ISE/ISE-PIC によるユーザーの制御

次のトピックでは、ISE/ISE-PIC によりユーザー認識とユーザー制御を実行する方法について説明します。

ISE/ISE-PIC アイデンティティ ソース

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開をシステムと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、またはRSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE/ISE-PIC は、ISE ゲスト サービス ユーザーの失敗したログイン試行またはアクティビティは報告しません。

ユーザーの認識と制御に加えて、ISE Cisco TrustSec ネットワークでトラフィックを分類するために ISE を使用してセキュリティグループタグ（SGT）を定義して使用する場合は、送信元と宛先の両方の一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、IP アドレスまたはネットワーク オブジェクトではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。詳細については、「ダイナミック属性の条件の設定」を参照してください。 を使用する場合は「ISE/ISE-PIC のガイドラインと制限事項 （4 ページ）」も参照してください。

（注） システムは IEEE 802.1x マシン認証を解析しませんが、802.1x ユーザー認証を解析します。ISE で 802.1x を使用している場合は、ユーザー認証を含める必要があります。802.1x マシン認証は、ポリシーで使用できる Management Center にユーザーアイデンティティを提供しません。

Cisco ISE/ISE-PIC の詳細については、『Cisco Identity Services Engine Passive Identity Connector 管理者ガイド』または『Cisco Identity Services Engine Administrator Guide』を参照してください。

（注） 最新バージョンの ISE/ISE-PIC を使用して、最新の機能セットと最大数の問題修正を入手することを強くお勧めします。

送信元および宛先セキュリティグループタグ（SGT）の照合

Cisco TrustSec ネットワークでトラフィックを分類するために ISE を使用してセキュリティグループタグ（SGT）を定義して使用する場合は、送信元と宛先の両方の一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、IP アドレスまたはネットワークオブジェクトではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。詳細については、「ダイナミック属性の条件の設定」を参照してください。 を使用する場合、

SGT タグの照合には、次の利点があります。

- Management Center は、ISE から Security Group Tag eXchange Protocol（SXP）マッピングに登録できます。

  ISE は SXP を使用して、IP-to-SGT マッピング データベースを管理対象デバイスに伝搬します。ISE サーバーを使用するように Management Center を設定する場合は、ISE から SXP トピックをリッスンするオプションを有効にします。有効にすると、Management Center は ISE から直接セキュリティグループタグとマッピングについて学習します。次に、Management Center は SGT とマッピングを管理対象デバイスにパブリッシュします。

  SXP トピックは、ISE と他の SXP 準拠デバイス（スイッチなど）の間の SXP プロトコルを通じて学習した静的マッピングと動的マッピングに基づいてセキュリティグループタグを受信します。

  ISE でセキュリティ グループ タグを作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。また、ユーザーアカウントに SGT を割り当て、SGT がユーザーのトラフィックに割り当てられるようにすることもできます。ネットワーク内のスイッチおよびルータがそのように設定されている場合、これらのタグは、ISE、Cisco TrustSec クラウドによって制御されるネットワークに入るときにパケットに割り当てられます。

  SXP は ISE-PIC ではサポートされていません。

- Management Center および管理対象デバイスは、追加のポリシーを展開しなくても、SGT マッピングについて学習できます（つまり、アクセス コントロール ポリシーを展開しなくても SGT マッピングの接続イベントを表示できます）。
- Cisco TrustSec をサポートしているため、ネットワークをセグメント化して重要なビジネス資産を保護することができます。
- 管理対象デバイスは、アクセス コントロール ルールのトラフィック一致基準として SGT を評価するときに、次の優先順位を使用します。

  1. パケット内で定義されている送信元 SGT タグ（存在する場合）。

     SGT タグがパケットに含まれるようにするには、ネットワーク内のスイッチとルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。

     SGT タグがパケットに含まれるようにするには、ネットワーク内のスイッチとルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。

  2. ISE セッション ディレクトリからダウンロードされるユーザー セッションに割り当てられた SGT。SGT は、送信元または宛先と照合することができます。
  3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが SGT の範囲内にある場合、トラフィックは SGT を使用するアクセス コントロール ルールと一致します。SGT は、送信元または宛先と照合することができます。

次に例を示します。

- ISE で、Guest Users という名前の SGT タグを作成し、それを 192.0.2.0/24 ネットワークに関連付けます。

  たとえば、Guest Users をアクセス コントロール ルール内の送信元 SGT 条件として使用し、ネットワークにアクセスするすべてのユーザーによる特定の URL、Web サイト カテゴリ、またはネットワークへのアクセスを制限することができます。

- ISE で、Restricted Networks という名前の SGT タグを作成し、それを 198.51.100.0/8 ネットワークに関連付けます。

  たとえば、Restricted Networks を宛先 SGT ルール条件として使用し、Guest Users や、ネットワークへのアクセスを許可されていないユーザーを持つ他のネットワークからのアクセスをブロックすることができます。

関連トピック

ISE/ISE-PIC のガイドラインと制限事項 （4 ページ）

ISE/ISE-PIC 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

ISE/ISE-PIC の要件と前提条件

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

ISE/ISE-PIC のガイドラインと制限事項

ISE/ISE-PIC を構成する際に、このセクションで説明されているガイドラインを使用してください。

ISE/ISE-PIC バージョンと設定の互換性

ご使用の ISE/ISE-PIC バージョンと設定は、次のように Secure Firewall Management Center との統合や相互作用に影響を与えます。

- 最新バージョンの ISE/ISE-PIC を使用して最新の機能セットを入手することを強くお勧めします。
- ISE/ISE-PIC サーバーと Secure Firewall Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザーのタイムアウトを実行する可能性があります。
- ISE または ISE-PIC データを使用してユーザー制御を実装するには、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 の説明に従って、pxGrid のペルソナを想定して ISE サーバーのレルムを設定し有効にします。

- ISE サーバーに接続する各 Secure Firewall Management Center ホスト名は一意である必要があります。そうでない場合、Secure Firewall Management Center のいずれかへの接続は廃棄されます。
- 多数のユーザーグループをモニターするように ISE/ISE-PIC を設定した場合、システムは管理対象デバイスのメモリ制限のためにグループに基づいてユーザーマッピングをドロップすることがあります。その結果、レルムまたはユーザー条件を使用するルールが想定どおりに実行されない可能性があります。

  6.7 以降を実行しているデバイスの場合、**configure identity-subnet-filter** コマンドを使用して、管理対象デバイスがモニタするサブネットを制限することもできます。詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

  または、ネットワークオブジェクトを設定し、そのオブジェクトを ID ポリシーのアイデンティティマッピングフィルタとして適用できます。アイデンティティポリシーの作成を参照してください。

システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、Cisco Firepower Compatibility Guide を参照してください。

IPv6 のサポート

- ISE/ISE-PIC のバージョン 2.x の互換性のあるバージョンには、IPv6 対応エンドポイントのサポートが含まれています。
- ISE/ISE-PIC のバージョン 3.0（パッチ 2）以降では、ISE/ISE-PIC と Management Center 間の IPv6 通信が可能です。

ISE でのクライアントの認証

ISE サーバーと Management Center 間の接続を確立するには、ISE のクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。

到達不能なセッションは削除されます。

ISE/ISE-PIC のユーザーセッションが到達不能として報告された場合、Secure Firewall Management Center ではそのセッションがプルーニングされ、同じ IP を持つ別のユーザーは到達不能なユーザーのアイデンティティルールに一致できません。
[プロバイダー（Providers）]>[エンドポイントプローブ（Endpoint Probes）] に移動し、次のいずれかをクリックして、ISE/ISE-PIC でこの動作を制御できます。

- [有効（Enabled）] にすると、ISE/ISE-PIC がエンドポイント接続を監視し、Secure Firewall Management Center で到達不能なユーザーからのセッションをプルーニングできます。
- [無効（Disabled）] にすると、ISE/ISE-PIC はエンドポイント接続を無視します。

セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）

セキュリティグループタグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス（SGA）と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティグループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。

セキュリティ グループ タグは、アクセス コントロール ルール内の送信元および宛先の両方の一致基準として使用できます。

（注） ISE SGT 属性タグのみを使用してユーザー制御を実装する場合、ISE サーバー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。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザー制御とみなされず、アイデンティティ ソースとして ISE/ISE-PIC を使用しない場合にのみ機能します。カスタム SGT 条件 を参照してください。

送信元 SGT タグに加えて宛先 SGT タグを照合するには、次の条件が適用されます。

必要な ISE バージョン：2.6 パッチ 6 以降、2.7 パッチ 2 以降

ルータのサポート：イーサネットを介した SGT インライン タギングをサポートする任意のシスコ ルータ。詳細については、『Cisco Group Based Policy Platform and Capability Matrix Release』などの参考資料を参照してください。

制限事項

- サービス品質（QoS）ポリシーは、送信元 SGT 照合のみを使用し、宛先 SGT 照合は使用しません。
- RA-VPN は、RADIUS を介した SGT マッピングの直接の受信はしません。

ISE と高可用性

プライマリ ISE/ISE-PIC サーバーで障害が発生すると、次のようなことが起きます。

pxGrid v2 との統合の結果として、Management Center は、一方が接続を受け入れるまで設定された両方の ISE ホスト間のラウンドロビンを行います。

接続が失われると、Management Center は接続されたホストへのラウンドロビンの試行を再開します。

エンドポイント ロケーション（Endpoint Location）（またはロケーション IP（Location IP））

[エンドポイント ロケーション（Endpoint Location）] 属性は、ISE によって識別される、ユーザーの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

[エンドポイント ロケーション（Endpoint Location）]（[ロケーション IP（Location IP）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ISE 属性

ISE 接続を設定すると、ISE 属性データが Secure Firewall Management Center データベースに入力されます。ユーザー認識とユーザー制御に使用できる ISE 属性は、次のとおりです。 これは、ISE-PIC ではサポートされません。

エンドポイント プロファイル（Endpoint Profile）（またはデバイス タイプ（Device Type））

[エンドポイント プロファイル（Endpoint Profile）] 属性は、ISE によって識別されるユーザーのエンドポイント デバイス タイプです。

[エンドポイント プロファイル（Endpoint Profile）]（[デバイス タイプ（Device Type）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ユーザー制御用 ISE/ISE-PIC の設定方法

ISE/ISE-PIC は、次の設定のいずれかで使用できます。

- レルム、アイデンティティ ポリシー、および関連付けられたアクセス コントロール ポリシーを使用。

  レルムを使用して、ポリシー内のネットワーク リソースへのユーザー アクセスを制御します。ポリシーでは、ISE/ISE-PIC セキュリティ グループ タグ（SGT）のメタデータを引き続き使用できます。

- アクセス コントロール ポリシーのみを使用。レルムまたはアイデンティティ ポリシーは必要ありません。

  SGT メタデータのみを使用してネットワーク アクセスを制御するには、この方法を使用します。

関連トピック

レルムなしで ISE を設定する方法 （7 ページ）
レルムを使用したユーザー制御用 ISE/ISE-PIC の設定方法 （9 ページ）

レルムなしで ISE を設定する方法

このトピックでは、SGT タグを使用してネットワークへのアクセスを許可またはブロックできるように ISE を設定するために必要なタスクの概要について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	SGT 照合：ISE で SXP を有効にします。	これにより、SGT メタデータの変更時に Management Center が ISE から更新を受信できるようになります。
ステップ 2	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバー、および Management Center の間で安全に接続するために必要です（「Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （14 ページ）」を参照）。
ステップ 3	Management Center に証明書をインポートします。	証明書は次のようにインポートする必要があります。 • pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト** > **オブジェクト管理** > **PKI** > **内部証明書**） • pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**） • MNT 証明書：信頼できる CA
ステップ 4	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザー アクティビティを制御できます。ユーザー制御用 ISE の設定 （18 ページ）を参照してください。
ステップ 5	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元および宛先の SGT メタデータを使用できます。アクセス コントロール ルールの概要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 6	管理対象デバイスにアクセスコントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開 を参照してください。

次のタスク

Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （14 ページ）

レルムを使用したユーザー制御用 ISE/ISE-PIC の設定方法

始める前に

このトピックでは、ユーザ制御用 ISE/ISE-PIC を設定し、ユーザまたはグループによるネットワークへのアクセスを許可またはブロックできるようにするために必要なタスクの概要について説明します。ユーザーおよびグループは、レルムがサポートされているサーバーに記載されている任意のサーバーに保存できます。

手順

	コマンドまたはアクション	目的
ステップ 1	宛先 SGT のみ：ISE で SXP を有効にします。	これにより、SGT メタデータの変更時に Management Center が ISE から更新を受信できるようになります。
ステップ 2	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバー、および Management Center の間で安全に接続するために必要ですその場合は、次のトピックを参照してください。 • pxGrid サーバーおよび MNT サーバー証明書：Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （14 ページ） • pxGrid クライアント証明書：自己署名証明書の生成 （16 ページ）
ステップ 3	Management Center に証明書をインポートします。	証明書は次のようにインポートする必要があります。

	コマンドまたはアクション	目的
		• pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト** > **オブジェクト管理** > **PKI** > **内部証明書**） • pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**） • MNT 証明書：信頼できる CA
ステップ 4	レルムを作成します。	レルムの作成は、選択したユーザーおよびグループによるネットワークへのアクセスを制御するためにのみ必要です。 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を参照してください。
ステップ 5	ユーザーおよびグループをダウンロードし、レルムを有効にします。	ユーザーおよびグループをダウンロードすると、それらをアクセス コントロールルールで使用できるようになります。ユーザーとグループの同期を参照してください。
ステップ 6	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザー アクティビティを制御できます。ユーザー制御用 ISE の設定 （18 ページ）を参照してください。
ステップ 7	アイデンティティ ポリシーを作成します。	アイデンティティ ポリシーは、1 つ以上のアイデンティティ ルールのコンテナです。アイデンティティ ポリシーの作成を参照してください。
ステップ 8	アイデンティティ ルールを作成します。	アイデンティティ ルールは、ユーザーおよびグループによるネットワークへのアクセスを制御するためにレルムがどのように使用されるかを指定します。アイデンティティ ルールの作成を参照してください。

	コマンドまたはアクション	目的
ステップ 9	アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます。	これにより、アクセス コントロール ポリシーがレルム内のユーザーとグループを使用できるようになります。
ステップ 10	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元および宛先の SGT メタデータを使用できます。アクセス コントロール ルールの概要を参照してください。
ステップ 11	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開 を参照してください。

次のタスク

Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （14 ページ）

ISE/ISE-PIC の設定

次のトピックでは、Management Center のアイデンティティ ポリシーで使用するように ISE/ISE-PIC サーバーを設定する方法について説明します。

このトピックでは、次の方法について説明します。

- Management Center で認証するために ISE/ISE-PIC サーバーから証明書をエクスポートします。
- Management Center を ISE サーバーのセキュリティ グループ タグ（SGT）で更新できるように、SXP トピックを公開します。

関連トピック

ISE でのセキュリティ グループと SXP パブリッシングの設定 （12 ページ）
Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （14 ページ）

ISE でのセキュリティ グループと SXP パブリッシングの設定

Cisco Identity Services Engine（ISE）では、TrustSec ポリシーとセキュリティグループタグ（SGT）を作成するために実行を必要とする設定が多数あります。TrustSec の実装の詳細については、ISE のマニュアルを参照してください。

次の手順では、脅威に対する防御デバイスがスタティック SGT から IP アドレスへのマッピングをダウンロードして適用できるようにするために ISE で設定する必要があるコア設定のハイライトを示します。これは、アクセス制御ルールでの送信元と宛先 SGT の照合に使用できます。詳細については、ISE のマニュアルを参照してください。

この手順のスクリーンショットは、ISE 2.4 に基づいています。これらの機能にアクセスするための正確な手順は後続のリリースで変更される可能性がありますが、概念と要件は同じです。ISE 2.4 以降、特に 2.6 以降が推奨されますが、ISE 2.2 パッチ 1 以降でもこの設定は動作します。

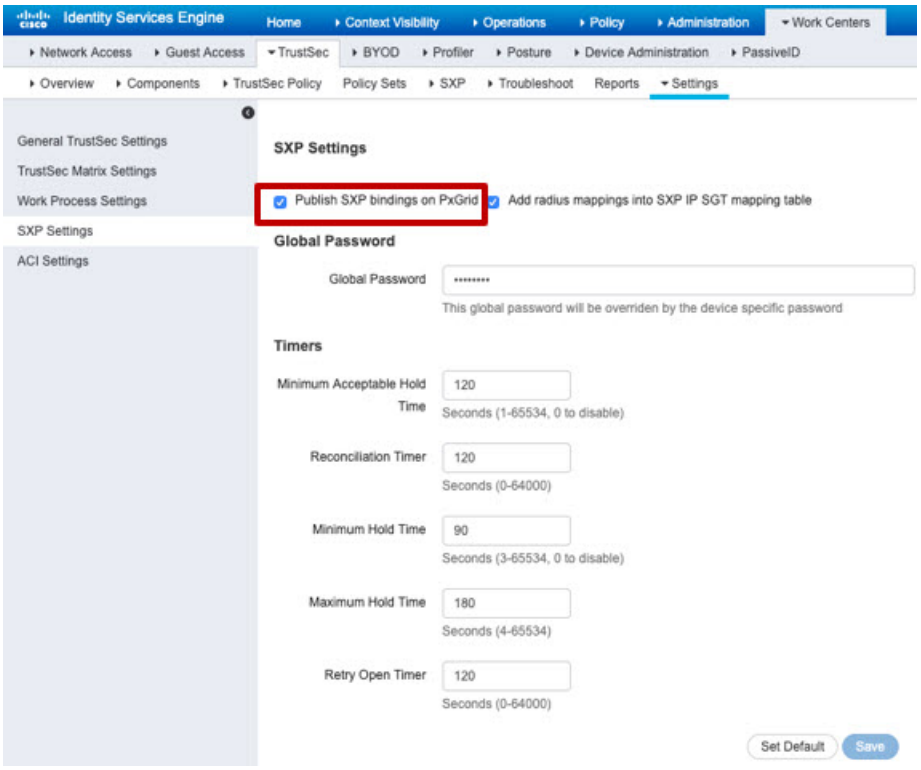
始める前に

SGT から IP アドレスへのスタティックマッピングを公開し、ユーザーセッションからと SGT へのマッピングを取得して脅威に対する防御デバイスがそれらを受信できるようにするには、ISE Plus ライセンスが必要です。

手順

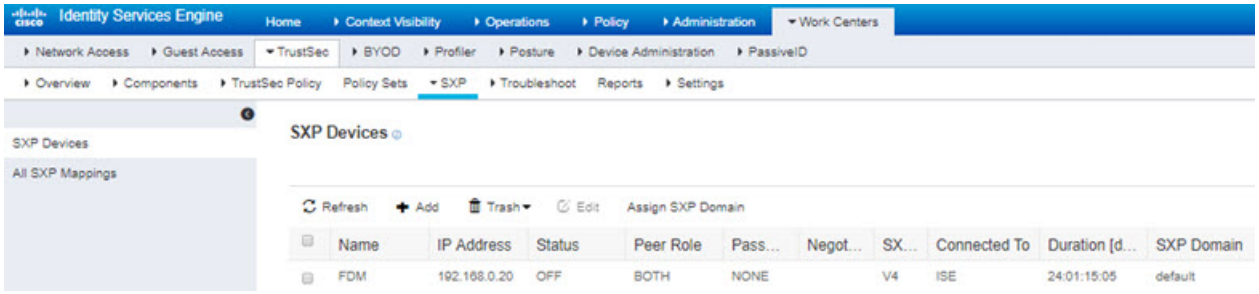
ステップ 1 **[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP設定（SXP Settings）]** を選択し、[PxGridでSXPバインディングを公開（Publish SXP Bindings on PxGrid）] オプションを選択します。

このオプションにより、ISE は SXP を使用して SGT マッピングを送信します。リストから SXP トピックまでを "確認する" には、Threat Defense デバイスに対してこのオプションを選択する必要があります。このオプションは、Threat Defense デバイスが静的 SGT-to-IP アドレスマッピング情報を取得するために選択する必要があります。単に、パケット内で定義された SGT タグ、またはユーザーセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

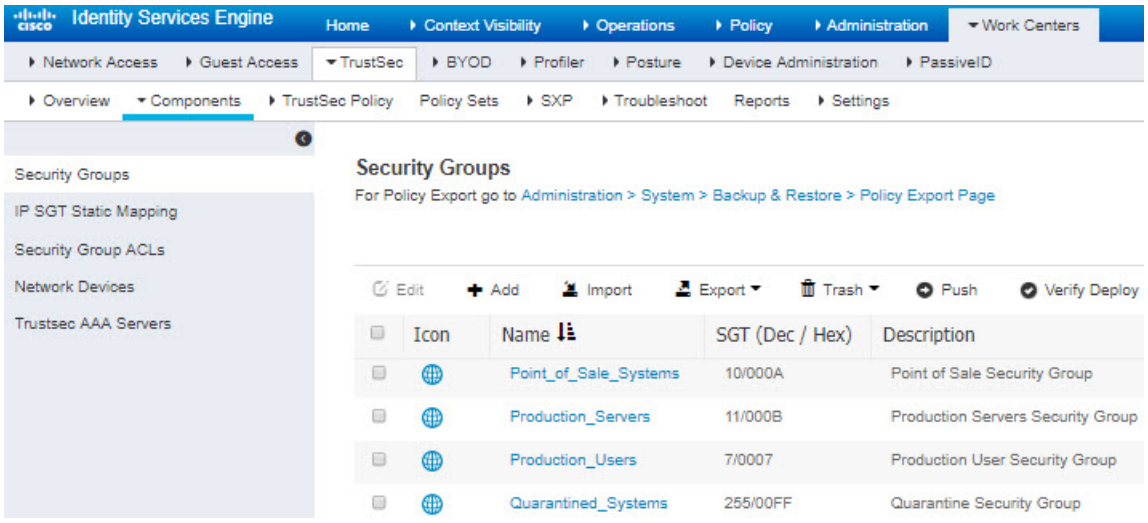


ステップ 2 **[ワークセンター（Work Centers）] > [TrustSec] > [SXP] > [SXPデバイス（SXP Devices）]** を選択し、デバイスを追加します。

これは実際のデバイスである必要はありませんが、脅威に対する防御 デバイスの管理 IP アドレスを使用することもできます。このテーブルには、ISE が静的 SGT-to-IP アドレスマッピングをパブリッシュするためのデバイスが 1 つ以上必要です。単に、パケット内で定義された SGT タグ、またはユーザーセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

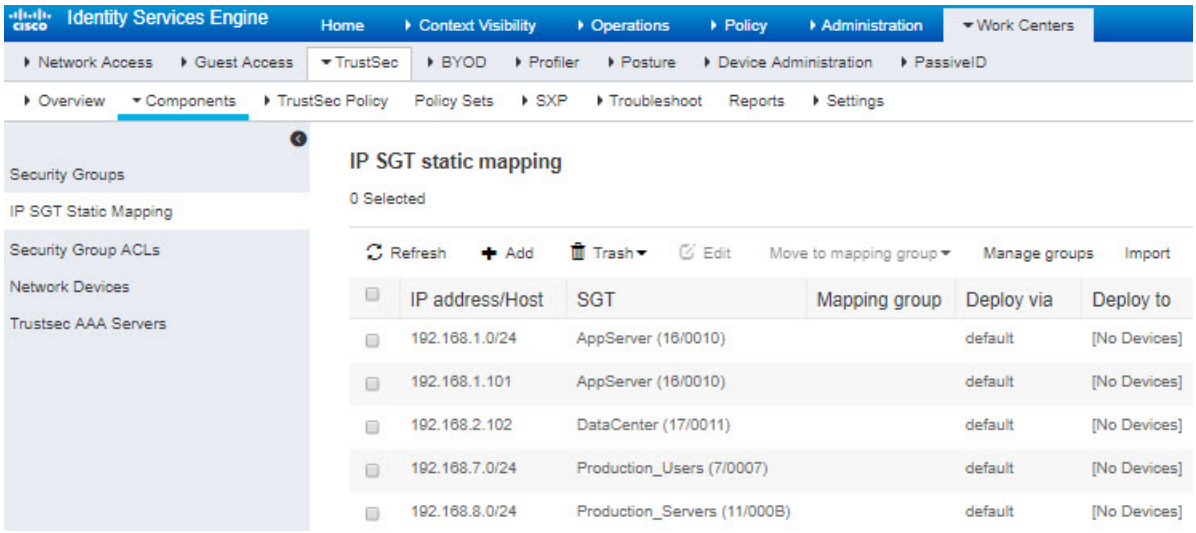


ステップ 3 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]** の順に選択し、セキュリティグループタグが定義されていることを確認します。必要に応じて新しいタグを作成します。



ステップ 4 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGT スタティックマッピング（IP SGT Static Mapping）]** を選択し、ホストとネットワーク IP アドレスをセキュリティ グループ タグにマッピングします。

単に、パケット内で定義された SGT タグ、またはユーザーセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。



Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート

ここでは、次のことを行う方法について説明します。

- ISE/ISE-PIC サーバーからシステム証明書をエクスポートします。

これらの証明書は、ISE/ISE-PIC サーバーに安全に接続するために必要です。ISE システムの設定に応じ、次のうち 1 つまたは最大 3 つの証明書をエクスポートする必要があります。

- pxGrid サーバー用の証明書
- モニターリング（MNT）サーバー用の証明書
- pxGrid クライアント（つまり、Management Center）用の証明書（秘密キーを含む）

  最初の 2 つの証明書とは異なり、これは自己署名証明書です。

- これらの証明書を Management Center にインポートします。
  - pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト** > **オブジェクト管理** > **PKI** > **内部証明書**）
  - pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**）
  - MNT 証明書：信頼できる CA

関連トピック

システム証明書のエクスポート （15 ページ）
ISE/ISE-PIC 証明書のインポート （17 ページ）

システム証明書のエクスポート

システム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

手順

ステップ 1 Cisco ISE GUI で、**[メニュー（Menu）]** アイコン（☰）をクリックし、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** の順に選択します。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、**[エクスポート（Export）]** をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント 値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他の Cisco ISE ノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）]をクリックして、クライアントブラウザを実行しているファイルシステムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は PEM 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は PEM 形式の証明書と暗号化された秘密キーファイルを含む .zip ファイルとしてエクスポートされます。

自己署名証明書の生成

自己署名証明書を生成することで、新しいローカル証明書を追加します。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境に Cisco ISE を展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

（注） 自己署名証明書を使用しており、Cisco ISE ノードのホスト名を変更する場合は、 Cisco ISE ノードの管理ポータルにログインし、古いホスト名が使用されている自己署名証明書を削除してから、新しい自己署名証明書を生成します。そうしないと、Cisco ISE は古いホスト名が使用された自己署名証明書を引き続き使用します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

手順

ステップ 1 Cisco ISE GUI で、[Menu] アイコン（☰）をクリックし、**[Administration]** > **[System]** > **[Certificates]** > **[System Certificates]**を選択します。

セカンダリノードから自己署名証明書を生成するには、**[管理（Administration）]** > **[システム（System）]** > **[サーバー証明書（Server Certificate）]** を選択します。

ステップ 2 ISE-PIC GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。 **[証明書（Certificates）]** > **[システム証明書（System Certificates）]**の順に選択します。

ステップ 3 [自己署名証明書の生成（Generate Self Signed Certificate）] をクリックし、表示されるウィンドウに詳細を入力します。

ステップ 4 この証明書を使用するサービスに基づいて [使用方法（Usage）] 領域のチェックボックスをオンにします。

ステップ 5 証明書を生成するには、[送信（Submit）] をクリックします。

CLI からセカンダリノードを再起動するには、次の順序で次のコマンドを入力します。

a) **application stop ise**
b) **application start ise**

ISE/ISE-PIC 証明書のインポート

この手順は任意です。ユーザー制御用 ISE の設定 （18 ページ） で説明しているように、ISE/ISE-PIC アイデンティティソースを作成するときに ISE サーバー証明書をインポートすることもできます。

始める前に

システム証明書のエクスポート （15 ページ）の説明に従って、ISE/ISE-PIC サーバから証明書をエクスポートします。証明書とキーは、Management Center へのログイン元のマシンに存在している必要があります。

次のように証明書をインポートする必要があります。

- pxGrid クライアント証明書：キーを使用する内部証明書（**オブジェクト**>**オブジェクト管理** > **PKI** > **内部証明書**）
- pxGrid サーバー証明書：信頼できる CA（**[Objects]** > **[Object Management]** > **[PKI]** > **[Trusted CAs]**）
- MNT 証明書：信頼できる CA

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 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** をクリックします。

ステップ 3 [PKI] を展開します。

ステップ 4 [内部証明書（Internal Cert）] をクリックします。

ステップ 5 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 6 画面の指示に従って、証明書と秘密キーをインポートします。

ステップ 7 [信頼できるCA（Add Trusted CAs）] をクリックします。

ステップ 8 [信頼できるCAの追加（Add Trusted CA）] をクリックします。

ステップ 9 画面の指示に従って、pxGrid サーバー証明書をインポートします。

ステップ 10 必要に応じ、上記の手順を繰り返して MNT サーバーの信頼できる CA をインポートします。

次のタスク

ユーザー制御用 ISE の設定 （18 ページ）

ユーザー制御用 ISE の設定

次の手順では、ISE/ISE-PIC アイデンティティソースを設定する方法について説明します。このタスクを実行するには、グローバルドメインに属している必要があります。

始める前に

- Microsoft Active Directory サーバーまたはサポート対象の LDAP サーバーからユーザーセッションを取得するには、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の説明に従って、pxGrid ペルソナを想定し、ISE サーバーのレルムを設定して有効にします。
- SXP を介して公開された SGT から IP アドレスへのマッピングを含む、ISE で定義されているすべてのマッピングを取得するには、次の手順を実行します。別の方法として、次のオプションがあります。
  - パケット内の SGT 情報のみを使用し、ISE からダウンロードされたマッピングを使用しないようにするには、アクセスコントロールルールの作成および編集に記載されている手順をスキップしてください。この場合、送信元条件としてのみ SGT タグを使用できます。これらのタグは、宛先の基準に一致しません。
  - パケットおよびユーザーと IP アドレス/SGT のマッピングでのみ SGT を使用するには、ISE ID ソースの SXP トピックにサブスクライブしたり、SXP マッピングをパブリッシュするように ISE を設定したりしないでください。この情報は送信元と宛先の両方の一致条件に使用できます。
- ISE/ISE-PIC サーバーから証明書をエクスポートし、オプションで「Management Center で使用するための ISE/ISE-PIC サーバーからの証明書のエクスポート （14 ページ）」の説明に従って証明書を Management Center にインポートします。
- Management Center を ISE サーバーのセキュリティグループタグ（SGT）で更新できるように SXP トピックを公開する場合は、「ISE/ISE-PIC の設定 （11 ページ）」を参照してください。

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）] > [アイデンティティ ソース（Identity Sources）]** をクリックします。

ステップ 3 [サービス タイプ（Service Type）] で [Identity Services Engine] をクリックし、ISE 接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 4 [プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）]、およびオプションで [セカンダリ ホスト名/IP アドレス（Secondary Host Name/IP Address）] を入力します。

ステップ 5 [pxGridサーバーCA（pxGrid Server CA）] および [MNTサーバーCA（MNT Server CA）] リストから該当する認証局を、[pxGridクライアント証明書] [FMCサーバー証明書（FMC Server Certificate）] リストから適切な証明書をそれぞれクリックします。また、**Add**(＋)をクリックして証明書を追加することもできます。

（注） [pxGridクライアント証明書（pxGrid Client Certificate）] [FMCサーバー証明書（FMC Server Certificate）] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ステップ 6 （オプション）CIDR ブロック表記を使用して [ISE ネットワーク フィルタ（ISE Network Filter）] を入力します。

ステップ 7 [サブスクライブ先（Subscribe To）] セクションで、次のことを確認します。

- ISE サーバーから ISE ユーザー セッション情報を受信するための [セッションディレクトリのトピック（Session Directory Topic）]。
- ISE サーバーから利用可能な場合に SGT から IP へのマッピングの更新を受信するための [SXPトピック（SXP Topic）]。このオプションは、アクセス コントロール ルールで宛先の SGT タグを使用するために必要です。

ステップ 8 接続をテストするには、[テスト（Test）] をクリックします。

テストが失敗した場合、接続障害に関する詳細については、[その他のログ（Additional Logs）] をクリックします。

次のタスク

- アイデンティティ ポリシーの作成の説明に従って、制御するユーザーおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- Cisco ISE のセキュリティ グループ タグ（SGT）をアクセス コントロール ポリシーのダイナミック属性として使用します。

  詳細については、ダイナミック属性の条件の設定を参照してください。

- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- 『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「*Using Workflows*」の説明に従ってユーザーアクティビティをモニターします。

関連トピック

ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング （21 ページ）
信頼できる認証局オブジェクト
内部証明書オブジェクト

ISE/ISE-PIC 設定フィールド

次のフィールドを使用して /ISE-PIC への接続を設定します。

プライマリおよびセカンダリ ホスト名/IP アドレス（Primary and Secondary Host Name/IP Address）

プライマリ（およびオプションでセカンダリ）pxGrid ISE サーバのホスト名または IP アドレス。

指定するホスト名で使用されるポートには、ISE と Management Center の両方から到達可能である必要があります。

pxGrid サーバー CA（pxGrid Server CA）

pxGrid フレームワークの信頼された証明機関。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT サーバー CA（MNT Server CA）

一括ダウンロード実行時の ISE 証明書の信頼された証明機関。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

pxGrid クライアント証明書

/ISE-PIC への接続時、または一括ダウンロードの実行時に Secure Firewall Management Center が /ISE-PIC に提供する必要がある内部証明書およびキー。

（注） [pxGridクライアント証明書（pxGrid Client Certificate）] [FMCサーバー証明書（FMC Server Certificate）] には、clientAuth 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ISE ネットワーク フィルタ（ISE Network Filter）

オプションのフィルタで、ISE が Secure Firewall Management Center にレポートするデータを制限するために設定できます。ネットワーク フィルタを指定する場合、ISE はそのフィ

ルタ内のネットワークからデータをレポートします。次の方法でフィルタを指定できます。

- **任意（Any）**のフィルタを指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

（注） このバージョンのシステムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

登録：

[セッションディレクトリのトピック（Session Directory Topic）]：このボックスをオンにして、ISE サーバーのユーザーセッションの情報をサブスクライブします。SGT とエンドポイントのメタデータが含まれます。

[SXP トピック（SXP Topic）]：このボックスをオンにして、ISE サーバーからの SXP マッピングをサブスクライブします。

関連トピック

ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング （21 ページ）
信頼できる認証局オブジェクト
内部証明書オブジェクト

ISE/ISE-PIC または Cisco TrustSec の問題のトラブルシューティング

Cisco TrustSec の問題のトラブルシューティング

デバイスインターフェイスでは、ISE / ISE-PIC またはネットワーク上のシスコデバイスからセキュリティグループタグ（SGT）を伝達するように設定できます（Cisco TrustSec と呼ばれます）。デバイス管理ページ（**[Devices]** > **[Device Management]**）では、デバイスの再起動後にインターフェイスの [Propagate Security Group Tag] チェックボックスがオンになります。インターフェイスが TrustSec データを伝播しないようにするには、このボックスをオフにします。

ISE /ISE-PIC の問題のトラブルシューティング

関連の他のトラブルシューティングについては、レルムとユーザーのダウンロードのトラブルシュートおよびユーザー制御のトラブルシューティングを参照してください。

ISE または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE とシステムを正常に統合するには、ISE 内の pxGrid アイデンティティマッピング機能を有効にする必要があります。
- プライマリ サーバーが失敗した場合は、セカンダリをプライマリに手動で昇格させる必要があります。自動でフェール オーバーすることはありません。
- ISE サーバーと Management Center 間の接続を確立するには、ISE のクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

  Cisco Identity Services Engine Administrator Guideの「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。
- [pxGridクライアント証明書（pxGrid Client Certificate）][FMCサーバー証明書（FMC Server Certificate）] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。
- ISE サーバの時刻は、Secure Firewall Management Center の時刻と同期している必要があります。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。
- 展開にプライマリとセカンダリの pxGrid ノードが含まれている場合は、
  - 両方のノードの証明書が、同じ認証局によって署名される必要があります。
  - ホスト名で使用されるポートが、ISE サーバーと Management Center の両方から到達可能である必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ユーザーから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングを ISE から受信するときに、サブネットを除外するには **configure identity-subnet-filter** {**add** | **remove**} コマンドを使用します。通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。

ISE または ISE-PIC によって報告されるユーザー データに関する問題が発生した場合は、次の点に注意してください。

- 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。ISEユーザから見えるアクティビティは、システムがユーザのダウンロードで情報の取得に成功するまでアクセス コントロール ルールで処理されず、Web インターフェイスに表示されません。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Management Centerは、ISE ゲスト サービス ユーザのユーザ データは受信しません。

- ISE が TS エージェントと同じユーザーをモニターする場合、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 ISE が同じ IP アドレスによる同一の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。
- 使用する ISE のバージョンと設定は、システムでの ISE の使用方法に影響を与えます。詳細については、ISE/ISE-PIC アイデンティティ ソース （1 ページ）を参照してください。
- Management Center の高可用性が設定されているとプライマリが失敗する場合は、ISE/ISE-PIC のガイドラインと制限事項 （4 ページ）の ISE と高可用性に関する項を参照してください。
- ISE-PIC は ISE 属性のデータを提供しません。
- ISE-PIC は ISE ANC の修復を実行できません。
- Active FTP sessions are displayed as the **Unknown** user in events. これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバーが接続を開始し、FTP サーバーには関連付けられているユーザー名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

サポートされている機能に問題がある場合は、ISE/ISE-PIC アイデンティティ ソース （1 ページ）で詳細を参照してバージョンの互換性を確認してください。

ISE/ISE-PIC ユーザータイムアウト

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 フィールドを参照してください。

ISE/ISE-PIC の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
pxGrid 2.0 は、サポートされている ISE/ISE-PIC バージョンのデフォルトです	6.7.0	6.7.0	次の点に注意してください。 • サポートされる ISE/ISE-PIC バージョン：2.6 パッチ 6 以降、2.7 パッチ 2 以降 • 適応型ネットワーク制御（ANC）ポリシーは、Endpoint Protection Service（EPS; エンドポイント保護サービス）の修復に取って代わります。Management Center で EPS ポリシーが設定されている場合は、それらを移行して ANC を使用する必要があります。

機能	最小 Management Center	最小 Threat Defense	詳細
必要に応じて、ユーザーから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングを ISE から受信するときに、サブネットを除外します。通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。	6.7.0	6.7.0	新しいコマンド：**configure identity-subnet-filter** {**add** | **remove**}
宛先セキュリティ グループタグ（SGT）の照合	6.5.0	6.5.0	導入された機能。アクセス コントロール ルール内の送信元および宛先の両方の一致基準に ISE SGT タグを使用できるようにします。 SGT タグは、ISE によって取得されたタグからホスト/ネットワークへのマッピングです。 新規/変更された画面： • 宛先 SGT 照合を設定するための新しいオプション： **[システム（System）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）] > [ISE/ISE-PIC]** • [セッションディレクトリのトピック（Session Directory Topic）]：ISE ユーザー セッションの情報をサブスクライブします。 • [SXP トピック（SXP Topic）]：ISE サーバでの SGT タグの更新をサブスクライブします。 • **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** の新しい列および名前が変更された列 • 名前の変更：[セキュリティグループタグ（Security Groups Tags）] が [送信元SGT（Source SGT）] に名称変更されました • 新規：[宛先SGT（Destination SGT）]
ISE-PIC との統合	6.2.1	6.2.1	ISE-PIC のデータを使用できるようになりました。

機能	最小 Management Center	最小 Threat Defense	詳細
ユーザ制御用の SGT タグ。	6.2.1	6.2.0	ISE セキュリティ グループ タグ（SGT）データに基づいてユーザ制御を実行するために、レルムまたはアイデンティティ ポリシーを作成する必要がなくなりました。
ISE との統合。	6.0	6.0	導入された機能。シスコの Platform Exchange Grid（PxGrid）に登録することで、Firepower Management Center で追加のユーザー データ、デバイス タイプ データ、デバイス ロケーション データ、およびセキュリティ グループ タグ（SGT：ネットワーク アクセス コントロールを提供するために ISE によって使用される方式）をダウンロードできます。

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。