



アイデンティティ ポリシーの作成および管理

次のトピックでは、アイデンティティ ルールとアイデンティティ ポリシーの作成方法と管理方法について説明します。

- [アイデンティティ ポリシーについて \(1 ページ\)](#)
- [アイデンティティ ルールの作成 \(2 ページ\)](#)
- [アイデンティティ ポリシーの作成 \(7 ページ\)](#)
- [アイデンティティ ルールの管理 \(8 ページ\)](#)
- [アイデンティティ ポリシーの管理 \(9 ページ\)](#)

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、レルムおよび認証方式（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、使用する予定のレルムと認証方式を、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)] > [レルム (Realms)]** でアイデンティティ ポリシー外のレルムを設定します。詳細については、[レルムの作成](#)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/ISE-PIC 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/ISE-PIC 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。
- リモートアクセス VPN ポリシー内では、アクティブな認証アイデンティティ ソースであるリモートアクセス VPN を設定します。詳細については、[リモートアクセス VPN 認証](#)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ルムと関連付け、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/ISE-PIC 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

[アイデンティティ ポリシーの設定方法](#)

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 \(3 ページ\)](#) 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 [Policies] > [Access Control] > [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 [レルム (Realms)] 一覧から、アイデンティティルールのレルムを選択します。各アイデンティティルールにレルムを関連付ける必要があります。
- レル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です。この場合は、ISE サーバのレル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、ルールのプリエンブ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。

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)

指定したレー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。

さらに、VPNが有効になっている場合 (少なくとも1つの管理対象デバイスで設定されている場合)、リモートアクセスVPNセッションはVPNによってアクティブに認証されます。他のセッションはルールアクションを使用します。つまり、VPNが有効になっている場合は、選択したアクションに関係なく、すべてのセッションでVPN IDの判別が最初に行われます。指定されたレーム上にVPN IDが見つかった場合、これは使用されるアイデンティティソースになります。選択されていても、追加のキャプティブポータルアクティブ認証は実行されません。

VPNアイデンティティソースが見つからない場合は、指定されたアクションに従ってプロセスが続行されます。アイデンティティポリシーをVPN認証のみに制限することはできません。VPN IDが見つからない場合は、選択されたアクションに従ってルールが適用されるためです。



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[パッシブまたはVPN IDを確立できない場合はアクティブ認証を使用する (Use active authentication if passive or VPN identity cannot be established)]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ム。アイデンティティルールのレームとして選択する前に、レームを完全に設定する必要があります。



- (注) リモートアクセス VPN が有効で、展開で VPN 認証に RADIUS サーバグループを使用している場合は、この RADIUS サーバグループに関連付けられているレルムを指定してください。



- (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。

パッシブまたは VPN ID を確立できない場合は、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)

このオプションを選択すると、キャプティブポータルアクティブ認証に指定された回数失敗したユーザがゲストとしてネットワークにアクセスできます。これらのユーザは、Firepower Management Console ではユーザ名 (ユーザ名が AD または LDAP サーバに存在する場合) または [ゲスト (Guest)] (ユーザ名が不明の場合) で表示されます。これらのユーザのレルムは、アイデンティティルールで指定されたレルムです。(デフォルトでは、失敗したログインの数は 3 回です。)

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。

認証プロトコル

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的方法です。選択は、レルム、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。

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 (Access)
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ムでユーザやグループを使用するために必要です。[レームの作成](#)の説明に従って1つ以上のレームを作成し、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/ISE-PIC 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** **[Policies] > [Access Control] > [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 \(2 ページ\)](#) で説明されているように、[ルール追加 (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で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 \(2 ページ\)](#) 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。

関連トピック

[ユーザ制御のトラブルシューティング](#)

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 (Access)
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** **[Policies] > [Access Control] > [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 \(7 ページ\)](#) 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。

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** [Policies] > [Access Control] > [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 (Delete)] (🗑) 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 (Edit)] (✎) をクリックし、[アイデンティティポリシーの作成 \(7 ページ\)](#) 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。

