



Cisco Identity Services Engine の統合

- [Identity Services Engine サービスの概要 \(8-1 ページ\)](#)
- [Identity Services Engine の証明書 \(8-2 ページ\)](#)
- [ISE サービスを認証および統合するためのタスク \(8-4 ページ\)](#)
- [ISE サービスへの接続 \(8-6 ページ\)](#)
- [Identity Services Engine に関する問題のトラブルシューティング \(8-8 ページ\)](#)

Identity Services Engine 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で実行されるアプリケーションです。AsyncOS は ISE サーバからユーザ ID 情報にアクセスできます。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名および関連するセキュリティグループタグが Identity Services Engine から取得され、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識別が許可されます。



(注) ISE サービスはコネクタ モードでは使用できません。

関連項目

- [pxGrid について \(8-1 ページ\)](#)
- [ISE サーバの展開とフェールオーバーについて \(8-2 ページ\)](#)

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 (Web セキュリティ アプライアンスなど)。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) とユーザ 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: 本書では、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 pxGrid ノードです。

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 サーバの展開とフェールオーバーについて

単一の ISE 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、ポリシー サービス、およびモニタリングが実行されます。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 ノードを「分散展開」でセットアップする必要があります。Web セキュリティ アプライアンスで ISE 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 構成は以下のとおりです。

- 2 つの pxGrid ノード
- 2 つのモニタリング 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

- [Identity Services Engine の証明書 \(8-2 ページ\)](#)
- [ISE サービスを認証および統合するためのタスク \(8-4 ページ\)](#)
- [ISE サービスへの接続 \(8-6 ページ\)](#)
- [Identity Services Engine に関する問題のトラブルシューティング \(8-8 ページ\)](#)

Identity Services Engine の証明書



(注)

ここでは、ISE 接続に必要な証明書について説明します。[ISE サービスを認証および統合するためのタスク \(8-4 ページ\)](#)には、これらの証明書に関する詳細情報が記載されています。[証明書の管理 \(22-26 ページ\)](#)には、AsyncOS の一般的な証書管理情報が記載されています。

Web セキュリティ アプライアンスと各 ISE サーバ間の相互認証と安全な通信のために、一連の 3 つの証明書が必要です。

- **WSA クライアント証明書:** ISE サーバで Web セキュリティ アプライアンスを認証するために使用されます。
- **ISE 管理証明書:** Web セキュリティ アプライアンスで ISE サーバの認証に使用され、ポート 443 での ISE ユーザプロファイルデータの一括ダウンロードを許可します。
- **ISE pxGrid 証明書:** Web セキュリティ アプライアンスで ISE サーバの認証に使用され、ポート 5222 での WSA-ISE データ サブスクリプション (ISE サーバ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) を許可します。

この 3 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 WSA 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 サーバにも、CA 署名付き証明書が必要な場合に、自己署名 ISE 管理証明書や 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 \(8-3 ページ\)](#)
- [CA 署名付き証明書の使用 \(8-3 ページ\)](#)
- [Identity Services Engine サービスの概要 \(8-1 ページ\)](#)
- [ISE サービスを認証および統合するためのタスク \(8-4 ページ\)](#)
- [ISE サービスへの接続 \(8-6 ページ\)](#)

自己署名証明書の使用

自己署名証明書が ISE サーバで使用される場合は、3 つのすべての証明書: ISE サーバで開発された ISE pxGrid 証明書および ISE 管理証明書、WSA で開発された WSA クライアント証明書を、ISE サーバ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 ([管理 (Administration)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)])。

CA 署名付き証明書の使用

CA 署名付き証明書の場合:

- ISE サーバで、WSA 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)])。
- WSA 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 管理証明書および 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。

ISE サービスを認証および統合するためのタスク

手順	タスク	関連項目および手順へのリンク
1a	WSA に、WSA クライアント証明書を追加します。	<ul style="list-style-type: none"> CA 署名付きまたは自己署名の WSA クライアント証明書を作成するか、WSA にアップロードします。 <p>ISE サービスへの接続(8-6 ページ) および 証明書の管理(22-26 ページ) を参照してください。</p>
1b	WSA に、ISE サーバへのアップロード用にこの WSA クライアント証明書をダウンロードします。	<ul style="list-style-type: none"> WSA クライアント証明書をダウンロードして保存し、ISE サーバに転送します。 <p>ISE サービスへの接続(8-6 ページ) を参照してください。</p>
2	WSA クライアント証明書が自己署名の場合は、署名証明書とともに ISE サーバにアップロードします。	<ul style="list-style-type: none"> 前のステップで WSA からダウンロードした WSA クライアント証明書をインポートし、ISE サーバの信頼できる証明書ストアに追加します。([管理(Administration)] > [証明書(Certificates)] > [信頼できる証明書(Trusted Certificates)] > [インポート(Import)])。 また、この WSA クライアント証明書に適した署名証明書が、ISE サーバの信頼できる証明書ストアに追加されていることを確認します(自己署名証明書の使用(8-3 ページ) 参照)。
3	ISE サーバに、ISE 管理証明書および pxGrid 証明書を追加します。	<ul style="list-style-type: none"> [管理(Administration)] > [証明書(Certificates)] ページに移動し、ISE 管理証明書および pxGrid 証明書を作成するか、またはアップロードします。 <ul style="list-style-type: none"> CA 署名付き証明書の場合は、Admin と pxGrid 用として 2 つの証明書署名要求を作成し、証明書に署名してもらいます。 署名付き証明書を受信したら、両証明書を ISE サーバにアップロードします。 両証明書に対し、「CA 署名付き証明書とバインドさせる」操作を行います。 ISE サーバの信頼できる証明書ストアに CA ルート証明書が追加されていることを確認します。 ISE サーバを再起動します。 自己署名証明書の場合は、[管理(Administration)] > [証明書(Certificates)] > [システム証明書(System Certificates)] に移動し、2 つの自己署名証明書(pxGrid と管理用に 1 つずつ)を生成します。(両方に対して共通の証明書を 1 つ生成することも選択できます)。 信頼できる証明書ストアに両証明書を追加します。 WSA にインポートする自己署名証明書をエクスポートします。 <p>(注) これらの ISE 管理証明書および pxGrid 証明書に適した自己署名または CA ルート証明書が、信頼できる証明書ストアに追加されたことを確認します(Identity Services Engine の証明書(8-2 ページ) 参照)。</p>

手順	タスク	関連項目および手順へのリンク
4	ISE サーバが WSA アクセス用に正しく設定されていることを確認する。	<p>識別トピック サブスクリバ(WSA 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 サーバを設定する必要があります。基本的な手順は以下のとおりです。</p> <ul style="list-style-type: none"> • [自動登録の有効化(Enable Auto Registration)] がオンになっていることを確認します([管理(Administration)] > [pxGrid サービス(pxGrid Services)] > [右上(Top Right)])。 • ISE サーバから既存の WSA クライアントをすべて削除します([管理(Administration)] > [pxGrid サービス(pxGrid Services)] > [クライアント(Clients)])。 • ISE サーバのフッターが [pxGrid に接続(Connected to pxGrid)] に設定されていることを確認します([管理(Administration)] > [pxGrid サービス(pxGrid Services)])。 • ISE サーバに SGT グループを設定します([ポリシー(Policy)] > [結果(Results)] > [TrustSec] > [セキュリティグループ(Security Groups)])。 • ユーザに SGT グループを関連付けるポリシーを設定します。 <p>詳細については、『Cisco Identity Services Engine documentation』を参照してください。</p>
5	WSA に、エクスポートされた ISE 管理証明書および pxGrid 証明書を追加します。	<ul style="list-style-type: none"> • この WSA で設定する各 ISE サーバの ISE 管理証明書および pxGrid 証明書をアップロードします。ISE サービスへの接続(8-6 ページ)を参照してください。 <ul style="list-style-type: none"> - ISE 管理と pxGrid の両方に対して 1 つの自己証明証明書を使用する場合は、[ISE 管理証明書(ISE Admin Certificate)] と [ISE pxGrid 証明書(ISE pxGrid Certificate)] フィールドにそれぞれファイルをアップロードします(つまり、合計 2 回アップロードします)。ISE サービスへの接続(8-6 ページ)を参照してください。 - CA 署名付き証明書を使用する場合は、ISE 証明書の各ペアに署名している認証局が WSA の信頼できるルート証明書リストに含まれていることを確認します。含まれていない場合は、CA ルート証明書をインポートします。信頼できるルート証明書の管理(22-27 ページ)を参照してください。 <p> (注) ISE 管理証明書と pxGrid 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、WSA で [ISE 管理証明書(ISE Admin Certificate)] と [ISE pxGrid 証明書(ISE pxGrid Certificate)] フィールドにルート CA 証明書自体がアップロードされていることを確認します([ネットワーク(Network)] > [Identity Services Engine])。</p>

手順	タスク	関連項目および手順へのリンク
6	ISE アクセスおよびログイン用 WSA の設定を完了します	<ul style="list-style-type: none"> • ISE サービスへの接続(8-6 ページ)。 • 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(21-32 ページ))。 • ISE 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と編集(21-8 ページ))。 • ISE サービス ログが作成されたことを確認します。作成されていない場合は追加します(ログ サブスクリプションの追加と編集(21-8 ページ))。 • ユーザの識別と認証のために ISE にアクセスする識別プロファイルを定義します(ユーザおよびクライアント ソフトウェアの分類(6-3 ページ))。 • ISE ID を使用してユーザ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(10-11 ページ))。



(注) ISE サーバで証明書をアップロードしたり変更するたびに、ISE サービスを再起動する必要があります。また、サービスと接続が復元されるまでに数分かかることがあります。

関連項目

- [Identity Services Engine サービスの概要\(8-1 ページ\)](#)
- [Identity Services Engine の証明書\(8-2 ページ\)](#)
- [Identity Services Engine に関する問題のトラブルシューティング\(8-8 ページ\)](#)

ISE サービスへの接続

はじめる前に

- 各 ISE サーバが WSA 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 サービスを認証および統合するためのタスク\(8-4 ページ\)](#)を参照)。
- ISE サーバの接続情報を取得します。
- 有効な ISE 関連の証明書(クライアント、ポータル、pxGrid)およびキーを取得します。また、[Identity Services Engine の証明書\(8-2 ページ\)](#)も参照してください。

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

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

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

- 手順 4 ホスト名または IPv4 アドレスを使用して **プライマリ ISE pxGrid ノード**を識別します。
- WSA-ISE データ サブスクリプション(ISE サーバに対して進行中のクエリ)用の **ISE pxGrid ノード証明書**を入力します。
証明書ファイルを参照して選択し、[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\(22-28 ページ\)](#)を参照してください。
- 手順 5 フェールオーバー用にセカンダリ ISE サーバ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**セカンダリ ISE pxGrid ノード**を識別します。
- セカンダリ **ISE pxGrid ノード証明書**を入力します。
証明書ファイルを参照して選択し、[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\(22-28 ページ\)](#)を参照してください。



(注) プライマリからセカンダリ ISE サーバへのフェールオーバー中、既存の ISE SGT キャッシュに含まれていないユーザは、WSA 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。

- 手順 6 **ISE モニタリング ノード管理証明書**をアップロードします。
- ISE ユーザ プロファイルデータを WSA に一括ダウンロードするために使用する、**プライマリ ISE モニタリング ノード管理証明書**を入力します。
証明書ファイルを参照して選択し、[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\(22-28 ページ\)](#)を参照してください。
 - フェールオーバー用に別の ISE サーバを使用している場合は、**セカンダリ ISE モニタリング ノード管理証明書**を入力します。
- 手順 7 WSA と ISE サーバの相互認証用の **WSA クライアント認証**を入力します。



(注) これは、CA の信頼できるルート証明書である必要があります。関連情報については、[Identity Services Engine の証明書\(8-2 ページ\)](#)を参照してください。

- [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。
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\(22-28 ページ\)](#)を参照してください)。
- [生成された証明書とキーを使用(Use Generated Certificate and Key)]
[新しい証明書とキーを生成(Generate New Certificate and Key)] 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生成\(22-28 ページ\)](#)を参照してください)。

- 手順 8 WSA クライアント証明書をダウンロードして保存し、ISE サーバホストにアップロードします(選択したサーバで、[管理(Administration)] > [証明書(Certificates)] > [信頼できる証明書(Trusted Certificates)] > [インポート(Import)])。
- 手順 9 (任意)[テスト開始(Start Test)] をクリックして、ISE pxGrid ノードとの接続をテストします。
- 手順 10 [送信(Submit)] をクリックします。

次の作業

- エンドユーザおよびクライアント ソフトウェアの分類(6-1 ページ)
- インターネット要求を制御するポリシーの作成(10-1 ページ)

関連情報

- <http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-de-sign-guides-list.html>、特に「How To Integrate Cisco WSA using ISE and TrustSec through pxGrid」。

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(A-11 ページ)
 - ISE 問題のトラブルシューティング ツール(A-11 ページ)
 - ISE サーバの接続に関する問題(A-12 ページ)
 - ISE 関連の重要なログ メッセージ(A-13 ページ)