初期設定の完了

- 初期設定ワークフロー （1 ページ）
- 互換性のあるブラウザ （1 ページ）
- Catalyst Center への初回ログイン （2 ページ）
- クイック スタート ワークフローの完了 （4 ページ）
- Cisco ISE と Catalyst Center の統合 （8 ページ）
- 認証サーバーとポリシーサーバーの設定 （16 ページ）
- SNMP プロパティの設定 （20 ページ）

初期設定ワークフロー

インストールしたすべての Catalyst Center アプライアンスの設定が完了したら、この章で説明するタスクを実行して、Catalyst Center を実稼働に使用する準備をします。次の点を考慮してください。

- この作業を完了するために必要なパラメータ情報については、必要な初期設定情報を参照してください。
- 実稼働環境に高可用性（HA）を展開している場合、HA の動作を最適化するためにクラスタノード間でサービスを再配布する必要があります（HA のアクティブ化を参照）。アプライアンスの SNMP 設定を行った後、この手順を完了します。

互換性のあるブラウザ

Catalyst Center の GUI は次の HTTPS 対応ブラウザと互換性があります。

- Google Chrome：バージョン 93 以降
- Mozilla Firefox：バージョン 92 以降

Catalyst Center へのログインに使用するクライアント システムは、64 ビット オペレーティング システムとブラウザを装備していることが推奨されます。

Catalyst Center への初回ログイン

Catalyst Center アプライアンスをインストールして設定した後、次の手順に従って初めてその GUI にログインします。初回は管理者スーパーユーザーとしてログインします（ユーザー名は「admin」で PER-ADMIN-ROLE が割り当てられます）。

（注） Catalyst Center にアクセスする際には、互換性のある HTTPS 対応ブラウザを使用してください。詳細については、互換性のあるブラウザ （1 ページ）を参照してください。

Before you begin

Catalyst Center にログインできるように、次の情報を用意してください。

- *admin* スーパーユーザーのユーザー名とパスワードを、Catalyst Center アプライアンスの設定時に指定しました。
- 必要な初期設定情報に記載されている情報。

手順

ステップ 1 Catalyst Center GUI にアクセスします。

a) Catalyst Center アプライアンスの再起動が完了したら、互換性のある HTTPS 対応のブラウザを起動します。

b) **`HTTPS://`** と設定プロセスの最後に表示された Catalyst Center GUI の IP アドレスを使用して、Catalyst Center GUI にアクセスするホスト IP アドレスを入力します。

IP アドレスを入力すると、次のいずれかのメッセージが表示されます（使用しているブラウザによって異なります）。

- Google Chrome：接続のプライバシーは保護されません
- Mozilla Firefox：警告：今後セキュリティリスクが見つかる潜在的可能性があります

c) [**Advanced**] をクリックして続行します。

次のいずれかのメッセージが表示されます。

- Google Chrome：

```
This server could not prove that it is GUI-IP-address; its security certificate is not
trusted by your computer's
 operating system. This may be caused by a misconfiguration or an attacker intercepting your
 connection.
```

- Mozilla Firefox：

```
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates.
```

```
Firefox does not trust GUI-IP-address because its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate
certificates.
```

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Catalyst Center での証明書の使用方法については、『*Cisco Catalyst Center Administrator Guide*』の「Certificate and Private Key Support」の項を参照してください。

d) 続行するには、次のいずれかのタスクを実行します。

- Google Chrome：*GUI-IP-address*（**安全でない**）リンクをクリックして**開きます**。
- Mozilla Firefox：**[リスクを理解して続行する（Accept the Risk and Continue）]** をクリックします。

ステップ 2 Catalyst Center にログインします。

a) Catalyst Center ログインウィンドウが開いたら、次のいずれかの構成ウィザード完了タスクを実行します。

- Maglev 構成ウィザードを完了し、[**Start using DNAC pre manufactured cluster**] オプションを選択した場合は、管理者のユーザー名（**admin**）とパスワード（**P@ssword9**）を入力します。
- Maglev 構成ウィザードを完了し、[**Start configuration of DNAC in advanced mode**] オプションを選択した場合は、Catalyst Center アプライアンスの構成時に設定した管理者のユーザー名（**admin**）とパスワードを入力します。
- インストール構成ウィザードを完了したら、管理者のユーザー名（**admin**）を入力し、ウィザードの最後のウィンドウからコピーしたパスワード（**P@ssword9**）を貼り付けます。
- 高度なインストール構成ウィザードを完了した場合は、Catalyst Center アプライアンスの構成時に設定した管理者のユーザー名（**admin**）とパスワードを入力します。

b) [Log In] をクリックします。

ステップ 3 セキュリティ対策として新しい管理ユーザーを設定します。

a) [**Username**] フィールドに、管理者ユーザーのユーザー名を入力します。

b) [**Password**] および [**Confirm Password**] フィールドに管理者ユーザーのパスワードを入力します。

このパスワードが パスワード要件 に準拠していることを確認してください。

c) [Submit] をクリックします。

Catalyst Center ログアウトされます。

ステップ 4 Catalyst Center に再度ログインします：

a) [Log In] をクリックします。

b) 新しい管理者ユーザーに関して設定したユーザー名とパスワードを入力します。

c) [Log In] をクリックします。

cisco.com のログイン情報を使用して認証するように求められます。これらのログイン情報は、ソフトウェアダウンロードの登録と、システム通信の受信に使用されます。

ステップ 5 [Authenticate] をクリックします。

（注）
今すぐ認証を行わない場合は、[**Skip**] をクリックします。

ステップ 6 [**Activate your device**] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[**Next**] をクリックします。

[Terms & Conditions] 画面が開き、ソフトウェアのシスコ エンドユーザー ライセンス契約（EULA）および現在利用可能な補足条件へのリンクが表示されます。

ステップ 7 各ドキュメントを確認したら、[**Next**] をクリックして EULA に同意します。

[Quick Start Overview] スライダが開きます。[>] をクリックすると、Catalyst Center の使用を開始するために、クイック スタート ワークフローで完了までサポートされるタスクの説明が表示されます。

クイック スタート ワークフローの完了

管理者スーパーユーザーとして初めてログインすると（ユーザー名 `admin` と SUPER-ADMIN-ROLE が割り当てられた）、クイック スタート ワークフローが自動的に開始されます。このワークフローを完了して、Catalyst Center がデバイスからのテレメトリの収集を管理および有効化するデバイスを検出します。

Before you begin

次のことを確認してください。

- 初めて Catalyst Center にログインし、新しい管理者ユーザーを作成しました。詳細については、Catalyst Center への初回ログイン （2 ページ）を参照してください。
- 必要な初期設定情報 に記載されている情報を用意します。

手順

ステップ 1 [**Quick Start Overview**] スライダで、[**Let's Do it**] をクリックします。

ステップ 2 [**Discover Devices: Provide IP Ranges**] 画面で、次の情報を入力し、[**Next**] をクリックします。

- デバイス検出ジョブの名前。
- 検出するデバイスの IP アドレスの範囲。追加の範囲を入力するには、[+] をクリックします。
- アプライアンスのループバックアドレスを優先管理 IP アドレスとして指定するかどうかを指定します。詳細については、『*Cisco Catalyst Center User Guide*』の「Preferred Management IP Address」を参照してください。

ステップ 3 [**Discover Devices: Provide Credentials**] 画面で、設定するログイン情報のタイプに関する情報（次の表を参照）を入力し、[**Next**] をクリックします。

フィールド	説明
[CLI (SSH) Credentials]	
Username	ネットワーク内のデバイスの CLI にログインするために使用するユーザー名。
パスワード	ネットワーク内のデバイスの CLI にログインするために使用するパスワード。入力するパスワードは、8 文字以上にする必要があります。
Name/Description	CLI ログイン情報の名前または説明。
パスワードの有効化	CLI でより高い権限レベルを有効にするために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。
[SNMP Credentials: SNMPv2c Read] タブ （注） Catalyst Center は、FIPS モードが有効になっている場合、SNMPv2c ログイン情報をサポートしません。代わりに、SNMPv3 ログイン情報を入力する必要があります。FIPS モードの詳細については、Maglev ウィザードを使用したプライマリノードの設定を参照してください。	
Name/Description	SNMPv2c 読み取りコミュニティストリングの名前または説明。
Community String	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティ ストリング パスワード。
[SNMP Credentials: SNMPv2c Write] タブ	
Name/Description	SNMPv2c 書き込みコミュニティストリングの名前または説明。
Community String	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。
[SNMP Credentials: SNMPv3]	
Name/Description	SNMPv3 ログイン情報の名前または説明。
Username	SNMPv3 ログイン情報に関連付けられているユーザー名。

フィールド	説明
Mode	SNMP メッセージを必要とするセキュリティレベル。 • [No Authentication, No Privacy]（noAuthnoPriv）：認証も暗号化も行いません。 • [Authentication, No Privacy]（authNoPriv）：認証は行いますが、暗号化は行いません。 • [Authentication and Privacy]（authPriv）：認証と暗号化の両方を行います。 （注） FIPS モードが有効な場合、Catalyst Center では [Authentication and Privacy] モードのみがサポートされます。
Authentication Password	SNMPv3 を使用するデバイスから情報にアクセスするために必要なパスワード。パスワードの長さは、最低 8 文字である必要があります。次の点に注意してください。 • 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Authentication Type	[Authentication and Privacy] または [Authentication、No Privacy] が認証モードとして設定されている場合に使用されるハッシュベースのメッセージ認証コード（HMAC）タイプ。 • [SHA]：HMAC-SHA 認証。 • [MD5]：HMAC-MD5 認証。 （注） Catalyst Center は、FIPS モードが有効になっている場合、この認証タイプをサポートしません。

フィールド	説明
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 およびCISCOAES256のみでサポートされています。Assurance機能はサポートされていません。 • プライバシー タイプ AES128 は、検出、インベントリ、およびAssuranceでサポートされています。
Privacy Password	AES128、AES192、およびAES256暗号化標準規格でサポートされているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
NETCONF	
Port	Cisco IOS-XE を実行するワイヤレスコントローラを検出するために Catalyst Center が使用する必要がある NETCONF ポート。

ステップ 4 [Create Site] 画面で、テレメトリを容易にするために検出するデバイスを 1 つのサイトにグループ化し、[Next] をクリックします。

サイトの情報を手動で入力するか、提供されたマップで使用する場所をクリックします。

ステップ 5 [Enable Telemetry] 画面で、Catalyst Center にテレメトリを収集させるネットワークコンポーネントを選択し、[Next] をクリックします。

（注）
[Enable Telemetry] オプションと [Disable Telemetry] オプションの両方がグレー表示されている場合、これは、デバイスがテレメトリをサポートできないか、デバイスがテレメトリの有効化をサポートしていない OS バージョンを実行していることを示しています。

ステップ 6 [**Summary**] 画面で、入力した設定を確認し、次のいずれかを実行します。

- 変更を加える場合は、該当する [Edit] リンクをクリックして、関連画面を開きます。
- 設定に問題がなければ、[Start Discovery and Telemetry] をクリックします。Catalyst Center により設定が検証され、問題が発生しないことが確認されます。検証が完了すると、画面が更新されます。

  Catalyst Center により、ネットワークのデバイスを検出し、選択したネットワークコンポーネントのテレメトリを有効にするプロセスが開始されます。このプロセスには 30 分以上かかります（大規模なネットワークの場合はさらに長くなります）。

ステップ 7 ホームページの上部に、クイックスタート ワークフローが完了したことを示すメッセージが表示されたら、次のいずれかのタスクを実行します。

- [View Discovery] をクリックして [Discovery] ページを開き、ネットワーク内のデバイスが検出されたことを確認します。
- [Go to Network Settings] リンクをクリックして、[Device Credentials] ページを開きます。ここから、以前に入力したログイン情報がサイトに設定されていることを確認できます。
- [View Activity Page] リンクをクリックして [Tasks] ページを開き、Catalyst Center ですでに実行がスケジュールされているタスク（セキュリティアドバイザリの毎週のネットワークスキャンなど）を表示します。
- [Workflow Home] リンクをクリックして、ネットワークのセットアップと維持に役立つガイド付きワークフローにアクセスします。

Cisco ISE と Catalyst Center の統合

Catalyst Center は、Cisco ISE と信頼された通信リンクを作成するメカニズムを備えており、Cisco ISE と安全な方法でデータを共有できます。Cisco ISE が Catalyst Center に登録されると、Catalyst Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。ユーザーは Catalyst Center を使用してデバイスを検出でき、検出されたデバイスは両方のアプリケーションに表示されるため、Catalyst Center と Cisco ISE の両方の機能を適用できます。また Catalyst Center デバイスと Cisco ISE デバイスはすべて、デバイス名で一意に識別されます。

Catalyst Center デバイスは、Catalyst Center サイト階層内の特定のサイトにプロビジョニングされて割り当てられると、すぐに Cisco ISE にプッシュされます。Catalyst Center デバイスのアップデート（IP アドレス、SNMP または CLI のログイン情報、Cisco ISE 共有秘密情報など）はすべて、自動的に ISE 上の対応するデバイスインスタンスに送信されます。

（注） Catalyst Center デバイスが Cisco ISE にプッシュされるのは、Cisco ISE が AAA サーバーとして設定されている特定のサイトにそれらのデバイスが関連付けられている場合に限ります。

始める前に

Cisco ISE を Catalyst Center と統合する前に、次の前提条件を満たしていることを確認します。

- ネットワークに 1 つ以上の Cisco ISE ホストを展開済みであること。サポートされている Cisco ISE バージョンの詳細については、『Catalyst Center Compatibility Matrix』を参照してください。Cisco ISE のインストールについては、Cisco Identity Services Engine インストールおよびアップグレードガイド [英語] を参照してください。
- スタンドアロン Cisco ISE 展開環境がある場合は、Catalyst Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。

（注） pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Catalyst Center 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 Cisco ISE 展開がある場合：
  - Catalyst Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

（注） PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

  - 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。これを行うこともできますが、PAN 上で pxGrid サービスを有効化する必要はありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
  - TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA Servers]** でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。
- ネットワーク管理者ロールの権限を持つユーザーのみが Cisco ISE と Catalyst Center を統合できます。

- Cisco ISE で [Use CSRF Check for Enhanced Security] オプションが有効になっている場合、Catalyst Center は ERS API アクセスをサポートしません。
- ポート 443、5222、8910、9060 で Catalyst Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Catalyst Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE サービスで使用される証明書に対してオンライン証明書ステータスプロトコル（OCSP）または証明書失効リスト（CRL）検証が定義されている場合、Catalyst Center は証明書失効ステータスをチェックします。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名（SAN）のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- FQDN のみのシステム証明書を使用できるかどうかは、Catalyst Center 展開で LAN 自動化が有効になっているかどうかによって異なります。詳細については、『*Catalyst Center Security Best Practices Guide*』の「Generate a Certificate Request Using Open SSL」トピックのステップ 3 にある「**alt_names**」セクションの箇条書きを参照してください。

（注） Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、*Cisco Cloud APIC リリースノート* [英語] を参照してください。

Catalyst Center に対応した Cisco ISE の設定の詳細については、『Cisco Identity Services Engine 管理者ガイド』の「Integration with Catalyst Center」を参照してください。

手順

ステップ 1 Cisco ISE の pxGrid サービスと ERS を有効にします。

a) プライマリポリシー管理ノードにログインします。

b) Cisco ISE GUI で、メニューアイコンをクリックして次を選択します。 **[Administration]** > **[System]** > **[Deployment]**。

[Deployment Nodes] ウィンドウが表示されます。

c) pxGrid サービスを有効化する Cisco ISE ノードのホスト名をクリックします。分散型展開の場合、これは展開環境内の任意の Cisco ISE ノードです。

[ノードの編集（Edit Node）] ウィンドウが表示されます。

d) [General Settings] タブをクリックし、[pxGrid] チェックボックスをオンにして、[Save] をクリックします。

e) Cisco ISE GUI で、メニューアイコンをクリックして次を選択します。 **[Administration]** > **[System]** > **[Settings]**。

f) 左側のナビゲーションペインから、[**API Settings** > **API Service Settings**] を選択します。

g) [**ERS (Read/Write)**] を有効にして、[**OK**] をクリックします。

h) **[保存（Save）]** をクリックします。

ステップ 2 Cisco ISE ノードを AAA サーバとして Catalyst Center に追加します。

a) Catalyst Center GUI にログインします。

b) メインメニューから次を選択します。**[System]** > **[System 360]** の順に選択します。

c) [Identity Services Engine（ISE）] ペインで、**[設定（Configure）]** リンクをクリックします。

d) [**Authentication and Policy Servers**] ウィンドウで、[**Add**] をクリックし、ドロップダウンリストから [**ISE**] を選択します。

e) [**Add ISE server**] スライドインペインで、次の情報を入力します。

- [Server IP Address] フィールドに、Cisco ISE サーバーの IP アドレスを入力します。
- ネットワークデバイスと Cisco ISE の通信を保護するために使用する **[共有秘密（Shared Secret）]** を入力します。
- 該当する Cisco ISE 管理ログイン情報を [Username] と [Password] フィールドに入力します。
- Cisco ISE ノードの **FQDN** を入力します。
- （任意）Cisco ISE PSN が背後に配置されているロードバランサの**仮想 IP アドレス**を入力します。異なるロードバランサの背後に複数のポリシー サービス ノード ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。
- [Connect to pxGrid]：pxGrid 接続を有効にするには、[Advanced Settings] でこのチェックボックスをオンにします。

  Catalyst Center システム証明書を pxGrid クライアント証明書として使用する場合（pxGrid クライアントとして Catalyst Center システムを認証するために ISE に送信）、[**Use Catalyst Center Certificate for pxGrid**] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ認証局（CA）で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Catalyst Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

  このオプションを有効にする場合は、次のことを確認してください。

  - Catalyst Center 証明書が、Cisco ISE で使用中の CA と同じ CA によって生成されていること（そうでない場合、pxGrid 認証は失敗します）。
  - [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。

- [Advanced Settings] エリアで、以下の手順を実行します。
  - [**RADIUS**] または [**TACACS**] のチェックボックスをオンにして、使用する必要があるプロトコルを選択できます。
  - 次のフィールドに必要な値を入力します：[**Authentication Port**]、[**Accounting Port**]、[**Retries**]、および [**Timeout seconds**]。

（注）
このオプションは、Catalyst Center がサードパーティの証明書を使用している場合にのみ使用できます。Catalyst Center がデフォルトの自己署名システム証明書を使用する場合、このオプションは無効になっています。

f) [Add] をクリックします。

Cisco ISE との統合を開始すると、Cisco ISE からの証明書がまだ信頼されていないという通知が表示されます。証明書を表示して詳細を確認できます。

[**Accept**] をクリックして証明書を信頼し、統合プロセスを続行するか、証明書を信頼せず、統合プロセスを終了する場合は、[**Decline**] を選択します。

統合が正常に完了すると、確認メッセージが表示されます。

統合プロセスに問題がある場合は、エラーメッセージが表示されます。必要に応じて、編集または再試行のオプションが表示されます。

- Cisco ISE 管理ログイン情報が無効であるというエラーメッセージが表示された場合は、[Edit] をクリックし、正しい情報を再入力します。
- 統合プロセスで証明書にエラーが見つかった場合は、Cisco ISE サーバエントリを削除し、証明書の問題が解決した後に統合を最初からやり直す必要があります。

ステップ 3 Catalyst Center が Cisco ISE に接続していること、Cisco ISE SGT グループとデバイスが Catalyst Center にプッシュされることを確認します。

a) Catalyst Center GUI にログインします。
b) メインメニューから次を選択します。**[System]** > **[System 360]** の順に選択します。
c) [Identity Services Engine（ISE）] ペインで、リストされているすべての ISE サーバーのステータスの表示が [Available] または [Configured] になっていることを確認します。
d) [Identity Services Engine（ISE）] ペインで、**[Update（更新）]** リンクをクリックします。
e) **[認証サーバとポリシーサーバ（Authentication And Policy Servers）]** ウィンドウで、 Cisco ISE AAA サーバのステータスがまだ**[アクティブ（Active）]**であることを確認します。

ステップ 4 次のように Cisco ISE が Catalyst Centerに接続され、接続にサブスクライバがあることを確認します。

a) [Identity Services Engine (ISE) Deployment] ペインで pxGrid サーバーとして表示されている Cisco ISE ノードにログインします。
b) **[Administration]** > **[pxGrid Services]** の順に選択し、[Web Clients] タブをクリックします。

Catalyst Center サーバーの IP アドレスとともに pxGrid クライアントがリストに表示されます。

グループベースのアクセスコントロール：ポリシーデータの移行と同期

Catalyst Center の使用を開始する場合

Catalyst Center の以前のリリースでは、グループベースのアクセス コントロール ポリシー機能でポリシーのアクセス契約とポリシーを Catalyst Center ローカルに保存していました。Catalyst Center では同じデータを Cisco ISE にも反映します。Cisco ISE ではネットワークにランタイムポリシーサービスも提供します。その一環でグループベースのアクセス コントロール ポリシーがネットワークデバイスにダウンロードされます。通常、Catalyst Center のポリシー情報は Cisco ISE のポリシー情報と一致します。ただし、データが同期されていない可能性があり、その場合はデータが一致していない可能性があります。そのため、新規またはアップグレードで Catalyst Center をインストールした後は、グループベースのアクセスコントロール機能を使用する前に、次の手順を実行する必要があります。

- Cisco ISE を Catalyst Center と統合する（未統合の場合）。
- Cisco ISE をアップグレードする（必須バージョンさえない場合）。Cisco ISE の必須バージョンについては「Catalyst Centerリリースノート」を参照してください。
- ポリシーの移行と同期を実行する。

「移行と同期」とは何ですか。

Catalyst Center は統合された Cisco ISE に含まれるグループベースのアクセス コントロール ポリシー データをすべて読み取り、そのデータを Catalyst Center のポリシーデータと比較します。以前のバージョンからアップグレードした場合は、既存のポリシーデータが保持されます。Catalyst Center のグループベースのアクセス コントロール ポリシーを管理するには、先にポリシーを同期しておく必要があります。

移行と同期はどのように機能しますか。

通常、Cisco ISE と Catalyst Center のポリシーデータは一貫しているため、データの処理や変換は特に必要ありません。ささいな不一致や不整合がある場合、移行中に一部のデータのみが変換されることがあります。競合がある場合は、ネットワーク内でポリシーの挙動が変わらないように Cisco ISE のデータが優先されます。次のリストは、移行中に実行されるアクションを示しています。

- セキュリティグループ：数値であるセキュリティグループタグ（SGT）は、セキュリティグループを一意に識別します。Cisco ISEセキュリティグループが Catalyst Center のセキュリティグループと比較されます。

- 名前と SGT の値が同じであれば、何も変更されません。Catalyst Center の情報はCisco ISE と一貫性があり、変更する必要はありません。
- Cisco ISE セキュリティグループの SGT 値が Catalyst Center に存在しない場合は、Catalyst Center に新しいセキュリティグループが作成されます。新しいセキュリティグループには「Default_VN」のデフォルトの関連付けが施されます。
- Cisco ISE セキュリティグループの SGT 値が Catalyst Center に存在しているが、名前が一致しない場合は、Cisco ISE セキュリティグループの名前が Catalyst Center のセキュリティグループの名前に置き換えられます。
- Cisco ISE セキュリティグループの名前が同じであるが、SGT 値が異なる場合は、Cisco ISE からセキュリティグループが移行されます。この処理では名前とタグの値は保持されますが、Catalyst Center セキュリティグループの名前は変更されます。「_DNA」というサフィックスが追加されます。

契約

ポリシーで参照される Cisco ISE の SGACL はすべて、Catalyst Center の契約と比較されます。

- SGACL と契約の名前と内容が同一の場合、それ以上のアクションは必要ありません。Catalyst Center の情報はCisco ISE と一貫性があり、変更する必要はありません。
  - SGACL と契約の名前が同一で、内容が異なっている場合、Cisco ISE から SGACL の内容が移行されます。Catalyst Center の以前の契約内容は破棄されます。

SGACL が Catalyst Center に存在しない場合、その名前で新しい契約が作成され、Cisco ISE からSGACL の内容が移行されます。

（注） Cisco ISE SGACL の内容に沿って新しいアクセス契約を作成する場合、Catalyst Center によってテキストコマンドラインが解析され、それらの SGACL コマンドが可能な限りモデル化されたアクセス契約としてレンダリングされます。ACE 行がそれぞれ「高度な」アプリケーション行としてレンダリングされます。Cisco ISE SGACL に正常に解析できないテキストが含まれている場合、SGACL テキストの内容はモデル化された形式に変換されません。これは raw コマンドラインテキストとして保存されます。この SGACL 契約文は編集できますが、移行中、テキストの内容の解析または構文チェックは実行されません。

ポリシー

ポリシーは、送信元グループと宛先グループのペアで一意に識別されます。すべての Cisco ISE TrustSec イーグレス ポリシー マトリックス ポリシーが、Catalyst Center のポリシーと比較されます。

- 送信元グループと宛先グループのポリシーで Cisco ISE の同じ SGACL または契約名を参照している場合、変更は行われません。

- 送信元グループと宛先グループのポリシーで Cisco ISE の別の SGACL または契約名を参照している場合、ポリシーでは Cisco ISE の契約名が参照されます。この結果、Catalyst Center で以前の契約参照が上書きされます。
- Cisco ISE のデフォルトポリシーがチェックされ、Catalyst Center に移行されます。

（注） Catalyst Center はアクセスポリシー内の 1つの契約をサポートします。Cisco ISE にはアクセスポリシーで複数の SGACL を使用するオプションがありますが、Cisco ISE ではこのオプションはデフォルトで無効になっていて、一般的には使用されていません。以前のリリースの Catalyst Center を使用してグループベースのアクセス コントロール ポリシーを管理していた既存の SDA のお客様は、このオプションを使用しないでください。

Cisco ISE で複数の SGACL を許可するオプションを有効にしてポリシー作成時に使用した場合、それらのポリシーはこのリリースでは Catalyst Center に移行できません。[multiple SGACL] オプションを利用し、移行できない具体的なポリシー機能は次のとおりです。

- 1 つのポリシーに含まれる複数の SGACL。
- ポリシーレベルの catch-all ルールは [Permit] または [Deny] に設定されています現在の移行では [None] の値のみCatalyst Centerサポートされています。
- お客様が作成した SGACL を使用するよう設定されたデフォルトポリシー。ただし、Catalyst Center への移行では現在、 [Permit IP]、[Permit_IP_Log]、[Deny IP]、[Deny_IP_Log] の標準値のみサポートされています。

ポリシーの移行と同期の操作中に前述のいずれかの SGACL が検出された場合、通知が生成されます。続行するには、次のいずれかのオプションを選択する必要があります。

- [Manage Group-Based Access Control policy in Catalyst Center]：このオプションが選択されている場合は、Catalyst Center でグループベースのアクセス コントロール ポリシーの管理がすべて実行されます。Cisco ISE セキュリティグループ、SGCAL、イーグレスポリシーを管理する Cisco ISE のユーザインターフェイス画面は、読み取り専用モードで使用できます。（Cisco ISE で複数の SGACL を使用しているために）ポリシーの移行中に問題が生じた場合、これらのポリシーには Catalyst Center で選択した契約が含まれなくなります。このポリシーではデフォルトポリシーが使用され、移行が完了したら、そのポリシーに対応する契約を新しく選択できます。デフォルトポリシーの移行中に問題が発生した場合は、デフォルトポリシーが [Permit] に設定されます。
- [Manage Group-Based Access Control Policy in Cisco ISE]：このオプションが選択されている場合は、Catalyst Center グループベースのアクセス コントロール ポリシーの管理がすべて非アクティブになります。Cisco ISE は変更されず、ネットワーク内のポリシーの適用には影響しません。グループベースのアクセス コントロール ポリシーは、TrustSec ワークセンターの Cisco ISE で管理されます。
- [Manage Group-Based Access Control policy in both Catalyst Center and Cisco ISE]：このオプションの場合、Cisco ISE で加えられたポリシーの変更が Catalyst Center と同期されないため、一般的な使用には推奨されません。2つのシステムを常に同期してオクことはできま

せん。このオプションは短期または暫定オプションとして意図されており、Cisco ISE で [Allow Multiple SQUADl] オプションを有効にした場合にのみ考慮する必要があります。Cisco ISE の更新に関してより多くの時間と柔軟性が必要な場合は、このオプションを使用できます。

認証サーバーとポリシーサーバーの設定

Catalyst Center は AAA サーバをユーザ認証に使用し、Cisco ISE をユーザ認証とアクセス制御の両方に使用します。この手順を使って Cisco ISE を含む AAA サーバを設定します。

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Catalyst Center および Cisco ISE が統合されていることを確認します。
- Catalyst Center の FIPS モードが有効になっている場合は、Catalyst Center と Cisco ISE の統合時に KeyWrap を有効にしてください。「Cisco ISE と Cisco DNA Center の統合」の手順 2e を参照してください。

（注） Catalyst Center と Cisco ISE がすでに統合されている場合、KeyWrap を有効にすることはできません。この機能を有効にするには、Cisco ISE を削除してから Catalyst Center と再統合する必要があります。

- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、必ず次のタスクを実行してください。
  - AAA サーバーで Catalyst Center を登録します。これには、AAA サーバーと Catalyst Center の共有秘密を定義することが含まれます。
  - AAA サーバーで Catalyst Center の属性名を定義します。
  - Catalyst Center マルチホストクラスタの設定の場合は、AAA サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- Cisco ISE を設定する前に、以下の点を確認してください。
  - Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『Catalyst Center Compatibility Matrix』を参照してください。Cisco ISE のインストールについては、Cisco Identity Services Engine インストールおよびアップグレードガイド [英語] を参照してください。
  - スタンドアロン ISE 展開環境がある場合は、Catalyst Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。

（注） pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Catalyst Center 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 Cisco ISE 展開がある場合：
  - Catalyst Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

（注） PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

  - 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。これを行うこともできますが、PAN 上で pxGrid サービスを有効化する必要はありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
  - TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA Servers]** でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

- ポート 443、5222、8910、9060 で Catalyst Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Catalyst Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名（SAN）のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Catalyst Center システム証明書の SAN フィールドに、Catalyst Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

（注） Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、Cisco Cloud APIC リリースノート [英語] を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]**。

ステップ 2 [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。

ステップ 3 プライマリ AAA サーバーを設定するには、次の情報を入力します。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

ステップ 4 Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address]：ISE サーバーの IP アドレス。
- [Shared Secret]：デバイス認証のキー。
- [Username]：Cisco ISE CLI にログインするために使用するユーザー名。

  （注）
  このユーザーにはスーパーユーザーの管理権限が必要です。

- [Password]：Cisco ISE CLI ユーザー名に対応するパスワード。
- [FQDN]：Cisco ISE サーバーの完全修飾ドメイン名（FQDN）。

  （注）
  - Cisco ISE（**[Administration]** > **[Deployment]** > **[Deployment Nodes]** > **[List]**）で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
  - 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名（CN）または Subject Alternative Name（SAN）と一致する必要があります 。

FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。

hostname.domainname.com

たとえば、Cisco ISE サーバーの FQDN は ise.cisco.com である可能性があります。

- [Virtual IP Address（es）]：Cisco ISE ポリシーサービスノード（PSN）が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

ステップ 5 [Advanced Settings] をクリックして、設定を構成します。

- [Connect to pxGrid]：pxGrid 接続を有効にするには、このチェックボックスをオンにします。

  Catalyst Center システム証明書を pxGrid クライアント証明書として使用する場合（pxGrid クライアントとして Catalyst Center システムを認証するために Cisco ISE に送信）、[**Use Catalyst Center Certificate for pxGrid**] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Catalyst Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

  このオプションを有効にする場合は、次のことを確認してください。

  - Catalyst Center 証明書が、Cisco ISE で使用中の CA と同じ認証局（CA）によって生成されていること（そうでない場合、pxGrid 認証は失敗します）。
  - [Certificate Extended Key Use（EKU）] フィールドに「クライアント認証」が含まれていること。

- [Protocol]：[TACACS] と [RADIUS]（デフォルト）。両方のプロトコルを選択できます。

  注目
  ここで Cisco ISE サーバーの TACAS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design]** > **[Network Settings]** > **[Network]**で Cisco ISE サーバーを TACAS サーバーとして設定できません。

- [Authentication Port]：AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- [Accounting Port]：AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- [Port]：デフォルトの TACACS ポートは 49 です。
- [Retries]：接続の試行が中止される前に、Catalyst Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- [Timeout]：接続の試行が中止される前に、デバイスが AAA サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

（注）
必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Catalyst Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、[Authentication and Policy Servers] ウィンドウと [System 360] ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「進行中」
- [System 360] ウィンドウ：「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「アクティブ」
- [System 360] ウィンドウ：「プライマリ使用可能」および「pxGrid 使用可能」

設定された Cisco ISE サーバーのステータスがパスワードの変更により [FAILED] と表示されている場合は、[Retry] をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

SNMP プロパティの設定

SNMP の再試行とタイムアウトの値を設定できます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[Device Settings]** > **[SNMP]** の順に選択します。

ステップ 2 次のフィールドを設定します。

- [Retries]：許容されるデバイス接続の最大試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
- [Timeout (in Seconds)]：タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Catalyst Center が待機する秒数。有効な値は 5 秒間隔で 1 ～ 300 秒の範囲内です。デフォルトは 5 秒です。

ステップ 3 **[保存（Save）]**をクリックします。

（注）
デフォルトの設定に戻すには、**[リセットして保存（Reset and 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。