



[Realms]

次のトピックでは、レルムとアイデンティティ ポリシーについて説明します。

- [レルムのライセンス要件](#) (1 ページ)
- [レルムの要件と前提条件](#) (1 ページ)
- [Microsoft Azure AD \(SAML\) レルムを作成する](#) (2 ページ)
- [LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する](#) (32 ページ)
- [レルムシーケンスを作成する](#) (57 ページ)
- [クロスドメイン信頼に対して Firewall Management Center を構成する：手順](#) (58 ページ)
- [レルムを管理する](#) (67 ページ)
- [レルムを比較する](#) (67 ページ)
- [レルムとユーザーのダウンロードをトラブルシュートする](#) (68 ページ)
- [レルムの履歴](#) (77 ページ)

レルムのライセンス要件

Threat Defense License

任意

レルムの要件と前提条件

Model support

任意

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

Microsoft Azure AD (SAML) レルムを作成する

Microsoft Azure Active Directory (AD) (現在名: *Entra ID*) レルムは、パッシブ認証またはアクティブ認証のいずれかに使用できます。

変更管理を有効にした場合は、この手順で使用されるすべての証明書を承認する必要があります。新しいチケットを開くか、既存のチケットを編集してください。詳細については、「[変更管理チケットの作成](#)」を参照してください。[変更管理をサポートするポリシーとオブジェクト](#)

パッシブ認証

パッシブ認証は、ユーザーが Cisco ISE で認証されるときに発生します。

ユーザーとグループのリポジトリの選択に応じて、次のオプションが使用できます。

- Cisco ISE をユーザーのリポジトリとして使用するには、Entra ID を使用してパッシブ認証を実行します。詳細については、以下を参照してください。
 - [リソース独自のパスワードログイン情報を使用する Entra ID と Cisco ISE について \(4 ページ\)](#)
 - [TEAP/EAP-TLS を使用する Entra ID と Cisco ISE について \(5 ページ\)](#)
- Entra ID からグループをダウンロードする場合。

Entra ID の設定の詳細については、「[パッシブ認証用の Microsoft Entra ID を構成する \(7 ページ\)](#)」を参照してください。

アクティブ認証

アクティブ認証は、ユーザーが事前設定済みの管理対象デバイス経由で認証されるときに発生します。アクティブ認証はキャプティブポータルとも呼ばれます。アクティブ認証は通常、パッシブ認証と同じユーザーリポジトリを使用します (例外として、ISE/ISE-PIC、TS エージェント、および Passive Identity Agent はパッシブのみです)。

Microsoft Entra ID をキャプティブポータルとして使用するには、ユーザーが Entra ID で認証される必要があります。以下の間の信頼関係を確立するためにセキュリティアサーションマークアップ言語 (SAML) が使用されるため、これは SAML レルムと呼ばれます。

- サービスプロバイダー (Secure Firewall Threat Defense デバイスまたは認証要求の送信先デバイス)。
- ID プロバイダー (Microsoft Entra ID)。

SAML は、OASIS 標準化団体によって開発されたオープンな標準です。詳細については、「[SAML の概要](#)」を参照してください。

詳細については、「[Microsoft Azure AD \(SAML\) realm for active authentication \(captive portal\) を作成する方法 \(16 ページ\)](#)」を参照してください。

パッシブ認証向け Microsoft Azure AD (SAML)を作成する方法

このトピックでは、Secure Firewall Management Center と使用するパッシブ認証用 Microsoft Azure AD (SAML) レルム（現在名：*Entra ID*）作成時のタスクについて概説します。

手順

	コマンドまたはアクション	目的
ステップ 1	Dynamic Attributes Connector をイネーブ ルにします。	Dynamic Attributes Connector は、Microsoft Azure AD (SAML) レルムを使用するために必要です。最初に行うことも、レルムの作成時に有効にすることもできます。詳細については、 dynamic attributes connector の有効化 を参照してください。
ステップ 2	Microsoft Entra ID を構成します。	イベントハブのセットアップ、Microsoft Graph API へのアクセス権限のアプリケーションへの付与、監査ログの有効化など、いくつかの設定タスクが必要です。 パッシブ認証用の Microsoft Entra ID を構成する (7 ページ) を参照してください。
ステップ 3	Cisco ISE を設定します。	ISE を設定する方法は、ユーザーがシステムで認証する方法によって異なります。詳細については、 Microsoft Azure AD (SAML) 向けの Cisco ISE を構成する方法 (6 ページ) を参照してください。
ステップ 4	Cisco ISE アイデンティティソースを作成します。	アイデンティティソースにより、ISE は、Secure Firewall Management Center との通信が可能になります。
ステップ 5	Microsoft Azure AD (SAML) レルムの設定に必要な情報を取得します。	この情報には、Microsoft Entra ID に保存されているクライアント ID/テナント ID、クライアントシークレットなどの情報が含まれます。

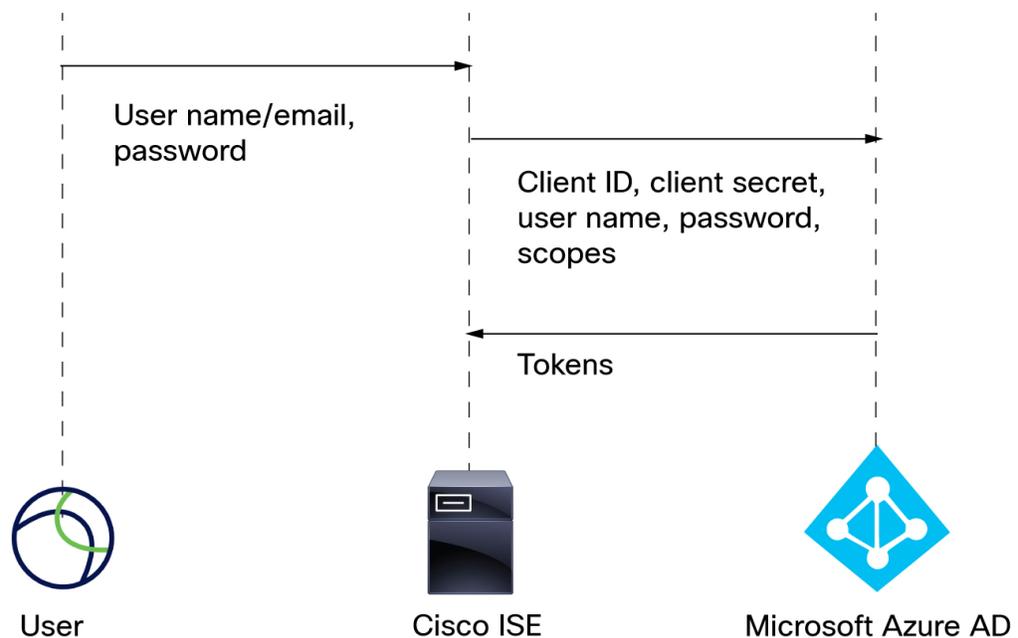
	コマンドまたはアクション	目的
ステップ 6	レルムを設定して確認します。	<p>アクセス コントロール ポリシーでのレルムの使用を開始する前に、レルムの設定をテストします。</p> <p>Microsoft Azure AD (SAML) レルムを作成する (2 ページ) の説明に従って、Microsoft Azure AD (SAML) レルムを作成します。</p>
ステップ 7	Microsoft Azure AD (SAML) レルムを使用して、アクセス コントロール ポリシーおよびルールを作成します。	<p>他のタイプのレルムとは異なり、ID ポリシーを作成したり、ID ポリシーをアクセス コントロール ポリシーに関連付ける必要はありません。</p> <p>基本的なアクセス コントロール ポリシーの作成およびアクセス コントロール ルールの作成および編集を参照してください。</p>

次のタスク

「リソース独自のパスワードログイン情報を使用する Entra ID と Cisco ISE について (4 ページ)」を参照してください。

リソース独自のパスワードログイン情報を使用する Entra ID と Cisco ISE について

以下の図は、Cisco ISE の Azure AD (現在名: *Entra ID*) レルムと Resource Owned Password Credentials (ROPC) をまとめたものです。



ROPC を使用すると、次の操作が行われます。

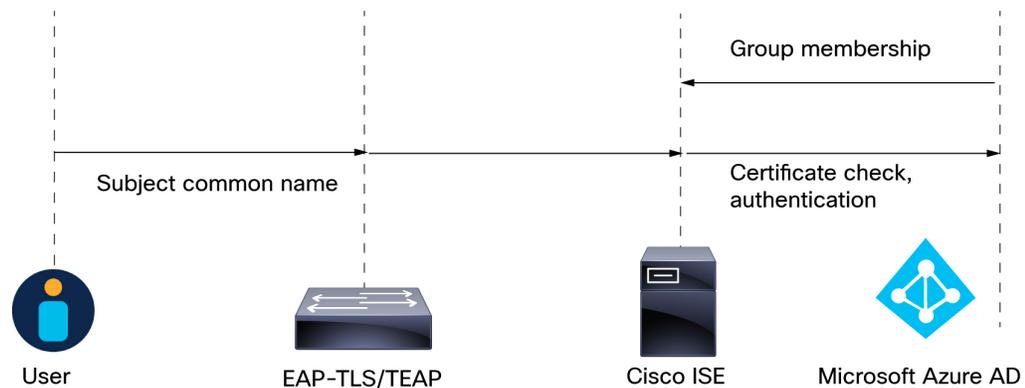
1. ユーザーは、Cisco Secure Client などの VPN クライアントを使用して、ユーザー名（または電子メールアドレス）とパスワードでログインします。
2. クライアント ID、クライアントシークレット、ユーザー名、パスワードおよびスコープが、Entra ID に送信されます。
3. トークンは、Entra ID から Cisco ISE に送信され、そこからユーザーセッションが Secure Firewall Management Center に送信されます。

Cisco ISE の設定の詳細については、「[Configure ISE 3.0 REST ID with Azure Active Directory](#)」
[英語] を参照してください。

その他のリソース：[Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials](#)
(learn.microsoft.com)

TEAP/EAP-TLS を使用する Entra ID と Cisco ISE について

[RFC7170](#) で定義されている Tunnel Extensible Authentication Protocol (TEAP) は、ISE および Secure Firewall Management Center で次のように使用できます。



以下は、『[Configure Cisco ISE 3.2 EAP-TLS with Microsoft Azure Active Directory](#)』に基づいています。

1. ユーザーの証明書は、内部方式として EAP-TLS または EAP-TLS を使用した TEAP を介して ISE に送信されます。
2. ISE は、ユーザーの証明書を評価します（有効期間、信頼された証明機関、証明書失効リストなど）。
3. ISE は、証明書のサブジェクト名（CN）を取得し、Azure Graph API へのルックアップを実行して、ユーザーのグループとその他の属性を取得します。これは、Azure ではユーザープリンシパル名（UPN）と呼ばれます。
4. ISE の承認ポリシーは、Azure から返されるユーザーの属性に対して評価されます。

Microsoft Azure AD (SAML) 向けの Cisco ISE を構成する方法

Microsoft Azure AD (SAML)（現在名：*Entra ID*）レルムでは、ISE がユーザーセッション（ログイン、ログアウト）を Secure Firewall Management Center に送信します。このトピックでは、Azure AD レルムで使用するために ISE を設定する方法について説明します。

リソース所有者パスワードクレデンシャル認証

リソース所有者パスワードクレデンシャル（ROPC）を使用して、Representational State Transfer（REST）アイデンティティ（ID）サービスを介して導入された Microsoft Azure AD (SAML) で ISE を使用するには、「[Configure ISE 3.0 REST ID with Azure Active Directory](#)」[英語]を参照してください。

TEAP/EAP-TLS

認証プロトコルとして EAP-TLS または TEAP を使用して、Azure AD グループメンバーシップおよびその他のユーザー属性に基づく認証ポリシーで ISE を使用するには、「[Configure Cisco ISE 3.2 EAP-TLS with Microsoft Azure Active Directory](#)」を参照してください。

次の作業

[Microsoft Azure AD \(SAML\) レルムに必要な情報を取得する](#)（9 ページ）

パッシブ認証用の Microsoft Entra ID を構成する

このトピックでは、Secure Firewall Management Center 併用できるレルムとして Microsoft Entra ID (旧称: *Microsoft Azure Active Directory (AD)*) を設定する方法の基本情報を提供します。ここでは Entra ID に精通していることを前提とします。精通していない場合は、開始前にドキュメントまたはサポートリソースをご確認ください。

Microsoft Graph の権限をアプリケーションに付与する

Microsoft サイトの「[Authorization and the Microsoft Graph Security API](#)」で説明されているように、Microsoft Graph に対する次の権限を Entra ID アプリケーションに付与します。

- Reader ロール
- User.Read.All 権限
- Group.Read.All 権限

このアクセス許可により、Secure Firewall Management Center は、最初に Entra ID からユーザーとグループをダウンロードできるようになります。

Secure Firewall Management Center で Entra ID レルムを設定するためにこの手順から必要な情報:

- 登録したアプリの名前
- アプリケーション (クライアント) ID
- クライアントシークレット
- ディレクトリ (テナント) ID

イベントハブをセットアップする

Microsoft サイトの「[Quickstart: Create an event hub using Azure portal](#)」で説明されているように、イベントハブをセットアップします。Secure Firewall Management Center は、イベントハブ監査ログを使用して、定期的なアップデートをユーザーとグループにダウンロードします。

詳細: 「[Features and terminology in Azure Event Hubs](#)」。



重要 [標準 (Standard)] 以上の価格帯を選択する必要があります。[基本 (Basic)] を選択した場合、レルムは使用できません。

Secure Firewall Management Center で Entra ID レルムを設定するためにこの手順から必要な情報:

- 名前空間の名前
- 接続文字列 - 主キー
- イベントハブ名

- コンシューマグループ名

監査ログを有効にする

Microsoft サイトの「[Tutorial: Stream Azure Active Directory logs to an Azure event hub](#)」で説明されているように、監査ログを有効にします。

Entra ID の Cisco ISE を構成する

ユーザーセッション情報を Secure Firewall Management Center に送信するには、「[Azure Active Directory を使用して ISE 3.0 REST ID を構成する](#)」で説明されているように、Entra ID に Cisco ISE を構成します。

次の作業

「[Microsoft Azure AD \(SAML\) 向けの Cisco ISE を構成する方法 \(6 ページ\)](#)」を参照してください。

Entra ID の基本設定を構成する

Microsoft Graph の権限をアプリケーションに付与する

Microsoft サイトの「[Authorization と Microsoft Graph Security API](#)」に記載されているように、Entra ID アプリケーション（旧称：Azure AD）に Microsoft Graph に対する次の権限を付与します。

- Reader ロール
- User.Read.All 権限
- Group.Read.All 権限

このアクセス許可により、Firewall Management Center は、最初に Entra ID からユーザーとグループをダウンロードできるようになります。

Firewall Management Center で Entra ID レalmを設定するためにこの手順から必要な情報：

- 登録したアプリの名前
- アプリケーション（クライアント）ID
- クライアントシークレット
- ディレクトリ（テナント）ID

イベントハブをセットアップする

Microsoft サイトの「[Quickstart: Create an event hub using Azure portal](#)」で説明されているように、イベントハブをセットアップします。Firewall Management Center は、イベントハブ監査ログを使用して、定期的なアップデートをユーザーとグループにダウンロードします。

詳細：「[Features and terminology in Azure Event Hubs](#)」。



重要 [標準 (Standard)]以上の価格帯を選択する必要があります。[基本 (Basic)]を選択した場合、レルムは使用できません。

Secure Firewall Management Center で Entra ID レルムを設定するためにこの手順から必要な情報：

- 名前空間の名前
- 接続文字列 - 主キー
- イベントハブ名
- コンシューマグループ名

監査ログを有効にする

Microsoft サイトの「[Tutorial: Stream Azure Active Directory logs to an Azure event hub](#)」で説明されているように、監査ログを有効にします。

Microsoft Azure AD (SAML) レルムに必要な情報を取得する

このタスクでは、Secure Firewall Management Center で Microsoft Azure AD (SAML) (現在名：Entra ID) レルムを設定するために必要な情報の取得方法を説明します。[パッシブ認証用の Microsoft Entra ID を構成する \(7 ページ\)](#) で説明されているように Microsoft Entra ID の設定時に、この情報をすでに取得している場合があります。

手順

- ステップ 1** 少なくとも製品デザイナー (Product Designer) ロールを持つユーザーとして <https://portal.azure.com/> にログインします。
- ステップ 2** ページの上部で、[Microsoft Entra ID] をクリックします。
- ステップ 3** 左側の列で、[アプリの登録 (App Registrations)] をクリックします。
- ステップ 4** 必要に応じて、表示されたアプリのリストをフィルタ処理して、使用するアプリを表示します。
- ステップ 5** アプリの名前をクリックします。

Display name	: docs-test	Client credentials	: 0_certificate_1_secret
Application (client) ID	: 7 [redacted] c11	Redirect URIs	: Add a Redirect URI
Object ID	: [redacted] 1b9	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: [redacted] 90	Managed application in l...	: docs-test
Supported account types	: My organization only		

ステップ 6 このページの次の値の横にある **Copy** (📄) をクリックし、それらの値をテキストファイルに貼り付けます。

- [Application (Client) ID]
- ディレクトリ (テナント) ID

ステップ 7 [クライアントのログイン情報 (Client Credentials)] をクリックします。

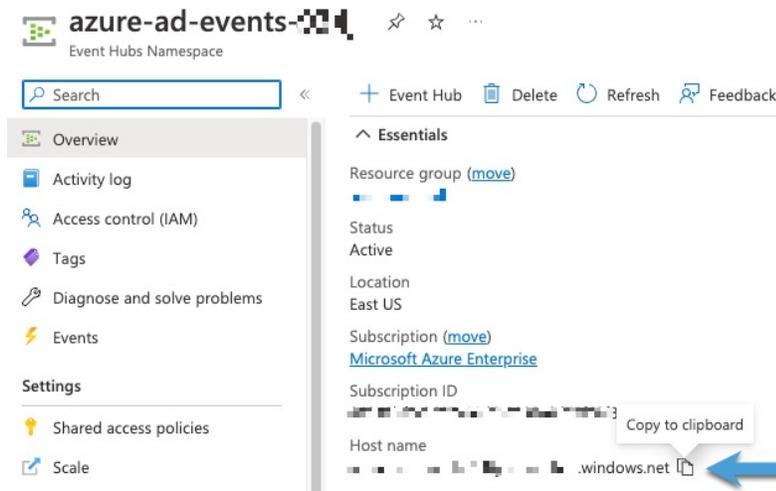
ステップ 8 クライアントシークレット値 (クライアントシークレット ID ではありません) がすでにわかっている場合を除き、次のように新しいクライアントシークレットを作成する必要があります。

- [新しいクライアントシークレット (New Client Secret)] をクリックします。
- 表示されたフィールドに必要な情報を入力します。
- [Add] をクリックします。
- 次の図に示すように、[値 (Value)] の横にある **Copy** (📄) をクリックします。



ステップ 9 <https://portal.azure.com/> から、[(イベントハブの名前) (Event Hubs)] > の順にクリックします。

ステップ 10 右側のペインで、[ホスト名 (Host name)] の値の横にある **Copy** (📄) をクリックして値をクリップボードに貼り付けます。これは、イベントハブホスト名です。

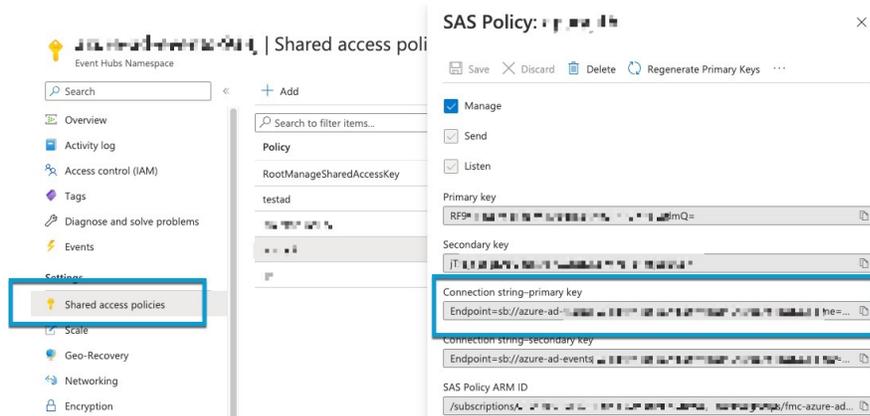


ステップ 11 イベントハブの名前を書き留めるか、テキストファイルにコピーします (ページの上部にある [Event Hubs名前空間 (Event Hubs Namespace)] と同じ)。

ステップ 12 左側のペインの [設定 (Settings)] で、[共有アクセスポリシー (Shared access policies)] をクリックします。

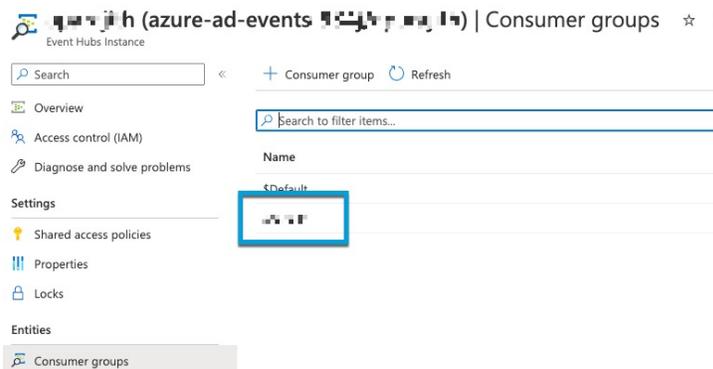
ステップ 13 ポリシーの名前をクリックします。

ステップ 14 [接続文字列-主キー (Connection string-primary key)] の横にある **Copy** (📄) をクリックします。



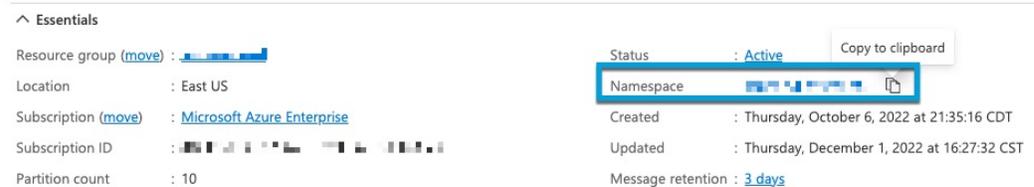
ステップ 15 [概要 (Overview)] > [エンティティ (Entities)] > [イベントハブ (Event Hubs)] > (イベントハブの名前) > [エンティティ (Entities)] > [コンシューマグループ (Consumer Groups)] の順にクリックします。

次の値を書き留めるか、クリップボードにコピーします。これは、コンシューマグループ名です。



ステップ 16 左側のペインで [概要 (Overview)] をクリックします。

ステップ 17 [名前空間 (Namespace)] の横にある **Copy** (📄) をクリックします。



これは、イベントハブトピック名です。

パッシブ認証用の Microsoft Azure AD (SAML) レルムを作成する

次のトピックでは、パッシブ認証に対して Microsoft Azure AD (SAML) (現在名: *Entra ID*) レルムを生成する際に必要な複数手順のウィザードを実行する方法を説明します。

Microsoft Azure Active Directory (AD) レルムと Cisco ISE を使用すると、ユーザーを認証したり、ユーザー制御のためにユーザーセッションを取得したりできます。Entra ID からグループを、Cisco ISE からログインユーザーセッションデータ取得します。

次の選択肢があります。

- リソース所有者のパスワードクレデンシャル (ROPC) : ユーザーが、ユーザー名とパスワードを使用して Cisco Secure Client などのクライアントにログインできるようにします。ISE はユーザーセッションを Secure Firewall Management Center に送信します。詳細については、[リソース独自のパスワードログイン情報を使用する Entra ID と Cisco ISE について \(4 ページ\)](#) を参照してください。

その他のリソース : [Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials](#) (learn.microsoft.com)

- トンネルベースの拡張可能認証プロトコル (TEAP) および Transport Layer Security (TLS) を使用する拡張可能認証プロトコル (EAP) チューニング、略して EAP/TEAP-TLS : TEAP は、安全なトンネルを確立し、その安全なトンネルの保護下で他の EAP メソッドを実行するトンネルベースの EAP メソッドです。ISE は、ユーザークレデンシャルを検証し、ユーザーセッションを Secure Firewall Management Center に送信するために使用されます。詳細については、[TEAP/EAP-TLS を使用する Entra ID と Cisco ISE について \(5 ページ\)](#) を参照してください。

レルムを設定するには、次の順序ですべてのタスクを実行します。

1. [Entra ID の基本設定を構成する \(8 ページ\)](#)。
2. 「[Microsoft Azure AD \(SAML\) レルムに必要な情報を取得する \(9 ページ\)](#)」で説明されている、レルムに必要な情報を取得します。
3. [Microsoft Azure AD \(SAML\) レルム : SAML の詳細 \(12 ページ\)](#)。

Microsoft Azure AD (SAML) レルム : SAML の詳細

このタスクでは、Microsoft Azure AD (SAML) レルムを作成する複数ステップのウィザードの最初のステップについて説明します。レルムを設定するには、ウィザードのすべてのステップを完了する必要があります。手順は、アクティブ認証用のレルムを作成するか、パッシブ認証用のレルムを作成するかによって異なります。

始める前に

レルムを作成する前に、次のタスクをすべて実行します。

- (Cisco ISE によるパッシブ認証のみ) ユーザーおよびグループのリポジトリとして Cisco ISE を使用している場合は、ISE を設定します。

- [リソース独自のパスワードログイン情報を使用する Entra ID と Cisco ISE について \(4 ページ\)](#)
- [TEAP/EAP-TLS を使用する Entra ID と Cisco ISE について \(5 ページ\)](#)
- Entra ID をユーザーとグループのリポジトリとして使用するには、「[パッシブ認証用の Microsoft Entra ID を構成する \(7 ページ\)](#)」を参照してください。
- 「[Microsoft Azure AD \(SAML\) レルムに必要な情報を取得する \(9 ページ\)](#)」で説明されている、レルムに必要な情報を取得します。

手順

ステップ 1 Secure Firewall Management Center にログインします。

ステップ 2 **Integration > Other Integrations > Realms > Realms** をクリックします。

ステップ 3 [レルムを追加 (Add Realm)] > [SAML - Azure AD] をクリックします。

ステップ 4 次の情報を入力します。

項目	説明
名前 (Name)	レルムを識別する一意の名前。
説明	(オプション) レルムの説明。
アイデンティティ プロバイダー	常に [Azure AD] が表示されます。
設定の種類	次のいずれかをクリックします。 <ul style="list-style-type: none"> • パッシブ認証の場合は、[ISEによるパッシブ認証 (Passive authentication with ISE)]。 • パッシブ認証またはアクティブ認証 (つまり、キャプティブポータル) のユーザーストアとして Entra ID を使用するための Azure AD を使用するパッシブ認証またはキャプティブポータル

ステップ 5 [次へ (Next)] をクリックします。

次のタスク

次のいずれかです。

- パッシブ認証 : 「[Microsoft Azure AD \(SAML\) レルム : Azure AD の詳細 \(14 ページ\)](#)」。

- アクティブ認証 : 「[Microsoft Azure AD \(SAML\) レルム : SAML サービスプロバイダー \(SP\) のメタデータ \(28 ページ\)](#)」。

Microsoft Azure AD (SAML) レルム : Azure AD の詳細

このタスクでは、Microsoft Azure AD (SAML) レルムを作成できる複数ページのウィザードの 1 ページについて説明しました。

手順

ステップ 1 ウィザードの前の手順から続行します。

ステップ 2 次の情報を入力します。

項目	説明
名前 (Name)	このレルムを識別するための一意の名前を入力します。
クライアントのシークレット (Client Secret)	以下で説明されている、取得済みの情報を入力します。
テナント ID	<ul style="list-style-type: none"> • パッシブ認証 : 「パッシブ認証向け Microsoft Azure AD (SAML) を作成する方法 (3 ページ)」
イベントハブホスト名 (Event Hubs Host Name)	<ul style="list-style-type: none"> • アクティブ認証 : 「Microsoft Azure AD (SAML) レルムに必要な情報を取得する (アクティブ認証のみ) (22 ページ)」
イベントハブ名 (Event Hub Name)	
イベントハブ接続文字列 (Event Hub Connection String)	
(任意) ユーザグループ	Slider enabled (<input checked="" type="checkbox"/>) にスライドして、ポリシーに含めるグループまたはポリシーから除外するグループを指定します。
(任意) 除外するユーザーグループ (Excluded User Groups)	このフィールドに 1 つ以上のグループ名を入力した場合は、それ以外のすべてのグループとそれらのグループに含まれるユーザーがダウンロードされ、ユーザー認識やユーザー制御に利用できます。 1 行に 1 つのグループ名を入力し、その後に改行します。グループ名では大文字と小文字が区別されます。

項目	説明
(オプション) 含めるユーザーグループ (Included User Groups)	このフィールドに1つ以上のグループ名を入力した場合は、それらのグループとそれらのグループに含まれるユーザーだけがダウンロードされ、ユーザーデータはユーザー認識やユーザー制御に利用できます。 1行に1つのグループ名を入力し、その後に改行します。グループ名では大文字と小文字が区別されます。

- ステップ 3** [テスト (Test)] をクリックします。
次の手順に進む前に、テスト接続が成功することを確認します。
- ステップ 4** [次へ (Next)] をクリックします。

Microsoft Azure AD (SAML) レルム : ユーザー セッション タイムアウト

このタスクでは、Microsoft Azure AD (SAML) レルムを作成できる複数ページのウィザードの1ページについて説明しました。

このオプションでは、非アクティブなセッションがシステムによって終了されるまでの秒数を設定します。

手順

- ステップ 1** ウィザードの前の手順から続行します。
- ステップ 2** 次の情報を入力します。

項目	説明
ISE ユーザー	デフォルト値は 1440 分 (24 時間) です。
キャプティブポータルユーザー	デフォルト値は 1440 分 (24 時間) です。

このタイムアウトを過ぎると、ユーザーのセッションは終了します。ユーザーが再度ログインせずにネットワークにアクセスし続けている場合、ユーザーは Firewall Management Center により不明として認識されます ([失敗したキャプティブポータルユーザー (Failed Captive Portal Users)] を除く)。

- ステップ 3** [Save (保存)] をクリックします。

Microsoft Azure AD (SAML) realm for active authentication (captive portal) を作成する方法

このトピックでは、Secure Firewall Management Center で使用する Microsoft Azure Active Directory (AD) レルム (現在名: *Entra ID*) を作成するハイレベルタスクについて説明します。

始める前に

変更管理を有効にした場合は、レルムを作成する前に、次の各オブジェクトのチケットを開くか、編集、割り当て、および承認する必要があります。

- [ベースURL (Base URL)]
- サービスプロバイダー証明書の登録 (PKCS12 形式)
- アイデンティティ プロバイダー証明書の登録 (手動形式)
- レルム自体 (レルムの作成が完了するまでチケットを作成して割り当ててから、承認します)

詳細については、「[設定変更のためのチケットのオープン](#)」および「[変更管理をサポートするポリシーとオブジェクト](#)」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	DNS サーバーを使用して完全修飾ホスト名 (FQDN) を作成し、Firewall Threat Defense の内部証明書を Secure Firewall Management Center にアップロードします。これまでに行ったことがない場合は、 このようなリソース を参照できます。Secure Firewall Management Center で管理されるデバイスの 1 つにあるルーテッドインターフェイスの IP アドレスを指定します。	DNS サーバーの資料を参照してください。
ステップ 2	Dynamic Attributes Connector をイネーブルにします。	Dynamic Attributes Connector は、Microsoft Azure AD レルムを使用するために必要です。最初に行うことも、レルムの作成時に有効にすることもできます。詳細については、 dynamic attributes connector の有効化を参照してください。
ステップ 3	内部証明書が関連付けられたネットワークオブジェクトを作成します。	ネットワークオブジェクトの作成 を参照してください。

	コマンドまたはアクション	目的
ステップ 4	署名済み証明書を取得したら、Entra ID 認証リクエストの送信先となる Secure Firewall Threat Defense にアップロードします。	<p>証明書は、信頼できる認証局 (CA) によって署名され、.p12 形式 (PKCS#12 と呼ばれます。ssl.com の この記事 も参照してください) で提供される必要があります。</p> <p>背景については、『Cisco Secure Firewall Management Center Device Configuration Guide』または stackoverflow.com の公開キーインフラストラクチャに関するセクションを参照してください。</p> <p>署名付き証明書をアップロードするには、PKCS12 ファイルを使用した証明書のインストール を参照してください。</p>
ステップ 5	Microsoft Entra ID の基本設定を構成します。	<p>イベントハブのセットアップ、Microsoft Graph API へのアクセス権限のアプリケーションへの付与、監査ログの有効化など、いくつかの設定タスクが必要です。</p> <p>Entra ID の基本設定を構成する (8 ページ) を参照してください。</p>
ステップ 6	Entra ID でシングルサインオン (SSO) アプリケーションを作成します。	<p>SSO アプリケーションを使用すると、保護されたネットワークリソースへのアクセスを要求するユーザーが Entra ID で認証できるようになります。SSO アプリケーションには、レールの作成を簡素化するために使用できるフェデレーション XML と、Entra ID でのセキュリティ認証のために Secure Firewall Threat Defense が必要とするアイデンティティプロバイダー証明書の両方が含まれています。</p> <p>Entra ID でシングルサインオン (SSO) アプリケーションを構成する (20 ページ) を参照してください。</p>
ステップ 7	Microsoft Azure AD (SAML) レールの設定に必要な情報を取得します。	この情報には、Microsoft Entra ID に保存されているクライアント ID/テナント ID、クライアントシークレットなどの情報が含まれます。

	コマンドまたはアクション	目的
		Microsoft Azure AD (SAML) レルムに必要な情報を取得する (9 ページ) を参照してください。
ステップ 8	ユーザーが HTTPS プロトコルを使用して Web ページにアクセスできるようにするため、Azure 認証サービスの 復号 - 再署名 ルールを使用して a decryption policy を設定します。	Microsoft Azure AD (SAML) レルムは、HTTPS トラフィックがレルムに送信される前に復号された場合にのみユーザーを認証できます。Microsoft Azure AD (SAML) レルム自体は、システムからは Azure 認証サービス アプリケーションとして認識されます。 復号/再署名アクションを使用して複合ルールを作成する (21 ページ) 。
ステップ 9	アクティブ認証ルールを含むアイデンティティポリシーを作成します。	Microsoft Azure AD (SAML) レルムによる認証後、アイデンティティポリシーによって、レルムアクセスリソースで選択したユーザーが有効になります。 詳細については、「 アイデンティティポリシーの作成 」を参照してください。
ステップ 10	Microsoft Azure AD レルムを使用して、アクセスコントロールポリシーおよびルールを作成します。	他のタイプのレルムとは異なり、ID ポリシーを作成したり、ID ポリシーをアクセスコントロールポリシーに関連付ける必要はありません。 基本的なアクセスコントロールポリシーの作成およびアクセスコントロールルールの作成および編集 を参照してください。
ステップ 11	アイデンティティと decryption policies をアクセスコントロールポリシーに関連付けます (ステップ 3)。	この最後の手順により、システムは Microsoft Azure AD (SAML) レルムを使用してユーザーを認証します。 詳細については、 アクセス制御への他のポリシーの関連付け を参照してください。

次のタスク

「[Entra ID の基本設定を構成する \(8 ページ\)](#)」を参照してください。

Entra ID の基本設定を構成する

Microsoft Graph の権限をアプリケーションに付与する

Microsoft サイトの「[Authorization と Microsoft Graph Security API](#)」に記載されているように、Entra ID アプリケーション（旧称：Azure AD）に Microsoft Graph に対する次の権限を付与します。

- Reader ロール
- User.Read.All 権限
- Group.Read.All 権限

このアクセス許可により、Firewall Management Center は、最初に Entra ID からユーザーとグループをダウンロードできるようになります。

Firewall Management Center で Entra ID レルムを設定するためにこの手順から必要な情報：

- 登録したアプリの名前
- アプリケーション（クライアント）ID
- クライアントシークレット
- ディレクトリ（テナント）ID

イベントハブをセットアップする

Microsoft サイトの「[Quickstart: Create an event hub using Azure portal](#)」で説明されているように、イベントハブをセットアップします。Firewall Management Center は、イベントハブ監査ログを使用して、定期的なアップデートをユーザーとグループにダウンロードします。

詳細：「[Features and terminology in Azure Event Hubs](#)」。



重要 [標準（Standard）]以上の価格帯を選択する必要があります。[基本（Basic）]を選択した場合、レルムは使用できません。

Secure Firewall Management Center で Entra ID レルムを設定するためにこの手順から必要な情報：

- 名前空間の名前
- 接続文字列 - 主キー
- イベントハブ名
- コンシューマグループ名

監査ログを有効にする

Microsoft サイトの「[Tutorial: Stream Azure Active Directory logs to an Azure event hub](#)」で説明されているように、監査ログを有効にします。

Entra ID でシングルサインオン (SSO) アプリケーションを構成する

このトピックでは、ネットワークユーザーが保護されたネットワークにアクセスしようとする際に、Entra ID からのシングルサインオン (SSO) を処理するアプリケーションを Microsoft Entra ID で作成する方法について説明します。

アプリケーションの作成

Microsoft Entra ID ポータルで、ホームページの [エンタープライズアプリケーション (Enterprise Applications)] をクリックし、learn.microsoft.com の「[Configure Microsoft Entra SSO](#)」の手順に従います。

次の図は、SSO アプリケーション設定の一部を示しています。Microsoft Azure AD (SAML) レルムを設定する場合は、このページで一部の情報を指定する必要があります。詳細については、「[Microsoft Azure AD \(SAML\) レルムに必要な情報を取得する \(アクティブ認証のみ\) \(22 ページ\)](#)」を参照してください。

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

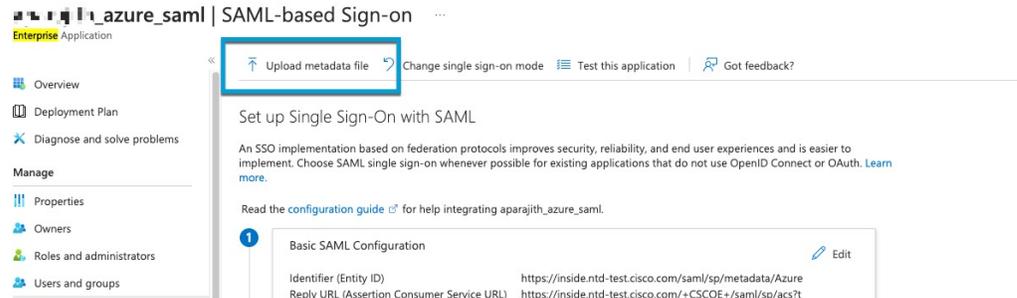
Read the [configuration guide](#) for help integrating `aparajith_azure_saml`.

1	Basic SAML Configuration Edit <table border="0"> <tr> <td>Identifier (Entity ID)</td> <td>https://[redacted]/saml/sp/metadata/Azure</td> </tr> <tr> <td>Reply URL (Assertion Consumer Service URL)</td> <td>https://[redacted]/v/+CSCOE+/saml/sp/acs?gname=[redacted]</td> </tr> <tr> <td>Sign on URL</td> <td>https://samltoolkit.azurewebsites.net/</td> </tr> <tr> <td>Relay State (Optional)</td> <td>Optional</td> </tr> <tr> <td>Logout URL (Optional)</td> <td>Optional</td> </tr> </table>	Identifier (Entity ID)	https://[redacted]/saml/sp/metadata/Azure	Reply URL (Assertion Consumer Service URL)	https://[redacted]/v/+CSCOE+/saml/sp/acs?gname=[redacted]	Sign on URL	https://samltoolkit.azurewebsites.net/	Relay State (Optional)	Optional	Logout URL (Optional)	Optional
Identifier (Entity ID)	https://[redacted]/saml/sp/metadata/Azure										
Reply URL (Assertion Consumer Service URL)	https://[redacted]/v/+CSCOE+/saml/sp/acs?gname=[redacted]										
Sign on URL	https://samltoolkit.azurewebsites.net/										
Relay State (Optional)	Optional										
Logout URL (Optional)	Optional										
2	Attributes & Claims Edit <table border="0"> <tr> <td>givenname</td> <td>user.givenname</td> </tr> <tr> <td>surname</td> <td>user.surname</td> </tr> <tr> <td>emailaddress</td> <td>user.mail</td> </tr> <tr> <td>name</td> <td>user.userprincipalname</td> </tr> <tr> <td>Unique User Identifier</td> <td>user.userprincipalname</td> </tr> </table>	givenname	user.givenname	surname	user.surname	emailaddress	user.mail	name	user.userprincipalname	Unique User Identifier	user.userprincipalname
givenname	user.givenname										
surname	user.surname										
emailaddress	user.mail										
name	user.userprincipalname										
Unique User Identifier	user.userprincipalname										
3	SAML Certificates Edit <table border="0"> <tr> <td>Token signing certificate</td> <td></td> </tr> <tr> <td>Status</td> <td>Active</td> </tr> <tr> <td>Thumbprint</td> <td>DE387[redacted]B5A7</td> </tr> <tr> <td>Expiration</td> <td>5/16/2025 12:04:26 AM</td> </tr> </table>	Token signing certificate		Status	Active	Thumbprint	DE387[redacted]B5A7	Expiration	5/16/2025 12:04:26 AM		
Token signing certificate											
Status	Active										
Thumbprint	DE387[redacted]B5A7										
Expiration	5/16/2025 12:04:26 AM										

(オプション) サービスプロバイダーのメタデータのアップロード

Microsoft Azure AD (SAML) レルムをすでに設定している場合は、ページの上にある [メタデータファイルのアップロード (Upload metadata file)] をクリックすれば、SSO アプリケーションの設定値を迅速に入力できます。

次の図は例を示しています。



SSO アプリケーションへのユーザーとグループの追加

learn.microsoft.com の「[Add a user account to an enterprise application](#)」の説明に従って、ユーザーとグループをアプリケーションに追加します。

次の作業

「[Microsoft Azure AD \(SAML\) レルムに必要な情報を取得する \(アクティブ認証のみ\)](#) (22 ページ)」を参照してください。

復号/再署名アクションを使用して複合ルールを作成する

この手順では、トラフィックが SAML レルムに到達する前に、トラフィックを復号して再署名する a decryption policy を作成する方法について説明します。レルムは、トラフィックが復号された後のみトラフィックを認証できます。

手順

- ステップ 1 まだ Secure Firewall Management Center にログインしていない場合は、ログインします。
- ステップ 2 「PKI」の説明に従って、TLS/SSL トラフィックを復号するための内部認証局オブジェクトを作成します (まだ作成していない場合)。
- ステップ 3 **Policies > Access Control heading > Decryption** をクリックします。
- ステップ 4 [新しいポリシー (New Policy)] をクリックします。
- ステップ 5 ポリシーの [名前 (Name)] を入力し、[デフォルトのアクション (Default Action)] を選択します。デフォルトのアクションについては、[復号ポリシーのデフォルトアクション](#)を参照してください。
- ステップ 6 [保存 (Save)] をクリックします。
- ステップ 7 [ルールの追加 (Add Rule)] をクリックします。

- ステップ 8 ルールの [名前 (Name)] を入力します。
- ステップ 9 [アクション (Action)] 一覧から、[復号-再署名 (Decrypt - Resign)] を選択します。
- ステップ 10 [含める (With)] リストから、サービスプロバイダーの証明書オブジェクトを選択します。
- ステップ 11 [アプリケーション (Applications)] タブページをクリックします。
- ステップ 12 [使用可能なアプリケーション (Available Applications)] セクションで、検索フィールドに **Azure Authentication Service** と入力します。
- ステップ 13 [Azure認証 (Azure Authentication)] をクリックし、[ルールに追加 (Add to Rule)] をクリックします。
- 次の図は例を示しています。

- ステップ 14 (オプション) **復号ルール条件**の説明に従って、他のオプションを設定します。
- ステップ 15 [追加 (Add)] をクリックします。
- ステップ 16 ページの上部にある [保存 (Save)] をクリックします。

次のタスク

Microsoft Azure AD (SAML) レルムに必要な情報を取得する (アクティブ認証のみ)

このタスクでは、Firewall Management Center で Microsoft Azure AD (SAML) レルム (現在名: *Entra ID*) の設定に必要な情報を収集する方法を説明します。

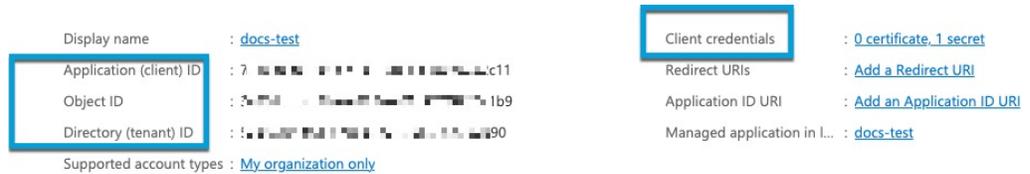
手順

- ステップ 1 少なくとも製品デザイナー (Product Designer) ロールを持つユーザーとして <https://portal.azure.com/> にログインします。
- ステップ 2 ページの上部で、[Microsoft Entra ID] をクリックします。

ステップ 3 左側の列で、[アプリの登録 (App Registrations)] をクリックします。

ステップ 4 必要に応じて、表示されたアプリのリストをフィルタ処理して、使用するアプリを表示します。

ステップ 5 アプリの名前をクリックします。



ステップ 6 このページの次の値の横にある **Copy** (📄) をクリックし、それらの値をテキストファイルに貼り付けます。

- [Application (Client) ID]
- ディレクトリ (テナント) ID

ステップ 7 [クライアントのログイン情報 (Client Credentials)] をクリックします。

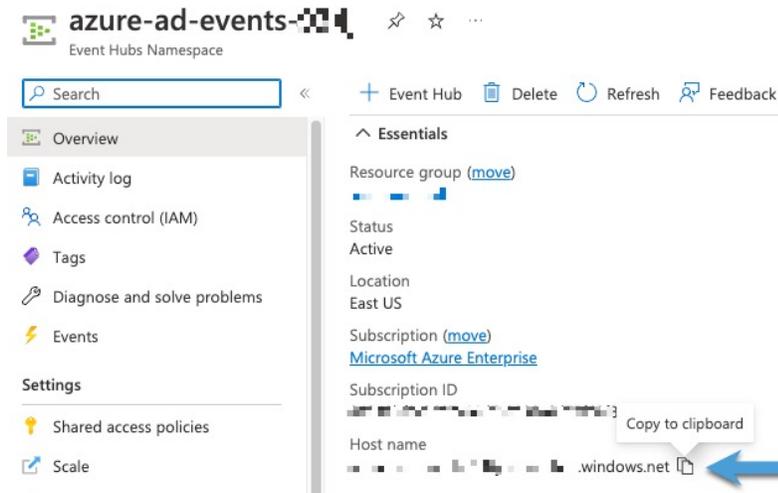
ステップ 8 クライアントシークレット値 (クライアントシークレット IDではありません) がすでにわかっている場合を除き、次のように新しいクライアントシークレットを作成する必要があります。

- [新しいクライアントシークレット (New Client Secret)] をクリックします。
- 表示されたフィールドに必要な情報を入力します。
- [Add] をクリックします。
- 次の図に示すように、[値 (Value)] の横にある **Copy** (📄) をクリックします。

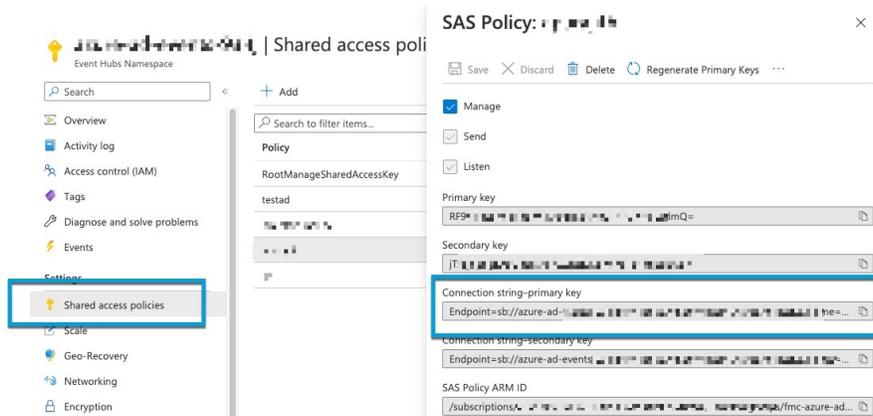


ステップ 9 <https://portal.azure.com/> から、[(イベントハブの名前) (Event Hubs)] > の順にクリックします。

ステップ 10 右側のペインで、[ホスト名 (Host name)] の値の横にある **Copy** (📄) をクリックして値をクリップボードに貼り付けます。これは、イベントハブホスト名です。

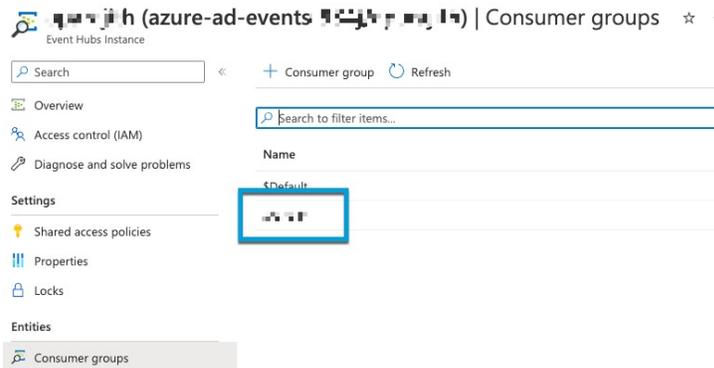


- ステップ 11** イベントハブの名前を書き留めるか、テキストファイルにコピーします (ページの上部にある [Event Hubs名前空間 (Event Hubs Namespace)] と同じ)。
- ステップ 12** 左側のペインの [設定 (Settings)] で、[共有アクセスポリシー (Shared access policies)] をクリックします。
- ステップ 13** ポリシーの名前をクリックします。
- ステップ 14** [接続文字列-主キー (Connection string-primary key)] の横にある **Copy** (📄) をクリックします。



- ステップ 15** [概要 (Overview)] > [エンティティ (Entities)] > [イベントハブ (Event Hubs)] > (イベントハブの名前) > [エンティティ (Entities)] > [コンシューマグループ (Consumer Groups)] の順にクリックします。

次の値を書き留めるか、クリップボードにコピーします。これは、コンシューマグループ名です。



ステップ 16 左側のペインで [概要 (Overview)] をクリックします。

ステップ 17 [名前空間 (Namespace)] の横にある **Copy** (📄) をクリックします。



これは、イベントハブトピック名です。

ステップ 18 ホームページに戻り、必要に応じてログインします：<https://portal.azure.com/#home>。

ステップ 19 [Microsoft Entra ID] をクリックします。

ステップ 20 左側のペインで [エンタープライズアプリケーション (Enterprise Applications)] をクリックします。

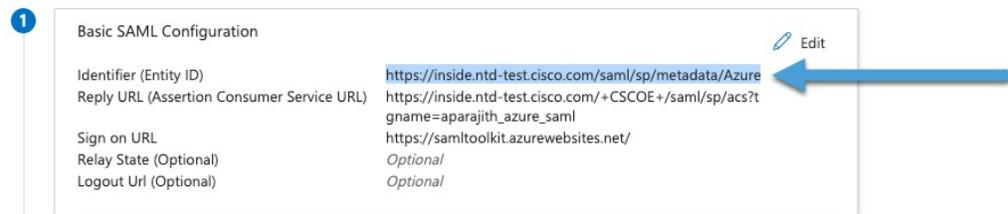
ステップ 21 必要に応じて、アプリケーションのリストをフィルタリングして、該当するアプリケーションを見つけます。

ステップ 22 エンタープライズアプリケーションの名前をクリックします。

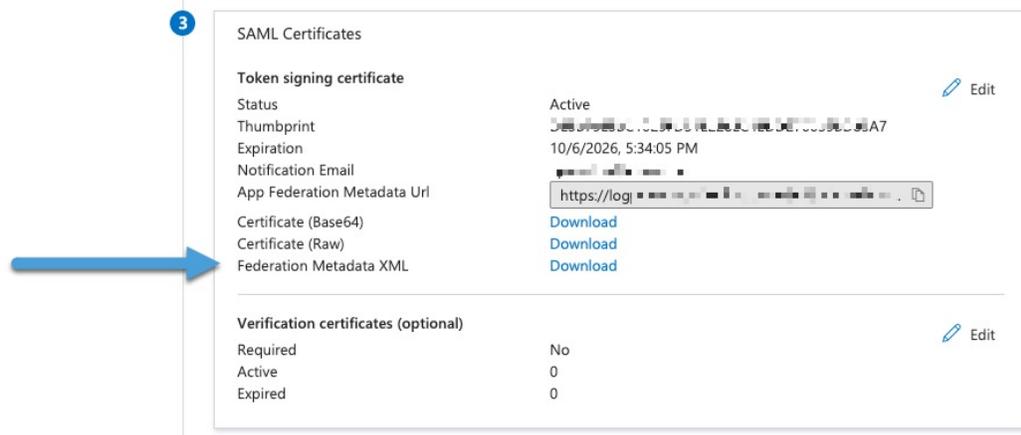
ステップ 23 [シングルサインオンの設定 (Set up single sign on)] で [始める (Get Started)] をクリックします。

ステップ 24 SSO アプリケーションページで、[識別子 (エンティティ ID) (Identifier (Entity ID))] の値をクリップボードにコピーします。

次の図は例を示しています。

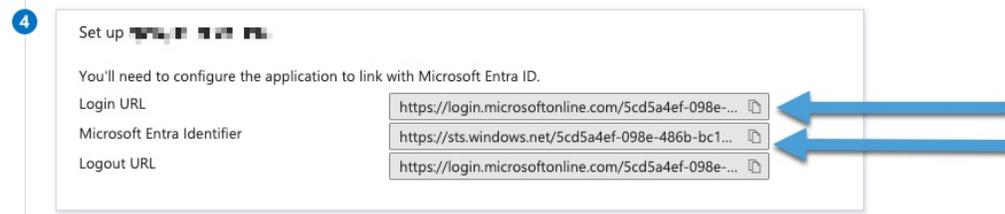


- ステップ 25** SSO アプリケーションページで、次の図に示すように、[フェデレーションメタデータXML (Federation Metadata XML)] の横にある [ダウンロード (Download)] リンクをクリックします。
次の図は例を示しています。



- ステップ 26** SSO アプリケーションをすでに設定している場合は、ここで終了できます。フェデレーションメタデータ XML には、Secure Firewall Management Center でアイデンティティプロバイダーを設定するために必要なすべての情報が含まれています。

- ステップ 27** (すでにフェデレーション XML をダウンロードしている場合は任意)。次の両方の値の横にある **Copy** (📄) をクリックし、テキストファイルに保存します。
次の図は例を示しています。



次のタスク

「復号/再署名アクションを使用して複合ルールを作成する (21 ページ)」を参照してください。

Microsoft Azure AD (SAML) realm for active authentication (captive portal) の作成

次のトピックでは、アクティブな認証用の Microsoft Azure AD (SAML) レalm (現在名: *Entra ID*) の作成に必要な複数手順のウィザードを実行する方法について説明します。

キャプティブポータルとも呼ばれるアクティブな認証では、Microsoft Entra ID はユーザーストアです。ユーザーがアクセス制御ルールで定義されている保護されたリソースにアクセスしようとする場合、そのユーザーは最初に Microsoft Entra ID で認証する必要があります。

レルムを設定するには、次の順序ですべてのタスクを実行します。

1. [Entra ID の基本設定を構成する \(8 ページ\)](#)。
2. [Entra ID でシングルサインオン \(SSO\) アプリケーションを構成する \(20 ページ\)](#)。
3. [Microsoft Azure AD \(SAML\) レルムに必要な情報を取得する \(アクティブ認証のみ\) \(22 ページ\)](#)

Microsoft Azure AD (SAML) レルム : SAML の詳細

このタスクでは、Microsoft Azure AD (SAML) レルムを作成する複数ステップのウィザードの最初のステップについて説明します。レルムを設定するには、ウィザードのすべてのステップを完了する必要があります。手順は、アクティブ認証用のレルムを作成するか、パッシブ認証用のレルムを作成するかによって異なります。

始める前に

レルムを作成する前に、次のタスクをすべて実行します。

- (Cisco ISE によるパッシブ認証のみ) ユーザーおよびグループのリポジトリとして Cisco ISE を使用している場合は、ISE を設定します。
 - [リソース独自のパスワードログイン情報を使用する Entra ID と Cisco ISE について \(4 ページ\)](#)
 - [TEAP/EAP-TLS を使用する Entra ID と Cisco ISE について \(5 ページ\)](#)
- Entra ID をユーザーとグループのリポジトリとして使用するには、「[パッシブ認証用の Microsoft Entra ID を構成する \(7 ページ\)](#)」を参照してください。
- 「[Microsoft Azure AD \(SAML\) レルムに必要な情報を取得する \(9 ページ\)](#)」で説明されている、レルムに必要な情報を取得します。

手順

-
- ステップ 1 Secure Firewall Management Center にログインします。
 - ステップ 2 **Integration > Other Integrations > Realms > Realms** をクリックします。
 - ステップ 3 [レルムを追加 (Add Realm)] > [SAML - Azure AD] をクリックします。
 - ステップ 4 次の情報を入力します。

項目	説明
名前 (Name)	レルムを識別する一意の名前。
説明	(オプション) レルムの説明。

項目	説明
アイデンティティ プロバイダー	常に [Azure AD] が表示されます。
設定の種類	次のいずれかをクリックします。 <ul style="list-style-type: none"> パッシブ認証の場合は、[ISEによるパッシブ認証 (Passive authentication with ISE)]。 パッシブ認証またはアクティブ認証 (つまり、キャプティブポータル) のユーザーストアとして Entra ID を使用するための Azure AD を使用するパッシブ認証またはキャプティブポータル

ステップ 5 [次へ (Next)] をクリックします。

次のタスク

次のいずれかです。

- パッシブ認証 : 「[Microsoft Azure AD \(SAML\) レルム : Azure AD の詳細 \(14 ページ\)](#)」。
- アクティブ認証 : 「[Microsoft Azure AD \(SAML\) レルム : SAML サービスプロバイダー \(SP\) のメタデータ \(28 ページ\)](#)」。

Microsoft Azure AD (SAML) レルム : SAML サービスプロバイダー (SP) のメタデータ

このタスクでは、Microsoft Azure AD (SAML) レルムを作成できる複数ページのウィザードの 1 ページについて説明しました。

始める前に

「[Microsoft Azure AD \(SAML\) レルム : SAML の詳細 \(12 ページ\)](#)」で説明されているタスクを完了する

手順

ステップ 1 [Microsoft Azure AD \(SAML\) レルム : SAML の詳細 \(12 ページ\)](#) から続行します。

ステップ 2 次の情報を入力します。

項目	説明
[ベース URL (Base URL)]	リストから、前に作成したネットワークオブジェクトをクリックします。ネットワークユーザーは、保護されたネットワークリソースにアクセスしようとする、この URL に誘導されます。 Add (+) をクリックして、ここでオブジェクトを作成することもできます。
Entity ID	SSO アプリケーションのエンティティ ID。
[Assertion Consumer Service (ASA) の URL (Assertion Consumer Services (ACS) URL)]	上記の値から自動的に生成されます。
[サービスプロバイダー証明書 (Service Provider Certificate)]	リストから、Secure Firewall Threat Defense への要求の復号に使用する証明書をクリックします。 Add (+) をクリックして、ここでオブジェクトを作成することもできます。
[サービスプロバイダーのメタデータのダウンロード (Download Service Provider Metadata)]	(オプション) サービスプロバイダー (つまり、管理対象デバイス) に関連付けられているメタデータをダウンロードして、Microsoft Entra ID SSO アプリケーションの設定を簡素化します。

ステップ 3 [次へ (Next)] をクリックします。

次のタスク

[Microsoft Azure AD \(SAML\) レルム : SAML アイデンティティ プロバイダー \(IdP\) メタデータ \(29 ページ\)](#) 。

Microsoft Azure AD (SAML) レルム : SAML アイデンティティ プロバイダー (IdP) メタデータ

このタスクでは、Microsoft Azure AD (SAML) レルムを作成できる複数ページのウィザードの 1 ページについて説明しました。

始める前に

「[Microsoft Azure AD \(SAML\) レルム : SAML サービスプロバイダー \(SP\) のメタデータ \(28 ページ\)](#)」で説明されているタスクを完了します。

手順

- ステップ 1** [Microsoft Azure AD \(SAML\) レルム : SAML サービスプロバイダー \(SP\) のメタデータ \(28 ページ\)](#) から続行します。
- ステップ 2** Entra ID SSO アプリケーションのフェデレーション XML を以前にダウンロードしている場合は、[\[XMLをアップロード \(Upload XML\)\]](#) をクリックして、アップロードします。その後、次の手順をスキップできます。
- ステップ 3** 次の情報を入力します。

項目	説明
Entity ID	アイデンティティ プロバイダーのエンティティ ID を入力します。
[シングルサインオン (SSO) URL (Single Sign on (SSO) URL)]	アプリケーションの SSO URL を入力します。
[IdP証明書 (IdP Certificate)]	リストで、Microsoft Entra ID 認証に使用する証明書をクリックします。 Add (+) をクリックして、ここでオブジェクトを作成することもできます。

- ステップ 4** [\[次へ \(Next\)\]](#) をクリックします。

次のタスク

[Microsoft Azure AD \(SAML\) レルム : SAML の詳細 \(12 ページ\)](#)。

Microsoft Azure AD (SAML) レルム : Azure AD の詳細

このタスクでは、Microsoft Azure AD (SAML) レルムを作成できる複数ページのウィザードの 1 ページについて説明しました。

手順

- ステップ 1** ウィザードの前の手順から続行します。
- ステップ 2** 次の情報を入力します。

項目	説明
名前 (Name)	このレルムを識別するための一意の名前を入力します。

項目	説明
クライアントのシークレット (Client Secret)	以下で説明されている、取得済みの情報を入力します。 <ul style="list-style-type: none"> パッシブ認証 : 「パッシブ認証向け Microsoft Azure AD (SAML)を作成する方法 (3 ページ)」 アクティブ認証 : 「Microsoft Azure AD (SAML) レルムに必要な情報を取得する (アクティブ認証のみ) (22 ページ)」
テナント ID	
イベントハブホスト名 (Event Hubs Host Name)	
イベントハブ名 (Event Hub Name)	
イベントハブ接続文字列 (Event Hub Connection String)	
(任意) ユーザ グループ	Slider enabled () にスライドして、ポリシーに含めるグループまたはポリシーから除外するグループを指定します。
(任意) 除外するユーザーグループ (Excluded User Groups)	このフィールドに1つ以上のグループ名を入力した場合は、それ以外のすべてのグループとそれらのグループに含まれるユーザーがダウンロードされ、ユーザー認識やユーザー制御に利用できます。 1行に1つのグループ名を入力し、その後に改行します。グループ名では大文字と小文字が区別されます。
(オプション) 含めるユーザーグループ (Included User Groups)	このフィールドに1つ以上のグループ名を入力した場合は、それらのグループとそれらのグループに含まれるユーザーだけがダウンロードされ、ユーザーデータはユーザー認識やユーザー制御に利用できます。 1行に1つのグループ名を入力し、その後に改行します。グループ名では大文字と小文字が区別されます。

ステップ 3 [テスト (Test)] をクリックします。
 次の手順に進む前に、テスト接続が成功することを確認します。

ステップ 4 [次へ (Next)] をクリックします。

Microsoft Azure AD (SAML) レルム : ユーザー セッション タイムアウト

このタスクでは、Microsoft Azure AD (SAML) レルムを作成できる複数ページのウィザードの1ページについて説明しました。

このオプションでは、非アクティブなセッションがシステムによって終了されるまでの秒数を設定します。

手順

ステップ 1 ウィザードの前の手順から続行します。

ステップ 2 次の情報を入力します。

項目	説明
ISE ユーザー	デフォルト値は 1440 分 (24 時間) です。
キャプティブポータルユーザー	デフォルト値は 1440 分 (24 時間) です。

このタイムアウトを過ぎると、ユーザーのセッションは終了します。ユーザーが再度ログインせずにネットワークにアクセスし続けている場合、ユーザーは Firewall Management Center により不明として認識されます ([失敗したキャプティブポータルユーザー (Failed Captive Portal Users)] を除く)。

ステップ 3 [Save (保存)] をクリックします。

LDAP レルムまたは Active Directory (AD) レルムおよびレルムディレクトリを作成する

レルムなしで ISE/ISE-PIC を設定する場合は、Secure Firewall Management Center でのユーザーの表示方法に影響するユーザーセッションタイムアウトがあることに注意してください。詳細については、[\[レルム \(Realm\)\] フィールド \(45 ページ\)](#) を参照してください。

次の手順では、レルム (Firewall Management Center と Active Directory レルム間の接続) とディレクトリ (Firewall Management Center と LDAP サーバーまたは Active Directory ドメインコントローラ間の接続) を作成できます。

(推奨) Firewall Management Center から Active Directory サーバーに安全に接続するには、まず次のタスクを実行します。

- [Active Directory \(AD\) サーバーのルート証明書をエクスポートする \(53 ページ\)](#)
- [Active Directory \(AD\) サーバーの名前を検索する \(53 ページ\)](#)

Microsoft 社は、2020 年に Active Directory サーバーで LDAP バインディングと LDAP 署名の適用を開始すると発表しました。Microsoft 社がこれらを要件にするのは、デフォルト設定で Microsoft Windows を使用する場合に権限昇格の脆弱性が存在するため、中間者攻撃者が認証要求を Windows LDAP サーバーに正常に転送できる可能性があるからです。詳細については、Microsoft 社のサポートサイトで「[2020 LDAP channel binding and LDAP signing requirement for Windows](#)」を参照してください。

レalmおよびディレクトリの設定フィールドに関する詳細については、[\[レalm \(Realm\) \] フィールド \(45 ページ\)](#) と [レalmディレクトリと同期フィールド \(49 ページ\)](#) を参照してください。

クロスドメイン信頼を使用してレalmを設定する段階的手順の例については、[クロスドメイン信頼に対して Firewall Management Center を構成する：手順 \(58 ページ\)](#) を参照してください。

Active Directory グローバルカタログサーバーは、レalmディレクトリとしてサポートされていません。グローバルカタログサーバーの詳細については、[learn.microsoft.com](#) の「[Global Catalog](#)」を参照してください。



- (注) すべての Microsoft Active Directory (AD) レalmに固有の [ADプライマリドメイン (AD Primary Domain)] を指定する必要があります。異なる Microsoft AD レalmに同じ [ADプライマリドメイン (AD Primary Domain)] を指定することはできますが、システムが適切に機能しなくなります。これは、システムにより各レalm内のすべてのユーザーとグループに 1 つの固有 ID が割り当てられるためです。そのため、システムは特定のユーザーまたはグループを明確に識別することができません。ユーザーとグループが適切に識別されないため、同じ [ADプライマリドメイン (AD Primary Domain)] を使用して複数のレalmを指定することはできません。これは、システムが一意的 ID を各レalmのすべてのユーザーとグループに割り当てるために発生します。そのため、システムは特定のユーザーまたはグループを明確に識別できません。

レalmなしで ISE/ISE-PIC を設定する場合は、Secure Firewall Management Centerでのユーザーの表示方法に影響するユーザーセッションタイムアウトがあることに注意してください。詳細については、[\[レalm \(Realm\) \] フィールド \(45 ページ\)](#) を参照してください。

始める前に

キャプティブポータルに Kerberos 認証を使用している場合は、開始する前に次のセクションを参照してください：[Kerberos 認証の前提条件 \(44 ページ\)](#)。

変更管理を有効にした場合は、レalmを作成する前に、次の各オブジェクトのチケットを開くか、編集、割り当て、および承認する必要があります。

- Microsoft AD または LDAP に安全に接続している場合は、サーバーの信頼された証明機関
- レalm自体

詳細については、「[設定変更のためのチケットのオープン](#)」および「[変更管理をサポートするポリシーとオブジェクト](#)」を参照してください。



重要 Secure Firewall Management Center と Active Directory ドメインコントローラ間の遅延を削減するには、地理的に Secure Firewall Management Center にできるだけ近いレalmディレクトリ（つまり、ドメインコントローラ）を構成することを強くお勧めします。

たとえば、Secure Firewall Management Center が北米にある場合は、同様に北米にあるレalmディレクトリを構成します。このように構成しないと、ユーザーやグループのダウンロードがタイムアウトするなどの問題が発生する可能性があります。

手順

- ステップ 1 Secure Firewall Management Center にログインします。
- ステップ 2 **Integration > Other Integrations > Realms > Realms** をクリックします。
- ステップ 3 新しいレalmを作成するには、[レalmの追加 (Add Realm)] ドロップダウンリストから選択します。
- ステップ 4 その他のタスク（レalmの有効化、無効化、削除など）を実行する場合は、[レalmを管理する \(67 ページ\)](#) を参照してください。
- ステップ 5 [レalm (Realm)] フィールド ([45 ページ](#)) で説明したように、レalm情報を入力します。
- ステップ 6 [ディレクトリサーバー設定 (Directory Server Configuration)] セクションで、[レalmディレクトリと同期フィールド \(49 ページ\)](#) の説明に従ってディレクトリを入力します。
- ステップ 7 (オプション) このレalmに別のドメインを設定するには、[Add another directory] をクリックします。
- ステップ 8 [Configure Groups and Users] をクリックします。
次の情報を入力します。

[Information]	説明
AD Primary Domain	<p>ユーザー認証が必要となる Active Directory サーバーのドメインです。詳細については、[レalm (Realm)] フィールド (45 ページ) を参照してください。</p> <p>ドメインの代替ユーザープリンシパル名 (UPN) サフィックスではなく、ドメインの元のドメイン名を使用してレalmを作成する必要があります。そうしない場合、ユーザーとグループはダウンロードに失敗し、アイデンティティポリシーは適用されません。たとえば、元のドメインが domain.example.com で、代替の UPN 名が domain2.mydomain.com の場合は、domain.example.com を使用するようレalmを設定する必要があります。代替の UPN サフィックスの設定の詳細については、learn.microsoft.com の「Configuring Alternate Login ID」などのリソースを参照してください。</p>
ベース DN (Base DN)	Firewall Management Center がユーザー データの検索を開始するサーバーのディレクトリ ツリー。

[Information]	説明
Group DN	Firewall Management Center がグループデータの検索を開始するサーバーのディレクトリツリー。
[Load Groups]	<p>クリックして、Active Directory サーバーからグループをロードします。グループが表示されない場合は、[AD Primary Domain]、[Base DN]、および[Group DN]フィールドに情報を入力するか、または情報を編集して、[Load Groups] をクリックします。</p> <p>これらのフィールドの詳細については、[レalm (Realm)] フィールド (45 ページ) を参照してください。</p>
[Available Groups] セクション	<p>[含めるグループとユーザー (Included Groups and Users)] または [除外するグループとユーザー (Excluded Groups and Users)] リストにグループを移動して、ポリシーで使用するグループを制限します。</p> <p>たとえば、1つのグループを [含めるグループとユーザー (Included Groups and Users)] リストに移動すると、そのグループのみポリシーで使用し、他のグループはすべて除外できます。</p> <p>[除外するグループとユーザー (Excluded Groups and Users)] のグループ、およびそれらに含まれるユーザーは、ユーザー認識と制御から除外されます。他のすべてのグループとユーザーは利用できます。</p> <p>詳細については、レalmディレクトリと同期フィールド (49 ページ) を参照してください。</p>

- ステップ 9** [レalm設定 (Realm Configuration)] タブをクリックします。
- ステップ 10** [Group Attribute] を入力し、(キャプティブポータルにケルベロス認証を使用する場合) [AD Join Username] と [AD Join Password] を入力します。詳細については、[レalmディレクトリと同期フィールド \(49 ページ\)](#) を参照してください。
- ステップ 11** Kerberos 認証を使用する場合は、[テスト (Test)] をクリックします。テストが失敗した場合は、少し待ってから再試行してください。
- ステップ 12** [ISE/ISE-PICユーザー (ISE/ISE-PIC Users)]、[ターミナルサーバーエージェントユーザー (Terminal Server Agent Users)]、[キャプティブポータルユーザー (Captive Portal Users)]、[失敗したキャプティブポータルユーザー (Failed Captive Portal Users)]、および[ゲストキャプティブポータルユーザー (Guest Captive Portal Users)] のユーザーセッションタイムアウト値を分単位で入力します。
- ステップ 13** レalmの設定が完了したら、[Save] をクリックします。

次のタスク

- [クロスドメイン信頼に対して Firewall Management Center を構成する : 手順 \(58 ページ\)](#)
- [ユーザーとグループを同期する \(56 ページ\)](#)

- レールムの編集、削除、有効化、または無効化を行います。 [レールムを管理する \(67ページ\)](#) を参照してください
- [レールムを比較する \(67ページ\)](#)。
- 必要に応じて、タスクのステータスをモニターします。 [Cisco Secure Firewall Management Center Administration Guide](#) の「[Viewing Task Messages](#)」を参照してください。

レールムとレールムシーケンスについて

レールムとは、Secure Firewall Management Center とモニタリング対象のサーバー上にあるユーザーアカウントの間の接続です。レールムでは、サーバーの接続設定と認証フィルタの設定を指定します。レールムでは次のことを実行できます。

- アクティビティをモニターするユーザーとユーザーグループを指定する。
- 権限のあるユーザー、および権限のない一部のユーザー（トラフィックベースの検出で検出されたPOP3およびIMAPユーザー、およびトラフィックベースの検出、TS エージェント、ISE/ISE-PICによって検出されたユーザー）のユーザーメタデータについてユーザーリポジトリをクエリする。

(*Microsoft AD* レールムのみ)。レールムシーケンスは、アイデンティティポリシーで使用する2つ以上のActive Directory レールムの順序付きリストです。レールムシーケンスをアイデンティティルールに関連付けると、レールムシーケンスで指定されている順序で、最初から最後までActive Directory ドメインが検索されます。

レールム内のディレクトリとして複数のドメインコントローラを追加できますが、同じ基本レールム情報を共有する必要があります。レールム内のディレクトリは、LDAP サーバのみ、またはActive Directory (AD) サーバのみである必要があります。レールムを有効にすると、保存された変更は次回Secure Firewall Management Centerがサーバーに照会するときに適用されます。

ユーザ認識を行うには、[サポートされるすべてのサーバタイプ](#)のレールムを設定する必要があります。システムは、これらの接続を使用して、POP3 および IMAP ユーザーに関連するデータについてサーバーにクエリし、トラフィックベースの検出で検出されたLDAP ユーザーに関するデータを収集します。

システムは、POP3 および IMAP ログイン内の電子メールアドレスを使用して、Active Directory、Microsoft Azure Active Directory、またはOpenLDAP 上のLDAP ユーザーに関連付けます。たとえば、LDAP ユーザーと電子メールアドレスが同じユーザーのPOP3 ログインを管理対象デバイスが検出すると、システムはLDAP ユーザーのメタデータをそのユーザーに関連付けます。

ユーザー制御を実行するために以下のいずれかを設定できます。

- Active Directory、Microsoft Azure Active Directory、サーバー、またはISE/ISE-PIC のレールムまたはレールムシーケンス



(注) SGT ISE 属性条件を設定する予定で、ユーザー、グループ、レールム、エンドポイントロケーション、エンドポイントプロファイルの条件を設定する予定はない場合、または ID ポリシーのみを使用してネットワークトラフィックをフィルタ処理する場合、Microsoft AD レールムやレールムシーケンスの設定は任意です。

レールムシーケンスは、Microsoft Azure AD レールムでは使用できません。

- TS エージェント用の Microsoft AD サーバーのレールムまたはレールムシーケンス。
- キャプティブポータルの場合は、LDAP レールム。
LDAP 用のレールムシーケンスはサポートされていません。

未定の ネストできます。Secure Firewall Management Center はそれらのグループとグループに含まれるユーザーをダウンロードします。LDAP レールムまたは [Active Directory \(AD\) レールム](#) および [レールムディレクトリを作成する \(32 ページ\)](#) の説明に従い、必要に応じて、ダウンロードするグループとユーザーを制限できます。

ユーザーの同期について

次のような特定の検出されたユーザーに関して、ユーザーとユーザーグループのメタデータを取得するために、Firewall Management Center と LDAP サーバーまたは Microsoft AD サーバー間の接続を確立するためのレールムまたはレールムシーケンスを設定できます。

- キャプティブポータルで認証されたか、または ISE/ISE-PIC で報告された LDAP および Microsoft AD のユーザー。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出で検出された POP3 と IMAP ユーザー ログイン (ユーザーが LDAP または AD ユーザーと同じ電子メールアドレスを持つ場合)。このメタデータは、ユーザ認識に使用できます。

Firewall Management Center は、ユーザーごとに次の情報とメタデータを取得します。

- LDAP ユーザー名
- 姓と名
- 電子メールアドレス (Email address)
- 部署名 (Department)
- 電話番号 (Telephone number)



重要 Secure Firewall Management Center と Active Directory ドメインコントローラ間の遅延を削減するには、地理的に Secure Firewall Management Center にできるだけ近いレルムディレクトリ（つまり、ドメインコントローラ）を構成することを強くお勧めします。

たとえば、Secure Firewall Management Center が北米にある場合は、同様に北米にあるレルムディレクトリを構成します。このように構成しないと、ユーザーやグループのダウンロードがタイムアウトするなどの問題が発生する可能性があります。

ユーザアクティビティ データについて

ユーザアクティビティ データはユーザアクティビティ データベースに保存され、ユーザのアイデンティティ データはユーザ データベースに保存されます。アクセス制御で保存できる使用可能なユーザーの最大数は Firewall Management Center モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス制御パラメータの範囲が広すぎる場合、Firewall Management Center はできるだけ多くのユーザーに関する情報を取得し、取得できなかったユーザーの数をメッセージセンターの [タスク (Tasks)] タブ ページで報告します。

オプションで、管理対象デバイスがユーザー認識データを監視するサブネットを制限するには、[Cisco Secure Firewall Threat Defense Command Reference](#) で説明されている **configure identity-subnet-filter** コマンドを使用できます。



(注) ユーザー リポジトリからシステムによって検出されたユーザーを削除しても、Firewall Management Center はユーザー データベースからそのユーザーを削除しません。そのため、手で削除する必要があります。ただし、LDAP に対する変更は、次に権限のあるユーザーのリストを Firewall Management Center が更新したときにアクセス 制御ルールに反映されます。

レルムおよび信頼できるドメイン

Firewall Management Center で Microsoft Active Directory (AD) レルムを構成すると、Microsoft Active Directory または LDAP ドメインに関連付けられます。

互いに信頼する Microsoft Active Directory (AD) ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザー アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。



(注) 信頼できるドメインは、Microsoft Active Directory ドメインにのみ適用されます。Microsoft Azure Active Directory または LDAP ドメインには適用されません。

システムと信頼できるドメイン

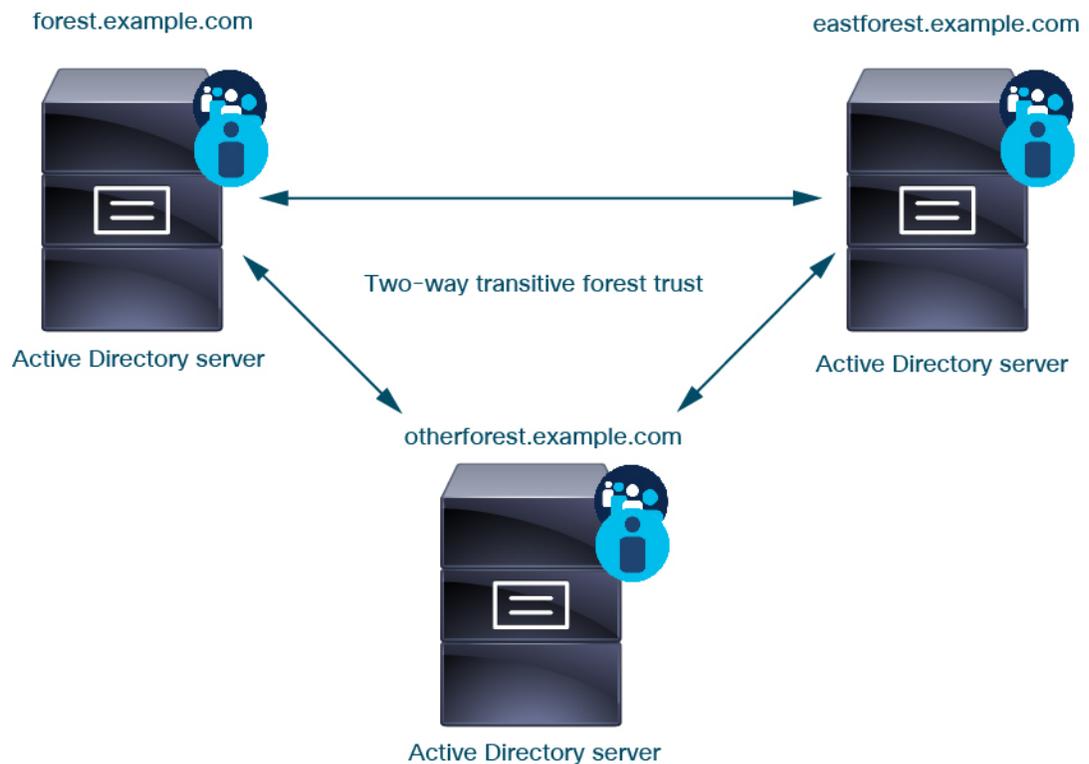
システムは、信頼関係で設定されている AD フォレストをサポートします。信頼関係にはいくつかのタイプがあります。このガイドでは、双方向の推移的なフォレストの信頼関係について説明します。次の簡単な例は、2つのフォレストを示しています。**forest.example.com** と **eastforest.example.com** 各フォレスト内のユーザーとグループは、他のフォレスト内の AD によって認証されます（フォレストをそのように設定している場合）。

ドメインごとに1つのレルムとドメインコントローラごとに1つのディレクトリを使用して設定したシステムでは、最大 100,000 の外部セキュリティプリンシパル（ユーザーとグループ）を検出できます。これらの外部セキュリティプリンシパルが別のレルムでダウンロードされたユーザーと一致する場合は、アクセスコントロールポリシーで使用できます。

アクセスコントロールポリシーで使用するユーザーが存在しないドメインには、レルムを設定する必要はありません。

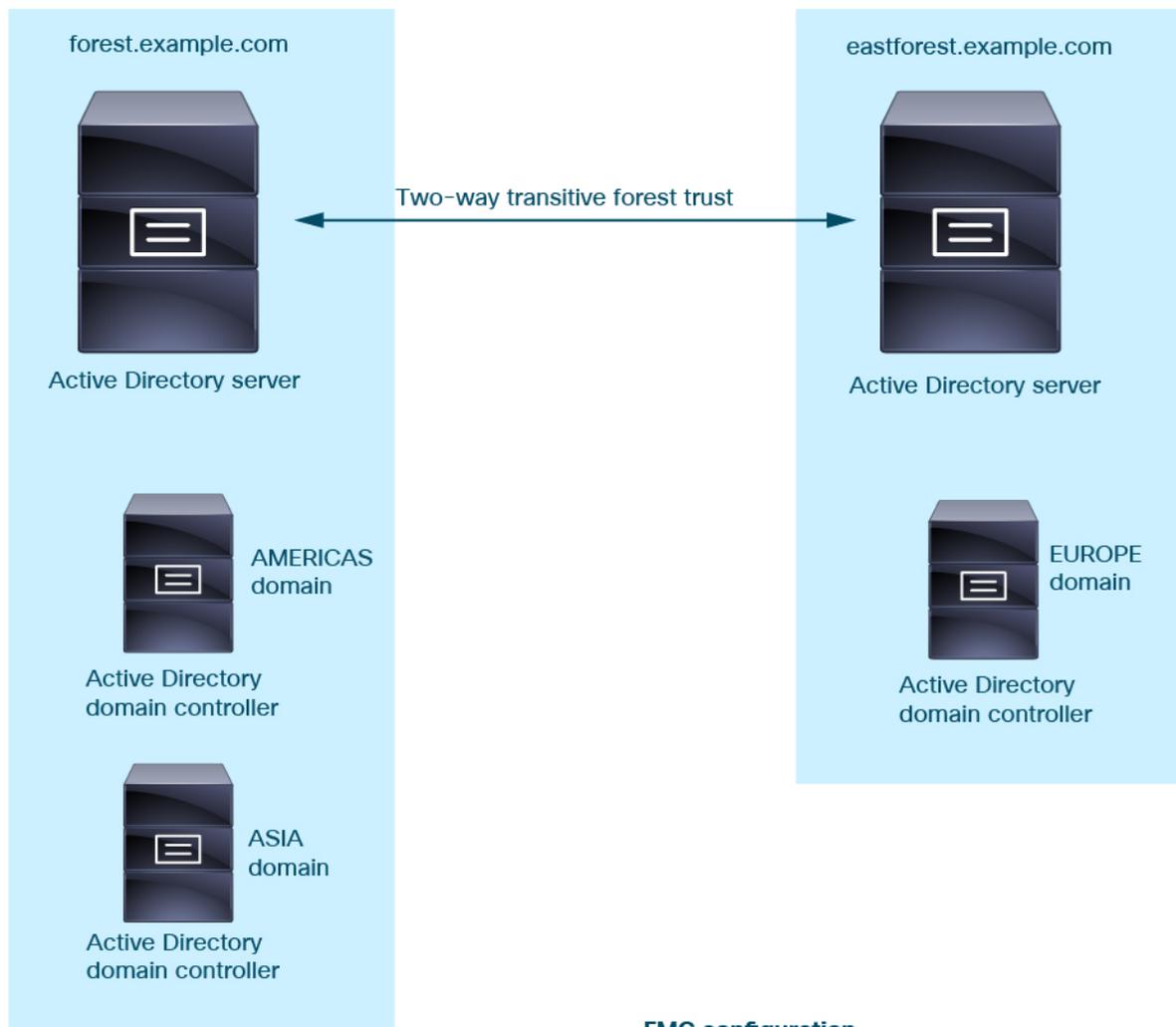


この例を続けるために、3つの AD フォレスト（1つはサブドメインまたは独立したフォレスト）があり、すべてが双方向の推移的なフォレストの関係として設定されていて、すべてのユーザーとグループが3つすべてのフォレストとシステムで使用可能だとします。（前述の例のように、3つすべての AD ドメインをレルムとして設定し、すべてのドメインコントローラをそれらのレルムのディレクトリとして設定する必要があります）。



最後に、双方向の推移的なフォレストの信頼関係を持つ2フォレストシステムのユーザーとグループにIDポリシーを適用できるように Firewall Management Center を設定することが可能です。各フォレストに少なくとも1つのドメインコントローラがあり、それぞれが異なるユーザーとグループを認証するとします。Firewall Management Center がこれらのユーザーとグループにIDポリシーを適用できるようにするには、関連するユーザーを含む各ドメインを Firewall Management Center レルムとして、また各ドメインコントローラをそれぞれのレルムの Firewall Management Center ディレクトリとして設定する必要があります。

Firewall Management Center を正しく設定しないと、一部のユーザーとグループがポリシーで使用できなくなります。この場合、ユーザーとグループの同期を試みると警告が表示されます。



FMC configuration



Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com

Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

前述の例を使用して、Firewall Management Center を次のように設定します。

- アクセスコントロールポリシーで制御するユーザーを含む **forest.example.com** のドメインのレルム
 - **AMERICAS.forest.example.com** のレルム内のディレクトリ
 - **ASIA.forest.example.com** のレルム内のディレクトリ
- アクセスコントロールポリシーで制御するユーザーを含む **eastforest.example.com** のドメインのレルム

- EUROPE.eastforest.example.com のレルム内のディレクトリ



- (注) Firewall Management Center は AD フィールド **msDS-PrincipalName** を使用して参照を解決し、各ドメインコントローラでユーザー名とグループ名を検索します。**msDS-PrincipalName** は NetBIOS 名を返します。

レルム向けにサポートされているサーバー

レルムを設定して次のサーバータイプに接続すると、Firewall Management Centerからの TCP/IP アクセスを提供できます。

サーバータイプ (Server Type)	ISE/ISE-PIC によるデータ取得のサポート	TS エージェントによるデータ取得のサポート	キャプティブポータルによるデータ取得のサポート
Windows Server 2012、2016、および 2019 上の Microsoft Active Directory	はい	はい	はい
Microsoft Azure AD	はい	いいえ	非対応
Linux 上の OpenLDAP	いいえ	非対応	○

Active Directory グローバルカタログサーバーは、レルムディレクトリとしてサポートされていません。グローバルカタログサーバーの詳細については、learn.microsoft.com の「[Global Catalog](#)」を参照してください。



- (注) TS エージェントが別のパッシブ認証 ID ソース (ISE/ISE-PIC) と共有されている Windows Server 上の Microsoft Active Directory にインストールされている場合、Firewall Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firewall Management Center に記録されます。

サーバーグループの設定に関して次の点に注意してください。

- ユーザーグループまたはグループ内のユーザーに対してユーザー制御を実行するには、LDAP または Active Directory サーバーでユーザーグループを設定する必要があります。
- グループ名は LDAP で内部的に使用されているため、**s-** で開始することはできません。

グループ名または組織単位名には、アスタリスク (*)、イコール (=)、バックスラッシュ (\) などの特殊文字は使用できません。使用すると、それらのグループまたは組織単位内のユーザーはダウンロードされず、アイデンティティポリシーでは使用できません。

- サーバー上のサブグループのメンバーであるユーザーを含む（または除外する）Active Directory レルムを設定するには、Windows Server 2012 では、Active Directory のグループあたりのユーザー数が 5000 人以下であることが Microsoft により推奨されていることに注意してください。詳細については、MSDN の「Active Directory Maximum Limits—Scalability」を参照してください。

必要に応じて、より多くのユーザーをサポートするため、このデフォルトの制限を引き上げるよう Active Directory サーバーの設定を変更できます。

- リモート デスクトップ サービス環境でサーバーにより報告されるユーザーを一意に識別するには、Cisco Terminal Services (TS) エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザーに別個のポートを割り当て、システムはこれらのユーザーを一意に識別できるようになります。（Microsoft により、ターミナル サービスという名称はリモート デスクトップ サービスに変更されました）。

TS エージェントの詳細については、『Cisco Terminal Services (TS) Agent Guide』を参照してください。

サポートされているサーバーオブジェクトクラスと属性名

Secure Firewall Management Center がサーバからユーザ メタデータを取得できるようにするには、レルム内のサーバが、次の表に記載されている属性名を使用する必要があります。サーバ上の属性名が正しくない場合、Secure Firewall Management Center はその属性の情報を使ってデータベースに入力できなくなります。

表 1: Secure Firewall Management Center フィールドへの属性名のマップ

メタデータ (Metadata)	Firewall Management Center 属性	LDAP オブジェクト クラス	Active Directory 属性	OpenLDAP 属性
LDAP ユーザー名	Username	<ul style="list-style-type: none"> • user • inetOrgPerson 	samaccountname	cn uid
名	First Name		givenname	givenname
姓	Last Name		sn	sn
電子メールアドレス	Email		mail userprincipalname (mail に値が設定されていない場合)	mail
department	部署名		department distinguishedname (department に値が設定されていない場合)	ou
telephone number	Phone		telephonenumber	telephonenumber



(注) グループの LDAP オブジェクト クラスは、group、groupOfNames (Active Directory の場合は group-of-names) 、または groupOfUniqueNames です。

オブジェクト クラスと属性の詳細については、次のリファレンスを参照してください。

- Microsoft Active Directory :
 - オブジェクト クラス : [MSDN](#) の「All Classes」
 - 属性 : [MSDN](#) の「All Attributes」
- OpenLDAP : [RFC 4512](#)

Kerberos 認証の前提条件

キャプティブ ポータル ユーザーの認証に Kerberos を使用している場合は、次の点に注意してください。

ホスト名の文字の制限

Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります (Windows で設定されている NetBIOS の制限)。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に設定します。詳細については、Microsoft のマニュアルサイト「[Naming conventions in Active Directory for computers, domains, sites, and OUs](#)」で、次のような記事を参照してください。

DNS 応答の文字の制限

DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、[RFC 6891 セクション 6.2.5](#) で説明されています。

[レルム (Realm)]フィールド

次のフィールドを使用して、レルムを設定します。

[レルムの構成 (Realm Configuration)]フィールド

これらの設定は、レルム内のすべての Active Directory サーバまたはドメインコントローラ (別名ディレクトリ) に適用されます。

名前

レルムの一意の名前。

- アイデンティティポリシーにレルムを使用する場合、英数字や特殊文字に対応しています。
- RA VPN 設定でレルムを使用する場合は、英数字、ハイフン (-)、下線 (_)、プラス (+) に対応しています。

説明

(オプション) レルムの説明を入力します。

タイプ

レルムのタイプで、Microsoft Active Directory 用の [AD]、その他のサポートされている LDAP リポジトリ用の [LDAP]、または [Local] です。サポートされている LDAP リポジトリの一覧については、[レルム向けにサポートされているサーバー \(42 ページ\)](#) を参照してください。LDAP リポジトリを使用してキャプティブポータルユーザーを認証できません。他はすべて Active Directory が必要です。



(注) キャプティブポータルのみ、LDAP レルムをサポートします。

レルムタイプ LOCAL は、ローカルユーザー設定の設定に使用されます。LOCAL レルムは、リモートアクセスユーザーの認証で使用されます。

LOCAL レルムの次のローカルユーザー情報を追加します。

- [Username] : ローカルユーザーの名前。
- [Password] : ローカルユーザーのパスワード。
- [Confirm Password] : ローカルユーザーのパスワードを確認します。



(注) LOCAL レルムにユーザーを追加するには、[Add another local user] をクリックします。

レルムの作成後にユーザーを追加し、ローカルユーザーのパスワードを更新できます。複数の LOCAL レルムも作成できますが、無効にすることはできません。

AD プライマリ ドメイン (AD Primary Domain)

Microsoft Active Directory レルム専用です。ユーザー認証が必要となる Active Directory サーバーのドメインです。



(注) すべての Microsoft Active Directory (AD) レルムに固有の [ADプライマリドメイン (AD Primary Domain)] を指定する必要があります。異なる Microsoft AD レルムに同じ [ADプライマリドメイン (AD Primary Domain)] を指定することはできませんが、システムが適切に機能しなくなります。これは、システムにより各レルム内のすべてのユーザーとグループに 1 つの固有 ID が割り当てられるためです。そのため、システムは特定のユーザまたはグループを明確に識別することができません。ユーザーとグループが適切に識別されないため、同じ [ADプライマリドメイン (AD Primary Domain)] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザーとグループに割り当てるために発生します。そのため、システムは特定のユーザーまたはグループを明確に識別できません。

AD 参加ユーザー名 (AD Join Username) 、AD 参加パスワード (AD Join Password)

(レルムの編集時に [Realm Configuration] タブページで使用できます) 。

Kerberos キャプティブ ポータル アクティブ認証を目的とした Microsoft Active Directory レルムでは、Active Directory ドメインでドメイン コンピュータ アカウントを作成するための適切な権限を持つ Active Directory ユーザーの識別用のユーザー名とパスワード。

次の点を考慮してください。

- DNS は、ドメイン名を Active Directory ドメイン コントローラの IP アドレスに解決できる必要があります。
- 指定するユーザは、コンピュータを Active Directory ドメインに参加させる必要があります。
- ユーザー名は完全修飾名である必要があります (たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します) 。

Kerberos (または Kerberos をオプションとする場合に **HTTP ネゴシエート**) を、アイデンティティルール の [認証プロトコル (Authentication Protocol)] として選択する場合、選択する [レルム (Realm)] は、Kerberos キャプティブポータルアクティブ認証を実行するように、[AD参加ユーザー名 (AD Join Username)] と [AD参加パスワード (AD Join Password)] を使用して設定する必要があります。



- (注) SHA-1 ハッシュアルゴリズムでは Active Directory サーバーにパスワードが保存されて安全ではないため、使用しないでください。詳細については、Open Web Application Security Project の Web サイトにある「[Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet](#)」や「[Password Storage Cheat Sheet](#)」などの参考資料を参照してください。

Active Directory との通信には SHA-256 を使用することを推奨します。

[ディレクトリ ユーザー名 (Directory Username)] と [ディレクトリパスワード (Directory Password)]

取得するユーザ情報に適切なアクセス権を持っているユーザの識別用のユーザ名とパスワード。

次の点に注意してください。

- OpenLDAP では、ユーザーのアクセス権限は、[OpenLDAP の仕様書](#)のセクション 8 で説明されている <level> パラメータにより決定されます。ユーザーの <level> は、auth 以上にする必要があります。
- ユーザー名は完全修飾名である必要があります (たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します) 。



- (注) SHA-1 ハッシュアルゴリズムでは Active Directory サーバーにパスワードが保存されて安全ではないため、使用しないでください。詳細については、Open Web Application Security Project の Web サイトにある「[Migrating your Certification Authority Hashing Algorithm from SHA1 to SHA2 on Microsoft TechNet](#)」や「[Password Storage Cheat Sheet](#)」などの参考資料を参照してください。

Active Directory との通信には SHA-256 を使用することを推奨します。

ベース DN (Base DN)

(オプション) Secure Firewall Management Center がユーザーデータの検索を開始するサーバーのディレクトリツリー。ベース DN を指定しない場合、サーバーに接続できる場合、システムは最上位 DN を取得します。

通常、ベース識別名 (DN) には企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、**ou=security,dc=example,dc=com** となります。

Group DN

(オプション) Secure Firewall Management Centerがグループ属性を持つユーザーを検索するサーバーのディレクトリツリー。サポートされているグループ属性の一覧については、[サポートされているサーバーオブジェクトクラスと属性名 \(43 ページ\)](#) を参照してください。グループ DN を指定しない場合、サーバーに接続できる場合、システムは最上位 DN を取得します。



(注) 次に、ディレクトリサーバーのユーザー、グループ、DN でシステムがサポートする文字のリストを示します。次に示す文字以外を使用すると、システムがユーザーとグループをダウンロードできなくなる可能性があります。

エンティティ	サポートされている文字
ユーザー名	<code>a-z A-Z 0-9 ! # \$ % ^ & () _ - { } ' . ~ `</code>
グループ名	<code>a-z A-Z 0-9 ! # \$ % ^ & () _ - { } ' . ~ `</code>
ベース DN とグループ DN	<code>a-z A-Z 0-9 ! @ \$ % ^ & * () _ - . ~ `</code>

ユーザー名では、どの場所でも (末尾を含む) スペースはサポートされていません。

既存のレルムを編集する場合、次のフィールドを使用できます。

[ユーザー セッション タイムアウト (User Session Timeout)]

(レルムの編集時に [Realm Configuration] タブページで使用できます)。

ユーザーセッションがタイムアウトするまでの分数を入力します。デフォルトは、ユーザーのログインイベントから 1440 分 (24 時間) 後です。このタイムアウトを過ぎると、ユーザーのセッションは終了します。ユーザーが再度ログインせずにネットワークにアクセスし続けている場合、ユーザーは Secure Firewall Management Center により不明として認識されます ([失敗したキャプティブポータルユーザー (Failed Captive Portal Users)]を除く)。

さらに、レルムなしで ISE/ISE-PIC を設定し、タイムアウトを超えた場合は、回避策が必要です。詳細については、[Cisco TAC](#) にお問い合わせください。

次のタイムアウト値を設定できます。

- [ユーザーエージェントおよびISE/ISE-PICユーザー (User Agent and ISE/ISE-PIC Users)]: パッシブ認証タイプであるユーザーエージェントまたはISE/ISE-PIC によってトラッキングされるユーザーのタイムアウト。

指定したタイムアウト値は、pxGrid SXP セッショントピック サブスクリプション (宛先 SGT マッピングなど) には適用されません。代わりに、ISE からの特定のマッピングの削除または更新メッセージがない限り、セッショントピック マッピングは保持されます。

ISE/ISE-PIC の詳細については、[ISE/ISE-PIC アイデンティティ ソース](#) を参照してください。

- [ターミナルサービスエージェントユーザー (Terminal Services Agent Users)] : パスワード認証タイプである TS エージェントによってトラッキングされるユーザーのタイムアウト。詳細については、[ターミナルサービス \(TS\) エージェントのアイデンティティ ソース](#)を参照してください。
- [キャプティブポータルユーザ (Captive Portal Users)] : アクティブ認証タイプであるキャプティブポータルを使用して正常にログインしたユーザのタイムアウト。詳細については、[キャプティブポータルのアイデンティティ ソース](#)を参照してください。
- [失敗したキャプティブポータルユーザ (Failed Captive Portal Users)] : キャプティブポータルを使用して正常にログインしていないユーザのタイムアウト。Secure Firewall Management Center によってユーザが認証失敗ユーザとして認識されるまでの、[最大ログイン試行回数 (Maximum login attempts)]を設定できます。アクセスコントロールポリシーを使用して、認証失敗ユーザにネットワークへのアクセス権を付与することもできます。この場合は、そのユーザにこのタイムアウト値が適用されます。
失敗したキャプティブポータルログインの詳細については、[キャプティブポータルフィールド](#)を参照してください。
- [ゲストキャプティブポータルユーザ (Guest Captive Portal Users)] : キャプティブポータルにゲストユーザとしてログインしているユーザのタイムアウト。詳細については、「[キャプティブポータルのアイデンティティ ソース](#)」を参照してください。

レルムディレクトリと同期フィールド

レルムディレクトリフィールド

これらの設定は、レルム内の個々のサーバー (Active Directory ドメインコントローラなど) に適用されます。

ホスト名/IP アドレス (Hostname/IP Address)

Active Directory ドメインコントローラマシンの完全修飾ホスト名。完全修飾名を確認するには、[Active Directory \(AD\) サーバーの名前を検索する \(53 ページ\)](#)を参照してください。

キャプティブポータルの認証に Kerberos を使用している場合は、次のことも理解してください。

Kerberos 認証を使用している場合、管理対象デバイスのホスト名は 15 文字未満にする必要があります (Windows で設定されている NetBIOS の制限)。そのようにしないと、キャプティブポータル認証が失敗します。管理対象デバイスのホスト名は、デバイスのセットアップ時に設定します。詳細については、Microsoft のマニュアルサイト「[Naming conventions in Active Directory for computers, domains, sites, and OUs](#)」で、次のような記事を参照してください。

DNS はホスト名に対して 64KB 以下の応答を返す必要があります。それ以外の場合、AD 接続テストは失敗します。この制限は両方向に適用され、[RFC 6891 セクション 6.2.5](#)で説明されています。

ポート

サーバーのポート。

暗号化 (Encryption)

(強く推奨) 使用する暗号化方式。

- **STARTTLS** : 暗号化 LDAP 接続
- **LDAPS** : 暗号化 LDAP 接続
- なし : 非暗号化 LDAP 接続 (保護されていないトラフィック)

Active Directory サーバーと安全に通信するには、[Active Directory \(AD\)](#) または [LDAP](#) に [安全に接続する \(52 ページ\)](#) を参照してください。

CA Certificate

サーバーへの認証に使用する TLS/SSL 証明書。TLS/SSL 証明書を使用するために、**STARTTLS** または **LDAPS** を [暗号化 (Encryption)] タイプとして設定できます。

認証に証明書を使用する場合、証明書のサーバー名は、サーバーの [Hostname/IP Address] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で **computer1.example.com** を使用している場合は、接続が失敗します。

ディレクトリサーバーへの接続に使用されるインターフェイス

Secure Firewall Threat Defense が Active Directory サーバーに安全に接続できるように、RA VPN 認証にのみ必要です。ただし、このインターフェイスは、ユーザーおよびグループのダウンロードには使用されません。

ルーテッドインターフェイス グループだけを選択できます。詳細については、[インターフェイス \(Interface\)](#) を参照してください。

次のいずれかをクリックします。

- ルートルックアップによる解決 : ルーティングを使用して Active Directory サーバーに接続します。
- [インターフェイスの選択 (Choose an interface)] : Active Directory サーバーに接続する特定の管理対象デバイス インターフェイス グループを選択します。

ユーザー同期フィールド

AD プライマリ ドメイン (AD Primary Domain)

Microsoft Active Directory レルム専用です。ユーザー認証が必要となる Active Directory サーバーのドメインです。



- (注) すべての Microsoft Active Directory (AD) レルムに固有の [ADプライマリドメイン (AD Primary Domain)] を指定する必要があります。異なる Microsoft AD レルムに同じ [ADプライマリドメイン (AD Primary Domain)] を指定することはできますが、システムが適切に機能しなくなります。これは、システムにより各レルム内のすべてのユーザーとグループに 1 つの固有 ID が割り当てられるためです。そのため、システムは特定のユーザーまたはグループを明確に識別することができません。ユーザーとグループが適切に識別されないため、同じ [ADプライマリドメイン (AD Primary Domain)] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザーとグループに割り当てるために発生します。そのため、システムは特定のユーザーまたはグループを明確に識別できません。

ユーザーとグループを検索するクエリを入力してください

[Base DN] :

(オプション) Firewall Management Centerがユーザーデータの検索を開始するサーバーのディレクトリ ツリー。

通常、ベース識別名 (DN) には企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、**ou=security,dc=example,dc=com** となります。

[Group DN] :

(オプション) Firewall Management Centerがグループ属性を持つユーザーを検索するサーバーのディレクトリ ツリー。サポートされているグループ属性の一覧については、[サポートされているサーバーオブジェクトクラスと属性名 \(43 ページ\)](#) を参照してください。



- (注) グループ名または組織単位名には、アスタリスク (*)、イコール (=)、バックスラッシュ (\) などの特殊文字は使用できません。使用した場合、それらのグループのユーザーはダウンロードされず、ID ポリシーで使用できないためです。

[Load Groups]

ユーザー認識用およびユーザー制御用にユーザーとグループをダウンロードできるようになります。

[使用可能なグループ (Available Groups)]、[含むに追加する (Add to Include)]、[除外するに追加する (Add to Exclude)]

ポリシーで使用できるグループを制限します。

- [使用可能なグループ (Available Groups)] フィールドに表示されているグループは、グループを [含むグループとユーザー (Included Groups and Users)] または [除外するグループとユーザー (Excluded Groups and Users)] フィールドに移動しない限り、ポリシーで利用できます。

- グループを [含めるグループとユーザー (Included Groups and Users)] フィールドに移動させた場合は、それらのグループとそれらのグループに含まれるユーザーだけがダウンロードされ、ユーザーデータはユーザー認識やユーザー制御に利用できます。
- グループを [除外するグループとユーザー (Excluded Groups and Users)] フィールドに移動させた場合は、それ以外のすべてのグループとそれらのグループに含まれるユーザーがダウンロードされ、ユーザー認識やユーザー制御に利用できます。
- 含まれないグループのユーザーを含めるには、[ユーザーの包含 (User Inclusion)] の下のフィールドにそのユーザー名を入力し、[追加 (Add)] をクリックします。
- 除外されないグループのユーザーを除外するには、[ユーザーの除外 (User Exclusion)] の下のフィールドにそのユーザー名を入力し、[追加 (Add)] をクリックします。



(注) Firewall Management Center にダウンロードされるユーザーは、数式 $R = I - (E+e) + i$ を使用して計算されます。

- R はダウンロードしたユーザーのリストです。
- I は含まれているグループです。
- E は除外されているグループです。
- e は除外されているユーザーです。
- i は含まれているユーザーです。

[Synchronize Now]

クリックして、グループとユーザーを AD と同期します。

自動同期の開始時間

AD からユーザーとグループをダウンロードする時間と時間間隔を入力します。

Active Directory (AD) または LDAP に安全に接続する

Active Directory または LDAP サーバーおよび Secure Firewall Management Center (強く推奨) 間でセキュアな接続を確立するには、次のすべてのタスクを実行する必要があります。

- サーバーのルート証明書をエクスポートします。
- ルート証明書を信頼できる CA 証明書 (**Objects > Object Management > PKI > Trusted CAs**) として Secure Firewall Management Center にインポートします。
- サーバーの完全修飾名を検索します。
- レルムディレクトリを作成します。

詳細については、次のいずれかのタスクを参照してください。

関連トピック

[Active Directory \(AD\) サーバーのルート証明書をエクスポートする](#) (53 ページ)

[Active Directory \(AD\) サーバーの名前を検索する](#) (53 ページ)

[LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する](#) (32 ページ)

Active Directory (AD) サーバーの名前を検索する

Firewall Management Center でレルムディレクトリを設定するには、次の手順で説明するように、完全修飾サーバー名を把握しておく必要があります。

これらのタスクは、Microsoft Active Directory にのみ適用されます。LDAP を使用する場合は、手順について適切な参考資料を参照してください。

始める前に

コンピュータの名前を表示できる権限を持つユーザーとして Active Directory サーバーにログインする必要があります。

手順

ステップ 1 Active Directory サーバーにログインします。

ステップ 2 [開始 (Start)] をクリックします。

ステップ 3 [この PC (This PC)] を右クリックします。

ステップ 4 [プロパティ (Properties)] をクリックします。

ステップ 5 [Advanced System Settings] をクリックします。

ステップ 6 [コンピュータ名 (Computer Name)] タブをクリックします。

ステップ 7 [フルコンピュータ名 (Full computer name)] の値をメモします。

Firewall Management Center でレルムディレクトリを構成する際は、この正確な名前を入力する必要があります。

次のタスク

[LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する](#) (32 ページ)。

関連トピック

[Active Directory \(AD\) サーバーのルート証明書をエクスポートする](#) (53 ページ)

Active Directory (AD) サーバーのルート証明書をエクスポートする

次のタスクでは、Active Directory サーバーのルート証明書をエクスポートする方法について説明します。これは、ユーザーアイデンティティ情報を取得するために Firewall Management Center に安全に接続する際に必要になります。

これらのタスクは、Microsoft Active Directory にのみ適用されます。LDAP を使用する場合は、手順について適切な参考資料を参照してください。

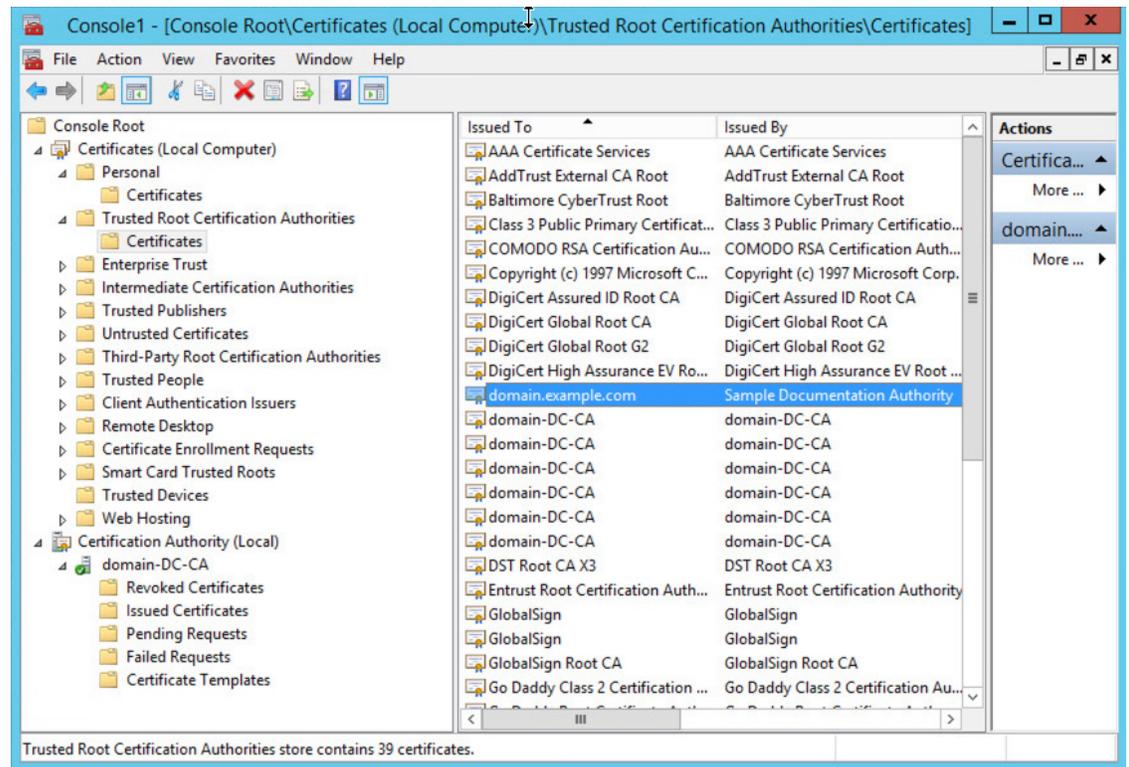
始める前に

Active Directory サーバーのルート証明書の名前が分かっている必要があります。ルート証明書の名前がドメインと同じである場合も異なっている場合もあります。次の手順は、名前を確認する一つの方法を示しています。ただし、他の方法も考えられます。

手順

ステップ 1 以下は、Active Directory サーバーのルート証明書の名前を確認する一つの方法です。詳細については、Microsoft 社のドキュメントを参照してください。

- a) Microsoft 管理コンソールを実行する権限を持つユーザーとして Active Directory サーバーにログインします。
- b) [開始 (Start)] をクリックして、**mmc** を入力します。
- c) [ファイル (File)] > [スナップインの追加と削除 (Add/Remove Snap-in)] をクリックします。
- d) 左側のペインにある [使用可能なスナップイン (Available Snap-ins)] リストから、[証明書 (ローカル) (Certificates (local))] をクリックします。
- e) [追加 (Add)] をクリックします。
- f) [証明書スナップイン (Certificates snap-in)] ダイアログボックスで、[コンピュータアカウント (Computer Account)] をクリックし、[次へ (Next)] をクリックします。
- g) [コンピュータの選択 (Select Computer)] ダイアログボックスで [ローカルコンピュータ (Local Computer)] をクリックし、[終了 (Finish)] をクリックします。
- h) Windows Server 2012 のみ。前の手順を繰り返して、証明機関スナップインを追加します。
- i) [コンソールルート (Console Root)] > [信頼された証明機関 (Trusted Certification Authorities)] > [証明書 (Certificates)] をクリックします。
サーバーの信頼できる証明書が右側のペインに表示されます。次の図は Windows Server 2012 の例であり、環境によっては異なっている可能性があります。



ステップ2 certutil コマンドを使用して証明書をエクスポートします。

これは、証明書をエクスポートする一つの方法に過ぎません。これは、証明書をエクスポートする便利な方法です。特に、Web ブラウザを実行して Active Directory サーバーから Firewall Management Center に接続できる場合に便利です。

- [開始 (Start)] をクリックして、**cmd** を入力します。
- certutil -ca.cert certificate-name** コマンドを入力します。
サーバーの証明書が画面に表示されます。
- BEGIN CERTIFICATE-----** で始まり **-----END CERTIFICATE-----** で終わる (これらの文字列を含む) 証明書全体をクリップボードにコピーします。

次のタスク

信頼できる CA オブジェクトの追加の説明に従って、Active Directory サーバーの証明書を信頼できる CA 証明書として Firewall Management Center にインポートします。

関連トピック

[Active Directory \(AD\) サーバーの名前を検索する \(53 ページ\)](#)

ユーザーとグループを同期する

ユーザーとグループの同期とは、グループとグループ内のユーザーに対して設定したレルムとディレクトリに対して、Firewall Management Center がクエリを実行することを意味します。Firewall Management Center が検出したすべてのユーザーを ID ポリシーで使用できます。

問題が見つかった場合は、Firewall Management Center がロードできないユーザーとグループを含むレルムを追加する必要があります。詳細は、[レルムおよび信頼できるドメイン \(38 ページ\)](#) を参照してください。

始める前に

各 Active Directory ドメインの Secure Firewall Management Center レルムと、各フォレストの Active Director ドメインコントローラごとの Firewall Management Center ディレクトリを作成します。[LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する \(32 ページ\)](#) を参照してください。



(注) Microsoft Azure AD レルムでは、ユーザーとグループの同期は必要ありません。

ユーザー制御で使用するユーザーを含むドメインに対してのみレルムを作成する必要があります。

未定の ネストできます。Secure Firewall Management Center はそれらのグループとグループに含まれるユーザーをダウンロードします。[LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する \(32 ページ\)](#) の説明に従い、必要に応じて、ダウンロードするグループとユーザーを制限できます。

ドメインの代替ユーザープリンシパル名 (UPN) サフィックスではなく、ドメインの元のドメイン名を使用してレルムを作成する必要があります。そうしない場合、ユーザーとグループはダウンロードに失敗し、アイデンティティポリシーは適用されません。たとえば、元のドメインが domain.example.com で、代替の UPN 名が domain2.mydomain.com の場合は、domain.example.com を使用するようにレルムを設定する必要があります。代替の UPN サフィックスの設定の詳細については、[learn.microsoft.com](#) の「[Configuring Alternate Login ID](#)」などのリソースを参照してください。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **Integration > Other Integrations > Realms > Realms** をクリックします。

ステップ 3 各レルムの横にある **Download** (↓) をクリックします。

ステップ 4 結果を表示するには、[Sync Results] タブをクリックします。

[Realms] 列に、Active Directory フォレスト内のユーザーとグループの同期に関する問題の有無が示されます。各レルムの横にある次のインジケータを探します。

[Realms] 列のインジケータ	意味
(なし)	エラーなく同期されたすべてのユーザーとグループ。対処不要です。
Yellow Triangle (⚠)	ユーザーとグループの同期中に問題が発生しました。各 Active Directory ドメインのレルムと各 Active Directory ドメインコントローラのディレクトリを追加したことを確認します。 詳細については、 クロスドメイン信頼をトラブルシューティングする (73 ページ) を参照してください。

レルムシーケンスを作成する

次の手順で、レルムシーケンスを作成できます。レルムシーケンスは、システムがアイデンティティポリシーを適用するときに検索するレルムの順序付きリストです。レルムを追加する場合とまったく同じ方法で、アイデンティティルールにレルムシーケンスを追加します。違いは、システムがアイデンティティポリシーを適用するときに、レルムシーケンスで指定された順序ですべてのレルムが検索されることです。

始める前に

Active Directory サーバーとの接続にそれぞれ対応する、少なくとも2つのレルムを作成して有効にする必要があります。LDAP レルムのレルムシーケンスは作成できません。

[LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する \(32 ページ\)](#) の説明に従って、レルムを作成します。

手順

- ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。
 - ステップ 2 **Integration > Other Integrations > Realms > Realm Sequences** をクリックします。
 - ステップ 3 [レルムシーケンス (Realm Sequences)] タブをクリックします。
 - ステップ 4 [シーケンスを追加 (Add Sequence)] をクリックします。
 - ステップ 5 [Name] フィールドに、レルムシーケンスを識別するための名前を入力します。
 - ステップ 6 (オプション) [Description] フィールドに、レルムシーケンスの説明を入力します。
 - ステップ 7 [Realms] で、**Add (+)** をクリックします。
 - ステップ 8 シーケンスに追加する各レルムの名前をクリックします。
- 検索を絞り込むには、[Filter] フィールドにレルム名のすべてまたは一部を入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Add Realm Sequence] ダイアログボックスで、システムが検索する順序でレルムをドラッグアンドドロップします。

次の図に、2つのレルムで構成されるレルムシーケンスの例を示します。

domain-europe.example.com レルムは、**domain.example.com** レルムの前にユーザーに対して検索されます。

The screenshot shows a dialog box titled "Add Realm Sequence". It has a "Name *" field containing "Americas and Europe", an empty "Description" field, and a "Realms" section. The "Realms" section includes a plus sign and the instruction "Drag and drop to order your realms". Below this, two realms are listed: "domain-europe.example.com (AD)" and "domain.example.com (AD)". At the bottom right, there are "Cancel" and "Save" buttons.

ステップ 11 [Save] をクリックします。

次のタスク

[「アイデンティティ ポリシーの作成」](#) を参照してください。

クロスドメイン信頼に対して Firewall Management Center を構成する：手順

ここでは、いくつかのトピックを通じて、クロスドメイン信頼を持つ2つのレルムを使用した Firewall Management Center の設定方法を解説します。

この段階的な手順の例には、2つのフォレスト：**forest.example.com** と **eastforest.example.com** が含まれます。フォレストは、各フォレスト内の特定のユーザーおよびグループが他のフォレスト内の Microsoft AD によって認証されるように設定されます。



(注) このトピックは、Microsoft AD レalmにのみ適用されます。Microsoft Azure AD レalmには適用されません。

次に、この例で使用する設定例を示します。



前述の例を使用して、Firewall Management Center を次のように設定します。

- アクセスコントロールポリシーで制御するユーザーを含む **forest.example.com** 内の任意のドメインのレalmとディレクトリ
- アクセスコントロールポリシーで制御するユーザーを含む **eastforest.example.com** 内の任意のドメインのレalmとディレクトリ

この例の各レalmには、Firewall Management Center でディレクトリとして設定されている1つのドメインコントローラがあります。この例のディレクトリは、次のように設定されています。

- **forest.example.com**
 - ユーザーのベース識別名 (DN) : **ou=UsersWest,dc=forest,dc=example,dc=com**
 - グループのベース DN : **ou=EngineeringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
 - ユーザーのベース DN : **ou=EastUsers,dc=eastforest,dc=example,dc=com**
 - グループのベース DN : **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

関連トピック

[クロスドメイントラスト向けに Secure Firewall Management Center を構成する手順1：レalmとディレクトリを構成する \(60 ページ\)](#)

クロスドメイントラスト向けに **Secure Firewall Management Center** を構成する手順 1 : レルムとディレクトリを構成する

これは、クロスドメインの信頼関係で設定された Active Directory サーバーを認識するように Firewall Management Center を設定する方法を説明する、段階的な手順の最初のタスクです。この設定は、企業組織で一般的になりつつあります。この設定例の概要については、[クロスドメイン信頼に対して Firewall Management Center を構成する : 手順 \(58 ページ\)](#) を参照してください。

ドメインごとに1つのレルムとドメインコントローラごとに1つのディレクトリを使用して設定したシステムでは、最大 100,000 の外部セキュリティプリンシパル (ユーザーとグループ) を検出できます。これらの外部セキュリティプリンシパルが別のレルムでダウンロードされたユーザーと一致する場合は、アクセス コントロール ポリシーで使用できます。

始める前に

Microsoft Active Directory サーバーは、クロスドメインの信頼関係で設定する必要があります。詳細については、[レルムおよび信頼できるドメイン \(38 ページ\)](#) を参照してください。

LDAP または Microsoft Azure AD でユーザーを認証する場合、この手順は使用できません。

手順

-
- ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。
 - ステップ 2 **Integration > Other Integrations > Realms > Realms** をクリックします。
 - ステップ 3 **[レルムを追加 (Add Realm)] > [Active Directory/LDAP]** をクリックします。
 - ステップ 4 **forest.example.com** を設定するために、次の情報を入力します。

Add New Realm

Name* Description

Type AD Primary Domain
E.g. domain.com

Directory Username* Directory Password*
E.g. user@domain.com

Base DN Group DN
E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

eastforest.example.com:389

Hostname/IP Address* Port*

Encryption CA Certificate

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface
Default: Management/Diagnostic Interface

5 ✔ Test connection succeeded

[Add another directory](#)

6

(注)

[Directory Username]には、Active Directory ドメイン内の任意のユーザーを指定できます。特別な権限は必要ありません。

ディレクトリサーバーへの接続に使用されるインターフェイスは、Active Directory サーバーに接続できる任意のインターフェイスです。

ステップ 5 [Test] をクリックし、テストが成功することを確認してから続行します。

ステップ 6 [Configure Groups and Users] をクリックします。

ステップ 7 設定が成功すると、次のようなページが表示されます。

forest.example.com
Enter description

Group and User Sync | Directory | Realm Configuration

AD Primary Domain
forest.example.com
E.g. domain.com

Enter query to look for users and groups
Enter the directory tree on the server where the Firepower Management Center should begin searching for user and group data.

Base DN
ou=UsersWest,dc=forest,dc=exa
E.g. ou=group,dc=cisco,dc=com

Group DN
ou=EngineeringWest,dc=forest,d
E.g. ou=group,dc=cisco,dc=com

Load Groups

Available Groups
Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

Search

CrossForestTest
AnotherCrosForestTest
EngineersWest
RegularGroup
CrossForestGroup

Included Groups and Users
All except excluded

Excluded Groups and Users
None

Groups and users are downloaded

(注)

グループとユーザーがダウンロードされていない場合は、[Base DN] フィールドと [Groups DN] フィールドの値を確認し、[Load Groups] をクリックします。

このページでは、その他のオプション設定を使用できます。詳細については、[レalm (Realm)] フィールド (45 ページ) およびレalmディレクトリと同期フィールド (49 ページ) を参照してください。

ステップ 8 このページまたはタブページで変更を行った場合は、[Save] をクリックします。

ステップ 9 **Integration > Other Integrations > Realms > Realms** をクリックします。

ステップ 10 [レalmを追加 (Add Realm)] をクリックします。

ステップ 11 **eastforest.example.com** を設定するために、次の情報を入力します。

?
✕

Add New Realm

Name*	Description
<input type="text" value="eastforest.example.com"/>	<input type="text"/>
Type	AD Primary Domain
<input type="text" value="AD"/>	<input type="text" value="eastforest.example.com"/> <small>E.g. domain.com</small>
Directory Username*	Directory Password*
<input type="text" value="limited.eastuser@eastforest.example.com"/> <small>E.g. user@domain.com</small>	<input type="text" value="....."/>
Base DN	Group DN
<input type="text" value="jUsers,dc=eastforest,dc=example,dc=com"/> <small>E.g. ou=group,dc=cisco,dc=com</small>	<input type="text" value="eering,dc=eastforest,dc=example,dc=com"/> <small>E.g. ou=group,dc=cisco,dc=com</small>

Directory Server Configuration

eastforest.example.com:636

Hostname/IP Address*	Port*
<input type="text" value="eastforest.example.com"/>	<input type="text" value="636"/>
Encryption	CA Certificate*
<input type="text" value="LDAPS"/>	<input type="text" value="EastForest"/>
Interface used to connect to Directory server ⓘ	
<input checked="" type="radio"/> Resolve via route lookup <input type="radio"/> Choose an interface <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;">Default: Management/Diagnostic Interface</div>	
<input type="button" value="Test"/> ✔ Test connection succeeded	

[Add another directory](#)

ステップ 12 [Test] をクリックし、テストが成功することを確認してから続行します。

ステップ 13 [Configure Groups and Users] をクリックします。

ステップ 14 設定が成功すると、次のようなページが表示されます。

eastforest.example.com
Cancel Save

Enter description

Group and User Sync
Directory
Realm Configuration

AD Primary Domain

eastforest.example.com

E.g. domain.com

Enter query to look for users and groups

Enter the directory tree on the server where the Firewall Management Center should begin searching for user and group data.

Base DN

ou=EastUsers,dc=eastforest,dc=

E.g. ou=group,dc=cisco,dc=com

Group DN

ou=EastEngineering,du=eastfore

E.g. ou=group,dc=cisco,dc=com

Load Groups

Available Groups

Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

No groups were found

Included Groups and Users

All except excluded

Excluded Groups and Users

None

Include

Exclude

関連トピック

[クロスドメイン信頼向けに Secure Firewall Management Center を構成する手順 2 : ユーザーとグループを同期する \(64 ページ\)](#)

クロスドメイン信頼向けに **Secure Firewall Management Center** を構成する手順 2 : ユーザーとグループを同期する

クロスドメインの信頼関係を持つ2つ以上の Active Directory サーバーを設定したら、ユーザーとグループをダウンロードする必要があります。このプロセスでは、Active Directory の設定で問題が発生する可能性があります（一方の Active Directory ドメインにはグループまたはユーザーがダウンロードされていて、もう一方にはダウンロードされていない場合など）。

始める前に

[クロスドメイントラスト向けに Secure Firewall Management Center を構成する手順 1 : レalmとディレクトリを構成する \(60 ページ\)](#) で説明されている作業を実行したことを確認します。

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **Integration > Other Integrations > Realms > Realms** をクリックします。

ステップ 3 クロスドメイン信頼の任意のレルムの行の末尾で、**Download Now**()をクリックし、[はい (Yes)] をクリックします。

ステップ 4 **Check Mark** () ([Notifications]) > [Tasks] をクリックします。

グループとユーザーのダウンロードに失敗した場合は、再試行してください。後続の試行が失敗した場合は、[レルム (Realm)] フィールド (45 ページ) およびレルムディレクトリと同期フィールド (49 ページ) の説明に従い、レルムとディレクトリの設定を確認します。

ステップ 5 **Integration > Other Integrations > Realms > Sync Results** をクリックします。

関連トピック

[クロスドメイン信頼向けに Secure Firewall Management Center を構成する手順 3 : 問題を解決する \(65 ページ\)](#)

クロスドメイン信頼向けに **Secure Firewall Management Center** を構成する手順 3 : 問題を解決する

Firewall Management Center でクロスドメイン信頼を設定する最後の手順は、ユーザーとグループがエラーなしでダウンロードされるようにすることです。ユーザーとグループが適切にダウンロードされない一般的な理由は、ユーザーとグループが属するレルムが Firewall Management Center にダウンロードされていないことです。

このトピックでは、ドメインコントローラ階層でグループを検索するようにレルムが設定されていないため、1つのフォレストで参照されているグループをダウンロードできないことを診断する方法について説明します。

始める前に

手順

ステップ 1 Secure Firewall Management Center にログインしていない場合はログインします。

ステップ 2 **Integration > Other Integrations > Realms > Realms** をクリックします。

[Realms] 列で、レルムの名前の横に **Yellow Triangle** () が表示されている場合、解決する必要がある問題があります。表示されていない場合、正しく設定されているため、終了できます。

ステップ 3 問題を表示するレルムからユーザーとグループを再度ダウンロードします。

a) [Realms] タブをクリックします。

b)  [(Download Now)] をクリックし、[Yes] をクリックします。

ステップ 4 [Sync Results] タブページをクリックします。

[Realms] カラムに **Yellow Triangle** (▲) が表示されている場合は、問題のあるレルムの横にある **Yellow Triangle** (▲) をクリックします。

ステップ 5 中央の列で、[Groups] または [Users] をクリックして詳細情報を検索します。

ステップ 6 [Groups] または [Users] タブページで、**Yellow Triangle** (▲) をクリックして詳細情報を表示します。

右側の列には、問題の原因を特定できる十分な情報が表示されます。

The screenshot displays the 'Sync Results' section of the management console. It features three main panels: 'Realms', 'Groups', and 'Users contained in the selected group'. Each panel has a search bar and a list of items. The 'Realms' panel lists 'forest.example.com' and 'eastforest.example.com', with a yellow triangle warning icon next to 'forest.example.com'. The 'Groups' panel lists 'CrossForestInvalidGroup', 'CrossForestValidGroup', and 'EngineersWest', with a yellow triangle warning icon next to 'CrossForestInvalidGroup'. The 'Users' panel lists 'EastForest.example.com\EastMarketingUsers' with a yellow triangle warning icon. To the right of these panels, there is a detailed error message for each warning icon, explaining that the realm or group contains references to user or groups in another domain that have not been synchronized.

前述の例では、**forest.example.com** には、Firewall Management Center によってダウンロードされていない別のグループ **EastMarketingUsers** を含むクロスドメイングループ **CrossForestInvalidGroup** が含まれています。**eastforest.example.com** レルムを再度同期した後、エラーが解決しない場合は、Active Directory ドメインコントローラに **EastMarketingUsers** が含まれていない可能性があります。

この問題を解決するには、次を実行します。

- **CrossForestInvalidGroup** から **EastMarketingUsers** を削除し、**forest.example.com** レルムを再度同期して、再確認します。
- **eastforest.example.com** レルムの [Group DN] から **ou=EastEngineering** 値を削除します。これにより、Firewall Management Center は Active Directory 階層の最上位レベルからグループを取得し、**eastforest.example.com** を同期して再確認します。

レルムを管理する

この項では、[レルム (Realms)] ページ上のコントロールを使用して、レルムに関するさまざまなメンテナンスタスクを実行する方法について説明します。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。代わりに **View** (👁) 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

手順

-
- ステップ 1** Secure Firewall Management Center にログインしていない場合はログインします。
 - ステップ 2** **Integration > Other Integrations > Realms > Realms** をクリックします。
 - ステップ 3** レルムを削除するには、**Delete** (🗑) をクリックします。
 - ステップ 4** レルムを編集するには、レルムの横にある **Edit** (✎) をクリックし、[LDAP レルムまたは Active Directory \(AD\) レルムおよびレルムディレクトリを作成する \(32 ページ\)](#) の説明に従って変更を行います。
 - ステップ 5** レルムを有効にするには、[状態 (State)] を右にスライドします。レルムを無効にするには、左にスライドします。
 - ステップ 6** ユーザーおよびユーザーグループをダウンロードするには、**Download** (⬇) をクリックします。
 - ステップ 7** レルムをコピーするには、**Copy** (📄) をクリックします。
 - ステップ 8** レルムを比較する方法については、[レルムを比較する \(67 ページ\)](#) を参照してください。
-

レルムを比較する

このタスクを実行するには、Admin、Access Admin、Network Admin、または Security Approver である必要があります。

手順

-
- ステップ 1** Secure Firewall Management Center にログインしていない場合はログインします。
 - ステップ 2** **Integration > Other Integrations > Realms > Realms** をクリックします。
 - ステップ 3** [レルムの比較 (Compare Realms)] をクリックします。
 - ステップ 4** [比較対象 (Compare Against)] リストから [レルムの比較 (Compare Realm)] を選択します。
 - ステップ 5** [レルム A (Realm A)] および [レルム B (Realm B)] リストから比較するレルムを選択します。

- ステップ 6** [OK] をクリック
- ステップ 7** 個々の変更を選択するには、タイトルバーの上の [前へ (Previous)] または [次へ (Next)] をクリックします。
- ステップ 8** (オプション) [比較レポート (Comparison Report)] をクリックして、レلم比較レポートを生成します。
- ステップ 9** (オプション) [新しい比較 (New Comparison)] をクリックして、新しいレلم比較ビューを生成します。

レلمとユーザーのダウンロードをトラブルシューティングする

予期しないサーバー接続の動作に気付いたら、レلم設定、デバイス設定、またはサーバー設定の調整を検討してください。関連の他のトラブルシューティングについては、次を参照してください。

- [Cisco ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング](#)
- [TS エージェント アイデンティティ ソースのトラブルシューティング](#)
- [キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング](#)
- [リモート アクセス VPN アイデンティティ ソースのトラブルシューティング](#)
- [ユーザー制御のトラブルシューティング](#)

症状: レلمとグループはレポートされますが、ダウンロードされません

Secure Firewall Management Center のヘルスマニターは、ユーザーまたはレلمの不一致を通知します。これらは次のように定義されています。

- ユーザーの不一致: ユーザーは、ダウンロードされることなく Secure Firewall Management Center に報告されます。
ユーザーの不一致の一般的な理由は、ユーザーが Secure Firewall Management Center へのダウンロードから除外されたグループに属していることです。Review the information discussed in [Cisco Secure Firewall Management Center Device Configuration Guide](#).
- レلمの不一致: ユーザーが、Firewall Management Center に認識されていないレلمに対応するドメインにログインした場合に不一致が起きます。

たとえば、Firewall Management Center で **domain.example.com** というドメインに対応するレلمを定義していても、**another-domain.example.com** というドメインからログインがレポートされる場合、これはレلمの不一致となります。このドメイン内のユーザーは Firewall Management Center によって [不明 (Unknown)] と識別されます。

あるヘルス警告がトリガーされると、パーセンテージの不一致のしきい値を設定します。次に例を示します。

- 50%のデフォルトの不一致のしきい値を使用すると、2つのミスマッチレルム8つの着信セッションでは、不一致割合は、25%と警告はトリガーされません。
- 30%の不一致のしきい値を設定すると、3つのミスマッチレルム5つの着信セッションでは、不一致割合は、60%および警告がトリガーされます。

不明なユーザーアイデンティティルールに一致しないには、ポリシーに適用されていません。(不明ユーザーに対してアイデンティティルールをセットアップすることはできませんが、ユーザーとレルムを正確に識別することによってルールの数を最小限に保つことをお勧めします。)

詳細については、[レルムまたはユーザーの不一致を検出する \(72 ページ\)](#) を参照してください。

症状：ユーザーがダウンロードされない

考えられる原因は次のとおりです。

- レルムの[タイプ (Type)]が正しく設定されていない場合は、システムにより必要とされる属性とリポジトリにより提供される属性が一致しないため、ユーザーとグループをダウンロードできません。たとえば、Microsoft Active Directory レルムの[タイプ (Type)]を[LDAP]として設定すると、システムではuid属性が必要になり、この属性はActive Directory ではnoneに設定されています。(Active Directory リポジトリでは、ユーザ ID に sAMAccountName が使用されます。)

ソリューション：レルムの[タイプ (Type)]フィールドを適切に設定します。Microsoft Active Directory の場合は[AD]に設定し、サポートされている別のLDAPリポジトリの場合は[LDAP]に設定します。

- グループ名または組織単位名に特殊文字が使用されているActive Directory グループのユーザーは、アイデンティティポリシールールで使用できない可能性があります。たとえば、グループ名または組織単位名にアスタリスク (*)、イコール (=)、バックスラッシュ (\) などの特殊文字が含まれている場合、これらのグループ内のユーザーはダウンロードされず、アイデンティティポリシーで使用できません。

解決策：グループ名または組織単位名から特殊文字を削除します。



重要 Secure Firewall Management Center と Active Directory ドメインコントローラ間の遅延を削減するには、地理的に Secure Firewall Management Center にできるだけ近いレルムディレクトリ (つまり、ドメインコントローラ) を構成することを強くお勧めします。

たとえば、Secure Firewall Management Center が北米にある場合は、同様に北米にあるレルムディレクトリを構成します。このように構成しないと、ユーザーやグループのダウンロードがタイムアウトするなどの問題が発生する可能性があります。

症状：レルム内の一部のユーザーがダウンロードされない

考えられる原因は次のとおりです。

- 1つのレルムで最大数を超えるユーザーをダウンロードしようとする、最大ユーザー数でダウンロードが停止し、正常性アラートが表示されます。ユーザーダウンロードの制限は、Secure Firewall Management Center モデルごとに設定されています。詳細については、[Microsoft Active Directory のユーザー制限](#)を参照してください。
- すべてのユーザーは、グループのメンバーである必要があります。グループのメンバーでないユーザーはダウンロードされません。

症状：アクセスコントロールポリシーがグループのメンバーシップと一致しない

この解決策は、他の AD ドメインとの信頼関係にある AD ドメインに適用されます。以下の説明で、外部ドメイン ドメインは、ユーザーがログインするドメイン以外のドメインを指します。

ユーザーが信頼されている外部ドメインで定義されたグループに属している場合、Secure Firewall Management Center は外部ドメインのメンバーシップを追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン コントローラ 1 と 2 は相互に信頼している
- グループ A はドメイン コントローラ 2 で定義されている
- コントローラ 1 のユーザー mparvinder はグループ A のメンバーである

ユーザー mparvinder はグループ A に属しているものの、メンバーシップグループ A を指定する Secure Firewall Management Center のアクセスコントロールポリシー ルールが一致しません。

解決策：グループ A に属する、すべてのドメイン 1 のアカウントを含むドメイン コントローラ 1 に同様のグループを作成します。グループ A またはグループ B のすべてのメンバーに一致するように、アクセスコントロールポリシー ルールを変更します。

症状：アクセスコントロールポリシーが子ドメインのメンバーシップと一致しない

ユーザーが親ドメインの子であるドメインに属している場合、Firepower はドメイン間の親/子関係を追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン child.parent.com はドメイン parent.com の子である
- ユーザー mparvinder は child.parent.com で定義されている

ユーザー mparvinder が子ドメインに属しているが、parent.com と一致する Firepower アクセスコントロールポリシーが child.parent.com ドメインの mparvinder と一致しません。

解決策：parent.com または child.parent.com のいずれかのメンバーシップに一致するようにアクセスコントロールポリシー ルールを変更します。

症状：レルムまたはレルム ディレクトリのテストが失敗する

ディレクトリ ページの [テスト (Test)] ボタンは、入力したホスト名または IP アドレスに LDAP クエリを送信します。失敗した場合は、次を確認してください。

- 入力した [ホスト名 (Hostname)] が、LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- 入力した [IP アドレス (IP Address)] が有効である。

レルム設定ページの [AD参加のテスト (Test AD Join)] ボタンは、次のことを確認します。

- DNS が、[ADプライマリドメイン (AD Primary Domain)] を LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- [AD参加ユーザ名 (AD Join Username)] と [AD参加パスワード (AD Join Password)] が正しい。
[AD参加ユーザ名 (AD Join Username)] は完全修飾名である必要があります (たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します)。
- ドメイン内にコンピュータを作成し、ドメインに Secure Firewall Management Center をドメインコンピュータとして参加させるための十分な権限がユーザーにある。

症状：予期しない時間にユーザー タイムアウトが発生する

予期しない間隔でユーザータイムアウトが実行されていることに気付いたら、ISE/ISE-PIC サーバーの時間が Secure Firewall Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザーのタイムアウトが実行される可能性があります。

予期しない間隔でユーザータイムアウトが実行されていることに気付いたら、ISE/ISE-PIC、または TS エージェントサーバーの時間が Secure Firewall Management Center の時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザーのタイムアウトが実行される可能性があります。

症状：未知の ISE/ISE-PIC ユーザーのユーザーデータが Web インターフェイスで表示されない

システムはデータがまだデータベースにない ISE/ISE-PIC または TS エージェントユーザーのアクティビティを検出すると、サーバーからそれらに関する情報を取得します。状況によっては、システムが Microsoft Windows サーバーからこの情報を正常に取得するためにさらに時間がかかることもあります。データ取得が成功するまで、ISE/ISE-PIC または TS エージェントユーザーから見えるアクティビティは Web インターフェイスに表示されません。

これにより、アクセスコントロールルールを使ったユーザートラフィックの処理も妨げられることがある点に注意してください。

症状：イベントのユーザデータが想定外の内容になる

ユーザーやユーザーアクティビティイベントに想定外の IP アドレスが含まれる場合は、レムを確認します。複数のレムに同一の [AD プライマリ ドメイン (AD Primary Domain)] の値を設定することはできません。

症状：ターミナルサーバからログインしたユーザが、システムによって一意に識別されない

導入されている構成にターミナルサーバが含まれ、これに接続されている1つまたは複数のサーバにレムが設定されている場合は、ターミナルサーバ環境でのユーザーログインを正確に報告するため Cisco Terminal Services (TS) エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザーに別個のポートを割り当て、システムはこれらのユーザーを Web インターフェイスで一意に識別できるようになります。

TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

レムまたはユーザーの不一致を検出する

この項では、レムまたはユーザーの不一致を検出する方法について説明します。これらは次のように定義されています。

- ユーザーの不一致：ユーザーは、ダウンロードされることなく Secure Firewall Management Center に報告されます。

ユーザーの不一致の一般的な理由は、ユーザーが Secure Firewall Management Center へのダウンロードから除外されたグループに属していることです。Review the information discussed in [Cisco Secure Firewall Management Center Device Configuration Guide](#).

- レムの不一致：ユーザーが、Firewall Management Center に認識されていないレムに対応するドメインにログインした場合に不一致が起きます。

詳細については、[レムとユーザーのダウンロードをトラブルシューティングする \(68 ページ\)](#) を参照してください。

不明なユーザーアイデンティティルールに一致しないには、ポリシーに適用されていません。(不明ユーザーに対してアイデンティティルールをセットアップすることはできますが、ユーザーとレムを正確に識別することによってルールの数を最小限に保つことをお勧めします。)

手順

ステップ 1 レムまたはユーザーの不一致の検出を有効にします。

- Firewall Management Center にログインしていない場合はログインします。
- System** (🔍) > **Health** > **Policy** をクリックします。
- 新しいヘルス ポリシーを作成するか、または既存のポリシーを編集します。

- d) [ポリシーの編集 (Editing Policy)] ページで、[ポリシーのランタイムの間隔 (Policy Runtime Interval)] を設定します。
これは、すべてのヘルス モニター タスクが実行される頻度です。
- e) 左側のペインで、[レルム (Realm)] をクリックします。
- f) 次の情報を入力します。
 - [有効 (Enabled)] : [オン (On)] をクリックします
 - **警告のユーザーに一致のしきい値 %**: ヘルス モニターに警告をトリガーするレルムの不一致またはユーザーの不一致のいずれかの割合。詳細については、[レルムとユーザーのダウンロードをトラブルシューティングする \(68 ページ\)](#) を参照してください。
- g) ページの下部で [ポリシーを保存して終了 (Save Policy & Exit)] をクリックします。
- h) *Cisco Secure Firewall Management Center Administration Guide* の「*Applying Health Policies*」で説明したように、管理対象デバイスに正常性ポリシーを適用します。

ステップ 2 次の方法のいずれかでユーザーとレルムの不一致を表示します。

- 警告しきい値を超過した場合は、**Firewall Management Center** の上部のナビゲーションで [警告 (Warning)] > [ヘルス (Health)] の順にクリックします。これにより、ヘルス モニターが開きます。
- **System (🔍) > Health > Monitor** をクリックします。

ステップ 3 [ヘルス モニター (Health Monitor)] ページの [表示 (Display)] 列で、[レルム : ドメイン (Realm: Domain)] または [レルム : ユーザー (Realm: User)] を展開し、不一致に関する詳細を表示します。

クロスドメイン信頼をトラブルシューティングする

クロスドメイン信頼の Firewall Management Center 設定のトラブルシューティングに関する一般的な問題は次のとおりです。

- 共有グループを持つすべてのフォレストにレルムまたはディレクトリを追加していない。
- ユーザーをダウンロード対象から除外し、除外したユーザーが別のレルムのグループで参照されるようにレルムを設定します。
- 特定の一時的な問題。

問題を理解する

Firewall Management Center がユーザーとグループを Active Directory フォレストと同期できる問題が存在する場合、次のような [Sync Results (同期結果)] タブページが表示されます。

The screenshot shows the 'Sync Results' page in the Active Directory console. It is divided into three main sections: 'Realms', 'Groups', and 'Users contained in the selected group'. Each section has a search bar and a list of items. In the 'Realms' section, 'forest.example.com' is listed with a yellow triangle icon. In the 'Groups' section, 'CrossForestGroup' and 'EngineersWest' are listed, with 'CrossForestGroup' having a yellow triangle icon. In the 'Users contained in the selected group' section, 'EASTFOREST0\EastMarketing' is listed with a yellow triangle icon. To the right of these sections, there are three error messages, each starting with a yellow triangle icon and providing details about synchronization problems, such as references to users or groups in other domains that have not been synchronized.

次の表で、情報の解釈方法について説明します。

列	意味
[Realms]	システムに設定されているすべてのレルムを表示します。 Refresh (🔄) をクリックして、レルムのリストを更新します。 Yellow Triangle (⚠️) はレルムの問題を示すために表示されます。 すべてのユーザーとグループが正常に同期された場合、レルムの横には何も表示されません。
Groups	[Groups] をクリックして、レルム内のすべてのグループを表示します。レルムと同様、 Yellow Triangle (⚠️) は問題を示すために表示されます。 Yellow Triangle (⚠️) をクリックして、問題の詳細を表示します。
ユーザー	[Users] をクリックして、すべてのユーザーをグループ別にソートして表示します。
選択したグループに含まれるユーザー	[Groups] 列で選択したグループ内のすべてのユーザーを表示します。 Yellow Triangle (⚠️) をクリックすると、テーブルの右側に詳細情報が表示されます。
選択したユーザーを含むグループ	選択したユーザーが属するすべてのグループを表示します。 Yellow Triangle (⚠️) をクリックすると、テーブルの右側に詳細情報が表示されます。

列	意味
エラーの詳細情報 (テーブルの右側に表示)。	<p>同期できなかったNetBIOSフォレスト名とグループ名が表示されます。ユーザーとグループを同期できない一般的な理由は次のとおりです。</p> <ul style="list-style-type: none"> 問題：グループとユーザーを含むフォレストに、Firewall Management Center で設定されている対応するレルムがありません。 <p>解決策：LDAP レルムまたは Active Directory (AD) レルムおよびレルムディレクトリを作成する (32 ページ) の説明に従って、グループを含むフォレストのレルムを追加します。</p> <ul style="list-style-type: none"> 問題：グループを Firewall Management Center へのダウンロード対象から除外しました。 <p>解決策：[Realms] タブページをクリックして、Edit (✎) をクリックし、[Excluded Groups and Users] リストから指定されたグループまたはユーザーを移動します。</p>

ユーザーとグループのダウンロードを再試行してください。

問題が一時的なものである可能性がある場合は、すべてのレルムのユーザーとグループをダウンロードします。

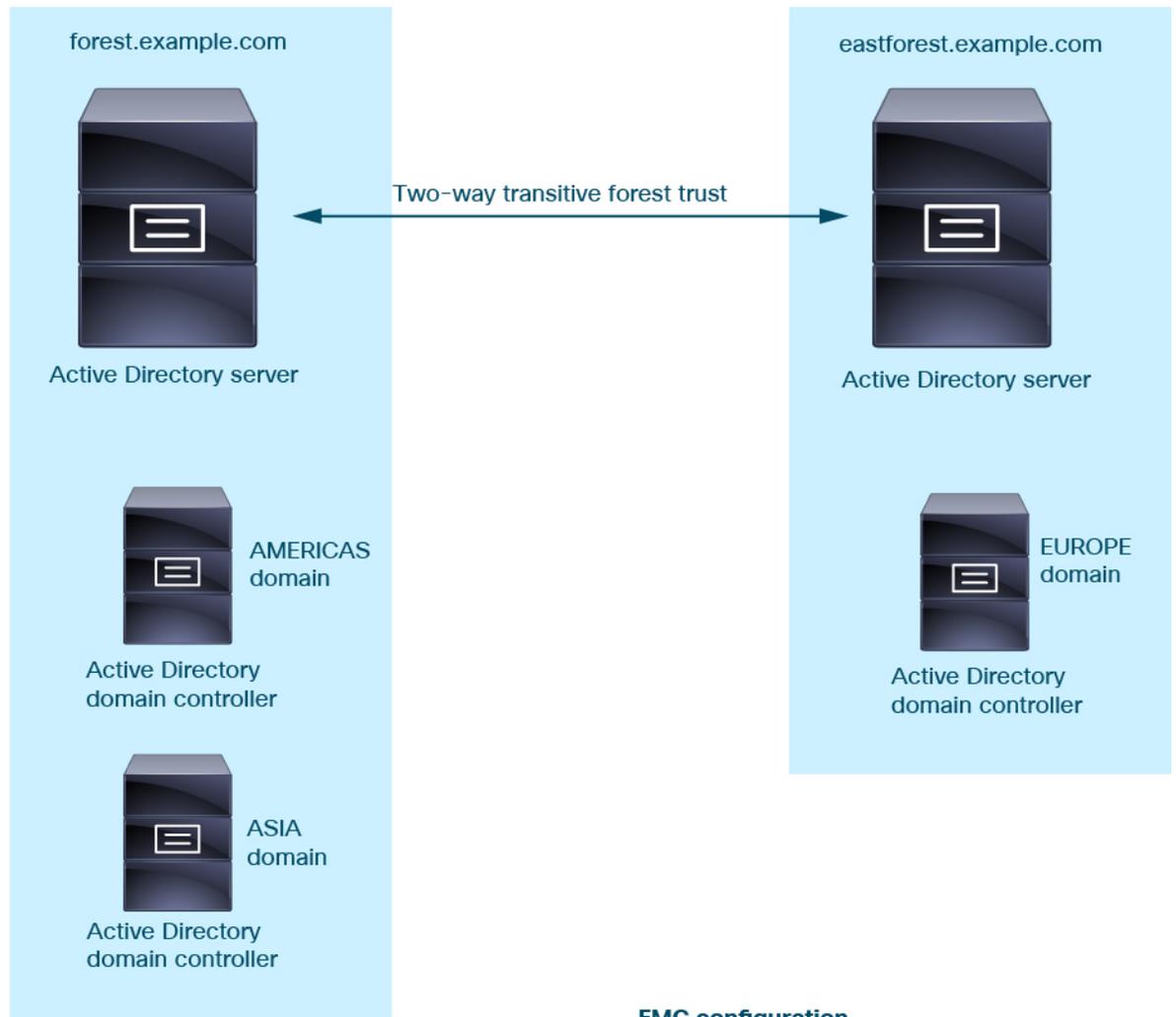
1. まだ Firewall Management Center にログインしていない場合は、ログインします。
2. **Integration > Other Integrations > Realms > Realms** をクリックします。
3. **Download** (↓) をクリックします。
4. [Sync Results] タブページをクリックします。
5. [Realms] 列のエントリに対するインジケータが表示されない場合、問題は解決しています。

すべてのフォレストのレルムを追加する

次の設定を確認します。

- ID ポリシーで使用するユーザーが存在する各フォレストの Firewall Management Center レルム。
- ID ポリシーで使用するユーザーを含むフォレスト内の各ドメインコントローラの Firewall Management Center ディレクトリ。

次の図は例を示しています。



FMC configuration



Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com

Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

レルムの履歴

表 2:

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Microsoft Azure Active Directory (SAML) レルム。	7.6.0	7.4.0	<p>You can now use Microsoft Azure Active Directory (AD) realms for active and passive authentication:</p> <ul style="list-style-type: none"> • Active authentication using Azure AD: Use Azure AD as a captive portal. • Passive authentication using Cisco ISE (introduced in Version 7.4.0): The Firewall Management Center gets groups from Azure AD and logged-in user session data from ISE. <p>We use SAML (Security Assertion Markup Language) to establish a trust relationship between a service provider (the devices that handle authentication requests) and an identity provider (Azure AD).</p> <p>Upgrade impact. If you had a Microsoft Azure AD realm configured before the upgrade, it is displayed as a SAML - Azure AD realm configured for passive authentication. All previous user session data is preserved.</p> <p>New/modified screens: Integration > Other Integrations > Realms > Add Realm > SAML - Azure AD</p> <p>New/modified CLI commands: none</p>
Microsoft Azure Active Directory (AD) レルム。	7.4.0	7.4.0	<p>Microsoft Azure Active Directory (AD) レルムと ISE を使用すると、ユーザーを認証したりユーザー制御のためにユーザーセッションを取得したりできます。</p> <p>新規/変更された画面 : [システム (System)] > [統合 (Integration)] > [レルム (Realms)] > [レルムを追加 (Add Realm)] > [Azure AD]</p>
プロキシシーケンス。	7.2.0	7.2.0	<p>プロキシシーケンスは、レルムシーケンスと同様に、Security Cloud Control が LDAP または Active Directory サーバーと通信できない場合に Security Cloud Control と通信できる、1 つ以上の管理対象デバイスです。</p> <p>新規/変更された画面 : [統合 (Integration)] > [その他の統合 (Other Integrations)] > [レルム (Realms)] > [プロキシシーケンス (Proxy Sequence)]</p>

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Active Directory ドメインのクロスドメイン信頼。	7.2.0	7.0.0	互いに信頼する Microsoft Active Directory (AD) ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザー アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。 Firewall Management Center は、アイデンティティルールのために Active Directory フォレストからユーザーを取得できます。
レルムシーケンス。	7.2.0	6.7.0	レルムシーケンスは、アイデンティティルールを適用する 2 つ以上のレルムの順序付きリストです。レルムシーケンスをアイデンティティポリシーに関連付けると、Firepower システムは、レルムシーケンスで指定されている順序で、最初から最後まで Active Directory ドメインを検索します。 新規/変更された画面：[統合 (Integration)] > [その他の統合 (Other Integrations)] > [レルム (Realms)] > [レルムシーケンス (Realm Sequences)] [システム (System)] > [統合 (Integration)] > [レルム (Realms)] > [レルムシーケンス (Realm Sequences)]
ユーザー制御用のレルム。	7.2.0	すべて	レルムは、Firewall Management Center と、Active Directory または LDAP のユーザーリポジトリ間の接続です。

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。