Cisco Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）の統合

この章で説明する内容は、次のとおりです。

Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要

Cisco Identity Services Engine（ISE）は、ID 管理を向上させるためにネットワーク上の個々のサーバーで実行されるアプリケーションです。 Secure Web Applianceは、ISE または ISE-PIC のサーバーからユーザーアイデンティティ情報にアクセスできます。ISE または ISE-PIC のいずれかが設定されている場合は、適切に設定された識別プロファイルに対してユーザー名および関連するセキュリティ グループ タグが ISE から、ユーザー名および Active Directory グループが ISE-PIC からそれぞれ取得され、それらのプロファイルを使用するように設定されたポリシーで透過的ユーザー識別が許可されます。

- セキュリティ グループ タグと Active Directory グループを使用してアクセス ポリシーを作成できます。

- ISE/ISE-PIC による透過的な識別に失敗したユーザーの場合、Active Directory ベースのレルムを使用してフォールバック認証を設定できます。「フォールバック認証 （5 ページ）」を参照してください。
- 仮想デスクトップ環境（Citrix、Microsoft 共有/リモート デスクトップ サービスなど）でユーザーの認証を設定できます。「ISE/ISE-PIC 統合での VDI（仮想デスクトップ インフラストラクチャ）ユーザー認証 （18 ページ）」を参照してください。

（注）

- ISE/ISE-PIC サービスはコネクタ モードでは使用できません。
- ISE/ISE-PIC バージョン 2.4、および PxGrid バージョン 2.0 がサポートされます。
- Secure Web Applianceの Web インターフェイスで ISE 設定ページを使用して、ISE または ISE-PIC サーバーの設定、証明書のアップロード、ISE または ISE-PIC のいずれかのサービスへの接続を実行します。ISE または ISE-PIC を設定する手順は似ています。ISE-PIC に固有の詳細が適宜記載されています。

Cisco Secure Web Appliance ISE バージョンのサポートマトリックスの詳細については、『ISE Compatibility Matrix Information』を参照してください。

表 *1 : Secure Web Appliance-ISE* スケール サポート マトリックス

モデル	AD グループが有効になっていないセッションスケール	AD グループが有効になっているセッションスケール	
-	サポートされている最大アクティブセッション数	サポートされている最大アクティブセッション数	サポートされている最大エンドポイント数 （各ユーザーの AD グループエントリと ISE データベース内のエンドポイント）
S680*、S690、S695	200K	125K	400K
S380*、S390、S600V	150K	50K	150K
S190、S195、S300V	50K	50K	75K
S100V	50K	40K	50K

（注）

*S380、S680 モデルは非対応。

関連項目

- pxGrid について （3 ページ）
- ISE/ISE-PIC サーバーの展開とフェールオーバーについて （3 ページ）

pxGrid について

シスコの Platform Exchange Grid（pxGrid）を使用すると、セキュリティ モニターリングとネットワーク検出システム、ID とアクセス管理プラットフォームなど、ネットワーク インフラストラクチャのコンポーネントを連携させることができます。これらのコンポーネントは pxGrid を使用して、パブリッシュまたはサブスクライブ メソッドにより情報を交換します。

以下の 3 つの主要 pxGrid コンポーネントがあります：pxGrid パブリッシャ、pxGrid クライアント、pxGrid コントローラ。

- pxGrid パブリッシャ：pxGrid クライアントの情報を提供します。
- pxGrid クライアント：パブリッシュされた情報をサブスクライブする任意のシステム（Secure Web Applianceなど）。パブリッシュされる情報には、セキュリティグループタグ（SGT）、Active Directory グループ、ユーザーグループおよびプロファイルの情報が含まれます。
- pxGrid コントローラ：クライアントの登録/管理およびトピック/サブスクリプション プロセスを制御する ISE/ISE-PIC pxGrid ノードが該当します。

各コンポーネントには信頼できる証明書が必要です。これらの証明書は各ホストプラットフォームにインストールしておく必要があります。

ISE/ISE-PIC サーバーの展開とフェールオーバーについて

単一の ISE/ISE-PIC ノードのセットアップはスタンドアロン展開と呼ばれ、この 1 つのノードによって、管理およびポリシー サービスが実行されます。フェールオーバーをサポートし、パフォーマンスを向上させるには、複数の ISE/ISE-PIC ノードを分散展開でセットアップする必要があります。 Secure Web Appliance で ISE/ISE-PIC フェールオーバーをサポートするために必要な最小限の分散 ISE/ISE-PIC 構成は以下のとおりです。

- 2 つの pxGrid ノード
- 2 つの管理ノード
- 1 つのポリシー サービス ノード

この構成は、『*Cisco Identity Services Engine Hardware Installation Guide*』では「中規模ネットワーク展開」と呼ばれています。詳細については、『Installation Guide』のネットワーク展開に関する項を参照してください。

関連項目

- ISE/ISE-PIC の証明書 （4 ページ）
- ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）
- ISE/ISE-PIC サービスへの接続 （8 ページ）
- Identity Services Engine に関する問題のトラブルシューティング （18 ページ）

ISE/ISE-PIC の証明書

（注） このセクションでは、ISE/ISE-PIC 接続に必要な証明書について説明します。ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）では、これらの証明書に関する詳細情報を提供します。証明書の管理（Certificate Management）は、AsyncOS の証明書の一般的な管理情報を提供します。

Secure Web Applianceと各 ISE/ISE-PIC サーバー間で相互認証と安全な通信を行うには、一連の 2 つの証明書が必要です。

- **Web Appliance クライアント証明書**： Secure Web Applianceを認証するために ISE/ISE-PIC サーバーで使用されます。
- **ISE pxGrid 証明書**： Secure Web Appliance-ISE/ISE-PIC データサブスクリプション（ISE/ISE-PIC サーバーに対する進行中のパブリッシュ/サブスクライブクエリー）向けに ISE/ISE-PIC サーバーを認証するためにポート 5222 で Secure Web Applianceによって使用されます。

この 2 つの証明書は、認証局（CA）による署名でも自己署名でもかまいません。CA 署名付き証明書が必要な場合、AsyncOS には自己署名 Web Appliance クライアント証明書、または証明書署名要求（CSR）を生成するオプションがあります。同様に ISE/ISE-PIC サーバーにも、CA 署名付き証明書が必要な場合に、自己署名 ISE/ISE-PIC pxGrid 証明書、または CSR を生成するオプションがあります。

関連項目

- 自己署名証明書の使用 （5 ページ）
- CA 署名付き証明書の使用 （5 ページ）
- Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要（1 ページ）
- ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）
- ISE/ISE-PIC サービスへの接続 （8 ページ）

自己署名証明書の使用

自己署名証明書がISE/ISE-PICサーバーで使用される場合は、ISE/ISE-PICサーバーで開発されたISE/ISE-PIC pxGrid証明書、 Secure Web Applianceで開発されたWeb Applianceクライアント証明書を、ISE/ISE-PICサーバー上の信頼できる証明書ストアに追加する必要があります（**ISE**の場合は[管理（Administration）]>[証明書（Certificates）]>[信頼できる証明書（Trusted Certificates）]>[インポート（Import）]、**ISE-PIC**の場合は[証明書（Certificates）]>[信頼できる証明書（Trusted Certificates）]>[インポート（Import）]）。

⚠

注意 認証に自己署名証明書を使用するのは、他の認証方法ほど安全ではないためお勧めしません。また、自己署名証明書は失効ポリシーをサポートしていません。

CA署名付き証明書の使用

CA署名付き証明書の場合：

- ISE/ISE-PICサーバーで、Web Applianceクライアント証明書に適したCAルート証明書が信頼できる証明書ストアにあることを確認します（[管理（Administration）]>[証明書（Certificates）]>[信頼できる証明書（Trusted Certificates）]）。
- Secure Web Applianceで、適切なCAルート証明書が信頼できる証明書リストにあることを確認します（[ネットワーク（Network）]>[証明書管理（Certificate Management）]>[信頼できるルート証明書の管理（Manage Trusted Root Certificates）]）。
- [Identity Services Engine]ページ（[ネットワーク（Network）]>[Identity Services Engine]）で、ISE/ISE-PIC pxGrid証明書用のCAルート証明書がアップロードされていることを確認します。

フォールバック認証

ISE/ISE-PICで利用できないユーザー情報については、フォールバック認証を設定できます。フォールバック認証が成功するには、次のものが必要です。

- Active Directoryベースのレルムのフォールバックオプションで設定された識別プロファイル。
- フォールバックオプションを含む正しい識別プロファイルを使用したアクセスポリシー。

ISE/ISE-PIC サービスを統合するためのタスク

（注）

- ISE/ISE-PIC バージョン 2.4、および PxGrid バージョン 2.0 がサポートされます。
- ISE-PIC で既存のアクセス ポリシーの使用を続行するには、ISE-PIC を使用する各識別プロファイルを編集してユーザーを透過的に識別する必要があります。これは、CDA を使用した識別プロファイルに適用されます。CDA 識別から ISE-PIC ベースの識別に移行している場合は、それぞれの識別プロファイルを編集する必要があります。

（注）

- AsyncOS 11.5 以前のバージョンから AsyncOS 11.7 以降のバージョンにアップグレードする場合は、 Secure Web Applianceで ISE を再設定します。
- 証明書は ISE/ISE-PIC デバイスを介して生成する必要があり、生成された証明書は Secure Web Applianceにアップロードする必要があります。

ステップ	タスク	トピックおよび手順へのリンク
1	ISE/ISE-PIC デバイスを介した証明書の生成。	ISE/ISE-PIC を介した証明書の生成 （7 ページ）
2	Secure Web Applianceにアクセスするために ISE/ISE-PIC を設定する。	Secure Web Applianceにアクセスするための ISE/ISE-PIC サーバーの設定 （7 ページ）
3	Secure Web Applianceで ISE/ISE-PIC サービスを設定および有効にする。	ISE/ISE-PIC サービスへの接続 （8 ページ）
4	Secure Web Appliance クライアント証明書が自己署名済みの場合は、 ISE/ISE-PIC にインポートする。	自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC スタンドアロン展開へのインポート （11 ページ） 自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC 分散型展開へのインポート （12 ページ）
5	必要に応じて、 Secure Web Applianceでロギングを設定する。	ISE/ISE-PIC へのロギングの設定 （13 ページ）
6	ISE/ISE-PIC ERS サーバーの詳細を取得します。	ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得 （14 ページ）

関連項目

- Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要（1 ページ）
- ISE/ISE-PIC の証明書 （4 ページ）
- Identity Services Engine に関する問題のトラブルシューティング （18 ページ）

ISE/ISE-PIC を介した証明書の生成

（注） ISE/ISE-PIC デバイスを介して生成される証明書は、PKCS12 形式である必要があります。

- **ISE/ISE-PIC**：

ステップ 1 [ワークセンター（Work Centers）] > [PassiveID] > [サブスクライバ（Subscribers）] > [証明書（Certificates）] を選択します。

ステップ 2 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウンリストから [PKCS12形式（PKCS 12 format）] を選択します。[証明書（Certificates）] タブでその他の必要な情報を入力し、pxGrid 証明書を生成します。

ステップ 3 次の `openssl` コマンドを使用して、生成された XXX.pk12 ファイルからルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを抽出します。

- **ルート CA**： openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem
- **Web Appliance クライアント証明書**：openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem
- **Web Appliance クライアントキー**：openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem

（注） 証明書パスワードは、手順 2 の実行中に ISE Web インターフェイスで入力したものを使用してください。

（注） セカンダリ/フェールオーバー ISE サーバーを介してセカンダリルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを生成するには、同じ手順を実行します。

Secure Web Applianceにアクセスするための ISE/ISE-PIC サーバーの設定

- **ISE**

- 識別トピックサブスクライバ（Secure Web Applianceなど）がリアルタイムでセッションコンテキストを取得できるように、各 ISE サーバーを設定する必要があります。

  1. **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [設定（Settings）] > [pxGridの設定（pxGrid Settings）]** を選択します。
  2. **[新しい証明書ベースのアカウントを自動的に承認する（Automatically approve new certificate-based accounts）]** がオンになっていることを確認します。

  ISE/ISE-PIC での認証に関与しない、設定済みの古い Secure Web Applianceをすべて削除します。

  ISE サーバーのフッターが緑で、**「pxGrid に接続されました（Connected to pxGrid）」**と表示されていることを確認します。

- **ISE-PIC**

  - 識別トピックサブスクライバ（Secure Web Applianceなど）がリアルタイムでセッションコンテキストを取得できるように、各 ISE-PIC サーバーを設定する必要があります。

    1. **[サブスクライバ（Subscribers）] > [設定（Settings）]** を選択します。
    2. **[新しい証明書ベースのアカウントを自動的に承認する（Automatically approve new certificate-based accounts）]** がオンになっていることを確認します。

    ISE/ISE-PIC での認証に関与しない、設定済みの古い Secure Web Applianceをすべて削除します。

    ISE サーバーのフッターが緑で、**「pxGrid に接続されました（Connected to pxGrid）」**と表示されていることを確認します。

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

ISE/ISE-PIC サービスへの接続

（注） ISE 管理証明書、pxGrid 証明書、および MNT 証明書がルート CA 証明書によって署名されている場合は、アプライアンスで [ISE pxGrid ノード証明書（ISE pxGrid Node Certificate）] フィールドにルート CA 証明書自体をアップロードします（[ネットワーク（Network）] > [Identity Services Engine]）。

始める前に

- 各 ISE/ISE-PIC サーバーが Secure Web Applianceへのアクセス用に正しく設定されていることを確認します（ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）を参照）。

- 有効な ISE/ISE-PIC 関連の証明書およびキーを取得します。関連情報については、ISE/ISE-PIC を介した証明書の生成 （7 ページ）を参照してください。
- 取得した RootCA.pem を Secure Web Applianceにインポートします（[ネットワーク（Network）] > [CertificateManagement] > [TrustedRootCertificate] > [ManageTrustedRootCertificate 上のクライアント（Client on ManageTrustedRootCertificate）]）。生成された XXX.pk12 ファイルからルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを抽出するには、ISE/ISE-PIC を介した証明書の生成 （7 ページ）を参照してください。

（注） セカンダリ XXXX.pk12 ファイルから抽出された RootCA.pem について同じ手順に実行します（セカンダリ/フェールオーバー ISE サーバーが使用可能な場合）。

- Secure Web Applianceの Web インターフェイスで ISE 設定ページを使用して、ISE または ISE-PIC サーバーの設定、証明書のアップロード、ISE または ISE-PIC のいずれかのサービスへの接続を実行します。ISE と ISE-PIC を設定する手順は同じです。ISE-PIC 設定に固有の詳細が適宜記載されています。
- ISE/ISE-PIC が提供する Active Directory グループを使用してアクセスポリシーを構築する場合は、ERS を有効にします。
- AsyncOS 15.0 リリースの一部として、OpenSSL バージョン 1.1.1 およびライブラリは IP ベースの証明書を受け入れなくなりました。[テスト開始（Start Test）] が成功し、ISE が期待どおりに機能することを確認するには、SWA ISE 設定でホスト名のみを使用する必要があります。

ステップ 1 [ネットワーク（Network）] > [Identification Service Engine] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ISE/ISE-PIC を初めて設定する場合は、[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 3 [ISEサービスを有効にする（Enable ISE Service）] をオンにします。

ステップ 4 ホスト名または IPv4 アドレスを使用して**プライマリ管理ノード**を特定し、 Secure Web Applianceの [プライマリ ISE pxGrid ノード（Primary ISE pxGrid Node）] タブに次の情報を入力します。

a) Secure Web Appliance-ISE/ISE-PIC データサブスクリプション（ISE/ISE-PIC サーバーに対して進行中のクエリー）用の **ISE pxGrid ノード証明書**を指定します。

プライマリ ISE サーバーからルート CA として生成される証明書（つまり、RootCA.pem）（または、すべての中間証明書を含む証明書チェーン）を参照して選択し、ISE/ISE-PIC を介した証明書の生成（7 ページ）を参照して [ファイルのアップロード（Upload File）] をクリックします。詳細については、証明書およびキーのアップロードを参照してください。

ステップ 5 フェールオーバー用に 2 台目の ISE/ISE-PIC サーバーを使用している場合は、ホスト名または IPv4 アドレスを使用してその**プライマリ管理ノード**を特定し、ホスト名または IPv4 アドレスを使用して Secure Web Applianceの [セカンダリISE pxGridノード（Secondary ISE pxGrid Node）] タブに次の情報を入力します。

a) セカンダリ **ISE pxGrid ノード証明書**を入力します。

セカンダリ ISE サーバーからルート CA として生成される証明書（つまり、**RootCA.pem**）（または、すべての中間証明書を含む証明書チェーン）を参照して選択し、ISE/ISE-PIC を介した証明書の生成 （7 ページ）を参照して [ファイルのアップロード（Upload File）] をクリックします。詳細については、証明書およびキーのアップロードを参照してください。

（注） プライマリからセカンダリの ISE サーバーにフェールオーバーするときに、既存の ISE SGT キャッシュに含まれていないユーザーは、 Secure Web Applianceの設定に応じて、認証が必要になるか、またはゲスト認証が割り当てられます。ISE フェールオーバーが完了すると、通常の ISE 認証が再開されます。

ステップ 6 Secure Web Appliance-ISE/ISE-PIC サーバーの相互認証用の **Web Appliance クライアント証明書**を指定します。

- **[アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）]**

証明書とキーの両方に対して、[選択（Choose）] をクリックして各ファイルを参照します。

（注） ISE/ISE-PIC デバイスを介して生成された publicCert.pem と privateKey.pem を選択してアップロードします。「ISE/ISE-PIC を介した証明書の生成 （7 ページ）」を参照してください。

キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] チェックボックスをオンにします。

[ファイルのアップロード（Upload Files）] をクリックします。（このオプションの詳細については、証明書およびキーのアップロードを参照してください）。

ステップ 7 ISE SGT eXchange Protocol（SXP）サービスを有効にします。

Secure Web Applianceが ISE サービスから SXP バインディングトピックを取得する方法については、SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化 （16 ページ）を参照してください。

ステップ 8 ISE 外部 Restful サービス（ERS）を有効にします。

- ERS 管理者のユーザー名とパスワードを入力します。ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得 （14 ページ）を参照。
- ERS が同じ ISE または ISE/ISE-PIC pxGrid ノードで使用可能な場合は、[ISE pxGridノードと同じサーバー名（Server name same as ISE pxGrid Node）] チェックボックスを確認します。同じノードで使用できない場合は、プライマリおよびセカンダリ（設定されている場合）サーバーのホスト名または IPv4 アドレスを入力します。

ステップ 9 **[テスト開始（Start Test）]** をクリックして、ISE/ISE-PIC の pxGrid ノードと同じ接続をテストします。

ステップ 10　[送信（Submit）] をクリックします。

次のタスク

- ユーザーおよびクライアント ソフトウェアの分類
- インターネット要求を制御するポリシーの作成

関連情報

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html 特に「How To Integrate Cisco Secure Web Appliance using ISE/ISE-PIC and TrustSec through pxGrid..」。

自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC スタンドアロン展開へのインポート

基本的な手順は以下のとおりです。

- **ISE 管理ノード**
  - **[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** の順に選択します。

  次のオプションがオンになっていることを確認してください。
  - [ISE内の認証用に信頼する（Trust for authentication within ISE）]
  - [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
  - [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]
- **ISE-PIC 管理ノード**
  - **[証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** の順に選択します。

    次のオプションがオンになっていることを確認してください。
    - [ISE内の認証用に信頼する（Trust for authentication within ISE）]
    - [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
    - [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC 分散型展開へのインポート

基本的な手順は以下のとおりです。

- **ISE 管理ノード**：
  - **[管理（Administration）]** > **[証明書（Certificates）]** > **[証明書の管理（Certificate Management）]** > **[信頼できる証明書（Trusted Certificates）]** > **[インポート（Import）]** の順に選択します。

  次のオプションがオンになっていることを確認してください。
  - [ISE内の認証用に信頼する（Trust for authentication within ISE）]
  - [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
  - [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]

- **ISE-PIC 管理ノード**：
  - **[証明書（Certificates）]** > **[証明書の管理（Certificate Management）]** > **[信頼できる証明書（Trusted Certificates）]** > **[インポート（Import）]** の順に選択します。

    次のオプションがオンになっていることを確認してください。
    - [ISE内の認証用に信頼する（Trust for authentication within ISE）]
    - [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
    - [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

（注） 分散型 ISE 展開では、 Secure Web Applianceは MNT、PAN、および PxGrid ノードと通信します。この場合、証明書またはすべての証明書の発行者が、「抽出されたルート証明書」（つまり、ISE/ISE-PIC デバイスを介して生成された RootCA）で使用できる必要があります。「ISE/ISE-PIC を介した証明書の生成 （7 ページ）」を参照してください。

ステップ 1 ISE/ISE-PIC を介した証明書の生成 （7 ページ）の手順に従って、RootCA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを生成します。

ステップ 2 **ISE/ISE-PIC 管理ノード**で、[ISE/ISE-PIC] > [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] から自己署名証明書を手動でエクスポートします。

1. [pxGrid]、[EAP認証（EAP Authentication）]、[管理（Admin）]、[ポータル（Portal）]、[RADIUS DTLS] のいずれかによって使用されている（Used by）証明書を選択します。
2. [エクスポート（Export）] をクリックし、生成された .pem ファイルを保存します。

すべての ISE/ISE-PIC 分散ノードについて上記の手順を繰り返します。

ステップ 3 `openssl` コマンドを使用して、ダウンロードした証明書ファイルを RootCA.pem に手動で追加します。ISE/ISE-PIC デバイスを介して RootCA.pem で証明書ファイルを生成および抽出する方法については、ISE/ISE-PIC を介した証明書の生成 （7 ページ）を参照してください。

1. ダウンロードした証明書に対して次のコマンドを実行します。

   ```
   Example:

   openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:

   例（出力）：

   Issuer: CN=isehcamnt2.node
   Subject: CN=isehcamnt2.node
   ```

2. 内容を次のように変更します。

   ```
   Example:
   Subject=/CN=isehcamnt2.node
   Issuer=/CN=isehcamnt2.node
   ```

3. RootCA.pem に次の行を追加します。

   ```
   Bag Attributes: <Empty Attributes>
   ```

4. 手順 (2) のサブジェクトおよび発行者を RootCA.pem に（手順 (3) の行とともに）追加します。

   ```
   Example:
   Bag Attributes: <Empty Attributes>
   Subject=/CN=isehcamnt2.node
   Issuer=/CN=isehcamnt2.node
   ```

5. ダウンロードした証明書ファイルの内容全体をコピーし、RootCA の末尾（手順 (4) のデータの後）に貼り付けます。

   ダウンロードされたすべての分散型 ISE/ISE-PIC ノードの証明書について手順 (1) ～ (5) を繰り返し、変更された RootCA 証明書を保存します。

ステップ 4 Secure Web Applianceの ISE 設定ページで、変更された RootCA.pem をアップロードします。ISE/ISE-PIC サービスへの接続 （8 ページ） を参照してください。

ISE/ISE-PIC へのロギングの設定

- 認証メカニズムをログ記録するために、アクセスログにカスタムフィールド%mを追加します（アクセス ログのカスタマイズ）。
- ISE/ISE-PIC サービスログが作成されていることを確認します。作成されていない場合は作成します（ログ サブスクリプションの追加および編集）。

- ユーザーの識別と認証のために ISE/ISE-PIC にアクセスする識別プロファイルを定義します（「ユーザーおよびクライアントソフトウェアの分類」、117 ページ）。
- ISE/ISE-PIC ID を使用して、ユーザー要求の条件とアクションを定義するアクセスポリシーを設定します（「ポリシーの設定」、191 ページ）。

ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得

- ISE/ISE-PIC で Cisco ISE の REST API（API で HTTPS ポート 9060 を使用）を有効にします。

（注） グループに基づいてセキュリティポリシーを設定するには、Secure Web Applianceで ISE 外部 RESTful サービス（ERS）を有効にする必要があります（[ネットワーク（Network）] > [Identity Services Engine]）。これは、バージョン 11.7 以降に適用されます。

  - **ISE**
    - **[管理（Administration）] > [設定（Settings）] > [ERS設定（ERS Settings）] > [プライマリ管理ノードのERS設定（ERS settings for primary admin node）] > [ERSを有効化する（Enable ERS）]** を選択します。

      セカンダリ ノードがある場合は、**[その他すべてのノードの読み取り用ERS（ERS for Read for All Other Nodes）]** を有効にします。
  - **ISE-PIC**
    - **[設定（Settings）] > [ERS設定（ERS Settings）] > [ERSを有効化する（Enable ERS）]** を選択します。

- 正しい外部 RESTful サービス グループで ISE 管理者を作成していることを確認します。外部 RESTful サービス管理者グループには、ERS API へのフル アクセス（GET、POST、DELETE、PUT）が含まれています。このユーザーは、ERS API 要求を作成、読み取り、更新、および削除できます。外部 RESTful サービス オペレータ：読み取り専用アクセス（GET 要求のみ）。
  - **ISE**
    - **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）]** を選択します。
  - **ISE-PIC**
    - **[管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者ユーザー（Admin Users）]** を選択します。

ERS サービスが ISE/ISE-PIC pxGrid ノードではなく別のサーバーで使用可能な場合は、プライマリおよびセカンダリ（設定されている場合）サーバーのホスト名または IPv4 アドレスが必要です。

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

ISE-SXP 統合の設定

このセクションは、次のトピックで構成されています。

SGT から IP へのアドレスマッピングの ISE-SXP プロトコルについて

SGT Exchange Protocol（SXP）は、ネットワークデバイス間で IP-SGT バインディングを伝播するために開発されたプロトコルです。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 Identity Services Engine（ISE）の展開を Cisco Secure Web Applianceと統合して、パッシブ認証に使用できます。 Secure Web Applianceは、ISE から SXP マッピングをサブスクライブできます。ISE は SXP を使用して、SGT から IP へのアドレス マッピング データベースを管理対象デバイスに伝播します。ISE サーバーを使用するように Secure Web Appliance 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。これにより、 Secure Web Applianceは ISE から直接 SGT と IP アドレスマッピングについて学習します。

Secure Web Applianceは、ダミーのユーザー認証 IP アドレスを生成します。これには、ISE クラスタの IP アドレスとクライアントの IP アドレスが含まれます。したがって、複数のクライアント IP アドレスをクラスタ IP アドレスで認証できます。

注意事項と制約事項

SGT から IP アドレスへのマッピングの ISE-SXP プロトコルに関するガイドラインと制限は次のとおりです。

- IPv6 対応のエンドポイントは、 Secure Web Appliance リリース 14.5 ではサポートされません。
- Secure Web Appliance リリース 14.5 では、ユーザー名とグループマッピングは、SGT から IP アドレスへのマッピングでは使用できません。したがって、管理者は Secure Web

Applianceの ISE ユーザーおよびグループに基づいてポリシーを作成することはできません。ただし、SGT を使用してポリシーを作成できます。

- 一括ダウンロードプロセスの再起動タイムスタンプをスケジュールするには、isedプロセスを再起動する時刻を HH::MM 形式（24 時間）で設定する必要があります。

（注） ユーザー認証プロセスが示される時刻は 1 日の中で短時間に設定することをお勧めします。たとえば、00:00 時に設定します。

前提条件

SGT から IP アドレスへのマッピングの ISE-SXP プロトコルに関する前提条件は次のとおりです。

- 信頼できるルート証明書が必要です。信頼できるルート証明書を追加するには、「信頼できるルート証明書の管理」を参照してください。

SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化

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は、SXP を介して公開できます。次のメカニズムを使用して、ISE-SXP 情報を取得できます。

- 一括ダウンロード：isedプロセスの再起動後、 Secure Web Applianceは、集約ノードで使用可能なすべての ISE-SXP エントリの情報を取得するために、一括ダウンロード要求を ISEアグリゲータノードに送信します。AsyncOS コマンドラインインターフェイス（CLI）を使用して、再起動のタイムスタンプをスケジュールできます。
- 差分更新： Secure Web Applianceは、WebSocket を介して登録し、差分更新メッセージを取得します。メッセージには次の 2 つのタイプがあります。
  - 作成：新しく作成されたすべてのエントリ
  - 削除：すべての SXP 更新エントリ

（注） Secure Web Applianceは、更新されたエントリごとに 2 つのメッセージ（「削除（Delete）」の後に「作成（Create）」）を受信します。

再起動をスケジュールすることができます。

ステップ 1 **[ネットワーク（Network）]** > **[Identification Service Engine]**を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [ISEサービスを有効にする（Enable ISE Service）] をオンにします。

ステップ 4 Secure Web Applianceで ISE サービスから SXP バインディングトピックを取得できるようにするには、[有効（Enable）] をオンにします。

デフォルトでは、ISE SGT eXchange Protocol（SXP）サービスは無効になっています。

ステップ 5 [テスト開始（Start Test）] をクリックして接続をテストします。

（注） SXP 情報は、ISE-SGT eXchange Protocol（SXP）サービスが有効になっている場合にのみ表示されます。

ステップ 6 **[送信（Submit）]** をクリックします。

ISE-SXP プロトコルのコンフィギュレーションの確認

次のいずれかの方法を使用して、ISE-SXP プロトコルのコンフィギュレーションを確認できます。

- SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化 （16 ページ） で [テスト開始（Start Test）] をクリックして、表示された情報を確認します。
- AsyncOS コマンド ライン インターフェース（CLI）の **ISEDATA** コマンドの下で **STATISTICS** コマンドを使用します。

STATISTICS コマンドを使用すると、次の情報が表示されます。

- ERS ホスト名
- ERS 接続時間
- セッション一括ダウンロード
- グループ一括ダウンロード
- SGT 一括ダウンロード
- SXP 一括ダウンロード
- セッションの更新
- グループの更新
- SXP の更新
- Memory Allocation
- メモリの割り当て解除
- Total Session Count

ユーザー名は次の形式で生成されます。

```
isesxp_<ISE-node-ip>_sgt<SGT number>_<Client IP address>
```

例：isesxp_10.10.2.68_sgt18_10.10.10.10

ISE/ISE-PIC 統合での VDI（仮想デスクトップ インフラストラクチャ）ユーザー認証

使用される送信元ポートに基づいて VDI 環境のユーザーの ISE/ISE-PIC による透過的な識別を設定できます。

Cisco Terminal Services（TS）エージェントを VDI サーバーにインストールする必要があります。Cisco TS エージェントは、ISE/ISE-PIC にアイデンティティ情報を提供します。アイデンティティ情報には、ドメイン、ユーザー名、および各ユーザーが使用するポート範囲が含まれます。

- サポートサイト（https://www.cisco.com/c/en/us/support/index.html）から Cisco TS エージェントをダウンロードします。
- 詳細については、『Cisco Terminal Services (TS) Agent Guide』（https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html）を参照してください。
- Cisco TS エージェントと連携するように ISE/ISE-PIC API プロバイダを設定します。API コールの送信については、Cisco TS エージェントのドキュメントを参照してください。

（注）

- VDI 環境ユーザーのフォールバック認証はサポートされていません。
- シスコ ターミナル サービス エージェントと Microsoft サーバー設定で、リモート デスクトップ セッションの最大数が同じであることを確認します。これにより、誤ったセッション情報が ISE から Secure Web Applianceに送信されないようにし、新しいセッションの誤認証が回避されます。

Identity Services Engine に関する問題のトラブルシューティング

- Identity Services Engine に関する問題
  - ISE 問題のトラブルシューティング ツール
  - ISE サーバーの接続に関する問題
  - ISE 関連の重要なログ メッセージ

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。