



## 管理 ISE-PIC

- [ISE-PIC ノードの管理 \(1 ページ\)](#)
- [ISE-PIC のインストールの管理 \(7 ページ\)](#)
- [での設定の管理 ISE-PIC \(32 ページ\)](#)

### ISE-PIC ノードの管理

セカンダリノードの追加または削除、ノード間のデータの同期、セカンダリノードのプライマリノードへの昇格などを行います。

### Cisco ISE-PIC 展開のセットアップ

『*Cisco Identity Services Engine Hardware Installation Guide*』で説明されているように Cisco ISE-PIC をすべてのノードにインストールした後、ノードはスタンドアロン状態で稼働します。次に、1つのノードをプライマリ管理ノード (PAN) として定義し、セカンダリノードを PAN に登録する必要があります。

すべての Cisco ISE-PIC システムおよび機能に関連する設定は、PAN でだけ実行する必要があります。PAN で行った設定の変更は、展開内のセカンダリノードに複製されます。セカンダリノードからは、セカンダリノードを PAN に昇格させるアクションのみを実行できます。

セカンダリノードを PAN に登録した後は、そのセカンダリノードの管理者ポータルにログインする場合にも、PAN のログインクレデンシャルを使用する必要があります。

### プライマリからセカンダリ ISE-PIC ノードへのデータレプリケーション

1つの Cisco ISE ノードをセカンダリノードとして登録すると、Cisco ISE-PIC はプライマリノードからセカンダリノードへのデータレプリケーションチャンネルをすぐに作成し、複製のプロセスを開始します。複製は、プライマリノードからセカンダリノードに Cisco ISE-PIC 設定データを共有するプロセスです。複製によって、展開を構成する2つの Cisco ISE-PIC ノードの設定データの整合性を確実に維持できます。

通常、最初に ISE-PIC ノードをセカンダリ ノードとして登録したときに、完全な複製が実行されます。完全な複製の実行後は差分複製が実行され、PAN での設定データに対する新しい変更（追加、変更、削除など）がセカンダリ ノードに反映されます。複製のプロセスでは、展開内の Cisco ISE-PIC ノードが同期されます。Cisco ISE-PIC 管理者ポータルでの展開のページから [ノードステータス (Node Status)] 列で複製のステータスを表示できます。セカンダリ ノードとして Cisco ISE-PIC ノードを登録するか、または PAN との手動同期を実行すると、要求されたアクションが進行中であることを示すオレンジのアイコンがノードステータスに表示されます。これが完了すると、ノードステータスは、セカンダリ ノードが PAN と同期されたことを示す緑に変わります。

## Cisco ISE-PIC でのノードの変更による影響

Cisco ISE-PIC で次のいずれかの変更を行うと、そのノードが再起動するため、遅延が発生します。

- ノードの登録（スタンドアロンからセカンダリへ）
- ノードの登録解除（セカンダリからスタンドアロンへ）
- プライマリ ノードからスタンドアロンへの変更（他のノードが登録されていない場合は、プライマリからスタンドアロンに変更されます）
- ノードの昇格（セカンダリからプライマリへ）
- プライマリでのバックアップの復元（同期操作がトリガーされ、プライマリ ノードからセカンダリ ノードにデータが複製されます）



(注) セカンダリ管理ノードをプライマリ PAN の位置に昇格させると、プライマリノードがセカンダリロールになります。これにより、プライマリノードとセカンダリノードの両方が再起動し、遅延が発生します。

## 展開で 2 つのノードを設定する場合のガイドライン

2 つのノードを使用して Cisco ISE-PIC をセットアップする前に、次の内容をよく読んでください。

- 両方のノードに同じ Network Time Protocol (NTP) サーバーを選択します。ノード間のタイムゾーンの問題を回避するには、各ノードのセットアップ中に同じ NTP サーバー名を指定する必要があります。この設定で、展開内にあるさまざまなノードからのレポートとログが常にタイムスタンプで同期されるようになります。
- Cisco ISE-PIC のインストール時に Cisco ISE-PIC の管理者パスワードを設定します。以前の Cisco ISE-PIC 管理者のデフォルトのログインクレデンシャル (admin/cisco) は無効になっています。初期セットアップ中に作成したユーザー名とパスワードを使用するか、または後でパスワードを変更した場合はそのパスワードを使用します。

- ドメイン ネーム システム (DNS) サーバーを設定します。DNS サーバーでの展開に含まれる両方の Cisco ISE-PIC ノードの IP アドレスと完全修飾ドメイン名 (FQDN) を入力します。解決できない場合は、ノード登録が失敗します。
- DNS サーバーからのハイアベイラビリティ展開の Cisco ISE-PIC ノードの両方に正引きと逆引きの DNS ルックアップを設定します。設定しなかった場合、Cisco ISE-PIC ノードの登録時および再起動時に、展開に関する問題が発生することがあります。両方のノードに逆引き DNS ルックアップが設定されていない場合は、パフォーマンスが低下する可能性があります。
- (任意) PAN からセカンダリ Cisco ISE-PIC ノードを登録解除して、Cisco ISE-PIC をアンインストールします。
- PAN と、セカンダリノードとして登録しようとしているスタンドアロンノードで、同じバージョンの Cisco ISE-PIC が実行されていることを確認します。

## 展開内のノードの表示

[展開ノード (Deployment Nodes)] ウィンドウで、展開を構成するプライマリとセカンダリの ISE-PIC ノードを表示できます。

**ステップ 1** プライマリ Cisco ISE-PIC 管理者ポータルにログインします。

**ステップ 2** [管理 (Administration)] > [展開 (Deployment)] の順に選択します。

展開を構成するすべての Cisco ISE ノードが表示されます。

## セカンダリ Cisco ISE-PIC ノードの登録

セカンダリ ノードを登録した後、プライマリ ノードのデータベースにセカンダリ ノードの設定が追加され、セカンダリ ノードのアプリケーションサーバーが再起動します。再起動が完了すると、PAN の [展開 (Deployment)] ページから行ったすべての設定変更を表示できます。ただし、変更が反映され、[展開 (Deployment)] ページに表示されるには 5 分間の遅延が生じます。

**ステップ 1** PAN にログインします。

**ステップ 2** [管理 (Administration)] > [展開 (Deployment)] を選択します。

展開にセカンダリノードが登録されていない場合は、ページの下部に [セカンダリノードの追加 (Add Secondary Node)] セクションが表示されます。

**ステップ 3** [セカンダリノードの追加 (Add Secondary Node)] セクションで、セカンダリ Cisco ISE ノードの DNS 解決可能なホスト名を入力します。

Cisco ISE-PIC ノードの登録時にホスト名を使用する場合、登録するスタンドアロンノードの完全修飾ドメイン名 (FQDN) (たとえば、*abc.xyz.com*) は、PAN から DNS を使用して解決できる必要があります。解

決できない場合は、ノード登録が失敗します。DNS サーバーでセカンダリ ノードの IP アドレスおよび FQDN を事前に定義しておく必要があります。

**ステップ 4** [ユーザー名 (Username) ] フィールドおよび [パスワード (Password) ] フィールドに、スタンドアロン ノードの UI ベースの管理者クレデンシアルを入力します。

**ステップ 5** [保存 (Save) ] をクリックします。

Cisco ISE-PIC はセカンダリノードに接続し、ホスト名、デフォルトゲートウェイなどの基本情報を取得して表示します。

セカンダリノードが展開に登録されるとノードが再起動しますが、[展開 (Deployment) ] ページからセカンダリノードの情報が表示されるまでに最大 5 分かかることがあります。

セカンダリノードが正常に登録されると、[展開 (Deployment) ] ページの[セカンダリノード (Secondary Node) ] セクションにそのノードの詳細が表示されます。

セカンダリ ノードが正常に登録されると、PAN で、ノードの正常な登録を確認するアラームを受信します。セカンダリ ノードの PAN への登録が失敗した場合は、このアラームは生成されません。ノードが登録されると、そのノードのアプリケーションサーバーが再起動します。登録およびデータベース同期が正常に完了した後、セカンダリ ノードのユーザーインターフェイスにログインするにはプライマリ管理ノードのクレデンシアルを入力します。



(注) 展開の既存のプライマリ ノードに加えて、新しいノードの登録に成功した場合は、新しく登録されたノードに対応するアラームは表示されません。設定変更アラームは、新しく登録されたノードに対応する情報を反映します。新しいノードが正常に登録されたことを確認するためにこの情報を使用できます。

## プライマリおよびセカンダリの Cisco ISE-PIC ノードの同期

Cisco ISE-PIC の構成に変更を加えることができるのは、プライマリ PAN からのみです。設定変更はすべてのセカンダリ ノードに複製されます。何らかの理由でこの複製が正しく実行されない場合は、プライマリ PAN に手動でセカンダリ PAN を同期できます。

**ステップ 1** プライマリ PAN にログインします。

**ステップ 2** [管理 (Administration) ] > [展開 (Deployment) ] の順に選択します。

**ステップ 3** プライマリ PAN と同期させるノードの横にあるチェックボックスをオンにし、[同期を更新 (Syncup) ] をクリックして完全データベース複製を強制的に実行します。

## セカンダリ PAN のプライマリへの手動昇格

プライマリ PAN が失敗し場合は、セカンダリ PAN を新しいプライマリ PAN に手動で昇格させる必要があります。

### 始める前に

プライマリ PAN に昇格するように設定された 2 番目の Cisco ISE-PIC ノードがあることを確認します。

**ステップ 1** セカンダリ PAN GUI にログインします。

**ステップ 2** [管理 (Administration)] > [展開 (Deployment)] の順に選択します。

**ステップ 3** [ノードの編集 (Edit Node)] ウィンドウで、[プライマリに昇格 (Promote to Primary)] をクリックします。

**ステップ 4** [保存 (Save)] をクリックします。

### 次のタスク

元はプライマリ PAN であったノードが復帰した場合は、自動的にレベルが下げられ、セカンダリ PAN になります。このノード (元のプライマリ PAN) で手動で同期を実行し、ノードを展開に戻す必要があります。

## 展開からのノードの削除

展開からノードを削除するには、ノードの登録を解除する必要があります。登録解除されたノードは、スタンドアロン Cisco ISE-PIC ノードになります。

ノードの登録が取り消されると、エンドポイントデータは失われます。ノードがスタンドアロンノードになった後で、そのノードでエンドポイントデータを保持するには、プライマリ PAN からバックアップを取得し、そのノードでこのデータ バックアップを復元できます。

プライマリ PAN の [展開 (Deployment)] ウィンドウからこれらの変更を表示できます。ただし、変更が反映され、[展開 (Deployment)] ウィンドウに表示されるには 5 分間の遅延が生じます。

### 始める前に

展開からノードを削除するには、ノードの登録を解除する必要があります。PAN からセカンダリ ノードの登録を解除すると、登録解除されたノードのステータスがスタンドアロンに変わり、プライマリ ノードとセカンダリ ノード間の接続が失われます。複製の更新は、登録解除されたスタンドアロン ノードに送信されなくなります。

展開からセカンダリ ノードを削除する前に、必要に応じて後で復元できるように Cisco ISE-PIC 設定のバックアップを実行します。

- 
- ステップ1 [管理 (Administration)] > [展開 (Deployment)] の順に選択します。
- ステップ2 セカンダリ ノードの詳細の隣にある [登録解除 (Deregister)] をクリックします。
- ステップ3 [OK] をクリックします。
- ステップ4 プライマリ PAN のアラームの受信を確認し、セカンダリ ノードの登録が正常に解除されたことを確認します。セカンダリ ノードのプライマリ PAN からの登録の解除が失敗した場合は、このアラームは生成されません。
- 

## Cisco ISE-PIC ノードのホスト名または IP アドレスの変更

スタンドアロン Cisco ISE-PIC ノードのホスト名、IP アドレス、またはドメイン名を変更できます。ただし、ノードのホスト名として **localhost** を使用することはできません。

### 始める前に

Cisco ISE-PIC ノードが 2 ノード展開の一部である場合、展開から削除し、スタンドアロンノードであることを確認する必要があります。

- 
- ステップ1 Cisco ISE CLI から **hostname**、**ip address**、または **ip domain-name** の各コマンドを使用して Cisco ISE-PIC ノードのホスト名または IP アドレスを変更します。
- ステップ2 すべてのサービスを再起動するために、Cisco ISE CLI から **application stop ise** コマンドを使用して Cisco ISE-PIC アプリケーション設定をリセットします。
- ステップ3 Cisco ISE-PIC ノードは、2 ノード展開の一部である場合はプライマリ PAN に登録します。

(注) Cisco ISE-PIC ノードの登録時にホスト名を使用する場合、登録するスタンドアロンノードの完全修飾ドメイン名 (FQDN) (たとえば、*abc.xyz.com*) は、プライマリ PAN から DNS を使用して解決できる必要があります。解決できない場合は、ノード登録が失敗します。DNS サーバーに、展開の一部である Cisco ISE-PIC ノードの IP アドレスと FQDN を入力する必要があります。

セカンダリノードとして Cisco ISE-PIC ノードを登録した後、プライマリ PAN は IP アドレス、ホスト名、またはドメイン名への変更を展開内の他の Cisco ISE-PIC ノードに複製します。

---

## Cisco ISE-PIC アプライアンス ハードウェアの交換

Cisco ISE-PIC アプライアンス ハードウェアは、ハードウェアに問題がある場合のみ交換する必要があります。ソフトウェアに問題がある場合は、アプリケーションのイメージを再作成し、Cisco ISE-PIC ソフトウェアを再インストールできます。

- 
- ステップ1 新しいノードで Cisco ISE-PIC ソフトウェアを再インストールするか、またはイメージを再作成します。

- ステップ2** プライマリおよびセカンダリ PAN の UDI を使用してライセンスを取得し、プライマリ PAN にインストールします。
- ステップ3** 置き換えられたプライマリ PAN でバックアップを復元します。  
復元スクリプトはセカンダリ PAN でデータの同期を試行しますが、現在セカンダリ PAN はスタンドアロンノードであり、同期は失敗します。データは、プライマリ PAN でバックアップが実行された時刻に設定されます。
- ステップ4** 新しいノードをセカンダリ サーバーとしてプライマリ PAN に登録します。

---

## ISE-PIC のインストールの管理

パッチのインストール、バックアップの実行、またはシステムの復元の実装を行います。

### ソフトウェアパッチのインストール

- ステップ1** [管理 (Administration)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] を選択し、[インストール (Install)] をクリックします。
- ステップ2** [参照 (Browse)] をクリックし、Cisco.com からダウンロードしたパッチを選択します。
- ステップ3** [インストール (Install)] をクリックしてパッチをインストールします。  
PAN でのパッチのインストールが完了すると、Cisco ISE-PIC から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。
- (注) パッチインストールの進行中は、[パッチ管理 (Patch Management)] ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。
- ステップ4** [管理 (Administration)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] を選択して、[パッチのインストール (Patch Installation)] ページに戻ります。
- ステップ5** インストールしたパッチの横のオプションボタンをクリックし、[ノードステータスを表示 (Show Node Status)] をクリックしてインストールが完了したことを確認します。

---

### Cisco ISE-PIC ソフトウェアパッチ

Cisco ISE-PIC ソフトウェアのパッチは常に累積されます。Cisco ISE-PIC では、パッチのインストールおよびロールバックを CLI または GUI から実行できます。

展開内の Cisco ISE-PIC サーバーにパッチをインストールする作業は、プライマリ PAN から行うことができます。プライマリ PAN からパッチをインストールするには、Cisco.com からクライアントブラウザを実行しているシステムにパッチをダウンロードします。

GUI からパッチをインストールする場合、パッチは最初にプライマリ PAN に自動的にインストールされます。その後、システムは、GUI にリストされている順序で、展開内の他のノード

にパッチをインストールします。ノードが更新される順序を制御することはできません。パッチバージョンを手動でインストール、ロールバック、および表示することもできます。Cisco ISE GUI で [メニュー (Menu) ] アイコン (☰) をクリックして、[管理 (Administration) ] > [システム (System) ] > [メンテナンス (Maintenance) ] > [パッチ管理 (Patch Management) ]。

CLI からパッチをインストールする場合は、ノードの更新順序を制御できます。ただし、最初にプライマリ PAN にパッチをインストールすることを推奨します。残りのノードでのインストールの順序は関係ありません。プロセスを高速化するために、パッチを複数のノードに同時にインストールできます。

展開全体をアップグレードする前にいくつかのノードでパッチを検証する場合、CLI を使用すると、選択したノードでパッチをインストールできます。パッチをインストールするには、次の CLI コマンドを使用します。

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

詳細については、『Cisco Identity Services Engine CLI リファレンスガイド』の「EXEC モードの Cisco ISE CLI コマンド」の章にある「patch install」の項を参照してください。

必要なパッチバージョンを直接インストールすることができます。たとえば、Cisco ISE 2.x を使用していて、Cisco ISE 2.x パッチ 5 をインストールする場合、以前のパッチ (Cisco ISE 2.x パッチ 1 ~ 4 など) をインストールしなくても、Cisco ISE 2.x パッチ 5 を直接インストールできます。CLI でパッチバージョンを表示するには、次の CLI コマンドを使用します。

```
show version
```

## ソフトウェアパッチインストールのガイドライン

ISE ノードにパッチをインストールすると、インストールの完了後にノードが再起動されます。再びログインできる状態になるまで、数分かかることがあります。メンテナンスウィンドウ中にパッチをインストールするようにスケジュール設定し、一時的な機能停止を回避することができます。

インストールするパッチが、ネットワーク内に展開されている Cisco ISE-PIC のバージョンに適用されるものであることを確認してください。Cisco ISE-PIC はパッチファイルのバージョンの不一致とあらゆるエラーをレポートします。



(注) Cisco ISE パッチは、ISE-PIC にもインストールできます。

Cisco ISE-PIC に現在インストールされているパッチよりも低いバージョンのパッチをインストールできません。同様に、あるバージョンのパッチの変更をロールバックしようとしたときに、それよりも高いバージョンのパッチがその時点で Cisco ISE-PIC にインストール済みの場合は、ロールバックはできません。たとえば、パッチ 3 が Cisco ISE-PIC サーバーにインストール済みの場合に、パッチ 1 または 2 をインストールしたり、パッチ 1 または 2 にロールバックすることはできません。

2 ノード展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco ISE-PIC によってそのパッチが展開内のプライマリノードとセカンダリノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco ISE-PIC はセカンダ



リノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。

## ソフトウェアパッチのロールバック

複数のノードの展開の一部である PAN からパッチのロールバックを実行するときは、Cisco ISE-PIC によってそのパッチが展開内のプライマリノードとセカンダリノードにロールバックされます。

**ステップ 1** [管理 (Administration)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] ISE-PIC GUI で [メニュー (Menu)] アイコン (☰) をクリックして、

**ステップ 2** 変更をロールバックするパッチバージョンのオプションボタンをクリックしてから、[ロールバック (Rollback)] をクリックします。

(注) パッチのロールバックの進行中は、[パッチ管理 (Patch Management)] ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

PAN からのパッチのロールバックが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

**ステップ 3** ログイン後に、ページの一番下にある [アラーム (Alarms)] リンクをクリックしてロールバック操作のステータスを表示します。

**ステップ 4** パッチのロールバックの進行状況を表示するには、[パッチ管理 (Patch Management)] ページでパッチを選択し、[ノードステータスを表示 (Show Node Status)] をクリックします。

**ステップ 5** パッチのオプションボタンをクリックし、セカンダリノード上で [ノードステータスを表示 (Show Node Status)] をクリックして、そのパッチが展開内のすべてのノードからロールバックされたことを確認します。

そのパッチがロールバックされていないセカンダリノードがある場合は、そのノードが稼働中であることを確認してから、プロセスをもう一度実行して残りのノードから変更をロールバックしてください。Cisco ISE-PIC は、このバージョンのパッチがインストールされているノードからのみパッチをロールバックします。

## ソフトウェアパッチ ロールバックのガイドライン

展開の Cisco ISE-PIC ノードからパッチをロールバックするには、最初に PAN から変更をロールバックします。これに成功すると、セカンダリノードからパッチがロールバックされます。PAN でロールバックプロセスが失敗した場合は、セカンダリノードからのパッチロールバックは行われません。

Cisco ISE-PIC によるセカンダリノードからのパッチロールバックが進行中のときも、引き続き PAN GUI から他のタスクを実行できます。セカンダリノードは、ロールバック後に再起動されます。

## バックアップと復元データ



(注) シスコ ISE-PIC は、多くの場合、Cisco ISE のバックアップおよび復元の手順と同じように機能します。そのため、Cisco ISE-PIC に関連する操作や機能を示すために Cisco ISE という用語を同義で使用する場合があります。

Cisco ISE-PIC では、プライマリノードまたはスタンドアロンノードからデータをバックアップできます。バックアップは CLI またはユーザー インターフェイスから実行できます。

Cisco ISE-PIC では次のタイプのデータのバックアップが可能です。

- 設定データ：アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。
- 運用データ：モニタリングおよびトラブルシューティング データが含まれます。

## バックアップ/復元リポジトリ

Cisco ISE-PIC では、リポジトリを作成および削除できます。次のタイプのリポジトリを作成できます。

- ディスク (DISK)
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

KVM を使用して作成された仮想 CD-ROM を CD-ROM としてリポジトリ タイプを作成できます。



(注) リポジトリは、各デバイスに対してローカルです。



(注) 小規模な展開 (100 個以下のエンドポイント) では、10 GB のリポジトリを、中規模の展開では 100 GB のリポジトリを、大規模な展開では 200 GB のリポジトリを用意することを推奨します。

## リポジトリの作成

リポジトリを作成するには、CLIとGUIを使用できます。次の理由により、GUIを使用することを推奨します。

- CLIで作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。これらのリポジトリは、GUIのリポジトリ ページに表示されません。
- プライマリ PAN で作成されたリポジトリが他の展開ノードに複製されます。

キーはプライマリ PAN でのみ GUI で生成されます。このため、アップグレード時に新しいプライマリ管理ノードの GUI でキーを再生成して、SFTP サーバーにエクスポートする必要があります。展開からノードを除去する場合、管理対象以外のノードの GUI でキーを生成し、SFTP サーバーにエクスポートする必要があります。

RSA 公開キー認証を使用する Cisco ISE-PIC の SFTP リポジトリを設定できます。データベースとログを暗号化するために管理者が作成したパスワードを使用する代わりに、セキュアキーを使用する RSA 公開キー認証を選択できます。RSA 公開キーを使用して作成された SFTP リポジトリの場合、GUI から作成されたリポジトリは CLI では複製されず、CLI から作成されたリポジトリは GUI では複製されません。CLI と GUI で同じリポジトリを設定するには、CLI と GUI の両方で RSA 公開キーを生成し、この両方のキーを SFTP サーバーにエクスポートします。



- (注) Cisco ISE は、FIPS モードが ISE で有効になっていない場合でも、FIPS モードで発信 SSH または SFTP 接続を開始します。ISE と通信するリモート SSH または SFTP サーバーが FIPS 140 承認暗号化アルゴリズムを許可していることを確認します。

Cisco ISE では、組み込みの FIPS 140 の検証済み暗号化モジュールが使用されています。FIPS コンプライアンスの要求の詳細については、『[FIPS Compliance Letter](#)』を参照してください。

### 始める前に

- RSA 公開キー認証を使用して SFTP リポジトリを作成する場合は、次の手順を実行します。
  - SFTP リポジトリの RSA 公開キー認証を有効にします。
  - 管理 CLI ユーザーとしてログインする必要があります。 `crypto host_key add` コマンドを使用して Cisco ISE CLI から SFTP サーバーのホストキーを入力します。ホストキー文字列は、リポジトリの設定ページで、[パス (Path)] フィールドに入力したホスト名と一致する必要があります。
  - GUI でキーペアを生成し、ローカルシステムに公開キーをエクスポートします。Cisco ISE CLI から `crypto key generate rsa passphrase test123` コマンドを使用してキーペアを生成し（この場合パスフレーズは 14 文字以上でなければなりません）、キーを任意のリポジトリ（ローカルディスクまたは設定されているその他のリポジトリ）にエクスポートします。

- エクスポートした RSA 公開キーを PKI 対応の SFTP サーバーにコピーし、「authorized\_keys」ファイルに追加します。



- (注) プライマリ PAN とプライマリ MnT が別々のノードである場合、[リポジトリリスト (Repository List)] ウィンドウの [キーペアの生成 (Generate Key Pairs)] オプションを使用して、プライマリ PAN とプライマリ MnT ノードの両方の RSA キーを生成できます。[リポジトリリスト (Repository List)] ウィンドウの [公開キーのエクスポート (Export Public Key)] オプションを使用して、プライマリ PAN ノードとプライマリ MnT ノードの両方から生成された RSA キーをエクスポートできます。

- ステップ 1** [管理 (Administration)] > [メンテナンス (Maintenance)] > [リポジトリ (Repository)] を選択します。
- ステップ 2** [追加 (Add)] をクリックして、新しいリポジトリを追加します。
- ステップ 3** 新しいリポジトリのセットアップの必要に応じて値を入力します。フィールドの説明については、[リポジトリの設定 \(13 ページ\)](#) を参照してください。
- ステップ 4** [送信 (Submit)] をクリックしてリポジトリを作成します。
- ステップ 5** 左側の [操作 (Operations)] ナビゲーションペインで [リポジトリ (Repository)] をクリックするか、または [リポジトリ (Repository)] ウィンドウ上部の [リポジトリリスト (Repository List)] リンクをクリックして、リポジトリのリストページに移動して、リポジトリが正常に作成されていることを確認します。

#### 次のタスク

- 作成したリポジトリが有効であることを確認します。これは、[リポジトリのリスト (Repository Listing)] ウィンドウから行います。対応するリポジトリを選択し、[検証 (Validate)] をクリックします。また、Cisco ISE コマンドラインインターフェイスから次のコマンドを実行することもできます。

```
show repository repository_name
```

ここで、*repository\_name* は作成したリポジトリの名前です。



- (注) リポジトリの作成時に指定したパスが存在しない場合、次のエラーが表示されます。

```
%Invalid Directory
```

- オンデマンドバックアップを実行するかバックアップのスケジュールを設定します。

## リポジトリの設定

次の表では、リポジトリを作成してバックアップファイルを保存するために使用できる [リポジトリリスト (Repository List)] ウィンドウのフィールドについて説明します。このウィンドウを表示するには、[メニュー (Menu)] アイコン (☰) をクリックして、[管理 (Administration)] > [メンテナンス (Maintenance)] > [リポジトリ (Repository)] の順に選択します。

表 1: リポジトリの設定

フィールド	使用上のガイドライン
リポジトリ (Repository)	リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。
プロトコル (Protocol)	使用する使用可能なプロトコルの 1 つを選択します。
ホスト (Host)	(TFTP、HTTP、HTTPS、FTP、SFTP、および NFS で必須) リポジトリの作成先サーバーのホスト名または IP アドレス (IPv4 または IPv6) を入力します。  (注) IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。
パス (Path)	リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。  !、?、~のような一部の特殊文字 (上記のリストには含まれていません) は、GUI を使用した FTP および SFTP パスワード設定に使用できることに注意してください。ただし、これらの特殊文字は、CLI または Open API による設定には使用できません。

### 関連トピック

[バックアップ/復元リポジトリ](#)

[リポジトリの作成 \(11 ページ\)](#)

## SFTP リポジトリでの RSA 公開キー認証の有効化

SFTP サーバーでは、各ノードに2つの RSA 公開キー（CLI 用と GUI 用にそれぞれ1つずつ）が必要です。SFTP リポジトリで RSA 公開キー認証を有効にするには、次の手順を実行します。



- (注) SFTP リポジトリで RSA 公開キー認証を有効にすると、SFTP ログイン情報を使用してログインできなくなります。PKI ベースの認証またはログイン情報ベースの認証を使用できます。ログイン情報ベースの認証を再度使用する場合は、SFTP サーバーから公開キーペアを削除する必要があります。

**ステップ 1** `/Etc/ssh/sshd_config` ファイルを編集する権限を持つアカウントで SFTP サーバーにログインします。

- (注) `sshd_config` ファイルのロケーションは、インストールされているオペレーティングシステムによって異なる可能性があります。

**ステップ 2** `vi etc/ssh/sshd_config` コマンドを入力します。

`Sshd_config` ファイルの内容がリストされます。

**ステップ 3** RSA 公開キー認証を有効にするには、以下の行の「#」記号を削除します。

- `RSAAuthentication yes`
- `PubkeyAuthentication yes`

(注) `Public Auth Key` が `no` の場合は `yes` に変更してください。

- `AuthorizedKeysFile ~/.ssh/authorized_keys`

## オンデマンドおよびスケジュール バックアップ

プライマリ PAN のオンデマンドバックアップを設定できます。バックアップデータがすぐに必要な場合にオンデマンドバックアップを実行します。

システムレベルのバックアップは、1 回のみ、毎日、毎週、または毎月実行するようにスケジュールできます。バックアップ操作は長時間かかる場合がありますが、スケジュールできるため中断が発生することはありません。管理者ポータルからバックアップをスケジュールできます。



- 
- (注) 内部 CA を使用している場合は、CLI を使用して証明書とキーをエクスポートする必要があります。管理ポータルでのバックアップでは、CA チェーンはバックアップされません。

詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Basic Setup」の章にある「Export Cisco ISE CA Certificates and Keys」の項を参照してください。

---



- 
- (注) Cisco ISE の設定バックアップおよび運用バックアップは、短時間でシステムがオーバーロードになる可能性があります。この一時的なシステムオーバーロードで予想される動作は、システムの設定とモニタリングデータベースのサイズによって異なります。
- 

### オンデマンドバックアップの実行

オンデマンドバックアップを実行して、設定データまたはモニタリング（運用）データを即座にバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE-PIC が復元されます。



**重要** バックアップと復元を行う場合、復元によってターゲットシステム上の信頼できる証明書の一覧がソースシステムの証明書の一覧によって書き換えられます。バックアップおよび復元機能に内部認証局 (CA) の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

• **オプション 1 :**

CA 証明書をソース ISE-PIC ノードから CLI を使用してエクスポートし、ターゲットシステムに CLI を使用してインポートします。

**長所 :** ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

**短所 :** 復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

• **オプション 2 :**

復元処理の後、内部 CA のすべての新しい証明書を生成します。

**長所 :** このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

**短所 :** 復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

**始める前に**

- オンデマンドバックアップを実行する前に、Cisco ISE-PIC 内のバックアップデータタイプの基本を理解しておく必要があります。
- バックアップファイルを保存するためのリポジトリが作成されていることを確認します。
- ローカルリポジトリを使用してバックアップしないでください。

**ステップ 1** ISE-PIC GUI で [メニュー (Menu) ] アイコン (☰) をクリックして、[管理 (Administration) ] > [メンテナンス (Maintenance) ] > [バックアップ/復元 (Backup and Restore) ] を選択します。

**ステップ 2** バックアップのタイプ [設定 (Configuration) ] または [動作中 (Operational) ] を選択します。

**ステップ 3** [すぐにバックアップ (Backup Now) ] をクリックします。

**ステップ 4** バックアップを実行するために必要な値を入力します。

**ステップ 5** [バックアップ (Backup) ] をクリックします。



**ステップ 6** バックアップが正常に完了したことを確認します。

Cisco ISE-PIC はタイムスタンプを持つバックアップファイル名を付け、指定されたりポジトリにファイルを保存します。タイムスタンプに加えて、Cisco ISE-PIC は設定バックアップには CFG タグ、操作バックアップには OPS タグを追加します。バックアップファイルが指定リポジトリにあることを確認します。

バックアップの実行中はノードを昇格しないでください。これによりすべてのプロセスがシャットダウンし、バックアップを同時に実行中の場合はデータに不一致が生じる場合があります。ノードを変更する際は、バックアップが完了するまで待ってください。

(注) バックアップが実行されているときに、高い CPU 使用率が観察されたり、[負荷平均が高い (High Load Average) ]アラームが表示されたりする可能性があります。バックアップが完了すると、CPU 使用率は通常に戻ります。

---

### バックアップのスケジュール

オンデマンドバックアップを実行して、設定データまたはモニターリング (運用) データを即座にバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE-PIC が復元されます。



**重要** バックアップと復元を行う場合、復元によってターゲットシステム上の信頼できる証明書がリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局 (CA) の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

• **オプション 1 :**

CA 証明書をソース ISE-PIC ノードから CLI を使用してエクスポートし、ターゲットシステムに CLI を使用してインポートします。

**長所 :** ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲットシステムによって発行された新しい証明書は、同じキーによって署名されます。

**短所 :** 復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

• **オプション 2 :**

復元処理の後、内部 CA のすべての新しい証明書を生成します。

**長所 :** このオプションは推奨される適切な方法です。元のソースの証明書または元のターゲットの証明書が使用されます。元のソースシステムによって発行された証明書は引き続き信頼されます。

**短所 :** 復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

**始める前に**

- バックアップをスケジュールする前に、Cisco ISE-PIC 内のバックアップデータタイプの基本を理解しておく必要があります。
- リポジトリを設定していることを確認します。
- ローカルリポジトリを使用してバックアップしないでください。



(注) バックアップ/復元操作では、次のリポジトリタイプはサポートされていません。CD-ROM、HTTP、HTTPS、または TFTP。これは、これらのリポジトリタイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

## CLI を使用したバックアップ

CLI と GUI の両方からバックアップのスケジュールを設定できますが、GUI の使用を推奨します。ただし、セカンダリ モニターリング ノードの操作バックアップは、CLI からのみ実行できます。

## バックアップ履歴

バックアップ履歴は、スケジュールまたはオンデマンドバックアップに関する基本情報です。バックアップ履歴には、バックアップ名、バックアップファイルのサイズ、バックアップが保存されているリポジトリ、バックアップが取られたタイムスタンプを表示します。この情報は、操作監査レポートまたは、履歴テーブルの [バックアップ/復元 (Backup and Restore)] ページから入手できます。

バックアップが失敗すると、Cisco ISE-PIC がアラームをトリガーします。バックアップ履歴ページに失敗の原因が表示されます。障害の原因は操作監査レポートにも記載されます。障害の原因が欠落しているか明確でない場合は、Cisco ISE CLI から **backup-logs** コマンドを実行し、ADE.log でより詳細な情報を確認できます。

バックアップ操作の実行中は、**show backup status** CLI コマンドを使用して、バックアップ操作の進行状況を確認することができます。

バックアップ履歴は、Cisco ADE オペレーティングシステムの設定データとともに保存されています。つまり、アプリケーションのアップグレード後もそこに残っており、PAN のイメージを再作成した場合にのみ削除されます。

## バックアップの失敗

バックアップが失敗した場合は、次を確認してください。

- NTP 同期またはサービス障害の問題があるかどうかを確認します。Cisco ISE の NTP サービスが動作していない場合、Cisco ISE では、[NTP サービスの障害 (NTP Service Failure)] のアラームが発生します。Cisco ISE が、設定されているすべての NTP サーバーと同期できない場合、Cisco ISE では、[NTP 同期に失敗 (NTP Sync Failure)] のアラームが発生します。NTP サービスがダウンしている場合、または同期の問題がある場合は、Cisco ISE のバックアップが失敗する可能性があります。バックアップ操作を再試行する前に、[アラーム (Alarm)] ダッシュレットを確認し、NTP 同期またはサービスの問題を修正してください。
- 他のバックアップが同時に実行されていないことを確認します。
- 設定したリポジトリの使用可能なディスク領域を確認します。
  - (操作) バックアップのモニターリングは、モニターリングデータがモニターリングデータベースに割り当てられたサイズの 75% を超えると失敗します。たとえばノードに 600 GB 割り当てられており、モニターリング データがストレージの 450 GB を超える領域を消費すると、モニターリングのバックアップは失敗します。
  - データベースのディスク使用量が 90% を超える場合、消去が発生してデータベースを割り当てられたサイズの 75% 以下のサイズにします。

- 消去が進行中かどうかを確認します。消去の進行中はバックアップ/復元操作は動作しません。
- リポジトリが正しく設定されていることを確認します。

## Cisco ISE 復元操作

プライマリまたはスタンドアロンノードで設定データを復元できます。プライマリ PAN にデータを復元したら、手動でセカンダリ ノードをプライマリ PAN と同期する必要があります。



- (注) Cisco ISE-PIC の新しいバックアップ/復元ユーザー インターフェイスでは、バックアップ ファイル名にメタデータが使用されます。したがって、バックアップが完了後に、バックアップ ファイル名を手動で変更しないでください。バックアップ ファイルの名前を手動で変更すると、Cisco ISE-PIC バックアップ/復元ユーザー インターフェイスがそのバックアップ ファイルを認識できなくなります。バックアップファイル名を変更しなければならない場合は、バックアップの復元に Cisco ISE CLI を使用する必要があります。

### データの復元に関するガイドライン



- (注) • Cisco ISE リリース 3.2 以降では、ルート CA の再生成は復元フローで自動的に行われます。したがって、構成バックアップ後のルート CA の再生成は必要ありません。

次は、Cisco ISE-PIC バックアップ データを復元する場合に従うべきガイドラインです。

- Cisco ISE では、ある ISE ノード (A) からバックアップを取得して、別の ISE ノード (B) に復元することができます。両方のノードは同じホスト名 (IP アドレスは異なる) です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータル グループ タグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。
- あるタイムゾーン内のプライマリ PAN からバックアップを取得して、別のタイムゾーン内の別の Cisco ISE-PIC ノードに復元する場合、復元プロセスが失敗することがあります。この問題は、バックアップファイルのタイムスタンプが、バックアップが復元される Cisco ISE-PIC ノードのシステム時刻より新しい場合に発生します。同じバックアップを、取得後 1 日経過してから復元すると、バックアップファイルのタイムスタンプが過去のものになり、復元プロセスは成功します。
- バックアップを取得したホスト名と別のホスト名を持つプライマリ PAN にバックアップを復元すると、プライマリ PAN はスタンドアロン ノードになります。展開が切断し、セカンダリ ノードは機能しなくなります。スタンドアロン ノードをプライマリ ノードにし、セカンダリ ノードの設定をリセットしてプライマリ ノードに再登録する必要があります。Cisco ISE-PIC ノードの設定をリセットするには、Cisco ISE CLI から次のコマンドを入力してください。
  - `application reset-config ise`

- システムのタイムゾーンは、最初の Cisco ISE-PIC インストールおよびセットアップ後に変更しないことを推奨します。
- 展開の 1 つ以上のノードの証明書設定を変更した場合は、データを復元するための別のバックアップをスタンドアロン Cisco ISE-PIC ノードまたはプライマリ PAN から取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。
- プライマリ PAN 上で設定バックアップを復元した後に、以前にエクスポートした Cisco ISE CA 証明書およびキーをインポートできます。



(注) Cisco ISE CA 証明書およびキーをエクスポートしなかった場合は、プライマリ PAN 上で設定バックアップを復元した後に、プライマリ PAN でルート CA および下位 CA を生成します。

- 適切な FQDN（プラチナ データベースの FQDN）を使用せずにプラチナ データベースを復元する場合は、CA 証明書を再生成する必要があります。（このウィンドウを表示するには、[メニュー（Menu）] アイコン (☰) をクリックして、[管理（Administration）]> [証明書（Certificates）]> [証明書署名要求（Certificate Signing Requests）]> [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA certificate chain）] を選択します）。ただし、適切な FQDN でプラチナデータベースを復元する場合は、CA 証明書が自動的に再生成されます。
- Cisco ISE-PIC がバックアップ ファイルを格納するデータ リポジトリが必要です。オンデマンドまたはスケジュール設定されたバックアップを実行する前に、リポジトリを作成する必要があります。
- スタンドアロンノードに障害が発生した場合、設定バックアップを実行して復元する必要があります。プライマリ PAN で障害が発生した場合、セカンダリ管理ノードをプライマリに昇格できます。その後、新しいプライマリ PAN にデータを復元できます。



(注) Cisco ISE-PIC では、**backup-logs** CLI コマンドも使用できます。このコマンドを使用して、ログやコンフィギュレーションファイルの収集を行い、これらをトラブルシューティングに利用できます。

## CLI からの設定またはモニターリング（操作）バックアップの復元

Cisco ISE CLI から設定データを復元するには、EXEC モードで **restore** コマンドを使用します。設定または操作バックアップからデータを復元するには、次のコマンドを使用します。

```
restore filename repository repository-name encryption-key hash|plain encryption-key name include-adeos
```

構文の説明

<b>restore</b>	設定または操作バックアップからデータを復元するには、このコマンドを入力します。
<i>filename</i>	リポジトリに存在するバックアップファイルのファイル名。最大120文字の英数字をサポートします。  (注) ファイル名の後に、 <b>tar.gpg</b> という拡張子を付ける必要があります ( <b>myfile.tar.gpg</b> など)。
<b>repository</b>	バックアップを含むリポジトリを指定します。
<i>repository-name</i>	バックアップを復元するリポジトリの名前。
<b>encryption-key</b>	(オプション) バックアップを復元するユーザー定義の暗号キーを指定します。
<b>hash</b>	バックアップを復元するためのハッシュされた暗号キー。使用する暗号化された (ハッシュ化された) 暗号キーを指定します。40文字まで指定します。
<b>plain</b>	バックアップを復元するためのプレーンテキストの暗号キー。使用する暗号化されたプレーンテキストの暗号キーを指定します。15文字まで指定します。
<i>encryption-key name</i>	暗号キーを入力します。
<b>include-adeos</b>	(オプション、設定バックアップのみに該当) 設定バックアップから ADE-OS 設定を復元する場合に、このコマンドオペレータパラメータを入力します。設定バックアップを復元する場合にこのパラメータを含めないと、Cisco ISE は Cisco ISE アプリケーション設定データのみを復元します。

### デフォルト

デフォルトの動作や値はありません。

### コマンドモード

EXEC

## 使用上のガイドライン

Cisco ISE-PIC で `restore` コマンドを使用すると、Cisco ISE-PIC サーバーが自動的に再起動します。

データの復元処理で、暗号キーはオプションです。暗号キーを指定しなかった以前のバックアップの復元をサポートするために、暗号キーなしで **restore** コマンドを使用できます。

## 例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore. Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

## 関連コマンド

	説明
<b>backup</b>	バックアップ（Cisco ISE-PIC と Cisco ADE OS）を実行して、そのバックアップをリポジトリに保存します。
<b>backup-logs</b>	システム ログをバックアップします。
<b>repository</b>	バックアップ設定のリポジトリ サブモードを入力します。
<b>show repository</b>	特定のリポジトリにある使用可能なバックアップ ファイルを表示します。
<b>show backup history</b>	システムのバックアップ履歴を表示します。
<b>show backup status</b>	バックアップ操作のステータスを表示します。
<b>show restore status</b>	復元操作のステータスを表示します。

いずれかのセカンダリ ノードでアプリケーション復元後の同期ステータスおよび複製ステータスが [非同期 (Out of Sync) ] になっている場合、該当セカンダリ ノードの証明書をプライマリ PAN に再インポートして、手動同期を実行する必要があります。

## GUI からの設定バックアップの復元

管理者ポータルで設定バックアップを復元できます。GUIには現在のリリースから取得されたバックアップのみが表示されます。このリリースより前のバックアップを復元するには、CLI から `restore` コマンドを使用します。

**ステップ 1** [管理 (Administration) ] > [メンテナンス (Maintenance) ] > [バックアップ/復元 (Backup and Restore) ] を選択します。

**ステップ 2** バックアップの名前を設定バックアップのリストから選択し、[復元 (Restore) ] をクリックします。

**ステップ 3** バックアップ時に使用した暗号キーを入力します。

**ステップ 4** [復元 (Restore) ] をクリックします。

### 次のタスク

Cisco ISE CA サービスを使用する場合は、次のことを実行する必要があります。

1. Cisco ISE CA ルート チェーン全体を再生成します。
2. Cisco ISE CA 証明書およびキーのバックアップをプライマリ PAN から取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI のルート CA または下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

### 復元履歴

[操作監査レポート (Operations Audit Report) ] ウィンドウから、すべての復元操作、ログイベント、ステータスに関する情報を取得できます。



(注) ただし [操作監査レポート (Operations Audit Report) ] には、前回の復元操作に対応する開始時間に関する情報はありません。

トラブルシューティング情報を入手するには、Cisco ISE CLI から `backup-logs` コマンドを実行して、`ADE.log` ファイルを調べる必要があります。

復元操作の進行中は、すべての Cisco ISE-PIC サービスは停止します。 `show restore status` CLI コマンドを使用して、復元操作の進行状況を確認できます。



## プライマリノードとセカンダリノードの同期

PANのバックアップファイルの復元後に、プライマリおよびセカンダリノードのCisco ISE-PICデータベースが自動的に同期されないことがあります。この場合には、PANからセカンダリISE-PICノードへの完全複製を手動で強制実行できます。強制同期は、PANからセカンダリノードにのみ可能です。同期操作中は、設定を変更することはできません。Cisco ISE-PICでは、同期が完全に完了した後にのみ、他のCisco ISE-PIC管理者ポータルページに移動して設定変更を行うことができます。

**ステップ1** [管理 (Administration)] > [展開 (Deployment)] の順に選択します。

**ステップ2** 非同期レプリケーションステータスのセカンダリノードの横にあるチェックボックスをオンにします。

**ステップ3** [同期を更新 (Syncup)] をクリックし、ノードがPANと同期されるまで待ちます。Cisco ISE-PIC管理者ポータルへのアクセスは、このプロセスが完了するのを待たなければなりません。

## スタンドアロンおよび2ノード展開での失われたノードの復元

この項では、スタンドアロンおよび2ノード展開での失われたノードの復元に使用できるトラブルシューティング情報を提供します。次の使用例の一部では、失われたデータの復旧にバックアップと復元機能を使用し、その他の使用例では、複製機能を使用しています。

### 2ノード展開での既存IPアドレスとホスト名を使用しての失われたノードの復元

#### シナリオ

2ノード展開では、自然災害が全ノードの損失につながります。復元後に、既存IPアドレスとホスト名を使用します。

たとえば、2つのノード、N1（プライマリポリシー管理ノードすなわちプライマリPAN）とN2（セカンダリポリシー管理ノードすなわちセカンダリPAN）があります。時刻T1に取得されたN1ノードのバックアップが利用可能です。自然災害のために、N1とN2両方のノードに障害が発生しました。

#### 前提

展開内のすべてのCisco ISE-PICノードが破壊されました同じホスト名とIPアドレスを使用して、新しいハードウェアのイメージが作成されました。

#### 解決手順

1. N1およびN2ノードの両方を置き換える必要があります。N1およびN2ノードはスタンドアロン構成になりました。
2. N1とN2のノードのUDIを使用してライセンスを取得し、N1ノードにインストールします。

3. 置き換えた N1 ノードでバックアップを復元する必要があります。復元スクリプトは N2 にデータを同期しようとしませんが、N2 はスタンドアロン ノードであるため同期は失敗します。N1 のデータは時刻 T1 にリセットされます。
4. N1 の管理者ポータルにログインして、N2 ノードを削除して再登録する必要があります。これで、N1 および N2 ノードのデータが時刻 T1 にリセットされます。

## 2 ノード展開の新 IP アドレスとホスト名を使用しての失われたノードの復元

### シナリオ

2 ノード展開では、自然災害が全ノードの損失につながります。新しいハードウェアのイメージが新しい場所で再作成され、新しい IP アドレスとホスト名が必要です。

たとえば、2 つの ISE-PIC、ノード N1（プライマリポリシー管理ノード（プライマリ PAN））と N2（セカンダリ ノード）があるとします。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。Cisco ISE-PIC ノードが新しいロケーションで置き換えられ、新しいホスト名は N1A（プライマリ PAN）および N2A（セカンダリ ノード）です。N1A および N2A はこの時点ではスタンドアロン ノードです。

### 前提条件

展開内のすべての Cisco ISE-PIC ノードが破壊されました新しいハードウェアのイメージが、異なるホスト名と IP アドレスを使用して異なる場所で作成されました。

### 解決手順

1. N1 のバックアップを入手し、これを N1A 上で復元します。復元スクリプトは、ホスト名とドメイン名の変更を認識し、現在のホスト名に基づいて展開設定内のホスト名とドメイン名を更新します。
2. 新しい自己署名証明書を生成する必要があります。
3. 古い N2 ノードを削除します。

新しい N2A ノードをセカンダリ ノードとして登録します。N1A ノードのデータが N2A ノードに複製されます。

## スタンドアロン展開の既存 IP アドレスとホスト名によるノードの復元

### シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。N1 データベースのバックアップは、時刻 T1 に取得されました。物理的な障害により N1 ノードがダウンし、イメージの再作成または新しいハードウェアが必要です。N1 ノードを、同じ IP アドレスとホスト名を使用して回復させる必要があります。

### 前提条件

この展開はスタンドアロン展開であり、新規またはイメージを再作成したハードウェアは、同じ IP アドレスとホスト名を持ちます。

### 解決手順

イメージの再作成後、または同一 IP アドレスとホスト名で新しい Cisco ISE-PIC ノードを導入した後に N1 ノードが起動したら、古い N1 ノードから取得したバックアップを復元する必要があります。ロールを変更する必要はありません。

## スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元

### シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。時刻 T1 に取得された N1 データベースのバックアップが利用可能です。物理的な障害により N1 ノードがダウンし、異なる IP アドレスとホスト名を使用した新しいハードウェアに別のロケーションで置き換えられます。

### 前提条件

これはスタンドアロン展開であり、置き換えられたハードウェアは、異なる IP アドレスとホスト名を持ちます。

### 解決手順

1. 新しいハードウェアで N1 ノードを置き換えます。このノードはスタンドアロン状態となり、ホスト名は N1B です。
2. バックアップを N1B ノード上で復元できます。ロールを変更する必要はありません。

## 設定のロールバック

### 問題

意図せずに設定を変更してしまい、後でそれが正しくないことがわかる場合があります。この場合、変更を行う前に取得したバックアップを復元することにより、元の構成に戻すことができます。

### 考えられる原因

N1（プライマリポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリポリシー管理ノードすなわちセカンダリ PAN）の 2 つのノードがあり、N1 ノードのバックアップを使用できます。N1 上で誤った変更をいくつか行い、変更を元に戻す必要があります。

### ソリューション

誤った設定変更を行う前に取得したN1ノードのバックアップを入手します。N1ノード上でこのバックアップを復元します。復元スクリプトにより、N1のデータでN2が同期されます。

## 2 ノード展開での障害発生時のプライマリノードの復元

### シナリオ

マルチノード展開内で、PANに障害が発生しました。

たとえば、2つのCisco ISE-PICノード、N1（PAN）とN2（セカンダリ管理ノード）があります。ハードウェアの問題でN1に障害が発生します。

### 前提条件

2ノード展開内のプライマリノードのみに障害が発生します。

### 解決手順

1. N2管理者ポータルにログインします。Cisco ISE GUIで[メニュー (Menu)]アイコン (☰) をクリックして、 を選択して、N2をプライマリノードとして設定します。

N1ノードが新しいハードウェアで置き換えられ、イメージが再作成され、スタンドアロン状態となります。

2. N2管理者ポータルで、セカンダリノードとして新しいN1ノードを登録します。

これで、N2ノードがプライマリノードになり、N1ノードがセカンダリノードになります。

N1ノードを再びプライマリノードにするには、N1の管理者ポータルにログインして、このノードをプライマリノードに設定します。N2は、自動的にセカンダリサーバーとなります。データが失われることはありません。

## 2 ノード展開での障害発生時のセカンダリノードの復元

### シナリオ

マルチノード展開で、1台のセカンダリノードに障害が発生しました。復元の必要はありません。

### 解決手順

1. セカンダリノードのイメージを再作成して、デフォルトのスタンドアロン状態にします。
2. プライマリノードから管理者ポータルにログインし、セカンダリノードを削除します。
3. セカンダリノードを再登録します。

データはプライマリノードからセカンダリノードに複製されます。復元の必要はありません。

## データベースの消去

消去プロセスでは、消去時にデータを保持する月数を指定することで、データベースのサイズを管理できます。デフォルトは3ヵ月間です。この値は、消去用のディスク容量使用率しきい値（合計ディスク容量の80%）に達したときに使用されます。このオプションでは、各月は30日で構成されます。デフォルトの3ヵ月は90日間です。

### データベースの消去に関するガイドライン

次に、データベースのディスク使用に関連して従うべきガイドラインをいくつか示します。

- データベースのディスク使用量がしきい値設定の80%（すなわち合計ディスク容量の60%）を超えた場合、データベースサイズが割り当てられたディスクサイズの最大値を超過しそうであることを示すクリティカルアラームが生成されます。ディスク使用量がしきい値設定の90%（すなわち合計ディスク容量の70%）を超えた場合、データベースサイズが割り当てられたディスクサイズの最大値を超過したことを示す、別のクリティカルアラームが生成されます。
- 消去は、データベースの使用済みディスク領域のパーセンテージにも基づきます。データベースの使用済みディスク容量がしきい値（デフォルトは合計ディスク容量の80%）以上になると、消去プロセスが開始されます。このプロセスは、管理者ポータルの設定に関係なく、最も古い7日間のモニターリングデータのみを削除します。ディスク領域が80%未満になるまで繰り返しプロセスを続行します。消去では、処理の前にデータベースのディスク領域制限が常にチェックされます。

### 運用データの消去

Cisco ISE モニターリング運用データベースには、Cisco ISE レポートとして生成された情報が含まれています。最近のCisco ISEのリリースには、モニターリング運用データを消去し、Cisco ISEの管理者 **application configure ise** を実行した後にモニターリングデータベースをリセットするためのオプションが備わっています。CLI コマンドを入力します。

ページオプションは、データのクリーンアップに使用します。また、保持する日数を尋ねるプロンプトを表示します。リセットオプションを使用すると、データベースが工場出荷時の初期状態にリセットされるため、バックアップされているすべてのデータが完全に削除されます。ファイルがファイルシステム領域を過度に消費している場合、データベースを指定することができます。



- (注) リセットオプションを使用すると、再起動するまでは Cisco ISE サービスが一時的に利用できなくなります。

### 関連トピック

[古い運用データの消去](#) (30 ページ)

## 古い運用データの消去

運用データはサーバーに一定期間集められています。すぐに削除することも、定期的に削除することもできます。[**データ消去の監査 (Data Purging Audit)**] レポートを表示して、データ消去が成功したかどうかを確認できます。

**ステップ 1** [管理 (Administration)] > [メンテナンス (Maintenance)] > [運用データの消去 (Operational Data Purging)] を選択します。

**ステップ 2** 次のいずれかを実行します。

- [データ保持期間 (Data Retention Period)] エリアで次の操作を行います。
  1. RADIUS または TACACS データを保持する期間を日単位で指定します。指定した期間より前のデータはすべてリポジトリにエクスポートされます。ISE-PIC には RADIUS または TACACS 機能がありませんが、インフラストラクチャの一部が Cisco ISE と共有されます。このため、データベースからこのような情報を定期的に消去する必要があります。
  2. [リポジトリ (Repository)] エリアで、[リポジトリのエクスポートを有効にする (Enable Export Repository)] チェックボックスをオンにし、データを保存するリポジトリを選択します。
  3. [暗号キー (Encryption Key)] フィールドに必要なパスワードを入力します。
  4. [保存 (Save)] をクリックします。

(注) 設定した保持期間が診断データに対応する既存の保持しきい値未満の場合、設定値は既存のしきい値を上書きします。たとえば、保持期間を 3 日に設定し、この値が診断テーブルの既存のしきい値 (たとえば、5 日のデフォルト) 未満の場合、データはこのウィンドウで設定した値 (3 日) に従って消去されます。
- [データを今すぐ消去 (Purge Data Now)] エリアで、次の操作を行います。
  1. すべてのデータを消去するか、または指定された日数よりも古いデータを消去します。データはリポジトリに保存されません。
  2. [消去 (Purge)] をクリックします。

## 完全な ISE インストールへの ISE-PIC のアップグレード

Cisco ISE-PIC は、完全な Cisco ISE GUI に基づくシンプルで直感的な GUI に表示されます。このため、ISE-PIC をインストールすると、ISE へ迅速かつ効率的にアップグレードできます。ISE-PIC から ISE の Essential ライセンスにアップグレードすると、ISE では引き続き、アップグレード前に ISE-PIC で使用可能だった機能がすべて提供されます。アップグレードした ISE-PIC ノードをプライマリ PAN として使用している場合は、すでに設定している設定値を設定し直す必要はありません。



- (注) アップグレードした既存の ISE-PIC ノードをプライマリ PAN として使用しない場合、アップグレード時にそのノードのデータは消去され、新しく追加したノードから、既存の完全な ISE 展開のデータにアクセスできるようになります。

ISE へのアップグレードの利点の詳細については、[ISE および CDA と ISE-PIC の比較](#)を参照してください。

## ライセンスの登録による ISE へのアップグレード

### 始める前に

ISE-PIC ノードは、Essential ライセンスを有効にすることで Cisco ISE ノードにアップグレードできます。Essential ライセンスを有効にする前に、ISE-PIC ノードで ISE-PIC と ISE-PIC のアップグレードライセンスの両方を購入して有効にする必要があります。Essentials ライセンスは、CSSM でライセンスを登録すると、[ライセンス (Licenses)] テーブルに表示されます。アプリケーションサービスはアップグレード中に再起動されます。

ライセンスモデルの詳細については、次を参照してください。 [ISE-PIC スマートライセンス](#)

- ステップ 1** セカンダリノードがインストールされている場合は、Cisco ISE-PIC のプライマリノードのインストールから、[管理 (Administration)] > [展開 (Deployment)] を選択し、セカンダリノードの登録を解除します。次に、両方のノードがプライマリノードになり、いずれかをアップグレードできます。
- ステップ 2** [管理 (Administration)] > [ライセンス (Licensing)] を選択します。
- ステップ 3** [ライセンスのインポート (Import License)] をクリックします。
- ステップ 4** [ファイルの選択 (Choose File)] をクリックし、アップグレードライセンス ファイルを参照して、[OK] をクリックします。
- ステップ 5** (注) この ISE-PIC ノードを既存の ISE 展開に追加する場合は、この手順を完了するとアップグレードが完了し、その展開のプライマリノードからノードを登録できるようになります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。  
<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html>
- [新しいライセンスファイルのインポート (Import New License File)] 画面で、[インポート (Import)] をクリックします。
- ステップ 6** このアップグレードされたノードを完全な ISE 展開のプライマリノードにするには、この時点で Essential ライセンスをインポートします。[ライセンスのインポート (Import License)] をもう一度クリックします。
- ステップ 7** [ファイルの選択 (Choose File)] をクリックし、シスコの担当者から受け取ったライセンスを参照して、[OK] をクリックします。
- ステップ 8** [新しいライセンスファイルのインポート (Import New License File)] 画面で、[インポート (Import)] をクリックします。

**ステップ 9** [OK] をクリックします。

ISE のプライマリノードにするアップグレードが開始され、「このノードはバックグラウンドで ISE にアップグレード中です。数分待ってから、ISE にログインしてください (*This node is now being upgraded to ISE in the background. Please wait several minutes and then log in to ISE.*) 」というメッセージが表示されます。

**ステップ 10** [OK] をクリックします。

数分後にログイン画面が表示されます。再度ログインし、Essential ライセンスのインストールで提供されるすべてのメニューにアクセスします。

アップグレードしたプライマリ ISE-PIC ノードが完全な ISE インストールのプライマリノードになり、以前のセカンダリノードがプライマリであり、ISE-PIC のスタンドアロンインストールの唯一のノードになります。これで、同じ方法で最後の ISE-PIC ノードを個別にアップグレードできるようになりました。

## での設定の管理 ISE-PIC

### ロールベース アクセス コントロール

Cisco ISE-PIC では、管理者に対して特定のシステム動作の権限を許可または拒否するロールベースアクセスコントロール (RBAC) ポリシーを定義することができます。これらの RBAC ポリシーは、個々の管理者の ID、または管理者が属する管理者グループの ID に基づいて定義されます。

さらにセキュリティを強化し、管理者ポータルにアクセスできる者を制御するために、次を実行します。

- リモートクライアントの IP アドレスに基づいて管理アクセスを設定します。
- 管理アカウントの強力なパスワードポリシーを定義します。
- 管理 GUI セッションのセッションタイムアウトを設定します。

### Cisco ISE-PIC 管理者

管理者は、次の目的で管理者ポータルを使用できます。

- 展開ノードのモニターリングとトラブルシューティングの管理。
- Cisco ISE-PIC のサービス管理者アカウント、およびシステム設定と操作の管理。
- 管理者パスワードおよびユーザーパスワードを変更します。

CLI 管理者は Cisco ISE アプリケーションの開始と停止、ソフトウェアパッチとアップグレードの適用、Cisco ISE アプライアンスのリロードとシャットダウン、およびすべてのシステムログとアプリケーションログの表示を行うことができます。CLI 管理者には特別な権限が付与



されているため、CLI 管理者クレデンシャルを保護し、Cisco ISE 展開を設定および管理する Web ベースの管理者を作成することが推奨されます。

セットアップ時に設定したユーザー名とパスワードは、CLI への管理アクセスにのみ使用されます。このロールは、CLI 管理ユーザー (CLI 管理者) と見なされます。デフォルトでは、CLI 管理ユーザーのユーザー名は `admin`、パスワードはセットアップで定義したパスワードです。デフォルトのパスワードはありません。この CLI 管理ユーザーはデフォルトの `admin` ユーザーであり、このユーザーアカウントは削除できません。ただし、他の管理者は編集することが可能で、これには対応するアカウントのパスワードを有効化、無効化、または変更するオプションが含まれています。

管理者を作成するか、または既存のユーザーを管理者ロールに昇格できます。管理者は、対応する管理者権限を無効にすることで、単純なネットワーク ユーザー ステータスに降格することもできます。

管理者は、Cisco ISE-PIC システムを設定および操作するローカル権限を持つユーザーです。

管理者は、1 つ以上の管理者グループに割り当てられます。利便性のため、これらの管理者グループはシステムで事前に定義されています。これについては、次の項で説明します。



- (注) Cisco ISE リリース 2.7 以降では、Cisco ISE でユーザーアカウントを作成するときに英数字の値を使用します。

#### 関連トピック

[Cisco ISE-PIC 管理者グループ \(33 ページ\)](#)

## Cisco ISE-PIC 管理者グループ

管理者グループは、Cisco ISE-PIC のロールベース アクセス コントロール (RBAC) グループです。同じグループに属するすべての管理者は、共通の ID を共有し、同じ権限を持ちます。特定の管理者グループのメンバーとしての管理者の ID は、許可ポリシーの条件として使用できます。管理者は、複数の管理者グループに属することができます。

どのアクセスレベルの管理者アカウントでも、管理者がアクセスできるすべてのウィンドウの、権限を持つオブジェクトを変更または削除できます。

次の表に、Cisco ISE-PIC で事前定義された管理者グループ、およびこれらのグループのメンバーが実行できるタスクを示します。これらの事前定義グループは、システムで管理者ユーザーを定義するにのみ使用できます。

表 2: Cisco ISE 管理者グループ、アクセス レベル、権限、および制約事項

管理者グループロール	アクセス レベル	権限	制約事項
スーパー管理者	すべての Cisco ISE-PIC 管理機能。デフォルトの管理者アカウントは、このグループに属します。	すべての Cisco ISE-PIC リソースに対する作成、読み取り、更新、削除、および実行 (CRUDX) 権限。	
外部 RESTful サービス (ERS) 管理者	GET、POST、DELETE、PUT など、すべての ERS API 要求へのフル アクセス	<ul style="list-style-type: none"> <li>ERS API 要求の作成、読み取り、更新、および削除</li> </ul>	ロールは、内部ユーザー、ID グループ、およびエンドポイントをサポートする ERS 許可のみを対象としています

## CLI 管理者と Web ベースの管理者の権限の比較

CLI 管理者は Cisco ISE-PIC アプリケーションの開始と停止、ソフトウェアパッチとアップグレードの適用、Cisco ISE-PIC アプライアンスのリロードとシャットダウン、およびすべてのシステムログとアプリケーションログの表示を行うことができます。CLI 管理者には特別な権限が付与されているため、CLI 管理者クレデンシャルを保護し、Cisco ISE-PIC の展開を設定および管理する Web ベースの管理者を作成することが推奨されます。

## 新しい管理者の作成

Cisco ISE-PIC 管理者は、特定の管理タスクを実行するために、特定のロールが割り当てられたアカウントが必要です。複数の管理者アカウントを作成して、管理者が実行する必要がある管理タスクに基づいて 1 つ以上のロールを割り当てることができます。

[管理者ユーザー (Admin Users)] ウィンドウを使用して、Cisco ISE-PIC 管理者の属性の表示、作成、変更、削除、ステータスの変更、複製、または検索を実行します。



(注) 管理者ユーザーのドメインが CLI と GUI の両方で同じである場合は、CLI で Active Directory アクセスを設定してから GUI に参加することをお勧めします。それ以外の場合は、そのドメインへの認証の失敗を回避するために、GUI からドメインに再参加する必要があります。

ステップ 1 [管理 (Administration)] > [管理者アクセス (Admin Access)] > [管理者ユーザー (Admin Users)] > [追加 (Add)] > [管理者ユーザーの作成 (Create an Admin User)] を選択します。

ステップ 2 フィールドに値を入力します。[名前 (Name)] フィールドでサポートされる文字は次のとおりです: # \$ ' ( ) \* + - . / @ \_。

管理者ユーザー名は一意にする必要があります。既存のユーザー名を入力した場合は、次のメッセージがエラー ポップアップ ウィンドウに表示されます。

User can't be created. A User with that name already exists.

**ステップ 3** [送信 (Submit) ] をクリックして、新しい管理者を Cisco ISE-PIC 内部データベースに作成します。

#### 関連トピック

[読み取り専用管理ポリシー](#)

[読み取り専用管理者のメニューアクセスのカスタマイズ](#)

## Cisco ISE-PIC への管理アクセス

Cisco ISE-PIC 管理者は、自分が属する管理者グループに基づいてさまざまな管理タスクを実行できます。これらの管理タスクは重要です。ネットワーク内の Cisco ISE-PIC の管理が許可されているユーザーにのみ、管理アクセス権を付与します。



- (注) Cisco ISE サーバーがネットワークに追加されると、その Web インターフェイスが起動した後に実行状態になるとマークされます。ただし、ポスチャサービスなどの一部のアドバンスト サービスが使用可能になるまでに時間がかかる場合があるため、すべてのサービスが完全に動作するまでに時間がかかることがあります。

#### 管理アクセスの方法

Cisco ISE サーバーには、いくつかの方法で接続することができます。ポリシー管理ノード (PAN) は、管理者ポータルを実行します。ログインするには管理者パスワードが必要です。他の ISE ペルソナサーバーには、CLI を実行する SSH またはコンソールを通じてアクセスできます。ここでは、各接続タイプで利用可能なプロセスとパスワードのオプションについて説明します。

- [管理者パスワード (Admin password) ]: インストール時に作成した Cisco ISE 管理者ユーザーのタイムアウトは、デフォルトで 45 日間です。[管理 (Administration) ] > [システム (System) ] > [管理者設定 (Admin Settings) ] からパスワードの有効期間をオフにすると、これを回避できます。[パスワードポリシー (Password Policy) ] タブをクリックし、[パスワードライフタイム (Password Lifetime) ] で [管理パスワードの有効期限 (Administrative passwords expire) ] チェックボックスをオフにします。

この操作を行わないと、パスワードの有効期限が切れます。管理者パスワードは CLI で **application reset-passwd** コマンドを実行してリセットできます。CLI にアクセスするコンソールに接続するか、またはブートオプションメニューにアクセスする ISE イメージファイルを再起動することにより、管理者パスワードをリセットできます。

- [CLI パスワード (CLI password) ]: CLI パスワードはインストール時に指定する必要があります。無効なパスワードが原因で CLI へのログインに問題がある場合は、CLI パスワードをリセットできます。コンソールに接続し、**password CLI** コマンドを実行して、パス

ワードをリセットします。詳細については、『[Cisco Identity Services Engine CLI リファレンスガイド](#)』を参照してください。

## 管理者アクセスの設定

Cisco ISE-PIC では、セキュリティ強化のために管理者アカウントにルールを定義できます。管理インターフェイスへのアクセスを制限したり、強力なパスワードの使用やパスワードの定期的な変更を管理者に強制することができます。Cisco ISE-PIC の [管理者アカウントの設定 (Administrator Account Settings)] で定義するパスワードポリシーは、すべての管理者アカウントに適用されます。

Cisco ISE-PIC では、管理者パスワードに UTF-8 文字は使用できません。

### 同時管理セッションとログインバナーの最大数の設定

同時管理 GUI または CLI (SSH) セッションの最大数、および管理 Web または CLI インターフェイスにアクセスする管理者を手助け、ガイドするログインバナーを設定できます。管理者のログイン前後に表示されるログインバナーを設定できます。デフォルトでは、これらのログインバナーは無効になっています。ただし、個々の管理者アカウントの同時セッションの最大数を設定することはできません。

- 
- ステップ 1 [管理 (Administration)] > [管理者アクセス (Admin Access)] > [アクセス設定 (Access Settings)] > [セッション (Session)] を選択します。
  - ステップ 2 GUI および CLI インターフェイスを介した同時管理セッションの、許可する最大数を入力します。同時管理 GUI セッションの有効範囲は 1 ~ 20 です。同時管理 CLI セッションの有効範囲は 1 ~ 10 です。
  - ステップ 3 Cisco ISE-PIC で管理者がログインする前にメッセージを表示する場合は、[プリログインバナー (Pre-login banner)] チェックボックスをオンにして、テキストボックスにメッセージを入力します。
  - ステップ 4 Cisco ISE-PIC で管理者がログインした後にメッセージを表示する場合は、[ポストログインバナー (Post-login banner)] チェックボックスをオンにして、テキストボックスにメッセージを入力します。
  - ステップ 5 [保存 (Save)] をクリックします。
- 

### IP アドレスの選択からの Cisco ISE-PIC への管理アクセスの許可

Cisco ISE-PIC では、管理者が Cisco ISE-PIC 管理インターフェイスにアクセスできる IP アドレスのリストを設定することができます。

- 
- ステップ 1 [管理 (Administration)] > [管理者アクセス (Admin Access)] > [アクセス設定 (Access Settings)] > [IP アクセス (IP Access)] を選択します。
  - ステップ 2 [リストされている IP アドレスのみに接続を許可する (Allow only listed IP addresses to connect)] オプションボタンをクリックします。

(注) 管理アクセスにはポート161 (SNMP) の接続を使用します。ただし、IPアクセス制限が設定されている場合は、実行元のノードで管理アクセスが設定されていないと snmpwalk が失敗します。

**ステップ3** [アクセス制限のIPリストの設定 (Configure IP List for Access Restriction)] 領域で、[追加 (Add)] をクリックします。

**ステップ4** [IP CIDR の追加 (Add IP CIDR)] ダイアログボックスで、[IP アドレス (IP Address)] フィールドに IP アドレスをクラスレスドメイン間ルーティング (CIDR) 形式で入力します。

(注) このIPアドレスは、IPv4またはIPv6アドレスにすることができます。ISE ノードに複数のIPv6アドレスを設定できます。

**ステップ5** [CIDR 形式のネットマスク (Netmask in CIDR format)] フィールドにサブネットマスクを入力します。

**ステップ6** [OK] をクリックします。ステップ4～7を繰り返して、他のIPアドレス範囲をこのリストに追加します。

**ステップ7** [保存 (Save)] をクリックして、変更内容を保存します。

**ステップ8** [IP アクセス (IP Access)] ウィンドウを更新するには、[リセット (Reset)] をクリックします。

---

## 管理者アカウントのパスワードポリシーの設定

Cisco ISE-PIC では、セキュリティ向上のために管理者アカウントにパスワードポリシーを作成することもできます。ここで定義したパスワードポリシーは、Cisco ISE-PIC 内のすべての管理者アカウントに適用されます。



- (注)
- 内部管理者ユーザーの電子メール通知は root@host に送信されます。電子メールアドレスは設定できません。多くの SMTP サーバーがこの電子メールを拒否します。  
未解決の不具合 CSCui5583 を確認できます。これは、電子メールアドレスの変更を許可する拡張機能です。
  - Cisco ISE-PIC では、管理者パスワードに UTF-8 文字は使用できません。

---

**ステップ1** [管理 (Administration)] > [管理者アクセス (Admin Access)] > [認証 (Authentication)] を選択します。

**ステップ2** [パスワードポリシー (Password Policy)] タブをクリックし、Cisco ISE の GUI と CLI のパスワード要件を設定するために必要な値を入力します。

**ステップ3** [保存 (Save)] をクリックして、管理者パスワードポリシーを保存します。

(注) 外部IDストアを使用してログイン時に管理者を認証する場合は、管理者プロファイルに適用されるパスワードポリシーにこの設定値が設定されている場合でも、外部IDストアが依然として管理者のユーザー名とパスワードを認証することに注意してください。

## 管理者アカウントのアカウント無効化ポリシーの設定

Cisco ISE-PIC では、設定した連続日数の間に管理者アカウントが認証されなかった場合は、管理者アカウントを無効にすることができます。

---

**ステップ 1** [管理 (Administration)] > [管理者アクセス (Admin Access)] > [認証 (Authentication)] > [アカウント無効化ポリシー (Account Disable Policy)] を選択します。

**ステップ 2** [非アクティブになってから  $n$  日後にアカウントを無効にする (Disable account after  $n$  days of inactivity)] チェックボックスをオンにして、対応するフィールドに日数を入力します。

このオプションでは、管理者アカウントが指定した日数の間非アクティブだった場合に管理者アカウントを無効にすることができます。

管理者アカウントを無効にして後で有効にすると、24 時間以上アクティブのままになりません。管理者アカウントを無効にしてもアクティブなままにしたい場合は、[ $n$  日間の非アクティブ後にアカウントを無効にする (Disable account after  $n$  days of inactivity)] チェックボックスをオフのままにします。

**ステップ 3** [保存 (Save)] をクリックして、管理者のグローバルアカウント無効化ポリシーを設定します。

---

## 管理者のセッションタイムアウトの設定

Cisco ISE-PIC を使用すると、管理 GUI セッションが非アクティブであっても依然として接続状態である時間を決定できます。分単位の時間を指定することができ、その時間が経過すると Cisco ISE-PIC は管理者をログアウトします。セッションのタイムアウト後、管理者は、Cisco ISE-PIC 管理者ポータルにアクセスするには再びログインする必要があります。

---

**ステップ 1** [管理 (Administration)] > [管理者アクセス (Admin Access)] > [セッションの設定 (Session Settings)] > [セッションタイムアウト (Session Timeout)] を選択します。

**ステップ 2** アクティビティがない場合に管理者をログアウトするまでに Cisco ISE-PIC が待機する時間 (分) を入力します。デフォルト値は 60 分です。有効な範囲は 6 ~ 100 分です。

**ステップ 3** [保存 (Save)] をクリックします。

---

## アクティブな管理セッションの終了

Cisco ISE-PIC では、すべてのアクティブな管理セッションが表示され、そこからセッションを選択し、必要が生じた場合はいつでも終了できます。同時管理 GUI セッションの最大数は 20 です。GUI セッションの最大数に達した場合、スーパー管理者グループに属する管理者がログインして一部のセッションを終了できます。

---

**ステップ 1** [管理 (Administration)] > [管理者アクセス (Admin Access)] > [セッションの設定 (Session Settings)] > [セッション情報 (Session Info)] を選択します。

**ステップ2** 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化 (Invalidate)] をクリックします。

## 管理ポータルで使用されるポート

管理ポータルは、HTTP ポート 80 と HTTPS ポート 443 を使用します。ユーザーはこれらの設定を変更できません。管理ポータルのリスクを軽減するために、これらのポートを使用するようにエンドユーザーポータルを設定することはできません。

## 通知をサポートするための SMTP サーバーの設定

アラーム前に実行するアクションを受信したりできるようにするには、Simple Mail Transfer Protocol (SMTP) サーバーを設定します。

電子メールを送信する ISE ノード

次のリストは、電子メールを送信する分散 ISE 環境のノードを示しています。

電子メールの目的	電子メールを送信するノード
ゲストの有効期限	プライマリ PAN
アラーム	アクティブな MnT
ゲストとスポンサーのポータルからのスポンサーとゲストの通知	PSN
パスワードの有効期限	プライマリ PAN

**ステップ1** [設定 (Settings)] > [SMTP サーバー (SMTP Server)] を選択します。

**ステップ2** [SMTPサーバー (SMTP Server)] フィールドにアウトバウンド SMTP サーバーのホスト名を入力します。この SMTP ホストサーバーは Cisco ISE-PIC サーバーからアクセス可能である必要があります。このフィールドの最大長は 60 文字です。

**ステップ3** [保存 (Save)] をクリックします。

アラーム通知の受信者は、[電子メールにシステムアラームを含む (Include system alarms in emails)] オプションが有効になっている内部管理者ユーザーです。アラーム通知を送信する送信者の電子メールアドレスは、ise@<hostname> としてハードコードされています。

## GUI からの外部 RESTful サービス API の有効化 : ERS 設定

### 始める前に

Cisco ISE REST API 用に開発されたアプリケーションから Cisco ISE にアクセスできるようにするには、Cisco ISE REST API をイネーブルにする必要があります。Cisco REST API は HTTPS ポート 9060 を使用します。このポートはデフォルトでは閉じられています。Cisco ISE REST API が Cisco ISE 管理用サーバーでイネーブルになっていない場合、クライアントアプリケーションは、サーバーから Guest REST API 要求に対するタイムアウト エラーを受信します。

すべてのタイプの外部 RESTful サービス要求はプライマリ ISE ノードに限り有効です。セカンダリ ノードは読み取りアクセス (GET 要求) に対応します。

---

**ステップ 1** [設定 (Settings)] > [ERS設定 (ERS Settings)] を選択します。

**ステップ 2** [読み取り/書き込み用に ERS を有効化 (Enable ERS for Read/Write)] を選択し、[保存 (Save)] をクリックします。

---

### 次のタスク

API コールと ISE-PIC の詳細については、『[ISE API Reference Guide](#)』を参照してください。

## セキュリティ設定の構成

セキュリティ設定を構成するには、次の手順を実行します。

---

**ステップ 1** [設定 (Settings)] > [セキュリティ設定 (Security Settings)] を選択します。

**ステップ 2** [セキュリティ設定 (Security Settings)] ウィンドウで、次の必須オプションを選択します。

1. TLS 1.0を許可 (Allow TLS 1.0) : 次のワークフローについて、従来のピアとの通信に TLS 1.0 を許可します。
  - Cisco ISE は、EAP サーバーとして設定されます
  - Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
  - Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます
  - Cisco ISE は、セキュアな LDAP クライアントとして設定されます
  - Cisco ISE は ERS サーバーとして設定されます

また、次の ISE コンポーネントとの通信用に TLS 1.0 を許可します。

- すべてのポータル
- 認証局



- MDM クライアント
- pxGrid
- PassiveID エージェント

(注) セキュリティを強化するために、TLS の上位バージョンを使用するようにクライアントとサーバーでネゴシエートすることをお勧めします。

2. TLS 1.1を許可 (Allow TLS 1.1) : 次のワークフローについて、従来のピアとの通信に TLS 1.1 を許可します。

- Cisco ISE は、EAP サーバーとして設定されます
- Cisco ISE は、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードします
- Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます
- Cisco ISE は、セキュアな LDAP クライアントとして設定されます
- Cisco ISE は ERS サーバーとして設定されます

また、次の ISE コンポーネントとの通信用に TLS 1.1 を許可します。

- Admin UI
- すべてのポータル
- 認証局
- 外部 RESTful サービス (ERS)
- MDM クライアント
- pxGrid

(注) セキュリティを強化するために、TLS の上位バージョンを使用するようにクライアントとサーバーでネゴシエートすることをお勧めします。

**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。