高度な論理式に対してライブラリ複合条件を手動で使用することができます。
ネットワーク条件	未サポート	ネットワーク条件のみが含まれているルールは移行されません。条件にネットワーク条件、およびサポート対象の他の条件が含まれている場合、ネットワーク条件は無視され、ルール条件の一部として移行されません。
ユーザ属性	一部サポートあり	「文字列」のデータ タイプ以外のデータ タイプによるユーザ属性を含む条件によるルールは移行されません。
ホスト属性	未サポート	条件でホスト属性を参照している場合、認証は失敗します。 ホスト（エンドポイント）属性を持つ条件が含まれている許可ポリシーは、Cisco ISE 許可ポリシーへ移行されません。

ルール要素	サポート状況	説明
TACACS 属性	未サポート	Cisco ISE は、Terminal Access Controller Access-Control System（TACACS）をサポートしません。TACACS 属性を使用する Cisco Secure ACS サービス セレクション ポリシー ルールは移行されません。

サポート対象属性およびデータ型

Cisco Secure ACS リリース 5.5 以降から Cisco ISE 2.4 に移行されるユーザ属性

Cisco Secure ACS Release 5.5 以降でサポートされるユーザ属性	Cisco ISE リリース 2.4 のターゲット データ タイプ
文字列	文字列
UI32	未サポート
IPv4	未サポート
ブール値	未サポート
日付	未サポート
列挙体	未サポート

ユーザ属性：ユーザとの関連

Cisco Secure ACS Release 5.5 以降のユーザに関連付けられている属性	Cisco ISE リリース 2.4
文字列	サポート対象
UI32	未サポート
IPv4	未サポート
ブール値	未サポート
日付	未サポート

Cisco Secure ACS リリース 5.5 または 5.6 から Cisco ISE リリース 2.4 に移行されるホスト属性

Cisco Secure ACS リリース 5.5 または 5.6 でサポートされるホスト属性	Cisco ISE リリース 2.4 のターゲット データ タイプ
文字列	文字列
UI32	UI32
IPv4	IPv4
ブール値	ブール値
日付	サポート対象外
列挙体	使用可能な値の整数

ホスト属性：ホストとの関連

Cisco Secure ACS Release 5.5 以降のホストに関連付けられている属性	Cisco ISE リリース 2.4
文字列	サポート対象
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）
ブール値	サポート（値は String に変換される）
日付	サポート（値は String に変換される）
列挙体	サポート（値は String に変換される）

Cisco Secure ACS リリース 5.5 から Cisco ISE リリース 2.4 に移行される RADIUS 属性

Cisco Secure ACS Release 5.5 以降でサポートされる RADIUS 属性	Cisco ISE リリース 2.4 のターゲット データ タイプ
UI32	UI32
UI64	UI64
IPv4	IPv4

Cisco Secure ACS Release 5.5 以降でサポートされる RADIUS 属性	Cisco ISE リリース 2.4 のターゲット データ タイプ
Hex String	Octect String
文字列	文字列
列挙体	使用可能な値の整数

RADIUS 属性：RADIUS サーバとの関連

Cisco Secure ACS リリース 5.5 以降の RADIUS に関連付けられている属性	Cisco ISE リリース 2.4
UI32	サポート対象
UI64	サポート対象
IPv4	サポート対象
Hex String	サポート（Hex String は Octet String に変換される）
文字列	サポート対象
列挙体	サポート（Enum は使用可能な値の整数）

データ情報マッピング

この項には、エクスポートプロセス中にマッピングされるデータ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 2.4 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
Name	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

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Single IP and subnet address	そのまま移行
Collection of IP and subnet addresses	未サポート
Exclude IP address	未サポート
TACACS information	TACACS は Cisco ISE リリース 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	このプロパティは Cisco ISE でのみ有効です（値はデフォルトで「unknown」）。
Software version	このプロパティは Cisco ISE でのみ有効です（値はデフォルトで「unknown」）。

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

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 2.4 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
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 リリース で、コロンを有効な文字として認識しないためです。

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
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

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

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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 2.4 には、ユーザ 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 2.4 へ、ユーザ ID グループおよびエンドポイント ID グループとして移行されます。これは、ユーザをユーザ ID グループに割り当て、エンドポイントをエンドポイント ID グループに割り当てる必要があるためです。

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がありません
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
Expiry days	未サポート

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

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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
Name	Name
Description	Description
Server connection information	そのまま移行（[サーバ接続（Server Connection）] タブ。A-10 ページの図 A-1 を参照）。

データ構造マッピング

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。A-10 ページの図 A-2 を参照）。
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。

図 *2 : [サーバ接続（Server Connection）] タブ*

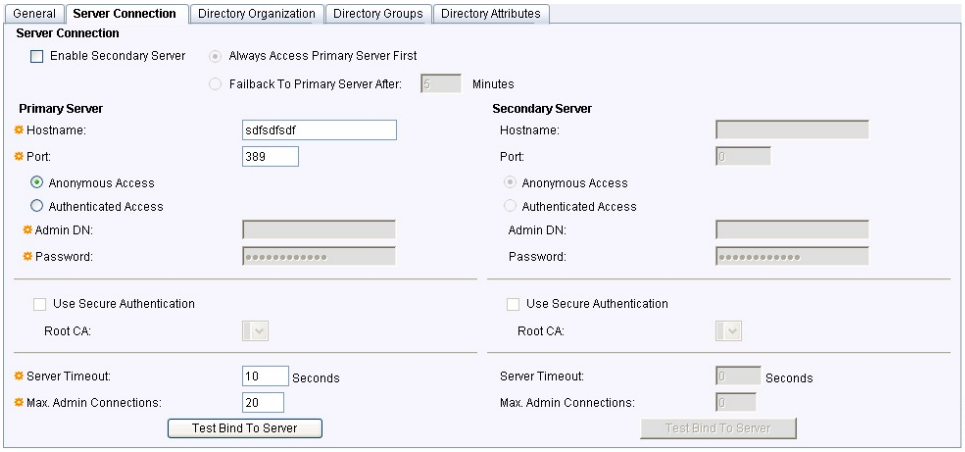
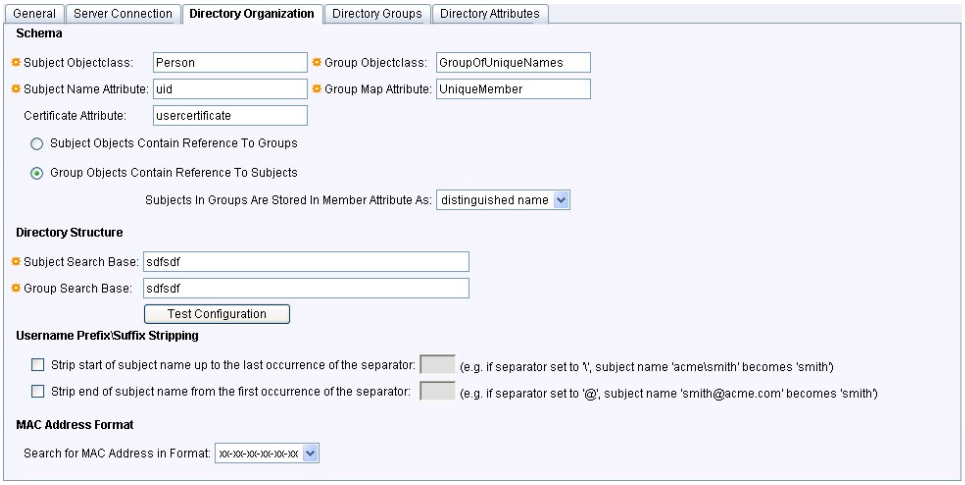


図 *3 : [ディレクトリ構成（Directory Organization）] タブ*



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
Name	Name
Description	Description
Principle user name（X.509 属性）	Principle user name（X.509 属性）
Binary certificate comparison with certificate from LDAP or AD	Binary certificate comparison with certificate from LDAP or AD
AD or LDAP name for certificate fetching	AD or LDAP name for certificate fetching。

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
Name	Name
Description	Description
Certificate based, certificate authentication profile	Certificate based, certificate authentication profile
Password based	Authentication search list

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）

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
Name	Name
Description	Description
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、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 属性

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
Name	Name
Description	Description
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
Name	Name
Description	Description

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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 リリース 5.5 以降のインストールの一部ではない、RADIUS ベンダーのみ移行する必要があります。これはユーザ定義ベンダーにのみ影響します。

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、ユーザ定義の 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）。

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	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
Description	Internal name
Name	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 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

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Mandatory field	なし
Add policy condition	なし
Policy condition display name	なし

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	ホストネーム
Shared secret	Shared secret
Authentication port	Authentication port
Accounting port	Accounting port
Server timeout	Server timeout
Connection attempts	Connection attempts

RADIUS トークン マッピング

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

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

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