

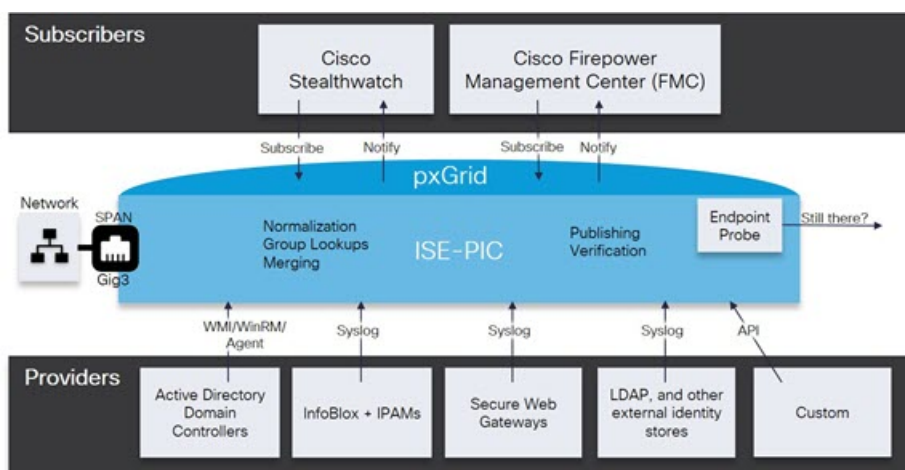


## サブスクライバ

ISE-PIC は、さまざまなプロバイダから収集し、Cisco ISE-PIC セッションディレクトリにより保存された認証済みユーザー ID を、Cisco Stealthwatch や Cisco Firepower Management Center (FMC) などのその他のネットワーク システムに送信するため、Cisco pxGrid サービスを使用します。

次の図では、pxGrid ノードが外部プロバイダからユーザー ID を収集しています。これらの ID は解析、マッピング、およびフォーマットされます。pxGrid はこれらのフォーマット済みのユーザー ID を取得し、ISE-PIC サブスクライバに送信します。

図 1: ISE-PIC フロー



Cisco ISE-PIC に接続するサブスクライバは、pxGrid サービスの使用を登録する必要があります。サブスクライバは、一意の名前と証明書ベースの相互認証を使用して pxGrid にログインできます。Cisco pxGrid サブスクライバは、有効な証明書を送信すると、ISE-PIC により自動的に承認されます。

サブスクライバは設定されている pxGrid サーバーのホスト名または IP アドレスのいずれかに接続できます。不必要なエラーが発生することを防ぎ、DNS クエリが適切に機能するようにするため、ホスト名を使用することが推奨されます。公開および登録するためにサブスクライバの pxGrid で作成される、情報トピックまたはチャンネル機能があります。Cisco ISE-PIC では SessionDirectory と IdentityGroup だけがサポートされています。機能情報は、公開、ダイレク

トクエリ、または一括ダウンロードクエリによりパブリッシャから取得でき、[Capabilities] タブの [Subscribers] で確認できます。

サブスクライバが ISE-PIC から情報を受信できるようにするには、次の操作を行います。

1. 必要に応じて、サブスクライバ側から証明書を生成します。
2. ISE-PICからサブスクライバの pxGrid 証明書の生成 (2 ページ) を参照してください。
3. サブスクライバの有効化 (4 ページ)。サブスクライバが ISE-PIC からユーザー ID を受信できるようにするため、このステップを実行するか、承認を自動的に有効にします。サブスクライバの設定 (4 ページ) を参照してください。
  - サブスクライバの pxGrid 証明書の生成 (2 ページ)
  - サブスクライバの有効化 (4 ページ)
  - ライブ ログからのサブスクライバ イベントの表示 (4 ページ)
  - サブスクライバの設定 (4 ページ)

## サブスクライバの pxGrid 証明書の生成

### 始める前に

インストール時に ISE-PIC により自動的に pxGrid サービスの自己署名証明書が生成され、プライマリ ISE-PIC ノードによりデジタル署名されます。その後、pxGrid とサブスクライバの間の相互信頼を保証するため、pxGrid サブスクライバの証明書を生成できます。これにより、ISE-PIC からサブスクライバにユーザー ID を渡すことが可能になります。

**ステップ 1** [サブスクライバ (Subscribers)] を選択し、[証明書 (Certificates)] タブに移動します。

**ステップ 2** [処理の選択 (I want to)] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- [単一の証明書の生成 (証明書署名要求なし) (Generate a single certificate without a certificate signing request)] : このオプションを選択した場合は、共通名 (CN) を入力する必要があります。[コモンネーム (Common Name)] フィールドに、pxGrid をプレフィックスとして含む pxGrid FQDN を入力します。たとえば `www.pxgrid-ise.ise.net` です。あるいはワイルドカードを使用します。たとえば `*.ise.net` です。
- [単一の証明書の生成 (証明書署名要求あり) (Generate a single certificate with a certificate signing request)] : このオプションを選択した場合は、証明書署名要求の詳細を入力する必要があります。
- [一括証明書の生成 (Generate bulk certificates)] : 必要な詳細を含む CSV ファイルをアップロードすることができます。
- [ルート証明書チェーンのダウンロード (Download root certificate chain)] : pxGrid クライアントの信頼できる証明書ストアに追加するために、ISE 公開ルート証明書をダウンロードします。ISE pxGrid ノードは、新規に署名された pxGrid クライアント証明書だけを信頼します (あるいはこの逆)。これにより、外部の認証局を使用する必要がなくなります。

**ステップ3** (オプション) この証明書の説明を入力できます。

**ステップ4** この証明書のベースとなる pxGrid 証明書テンプレートを表示または編集します。証明書テンプレートには、そのテンプレートに基づいて認証局 (CA) によって発行されたすべての証明書に共通のプロパティが含まれています。証明書テンプレートは、件名、サブジェクト代替名 (SAN)、キータイプ、キーサイズ、使用する必要がある SCEP RA プロファイル、証明書の有効期間、証明書がクライアントまたはサーバーの認証またはその両方に使用される必要があるかどうかを指定した拡張キーの使用状況 (EKU) を定義します。内部 Cisco ISE CA (ISE CA) は、証明書テンプレートを使用し、そのテンプレートに基づいて証明書を発行します。pxGrid の場合、パッシブ ID サービスを使用するときには pxGrid 証明書テンプレートだけを使用できます。また、このテンプレートではサブジェクト情報だけを編集できます。このテンプレートを編集するには、**[証明書 (Certificates)] > [証明書テンプレート (Certificate Templates)] [管理 (Administration)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [証明書テンプレート (Certificate Templates)]** を選択します。

**ステップ5** サブジェクト代替名 (SAN) を指定します。複数の SAN を追加できます。次のオプションを使用できます。

- **[FQDN]** : ISE ノードの完全修飾ドメイン名を入力します。たとえば `www.isepic.ise.net` です。あるいは FQDN にワイルドカードを使用します。たとえば `*.ise.net` です。

pxGrid FQDN も入力できる追加の行を FQDN に追加できます。これは **[コモンネーム (Common Name)]** フィールドで使用する FQDN と同一である必要があります。

- **[IP アドレス (IP address)]** : この証明書に関連付ける ISE ノードの IP アドレスを入力します。サブスクリイバが FQDN ではなく IP アドレスを使用する場合には、この情報を入力する必要があります。

(注) このフィールドは、**[一括証明書の生成 (Generate bulk certificates)]** オプションを選択している場合には表示されません。

**ステップ6** **[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、以下のいずれかのオプションを選択します。

- **[Private Enhanced Electronic Mail (PEM) 形式の証明書、PKCS8 PEM 形式のキー (証明書チェーンを含む) (Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))]** : ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-----BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE-----」タグで終わります。エンドエンティティの秘密キーは PKCS\* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY-----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY-----」タグで終わります。
- **[PKCS12 形式 (証明書チェーンを含む。つまり証明書チェーンとキーの両方で1ファイル) (PKCS12 format (including certificate chain; one file for both the certificate chain and key))]** : 1つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

**ステップ7** 証明書のパスワードを入力します。

**ステップ8** **[作成 (Create)]** をクリックします。

## サブスクライバの有効化

サブスクライバが Cisco ISEISE-PIC からユーザー ID を受信できるようにするため、このタスクを実行するか、または承認を自動的に有効にする必要があります。 [サブスクライバの設定 \(4 ページ\)](#) を参照してください。

**ステップ 1** [サブスクライバ (Subscribers)] を選択し、[クライアント (Clients)] タブが表示されることを確認します。

**ステップ 2** サブスクライバの隣にあるチェックボックスをオンにして [承認 (Approve)] をクリックします。

**ステップ 3** [リフレッシュ (Refresh)] をクリックすると、最新のステータスが表示されます。

## ライブ ログからのサブスクライバイベントの表示

[ライブ ログ (Live Logs)] ページにはすべてのサブスクライバイベントが表示されます。イベント情報には、イベントタイプ、タイムスタンプ、サブスクライバ名、機能名が含まれています。

[サブスクライバ (Subscribers)] に移動し、[ライブ ログ (Live Log)] タブを選択し、イベントリストを表示します。ログを消去して、リストを再同期またはリフレッシュすることもできます。

## サブスクライバの設定

**ステップ 1** [サブスクライバ (Subscribers)] を選択し、[設定 (Settings)] タブに移動します。

**ステップ 2** 必要に応じて、次のオプションを選択します。

- [新しいアカウントの自動承認 (Automatically Approve New Accounts)] : このチェックボックスをオンにすると、新しい pxGrid クライアントからの接続要求が自動的に承認されます。
- [パスワードベースのアカウント作成の許可 (Allow Password Based Account Creation)] : このチェックボックスをオンにすると、pxGrid クライアントのユーザー名/パスワードベースの認証が有効になります。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。

pxGrid クライアントは、REST API を介してユーザー名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

**ステップ 3** [保存 (Save)] をクリックします。

## 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。