



レルムとアイデンティティ ポリシー

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。

- [レルムとアイデンティティ ポリシーについて \(1 ページ\)](#)
- [レルムの作成 \(11 ページ\)](#)
- [アイデンティティ ポリシーの作成 \(19 ページ\)](#)
- [アイデンティティ ルールの作成 \(20 ページ\)](#)
- [レルムの管理 \(24 ページ\)](#)
- [アイデンティティ ポリシーの管理 \(26 ページ\)](#)
- [アイデンティティ ルールの管理 \(27 ページ\)](#)

レルムとアイデンティティ ポリシーについて

レルムは、同じディレクトリ クレデンシャルを共有する 1 つ以上の LDAP または Microsoft Active Directory サーバで構成されます。ユーザおよびユーザ グループ クエリやユーザ制御を実行したり、権限のあるアイデンティティ ソースを設定したりするには、レルムを設定する必要があります。1 つ以上のレルムを設定すると、アイデンティティ ポリシーを設定できます。

アイデンティティ ポリシーは、ネットワーク上のトラフィックを権限のあるアイデンティティ ソースおよびレルムと関連付けます。1 つ以上のアイデンティティ ポリシーを設定した後、1 つをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを管理対象デバイスに展開できます。

レルムについて

レルムとは、Firepower Management Center とモニタリング対象のサーバ上にあるユーザ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するユーザとユーザ グループを指定する。
- 権限のあるユーザ、および権限のあるユーザ以外の一部のユーザ（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、およびトラフィック ベースの検出、ユーザ

エージェント、TS エージェント、ISE によって検出されたユーザ) のユーザ メタデータについてユーザ リポジトリに照会する。

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 Firepower 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、[レールムがサポートされているサーバ](#)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 ユーザに関連するデータについてサーバにクエリし、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、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メールアドレスが同じユーザの 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 ユーザのメタデータをそのユーザに関連付けます。

ユーザ制御を実行するために以下のいずれかを設定できます。

- ユーザ エージェントまたは ISE 用の AD サーバのレールム



(注) SGTISE 属性条件を設定することを計画しているものの、ユーザ、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の設定は計画していない場合、レールムの設定はオプションです。

- TS エージェント用の AD サーバのレールム
- キャプティブ ポータル用の AD、Oracle Directory、OpenLDAP サーバのレールム

ユーザ ダウンロードについて

特定の検出されたユーザの、次のユーザとユーザ グループのメタデータを取得するために、Firepower Management Center と LDAP サーバまたは AD サーバとの間の接続を確立するためのレールムを設定することができます。

- キャプティブ ポータルで認証された、あるいはユーザ エージェントまたは ISE で報告された LDAP および AD ユーザ。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 ログイン (ユーザが LDAP または AD ユーザ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。

レールム内のディレクトリとして、LDAP サーバまたは Active Directory ドメイン コントローラ 接続を設定します。ユーザ認識とユーザ制御のためにレールムのユーザおよびユーザ グループ データをダウンロードするには、[アクセス コントロールのためのユーザおよびユーザ グループのダウンロード (Download users and user groups for access control)] をオンにする必要があります。

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

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

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の最大数は Firepower 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、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ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。



- (注) ユーザリポジトリからシステムによって検出されたユーザを削除しても、Firepower Management Center はユーザ データベースからそのユーザを削除しません。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、Firepower Management Center が次に権限のあるユーザのリストを更新したときにアクセス コントロール ルールに反映されます。

レールムおよび信頼できるドメイン

Firepower Management Center でレールムを設定すると、そのレールムは 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。

Firepower システムは、信頼できる AD ドメインをサポートしていません。つまり、Firepower システムは、どのドメインが互いに信頼しているかを追跡せず、どのドメインが互いの親ドメインまたは子ドメインかを認識しません。また、Firepower システムでは、信頼関係が Firepower システム外で実施される場合でも、クロスドメイン信頼を使用する環境のサポートを保証するテストがまだ行われていません。

詳細については、[レلمとユーザのダウンロードのトラブルシュート（7ページ）](#)を参照してください。

レلمがサポートされているサーバ

レلمを設定して次のサーバタイプに接続すると、Firepower Management CenterからのTCP/IPアクセスを提供できます。

サーバタイプ (Server Type)	ユーザ認識によるデータ取得のサポート	ユーザエージェントによるデータ取得のサポート	ISE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 2008 と Windows Server 2012 上の Microsoft Active Directory	○	○	○	○	○
Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0	○	×	○	×	○
Linux 上の OpenLDAP	○	×	×	×	○



(注) TS エージェントが別のパッシブ認証 ID ソース（ユーザエージェントまたはISE）と共有されている Windows サーバ上の Microsoft Active Directory にインストールされている場合、Firepower 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 Firepower Management Center に記録されます。

サーバグループの設定に関して次の点に注意してください。

- ユーザグループまたはグループ内のユーザに対してユーザ制御を実行するには、LDAP または Active Directory サーバでユーザグループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、Firepower Management Center はユーザグループ制御を実行できません。
- 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。

- サーバ上のサブグループのメンバーであるユーザを含む（または除外する）Active Directory レールムを設定するには、Windows Server 2008 または 2012 では、Active Directory のグループあたりのユーザ数が 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 サーバの設定を変更できます。

- ターミナル サービス環境でサーバにより報告されるユーザ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に別個のポートを割り当て、Firepower System はこれらのユーザを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。

サポートされているサーバオブジェクト クラスと属性名

Firepower 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、レールム内のサーバが、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、Firepower 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: Firepower 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	Oracle Directory Server 属性	OpenLDAP 属性
LDAP user name	[ユーザ名 (Username)]	ユーザまたは inetOrgPerson	samaccountname	cn uid	cn uid
first name	名		givenname	givenname	givenname
last name	姓		sn	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	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)	部署	ou
電話番号	電話		telephonenumber	適用対象外	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」
- Oracle :
 - オブジェクトクラス : [docs.oracle.com](#) の「LDAP Object Class Reference」
 - 属性 : [docs.oracle.com](#) の「LDAP Attribute Reference」
- OpenLDAP : [RFC 4512](#)

レームとユーザのダウンロードのトラブルシューティング

予期しないサーバ接続の動作に気付いたら、レーム設定、デバイス設定、またはサーバ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。

- [ユーザ 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](#)
- [ISE アイデンティティ ソース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](#)
- [ユーザ制御のトラブルシューティング](#)

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、Firepower 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 mparvinder はグループ A に属しているが、メンバーシップ グループ A を指定する Firepower 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لمまたはレلم 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لم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 Firepower 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にある。

症状：予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザ タイムアウトが実行されていることに気付いたら、ユーザ エージェント、ISE、TS エージェント サーバの時間が Firepower 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のタイムアウトが実行される可能性があります。

症状：レلم設定で指定したようにユーザが含まれない、または除外されない

サーバのサブグループのメンバーであるユーザを選別できる Active Directory レلمを設定する際は、Microsoft Windows サーバが報告するユーザの数を以下に制限することに注意します。

- Windows サーバ 2008 または 2012 では、グループごとに 5000 ユーザまで。Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0

必要に応じて、より多くのユーザ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サーバの設定を変更できます。

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لمの [タイプ (Type)] が正しく設定されていない場合は、FirePOWER 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لمの [タイプ (Type)] を [LDAP] として設定すると、FirePOWER 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：レールムの [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。

症状：未知の ISE とユーザ エージェントのユーザのユーザ 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、ユーザエージェントまたは TS エージェントユーザのアクティビティを検出すると、サーバ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、ユーザエージェント、TS エージェントユーザ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、アクセス制御ルールを使ったユーザ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ます。

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、レールムを確認します。複数のレールムに同一の [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ール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に別個のポートを割り当て、Firepower System はこれらのユーザを 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。

アイデンティティ ポリシーについて

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

このトピックの最後に記載されている例外を除き、使用する予定のレムと認証方式を、アイデンティティ ルールで起動する前に設定する必要があります。

- [システム (System)] > [統合 (Integration)] > [レム (Realms)] でアイデンティティ ポリシー外のレムを設定します。詳細については、[レムの作成 \(11 ページ\)](#) を参照してください。
- パッシブ認証のアイデンティティ ソースであるユーザ エージェントと ISE は、[システム (System)] > [統合 (Integration)] > [アイデンティティ ソース (Identity Sources)] で設定します。詳細については、[ユーザ制御のためのユーザエージェントの設定およびユーザ制御用 ISE の設定](#) を参照してください。
- パッシブ認証のアイデンティティ ソースである TS エージェントについては、Firepower システムの外で設定します。詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。
- アクティブ認証のアイデンティティ ソースであるキャプティブ ポータルについては、アイデンティティ ポリシー内で設定します。詳細については、[ユーザ制御のためのキャプティブ ポータルの設定方法](#) を参照してください。

単一のアイデンティティ ポリシーに複数のアイデンティティ ルールを追加した後、ルールの順番を決めます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールがそのトラフィックを処理するルールです。

1つ以上のアイデンティティ ポリシーを設定した後、1つのアイデンティティ 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があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致する場合、システムはトラフィックを指定されたレムと関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザを認証します。

アイデンティティ ポリシーを設定しない場合、システムはユーザ認証を実行しません。

アイデンティティ ポリシーの作成に関する例外

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ (SGT) を使用します。詳細については、[ISE SGT とカスタム SGT ルール条件との比較](#) を参照してください。

関連トピック

[ユーザ アイデンティティ ソース](#)

レムの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、Access Admin、Network Admin

レム設定フィールドの詳細については、[レム フィールド \(12 ページ\)](#) を参照してください。



- (注) すべての Microsoft Active Directory (AD) レムに固有の [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 AD レムに同じ [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ム内のすべてのユーザとグループに 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。

手順

- ステップ 1 Firepower Management Center にログインします。
- ステップ 2 [システム (System)] > [統合 (Integration)] をクリックします。
- ステップ 3 [レム (Realms)] をクリックします。
- ステップ 4 新しいレムを作成するには、[新規レム (New Realm)] をクリックします。
- ステップ 5 その他のタスク (レムの有効化、無効化、削除など) を実行する場合は、[レムの管理 \(24 ページ\)](#) を参照してください。
- ステップ 6 [レム フィールド \(12 ページ\)](#) で説明したように、レム情報を入力します。
- ステップ 7 [OK] をクリック
- ステップ 8 [レム ディレクトリの設定 \(16 ページ\)](#) で説明したように、少なくとも 1 つのディレクトリを設定します。
- ステップ 9 [ユーザとグループのダウンロード \(17 ページ\)](#) の説明に従って、(アクセス コントロールに必要な) ユーザとユーザ グループのダウンロードを設定します。
- ステップ 10 [レム設定 (Realm Configuration)] タブをクリックします。
- ステップ 11 [認証済みユーザ (Authenticated Users)]、[認証に失敗したユーザ (Failed Authentication Users)]、および [ゲストユーザ (Guest Users)] のユーザ セッション タイムアウト値を分単位で入力します。

次のタスク

- [レルム ディレクトリの設定 \(16 ページ\)](#)
- 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 \(24 ページ\)](#) を参照してください
- [レルムの比較 \(25 ページ\)](#)。
- 必要に応じて、タスクのステータスをモニタします ([タスク メッセージの表示](#) を参照)。

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。英数字や特殊文字に対応しています。

説明

(オプション) レルムの説明を入力します。

AD プライマリ ドメイン (AD Primary Domain)

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



- (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 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。

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

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 ユーザの識別用のユーザ名とパスワード。

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ない必要があります。
- 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）。

アイデンティティ ルールの [認証タイプ (Authentication Type)] に **Kerberos** を選択する場合（または Kerberos をオプションとして **HTTP Negotiate** を選択する場合）、Kerberos キャプティブ ポータル アクティブ認証を実行するには、[アクティブディレクトリ参加ユーザ名 (AD Join Username)] と [アクティブディレクトリ参加パスワード (AD Join Password)] を使用して、選択した [レールム (Realm)] を設定する必要があります。

[ディレクトリ ユーザ名 (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 では、ユーザに昇格された特権は必要ありません。ドメイン内の任意のユーザを指定できます。
- OpenLDAP では、ユーザのアクセス権限は、[OpenLDAP の仕様書の 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）。

ベース DN (Base DN)

Firepower Management Center がユーザ データの検索を開始するサーバのディレクトリ 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。

グループ DN (Group DN)

Firepower Management Center がグループ属性を持つユーザを検索するサーバのディレクトリ 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オブジェクトクラスと属性名 \(5 ページ\)](#) 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ないためです。

グループ属性 (Group Attribute)

(オプション) サーバのグループ属性：メンバー、または一意のメンバー。

タイプ (Type)

レルムのタイプで、Microsoft Active Directory 用の **AD** またはその他のサポートされている LDAP リポジトリ用の **LDAP** 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 \(4 ページ\)](#) を参照してください。



(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。

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。

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

ユーザ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、ユーザのセッションは終了します。ユーザ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、ユーザは Firepower Management Center により不明として認識されます。



(注) ユーザセッションタイムアウト値は、アクティブ認証 (キャプティブ ポータル) とパッシブ認証 (TS エージェント、ユーザエージェント、ISE) の両方に適用されます。大きな値を設定すると、ユーザセッションが終了しない可能性があり、他のユーザによってこれらのセッションが要求される場合があります。

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 (Active Directory ドメインコントローラなど) に適用されます。

暗号化 (Encryption)

Firepower Management Center サーバ接続に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)

ホスト名/IP アドレス (Hostname/IP Address)

Active Directory ドメインコントローラのホスト名または IP アドレス。[暗号化 (Encryption)] 方式を指定する場合は、このフィールドでホスト名を指定します。

[ポート (Port)]

Firepower Management Center コントローラ接続に使用するポート。

SSL 証明書 (SSL Certificate)

サーバへの認証に使用する SSL 証明書。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、証明書のサーバ名は、サーバの [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。

ユーザのダウンロード (User Download) フィールド

[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)]

ダウンロードしてユーザ認識やユーザ制御に使用できるようにするグループを特定します。

- [使用可能グループ ボックス (Available Groups)] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する (Add to Include)] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザ データはユーザ認識やユーザ制御に利用できます。
- グループを [除外するに追加する (Add to Exclude)] ボックスに追加すると、グループ名のみがダウンロードされます。グループ内のユーザはダウンロードされません。
- 含まれないグループのユーザを含めるには、[含めるグループ (Groups to Include)] の下のフィールドにそのユーザ名を入力し、[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を除外するには、[除外するグループ (Groups to Exclude)] の下のフィールドにそのユーザ名を入力し、[追加 (Add)] をクリックします。



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

- R はダウンロードしたユーザのリストです。
- 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です。

自動ダウンロードの開始、繰り返し設定 (Begin automatic download at, Repeat every)

自動ダウンロードの回数を指定します。

ユーザおよびグループのダウンロード（ユーザアクセス制御に必須）

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

レルム ディレクトリの設定

この手順では、LDAP サーバまたは Microsoft Active Directory ドメイン コントローラに対応するレルムディレクトリを作成できます。それぞれ異なるユーザやグループを認証する複数のドメイン コントローラを、1つの Active Directory サーバに設定することができます。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

レルム 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（12 ページ）](#) を参照してください。

始める前に

オプションで SSL 証明書を使用してディレクトリで認証するには、Firepower Management Center のアクセス元となるマシンで [証明書を作成](#) するか、証明書データとキーを利用可能にします。

手順

- ステップ 1** まだ実行していない場合は、Firepower Management Center にログインし、[統合 (Integration)] > [レルム (Realms)] をクリックします。
- ステップ 2** [レルム (Realms)] タブ ページで、ディレクトリの設定対象となるレルムの名前をクリックします。
- ステップ 3** [ディレクトリ (Directory)] タブ ページで、[ディレクトリの追加 (Add Directory)] をクリックします。
- ステップ 4** LDAP サーバまたは Active Directory ドメイン コントローラの [ホスト名/IP アドレス (Hostname / IP Address)] と [ポート (Port)] を入力します。
システムにより、指定したホスト名または IP アドレスに LDAP クエリが送信されます。ホスト名が 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場合は、[テスト (Test)] が成功します。
- ステップ 5** [暗号化モード (Encryption Mode)] を選択します。
- ステップ 6** (オプション) リストから [SSL 証明書 (SSL Certificate)] を 1 つ選択するか、追加アイコン (+) をクリックして証明書を追加します。
- ステップ 7** 接続をテストするには、[テスト (Test)] をクリックします。
- ステップ 8** [OK] をクリックします。

- ステップ 9** [保存 (Save)] をクリックします。[レルム (Realms)] タブ ページに戻ります。
- ステップ 10** レルムをまだ有効にしていない場合は、[レルム (Realms)] タブ ページで、[状態 (State)] を有効にします。

次のタスク

- [ユーザとグループのダウンロード \(17 ページ\)](#) .

ユーザとグループのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

このセクションでは、Active Directory サーバから Firepower Management Center にユーザとグループをダウンロードする方法について説明します。含めるグループを指定しなかった場合、システムは指定されたパラメータと一致するすべてのグループのユーザデータを取得します。パフォーマンス上の理由から、アクセスコントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

Firepower Management Center がサーバから取得可能なユーザの最大数は Firepower Management Center モデルによって異なります。レルムのダウンロードパラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数を Message Center の [タスク (Task)] タブで報告します。




- (注) Firepower Management Center では、Unicode 文字を含むユーザ名は表示されません。ユーザやグループをダウンロードする前に、Unicode 文字を英数字に置き換えてください。

レルム設定フィールドの詳細については、[レルム フィールド \(12 ページ\)](#) を参照してください。

手順

- ステップ 1** Firepower Management Center にログインします。
- ステップ 2** [システム (System)] > [統合 (Integration)] > [レルム (Realms)] をクリックします。
- ステップ 3** ユーザとグループを手動でダウンロードするには、ユーザやユーザグループをダウンロードするレルムの横にあるダウンロードアイコン (📄) をクリックします。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。残りの手順をスキップできます。

- ステップ 4** 自動でユーザとグループをダウンロードするようにレールムを設定するには、自動でユーザやグループをダウンロードするように設定するレールムの横にある編集アイコン () をクリックします。
- ステップ 5** [ユーザアクセス制御 (User Access Control)] タブ ページで、[(ユーザアクセス制御に必要な) ユーザとグループをダウンロードする (Download users and groups (required for user access control))] をオンにします。
- ステップ 6** 一覧から [自動ダウンロードの開始時間 (Begin automatic download at)] の時間を選択します。
- ステップ 7** [繰り返し設定 (Repeat Every)] 一覧からダウンロード間隔を選択します。
- ステップ 8** ダウンロードにユーザ グループを含めるか除外するには、[選択可能なグループ (Available Groups)] 列からユーザ グループを選択し、[含めるに追加 (Add to Include)] または [除外に追加 (Add to Exclude)] をクリックします。

複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク (*) をワイルドカード文字として使用できます。

(注) そのグループのユーザに対してユーザ制御を実行する場合は、[含めるに追加 (Add to Include)] をクリックする必要があります。

次の注意事項に従ってください。

- [使用可能グループボックス (Available Groups)] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する (Add to Include)] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザ データはユーザ認識やユーザ制御に利用できます。
- [除外に追加する (Add to Exclude)] ボックスにグループを移動させると、グループがダウンロードされ、ユーザ データはユーザ認識に利用できますが、ユーザ制御には利用できません。
- 含まれないグループのユーザを含めるには、[含めるグループ (Groups to Include)] の下のフィールドにそのユーザ名を入力し、[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を除外するには、[除外するグループ (Groups to Exclude)] の下のフィールドにそのユーザ名を入力し、[追加 (Add)] をクリックします。

アイデンティティ ポリシーの作成

スマート ライセ ンス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

始める前に

アイデンティティ ポリシーは、アクセス コントロール ポリシーのレールムでユーザやグループを使用するために必要です。[レールムの作成 \(11 ページ\)](#) の説明に従って 1 つ以上のレールムを作成し、有効にします。

次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。

- ISE アイデンティティ ソースを使用できます。
- アクセス コントロール ポリシーのユーザまたはグループは使用しません。
- アクセス コントロール ポリシーのセキュリティ グループ タグ (SGT) を使用します。詳細については、[ISE SGT とカスタム SGT ルール条件との比較](#)を参照してください。

手順

- ステップ 1** Firepower Management Center にログインします。
- ステップ 2** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [ID (Identity)] をクリックし、[新しいポリシー (New Policy)] をクリックします。
- ステップ 3** [名前 (Name)] を入力し、必要に応じて [説明 (Description)] を入力します。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** ポリシーにルールを追加するには、[アイデンティティ ルールの作成 \(20 ページ\)](#) で説明されているように、[ルールの追加 (Add Rule)] をクリックします。
- ステップ 6** ルール カテゴリを作成するには、[カテゴリの追加 (Add Category)] をクリックします。
- ステップ 7** キャプティブ ポータルのアクティブ認証を設定するには、[ユーザ制御のためのキャプティブ ポータルの設定方法](#)で説明されているように、[アクティブ認証 (Active Authentication)] タブをクリックします。
- ステップ 8** [保存 (Save)] をクリックして、アイデンティティ ポリシーを保存します。

次のタスク

- 照合するユーザおよび他のオプションを指定するルールを、アイデンティティ ポリシーに追加します（[アイデンティティ ルールの作成 \(20 ページ\)](#) を参照）。
- 指定したリソースへのアクセスを特定のユーザに許可またはブロックするには、このアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（[アクセス制御への他のポリシーの関連付け](#)を参照）。
- 設定変更を管理対象デバイスに展開します（[設定変更の展開](#)を参照）。


問題が発生した場合は、[ユーザ制御のトラブルシューティング](#)を参照してください。


アイデンティティ ルールの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

アイデンティティ ルールの設定オプションに関する詳細については、[アイデンティティ ルール フィールド \(21 ページ\)](#) を参照してください。

手順

- ステップ 1** まだ Firepower 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** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [ID (Identity)] をクリックします。
- ステップ 3** アイデンティティ ルールの追加先となるアイデンティティ ポリシーの横にある [編集 (edit)] () をクリックします。

代わりに表示アイコン () 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。
- ステップ 4** [ルールの追加 (Add Rule)] をクリックします。
- ステップ 5** 名前を入力します。
- ステップ 6** ルールを有効にするかどうかを指定します。
- ステップ 7** 既存のカテゴリにルールを追加するには、ルールを [挿入 (Insert)] する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加 (Add Category)] をクリックします。
- ステップ 8** 一覧からルール [アクション (Action)] を選択します。
- ステップ 9** [レールムおよび設定 (Realms & Settings)] タブをクリックします。

- ステップ 10** [レム (Realms)]一覧から、アイデンティティ ルールのレムを選択します。各アイデンティティ ルールにレムを関連付ける必要があります。
- レム要件の唯一の例外は、ISE SGT 属性タグのみを使用してユーザ制御を実装する場合があります。この場合は、ISE サーバのレムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。
- ステップ 11** キャプティブ ポータルを設定する場合は、[ユーザ制御のためのキャプティブ ポータルの設定方法](#)を参照してください。
- ステップ 12** (オプション) アイデンティティ ルールに条件を追加するには、[ルール条件タイプ](#)を参照してください。
- ステップ 13** [追加 (Add)]をクリックします。
- ステップ 14** ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリックメニューを使用してカットアンドペーストを実行します。ルールには1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワークトラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。
- ステップ 15** [保存 (Save)]をクリックします。

関連トピック

[Snort® の再起動シナリオ](#)

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

[有効 (Enabled)]

このオプションを選択すると、アイデンティティ ポリシーのアイデンティティ ルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

アクション (Action)

指定したレムでユーザに対して実行する認証のタイプを指定します。これには、[パッシブ認証 (Passive Authentication)] (デフォルト) 、[アクティブ認証 (Active Authentication)]、または[認証なし (No Authentication)]があります。アイデンティティ ルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。



注意 SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作](#)を参照してください。

アクティブ認証ルールには [アクティブ認証 (Active Authentication)] ルールアクションが含まれているか、または [パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する (Use active authentication if passive authentication cannot identify user)] が選択された [パッシブ認証 (Passive Authentication)] ルールアクションが含まれています。

Firepower システムのバージョンでサポートされるパッシブおよびアクティブ認証方式の詳細については、[ユーザアイデンティティ ソースについて](#)を参照してください。

レールム

指定されたアクションを実行するユーザが含まれるレールム。アイデンティティ ルールのレールムとして選択する前に、レールムを完全に設定する必要があります。



(注) [Kerberos] (または [Kerberos] をオプションとする場合は [HTTP ネゴシエート (HTTP Negotiate)]) を、アイデンティティ ルールの [認証タイプ (Authentication Type)] として選択する場合、選択する [レールム (Realm)] は、Kerberos キャプティブ ポータルアクティブ認証を実行できるように、[AD 参加ユーザ名 (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。

パッシブ認証がユーザを識別できない場合は、アクティブ認証を使用します。

このオプションを選択すると、パッシブまたは VPN 認証でユーザを識別できない場合にキャプティブ ポータルアクティブ認証を使用してユーザが認証されます。このオプションを選択するには、アイデンティティ ポリシーでキャプティブ ポータルアクティブ認証を設定する必要があります。

このオプションを無効にすると、VPN ID を持たないユーザまたはパッシブ認証では識別できないユーザは、「不明 (Unknown)」と識別されます。

認証でユーザを識別できない場合は特別 ID/ゲストとして識別する (Identify as Special Identities/Guest if authentication cannot identify user)

ルールアクションとして [アクティブ認証 (Active Authentication)] (つまり、キャプティブ ポータル認証) を設定している場合にのみ、このフィールドが表示されます。

認証タイプ

キャプティブ ポータルアクティブ認証を実行するために使用する方法です。選択は、レールム、LDAP、または AD のタイプによって異なります。

- 暗号化されていない HTTP 基本認証 (BA) 接続を使用してユーザを認証するには、[HTTP 基本 (HTTP Basic)] を選択します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

ほとんどの Web ブラウザは、**HTTP 基本** ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。

- NT LAN Manager (NTLM) 接続を使用してユーザを認証するには **NTLM** を選択します。この選択は AD レールムを選択するときのみ使用できます。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。
- Kerberos 接続を使用してユーザを認証する場合は、[Kerberos] を選択します。この選択は、セキュア LDAP (LDAPS) が有効になっているサーバに対して AD レールムを選択する場合にのみ可能です。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。



(注) 選択する [レールム (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ために、[AD 参加ユーザ名 (AD Join Username)] および [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) Kerberos キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名 (FQDN) を解決する DNS サーバを設定する必要があります。FQDN は、DNS の設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services および Firepower Threat Defense デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- キャプティブ ポータルサーバが認証接続に HTTP 基本認証、Kerberos、または NTLM を選択できるようにするには、[HTTP ネゴシエート (HTTP Negotiate)] を選択します。このタイプは AD レールムを選択するときのみ使用できます。



(注) 選択する [レルム (Realm)] は、[HTTP ネゴシエート (HTTP Negotiate)] で Kerberos キャプティブ ポータル アクティブ 認証を選択するために、[AD 参加ユーザ名 (AD Join Username)] および [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) [HTTP ネゴシエート (HTTP Negotiate)] キャプティブ ポータル を実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名 (FQDN) を解決する DNS サーバを設定する必要があります。キャプティブ ポータル に使用するデバイスの FQDN は、DNS の設定時に入力したホスト名と一致している必要があります。

ASA with FirePOWER Services デバイスの場合、FQDN は ASA FirePOWER モジュールの FQDN です。

レルムの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

このセクションでは、[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。次の点に注意してください。

- 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。
- 代わりに表示アイコン (🔑) 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 Firepower Management Center にログインします。

- ステップ2 [システム (System)] > [統合 (Integration)] をクリックします。
- ステップ3 [レーム (Realms)] をクリックします。
- ステップ4 レームを削除するには、削除アイコン (🗑️) をクリックします。
- ステップ5 レームを編集するには、レームの横にある編集アイコン (✎) をクリックし、[レームの作成 \(11 ページ\)](#) の説明に従って変更を行います。
- ステップ6 レームを有効にするには、[状態 (State)] を右にスライドします。レームを無効にするには、左にスライドします。
- ステップ7 ユーザおよびユーザグループをダウンロードするには、ダウンロードアイコン (📥) をクリックします。
- ステップ8 レームをコピーするには、コピーアイコン (📄) をクリックします。
- ステップ9 レームを比較する方法については、[レームの比較 \(25 ページ\)](#) を参照してください。

レームの比較

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、Security Approver、Access Admin、Network Admin

手順

- ステップ1 Firepower Management Center にログインします。
- ステップ2 [システム (System)] > [統合 (Integration)] をクリックします。
- ステップ3 [レーム (Realms)] をクリックします。
- ステップ4 [システム (System)] > [統合 (Integration)] をクリックします。
- ステップ5 [レーム (Realms)] をクリックします。
- ステップ6 [レームの比較 (Compare Realms)] をクリックします。
- ステップ7 [比較対象 (Compare Against)] リストから [レームの比較 (Compare Realm)] を選択します。
- ステップ8 [レーム A (Realm A)] および [レーム B (Realm B)] リストから比較するレームを選択します。
- ステップ9 [OK] をクリック
- ステップ10 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 11 (オプション) [比較レポート (Comparison Report)] をクリックして、レールム比較レポートを生成します。
- ステップ 12 (オプション) [新しい比較 (New Comparison)] をクリックして、新しいレールム比較ビューを生成します。

アイデンティティ ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

- ステップ 1 まだ Firepower 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 [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [ID (Identity)] をクリックします。
- ステップ 3 ポリシーを削除するには、削除 (🗑️) をクリックします。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。
- ステップ 4 ポリシーを編集するには、ポリシーの横にある編集 (✏️) をクリックし、[アイデンティティポリシーの作成 \(19 ページ\)](#) の説明に従って変更を行います。代わりに表示アイコン (🔍) 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。
- ステップ 5 ポリシーをコピーするには、コピーアイコン (📄) をクリックします。
- ステップ 6 ポリシーのレポートを生成するには、[現在のポリシーレポートの生成](#)の説明に従ってレポートアイコン (📄) をクリックします。
- ステップ 7 ポリシーを比較する方法については、[ポリシーの比較](#)を参照してください。

アイデンティティ ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意 (Any)	Control	任意 (Any)	任意 (Any)	Administrator、 Access Admin、 Network Admin

手順

- ステップ 1 まだ Firepower 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 [ポリシー (Policies)]>[アクセスコントロール (Access Control)]>[ID (Identity)]をクリックします。
- ステップ 3 編集するポリシーの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) 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。
- ステップ 4 アイデンティティ ルールを編集するには、編集アイコン (✎) をクリックし、[アイデンティティ ポリシーの作成 \(19 ページ\)](#) の説明に従って変更を行います。
- ステップ 5 アイデンティティ ルールを削除するには、削除アイコン (🗑) をクリックします。
- ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加 (Add Category)]をクリックし、位置とルールを選択します。
- ステップ 7 [保存 (Save)]をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

