ISE-PIC スタートアップ ガイド

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 ユーザー名と、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）] ウィンドウの [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、表示される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 102 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 91.3 以前のバージョン

- Google Chrome 103 以前のバージョン（バージョン 86 以降）
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

ISE コミュニティ リソース

ISE Pages Fail to Fully Load When Adblock Plus is Used

Diffie-Hellman アルゴリズムを使用したセキュアな SSH キー交換

Diffie-Hellman-Group14-SHA1 Secure Shell（SSH） キー交換のみを許可するように Cisco ISE-PIC を設定すします。Cisco ISE-PIC の CLI 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、ISE-PIC スマートライセンス （3 ページ） を参照してください。
2. DNS サーバーを適切に設定していることを確認します。これには、Cisco 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 サーバー （7 ページ） を参照してください。
3. NTP サーバー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。

最初のプロバイダとサブスクライバの設定が完了したら、追加のプロバイダを容易に作成できます（プロバイダを参照）。また ISE-PICで異なるプロバイダのパッシブ ID を管理できます（ISE-PIC でのサービスのモニターリングとトラブルシューティングを参照）

ISE-PIC スマートライセンス

ISE-PIC 3.1 以上のライセンスは、Cisco Smart Software Manager（CSSM）と呼ばれる集中型データベースを介して完全に管理されます。単一のトークン登録で、すべてのライセンスを簡単かつ効率的に登録、アクティブ化、および管理できます。

ISE-PIC 3.1 以上ではスマートライセンスのみをサポートし、従来のライセンスはサポートしません。従来の ISE-PIC ライセンスを所有している場合は、ライセンスをスマートライセンスに変換して、ISE-PIC 3.1 以上でのライセンスコンプライアンスを有効にする必要があります。

評価ライセンスは、ISE-PIC を初めてインストールしたときにデフォルトで有効になります。評価ライセンスは、すべての ISE-PIC 機能にアクセスできる 90 日間のライセンスです。評価期間中、ライセンス コンプライアンス ステータスは CSSM に報告されません。

ISE-PIC 管理ポータルの右上隅に、評価モードの残り日数を示すメッセージが表示されます。必要な ISE-PIC 機能を引き続き使用するには、必要なライセンスを購入してアクティブ化する必要があります。

スマートライセンストークンがアクティブで、ISE-PIC 管理ポータルに登録されている場合、CSSM は ISE-PIC ノードのライセンス コンプライアンス ステータスをモニターします。ライセンス コンプライアンス ステータスは、ISE-PIC の [ライセンス（Licenses）] テーブルに表示されます。この情報を表示するには、[管理（Administration）] > [システム（System）] > [ライセンス（Licensing）] を選択します。

ISE-PIC を CSSM に登録してから、ISE-PIC は 6 時間ごとにライセンス コンプライアンス ステータスを CSSM サーバーに報告します。ISE-PIC は、CSSM 証明書のローカルコピーを保存することで、CSSM サーバーと通信します。CSSM 証明書は、日常の同期中と [ライセンス（Licenses）]テーブルの更新時に自動的に再認証されます。通常、CSSM証明書の有効期間は 6 ヵ月です。

登録証明書は自動的に6ヵ月ごとに更新されます。スマートライセンスの登録証明書を手動で更新するには、[ライセンス（Licensing）] ウィンドウの上部にある [登録の更新（Renew Registration）] をクリックします。

ISE-PIC が CSSM サーバーと同期したときにコンプライアンスステータスに変更があった場合、[ライセンス（Licenses）] テーブルの [最後の認証（Last Authorization）] 列が変更内容に応じて更新されます。また、権限がコンプライアンスを満たさなくなった場合には、コンプライアンス違反となっている日数が [コンプライアンス違反の日数（Days Out of Compliance）] 列に表示されます。

次の場合は、ライセンス契約を更新する必要があります。

- 評価期間が終了し、まだライセンスを登録していない。
- ライセンスの有効期限が切れている。

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。Cisco ISE ライセンスの詳細については、『*Cisco Identity Services Engine* 管理者ガイド』を参照してください。

ISE-PIC 3.1 以上は VM 共通ライセンスをサポートしています。このライセンスは、3.1 より前のリリースでサポートされていた小規模 VM、中規模 VM、および大規模 VM ライセンスに代わるものです。この VM ライセンスは、オンプレミス展開とクラウド展開の両方の VM ノードを対象としています。レガシー VM ライセンスがある場合は、Cisco ISE 3.1 以上にアップグレードするときに、VM ライセンスを VM 共通ライセンスに移行する必要があります。レガシーライセンスを新しいライセンスタイプに変換するには、http://cs.co/scmswl で Support Case Manager を通じてオンラインでケースを開くか、http://cs.co/TAC-worldwide に記載されている連絡先情報を使用します。

ライセンス登録の成功または失敗、コンプライアンス違反のライセンス、評価ライセンスの有効期限切れ、スマートライセンス通信の失敗など、ライセンスステータスに関するアラームは [アラーム（Alarms）] ダッシュレットに表示されます。

ISE-PIC ライセンスパッケージ

ISE-PIC には、次のライセンスパッケージが用意されています。

ライセンスパッケージ	サブスクリプション	カバーされる機能	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 アップグレード	永久	• 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。

Essential	期間ベースのライセンス	• RADIUS 認証、許可、およびアカウンティング（802.1X、MAC 認証バイパス、Easy Connect、Web 認証を含む） • MACsec • シングルサインオン（SSO）、セキュリティアサーション マークアップ言語（SAML）、およびオープン データベース コネクティビティ（ODBC）標準に基づく認証 • ゲストアクセスとスポンサーサービス • モニタリング目的の Representational State Transfer（REST）API、および CRUD 操作用の外部 RESTful サービス API • パッシブ ID サービス • セキュアな有線およびワイヤレスアクセス	—
Evaluation	一時（90 日）	すべての ISE-PIC 機能を 90 日間有効化	—

スマートライセンスの登録とアクティブ化

始める前に

- 従来の ISE-PIC ライセンスを所有している場合は、ライセンスをスマートライセンスに変換する必要があります。
- 登録トークンを受信するには、新しいスマートライセンスタイプを CSSM に登録します。

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）] > [システム（System）] > [ライセンス（Licensing）]** を選択します。

ステップ 2 [登録の詳細（Registration Details）] をクリックします

ステップ 3 [登録の詳細（Registration Details）] 領域に、CSSM から [登録トークン（Registration Token）] フィールドで受信した登録トークンを入力します。

ステップ 4 [接続方式（Connection Method）] ドロップダウンリストから接続方式を選択します。

- [直接HTTPS（Direct HTTPS）]：インターネットへの直接接続を設定している場合にこのオプションを選択します。
- [HTTPSプロキシ（HTTPS Proxy）]：インターネットへの直接接続がなく、プロキシサーバーを使用する必要がある場合にこのオプションを選択します。スマートライセンスの登録後にプロキシサーバーの構成を変更した場合は、[ライセンス（Licensing）] ウィンドウでスマートライセンスの構成を更新する必要があります。ISE-PIC は、更新されたプロキシサーバーを使用して CSSM との接続を確立し、ISE-PIC サービスの中断を回避します。
- [トランスポートゲートウェイ（Transport Gateway）]：推奨される接続方式です。トランスポートゲートウェイを設定している場合、この接続がデフォルトで選択されます。別の接続方法を選択するには、トランスポートゲートウェイの設定を削除する必要があります。
- [SSMオンプレミスサーバー（SSM On-Prem Server）]：設定済みの SSM オンプレミスサーバーに接続する場合にこのオプションを選択します。

ステップ 5 [階層（Tier）] 領域と [仮想アプライアンス（Virtual Appliance）] 領域で、有効にする必要があるすべてのライセンスのチェックボックスをオンにします。選択したライセンスがアクティブ化され、その遵守状況が CSSM によって追跡されます。

ステップ 6 [登録（Register）] をクリックします。

ライセンストークンを登録すると、CSSMアカウントに特定の権限が含まれず、登録時にそれらを無効にしていなかった場合は、非準拠通知が ISE-PIC に表示されます。これらの利用資格を CSSM アカウントに追加し、[ライセンス（Licenses）] テーブルで [更新（Refresh）] をクリックして、非準拠通知を削除します。

ISE-PIC 登録をスマートアカウントから削除する一方で、評価期間の終了までスマートライセンスを引き続き使用するには、[Ciscoスマートライセンス（Cisco Smart Licensing）] 領域の上部にある [登録解除（Deregister）] をクリックします。まだ評価期間の残りの時間があれば、ISE-PIC はスマートライセンスのままです。評価期間の終了間近である場合は、ブラウザを更新したときに通知が表示されます。スマートライセンスの登録を解除したら、同一または別の UDI で登録するために登録プロセスを再度実行できます。

特定ライセンス予約

特定ライセンス予約は、組織のセキュリティ要件で ISE-PIC と CSSM 間の永続的な接続が許可されていない場合にスマートライセンスを管理するためのスマートライセンス方式です。特定ライセンス予約では、ISE-PIC ノードで特定のソフトウェア利用資格を予約できます。

予約する必要があるライセンスのタイプと数を定義して特定ライセンス予約を作成し、ISE-PIC ノードで予約をアクティブにします。登録して予約を有効にした ISE-PIC ノードは、ライセンスの使用を追跡し、ライセンス消費の遵守を適用します。

（注） 特定ライセンス予約を使用している場合、ISE-PIC ノードを Cisco ISE ノードにアップグレードすることはできません。アップグレードするには、まず特定ライセンス予約を返却し、スマートライセンス登録を有効にしてから、ISE-PIC アップグレードおよび Essential ライセンスをインストールする必要があります。

DNS サーバー

DNS サーバーを設定する場合は、次の処理を実行します。

- Cisco ISE に設定されている DNS サーバーで、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 サーバーで 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 サーバーで、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 応答にサーバー 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 サーバー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。

システム時刻とネットワーク タイム プロトコル サーバー設定の指定

Cisco ISE-PIC では、NTP サーバーを 3 台まで設定することができます。正確な時刻を維持し、異なるタイムゾーンの間で時刻を同期するために NTP サーバーを使用します。また、Cisco ISE-PIC が認証済みの NTP サーバーのみを使用する必要があるかどうかを指定したり、そのために 1 つまたは複数の認証キーを入力することもできます。

すべての Cisco ISE-PIC ノードを協定世界時（UTC）のタイムゾーンに設定することを推奨します。この手順では、展開内の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るようにします。

Cisco ISE は、NTP サーバーの公開キー認証をサポートしています。NTP バージョン 4 は対称キー暗号化を使用します。また、公開キー暗号化に基づく新しい Autokey セキュリティモデルも提供します。公開キー暗号化は、対称キー暗号化よりも安全であると見なされています。これは、セキュリティが各サーバーによって生成され、公開されないプライベート値に基づいているためです。Autokey セキュリティモデルでは、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 の CLI から NTP サーバーに Autokey セキュリティ モデルを設定できます。敵味方識別（IFF）システムは最も広く採用されているシステムであるため、このシステムを使用することを推奨します。

ステップ 1 Cisco ISE の GUI で [メニュー（Menu）] アイコン（☰）をクリックし、**[設定（Settings）] > [システム時刻（System Time）]** を選択します。

ステップ 2 [NTPサーバーの設定（NTP Server Configuration）] 領域で、NTP サーバーの一意の IP アドレス（IPv4 または IPv6 または完全修飾ドメイン名（FQDN））を入力します。

ステップ 3 （オプション）秘密キーを使用して NTP サーバーを認証する場合に、指定したサーバーのいずれかが認証キーによる認証を必要としている場合は、[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指定します。次の手順を実行します。

a) [追加（Add）] をクリックします。

b) [キー ID（Key ID）] フィールドと [キー値（Key Value）] フィールドに必要な値を入力します。[HMAC] ドロップダウンリストから、必要なハッシュ メッセージ認証コード（HMAC）値を選択します。[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) [OK] をクリックします。

d) [NTP サーバーの設定（NTP Server Configuration）] タブに戻ります。

ステップ 4 （オプション）公開キー認証を使用して NTP サーバーを認証するには、CLI から Cisco ISE に Autokey セキュリティモデルを設定します。Cisco ISE のリリースについては、『Cisco Identity Services Engine CLI リファレンス』の **ntp server** コマンドと **crypto** コマンドを参照してください。

ステップ 5 [保存（Save）] をクリックします。

（注） 3 つ以上の NTP サーバーを使用すると、サーバーの 1 つに障害が発生した、または 2 つのサーバーが同期しない場合でも、ネットワーク全体での正確な時刻の同期を保証します。https://insights.sei.cmu.edu/blog/best-practices-for-ntp-services を参照してください。

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、効果的なモニター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。

- [メイン（Main）] 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含まれています。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）] 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が表示されます。
- [プロバイダ（Providers）] : プロバイダはユーザー ID 情報を ISE-PIC に提供します。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 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、ユーザー 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）] : ユーザー ID 関連のアラーム。

- [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。

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。