ISE-PIC スタートアップ ガイド

インストールとライセンスの登録が完了したら、ISE-PICのスムーズな運用を確保するために、次の重要な手順を含む展開のセットアップと設定が完了していることを確認します。

（注） Cisco ISE-PIC のインストール、アップグレード、および設定の詳細とサポートについては、『*Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Upgrade Guide, Release 2.4*』を参照してください。

管理者アクセス コンソール

次の手順では、管理ポータルにログインする方法について説明します。

始める前に

Cisco ISE-PIC が正しくインストール（またはアップグレード）および設定されていることを確認します。Cisco ISE-PIC のインストール、アップグレード、および設定の詳細とサポートについては、『*Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Upgrade Guide*』を参照してください。

ステップ 1 Cisco ISE-PIC URL をブラウザのアドレス バーに入力します（たとえば https://<ise hostname or ip address>/admin/）。

ステップ 2 ユーザ名と、Cisco ISE の初期セットアップで指定して設定した大文字と小文字が区別されるパスワードを入力します。

ステップ 3 [ログイン（Login）] をクリックするか、Enter を押します。

ログインに失敗した場合は、[ログイン（Login）]ページの[ログインで問題が発生する場合（Problem logging in?）] リンクをクリックして、手順に従ってください。

管理者ログイン ブラウザのサポート

Cisco ISE 管理者ポータルは次の HTTPS 対応ブラウザをサポートしています。

- Mozilla Firefox 72 以前のバージョン
- Mozilla Firefox ESR 60.9 以前のバージョン
- Google Chrome 80 以前のバージョン
- Microsoft Internet Explorer 10.*x* および 11.*x*

  Internet Explorer 10.x を使用する場合は、TLS 1.1 と TLS 1.2 を有効にし、SSL 3.0 と TLS 1.0 を無効にします（[インターネットオプション（Internet Options）] > [詳細設定（Advanced）]）。

ISE コミュニティ リソース

ISE Pages Fail to Fully Load When Adblock Plus is Used

ログインの試行に失敗した後の管理者のロックアウト

管理者ユーザ ID に対して誤ったパスワードを何度も入力すると、アカウントは指定された時間一時停止されるか、またはロックアウトされます（設定による）。ロックアウトすることを選択した場合は、管理者ポータルによってシステムの「ロックアウト」が表示されます。Cisco ISE は、サーバ管理者ログイン レポートにログ エントリを追加し、その管理者 ID のクレデンシャルを一時停止します。その管理者 ID のパスワードをリセットするには、『Cisco Identity Services Engine Installation Guide』の「Reset a Disabled Password Due to Administrator Lockout」のセクションでの説明に従います。管理者アカウントが無効になるまでに失敗できる回数は設定可能です。詳細は、『*Cisco Identity Services Engine Administrator Guide*』の「Cisco ISE-PIC への管理アクセス」のセクションを参照してください。管理者ユーザアカウントがロックアウトされると、そのように設定されている場合、Cisco ISE からその管理者ユーザに電子メールが送信されます。

Diffie-Hellman アルゴリズムを使用した SSH キー交換の保護

Diffie-Hellman-Group14-SHA1 SSH キー交換しか許可しないように Cisco ISE-PIC を設定することができます。このためには、Cisco ISE-PIC コマンドライン インターフェイス（CLI）のコンフィギュレーション モードから次のコマンドを入力します。

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

次に例を示します。

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

初期セットアップと設定

Cisco ISE-PICをすぐに使用できるようにするには、次のフローに従います。

1. ライセンスをインストールして登録します。詳細については、Cisco ISE-PIC ライセンス （3 ページ）を参照してください。
2. DNS サーバを適切に設定していることを確認します。これには、ISE-PIC からのクライアント マシンの逆引きの設定も含まれます。詳細については、DNS サーバ （6 ページ）を参照してください。
3. NTP サーバのクロック設定を同期します。
4. ISE-PIC セットアップで、最初のプロバイダーを設定します。詳細については、PassiveID セットアップの使用を開始するを参照してください。
5. 1 つまたは複数のサブスクライバを設定します。詳細については、サブスクライバを参照してください。

最初のプロバイダーとサブスクライバのセットアップ後は、追加のプロバイダーを容易に作成でき（を参照プロバイダー）、ISE-PICで異なるプロバイダーからパッシブ ID を管理します（ISE-PIC でのサービスのモニタリングとトラブルシューティングを参照）。

Cisco ISE-PIC ライセンス

Cisco ISE-PIC は 90 日間の評価期間で提供されます。90 日間のライセンス評価期限が切れた後も Cisco ISE-PIC を使用し続けるには、ライセンスを取得してシステムに登録する必要があります。ISE-PIC からライセンス評価期限の 90 日前、60 日前、および 30 日前に通知があります。

各永久ライセンスは単一の ISE-PIC ノードにアップロードされ、環境内に 2 つのノードがある場合、2 つ目のノードには別途ライセンスが必要です。インストールが完了したら、UDI ごとに個別のライセンスを作成し、ライセンスを各ノードにそれぞれ追加します。

ライセンスのインストールと登録フロー

1. ISE-PIC のライセンスをインストールして登録します。ISE-PIC ライセンスのインストールと登録の詳細については、ライセンスの登録 （5 ページ）を参照してください。次のいずれかのタイミングでライセンスをインストールできます。
   - ISE-PIC のインストール直後
   - 90 日間の評価期間中いつでも

2. 基本の ISE 環境を簡単にアップグレードするには、Cisco ISE-PIC アップグレード ライセンスを最初にインストールし、次を実行します。
   - 以前の ISE-PIC ノードを環境のプライマリ管理ノード（PAN）として使用するために Base ISE ライセンスをインストールする。
   - アップグレードした PIC ISE-PIC ノードを既存の ISE 環境に追加する。

3. 基本の ISE 環境をアップグレードし、スマート ライセンスにアップグレードするには、他の関連ライセンス（Plus、Apex、TACACs+ など）をインストールします。ISE ライセンスのインストールの詳細については、『*Cisco Identity Services Engine Administrator Guide*』を参照してください。

Cisco ISE ライセンス パッケージ

表 *1:* すべての *Cisco ISE* ライセンス パッケージ オプション

ISE ライセンス パッケージ	永続/サブスクリプション（使用可能期間）	カバーされる ISE 機能	注記
ISE-PIC	永続	パッシブ ID サービス	ノードごとに 1 つのライセンス。各ライセンスでは、最大 3,000 の並列セッションをサポートしています。
ISE-PIC upgrade	永続	このライセンスでは、次のオプションを使用できます。 • 追加の並列セッションの有効化（300,000 まで） • 完全な ISE インスタンスへのアップグレード	ノードごとに 1 つのライセンス。各ライセンスでは、最大 300,000 の並列セッションをサポートしています。 このライセンスをインストールすると、アップグレードされたノードが既存の ISE 展開に参加できるようになります。あるいは、Base ライセンスをノードにインストールし、このノードを PAN として機能させることができます。

Base	永続	• 基本的なネットワーク アクセス：AAA、IEEE-802.1X • ゲスト サービス • リンク暗号化（MACSec） • TrustSec • ISEアプリケーション プログラミング インターフェイス	
Evaluation	一時（90 日）	すべての ISE-PIC の機能は 90 日間有効です。	

ライセンスの登録

始める前に

ISE-PIC のインストール後、90 日間の評価期間があります。作業をスムーズに続けるには、ISE-PIC ライセンスの購入、登録、インストールが必要です。期限の前に登録およびインストールしない場合、期限後にISE-PICにアクセスすると、すべてのISE-PICサービスが無効になり、自動的に[ライセンスのインポート（Import License）]に移動し、そこからプロセスを実行できます。ISE-PIC のライセンスについては、シスコ パートナー/アカウント チームにお問い合わせください。

ステップ 1 シスコの Web サイト（www.cisco.com）の注文システム（Cisco Commerce Workspace（CCW））から、必要なライセンスを注文します。環境内のノードごとに 1 つの ISE-PIC ライセンスが必要です（各環境につき最大 2 つのノード）。

約 1 時間後、製品認証キー（PAK）を含む電子メール確認が送信されます。

ステップ 2 Cisco ISE-PIC の管理ポータルから、ライセンシング ダッシュボード（**[管理（Administration）]** > **[ライセンシング（Licensing）]**）を選択します。[ライセンスの詳細（Licensing Details）]セクションのノード情報（製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN））を書き留めます。

ステップ 3 www.cisco.com/go/licensing に移動し、要求されたら、受け取ったライセンスの PAK、ノード情報、および会社に関する詳細を入力します。

1 日後に、シスコからライセンス ファイルが送信されます。

ステップ 4 システムの既知の場所にこのライセンス ファイルを保存します。

ステップ 5 Cisco ISE-PIC の管理ポータルから、**[管理（Administration）]** > **[ライセンシング（Licensing）]** を選択します。

ステップ 6 [ライセンス（Licenses）] セクションで、[ライセンスのインポート（Import License）] ボタンをクリックします。

ステップ 7 [Choose File（ファイルの選択）] をクリックし、システムで以前に保存したライセンス ファイルを選択します。

ステップ 8 [インポート（Import）] をクリックします。

新しいライセンスがシステムにインストールされました。

次のタスク

ライセンシング ダッシュボード（**[管理（Administration）]**>**[ライセンシング（Licensing）]**）を選択し、新たに入力したライセンスが正しい詳細とともに表示されることを確認します。

ライセンスの削除

始める前に

期限切れのライセンスや不要なライセンスを削除するとポップアップリマインダが表示されなくなり、ライセンスダッシュボードの領域が再利用されます。

ステップ 1 **[管理（Administration）]** > **[ライセンシング（Licensing）]** を選択します。

ステップ 2 [ライセンス ファイル（License Files）] セクションで、関連するファイル名の隣にあるチェックボックスをクリックし、[ライセンスの削除（Delete License）] をクリックします。

ステップ 3 [OK] をクリックします。

DNS サーバ

DNS サーバを設定する場合は、次の処理を実行します。

- Cisco ISE に設定されている DNS サーバで、使用するドメインのすべての正引きおよび逆引き DNS クエリを解決できるようにする必要があります。
- DNS 再帰によって遅延が発生してパフォーマンスが重大な悪影響を受ける可能性があるので、権威 DNS サーバで Active Directory レコードを解決することをお勧めします。
- すべての DNS サーバで、追加サイト情報の有無に関係なく、DC、GC、および KDC の SRV クエリに回答できるようにする必要があります。
- パフォーマンスを向上させるために、SRV 応答にサーバ IP アドレスを追加することを推奨します。
- パブリック インターネットでクエリを実行する DNS サーバを使用しないでください。不明な名前を解決する必要がある場合に、ネットワークの情報が漏洩する可能性があります。

システム時刻と NTP サーバ設定の指定

Cisco ISE-PIC では、Network Time Protocol（NTP）サーバを 3 台まで設定することができます。NTP サーバを使用すると、正確な時刻を維持でき、複数のタイムゾーンの間で時刻を同期できます。また、認証済みの NTP サーバのみを Cisco ISE-PIC で使用するかどうかを指定することもでき、そのための認証キーを入力できます。

シスコは、すべての Cisco ISE-PIC ノードを協定世界時（UTC）の時間帯に設定することを推奨します。この手順では、展開内にあるさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。

Cisco ISE は、NTP サーバの公開キー認証もサポートしています。NTPv4 は、対称キー暗号化を使用し、公開キー暗号化に基づく新しい Autokey 方式も提供します。公開キー暗号化は、一般に、各サーバによって生成され公開されない非公開の値に基づいているため、対称キー暗号化よりも安全であると考えられます。Autokey では、すべてのキー配布および管理機能には公開値のみが含まれているため、キーの配布と保管が大幅に簡素化されます。

コンフィギュレーション モードで Cisco ISE CLI から NTP サーバに Autokey を設定できます。IFF（identify Friend または Foe）識別方式は最も広く使用されている方式なので、この方式を使用することを推奨します。

ステップ 1 **[設定（Settings）]** > **[システム時刻（System Time）]** を選択します。

ステップ 2 NTP サーバに一意の IP アドレス（IPv4/IPv6/FQDN）を入力します。

ステップ 3 システムおよびネットワーク時間の維持に認証済みの NTP サーバだけを使用するように Cisco ISE を制限する場合は、[認証済みの NTP サーバのみ可能（Only allow authenticated NTP servers）] チェックボックスをオンにします。

ステップ 4 （オプション）秘密キーを使用して NTP サーバを認証する場合に、指定したサーバのいずれかが認証キーによる認証を必要とする場合は、[NTP 認証キー（NTP Authentication Keys）] タブをクリックし、1 つ以上の認証キーを次のように指定します。

a) [追加（Add）] をクリックします。

b) 必要な [キー ID（Key ID）] と [キー値（Key Value）] を入力します。 [信頼できるキー（Trusted Key）] オプションをアクティブにするか、または非アクティブにすることによって、そのキーが信頼できるかどうかを指定し、[OK] をクリックします。[キー ID（Key ID）] フィールドは 1 ～ 65535 の数値をサポートし、[キー値（Key Value）] フィールドは最大 15 文字の英数字をサポートします。

c) NTP サーバの認証キーの入力が終了したら、[NTP サーバ設定（NTP Server Configuration）] タブに戻ります。

ステップ 5 （オプション）公開キー認証を使用して NTP サーバを認証する場合は、コマンドラインインターフェイス（CLI）から Cisco ISE で Autokey を設定します。詳細については、ご使用のリリースの ISE の『Cisco Identity Services Engine CLI Reference Guide』で **ntp server** および **crypto** コマンドを参照してください。

ステップ 6 [保存（Save）] をクリックします。

ISE-PICホーム ダッシュボード

Cisco ISE-PICホーム ダッシュボードには、効果的なモニタリングおよびトラブルシューティングに必要不可欠な、統合され、関連付けられた概要と統計データが表示されます。ダッシュボードはリアルタイムに更新されます。特に指定がない限り、ダッシュレットには過去 24 時間のアクティビティが表示されます。

[ホーム（Home）] ページには、 ISE-PICホーム データのビューを表示する 2 つのデフォルト ダッシュボードがあります。

- [メイン（Main）] : このビューには、線形の [メトリクス（Metrics）] ダッシュボード、チャート ダッシュレット、およびリスト ダッシュレットが表示されます。ISE-PICでは、ダッシュレットは設定できません。一部のダッシュレットは無効になっています。これらのダッシュレットはISEのフルバージョンでのみ使用できます。たとえば、エンドポイントデータを表示するダッシュレットなどです。使用可能なダッシュレットには次のものがあります。
  - [パッシブ ID メトリック（Passive Identity Metrics）] : [パッシブ ID メトリック（Passive Identity Metrics）] では、現在追跡中の固有のライブ セッションの総数、システムに設定されている ID プロバイダーの総数、ID データをアクティブに配信しているエージェントの総数、および現在設定されているサブスクライバの総数の概要が示されます。
  - [プロバイダー（Providers）] : プロバイダーはユーザ ID 情報を ISE-PICに渡します。ISE-PIC プローブ(特定のソースからデータを収集するメカニズム）を設定します。プローブを介してプロバイダー ソースからの情報を受信します。たとえば、Active Directory（AD）プローブとエージェント プローブはいずれも ISE-PIC による AD からのデータ収集を支援しますが、syslog プローブは、syslog メッセージを読み取るパーサーからデータを収集します。
  - [サブスクライバ（Subscribers）] : サブスクライバは ISE-PIC に接続し、ユーザ ID 情報を取得します。
  - [OS タイプ（OS Types）] : 表示できる唯一の OS タイプは Windows です。Windows のタイプが Windows バージョン別に表示されます。プロバイダーは OS タイプを報告しませんが、ISE-PIC はこの情報を取得するため Active Directory を照会できます。ダッシュレットに表示できるエントリの最大数は 1000 です。この数を超えるエンドポイントがある場合、または Windows 以外の OS タイプを表示する場合には、ISE にアップグレードできます。
  - [アラーム（Alarms）] : ユーザ ID 関連アラーム。
- [その他（Additional）] : PIC のアクティブ セッションと、PIC システムのシステム概要を表示します。