

AD のクレデンシャルを使った ISE の管理ポータル アクセスの設定例

目次

[はじめに](#)

[前提条件](#)

[使用するコンポーネント](#)

[設定](#)

[AD への ISE の結合](#)

[ディレクトリ グループの選択](#)

[AD 用管理アクセスの有効化](#)

[管理グループから AD グループへのマッピングの設定](#)

[管理グループの RBAC アクセス許可の設定](#)

[AD クレデンシャルでの ISE へのアクセス](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Identity Services Engine (ISE) 管理 GUI への管理アクセスのために外部アイデンティティストアとして Microsoft Active Directory (AD) を使用するための設定例を示します。

前提条件

次の項目に関する知識が推奨されます。

- Cisco ISE バージョン 1.1.x 以降の設定
- Microsoft AD

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ISE バージョン 1.1.x
- Windows Server 2008 リリース 2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用されるすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中

のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

このセクションでは、Cisco ISE 管理 GUI への管理アクセスのために外部アイデンティティストアとして Microsoft AD を使用するための設定について説明します。

AD への ISE の結合

1. [Administration] > [Identity Management] > [External Identity Sources] > [Active Directory] を順に選択します。
2. AD の [Domain Name] と [Identity Store Name] を入力し、[Join] をクリックします。
3. コンピュータ オブジェクトに追加して変更を加えることのできる AD アカウントのクレデンシャルを入力し、[Save Configuration] をクリックします。

ディレクトリ グループの選択

1. [Administration] > [Identity Management] > [External Identity Sources] > [Active Directory] > [Groups] > [Add] > [Select groups form Directory] を順に選択します。
2. 管理者が属する 1 つ以上の AD グループをインポートします。

AD 用管理アクセスの有効化

AD のパスワード ベースの認証を有効にするには、次の手順を実行してください。

1. [Administration] > [System] > [Admin Access] > [Authentication] を順に選択します。
2. [Authentication Method] タブで [Password Based] オプションを選択します。
3. [Identity Source] ドロップダウン メニューから [AD] を選択します。
4. [Save Changes] をクリックします。

管理グループから AD グループへのマッピングの設定

Cisco ISE 管理グループを定義し、それを AD グループにマップします。これにより認証において、AD のグループ メンバーシップに基づいて管理者の役割ベース アクセス制御 (RBAC) 権限が判別されます。

1. [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [管理者 (Administrators)] > [管理者グループ (Admin Groups)] に移動します。
2. テーブルのヘッダーで [Add] をクリックして、新しい [Admin Group] 設定ペインを表示します。

3. 新しい管理グループの名前を入力します。
4. [Type] フィールドで [External check box] をオンにします。
5. [External Groups] ドロップダウン メニューから、[Select Directory Groups] セクションに定義されているとおりに、この管理グループをマップする AD グループを選択します。
6. [Save Changes] をクリックします。

管理グループの RBAC アクセス許可の設定

前のセクションで作成した管理グループに RBAC の権限を割り当てるには、次の手順を実行してください。

1. [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [許可 (Authorization)] > [ポリシー (Policy)] に移動します。
2. 右側にある [Actions] ドロップダウン メニューから [Insert New Policy Below] を選択して、新しいポリシーを追加します。
3. **ISE_administration_AD** という名前の新しいルールを作成し、[Enable Administrative Access for AD] セクションに定義されている管理グループにマップし、権限を割り当てます。**注:** この例では、**Super Admin** という名前の管理グループが割り当てられます。このグループは標準管理アカウントに相当します。
4. [Save Changes] をクリックすると、保存された変更の確認が GUI の右下隅に表示されます。

AD クレデンシャルでの ISE へのアクセス

AD クレデンシャルを使用して ISE にアクセスするには、次の手順を実行してください。

1. 管理 GUI からログアウトします。
2. [Identity Source] ドロップダウン メニューから [AD1] を選択します。
3. AD データベースからユーザ名とパスワードを入力し、ログインします。

注: ISE は、AD が到達不能になった場合、または使用されているアカウント認証情報が AD に存在しない場合に、デフォルトで内部ユーザストアに設定されます。これにより、AD が管理アクセス用に設定されているときには、内部ストアを使用すると、クイックログインが促進されます。

確認

設定が正しく機能することを確認するには、ISE GUI の右上隅で認証されたユーザ名を検証します。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [Cisco Identity Services Engine ユーザ ガイド、リリース 1.1 - ID および管理者アクセスの管理](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)