[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。

レルムとレルムシーケンスについて

レルムとは、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。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。レ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* レルムのみ）。レルムシーケンスは、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ルールに関連付けると、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 ドメインが検索されます。

レ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、同じ基本レルム情報を共有する必要があります。レ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。レルムを有効にすると、保存された変更は次回 Management Centerがサーバに照会するときに適用されます。

ユーザ認識を行うには、レルムがサポートされているサーバーのレ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 のレルムまたはレルムシーケンス

（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 レルムやレルムシーケンスの設定は任意です。

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

- TS エージェント用の Microsoft AD サーバーのレルムまたはレルムシーケンス。
- キャプティブポータルの場合は、LDAP レルム。

  LDAP 用のレ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。 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 レルムおよびレルムディレクトリの作成（20 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、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ルムまたはレ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。

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 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 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、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 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、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 コマンドリファレンスで説明されている **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、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、手動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 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

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。

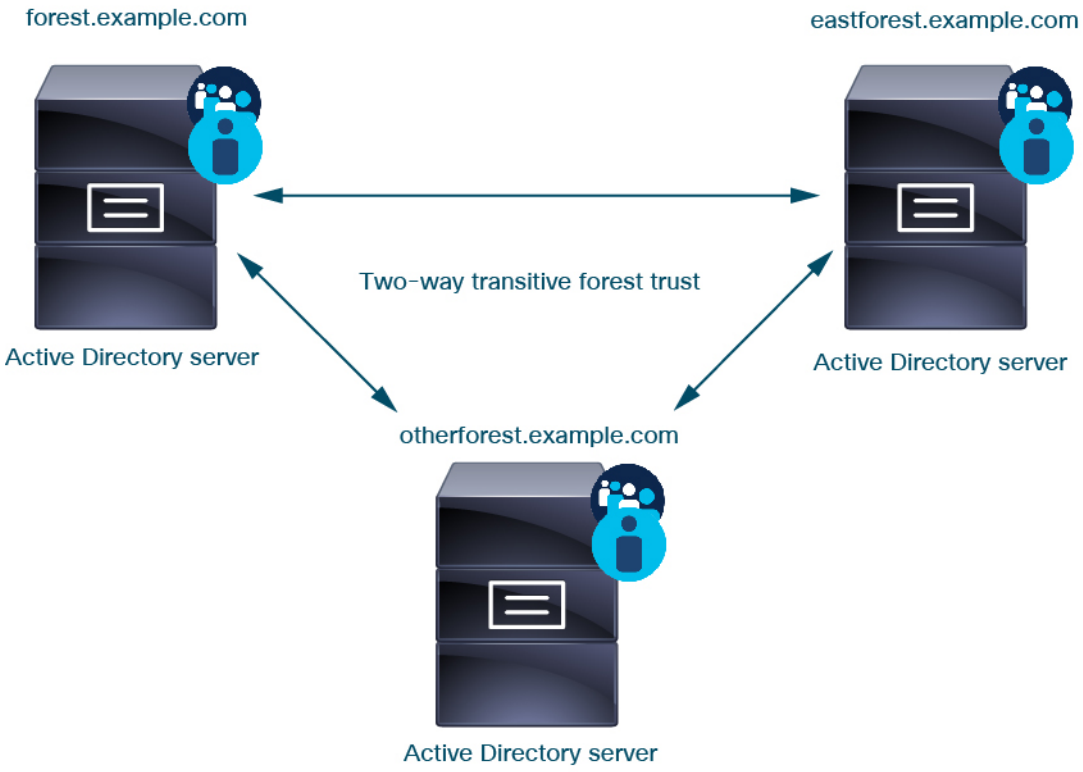
システムと信頼できるドメイン

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。

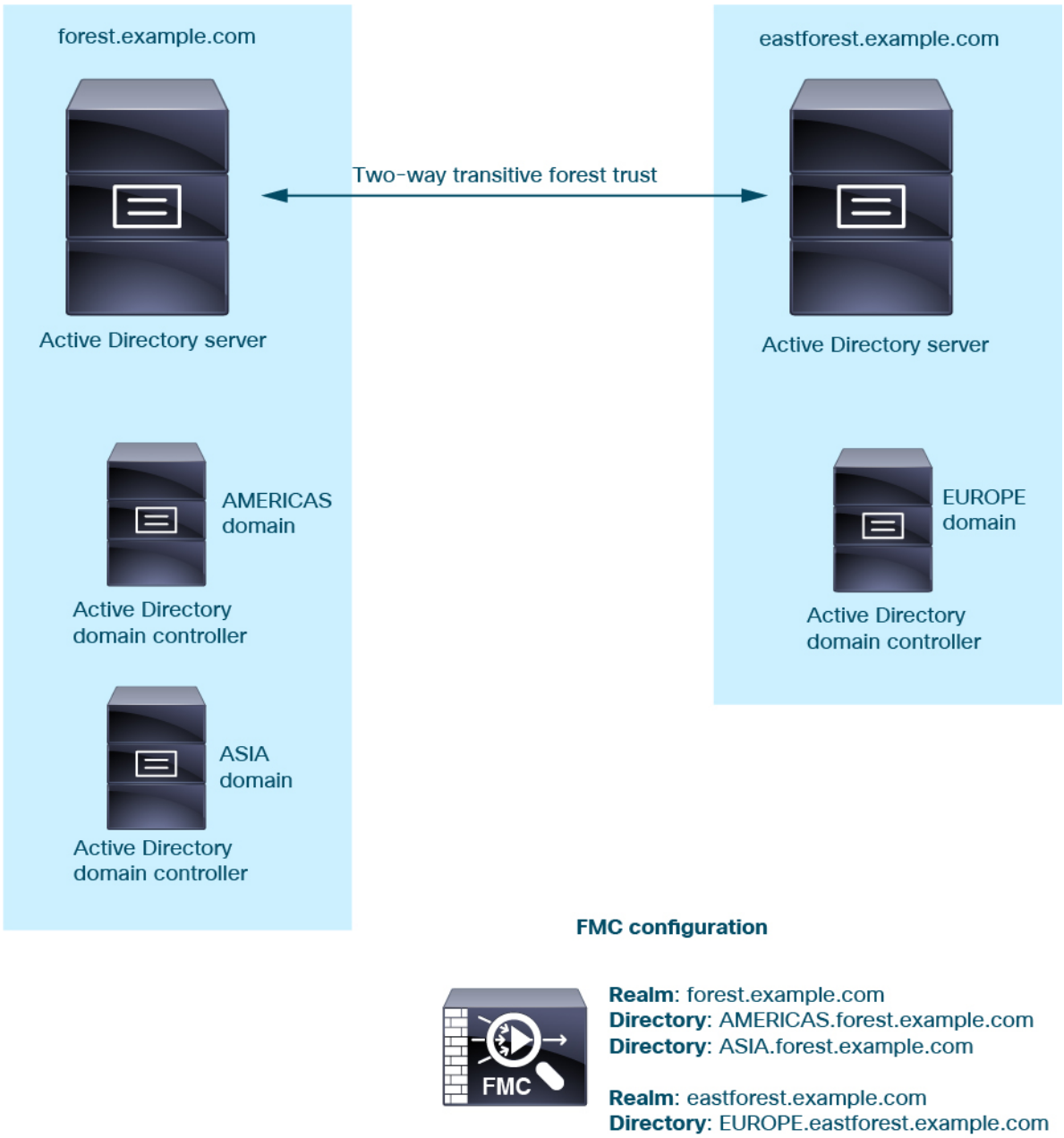
アクセス コントロール ポリシーで使用するユーザーが存在しないドメインには、レルムを設定する必要はありません。

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 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。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 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 Management Center ディレクトリとして設定する必要があります。

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。



前述の例を使用して、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） 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。

レルムが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 タイプに接続すると、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	対応	対応	対応
Microsoft Azure AD	対応	×	×
Linux 上の OpenLDAP	×	×	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、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 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

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、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**）	**Management Center** 属性	**LDAP** オブジェクトクラス	**Active Directory** 属性	**OpenLDAP** 属性
LDAP user name	ユーザ名（Username）	• user • inetOrgPerson	samaccountname	cn uid
first name	名		givenname	givenname
last name	姓		sn	sn
メール アドレス	E メール		メール アドレス userprincipalname（mail に値が設定されていない場合）	メール アドレス
部署	部署名（Department）		部署 distinguishedname（department に値が設定されていない場合）	ou
電話番号	電話		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

レルムのライセンス要件

Threat Defense ライセンス

任意（Any）

従来のライセンス

Control

レルムの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

パッシブ認証用の Microsoft Azure AD レルムの作成

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。Azure AD からグループを取得し、ISE からログイン ユーザー セッション データを取得します。

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 AnyConnect 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、Azure AD とリソース所有者のパスワードクレデンシャルを使用する ISE について （11 ページ）を参照してください。

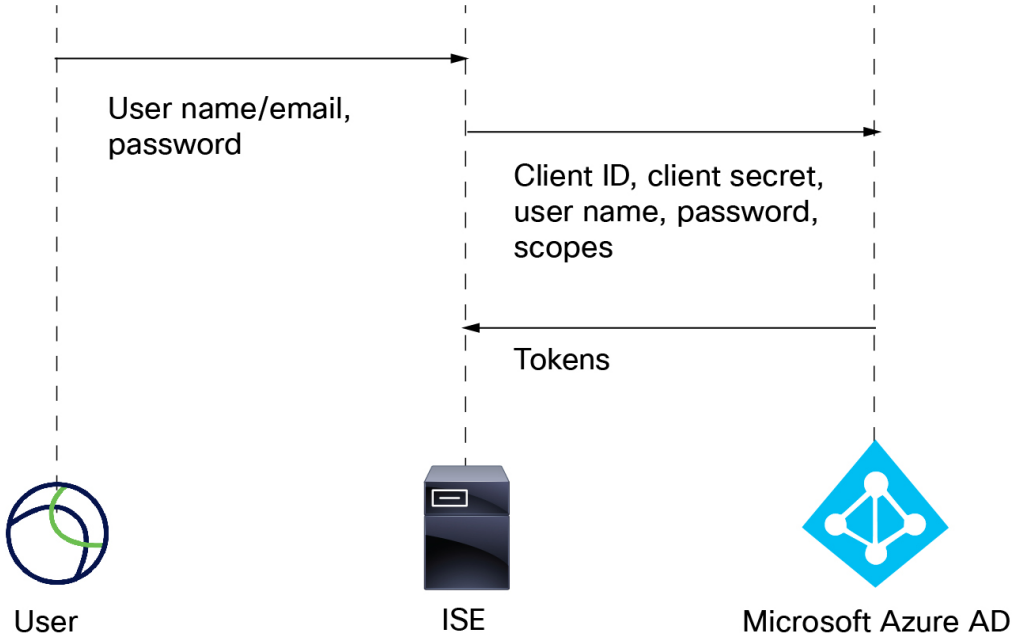
  その他のリソース：Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials（learn.microsoft.com）

- 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）チェーニング、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、Azure AD および ISE と TEAP/EAP-TLS について （12 ページ）を参照してください。

（注） Microsoft Azure AD レルムに関連するポリシーを展開する前に、Microsoft Azure Active Directory レルムのユーザー制限を参照してください。

AzureADとリソース所有者のパスワードクレデンシャルを使用するISEについて

次の図は、ISE とリソース所有者のパスワードクレデンシャル（ROPC）を使用する Azure AD レルム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。

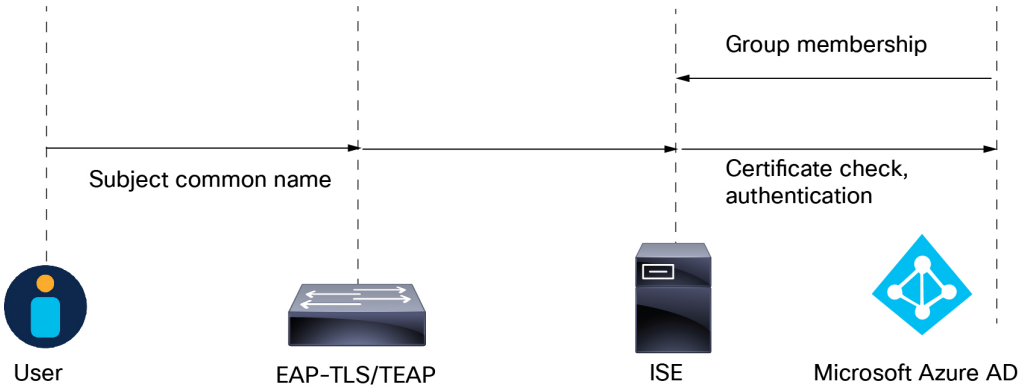
1. ユーザーは、AnyConnect などの VPN クライアントを使用して、ユーザー名（または電子メールアドレス）とパスワードでログインします。
2. クライアント ID、クライアントシークレット、ユーザー名、パスワード、およびスコープが Azure AD に送信されます。
3. トークンは Azure AD から ISE に送信され、ISE はユーザーセッションを Secure Firewall Management Center に送信します。

ISE の設定の詳細については、「Configure ISE 3.0 REST ID with Azure Active Directory」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）

Azure AD および ISE と TEAP/EAP-TLS 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 レルムの作成方法

このトピックでは、Secure Firewall Management Center で使用するパッシブ認証用の レルムを作成するタスクの概要を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Secure 動的属性コネクタ をイネーブルにします。	Cisco Secure 動的属性コネクタ は、 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、Cisco Secure 動的属性コネクタ の有効化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 2	Microsoft Azure AD を設定します。	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。 Microsoft Azure Active Directory の設定（14 ページ） を参照してください。
ステップ 3	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 に ISE を設定する方法 （15 ページ）を参照してください。
ステップ 4	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 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 Azure AD 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。
ステップ 6	レルムを設定して確認します。	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。 Azure AD レルムの作成 （18 ページ）の説明に従って、Microsoft Azure Active Directory レルムを作成します。
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。	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。

次のタスク

Azure AD とリソース所有者のパスワードクレデンシャルを使用する ISE について （11 ページ） を参照してください。

Microsoft Azure Active Directory の設定

このトピックでは、Management Center で使用できるレルムとして Microsoft Azure Active Directory（AD）を設定する方法に関する基本情報を提供します。Azure AD に精通していることを前提としています。そうでない場合は、開始する前にドキュメントまたはサポートリソースを確認してください。

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 Azure AD 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

この権限により、Management Center で最初に Azure AD からユーザーとグループをダウンロードできます。

Management Center で Azure AD レルムを設定するためにこの手順で必要な情報：

- 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。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。

Management Center で Azure AD レルムを設定するためにこの手順で必要な情報：

- 名前空間の名前
- **接続文字列 - 主キー**
- イベントハブ名

Azure AD レルムをセットアップするときに、ポート（**:9093**）をこの名前に付加する必要があります。

- 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。

Azure AD 用に ISE を設定する

ユーザーセッション情報を Management Center に送信するには、「Configure ISE 3.0 REST ID with Azure Active Directory」で説明されているように、Azure AD 用に ISE を設定します。

次の作業

Microsoft Azure AD に ISE を設定する方法 （15 ページ） を参照してください。

Microsoft Azure AD に ISE を設定する方法

Microsoft Azure AD レルムでは、Management Center へのユーザーセッション（ログイン、ログアウト）の送信は ISE で行う必要があります。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。

リソース所有パスワードクレデンシャル認証

リソース オーナー 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）サービスを介して実装された Microsoft Azure AD で ISE を使用する場合は、「Configure ISE 3.0 REST ID with Azure Active Directory」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 レルムに必要な情報の取得 （15 ページ）

Microsoft Azure AD レルムに必要な情報の取得

このタスクでは、Management Center で Microsoft Azure AD レルムをセットアップするために必要な情報を取得する方法について説明します。Microsoft Azure Active Directory の設定 （14 ページ）で説明されているように Microsoft Azure AD をセットアップしたときに、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。

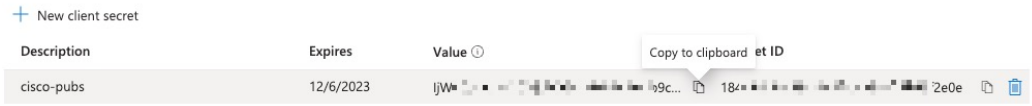
ステップ 6 このページの次の値の横にある [コピー（Copy）]（） をクリックし、それらの値をテキストファイルに貼り付けます。

- **[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。

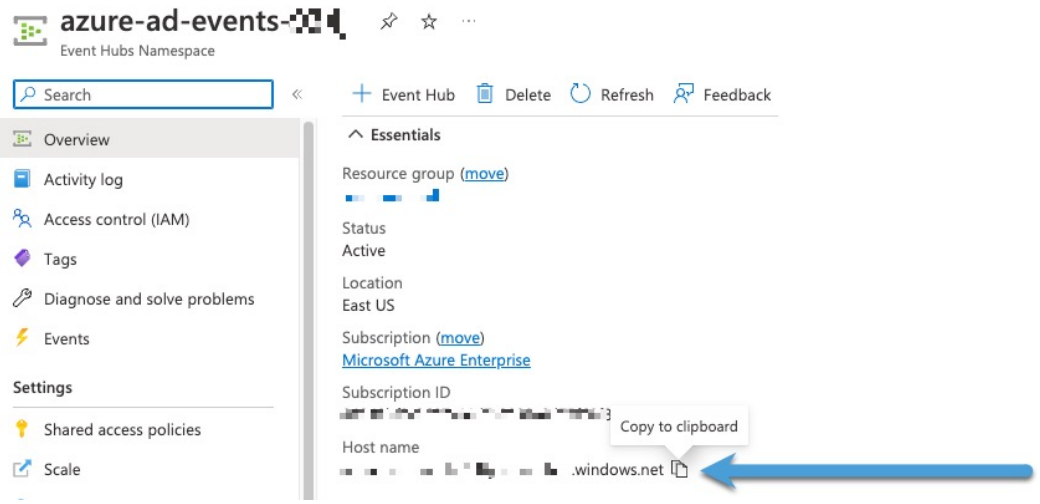
ステップ 8 クライアントシークレット値（クライアントシークレット ID ではありません）がすでにわかっている場合を除き、次のように新しいクライアントシークレットを作成する必要があります。

a) [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。
b) 表示されたフィールドに必要な情報を入力します。
c) [Add] をクリックします。
d) 次の図に示すように、[値（Value）] の横にある [コピー（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 [コピー（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。

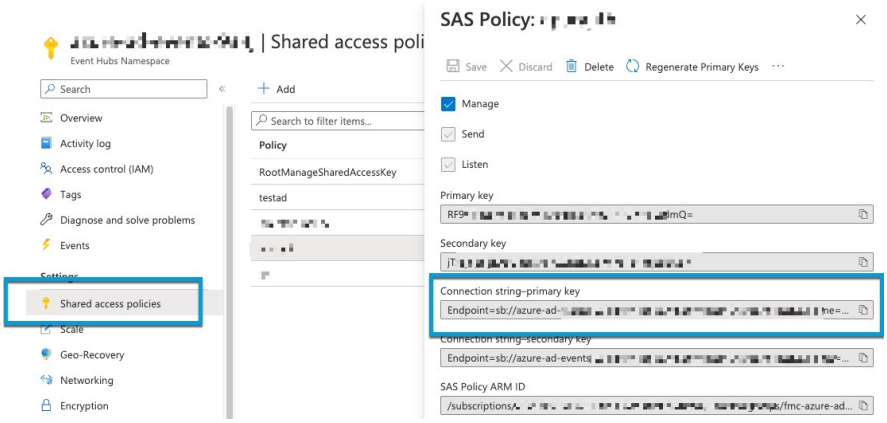


ステップ 11 イベントハブの名前を書き留めるか、テキストファイルにコピーします（ページの上部にある [Event Hubs名前空間（Event Hubs Namespace）] と同じ）。

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。

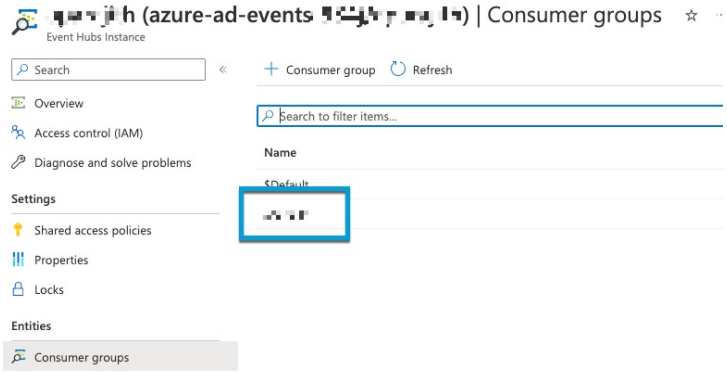
ステップ 13 ポリシーの名前をクリックします。

ステップ 14 [接続文字列-主キー（Connection string-primary key）] の横にある [コピー（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 [コピー（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。

Azure ADレルムの作成

次の手順で、レルム（Management Center と Microsoft Azure AD レルム間の接続）を作成できます。

始める前に

次のタスクをすべて完了します。

- ISE を設定する（Microsoft Azure AD に ISE を設定する方法 （15 ページ）を参照）
- ISE アイデンティティソースを作成する（ISE/ISE-PIC の設定を参照）
- Cisco Secure 動的属性コネクタを有効にする（Cisco Secure 動的属性コネクタ の有効化を参照）
- Azure AD レルムに必要な値を取得する（Microsoft Azure AD レルムに必要な情報の取得（15 ページ）を参照）
- Azure AD を設定する（Microsoft Azure Active Directory の設定 （14 ページ）を参照）

（注） Azure AD レルムを使用してユーザーと ID の制御を実行するには、関連付けられた Azure AD レルムを使用したアクセス コントロール ポリシーのみが必要です。ID ポリシーを作成する必要はありません。

手順

ステップ 1 management center にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** をクリックします。

ステップ 3 新しいレルムを作成するには、**[レルムを追加（Add Realm）]** > **[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	
（任意）**説明**	
Client ID	Microsoft Azure AD レルムに必要な情報の取得（15 ページ）の説明に従って、見つけた情報を入力します。
クライアントのシークレット（Client Secret）	
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）除外するユーザーグループ（Excluded User Groups）	ID 制御のためにユーザーをダウンロードしないグループを 1 つ以上入力します。これらのグループのユーザーは、アクセス コントロール ポリシーで使用できません。 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 5 その他のタスク（レルムの有効化、無効化、削除など）を実行する場合は、レルムの管理（46 ページ）を参照してください。

ステップ 6 Microsoft Azure AD レルムに必要な情報の取得（15 ページ）の説明に従って、見つけた値を入力します。

ステップ 7 [テスト（Test）] をクリックします。

ステップ 8 テストで表示されるエラーを修正します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

基本的なアクセス コントロール ポリシーの作成の説明に従って、アクセス コントロール ポリシーとアクセスコントロールルールを作成します。

（注） Microsoft Azure AD レルムに関連するポリシーを展開する前に、Microsoft Azure Active Directory レルムのユーザー制限を参照してください。

Azure ADのユーザー セッション タイムアウト

ISE/ISE-PIC の Azure AD ユーザー セッション タイムアウトは、Azure AD レルムを編集するときに [ユーザーセッションタイムアウト（User Session Timeout）] ページで使用できます。

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 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）。

LDAP レルムまたは Active Directory レルムおよびレルム ディレクトリの作成

レルムなしで ISE/ISE-PIC を設定する場合は、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 フィールド （24 ページ）を参照してください。

次の手順では、レルム（Management Center と Active Directory レルム間の接続）とディレクトリ（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）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 サーバーのルート証明書のエクスポート （33 ページ）
- Active Directory サーバーの名前の検索 （32 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に、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、Microwoft 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。

レルム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、レルム フィールド（24 ページ）と[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド（29 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ルム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のために Management Center を設定する：セットアップ （37 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） 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。

レルムなしで ISE/ISE-PIC を設定する場合は、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 フィールド （24 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 （24 ページ）。

（注） Microsoft Azure Active Directory は、キャプティブポータルではサポートされていません。

重要 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 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、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。

手順

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

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 3 新しいレルムを作成するには、[レルムの追加（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（レルムの有効化、無効化、削除など）を実行する場合は、レルムの管理（46 ページ）を参照してください。

ステップ 5 レルム フィールド （24 ページ）で説明したように、レルム情報を入力します。

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、[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド （29 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）このレルム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	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、レルム フィールド （24 ページ）を参照してください。
ベース DN（Base DN）	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。
Group DN	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。

[Information]	説明
[Load Groups]	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。 これらのフィールドの詳細については、レルム フィールド （24 ページ）を参照してください。
[Available Groups] セクション	[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。 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。 [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。 詳細については、[レルムディレクトリ（Realm Directory）]および[同期（Synchronize）] フィールド （29 ページ）を参照してください。

ステップ 9 [レルム設定（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、[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド （29 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 レルム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のために Management Center を設定する：セットアップ （37 ページ）
- ユーザーとグループの同期 （35 ページ）
- レルムの編集、削除、有効化、または無効化を行います。レルムの管理 （46 ページ）を参照してください

- レルムの比較 （46 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 アドミニストレーション ガイドの「*Viewing Task Messages*」を参照してください。

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 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。

レルムの設定（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（Name）]

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、レルムがサポートされているサーバー （7 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す。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ことができる必要があります。
- 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。

- Microsoft Active Directory の一部のバージョンでは、ユーザーとグループを読み取るために特定の権限が必要な場合があります。詳細については、Microsoft Active Directory に付属しているマニュアルを参照してください。
- 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。

グループ DN（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 （8 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	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
グループ名	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
ベース DN とグループ DN	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

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（Tterminal Services Agent Users）]：パッシブ認証タイプである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。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（Realm Directory）]および[同期（Synchronize）]フィールド

レルムのディレクトリ フィールド（Realm Directory Fields）

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 サーバーの名前の検索 （32 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 へのセキュアな接続 （32 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 [ホスト名/IP アドレス（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。

ユーザーの [同期（Synchronize）] 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）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）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 （8 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）] 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） 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 へのセキュアな接続

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

- Active Directory 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 Management Center にインポートします。
- Active Directory 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 サーバーのルート証明書のエクスポート （33 ページ）
Active Directory サーバーの名前の検索 （32 ページ）
LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （20 ページ）

Active Directory サーバーの名前の検索

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。

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。

Management Center でレルムディレクトリを設定するときには、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 レルムおよびレルムディレクトリの作成 （20 ページ）。

関連トピック

Active Directory サーバーのルート証明書のエクスポート （33 ページ）

Active Directory サーバーのルート証明書のエクスポート

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 Management Center に安全に接続する際に必要になります。

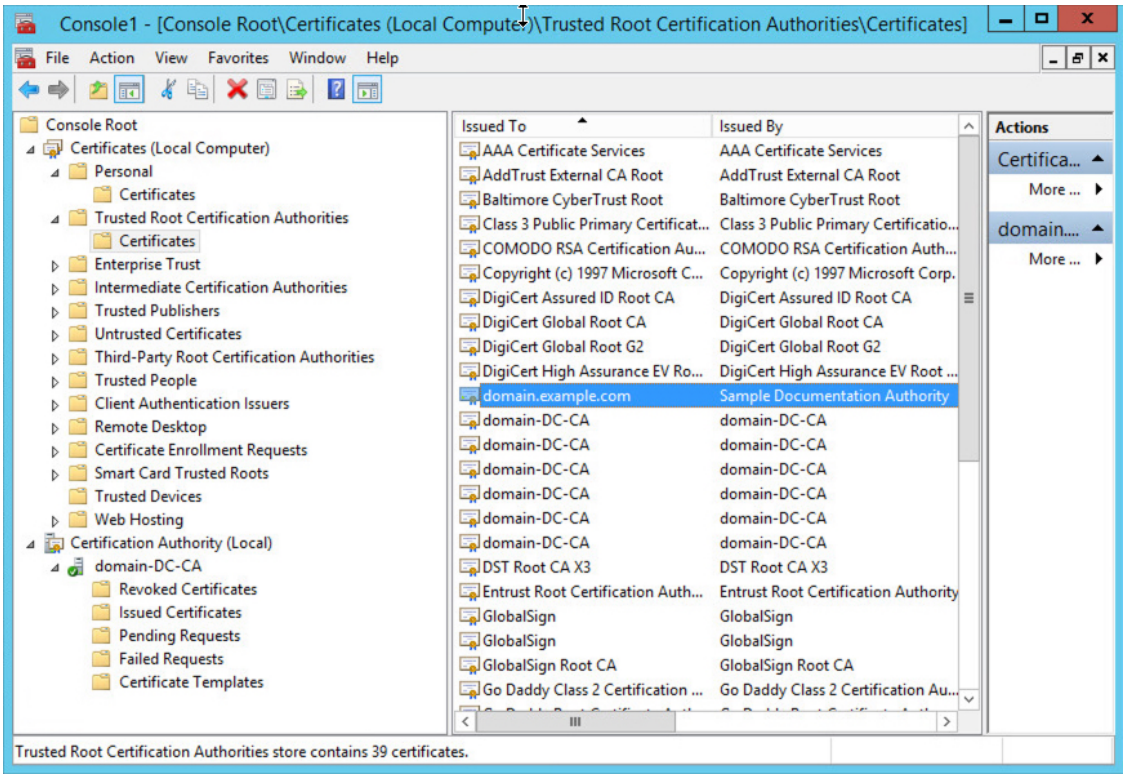
始める前に

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 Management Center に接続できる場合に便利です。

a) [開始（Start）] をクリックして、**cmd** を入力します。

b) **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。

c) **-----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 Management Center にインポートします。

関連トピック

Active Directory サーバーの名前の検索 （32 ページ）

ユーザーとグループの同期

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、Management Centerがクエリを実行することを意味します。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、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 （4 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 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 Management Center ディレクトリを作成します。LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （20 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。 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 レルムおよびレルムディレクトリの作成（20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。

手順

ステップ 1 まだ 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 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** をクリックします。

ステップ 3 各レルムの横にある [ダウンロード（Download）]（ アイコン） 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。

[Realms] 列のインジケータ	意味
[黄色い三角形（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のトラブルシュート（52 ページ）を参照してください。

レルムシーケンスの作成

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 レルムおよびレルムディレクトリの作成（20 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 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 **[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）]** をクリックします。

ステップ 3 [シーケンスを追加（Add Sequence）] をクリックします。

ステップ 4 [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 5 （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 6 [Realms]で、**Add** ( ) をクリックします。

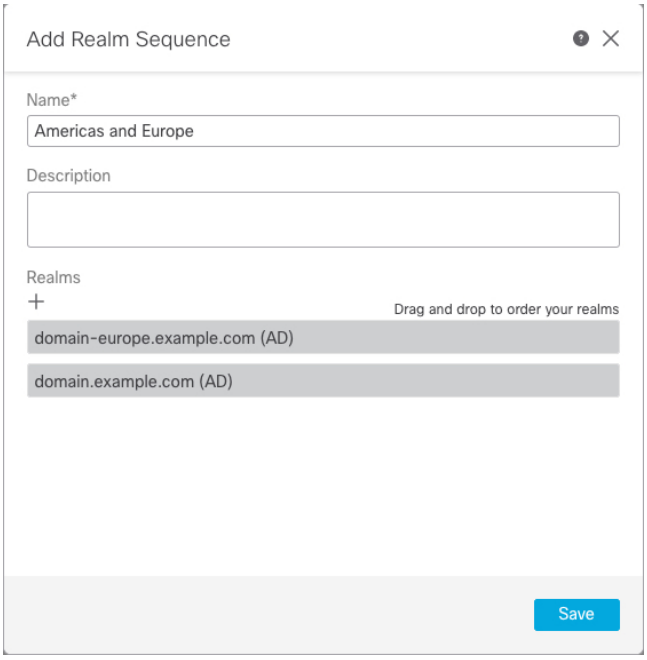
ステップ 7 シーケンスに追加する各レルムの名前をクリックします。

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 8 [OK] をクリックします。

ステップ 9 [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。



ステップ 10 [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のために Management Center を設定する：セットアップ

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 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 レルムにのみ適用されます。Microsoft Azure AD レルム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、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ルムとディレクトリ
- 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ルムとディレクトリ

この例の各レルムには、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=EngineringWest,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

クロスドメイン信頼のために Secure Firewall Management Center を設定する。ステップ 1：レルムとディレクトリの設定 （38 ページ）

クロスドメイン信頼のために Secure Firewall Management Center を設定する。ステップ 1：レルムとディレクトリの設定

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 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のために Management Center を設定する：セットアップ （37 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 （4 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。

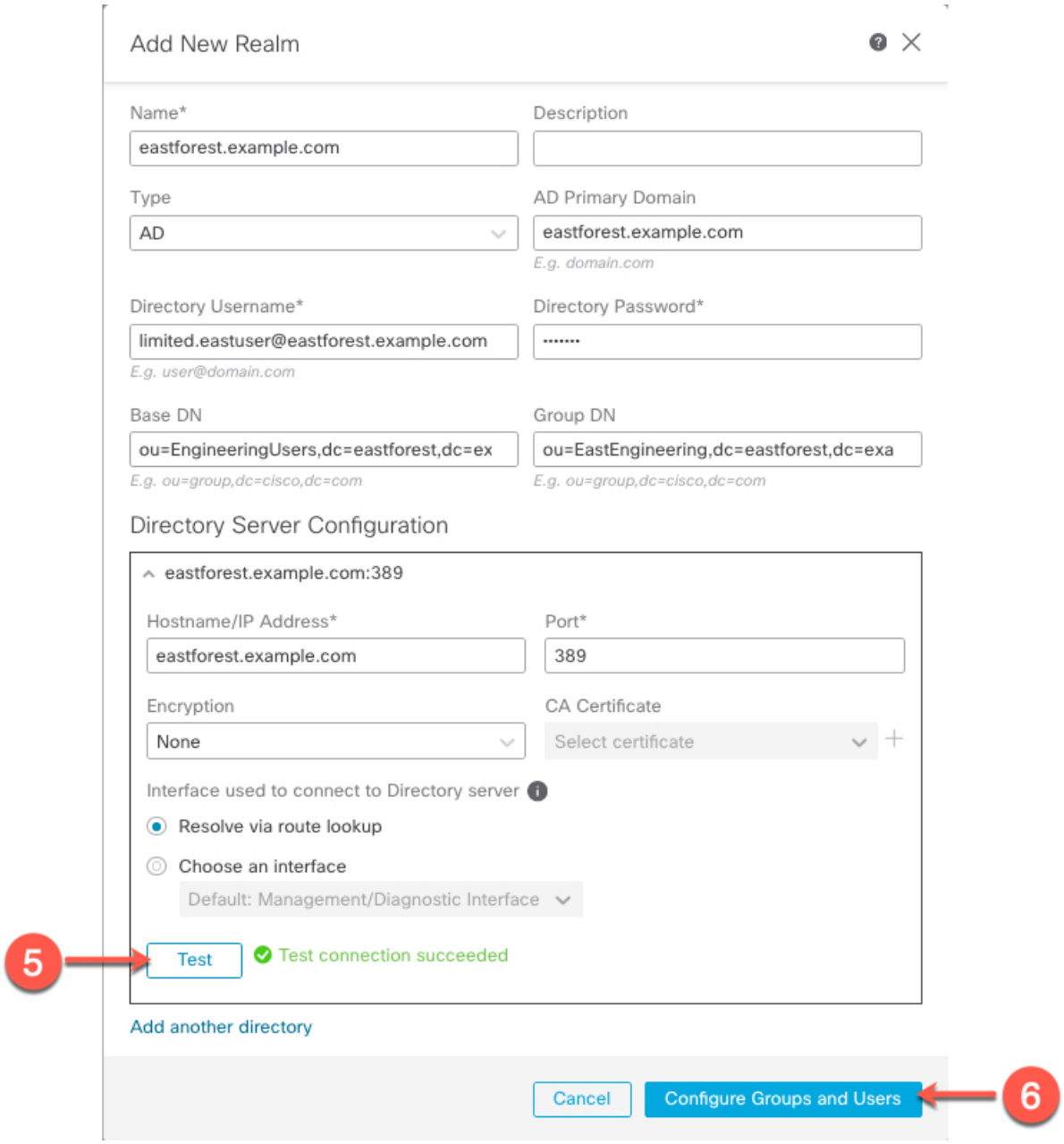
手順

ステップ 1 Management Center にログインします。

ステップ 2 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 3 [レルムの追加（Add Realm）] ドロップダウンリストから選択します。.

ステップ 4 **forest.example.com** を設定するために、次の情報を入力します。



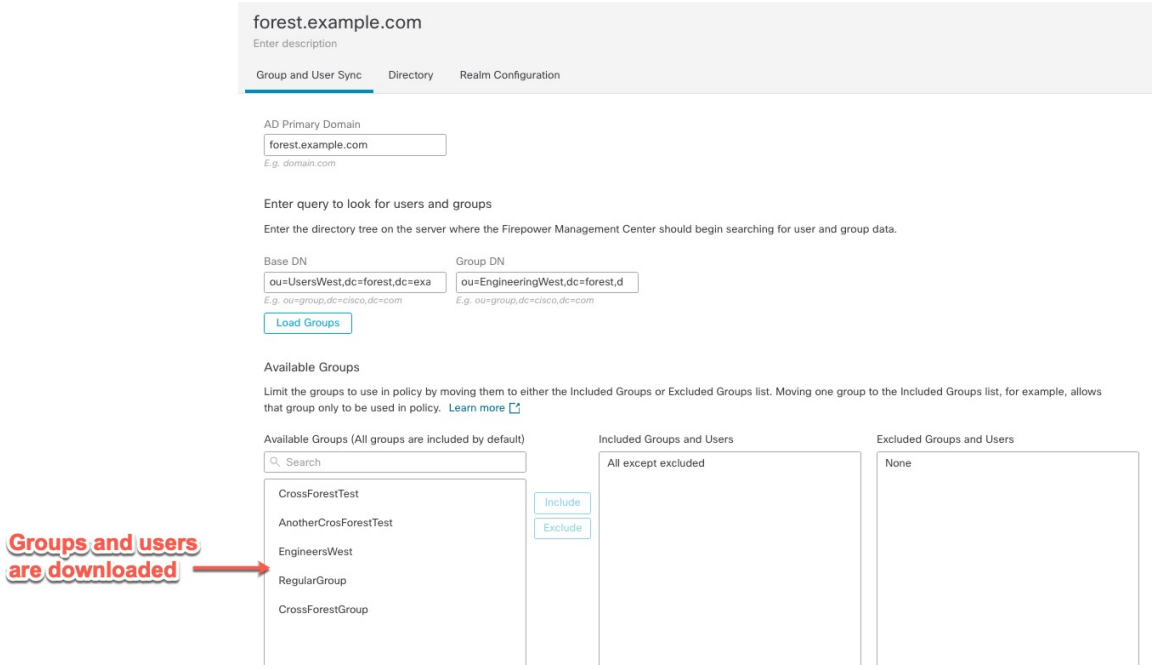
（注） [Directory Username] には、Active Directory ドメイン内の任意のユーザーを指定できます。特別な権限は必要ありません。

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。



（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。

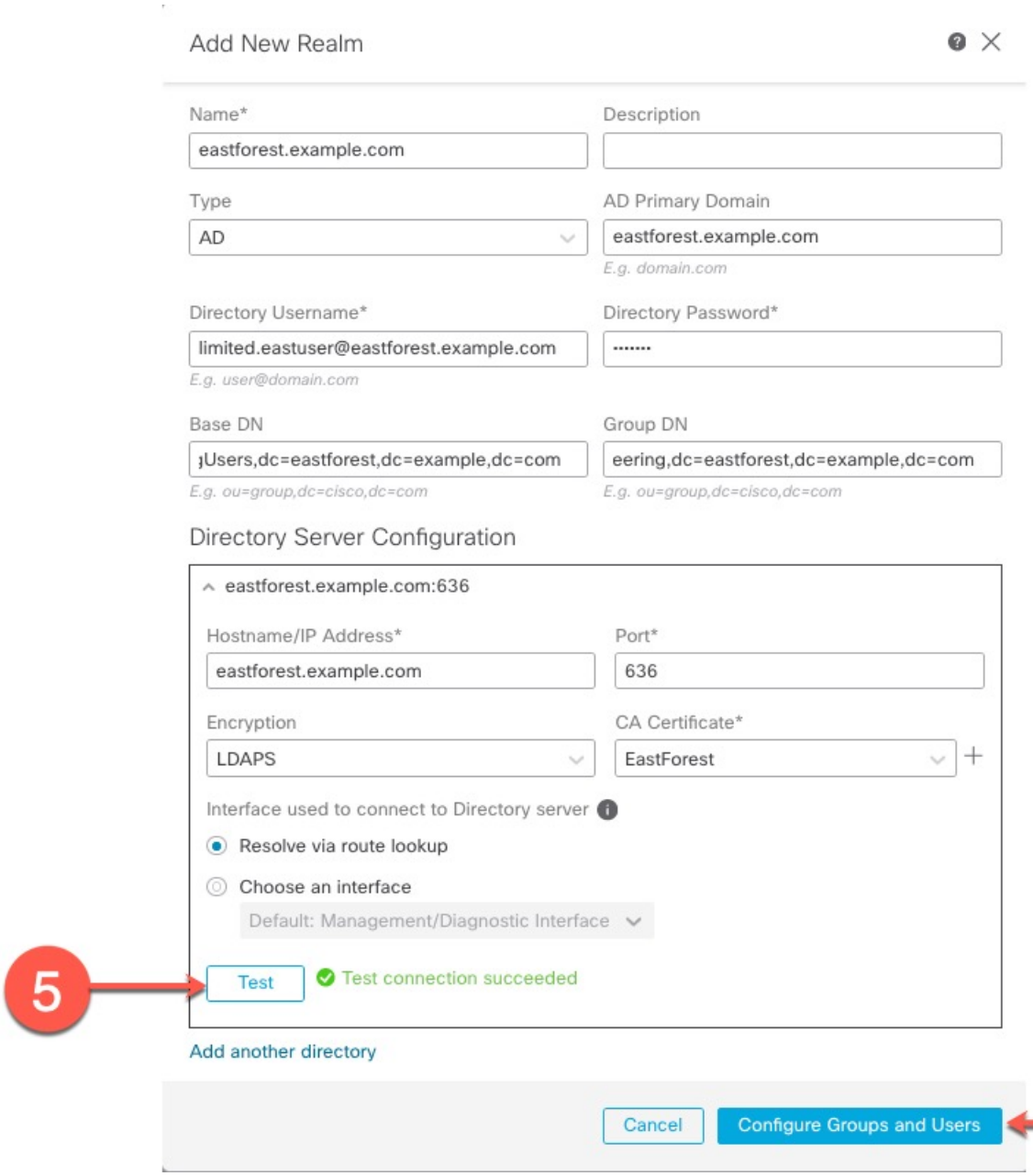
このページでは、その他のオプション設定を使用できます。詳細については、レルムフィールド（24 ページ）および[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド（29 ページ）を参照してください。

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 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）]** をクリックします。

ステップ 10 [レルムを追加（Add Realm）] をクリックします。

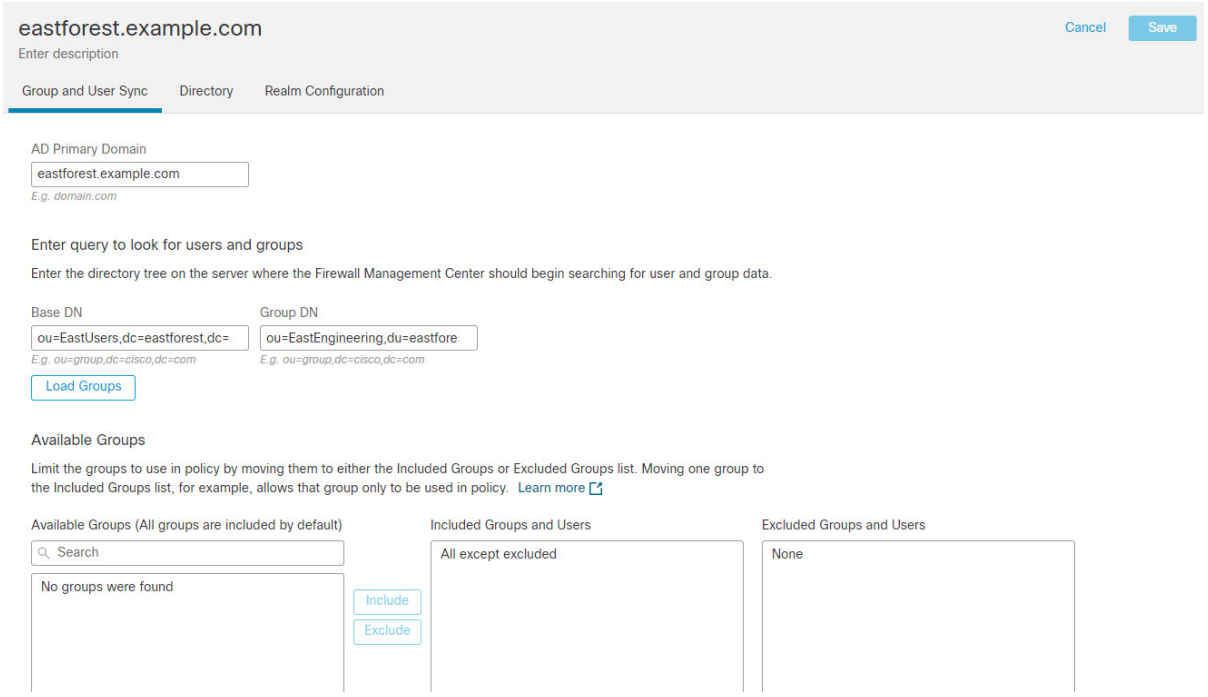
ステップ 11 **eastforest.example.com** を設定するために、次の情報を入力します。



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。



関連トピック

クロスドメイン信頼のための Management Center の設定。ステップ 2：ユーザーとグループの同期 （43 ページ）

クロスドメイン信頼のための Management Center の設定。ステップ 2：ユーザーとグループの同期

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

クロスドメイン信頼のために Secure Firewall Management Center を設定する。ステップ 1：レルムとディレクトリの設定 （38 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 Management Center にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（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、[Yes] をクリックします。

ステップ 4 [チェックマーク（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 フィールド（24 ページ）および[レルムディレクトリ（Realm Directory）] および [同期（Synchronize）] フィールド （29 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 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [同期結果（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のための Management Center の設定。ステップ 3：問題の解決 （44 ページ）

クロスドメイン信頼のための Management Center の設定。ステップ 3：問題の解決

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 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 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 **[統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [同期結果（Sync Results）]** をクリックします。

[Realms] 列で、レルムの名前の横に [黄色い三角形（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。

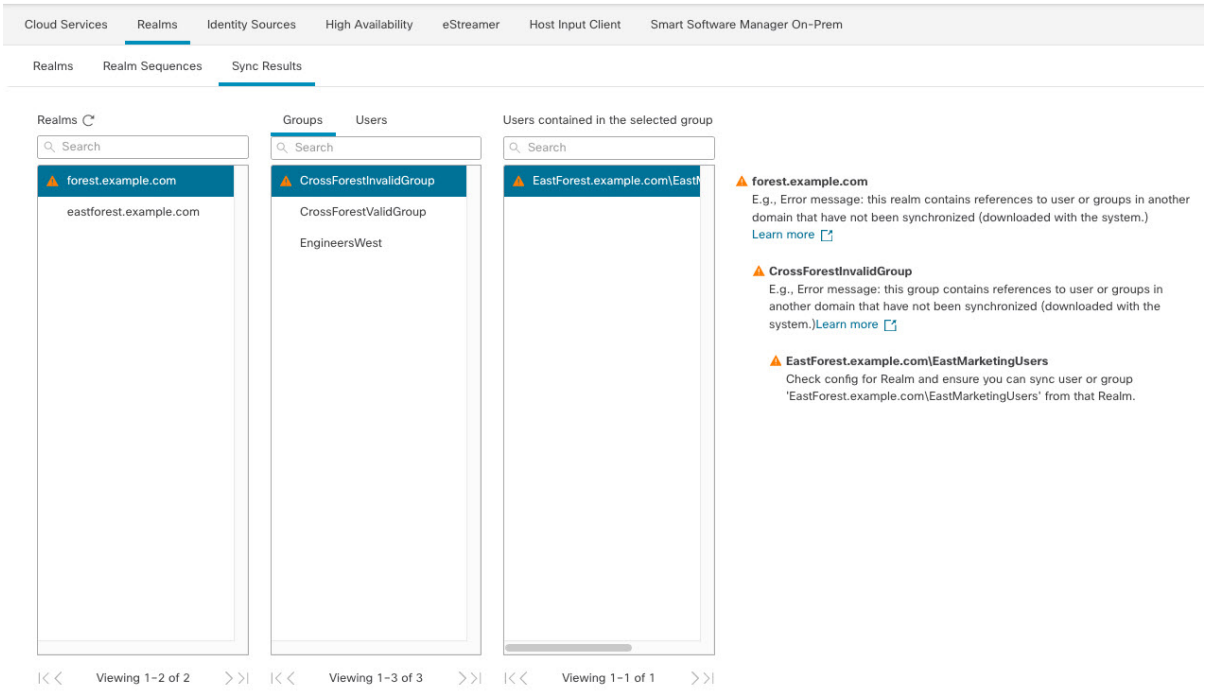
ステップ 4 [Sync Results] タブページをクリックします。

[Realms] カラムに [黄色い三角形（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 [黄色い三角形（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、[黄色い三角形（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。



前述の例では、**forest.example.com** には、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、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。

レルムの管理

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 [表示（View）]（） が表示される場合、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 まだ 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 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** をクリックします。

ステップ 3 レルムを削除するには、[削除（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 **[編集（Edit）]**（） をクリックし、LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （20 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、[ダウンロード（Download）]（アイコン） をクリックします。

ステップ 7 レルムをコピーするには、[コピー（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、レルムの比較 （46 ページ）を参照してください。

レルムの比較

このタスクを実行するには、管理者、アクセス管理者、ネットワーク管理者、またはセキュリティ承認者である必要があります。

手順

ステップ 1 Management Center にログインします。

ステップ 2 **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（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、レルム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、新しいレルム比較ビューを生成します。

レルムとユーザーのダウンロードのトラブルシュート

予期しないサーバー接続の動作に気付いたら、レルム設定、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。

- 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: レルム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

Management Center のヘルスモニターは、ユーザーまたはレルム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 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 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 デバイス構成ガイド.

- レルムの不一致：ユーザーが、Management Center に認識されていないレル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。

たとえば、Management Center で **domain.example.com** というドメインに対応するレルムを定義していても、**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、これはレルムの不一致となります。このドメイン内のユーザーは 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すが、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の検出 （51 ページ）を参照してください。

症状：ユーザ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 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 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、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と、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、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 `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 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 `mparvinder` は `child.parent.com` で定義されている

ユーザ `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 サーバーまたは 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 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

ユーザやユーザ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、レルムを確認します。複数のレルムに同一の [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ーが含まれ、これに接続されている 1 つまたは複数のサーバーにレルムが設定されている場合は、ターミナルサーバー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。

レルムまたはユーザーの不一致の検出

この項では、レル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 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 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 デバイス構成ガイド.

- レルムの不一致：ユーザーが、Management Center に認識されていないレル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、レルムとユーザーのダウンロードのトラブルシュート （47 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。）

手順

ステップ 1 レルムまたはユーザーの不一致の検出を有効にします。

a) Management Center にログインしていない場合はログインします。
b) **[System]** > **[Health]** > **[Policy]** をクリックします。
c) 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のトラブルシュート （47 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 アドミニストレーション ガイドの「*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、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。
- **[システム（System）] > [ヘルス（Health）] > [モニタ（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。

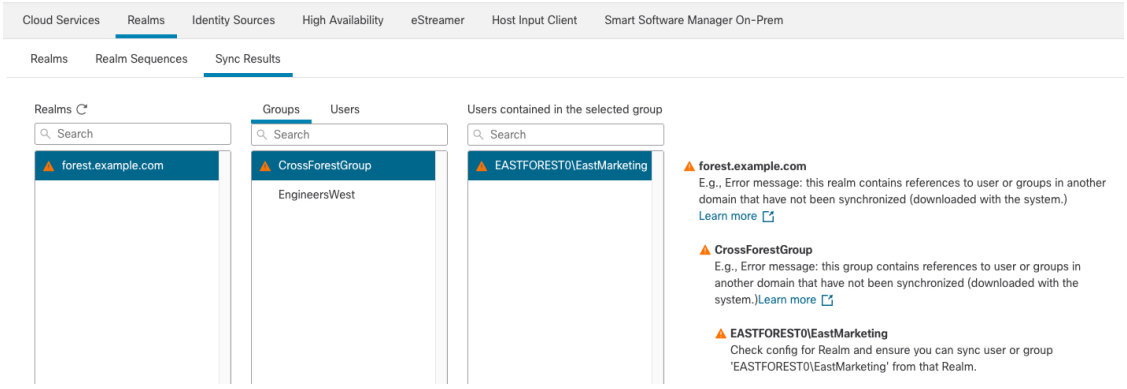
クロスドメイン信頼のトラブルシュート

クロスドメイン信頼の 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

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。



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。**[更新（Refresh）]**（） をクリックして、レルムのリストを更新します。 [黄色い三角形（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、[黄色い三角形（Yellow Triangle）]（） は問題を示すために表示されます。 [黄色い三角形（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。[黄色い三角形（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。[黄色い三角形（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）。	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。 • 問題：グループとユーザーを含むフォレストに、Management Centerで設定されている対応するレルムがありません。 解決策：LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成 （20 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。 • 問題：グループを Management Center へのダウンロード対象から除外しました。 解決策：[Realms] タブページをクリックして、**[編集（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。

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。

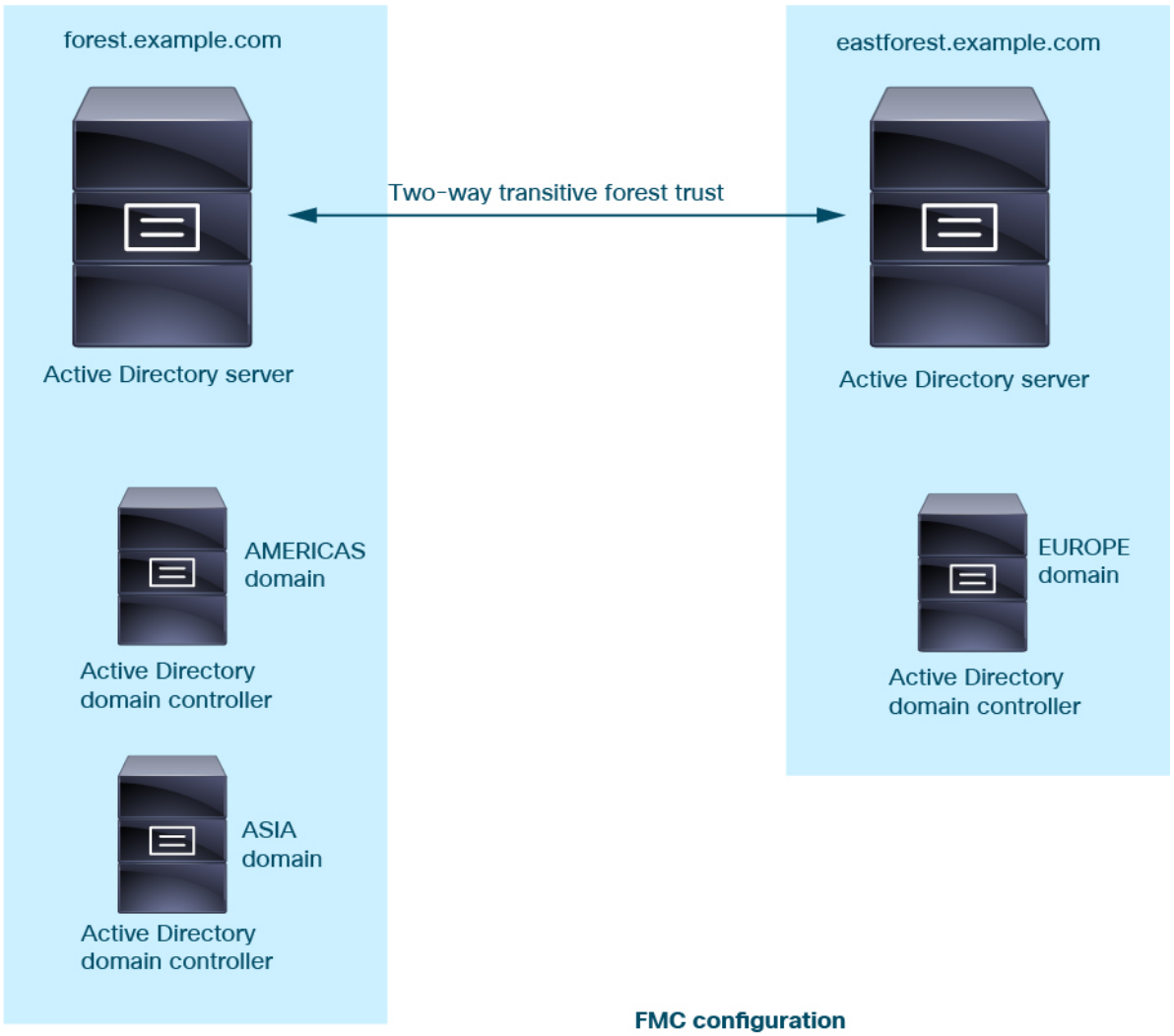
1. まだ Management Center にログインしていない場合は、ログインします。
2. **[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[レルム（Realms）]** をクリックします。
3. [ダウンロード（Download）]（⬇ アイコン） をクリックします。
4. [Sync Results] タブページをクリックします。
5. [Realms] 列のエントリに対するインジケータが表示されない場合、問題は解決しています。

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 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 Management Center ディレクトリ。

次の図は例を示しています。


forest.example.com
eastforest.example.com
Two-way transitive forest trust
Active Directory server
Active Directory server
AMERICAS
domain
Active Directory
domain controller
EUROPE
domain
Active Directory
domain controller
ASIA
domain
Active Directory
domain controller
FMC configuration
FMC
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

機能	最小 Management Center	最小 Threat Defense	詳細
Microsoft Azure Active Directory（AD）レルム。	7.4.0	7.4.0	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。 新規/変更された画面：**システム**（⚙）> **[統合（Integration）]** > **[レルム（Realms）]** > **[レルムの追加（Add Realm）]** > **[Azure AD]**
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。 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）]**
ユーザー制御用のレルム。	7.2.0	任意（Any）	レルムは、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。