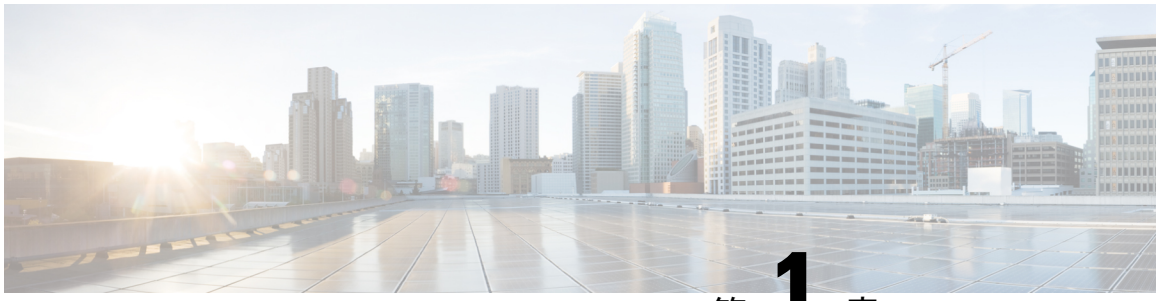
Cisco Identity Services Engine Passive Identity Connector リリース 2.7 管理者ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

ISE-PIC の概要

不正な脅威からネットワークを保護するには、ユーザーアイデンティティを認証する必要があります。これを行うために、セキュリティ製品がネットワークに実装されます。各セキュリティ製品には必要な認証を取得する独自の方法があり、多くの場合は、認証されたユーザーではなく、認証された IP アドレスを識別します。その結果、これらの製品は、ユーザーログイン情報に基づいて認証を実行するさまざまな外部サーバーと方式を参照し、分散型ネットワークを実現します。Cisco Identity Services Engine（ISE）の Passive Identity Connector（ISE-PIC）は、集中管理されたインストールと実装を提供し、さまざまな送信元からパッシブ認証データを簡単に収集し、それらのアイデンティティをセキュリティ製品のサブスクライバと共有できるようにします。

Cisco ISE-PIC の用語

このガイドでは、Cisco ISE-PIC について説明する際に次の用語を使用します。

用語	定義
GUI	グラフィック ユーザー インターフェイスGUI は、ISE-PIC のソフトウェアインストールのすべての画面とタブを示します。
NIC	ネットワーク インターフェイス カード。
ノード	個別の物理または仮想の Cisco ISE-PIC アプライアンス。

用語	定義
PAN	ISE-PIC 展開のメインノードはプライマリ管理ノード（PAN）であり、使用可能なすべてのアクションを実行できるノードです。ISE-PIC では、最大 2 つのノードをインストールできます。インストールする 2 番目のノードは、セカンダリ管理ノード（セカンダリ PAN）と呼ばれます。
パーサー	syslog メッセージを受信し、その入力を分割して管理、マッピング、および ISE-PIC にパブリッシュできる ISE-PIC のバックエンドコンポーネント。パーサーは、到着する syslog メッセージの各行の情報を調べて、重要な情報を探します。たとえば、「mac=」を検索するようにパーサーが設定されている場合、パーサーはそのフレーズを検索しながら各行を解析します。パーサーは、設定された主要なフレーズを検出すると、定義された情報を ISE に送信するように設定されています。
プライマリ ノード	ISE-PIC 展開のメインノードはプライマリ管理ノード（PAN）であり、使用可能なすべてのアクションを実行できるノードです。ISE-PIC では、最大 2 つのノードをインストールできます。インストールする 2 番目のノードは、セカンダリ管理ノード（セカンダリ PAN）と呼ばれます。
プローブ	プローブは特定の送信元からデータを収集するメカニズムです。プローブは任意のメカニズムを説明する一般的な用語ですが、データの収集方法や収集対象を具体的に説明するものではありません。たとえば、Active Directory（AD）のプローブは ISE-PIC が AD からデータを収集するのに役立ちますが、syslog のプローブは 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。
プロバイダー	ISE-PIC がユーザーアイデンティティ情報を受信し、マッピングし、公開するクライアントまたは送信元です。
セカンダリ ノード	ISE-PIC 展開のメインノードはプライマリ管理ノード（PAN）であり、使用可能なすべてのアクションを実行できるノードです。ISE-PIC では、最大 2 つのノードをインストールできます。インストールする 2 番目のノードは、セカンダリ管理ノード（セカンダリ PAN）と呼ばれます。
サブスクライバ	ユーザーアイデンティティ情報を受信するために ISE-PIC サービスをサブスクライブするシステム。

ISE-PIC 概要

パッシブ ID コネクタ（ISE-PIC）は一元的なワンストップ インストールおよび実装を提供します。これにより、ユーザー ID 情報を受信してさまざまなセキュリティ製品（Cisco Firepower Management Center（FMC）や Stealthwatch など）のサブスクライバと共有するように、ネットワークを容易に設定できます。パッシブ ID の完全なブローカとして、ISE-PIC はさまざまなプロバイダ ソース（Active Directory ドメイン コントローラ（AD DC）など）からユーザー ID を収集し、ユーザー ログイン情報を使用中の該当する IP アドレスにマッピングし、そのマッピング情報を、設定されているサブスクライバ セキュリティ製品と共有します。

パッシブ ID について

認証、許可、およびアカウンティング（AAA）サーバーを提供し、802.1X や Web 認証などのテクノロジーを使用する Cisco Identity Services Engine（ISE）などの製品は、ユーザーまたはエンドポイントと直接通信し、ネットワークへのアクセスを要求し、ログイン クレデンシャルを使用して ID を検証およびアクティブに認証します。

パッシブ ID サービスはユーザーを直接認証するのではなく、プロバイダと呼ばれる Active Directory などの外部認証サーバーからユーザー ID および IP アドレスを収集し、サブスクライバとこの情報を共有します。ISE-PICは、通常、ユーザーのログインとパスワードに基づいてプロバイダからユーザー ID 情報を受信し、ユーザー ID および関連する IP アドレスを照合するために必要な確認とサービスを実行し、認証済み IP アドレスをサブスクライバに提供します。

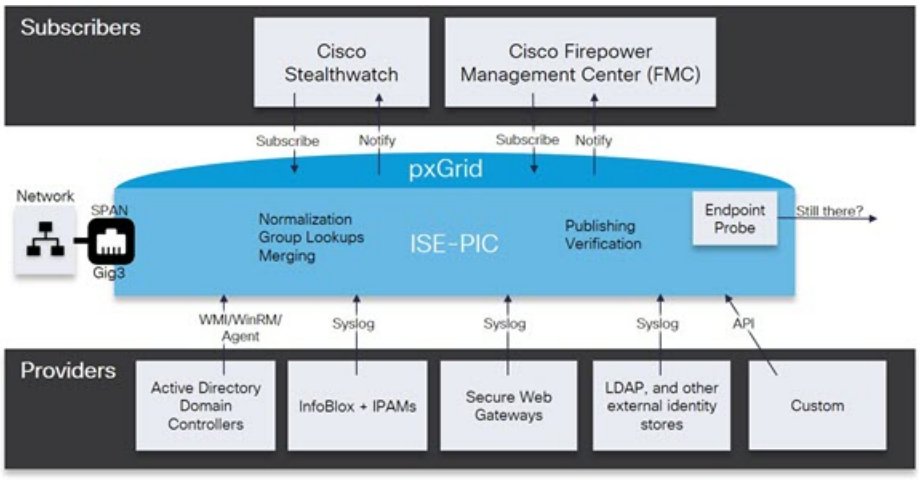
Passive Identity Connector（ISE-PIC）のフロー

ISE-PIC のフローは次のとおり。

1. プロバイダがユーザーまたはエンドポイントの認証を実行します。
2. プロバイダが認証済みのユーザー情報を ISE-PIC に送信します。
3. ISE-PIC によりユーザー情報の正規化、ルックアップ、マージ、解析、および IP アドレスへのマッピングが行われ、マッピングされた詳細情報が pxGrid に対して公開されます。
4. pxGrid サブスクライバはマッピングされたユーザーの詳細情報を受信します。

次の図に、ISE-PIC の全体的なフローを示します。

図 *1:* 全体的なフロー



Cisco ISE-PIC のアーキテクチャ、展開、およびノード

Cisco ISE-PIC アーキテクチャには、次のコンポーネントが含まれます。

- ノード：Cisco ISE-PIC では、次に示すように、最大 2 つのノードを設定できます。
- ネットワーク リソース
- エンドポイント

展開内の Cisco ISE-PIC ノードが 1 つの場合は「スタンドアロン展開」と呼ばれます。

Cisco ISE-PIC ノードを 2 つ含む展開は「ハイアベイラビリティ展開」と呼ばれ、1 つのノードがプライマリアプライアンス（プライマリ管理ノード、またはPAN）として機能します。ハイアベイラビリティ展開により、サービスの可用性が向上します。

PAN は、このネットワーク モデルに必要なすべての設定を提供し、セカンダリ Cisco ISE ノード（セカンダリ PAN）はバックアップロールで機能します。セカンダリノードはプライマリノードをサポートし、プライマリノードとの接続が失われるたびに機能を再開します。

Cisco ISE-PIC は、セカンダリノードがプライマリノードの状態と一致するように（したがって、バックアップとして使用できるように）、プライマリ Cisco ISE-PIC ノードが存在するコンテンツのすべてをセカンダリ ISE-PIC ノードと同期するか、複製します。

ISE Community Resource

展開とスケーリングの詳細については、「ISE Deployment Journey」を参照してください。

ISE-PIC の利点

ISE-PIC が提供するもの：

- さまざまなプロバイダーと連携する単一のアイデンティティ ソリューション。
- 設定、モニタリング、トラブルシューティングをシンプルにする使いやすい GUI
- シンプルなインストールと設定
- アクティブ認証用に ISE へ簡単にアップグレード。ISE-PIC から完全な ISE 展開へアップグレードし、ISE-PIC ノードを使用してスタンドアロン ISE 展開を作成するか、またはこのノードをプライマリノードとして既存の展開に追加すると、ISE はアップグレード前に ISE-PIC で使用可能だったすべての機能を引き続き提供し、既存の設定は保持されます。

（注） ISE にアップグレードするには、トライアルバージョンをダウンロードするか、またはライセンスのオプションについてシスコの担当者にお問い合わせください。

プライマリノードとしてではなく、既存の ISE 展開にアップグレードした ISE-PIC を追加すると、以前の ISE-PIC は上書きされます。

アップグレードフローの詳細については、完全な ISE インストールへの ISE-PIC のアップグレード （151 ページ）を参照してください。

ISE および CDA と ISE-PIC の比較

ISE-PIC には、ISE へのスムーズかつ容易なアップグレード機能などのさまざまな利点があります。ISE-PIC と ISE の他に、追加のセキュリティ メカニズムとして CDA が提供されています。3 つの製品の違いを次に示す表で説明します。

- ISE-PIC と ISE の詳細な比較 （5 ページ）
- ISE-PIC と ISE および CDA の比較の概要 （8 ページ）

ISE-PIC と ISE の詳細な比較

ISE-PIC はパッシブ ID だけを共有し、許可サービスまたは認証サービスは提供しません。これらのサービスは、認証、許可、およびアカウンティング（AAA）サーバーを提供する ISE により提供されます。2 つの製品の相違点について、次の表で詳しく説明します。

表 *1 : ISE-PIC* と *ISE* の比較

カテゴリ	機能	ISE-PIC	ISE
スマート ライセンス		—	√
認証タイプと許可タイプ	許可ポリシー	—	√
	TrustSec	—	√
	Active Directory パッシブ認証（WMI を含む）	√	√
パッシブ ID ソース		√	√
	Easy Connect	—	√
	SysLog ソース	√	√
	REST API ソース	√	√
	SPAN	√	√
	Security Group eXchange Protocol（SXP）	—	√
	RADIUS（RADIUS プロキシを含む）	—	√
	BYOD	—	√
	ゲスト	—	√
	ポスチャ（Posture）	—	√
	デバイス管理（TACACS+）	—	√
pxGrid	pxGrid コントローラ	√ Cisco サブスクライバ専用	√
	pxGrid コントローラ冗長性	√	√
	トピックの拡張性	—	√

カテゴリ	機能	ISE-PIC	ISE
証明局（CA）	pxGrid 証明書テンプレート	√	√
	エンドポイント CA	—	√
	Enrollment over secure transport（EST）	—	√
	その他の証明書テンプレート	—	√
可視性とコンテキスト	コンテキストディレクトリ	—	√
	プロファイリング	—	√

カテゴリ	機能	ISE-PIC	ISE
レポート		! （注） ISE-PIC に用意されているレポートを使用して、システムの正常性をモニターし、ネットワーク内の問題のトラブルシューティングを行うことができます。ただし、ISE と比較すると ISE-PIC では一部の機能だけが提供されるため、ISE-PIC. では一部の ISE レポートが使用できません。	√

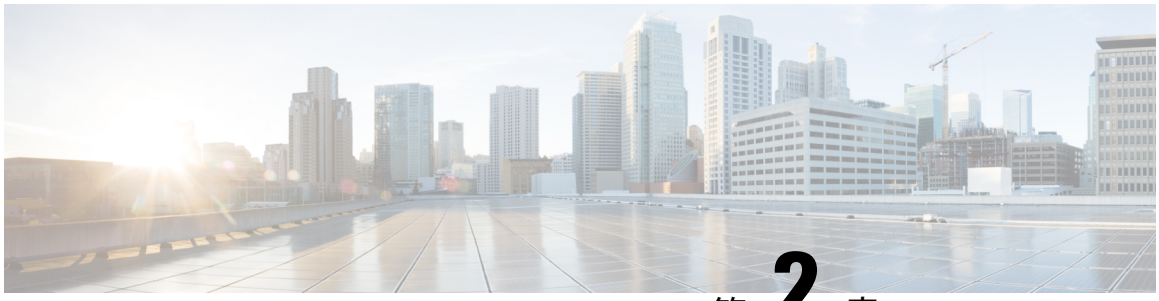
ISE-PIC と ISE および CDA の比較の概要

CDA は IP アドレスをユーザー名にマッピングするメカニズムです。CDA により、セキュリティ ゲートウェイはどのユーザーがネットワーク上のどの IP アドレスを使用しているかを認識でき、これらのユーザー（またはユーザーが属するグループ）に基づいて決定を下すことができます。ただし、ISE-PIC は、ユーザー名、MAC アドレス、ポートなどの追加データにアク

セスしてより正確にユーザー ID を収集します。次の表に ISE-PIC、ISE、および CDA の比較の概要を示します。

表 *2 : ISE* および *CDA* と *ISE-PIC* の比較

パッシブ認証の詳細	完全な ISE	ISE-PIC	CDA
ドメインコントローラの数	100	100	80
サブスクライバの数	20	20	—
WMI（エージェントレス）	対応	対応	対応
Windows サーバーエージェントが使用可能	対応	あり	—
DCOM が必要	いいえ（SPAN）	いいえ（SPAN）	あり
Easy Connect	あり	—	—
SPAN を使用した Kerberos スニフィング	対応	あり	—
バインド（IP アドレス、MAC アドレス、ユーザー名）	300,000	300,000	64,000



第 2 章

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

ログインの試行による管理者のロックアウト

管理者ユーザー 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）。ユーザーをロックアウトするように Cisco ISE が設定されている場合、管理ポータルによってシステムからロックアウトされます。Cisco ISE は、サーバー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 のログイン情報を一時停止します。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ログイン試行の回数は、『*Cisco Identity Services Engine Administrator Guide*』の「Cisco ISE-PIC への管理アクセス （156 ページ）」のセクションに記載されているとおりに設定されます。管理者ユーザーアカウントがロックアウトされると、関連付けられたユーザーに Cisco ISE から電子メールが送信されます（この情報が設定されている場合）。

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、Cisco ISE-PIC ライセンス （13 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 （16 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 （20 ページ）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 （79 ページ）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 （37 ページ）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 （163 ページ）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 （15 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 *3 :* 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、**[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

ステップ 4 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 5 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 6 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 7 [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 8 [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 9 [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 **[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。

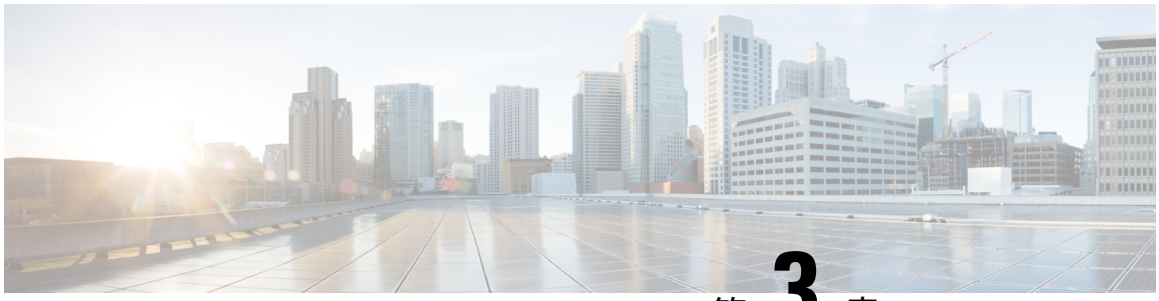
ステップ 5 [保存（Save）] をクリックします。

（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。



第 3 章

プローブおよびプロバイダとしての Active Directory

Active Directory（AD）は、ユーザー ID 情報（ユーザー名、IP アドレス、ドメイン名など）の取得元である安全性が高く正確なソースです。

AD プローブ（パッシブ ID サービス）は、WMI テクノロジーを使用して AD からユーザー ID 情報を収集しますが、その他のプローブはその他のテクノロジーや手法で AD をユーザー ID プロバイダとして使用します。ISE-PIC のその他のプローブとプロバイダ タイプの詳細については、プロバイダ （37 ページ）を参照してください。

Active Directory プローブを設定すると、次の（ソースとして Active Directory を使用する）その他のプローブも迅速に設定して有効にできます。

- Active Directory エージェント （40 ページ）

（注） Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

- SPAN （50 ページ）
- エンドポイント プローブ （77 ページ）

また、ユーザー情報の収集時に AD ユーザー グループを使用するために Active Directory プローブを設定します。AD、エージェント、SPAN、および syslog プローブで AD ユーザーグループを使用できます。AD グループの詳細については、Active Directory ユーザー グループの設定（25 ページ）を参照してください。

- Active Directory の使用 （19 ページ）
- Active Directory の設定 （32 ページ）

Active Directory の使用

パッシブ ID サービス 用の Active Directoryプローブを設定する前に、次のことを確認します。

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないこと。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないこと。
- 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、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 （16 ページ）を参照してください。
- NTP サーバーのクロック設定を同期します。詳細については、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 （16 ページ）を参照してください。

（注） Cisco ISE-PICが Active Directory に接続されているときに操作に関する問題がある場合は、[レポート（Reports）] の下にある [AD コネクタ操作レポート（AD Connector Operations Report）] を参照してください。詳細については、使用可能なレポート （167 ページ）を参照してください。

PassiveID セットアップの使用を開始する

ISE-PIC には、Active Directory からユーザー ID を受信するために、Active Directory を最初のユーザー ID プロバイダとして容易に設定できるウィザードがあります。ISE-PIC に Active Directory を設定することで、後でその他のプロバイダ タイプを設定するプロセスも簡素化されます。Active Directory を設定したら、ユーザーデータを受信するクライアントを定義するため、サブスクライバ（Cisco Firepower Management Center（FMC）や Stealthwatch など）を設定する必要があります。サブスクライバの詳細については、サブスクライバ （79 ページ） を参照してください。

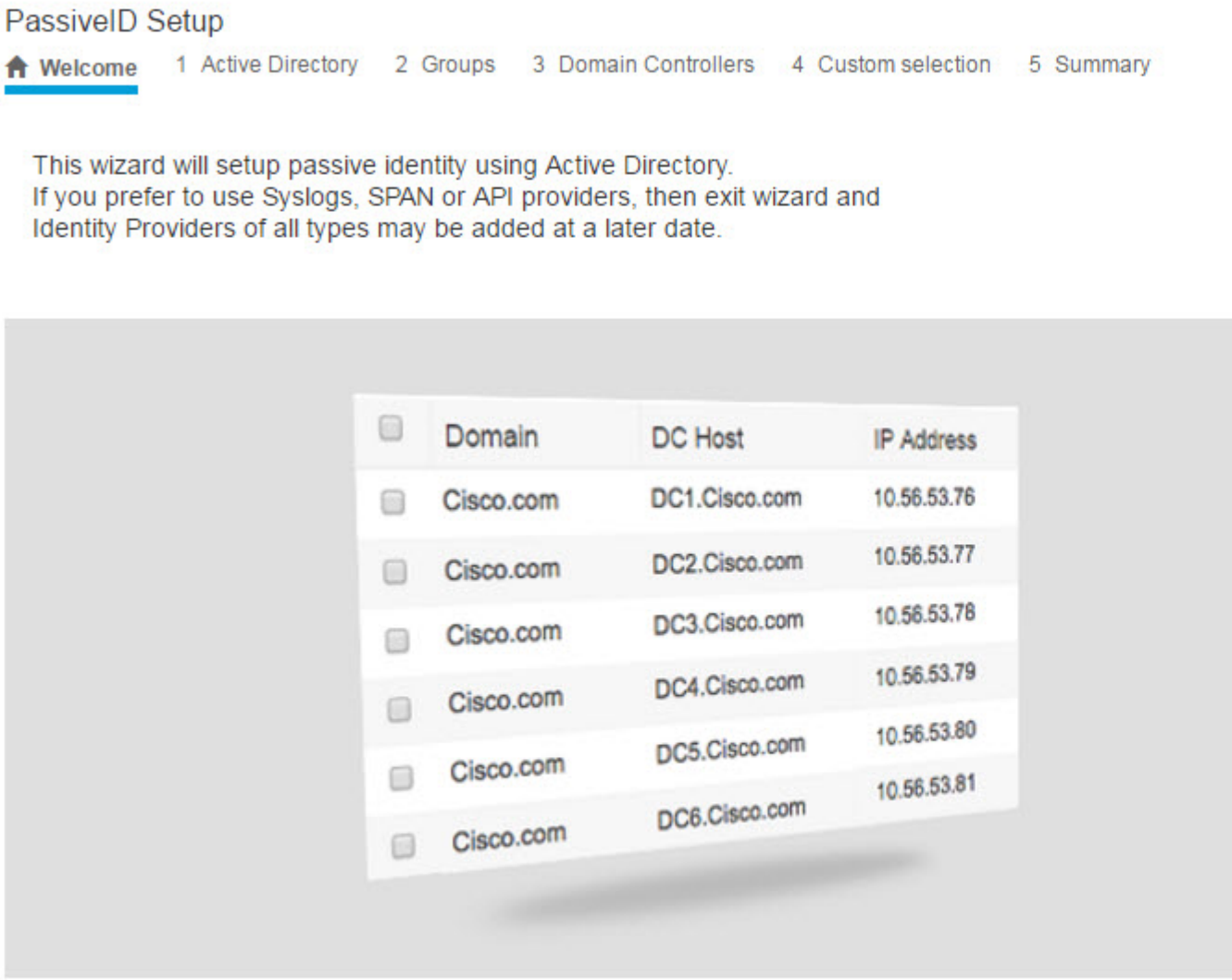
始める前に

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないことを確認します。
- 参加操作用の Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] を使用して設定されていないことを確認します。
- ISE-PIC のエントリがドメイン ネーム サーバー（DNS）にあることを確認します。ISE-PIC からのクライアントマシンの逆引き参照を適切に設定していることを確認します。詳細については、DNS サーバー （16 ページ）を参照してください。

ステップ 1 **[ホーム（Home）]** > **[概要（Introduction）]** を選択します。[パッシブ ID コネクタの概要（Passive Identity Connector Overview）] 画面で [パッシブ ID ウィザード（Passive Identity Wizard）] をクリックします。

[PassiveID セットアップ（PassiveID Setup）] が表示されます。

図 2 : [PassiveID セットアップ（PassiveID Setup）]



ステップ 2 [次へ（Next）] をクリックしてウィザードを開始します。

ステップ 3 この Active Directory の参加ポイントの一意の名前を入力します。このノードが接続されている Active Directory ドメインのドメイン名を入力し、Active Directory 管理者のユーザー名とパスワードを入力します。

管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。

ステップ 4 [次へ（Next）] をクリックし、Active Directory グループを定義し、追加してモニターするユーザー グループをすべてオンにします。

前のステップで設定した Active Directory 参加ポイントに基づいて Active Directory ユーザー グループが自動的に表示されます。

ステップ 5 [次へ（Next）] をクリックします。モニターする DC を選択します。[カスタム（Custom）] を選択した場合は、次の画面でモニターする特定の DC を選択します。完了したら、[次へ（Next）] をクリックします。

ステップ 6 [終了（Exit）] をクリックして、ウィザードを終了します。

次のタスク

最初のプロバイダとして Active Directory の設定を完了したら、追加のプロバイダ タイプも容易に設定できます。詳細については、プロバイダ （37 ページ）を参照してください。さらに、定義したいずれかのプロバイダが収集したユーザー ID 情報を受信するためのサブスクライバも設定できるようになりました。詳細については、サブスクライバ （79 ページ）を参照してください。

Active Directory（WMI）プローブの段階的なセットアップ

パッシブ ID サービス に Active Directory とWMI を設定するには、PassiveID セットアップの使用を開始する （20 ページ）を使用するか、この章の次の手順を実行します。

1. Active Directory プローブを設定します。Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE-PIC ノードの参加 （22 ページ）を参照してください。
2. AD ログイン イベントを受信する 1 つ以上の WMI 設定ノードの Active Directory ドメイン コントローラのリストを作成します。
3. Active Directory を ISE-PIC と統合するため Active Directory を設定します。
4. （オプション）Active Directory プロバイダの管理 （28 ページ）。

Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE-PIC ノードの参加

始める前に

Cisco ISE-PIC ノードが、NTP サーバー、DNS サーバー、ドメインコントローラ、グローバル カタログサーバーが配置されているネットワークと通信できることを確認します。

Active Directory と、エージェント、syslog、SPAN、およびエンドポイントの各プローブを使用するには、参加ポイントを作成する必要があります。

Active Directory と統合する際に IPv6 を使用する場合は、関連する ISE-PIC ノードで IPv6 アドレスが設定されていることを確認する必要があります。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 [追加（Add）] をクリックして、[Active Directory 参加ポイント名（Active Directory Join Point Name）] の設定のドメイン名と ID ストア名を入力します。

ステップ 3 [送信（Submit）] をクリックします。

新しく作成された参加ポイントをドメインに参加させるかどうかを確認するポップアップ ウィンドウが表示されます。すぐに参加させる場合は [はい（Yes）] をクリックします。

[いいえ（No）] をクリックした場合、設定を保存すると、Active Directory ドメインの設定がグローバルに保存されますが、いずれの Cisco ISE-PIC ノードもまだドメインに参加しません。

ステップ 4 作成した新しい Active Directory 参加ポイントの横にあるチェックボックスをオンにして [編集（Edit）] をクリックします。展開の参加/脱退テーブルに、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスが表示されます。

ステップ 5 参加ポイントがステップ 3 の間にドメインに参加しなかった場合は、関連する Cisco ISE-PIC ノードの横にあるチェックボックスをオンにし、[参加（Join）] をクリックして Active Directory ドメインに Cisco ISE-PIC ノードを参加させます。

設定を保存した場合も、これを明示的に実行する必要があります。1 回の操作で複数の Cisco ISE-PIC ノードをドメインに参加させるには、使用するアカウントのユーザー名とパスワードがすべての参加操作で同じである必要があります。各 Cisco ISE-PIC ノードを追加するために異なるユーザー名とパスワードが必要な場合は、Cisco ISE-PIC ノードごとに参加操作を個別に実行する必要があります。

ステップ 6 [ドメインへの参加（Join Domain）] ダイアログボックスで Active Directory のユーザー名とパスワードを入力します。

管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。

参加操作に使用するユーザーは、ドメイン自体に存在する必要があります。ユーザーが異なるドメインまたはサブドメインに存在する場合、ユーザー名は jdoe@acme.com のように、UPN 表記で表記する必要があります。

ステップ 7 （任意） [組織ユニットの指定（Specify Organizational Unit）] チェックボックスをオンにします。

このチェックボックスは、Cisco ISE-PIC ノードのマシンアカウントを CN=Computers,DC=someDomain,DC=someTLD 以外の特定の組織ユニットに配置する場合に、オンにする必要があります。Cisco ISE-PIC は、指定された組織ユニットの下にマシン アカウントを作成するか、またはマシン アカウントがすでにある場合は、この場所に移動します。組織ユニットが指定されない場合、Cisco ISE-PIC はデフォルトの場所を使用します。値は完全識別名（DN）形式で指定する必要があります。構文は、Microsoft のガイドラインに準拠する必要があります。特別な予約文字（/'+,;=<> など）、改行、スペース、およびキャリッジリターンは、バックスラッシュ（\）によってエスケープする必要があります。たとえば、OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ や Workstations,DC=someDomain,DC=someTLD のようにします。マシン アカウントがすでに作成されている場合、このチェックボックスをオンにする必要はありません。Active Directory ドメインに参加したマシン アカウントのロケーションを後で変更することもできます。

ステップ 8 [OK] をクリックします。

Active Directory ドメインに参加する複数のノードを選択できます。

参加操作に失敗した場合、失敗メッセージが表示されます。各ノードの失敗メッセージをクリックして、そのノードの詳細なログを表示します。

（注） 参加が完了すると、Cisco ISE-PIC によりその AD グループと対応するセキュリティ識別子（SID）が更新されます。Cisco ISE-PIC は自動的に SID の更新プロセスを開始します。このプロセスを完了できるようにする必要があります。

（注） DNS サービス（SRV）レコードが欠落している（参加しようとしているドメインに対し、ドメインコントローラが SRV レコードをアドバタイズしない）場合は、Active Directory ドメインに Cisco ISE-PIC を参加させることができない可能性があります。トラブルシューティング情報については、次の Microsoft Active Directory のマニュアルを参照してください。

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

（注） ISE には最大 200 のドメイン コントローラのみを追加できます。制限を超えると、「エラー発生 <DC FQDN> - DC の数が最大許容数である 200 を超えています（Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200）」というエラーが表示されます。

ドメイン コントローラの追加

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 （注） パッシブ ID サービスの新しいドメイン コントローラ（DC）を追加するには、その DC のログイン クレデンシャルが必要です。

[PassiveID] タブに移動し、[DC の追加（Add DCs）] をクリックします。

ステップ 4 モニター対象として参加ポイントに追加するドメイン コントローラの隣にあるチェックボックスをオンにし、[OK] をクリックします。
ドメイン コントローラが [PassiveID] タブの [ドメイン コントローラ（Domain Controllers）] リストに表示されます。

ステップ 5 ドメイン コントローラを設定します。

a) ドメイン コントローラをオンにし、[編集（Edit）] をクリックします。[アイテムの編集（Edit Item）] 画面が表示されます。
b) 必要に応じて、各種ドメイン コントローラ フィールドを編集します。
c) WMI プロトコルを選択した場合は、[設定（Configure）] をクリックして WMI を自動的に設定するか、または [テスト（Test）] をクリックして接続をテストします。

DC フェールオーバー メカニズムは DC 優先順位リストに基づいて管理されます。このリストは、フェールオーバーの発生時に DC が選択される順序を決定します。ある DC がオフラインであるか、何らかのエラーのため到達不能な場合には、優先順位リストにおける優先順位が下

がります。DC がオンラインに戻ると、優先順位リストにおけるその優先順位が適宜調整されます（上がります）。

Active Directory ユーザー グループの設定

Active Directory からユーザー ID 情報を収集するさまざまなプローブを使用する場合に、Active Directory ユーザー グループを使用できるようにするため、Active Directory ユーザー グループを設定します。内部的には、Cisco ISE はグループ名のあいまいさの問題を解決し、グループ マッピングを向上させるためにセキュリティ ID（SID）を使用します。SID により、グループ割り当てが正確に一致します。

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。グループを追加する参加ポイントをクリックします。

ステップ 2 [グループ（Groups）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

a) **[追加（Add）]** > **[ディレクトリからグループを選択（Select Groups From Directory）]** を選択して、既存のグループを選択します。

b) **[追加（Add）]** > **[グループの追加（Add Group）]** を選択して、グループを手動で追加します。グループ名と SID の両方を指定するか、またはグループ名のみを指定し、[SID を取得（Fetch SID）] を押します。

ユーザー インターフェイス ログインのグループ名に二重引用符（"）を使用しないでください。

ステップ 4 グループを手動で選択する場合は、フィルタを使用してグループを検索できます。たとえば、**admin*** をフィルタ基準として入力し、[グループの取得（Retrieve Groups）] をクリックすると、admin で始まるユーザー グループが表示されます。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。一度に取得できるのは 500 グループのみです。

ステップ 5 許可ポリシーで使用可能にするグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 グループを手動で追加する場合は、新しいグループの名前と SID を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

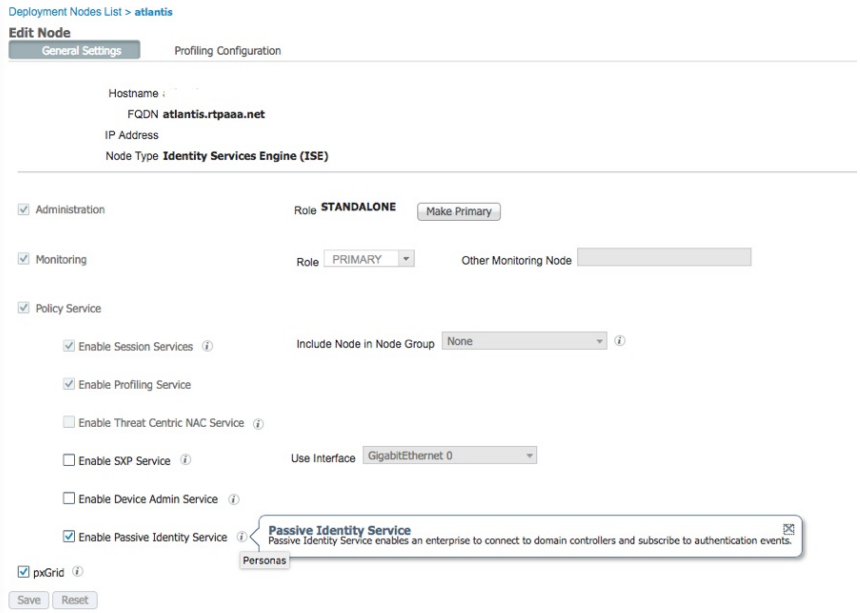
（注） グループを削除し、そのグループと同じ名前で新しいグループを作成する場合は、[SID 値の更新（Update SID Values）] をクリックして、新しく作成したグループに新しい SID を割り当てる必要があります。アップグレードすると、最初の参加の後に SID が自動的に更新されます。

パッシブ ID 用の WMI の設定

始める前に

AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。[管理（Administration）] > [システム（System）] > [展開（Deployment）] で、このノードのパッシブ ID が有効になっていることを確認します。

図 *3:*

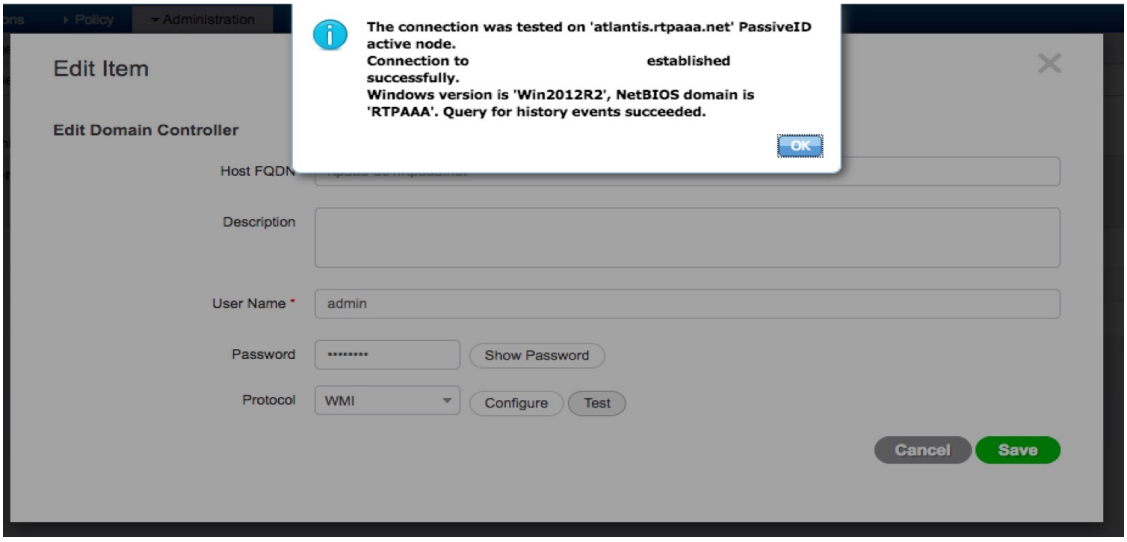


ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスとともに表示されます。

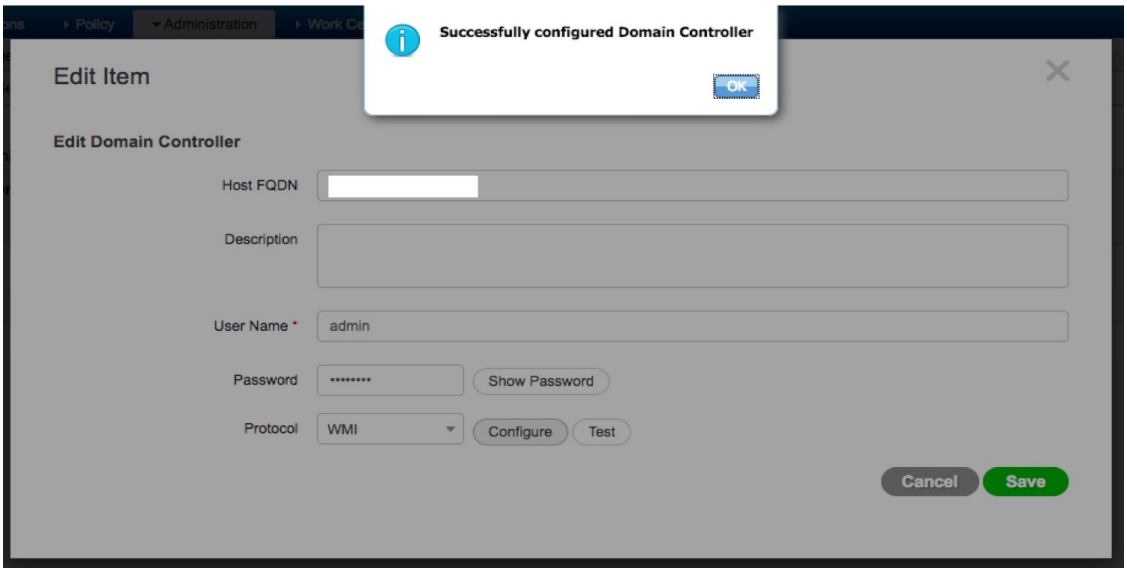
ステップ 3 [パッシブ ID（Passive ID）] タブに移動し、該当するドメイン コントローラの隣にあるチェックボックスをオンにし、[WMI の設定（Config WMI）] をクリックして、選択したドメイン コントローラが ISE-PIC により自動的に設定されるようにします。

図 4：



Active Directory とドメイン コントローラを手動で設定する場合、または設定の問題のトラブルシューティングを行う場合は、Active Directory と Cisco ISE-PIC の統合の前提条件 （189 ページ）を参照してください。

図 5：



（注） エージェントが Windows システムで正確な DC の詳細を取得できない場合は、DC と Cisco ISE 間の通信を再確立する必要があります。再確立するには、Cisco ISE IP アドレスと Cisco ISE FQDN（たとえば、Cisco ISE IP アドレス：https://10.0.0.0/ および Cisco ISE FQDN：https://ise1.cisco.com/）を Windows システム（**[このPC（This PC）]** > **[ローカルディスク（C:）（Local Disk (C:)）]** > **[Windows]** > **[System32]** > **[drivers]** > **[etc]**）の *hosts* ファイルに追加します。

Active Directory プロバイダの管理

Active Directory 参加ポイントの作成と設定が完了したら、次の作業を行い Active Directory プローブを管理します。

- Active Directory グループのためのユーザーのテスト （28 ページ）
- ノードの Active Directory の参加の表示 （29 ページ）
- Active Directory の問題の診断 （29 ページ）
- Active Directory ドメインの脱退 （30 ページ）
- Active Directory の設定の削除 （31 ページ）
- Active Directory デバッグ ログの有効化 （31 ページ）

Active Directory グループのためのユーザーのテスト

Active Directory からユーザー グループを検証するには、[ユーザーのテスト（Test User）] ツールを使用できます。単一の参加ポイントまたはスコープのテストを実行できます。

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- すべての参加ポイントのテストを実行するには、**[拡張ツール（Advanced Tools）]** > **[すべての参加ポイントのユーザーをテスト（Test User for All Join Points）]** を選択します。
- 特定の参加ポイントのテストを実行するには、参加ポイントを選択し、[編集（Edit）] をクリックします。Cisco ISE-PIC ノードを選択し、[ユーザーのテスト（Test User）] をクリックします。

ステップ 3 Active Directory のユーザー（またはホスト）のユーザー名とパスワードを入力します。

ステップ 4 認証タイプを選択します。ステップ 3 のパスワード入力は、ルックアップ オプションを選択する場合には必要ありません。

ステップ 5 すべての参加ポイントに対してこのテストを実行する場合は、このテストを実行する Cisco ISE-PIC ノードを選択します。

ステップ 6 Active Directory からグループを取得するには、[グループを取得（Retrieve Groups）] および [属性の取得（Retrieve Attributes）] チェック ボックスをオンにします。

ステップ 7 [テスト（Test）] をクリックします。
テスト操作の結果と手順が表示されます。手順で失敗の原因を特定し、トラブルシューティングできます。

また、Active Directory がそれぞれの処理手順を実行するのに要する時間（ミリ秒単位）を表示することもできます。操作にかかる時間がしきい値を超えると、Cisco ISE-PIC に警告メッセージが表示されます。

ノードの Active Directory の参加の表示

特定の Cisco ISE-PIC ノードのすべての Active Directory 参加ポイントのステータスまたはすべての Cisco ISE-PIC ノードのすべての参加ポイントのリストを表示するには、[Active Directory] ページの [ノード ビュー（Node View）] ボタンを使用できます。

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。

ステップ 2 [ノード ビュー（Node View）] をクリックします。

ステップ 3 [ISE Node（ISE ノード）] ドロップダウン リストからノードを選択します。
テーブルに、Active Directory のステータスがノード別に一覧されます。展開に複数の参加ポイントと複数の Cisco ISE-PIC ノードがある場合、このテーブルが更新されるまでに数分かかる場合があります。

ステップ 4 その Active Directory 参加ポイントのページに移動し、その他の特定のアクションを実行するには、参加ポイントの [名前（Name）] リンクをクリックします。

ステップ 5 [診断ツール（Diagnostic Tools）] ページに移動して特定の問題のトラブルシューティングを行うには、[診断概要（Diagnostic Summary）] 列のリンクをクリックします。診断ツールでは、ノードごとに各参加ポイントの最新の診断結果が表示されます。

Active Directory の問題の診断

診断ツールは、各 Cisco ISE-PIC ノードで実行されるサービスです。診断ツールを使用して、Active Directory 展開を自動的にテストおよび診断したり、Cisco ISE-PIC によって Active Directory が使用される場合に機能やパフォーマンスの障害の原因となる可能性がある問題を検出するための一連のテストを実行したりすることができます。

Cisco ISE-PIC が Active Directory に参加できない、または Active Directory に対して認証できない理由は、複数あります。このツールは、Cisco ISE-PIC を Active Directory に接続するための前提条件が正しく設定されていることを確認するのに役立ちます。また、ネットワーク、ファイアウォール設定、クロック同期、ユーザー認証などの問題の検出に役立ちます。このツールは、手順をステップごとに説明したガイドとして機能し、必要に応じて、中間の各レイヤの問題の修正を支援します。

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。

ステップ 2 [拡張ツール（Advanced Tools）] ドロップダウン リストをクリックし、[診断ツール（Diagnostic Tools）] を選択します。

ステップ 3 診断を実行する Cisco ISE-PIC ノードを選択します。

Cisco ISE-PIC ノードを選択しない場合は、すべてのノードでテストが実行されます。

ステップ 4 特定の Active Directory 参加ポイントを選択します。

Active Directory 参加ポイントを選択しない場合は、すべての参加ポイントでテストが実行されます。

ステップ 5 オンデマンドで、またはスケジュールに基づいて診断テストを実行できます。

- テストをすぐに実行するには、[テストを今すぐ実行（Run Tests Now）] を選択します。
- スケジュールした間隔でテストを実行するには、[スケジュールしたテストを実行する（Run Scheduled Tests）] チェックボックスをオンにし、開始時刻とテストの実行間隔（時、日、週単位）を指定します。このオプションを有効にすると、すべての診断テストがすべてのノードとインスタンスに対して実行され、[ホーム（Home）] ダッシュボードの [アラーム（Alarms）] ダッシュレットに障害が報告されます。

ステップ 6 警告ステータスまたは失敗ステータスのテストの詳細を確認するには、[テストの詳細の表示（View Test Details）] をクリックします。
このテーブルを使用して、特定のテストの再実行、実行中のテストの停止、特定のテストのレポートの表示を行うことができます。

Active Directory ドメインの脱退

この Active Directory ドメインまたはこの参加ポイントを使用してユーザー ID を収集する必要がない場合は、Active Directory ドメインを脱退できます。

コマンドライン インターフェイスから Cisco ISE-PIC アプリケーション設定をリセットする場合、またはバックアップやアップグレードの後に設定を復元する場合、脱退操作が実行され、Cisco ISE-PIC ノードがすでに参加している場合は、Active Directory ドメインから切断されます。ただし、Cisco ISE-PIC ノードのアカウントは、Active Directory ドメインから削除されません。脱退操作では Active Directory ドメインからノード アカウントも削除されるため、脱退操作は管理者ポータルから Active Directory クレデンシャルを使用して実行することを推奨します。これは、Cisco ISE-PIC ホスト名を変更する場合にも推奨されます。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 Cisco ISE-PIC ノードの隣にあるチェックボックスをオンにして [脱退（Leave）] をクリックします。

ステップ 4 Active Directory のユーザー名とパスワードを入力し、[OK] をクリックしてドメインを脱退し、Cisco ISE-PIC データベースからマシン アカウントを削除します。

Active Directory クレデンシャルを入力すると、Cisco ISE-PIC ノードは Active Directory ドメインを脱退し、Active Directory データベースから Cisco ISE-PIC マシン アカウントが削除されます。

（注） Active Directory データベースから Cisco ISE-PIC マシン アカウントを削除するには、ここに入力する Active Directory クレデンシャルに、ドメインからマシン アカウントを削除する権限がなければなりません。

ステップ 5 Active Directory クレデンシャルがない場合は、[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにして、[OK] をクリックします。

[クレデンシャルなしでドメインを脱退（Leave domain without credentials）] チェックボックスをオンにすると、プライマリ Cisco ISE-PIC ノードが Active Directory ドメインから脱退します。参加時に Active Directory で作成されたマシン アカウントは、Active Directory 管理者が手動で削除する必要があります。

Active Directory の設定の削除

特定の Active Directory 設定をプローブとして使用しない場合は、Active Directory の設定を削除する必要があります。別の Active Directory ドメインに参加する場合は、設定を削除しないでください。現在参加しているドメインから脱退し、新しいドメインに参加できます。この設定は唯一の設定であるため、削除しないでください。 ISE-PIC

始める前に

Active Directory ドメインが残っていることを確認します。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 設定された Active Directory の横のチェックボックスをオンにします。

ステップ 3 [ローカル ノード ステータス（Local Node Status）] が [参加していない（Not Joined）] としてリストされていることを確認します。

ステップ 4 [削除（Delete）] をクリックします。

Active Directory データベースから設定を削除しました。後で Active Directory を使用する場合は、有効な Active Directory の設定を再送信できます。

Active Directory デバッグ ログの有効化

Active Directory デバッグ ログはデフォルトでは記録されません。Active Directory のデバッグ ログを有効にすると、ISE-PIC のパフォーマンスに影響する場合があります。

ステップ 1 **[管理（Administration）] > [ロギング（Logging）] > [デバッグログ設定（Debug Log Configuration）]** を選択します。

ステップ 2 Active Directory のデバッグ情報を取得する Cisco ISE-PIC ノードの隣のオプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 3 [Active Directory] オプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 4 [Active Directory] の隣にあるドロップダウン リストから [DEBUG] を選択します。これにはエラー、警告、および verbose ログが含まれます。完全なログを取得するには、[TRACE] を選択します。

ステップ 5 [保存（Save）] をクリックします。

Active Directory の設定

Active Directory（AD）は、安全性が高く正確なソースであり、ここからユーザー情報（ユーザー名、IP アドレスなど）が取得されます。

参加ポイントを作成、編集することで Active Directory プローブを作成、管理するには、**[プロバイダー（Providers）]** > **[Active Directory]** を選択します。

詳細については、Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE-PIC ノードの参加 （22 ページ）を参照してください。

[プロバイダー（Providers）] > **[Active Directory]** を選択し、編集する参加ポイントをオンにして、**[編集（Edit）]** をクリックします。[ドメインへの参加（Join Domain）] 画面で、**[プロバイダー（Providers）]** > **[Active Directory]** を選択し、編集する参加ポイントをオンにして **[参加（Join）]** をクリックします。

表 *4 : Active Directory* 参加ポイント名の設定と *[ドメインへの参加（Join Domain）]* ウィンドウ

フィールド名	説明
参加ポイント名（Join Point Name）	設定したこの参加ポイントを容易に区別できる一意の名前。
Active Directory ドメイン（Active Directory Domain）	このノードが接続している Active Directory ドメインのドメイン名。
ドメイン管理者（Domain Administrator）	管理者権限を持つ Active Directory ユーザーのユーザープリンシパル名またはユーザーアカウント名。
パスワード（Password）	Active Directory で設定されているドメイン管理者のパスワード。
組織単位の指定（Specifiy Organizational Unit）	管理者の組織単位の情報を入力します。
クレデンシャルの保存（Store Credentials）	管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。 エンドポイントプローブの場合は、[クレデンシャルの保存（Store Credentials）] を選択する必要があります。

[プロバイダ（Providers）] > **[Active Directory]** を選択します。

表 *5 : [Active Directory* 参加/脱退（*Active Directory Join/Leave*）*]* ウィンドウ

フィールド名	説明
ISEノード（ISE Node）	インストール環境での特定のノードの URL。
ISE ノードのロール（ISE Node Role）	インストール環境でそのノードがプライマリ ノードまたはセカンダリ ノードのいずれであるかを指定します。
ステータス（Status）	ノードが Active Directory ドメインにアクティブに参加しているかどうかを示します。
ドメイン コントローラ（Domain Controller）	Active Directory に参加しているノードの場合、この列には Active Directory ドメインでノードが接続している特定のドメイン コントローラが示されます。
サイト（Site）	これは完全な ISE インストール環境にのみ関連します。詳細については、完全な ISE インストールへの ISE-PIC のアップグレード（151 ページ）を参照してください。

表 *6 : [*パッシブ *ID* ドメイン コントローラ（*DC*）（*Passive ID Domain Controllers (DC)*）*]* リスト

フィールド	説明
ドメイン（Domain）	ドメインコントローラが存在しているサーバーの完全修飾ドメイン名。
DC ホスト（DC Host）	ドメインコントローラが存在しているホスト。
サイト（Site）	これは完全な ISE インストール環境にのみ関連します。詳細については、完全な ISE インストールへの ISE-PIC のアップグレード（151 ページ）を参照してください。
IP アドレス（IP Address）	ドメイン コントローラの IP アドレス。

フィールド	説明
モニター方法（Monitor Using）	次のいずれかの方法で、ユーザーID情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するためにActive Directoryをモニターするエージェントを定義している場合は、Agentプロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント （40ページ） を参照してください。

表 *7 : [パッシブ ID ドメインコントローラ（DC）（Passive ID Domain Controllers (DC)）]* 編集ウィンドウ

フィールド名	説明
ホスト FQDN（Host FQDN）	ドメインコントローラが存在しているサーバーの完全修飾ドメイン名を入力します。
説明（Description）	このドメイン コントローラを容易に特定できるように、一意の説明を入力します。
ユーザー名（User Name）	Active Directory にアクセスするための管理者のユーザー名。
パスワード（Password）	Active Directory にアクセスするための管理者のパスワード。

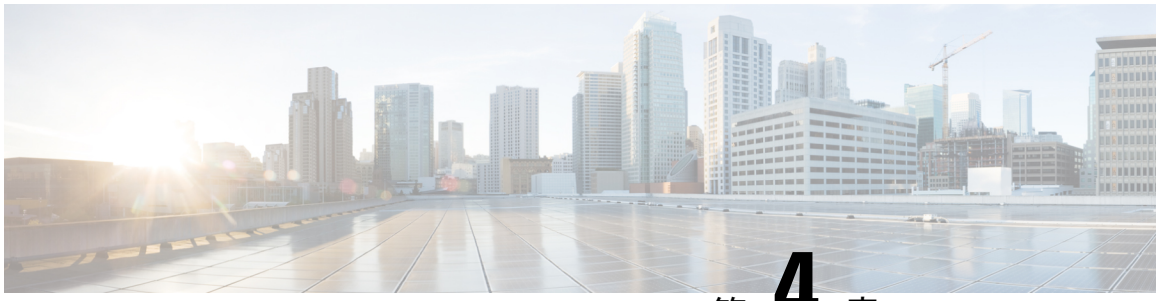
フィールド名	説明
プロトコル（**Protocol**）	次のいずれかの方法で、ユーザーID情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するために Active Directory をモニターするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント （40 ページ） を参照してください。

Active Directory グループは Active Directory から定義および管理されます。このノードに参加している Active Directory のグループは、このタブで確認できます。Active Directory の詳細については、https://msdn.microsoft.com/en-us/library/bb742437.aspx を参照してください。

[プロバイダー（Providers）] > **[Active Directory]** > **[詳細設定（Advanced Settings）]** を選択します。

表 *8 : Active Directory* の詳細設定

フィールド名	説明
履歴期間（History interval）	すでに発生したユーザー ログインの情報を パッシブ ID サービスが読み取る期間。これは、パッシブ ID サービスの起動時または再起動時に、このサービスが使用不可であった間に生成されたイベントを確認するために必要となります。エンドポイント プローブがアクティブな場合、この期間の頻度が維持されます。
ユーザー セッションのエージング タイム（User session aging time）	ユーザーがログインできる時間です。パッシブ ID サービスでは、DC からの新しいユーザー ログイン イベントが識別されますが、DC はユーザーがログオフする時点を報告しません。エージング タイムを使用すると、ISE-PIC で、ユーザーがログインする時間間隔を決定できます。
NTLM プロトコル設定（NTLM Protocol settings）	ISE-PIC と DC の間の通信プロトコルとして [NTLMv1] または [NTLMv2] を選択できます。推奨されるデフォルトは [NTLMv2] です。



第 4 章

プロバイダ

ISE-PIC が ID 情報を、サービスをサブスクライブするコンシューマ（サブスクライバ）に提供できるようにするため、最初に ISE-PIC プローブを設定する必要があります。このプローブは ID プロバイダに接続します。

次の表に、ISE-PIC で使用可能なすべてのプロバイダとプローブタイプの詳細を示します。Active Directory の詳細については、プローブおよびプロバイダとしての Active Directory （19 ページ）を参照してください。

定義できるプロバイダ タイプを次に示します。

表 *9:* プロバイダ タイプ

プロバイダ タイプ（プローブ）	説明	送信元システム（プロバイダ）	テクノロジー	収集されるユーザー ID 情報	ドキュメント リンク
Active Directory（AD）	ユーザー情報の取得元である安全性が高く正確で最も一般的なソース。 プローブとして機能する場合、AD は WMI テクノロジーを使用して認証済みユーザー ID を送信します。 また AD 自体が、プローブではなく、その他のプローブがユーザー データを取得するソース システム（プロバイダ）として機能します。	Active Directory ドメイン コントローラ	WMI	• ユーザー名（User name） • IP アドレス • ドメイン	プローブおよびプロバイダとしての Active Directory （19 ページ）
エージェント（Agents）	Active Directory ドメイン コントローラまたはメンバー サーバーにインストールされているネイティブ 32 ビット アプリケーション。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。		ドメイン コントローラまたはメンバー サーバーにインストールされているエージェント。	• ユーザー名（User name） • IP アドレス • ドメイン	Active Directory エージェント （40 ページ）
エンドポイント（Endpoint）			WMI	ユーザーが接続しているかどうか	エンドポイント プローブ （77 ページ）

プロバイダタイプ（プローブ）	説明	送信元システム（プロバイダ）	テクノロジー	収集されるユーザー ID 情報	ドキュメントリンク
	設定されているその他のプローブに加えて、ユーザーが接続しているかどうかを確認するため、常にバックグラウンドで実行されます。				
SPAN	ネットワーク トラフィックをリッスンし、Active Directory データに基づいてユーザー ID 情報を抽出するため、ネットワーク スイッチに導入されています。		SPAN（スイッチにインストール）と Kerberos メッセージ	• ユーザー名（User name） • IP アドレス • ドメイン	SPAN （50 ページ）
API プロバイダ	ISE-PIC が提供する RESTful API サービスを使用して、RESTful API クライアントと通信するようにプログラミングされている任意のシステムから、ユーザー ID 情報を収集します。	REST API クライアントと通信するようにプログラミングされている任意のシステム。	RESTful API。JSON 形式でサブスクライバに送信されるユーザー ID。	• ユーザー名（User name） • IP アドレス • ポート範囲（Port range） • ドメイン（Domain）	API プロバイダ （45 ページ）
Syslog	syslog メッセージを解析し、ユーザー ID（MAC アドレスを含む）を取得します。	• 標準 syslog メッセージ プロバイダ • DHCP サーバー	syslog メッセージ	• ユーザー名（User name） • IP アドレス • MAC アドレス • ドメイン	syslog プロバイダ （52 ページ）

（注） pxGrid は、セッショントピックに対して 1 秒あたり 200 イベントを送信して、クライアントのオーバーロードを回避します。パブリッシャが 200 を超えるイベントを送信すると、追加のイベントはキューに入り、次のバッチで送信されます。

pxGrid が長時間にわたって 1 秒あたり 200 を超えるイベントを継続的に受信する場合、バックログイベントを保存するために通常よりも多くのメモリが消費される可能性があり、pxGrid のパフォーマンスに影響を与える場合があります。

- Active Directory エージェント （40 ページ）
- API プロバイダ （45 ページ）
- SPAN （50 ページ）
- syslog プロバイダ （52 ページ）
- パッシブ ID サービスのフィルタリング （76 ページ）
- エンドポイント プローブ （77 ページ）

Active Directory エージェント

ISE-PICから、ネイティブ 32 ビット アプリケーション、ドメイン コントローラ（DC）エージェントを、（設定に応じて）Active Directory（AD）ドメイン コントローラ（DC）またはメンバー サーバー上の任意の場所にインストールし、AD からユーザー ID 情報を取得して、設定したサブスクライバにこれらの ID を送信します。エージェント プローブは、ユーザー ID 情報に Active Directory を使用する場合の簡単で効率的なソリューションです。エージェントは個別のドメインまたは AD ドメインにインストールできます。インストールされたエージェントは、1 分ごとに ISE-PIC にステータス更新情報を提供します。

エージェントは ISE-PIC が自動的にインストールおよび設定するか、またはユーザーが手動でインストールすることができます。インストールが完了すると、次のようになります。

- エージェントとその関連ファイルはパス **`Program Files/Cisco/Cisco ISE PassiveID Agent`** にインストールされています。
- エージェントのロギング レベルを指定する **`PICAgent.exe.config`** という設定ファイルがインストールされます。この設定ファイル内でロギング レベルを手動で変更できます。
- CiscoISEPICAgent.log ファイルにはすべてのロギング メッセージが保存されます。
- nodes.txt ファイルには、展開内でエージェントが通信できるすべてのノードのリストが含まれています。エージェントはリストの最初のノードと通信します。このノードと通信できない場合、エージェントはリストのノード順序に従ってノードとの通信を試行します。手動でのインストールの場合、このファイルを開き、ノード IP アドレスを入力する必要があります。（手動または自動での）インストールの完了後にこのファイルを変更するには、このファイルを手動で更新する必要があります。ファイルを開き、ノード IP アドレスを必要に応じて追加、変更、または削除します。

- Cisco ISE PassiveID Agent サービスはマシン上で稼働します。このサービスは [Windows サービス（Windows Services）] ダイアログボックスから管理できます。
- ISE-PIC は 74 個のドメインコントローラで検証されています。
- Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。エージェントをインストールできない場合、パッシブ ID サービスには Active Directory プローブを使用します。詳細については、プローブおよびプロバイダとしての Active Directory（19 ページ）を参照してください。

（注） メンバーサーバーで AD エージェントを実行している場合でも、Active Directory にログイン要求をクエリします。

Active Directory エージェントの自動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE-PIC が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、自動インストールを有効にし、ドメイン コントローラをモニターするようにエージェントを設定する方法について説明します。

始める前に

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバー （16 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。
- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダとしての Active Directory（19 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定 （25 ページ）を参照してください。

ステップ 1 **[プロバイダ（Providers）]** > **[エージェント（Agents）]** を選択します。

ステップ 2 新しいエージェントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 新しいエージェントを作成し、この設定で指定するホストに自動的にインストールするには、[新規エージェントの展開（Deploy New Agent）] を選択します。

ステップ 4 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （44 ページ）を参照してください。

ステップ 5 [展開（Deploy）] をクリックします。
設定で指定したドメインに基づいてエージェントが自動的にホストにインストールされ、設定が保存されます。エージェントは [エージェント（Agents）] テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 6 **[プロバイダ（Providers）]** > **[Active Directory]** を選択し、現在選択されているすべての参加ポイントを表示します。

ステップ 7 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 8 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 9 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）] をクリックします。

ステップ 10 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 11 **作成したエージェントを [エージェント（Agent）]** ドロップダウンリストから選択します。作成したエージェントのユーザー名とパスワードのログイン情報を入力し、**[保存（Save）]** をクリックします。

ユーザー名とパスワードのログイン情報は、ドメインコントローラにエージェントをインストールするために使用されます。最後に、[展開する（Deploy）] をクリックすると、*picagent.exe* が */opt/pbis/bin* から指定した Windows マシンにコピーされます。

Active Directory エージェントの手動インストールおよび展開

ユーザー ID についてドメイン コントローラをモニターするようにエージェント プロバイダを設定するときには、エージェントがメンバー サーバーまたはドメイン コントローラのいずれかにインストールされている必要があります。エージェントは ISE-PIC が自動的にインストールするか、またはユーザーが手動でインストールすることができます。手動または自動でのインストール後に、インストールされたエージェントが、デフォルト WMI ではなく指定のドメイン コントローラをモニターするように設定する必要があります。このプロセスでは、エージェントを手動でインストールし、ドメイン コントローラをモニターするように設定する方法について説明します。

始める前に

- サーバー側からの関連 DNS サーバーの逆引き参照を設定します。ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバー （16 ページ）を参照してください。
- エージェント用に指定されたマシンで Microsoft .NET Framework がバージョン 4.0 以上に更新されていることを確認します。.NET フレームワークの詳細については、https://www.microsoft.com/net/framework を参照してください。

- AD 参加ポイントを作成し、1 つ以上のドメイン コントローラを追加します。参加ポイントの作成の詳細については、プローブおよびプロバイダとしての Active Directory （19 ページ）を参照してください。

  AD、エージェント、SPAN、および syslog プローブで AD ユーザー グループを使用します。AD グループの詳細については、Active Directory ユーザー グループの設定 （25 ページ）を参照してください。

ステップ 1 **[プロバイダ（Providers）]** > **[エージェント（Agents）]** を選択します。

ステップ 2 [エージェントのダウンロード（Download Agent）] をクリックし、手動でインストールするための **`picagent-installer.zip`** ファイルをダウンロードします。
このファイルは Windows の標準ダウンロード フォルダにダウンロードされます。

ステップ 3 ZIP ファイルを指定のホスト マシンに保存してインストールを実行します。

ステップ 4 ISE-PIC GUI で **[プロバイダー（Providers）]** > **[エージェント（Agents）]** をもう一度選択します。

ステップ 5 新しいエージェントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 6 すでにホストマシンにインストールしているエージェントを設定するには、[既存のエージェントの登録（Register Existing Agent）] を選択します。

ステップ 7 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、Active Directory エージェントの設定 （44 ページ）を参照してください。

ステップ 8 **[保存（Save）]** をクリックします。
エージェント設定が保存されます。エージェントは[エージェント（Agents）]テーブルに表示されます。これで、指定したドメイン コントローラにこのエージェントを適用できます。これについては以降のステップで説明します。

ステップ 9 **[プロバイダー（Providers）]** > **[Active Directory]** を選択し、現在設定されているすべての参加ポイントを選択します。

ステップ 10 作成したエージェントを有効にする参加ポイントのリンクをクリックします。

ステップ 11 前提条件の一部として追加したドメインコントローラを設定するには、[パッシブ ID（Passive ID）] タブを選択します。

ステップ 12 作成したエージェントを使用してモニターするドメインコントローラを選択し、[編集（Edit）]をクリックします。

ステップ 13 [プロトコル（Protocol）] ドロップダウンリストから [エージェント（Agent）] を選択します。

ステップ 14 作成したエージェントを [エージェント（Agent）] ドロップダウンリストから選択します。エージェントに接続するためのユーザー名とパスワードを入力し、[保存（Save）] をクリックします。

ユーザーアカウントには、セキュリティイベントを読み取るために必要な権限が必要です。WMI ベースのエージェントのユーザーアカウントには、WMI/DCOM 権限が必要です。

エージェントのアンインストール

自動または手動でインストールされたエージェントは、Windowsから直接（手動で）簡単にアンインストールできます。

ステップ 1 [Windows] ダイアログで [プログラムと機能（Programs and Features）] に移動します。

ステップ 2 インストールされているプログラムのリストで [Cisco ISE PassiveID エージェント（Cisco ISE PassiveID Agent）] を見つけて選択します。

ステップ 3 [アンインストール（Uninstall）] をクリックします。

Active Directory エージェントの設定

ISE-PIC が、さまざまなドメイン コントローラ（DC）からユーザー ID 情報を取得し、その情報を ISE-PIC サブスクライバに配信するために、ネットワーク内の指定されたホストにエージェントを自動的にインストールすることを許可します。

エージェントを作成および管理するには、**[プロバイダー（Providers）]** > **[エージェント（Agents）]** を選択します。Active Directory エージェントの自動インストールおよび展開 （41 ページ）を参照してください。

表 *10* : *[エージェント（Agents）]* ウィンドウ

フィールド名	説明
Name	設定したエージェント名。
ホスト（Host）	エージェントがインストールされているホストの完全修飾ドメイン名。
モニターリング（Monitoring）	指定されたエージェントがモニターするドメインコントローラのカンマ区切りリストです。

表 *11* : 新規エージェント（*Agents New*）

フィールド	説明
新規エージェントの展開（Deploy New Agent）または既存のエージェントの登録（Register Existing Agent）	• 新規エージェントの展開（Deploy New Agent）：指定されたホストに新規エージェントをインストールします。 • 既存のエージェントの登録（Register Existing Agent）：ホストにエージェントを手動でインストールし、ISE-PIC がサービスを有効にできるようにするため、この画面でそのエージェントを設定します。

フィールド	説明
名前（**Name**）	エージェントを容易に把握できる名前を入力します。
説明（**Description**）	エージェントを容易に把握できる説明を入力します。
ホスト FQDN（**Host FQDN**）	エージェントがインストールされているホスト(既存のエージェントの登録の場合）またはインストールされるホスト（自動展開の場合）の完全修飾ドメイン名です。
ユーザー名（**User Name**）	エージェントをインストールするホストにアクセスするためのユーザー名を入力します。ISE-PIC はこれらのクレデンシャルを使用してエージェントを自動的にインストールします。 ユーザーアカウントには、リモートで接続して PIC エージェントをインストールするための権限が必要です。
パスワード	エージェントをインストールするホストにアクセスするためのパスワードを入力します。ISE-PIC はこれらのクレデンシャルを使用してエージェントを自動的にインストールします。

API プロバイダ

Cisco ISE-PIC の API プロバイダ機能では、カスタマイズしたプログラムまたはターミナル サーバー（TS）エージェントから組み込み ISE-PICREST API サービスにユーザー ID 情報をプッシュできます。これにより、ネットワークからプログラミング可能なクライアントをカスタマイズして、任意のネットワーク アクセス制御（NAC）システムから収集されたユーザー ID をこのサービスに送信するようにできます。さらに Cisco ISE-PIC API プロバイダにより、すべてのユーザーの IP アドレスが同一であるが、各ユーザーに固有のポートが割り当てられるネットワーク アプリケーション（Citrix サーバーの TS-Agent など）と対話できます。

たとえば、Active Directory（AD）サーバーに対して認証されたユーザーの ID マッピングを提供する Citrix サーバーで稼働するエージェントは、新しいユーザーがログインまたはログオフするたびに、ユーザー セッションを追加または削除する REST 要求を ISE-PIC に送信できます。ISE-PIC は、クライアントから送信されたユーザー ID 情報（IP アドレス、割り当てられたポートなど）を取得し、事前に設定されているサブスクライバ（Cisco Firepower Management Center（FMC）など）に送信します。

ISE-PIC REST API フレームワークは、HTTPS プロトコルを介した REST サービスを実装し（クライアント証明書の検証は不要）、ユーザー ID 情報が JSON（JavaScript Object Notation）形式で送信されます。JSON の詳細については、http://www.json.org/ を参照してください。

ISE-PIC REST API サービスは、1 つのシステムに同時にログインしている複数のユーザーを区別するため、ユーザーIDを解析し、その情報をポート範囲にマッピングします。ポートがユーザーに割り当てられるたびに、API がメッセージを ISE-PIC に送信します。

REST API プロバイダのフロー

カスタマイズしたクライアントを ISE-PIC のプロバイダとして宣言し、そのカスタマイズした特定のプログラム（クライアント）が RESTful 要求を送信できるようにして、ISE-PIC からカスタマイズしたクライアントへのブリッジを設定している場合、ISE-PIC REST サービスは次のように機能します。

1. Cisco ISE-PIC はクライアント認証のために認証トークンを必要とします。通信開始時と、ISE-PIC から以前のトークンの期限が切れたことが通知されるたびに、クライアント マシンのカスタマイズしたプログラムから認証トークンを求める要求が送信されます。この要求への応答としてトークンが返されます。これによりクライアントと ISE-PIC サービス間の継続的な通信が可能になります。
2. ユーザーがネットワークにログインすると、クライアントはユーザー ID 情報を取得し、API Add コマンドを使用してこの情報を ISE-PIC REST サービスに送信します。
3. Cisco ISE-PIC はユーザー ID 情報を受信してマッピングします。
4. Cisco ISE-PIC はマッピングされたユーザー ID 情報をサブスクライバに送信します。
5. 必要な場合は常に、カスタマイズされたマシンはユーザー情報削除要求を送信できます。このためには、Remove API コールを送信し、Add コールの送信時に応答として受信したユーザー ID を含めます。

ISE-PIC での REST API プロバイダの操作

ISE-PIC で REST サービスをアクティブにするには、次の手順に従います。

1. クライアント側を設定します。詳細については、クライアント ユーザー マニュアル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、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。ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバー （16 ページ）を参照してください。
3. パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定 （47 ページ）を参照してください。

（注） TS-Agent と連携するように API プロバイダを設定するには、ISE-PIC からそのエージェントへのブリッジの作成時に TS-Agent 情報を追加します。その後、TS-Agent のマニュアルで API コールの送信について確認してください。

4. 認証トークンを生成し、追加要求と削除要求を API サービスに送信します。

パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定

ISE-PIC REST API サービスが特定のクライアントから情報を受信できるようにするには、まず Cisco ISE-PIC でその特定のクライアントを定義する必要があります。異なる IP アドレスを使用して複数の REST API クライアントを定義できます。

始める前に

- 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。Cisco ISE-PIC の DNS サーバー設定要件の詳細については、DNS サーバー （16 ページ）を参照してください。

ステップ 1 [API プロバイダ（API Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しいクライアントを追加するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドに入力します。詳細については、API プロバイダの設定 （48 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックします。
クライアント設定が保存され、更新された [API プロバイダ（API Providers）] テーブルが画面に表示されます。これで、クライアントは ISE-PIC REST サービスにポストを送信できるようになりました。

次のタスク

認証トークンとユーザー ID を ISE-PIC REST サービスに送信するように、カスタマイズしたクライアントをセットアップします。ISE-PIC REST サービスへの API コールの送信 （47 ページ） を参照してください。

ISE-PIC REST サービスへの API コールの送信

始める前に

パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定 （47 ページ）

ステップ 1 Cisco ISE 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 [API プロバイダ（API Providers）] ウィンドウで指定および設定したユーザー名とパスワードを入力します。詳細については、パッシブ ID サービス の ISE-PIC REST サービスへのブリッジの設定 （47 ページ）を参照してください。

ステップ 3 Enter キーを押します。

ステップ 4 ターゲットノードの [URL アドレス（URL Address）] フィールドに API コールを入力します。

ステップ 5 [送信（Send）] をクリックして API コールを発行します。

次のタスク

さまざまなAPIコールとそのスキーマおよび結果の詳細については、API コール （49 ページ）を参照してください。

API プロバイダの設定

（注） 次のようにリクエスト コールを使用して完全な API 定義とオブジェクト スキーマを取得できます。

- 完全な API の指定（wadl）：https://YOUR_ISE:9094/application.wadl
- API モデルとオブジェクト スキーマ：https://YOUR_ISE:9094/application.wadl/xsd0.xsd

表 *12 : API* プロバイダの設定

フィールド	説明
名前	このクライアントを他のクライアントから容易に区別できる一意の名前を入力します。
説明（Description）	このクライアントのわかりやすい説明を入力します。
ステータス（Status）	設定完了後すぐにクライアントが REST サービスとやりとりできるようにするには、[有効（Enabled）] を選択します。
ホスト/IP（Host/ IP）	クライアント ホスト マシンの IP アドレスを入力します。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、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。
ユーザー名（User name）	REST サービスへの送信時に使用する一意のユーザー名を作成します。
パスワード（Password）	REST サービスへの送信時に使用する一意のパスワードを作成します。

API コール

Cisco ISE-PIC で パッシブ ID サービスのユーザー ID イベントを管理するには、次の API コールを使用します。

目的：認証トークンの生成

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/fmi_platform/v1/identityauth/generatetoken

  要求には BasicAuth 認証ヘッダーが含まれている必要があります。ISE-PIC GUI から以前に作成した API プロバイダのログイン情報を入力します。詳細については、API プロバイダの設定 （48 ページ）を参照してください。

- **応答ヘッダー**

  このヘッダーには X-auth-access-token が含まれています。これは、追加の REST 要求を送信するときに使用するトークンです。

- **応答本文**

  HTTP 204 No Content

目的：ユーザーの追加

- **要求**

  POST

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity

  POST 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

  201 Created

- **応答本文**

  {

  "user": "<ユーザー名>",

  "srcPatRange": {

  "userPatStart": <ユーザー PAT 開始値>,

  "userPatEnd": <ユーザー PAT 終了値>,

  "patRangeStart": <PAT 範囲開始値>

  },

  "srcIpAddress": "<src IP アドレス>",

"agentInfo": "<エージェント名>",

"timestamp": "<ISO_8601 形式、例：“YYYY-MM-DDTHH:MM:SSZ" >",

"domain": "<ドメイン>"

}

- **注記**
  - 上記の JSON で 1 つの IP ユーザー バインディングを作成するには srcPatRange を削除します。
  - 応答本文には「ID」（作成されたユーザーセッションバインディングの固有識別子）が含まれています。削除するユーザーを指定する DELETE 要求を送信するときに、この ID を使用してください。
  - この応答には、新たに作成されたユーザー セッション バインディングの URL であるセルフ リンクも含まれています。

目的：ユーザーの削除

- **要求**

  DELETE

  https://<PIC IP アドレス>:9094/api/identity/v1/identity/useridentity/<id>

  <id> に、Add 応答で受信した ID を入力します。

  DELETE 要求のヘッダーに X-auth-access-token を追加します（例：ヘッダー：X-auth-access-token、値：f3f25d81-3ac5-43ee-bbfb-20955643f6a7）。

- **応答ヘッダー**

  200 OK

- **応答本文**

  応答本文には、削除されたユーザーセッションバインディングの詳細が含まれています。

SPAN

SPANです。このとき、Active Directory が Cisco ISE-PIC と直接連携するように設定する必要はありません。SPAN はネットワーク トラフィックをスニフィングし、特に Kerberos メッセージを調べ、Active Directory により保存されているユーザー ID 情報を抽出し、その情報を ISE-PIC に送信します。ISE-PIC は次にその情報を解析し、最終的にはユーザー名、IP アドレス、およびドメイン名を、ISE-PIC からすでに設定しているサブスクライバに送信します。

SPAN がネットワークをリッスンし、Active Directory ユーザー情報を抽出できるようにするには、ISE-PIC と Active Directory の両方がネットワーク上の同一スイッチに接続している必要が

あります。これにより、SPAN は Active Directory からすべてのユーザー ID データをコピーおよびミラーリングできます。

SPAN により、ユーザー情報は次のように取得されます。

1. ユーザーエンドポイントがネットワークにログインします。
2. ログイン データとユーザー データは Kerberos メッセージに保存されます。
3. ユーザーがログインし、ユーザーデータがスイッチを通過すると、SPAN がネットワークデータをミラーリングします。
4. Cisco ISE-PIC は、ユーザー情報を取得するためネットワークをリッスンし、ミラーリングされたデータをスイッチから取得します。
5. Cisco ISE-PIC はユーザー情報を解析し、パッシブ ID マッピングを更新します。
6. Cisco ISE-PIC は解析後のユーザー情報をサブスクライバに送信します。

SPAN の使用

始める前に

ISE-PIC がネットワーク スイッチから SPAN トラフィックを受信できるようにするには、最初にそのスイッチをリッスンするノードとノードインターフェイスを定義する必要があります。インストールされている複数の ISE-PIC ノードをリッスンするには、SPAN を設定します。ネットワークをリッスンするように設定できるインターフェイスは、ノードごとに 1 つのみです。また、リッスンするために使用するインターフェイスは SPAN 専用である必要があります。

また、次の操作を行う必要があります。

- ネットワークで Active Directory が設定されていることを確認します。
- スイッチが ISE-PIC と通信できることを確認するために、Active Directory に接続しているネットワーク上のスイッチで CLI を実行します。
- AD からネットワークをミラーリングするようにスイッチを設定します。
- SPAN 専用の ISE-PIC ネットワーク インターフェイス カード（NIC）を設定します。この NIC は SPAN トラフィック専用で使用されます。
- SPAN 専用の NIC が、コマンドライン インターフェイスからアクティブにされていることを確認します。
- Kerberos トラフィックのみを SPAN ポートに送信する VACL を作成します。

ステップ 1 **[プロバイダ（Providers）] > [SPAN]** を選択して SPAN を設定します。

ステップ 2 （注） GigabitEthernet0 ネットワーク インターフェイス カード（NIC）は使用可能なままにし、SPAN の設定には使用可能な別の NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

わかりやすい説明を入力し（オプション）、[有効（Enabled）]ステータスを選択し、ネットワーク スイッチのリッスンに使用する関連 NIC とノードを選択します。詳細については、SPAN 設定 （52 ページ）を参照してください。

ステップ 3 **[保存（Save）]** をクリックします。
SPAN 設定が保存され、ISE-PIC がネットワーク トラフィックをアクティブにリッスンします。

SPAN 設定

SPANをクライアントネットワークにインストールすることで、展開した各ノードから、ISE-PICがユーザー ID を受信することを簡単に設定できます。

表 *13 : SPAN* 設定

フィールド	説明
説明（Description）	現在有効なノードとインターフェイスがわかる固有の説明を入力します。
ステータス（Status）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
インターフェイス NIC（Interface NIC）	ISE-PIC にインストールされているノードの 1 つまたは両方を選択してから、選択したノードごとに、ネットワークをリッスンして情報を得るノードインターフェイスを選択します。 （注） GigabitEthernet0 NIC を引き続き使用可能にし、SPAN の設定には他の使用可能な NIC を選択することを推奨します。GigabitEthernet0 は、システム管理の目的で使用されます。

syslog プロバイダ

ISE-PIC は syslog メッセージを配信する任意のクライアント（ID データプロバイダ）からの syslog メッセージを解析し、MAC アドレスなどのユーザー ID 情報を送信します。syslog メッセージには、通常の syslog メッセージ（InfoBlox、Blue Coat、BlueCat、Lucent などのプロバイダからのメッセージ）と DHCP syslog メッセージがあります。このマッピングされたユーザー ID データがサブスクライバに配信されます。

ユーザー ID データを受信する syslog クライアントを指定できます（syslog クライアントの設定 （53 ページ）を参照）。プロバイダの設定時に、接続方法（TCP または UDP）および解析に使用する syslog テンプレートを指定する必要があります。

（注） 設定されている接続タイプが TCP であり、メッセージヘッダーに問題があるためにホスト名を解析できない場合、ISE-PIC はパケットで受信した IP アドレスを、ISE-PIC で設定されている syslog メッセージのプロバイダリストにあるすべてのプロバイダの IP アドレスと照合しようとします。このリストを表示するには、**[プロバイダ（Providers）]** > **[syslog プロバイダ（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （60 ページ） を参照してください。

syslog プローブが受信した syslog メッセージを ISE-PIC パーサーに送信します。パーサーはユーザー ID 情報をマッピングし、その情報を ISE-PIC に公開します。次に ISE-PIC が、解析およびマッピングされたユーザー ID 情報を ISE-PIC サブスクライバに配信します。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE-PIC は、ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているいずれのユーザーとも一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

ISE-PIC からの syslog メッセージを解析してユーザー ID を取得するには、次の手順を実行します。

- ユーザー ID データの送信元 syslog クライアントを設定します。syslog クライアントの設定 （53 ページ）を参照してください。
- 1 つのメッセージヘッダーをカスタマイズします。syslog ヘッダーのカスタマイズ （60 ページ）を参照してください。
- テンプレートを作成してメッセージ本文をカスタマイズします。syslog メッセージ本文のカスタマイズ （59 ページ）を参照してください。
- 解析に使用するメッセージテンプレートとして syslog クライアントを設定する場合には、ISE-PIC で事前に定義されているメッセージテンプレートを使用します。あるいは、これらの事前に定義されたテンプレートに基づいてヘッダーまたは本文のテンプレートをカスタマイズします。Syslog 事前定義メッセージテンプレートの使用 （65 ページ） を参照してください。

syslog クライアントの設定

Cisco ISE-PIC が特定のクライアントからの syslog メッセージをリッスンできるようにするには、最初に Cisco ISE-PIC でそのクライアントを定義する必要があります。異なる IP アドレスを使用して複数のプロバイダを定義できます。

ステップ 1 [syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを設定するには、テーブルの上部で [追加（Add）] をクリックします。

ステップ 3 クライアントを正しく設定するため、すべての必須フィールドを入力し（詳細についてはSyslog の設定（54 ページ）を参照）、必要に応じてメッセージテンプレートを作成します（詳細についてはsyslog メッセージ本文のカスタマイズ （59 ページ）を参照）。

ステップ 4 **[送信（Submit）]** をクリックします。

Syslog の設定

特定のクライアントからの syslog メッセージを介してユーザー ID（MAC アドレスを含む）を受信するように Cisco ISE-PIC を設定します。異なる IP アドレスを使用して複数のプロバイダを定義できます。

表 *14 : syslog* プロバイダ

フィールド名	説明
Name	設定したこのクライアントを容易に区別できる一意の名前を入力します。
説明（Description）	この syslog プロバイダのわかりやすい説明。
ステータス（Status）	設定完了後すぐにクライアントを有効にするには、[有効化（Enabled）] を選択します。
Host	ホスト マシンの FQDN を入力します。

フィールド名	説明
接続タイプ（Connection Type）	ISE-PIC が syslog メッセージをリッスンするチャネルを指定するため、UDP または TCP を入力します。 （注） TCP が設定されている接続タイプである場合で、メッセージヘッダーとホスト名が解析できない問題がある場合は、Cisco ISE は syslog メッセージに設定されているプロバイダのリストにあるいずれかのプロバイダの IP アドレス宛のパケットで受信した IP アドレスと照合しようとします。 このリストを表示するには、**[プロバイダ（Providers）]** > **[syslog プロバイダ（Syslog Providers）]** を選択します。メッセージヘッダーを確認し、必要に応じて、解析が正常に実行されるようにカスタマイズすることをお勧めします。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （60 ページ） を参照してください。

フィールド名	説明
テンプレート（**Template**）	

フィールド名	説明
	テンプレートにより正確な本文メッセージ構造が指定されます。これにより、パーサーは syslog メッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。 たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。 このフィールドでは、syslog メッセージを認識して正しく解析するために使用される（syslog メッセージの本文の）テンプレートを指定します。 事前定義のドロップダウンリストから選択するか、または [新規（New）] をクリックして独自のカスタム テンプレートを作成します。新しいテンプレートの作成の詳細については、syslog メッセージ本文のカスタマイズ （59 ページ）を参照してください。ほとんどの事前定義テンプレートでは正規表現が使用されています。カスタム テンプレートでも正規表現を使用する必要があります。 （注） 編集または削除できるのはカスタム テンプレートだけであり、ドロップダウンの事前定義システム テンプレートは変更できません。 現在 ISE-PIC に含まれている事前定義 DHCP プロバイダ テンプレートを次に示します。 • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP （注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE はユーザー ID 情報を正しく解析して配

フィールド名	説明
	信するために、最初にローカルセッションディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。 DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。 Cisco ISE には次の事前定義の標準 syslog プロバイダテンプレートがあります。 • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN テンプレートについては、Syslog 事前定義メッセージテンプレートの使用（65 ページ） を参照してください。
デフォルト ドメイン（**Default Domain**）	syslog メッセージで特定のユーザーに対してドメインが指定されていない場合、このデフォルト ドメインが自動的にそのユーザーに割り当てられます。これにより、すべてのユーザーにドメインが割り当てられます。 デフォルト ドメインまたはメッセージから解析されたドメインにユーザー名が付加され、username@domain となります。したがって、ユーザーとユーザーグループに関する詳細情報を取得するためには、ドメインを含めます。

syslog メッセージ構造のカスタマイズ（テンプレート）

テンプレートは正確なメッセージ構造を指定します。これにより、パーサーはsyslogメッセージ内で解析、マッピング、配信する必要がある各情報部分を識別できます。たとえば、テンプレートでは正確なユーザー名部分を指定できます。これにより、パーサーは受信するすべてのメッセージでユーザー名を検出できます。テンプレートにより、新規マッピングメッセージとマッピング削除メッセージの両方に対応する構造が決定します。

Cisco ISE-PIC では、ISE-PIC パーサーが使用する 1 つのメッセージ ヘッダーと複数の本文構造をカスタマイズできます。

ISE-PIC パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

メッセージテンプレートをカスタマイズするときに、事前定義オプションで使用されている正規表現とメッセージ構造を調べ、ISE-PIC の事前定義メッセージテンプレートに基づいてカスタマイズを行うかどうかを決定できます。事前定義テンプレートの正規表現、メッセージ構造、例などの詳細については、Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照してください。

次の内容をカスタマイズできます。

- 1 つのメッセージ ヘッダー：syslog ヘッダーのカスタマイズ （60 ページ）
- 複数のメッセージ本文：syslog メッセージ本文のカスタマイズ （59 ページ）。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより Cisco ISE は ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合しようとします。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCPメッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCPメッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義のDHCPテンプレートを使用してください。

syslog メッセージ本文のカスタマイズ

Cisco ISE-PIC では、ISE-PIC パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます（メッセージ本文のカスタマイズ）。テンプレートには、ユーザー名、IPアドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） DHCP syslog メッセージにはユーザー名は含まれていません。したがって、これらのメッセージはパーサーから遅れて配信されます。これにより ISE は ユーザー ID 情報を正しく解析して配信するために、最初にローカル セッション ディレクトリに登録されているユーザー（[ライブセッション（Live Sessions）] で表示）を調べ、その後で各ユーザーの IP アドレスと受信した DHCP syslog メッセージに指定されている IP アドレスでユーザーの照合を試行します。DHCP syslog メッセージから受信したデータが、現在ログインしているユーザーに一致しない場合、メッセージは解析されず、ユーザー ID は配信されません。

DHCP メッセージの詳細情報を適切に照合、解析、マッピングするために必要な遅延は、カスタマイズされたテンプレートには適用できません。したがって、DHCP メッセージテンプレートをカスタマイズすることは推奨されません。代わりに、事前定義の DHCP テンプレートを使用してください。

syslog クライアント設定画面から、syslog メッセージ本文テンプレートを作成および編集します。

（注） 各自でカスタマイズしたテンプレートだけを編集できます。システムに用意されている事前定義テンプレートは変更できません。

ステップ 1 [syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 新しい syslog クライアントを追加するには [追加（Add）] をクリックし、すでに設定されているクライアントを更新するには [編集（Edit）] をクリックします。syslog クライアントの設定と更新については、syslog クライアントの設定 （53 ページ） を参照してください。

ステップ 3 [syslog プロバイダ（Syslog Providers）] ウィンドウで、[新規（New）] をクリックして新しいメッセージテンプレートを作成します。既存のテンプレートを編集するには、ドロップダウンリストからテンプレートを選択して [編集（Edit）] をクリックします。

ステップ 4 必須フィールドをすべて指定します。

値を正しく入力する方法の詳細については、syslog カスタマイズ テンプレートの設定と例 （62 ページ） を参照してください。

ステップ 5 [テスト（Test）] をクリックして、入力した文字列に基づいてメッセージが正しく解析されていることを確認します。

ステップ 6 [保存（Save）] をクリックします。

syslog ヘッダーのカスタマイズ

syslog ヘッダーには、メッセージの送信元のホスト名も含まれています。syslog メッセージが Cisco ISE-PIC メッセージパーサーで認識されない場合は、ホスト名の後に続く区切り文字を設

定し、Cisco ISE-PIC がホスト名を認識してメッセージを正しく解析できるようにすることで、メッセージヘッダーをカスタマイズする必要がある場合があります。この画面のフィールドの詳細については、syslog カスタマイズ テンプレートの設定と例 （62 ページ）を参照してください。カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダー タイプにこの設定が追加されます。

（注） 1 つのヘッダーだけをカスタマイズできます。ヘッダーをカスタマイズした後、[カスタムヘッダー（Custom Header）] をクリックしてテンプレートを作成すると、最新の設定のみが保存されます。

ステップ 1 [syslog プロバイダ（syslog Providers）] テーブルが表示されます。このテーブルには既存の各クライアントのステータス情報が含まれています。

ステップ 2 [カスタム ヘッダー（Custom Header）] をクリックして [syslog カスタム ヘッダー（Syslog Custom Header）] 画面を開きます。

ステップ 3 [サンプル syslog を貼り付ける（Paste sample syslog）] に、syslog メッセージのヘッダー形式の例を入力します。たとえば、メッセージの 1 つからヘッダー **<181>Oct 10 15:14:08 Cisco.com** をコピーして貼り付けます。

ステップ 4 [区切り文字（Separator）] フィールドで、単語をスペースとタブのいずれで区切るかを指定します。

ステップ 5 [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドで、ヘッダーのどの位置がホスト名であるかを指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。

[ホスト名（Hostname）] フィールドに、最初の 3 つのフィールドに示される詳細情報に基づいてホスト名が表示されます。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。

<181>Oct 10 15:14:08 Cisco.com

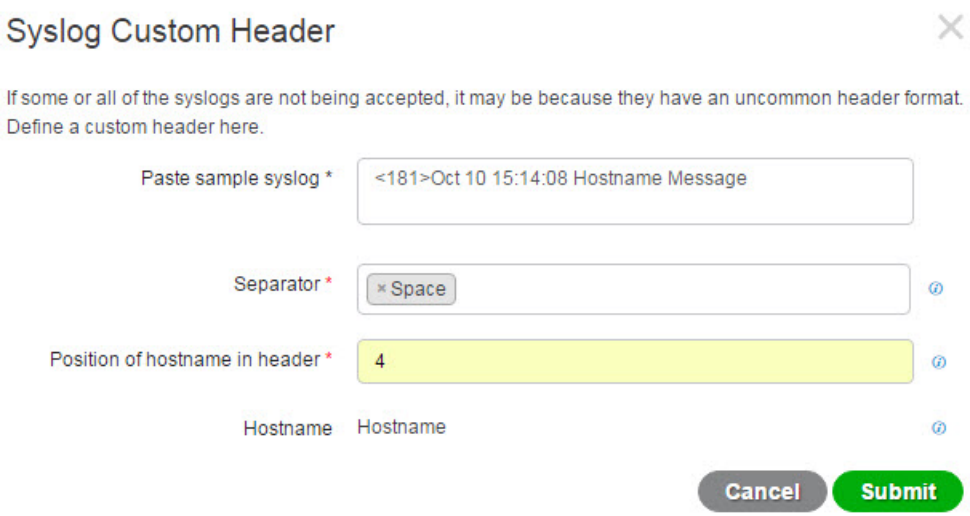
区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。

[ホスト名（Hostname）] には自動的に Cisco.com と表示されます。これは、[syslog の例を貼り付ける（Paste sample syslog）] フィールドに貼り付けたヘッダー フレーズの 4 番目の単語です。

ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

この例を次のスクリーン キャプチャに示します。

図 *6 : syslog* ヘッダーのカスタマイズ



ステップ 6 [送信（Submit）] をクリックします。
カスタマイズされたヘッダーの設定は保存され、メッセージを受信するたびにパーサーが使用するヘッダータイプにこの設定が追加されます。

syslog カスタマイズ テンプレートの設定と例

Cisco ISE-PIC では、ISE-PIC パーサーにより解析される syslog メッセージ テンプレートをカスタマイズできます。カスタマイズされたテンプレートは、新規マッピング メッセージとマッピング削除メッセージの両方に対応する構造を決定します。ISE-PIC パーサーが、メッセージがユーザー ID マッピングを追加するためのメッセージであるかまたは削除するためのメッセージであるかを正しく識別し、ユーザーの詳細情報を正しく解析できるようにするため、テンプレートには、ユーザー名、IP アドレス、MAC アドレス、およびドメインの構造を定義する正規表現が含まれている必要があります。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されます。カスタマイズテンプレートでも正規表現を使用してください。

syslog ヘッダーの各部分

ホスト名の後に続く区切り文字を設定することで、syslog プローブが認識する単一ヘッダーをカスタマイズできます。

次の表に、カスタムsyslogヘッダーに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 17 : カスタマイズ テンプレートの正規表現（65 ページ）を参照してください。

表 *15 : syslog* カスタム ヘッダー

フィールド	説明
syslog の例を貼り付ける（Paste sample syslog）	syslog メッセージにヘッダー形式の例を入力します。たとえば、次のヘッダーをコピーして貼り付けます。 `<181>Oct 10 15:14:08 Hostname Message`
区切り文字（Separator）	単語をスペースまたはタブのいずれで区切るかを指定します。
ヘッダーのホスト名の位置（Position of hostname in header）	ヘッダーでのホスト名の位置を指定します。たとえば、前述のヘッダーではホスト名は 4 番目の単語です。これを指定するには 4 と入力します。
ホストネーム	最初の 3 つのフィールドに示される詳細情報に基づいて、ホスト名を表示します。たとえば、[syslog の例を貼り付ける（Paste sample syslog）] でのヘッダーの例の場合は次のようになります。 <181>Oct 10 15:14:08 Hostname Message 区切り文字として [スペース（Space）] を指定し、[ヘッダーのホスト名の位置（Position of hostname in header）] には 4 を入力します。 [ホスト名（Hostname）] には Hostname が自動的に表示されます。 ホスト名が正しく表示されない場合は、[区切り文字（Separator）] フィールドと [ヘッダーのホスト名の位置（Position of hostname in header）] フィールドに入力したデータを確認してください。

メッセージ本文の syslog テンプレートの各部分と説明

次の表に、カスタマイズ syslog メッセージ テンプレートに組み込むことができるさまざまな部分とフィールドについて説明します。正規表現の詳細については、表 17 : カスタマイズ テンプレートの正規表現 （65 ページ）を参照してください。

表 *16 : syslog* テンプレート

パート	フィールド	説明
	名前	このテンプレートの目的がわかる一意の名前。
マッピング操作	新規マッピング	新しいユーザーを追加するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、F5 VPN にログインした新しいユーザーを示すには、このフィールドに「logged on from」と入力します。
	削除されたマッピング	ユーザーを削除するためにこのテンプレートで使用されるマッピングのタイプを記述する正規表現。たとえば、削除する必要がある ASA VPN のユーザーを示すには、このフィールドに「session disconnect」と入力します。
ユーザーデータ	IPアドレス	キャプチャする IP アドレスを示す正規表現。 たとえば Bluecat メッセージの場合、この IP アドレス範囲内のユーザーの ID をキャプチャするには、次のように入力します。 (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	ユーザー名	キャプチャするユーザー名形式を示す正規表現。
	ドメイン	キャプチャするドメインを示す正規表現。
	MAC アドレス	キャプチャする MAC アドレスの形式を示す正規表現。

正規表現の例

メッセージを解析するため、正規表現を使用します。ここでは、IPアドレス、ユーザー名、およびマッピング追加メッセージを解析する正規表現の例を示します。

たとえば、正規表現を使用して次のメッセージを解析します。

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

次の表に、正規表現の定義を示します。

表 *17*: カスタマイズ テンプレートの正規表現

パート	正規表現
IP アドレス	Address <([^\s]+)>|address ([^\s]+)
ユーザー名 （User name）	User <([^\s]+)>| Username = ([^\s]+)
マッピング追加メッセージ（Add mapping message）	(%ASA-4-722051|%ASA-6-713228)

Syslog 事前定義メッセージテンプレートの使用

syslog メッセージには、ヘッダーとメッセージ本文を含む標準構造があります。

ここでは、メッセージの送信元に基づいてサポートされているヘッダーの内容の詳細や、サポートされている本文の構造など、Cisco ISE-PIC が提供する事前定義テンプレートについて説明します。

また、システムで事前に定義されていないソース用に、カスタマイズした本文コンテンツを使用した独自のテンプレートも作成できます。ここでは、カスタムテンプレートでサポートされる構造について説明します。メッセージの解析時には、システムで事前定義されているヘッダーに加えて、使用する 1 つのカスタマイズヘッダーを設定できます。また、メッセージ本文には、複数のカスタマイズテンプレートを設定できます。ヘッダーのカスタマイズの詳細については、syslog ヘッダーのカスタマイズ （60 ページ） を参照してください。本文のカスタマイズの詳細については、syslog メッセージ本文のカスタマイズ （59 ページ） を参照してください。

（注） ほとんどの事前定義テンプレートでは正規表現が使用されており、カスタマイズテンプレートでも正規表現を使用する必要があります。

メッセージ ヘッダー

パーサーで認識されるヘッダータイプには、すべてのクライアントマシンのすべてのメッセージタイプ（新規および削除）について認識される 2 つのタイプがあります。これらのヘッダーは次のとおりです。

- <171>Host message
- <171>Oct 10 15:14:08 Host message

受信されたヘッダーはホスト名を検出するため解析されます。ホスト名は、IPアドレス、ホスト名、または完全 FQDN のいずれかです。

ヘッダーもカスタマイズできます。ヘッダーをカスタマイズするには、syslog ヘッダーのカスタマイズ （60 ページ）を参照してください。

syslog ASA VPN 事前定義テンプレート

ASA VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

本文メッセージ	解析例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	

本文メッセージ	解析例
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] （注） このメッセージタイプから解析されるIPアドレスは、メッセージに示されているようにプライベートIPアドレスです。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] （注） このメッセージタイプから解析されたIPアドレスはIPv4アドレスです。

マッピング削除本文メッセージ

ここではパーサーでASA VPNのためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.1.1.1]

本文メッセージ
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.

本文メッセージ
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

syslog Bluecat 事前定義テンプレート

Bluecat でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

ここでは、Bluecat syslog で新規マッピングとしてサポートされるメッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

本文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

マッピング削除メッセージ

Bluecat のマッピング削除メッセージはありません。

syslog F5 VPN 事前定義テンプレート

F5 VPN でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな F5 VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=UserA,ip=172.16.0.12]

本文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

マッピング削除メッセージ

現在、F5 VPN でサポートされている削除メッセージはありません。

syslog Infoblox 事前定義テンプレート

Infoblox でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな ASA VPN 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

本文メッセージ
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

マッピング削除メッセージ

受信された本文が解析され、次のようにユーザーの詳細が判明します。

- MAC アドレスが含まれている場合：

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC アドレスが含まれていない場合：

  [10.0.10.100]

本文メッセージ
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

syslog Linux DHCPd3 事前定義テンプレート

Linux DHCPd3 でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング メッセージ

次の表では、パーサーが認識するさまざまな Linux DHCPd3 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

マッピング削除本文メッセージ

ここではパーサーで Linux DHCPd3 のためにサポートされているマッピング削除メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0c:29:a2:18:34 ,10.0.10.100]

本文メッセージ
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

syslog MS DHCP 事前定義テンプレート

MS DHCP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな MS DHCP 本文メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

マッピング削除本文メッセージ

ここではパーサーで MS DHCP のためにサポートされているマッピング削除メッセージについて説明します。

受信すると、パーサーはカンマ（,）を検索してデータを分割し、これらの形式のメッセージが次の例に示すように解析されます。

[macAddress=000C29912E5D,ip=10.0.10.123]

本文メッセージ
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,0

syslog SafeConnect NAC 事前定義テンプレート

SafeConnect NAC でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな SafeConnect NAC 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

本文メッセージ
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

マッピング削除メッセージ

現在、Safe Connect でサポートされている削除メッセージはありません。

syslog Aerohive 事前定義テンプレート

Aerohive でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Aerohive 本文メッセージについて説明します。

本文で解析される詳細には、ユーザー名と IP アドレスがあります。解析に使用される正規表現の例を次に示します。

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,10.5.50.52]

本文メッセージ
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

マッピング削除メッセージ

現在、Aerohive からのマッピング削除メッセージはサポートされていません。

syslog Blue Coat 事前定義テンプレート：Main Proxy、Proxy SG、Squid Web Proxy

Blue Coat の次のメッセージ タイプがサポートされています。

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

BlueCoat メッセージでサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまな Blue Coat 本文メッセージについて説明します。

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[UserA,192.168.10.24]

本文メッセージ（この例は、**BlueCoat** プロキシ **SG** メッセージからの引用です）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

次の表では、新規マッピングメッセージに使用されるクライアント別の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){2,7}[a-zA-Z0-9]{1,})\s** ユーザー名（User name） **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat Proxy SG	新規マッピング **(\-\sPROXIED){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){2,7}[a-zA-Z0-9]{1,})\s[a-zA-Z0-9_]+\s** ユーザー名（User name） **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid Web Proxy	新規マッピング **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,}:){2,7}[a-zA-Z0-9]{1,})\sTCP** ユーザー名（User name） **\s([a-zA-Z0-9\._]+)\s\-\/**

マッピング削除メッセージ

Blue Coat クライアントではマッピング削除メッセージがサポートされていますが、現在利用できる例はありません。

次の表では、マッピング削除メッセージに使用されるクライアント別の既知の正規表現構造について説明します。

クライアント	正規表現
BlueCoat Main Proxy	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	現在利用できる例はありません。
BlueCoat Squid Web Proxy	**(TCP_MISS|TCP_NC_MISS){1}**

syslog ISE および ACS 事前定義テンプレート

パーサーは ISE または ACS クライアントをリッスンするときに、次のメッセージ タイプを受信します。

- 認証成功：ユーザーが ISE または ACS により認証されると、認証が成功したことを通知し、ユーザーの詳細情報を記述した認証成功メッセージが発行されます。このメッセージが解析され、このメッセージのユーザーの詳細とセッション ID が保存されます。
- アカウンティング開始およびアカウンティング更新メッセージ（新規マッピング）：アカウンティング開始メッセージまたはアカウンティング更新メッセージは、認証成功メッセージから保存されたユーザーの詳細とセッション ID を使用して解析され、ユーザーがマッピングされます。
- アカウンティング終了（マッピング削除）：システムからユーザーマッピングが削除されます。

ISE および ACS でサポートされる syslog メッセージの形式とタイプについて説明します。

認証成功メッセージ

認証成功メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **解析例**

  ユーザー名とセッション ID だけが解析されます。

  [UserA,5]

アカウンティング開始/更新（新規マッピング）メッセージ

新規マッピング メッセージとして次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

マッピング削除メッセージ

マッピング削除では次のメッセージがサポートされています。

- **ヘッダー**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  例：<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **本文**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **解析例**

  解析される詳細には、ユーザー名、フレーム IP アドレス、および MAC アドレス（メッセージに含まれている場合）などがあります。

  [UserA,10.0.0.16]

syslog Lucent QIP 事前定義テンプレート

Lucent QIP でサポートされる syslog メッセージの形式とタイプについて説明します。

ヘッダー

パーサーでサポートされるヘッダーはすべてのクライアントで同一です（Syslog 事前定義メッセージテンプレートの使用 （65 ページ）を参照）。

新規マッピング本文メッセージ

次の表では、パーサーが認識するさまざまなLucent QIP本文メッセージについて説明します。

これらのメッセージの正規表現構造を次に示します。

DHCP_GrantLease|:DHCP_RenewLease

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[00:0C:29:91:2E:5D,10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

マッピング削除本文メッセージ

これらのメッセージの正規表現構造を次に示します。

Delete Lease:|DHCP Auto Release:

受信された本文が解析され、次のようにユーザーの詳細が判明します。

[10.0.0.11]

本文メッセージ
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

パッシブ ID サービスのフィルタリング

特定のユーザーを名前やIPアドレスに基づいてフィルタリングできます。たとえばITサービスの管理者が、そのエンドポイントの標準ユーザーを支援するためにエンドポイントにログインする場合、管理者アクティビティをフィルタリングにより除外して[ライブセッション（Live Sessions）]に表示されないようにし、そのエンドポイントの標準ユーザーだけが表示されるようにできます。[ライブ セッション（Live Session）] には、マッピング フィルタでフィルタリングされていないパッシブ ID サービス コンポーネントが表示されます。フィルタは必要なだけ追加できます。「OR」論理演算子をフィルタの間に適用します。両方のフィールドを 1 つのフィルタで指定する場合は、「AND」論理演算子をこれらのフィールドの間に適用します。

ステップ 1 **[プロバイダ（Providers）]** > **[マッピング フィルタ（Mapping Filters）]** を選択します。

ステップ 2 [追加（Add）] をクリックし、フィルタするユーザーのユーザー名や IP アドレスを入力して、[送信（Submit）] をクリックします。

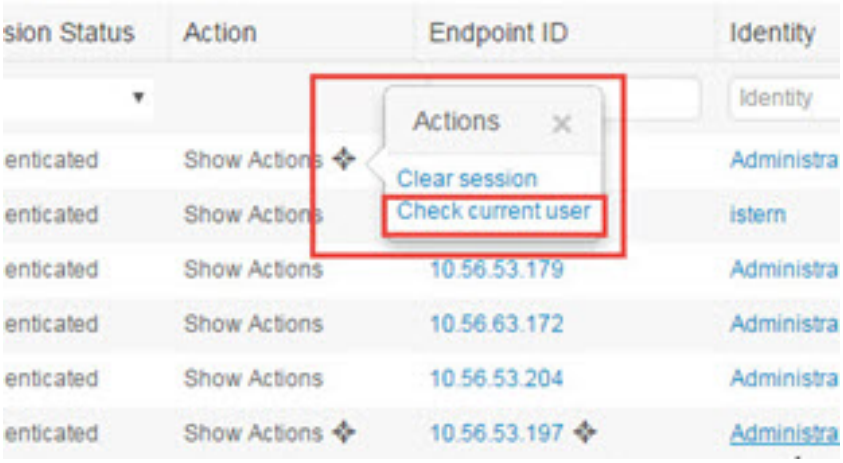
エンドポイント プローブ

設定可能なカスタム プロバイダの他に、インストール完了後にデフォルトで ISE-PICエンドポイント プローブが有効になります。エンドポイント プローブは、特定の各ユーザーがまだシステムにログインしているかどうかを定期的にチェックします。

（注） エンドポイントがバックグラウンドで実行されることを確認するには、まず最初の Active Directory 参加ポイントを設定し、[クレデンシャルの保存（Store Credentials）] を選択していることを確認します。エンドポイントプローブの設定の詳細については、エンドポイントプローブの使用 （78 ページ）を参照してください。

エンドポイントのステータスを手動で確認するには、**[アクション（Actions）]** 列から **[ライブセッション（Live Sessions）]** に移動し、**[アクションを表示（Show Actions）]** をクリックし、次の図に示すように **[現在のユーザーを確認（Check current user）]** を選択します。

図 7: 現在のユーザーの確認



エンドポイント ユーザーのステータスと手動でのチェックの実行の詳細については、ライブセッション （164 ページ）を参照してください。

エンドポイントプローブはユーザーが接続していることを認識します。特定のエンドポイントのセッションが最後に更新された時点から 4 時間経過している場合には、ユーザーがまだログインしているかどうかを確認し、次のデータを収集します。

- MAC アドレス
- オペレーティング システムのバージョン

このチェックに基づいてプローブは次の操作を実行します。

- ユーザーがまだログインしている場合、プローブは Cisco ISE-PIC を [アクティブユーザー（Active User）] ステータスで更新します。
- ユーザーがログアウトしている場合、セッション状態は [終了（Terminated）] に更新され、15 分経過後にユーザーはセッション ディレクトリから削除されます。
- ユーザーと通信できない場合、たとえばファイアウォールによって通信が防止されているか、エンドポイントがシャットダウンしている場合などには、ステータスが [到達不可能（Unreachable）] として更新され、サブスクライバ ポリシーによってユーザーセッションの処理方法が決定します。エンドポイントは引き続きセッション ディレクトリに残ります。

エンドポイント プローブの使用

始める前に

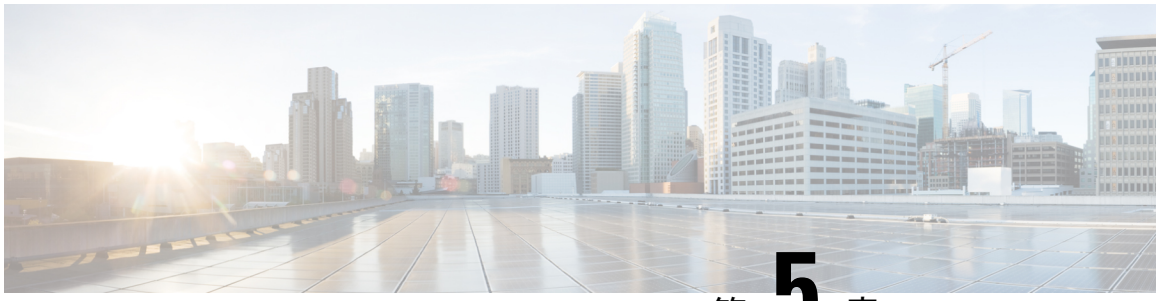
ISE-PIC がインストールされている場合、エンドポイント プローブがデフォルトで有効になっています。プローブを有効または無効にするには、次のように設定していることを確認してください。

- エンドポイントはポート 445 とのネットワーク接続が必要です。
- ISE-PIC で、最初の Active Directory 参加ポイントを設定します。参加ポイントの詳細については、プローブおよびプロバイダとしての Active Directory （19 ページ）を参照してください。

（注） エンドポイントがバックグラウンドで実行するようにするため、最初に 1 番目の Active Directory 参加ポイントを設定する必要があります。これにより、Active Directory プローブが完全に設定されていない場合でもエンドポイント プローブを実行できるようになります。

ステップ 1 **[プロバイダ（Providers）] > [エンドポイント プローブ（Endpoint Probes）]** を選択します。

ステップ 2 [有効（Enabled）] または [無効（Disabled）] を選択します。
画面は変更されません。ただし、選択内容に基づいてプローブが有効化または無効化されます。有効化された場合、プローブはバックグラウンドで稼働しており、データを収集しています。



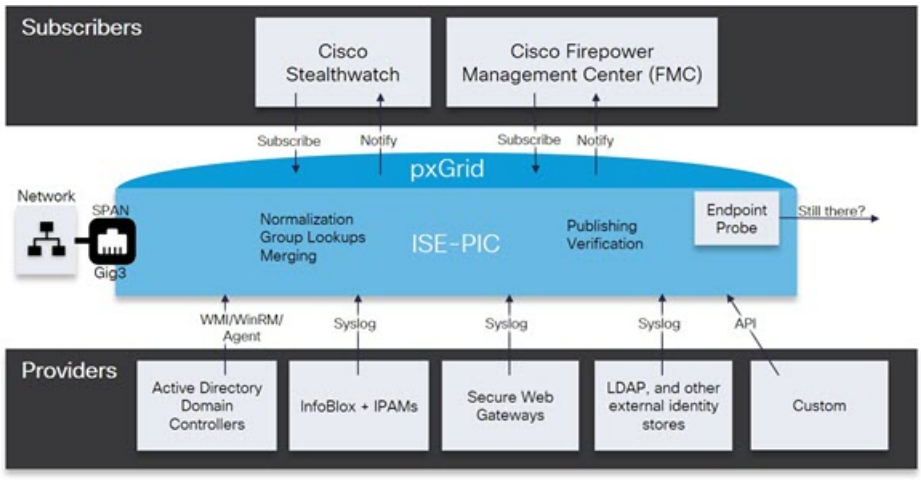
第 5 章

サブスクライバ

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

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

図 *8 : ISE-PIC* フロー



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

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

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

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

1. 必要に応じて、サブスクライバ側から証明書を生成します。
2. ISE-PICからサブスクライバの pxGrid 証明書の生成 （80 ページ）を参照してください。
3. サブスクライバの有効化 （82 ページ）。サブスクライバが ISE-PIC からユーザー ID を受信できるようにするため、このステップを実行するか、承認を自動的に有効にします。サブスクライバの設定 （82 ページ） を参照してください。

- サブスクライバの pxGrid 証明書の生成 （80 ページ）
- サブスクライバの有効化 （82 ページ）
- ライブ ログからのサブスクライバ イベントの表示 （82 ページ）
- サブスクライバの設定 （82 ページ）

サブスクライバの pxGrid 証明書の生成

始める前に

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

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

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

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

ステップ 3 （オプション）この証明書の説明を入力できます。

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

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

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

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

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

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

ステップ 6 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- [Private Enhanced Electronic Mail（PEM）形式の証明書、PKCS8 PEM 形式のキー（証明書チェーンを含む）（Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)）]：ルート証明書、中間 CA 証明書、およびエンドエンティティ証明書は PEM 形式で表されます。PEM 形式の証明書は BASE64 エンコード ASCII ファイルです。各証明書は「-------BEGIN CERTIFICATE-----」タグで始まり、「-----END CERTIFICATE----」タグで終わります。エンドエンティティの秘密キーは PKCS* PEM を使用して格納されています。「-----BEGIN ENCRYPTED PRIVATE KEY----」タグで始まり、「-----END ENCRYPTED PRIVATE KEY----」タグで終わります。

- [PKCS12 形式（証明書チェーンを含む。つまり証明書チェーンとキーの両方で 1 ファイル）（PKCS12 format (including certificate chain; one file for both the certificate chain and key)）]：1 つの暗号化ファイルにルート CA 証明書、中間 CA 証明書、およびエンドエンティティの証明書と秘密キーを格納するバイナリ形式。

ステップ 7 証明書のパスワードを入力します。

ステップ 8 [作成（Create）] をクリックします。

サブスクライバの有効化

サブスクライバが Cisco ISEISE-PIC からユーザー ID を受信できるようにするため、このタスクを実行するか、または承認を自動的に有効にする必要があります。 サブスクライバの設定（82 ページ）を参照してください。

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

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

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

ライブ ログからのサブスクライバ イベントの表示

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

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

サブスクライバの設定

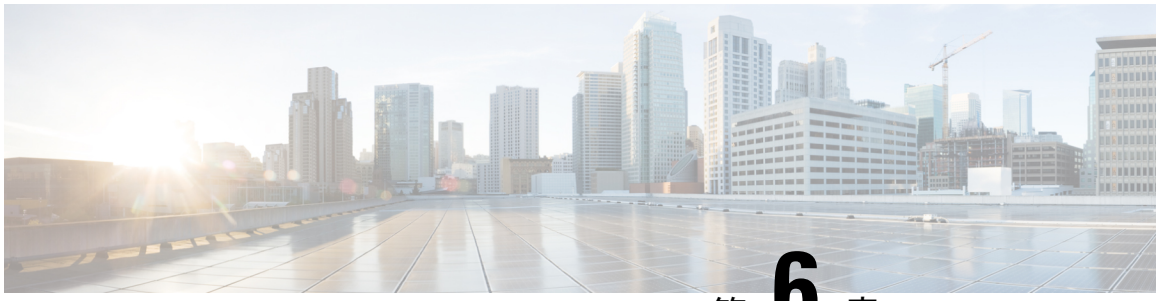
ステップ 1 [サブスクライバ（Subscribers）] を選択し、[設定（Settings）] タブに移動します。

ステップ 2 必要に応じて、次のオプションを選択します。

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

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

ステップ 3 [保存（Save）] をクリックします。



第 6 章

Cisco での証明書の管理 ISE-PIC

証明書は、個人、サーバー、会社、またはその他のエンティティを識別し、そのエンティティを公開キーに関連付ける電子文書です。公開キーインフラストラクチャ（PKI）は、セキュアな通信を可能にし、デジタル署名を使用してユーザーの ID を確認する暗号化技術です。証明書は、ネットワークに対するセキュアなアクセスを提供するために使用されます。証明書は、自己署名するか、外部の認証局（CA）がデジタル署名できます。自己署名証明書は、独自の作成者によって署名されます。CA 署名付きデジタル証明書は業界標準と見なされており、より安全です。ISE-PIC は pxGrid の外部 CA として機能し、pxGrid サブスクライバの pxGrid 証明書にデジタル署名できます。

Cisco ISE-PIC は、ノード間通信（各ノードが相互に通信するためにもう一方のノードに証明書を提示する）や pxGrid との通信（ISE-PIC と pxGrid が相互に証明書を提示する）のために証明書を使用します。これら 2 つの目的それぞれに、1 つの証明書をノードごとに生成できます。証明書は pxGrid に対して Cisco ISE ノードを識別し、pxGrid と Cisco ISE ノード間の通信を確保します。

インストール時に、ISE-PIC は ISE-PIC ノードごとの自己署名証明書（インストール時に管理者はプライマリノードからセカンダリノーそに対して自動的に生成された証明書を承認するように求められます）と、プライマリ ISE-PIC ノードによってデジタル署名された pxGrid サービス用の証明書が自動的に生成されます。その後、pxGrid とサブスクライバの間の相互信頼を保証するため、pxGrid サブスクライバの証明書を生成できます。これにより、ISE-PIC からサブスクライバにユーザー ID を渡すことが可能になります。ISE-PIC の [証明書（Certificate）] メニューは、証明書の表示、追加の ISE-PIC 証明書の生成、および一部の高度なタスクの実行に使用できます。

（注） 管理者は企業証明書を使用できますが、デフォルトでは、サブスクライバの pxGrid 証明書の発行には内部認証局を使用するように ISE-PIC は設計されています。

• 証明書署名要求 （100 ページ）
• Cisco ISE CA サービス （108 ページ）
• OCSP サービス （117 ページ）

Cisco ISE-PIC の証明書の一致

展開内でCisco ISE-PICノードをセットアップすると、ノードが相互に通信します。システムは各ISE-PICノードのFQDNを調べ、FQDNが一致することを確認します（たとえばise1.cisco.comとise2.cisco.com、またはワイルドカード証明書を使用している場合は*.cisco.com）。また、外部マシンからCisco ISE-PICサーバーに証明書が提示される場合、認証のために提示される外部証明書が、Cisco ISE-PICサーバーの証明書と照合されます。2つの証明書が一致すると、認証は成功します。

Cisco ISE-PIC は、サブジェクト名の一致を次のようにして確認します。

1. Cisco ISE-PIC により証明書のサブジェクト代替名の拡張が確認されます。サブジェクト代替名に 1 つ以上の DNS 名が含まれている場合は、それらの DNS 名の 1 つが Cisco ISE ノードの FQDN に一致している必要があります。ワイルドカード証明書が使用されている場合、ワイルドカード ドメイン名は Cisco ISE ノードの FQDN ドメインに一致している必要があります。
2. サブジェクト代替名に DNS 名が存在しない場合、またはサブジェクト代替名全体が欠落している場合は、証明書の **[サブジェクト（Subject）]** フィールドの一般名または証明書の **[サブジェクト（Subject）]** フィールドのワイルドカードドメインが、ノードのFQDNに一致している必要があります。
3. 一致しない場合、証明書は拒否されます。

ワイルドカード証明書

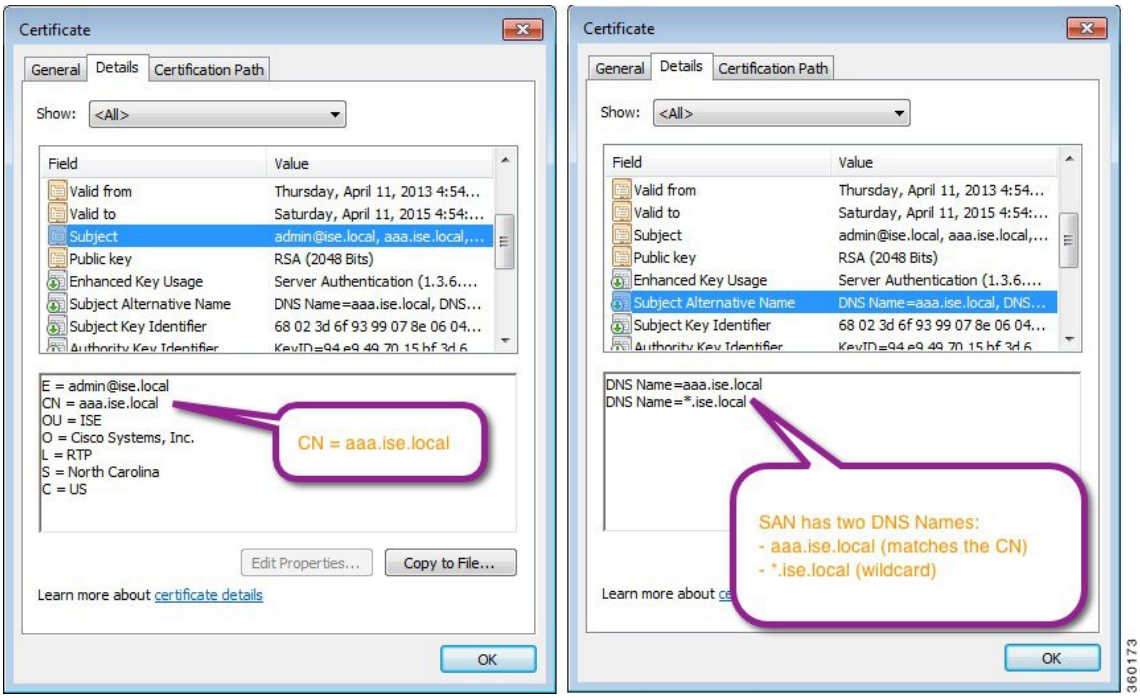
ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用しており、組織内の複数のホスト間で証明書を共有できます。たとえば、証明書サブジェクトの [CN] 値は aaa.ise.local などの汎用ホスト名であり、SAN フィールドには、同じ汎用ホスト名と DNS.1=aaa.ise.local や DNS.2=*.ise.local などのワイルドカード表記が含まれます。

psn.ise.local のように、*.ise.local を使用してワイルドカード証明書を設定すると、その同じ証明書を使用して、次のようなDNS名が「.ise.local」で終了する他のすべてのホストを保護することができます

ワイルドカード証明書は通常の証明書と同じ方法で通信を保護し、要求は同じ検証方式を使用して処理されます。

次の図に、Web サイトの保護に使用されるワイルドカード証明書の例を示します。

図 *9*：ワイルドカード証明書の例



SAN フィールドでアスタリスク（*）を使用すると、（複数のノードをインストールしている場合は）すべてのノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバー証明書を個別に割り当てる場合よりも安全性が低いと見なされます。

（注） FQDN の例の一部は、ISE のフル インストールの例であるため、ISE-PIC のインストールに関連するアドレスとは異なることがあります。

ワイルドカード証明書を使用する利点

- コスト削減：サードパーティ CA によって署名された証明書は、特にサーバーの数が増えると高額になります。ワイルドカード証明書は、Cisco ISE 展開内の複数ノードで使用できます。
- 運用効率：ワイルドカード証明書により、すべての PSN が EAP と Web サービス用に同じ証明書を共有できます。証明書を 1 回作成して、すべての PSN に適用することにより、コストを大幅に削減できるだけでなく、証明書の管理も簡素化されます。
- 認証エラーの削減：ワイルドカード証明書は、クライアントがプロファイル内に信頼できる証明書を保存しており、そのクライアントが iOS のキーチェーン（署名ルートが信頼されている）に従っていない Apple iOS デバイスで発生する問題に対処します。iOS クライアントが最初に PSN と通信する際、このクライアントはその PSN の証明書を（信頼でき

る CA が署名している場合でも）明示的に信頼しません。ワイルドカード証明書を使用すると、この証明書がすべての PSN で同一になるため、ユーザーは証明書の受け入れを 1 回行えばよく、その後の異なる PSN に対する認証はエラーやプロンプトが表示されることなく進行します。

- 簡略化されたサプリカントの設定：たとえば、PEAP-MSCHAPv2 と信頼できるサーバー証明書がある Microsoft Windows サプリカントでは、各サーバー証明書を信頼するように指定することが必要とされており、そのように指定しない場合は、そのクライアントが別の PSN を使用して接続を行うと、各 PSN 証明書を信用するように、ユーザーにプロンプトが出される可能性があります。ワイルドカード証明書を使用すると、各 PSN の個別の証明書ではなく、単一のサーバー証明書を信頼するだけで済みます。
- ワイルドカード証明書を使用すると、プロンプトの提示が減り、よりシームレスな接続が実現されることにより、ユーザー エクスペリエンスが改善されます。

ワイルドカード証明書を使用することの欠点

次に、ワイルドカード証明書の使用に関連するセキュリティ上の考慮事項の一部を説明します。

- 監査性と否認防止性の低下
- 秘密キーの露出の増加
- 一般的ではなく、管理者により理解されていない

ワイルドカード証明書は各 Cisco ISE ノードで固有のサーバー証明書を使用するよりも安全性が低いと見なされています。ただし、コスト、およびその他の運用関連の要因がセキュリティリスクに勝っています。

Cisco 適応型セキュリティアプライアンスなどのセキュリティデバイスも、ワイルドカード証明書をサポートしています。

ワイルドカード証明書を展開する場合には注意が必要です。たとえば、*.company.local を使用して証明書を作成したとします。該当の秘密キーを攻撃者が回復できた場合、攻撃者は company.local ドメイン内のすべてのサーバーをスプーフィングすることができます。したがって、このタイプの危険を回避するために、ドメイン領域を分割することがベストプラクティスと見なされています。

この想定される問題に対処し、利用範囲を制限するために、ワイルドカード証明書を使用して組織の特定のサブドメインを保護することもできます。ワイルドカードを指定する一般名のサブドメイン領域に、アスタリスク（*）を追加します。

たとえば、*.ise.company.local に対してワイルドカード証明書を設定すると、その証明書は次のような、DNS 名が「.ise.company.local」で終わるすべてのホストを保護するために使用できます。

- psn.ise.company.local
- mydevices.ise.company.local

• sponsor.ise.company.local

ワイルドカード証明書の互換性

ワイルドカード証明書は通常、証明書サブジェクトの共通名としてリストされているワイルドカードを使用して作成されます。Cisco ISE は、このタイプの作成をサポートします。ただし、すべてのエンドポイントサプリカントが証明書サブジェクトのワイルドカード文字をサポートしているわけではありません。

テスト済みのすべての Microsoft ネイティブサプリカント（販売が終了している Windows Mobile を含む）の一部は、証明書サブジェクトのワイルドカード文字をサポートしていません。

Cisco AnyConnect Network Access Manager など、[サブジェクト（Subject）] フィールドでのワイルドカード文字の使用をサポートできる他のサプリカントを使用できます。

また、DigiCert の Wildcard Plus など、証明書のサブジェクト代替名に特定のサブドメインを含めることで、互換性のないデバイスを使用するように設計された、特別なワイルドカード証明書を使用することもできます。

Microsoft サプリカントの制限はワイルドカード証明書の使用にとって妨げになるように見えますが、Microsoft のネイティブサプリカントを含む、セキュアなアクセスについてテスト済みのすべてのデバイスを使用できるようにする代替の方法があります。

これを行うには、サブジェクトにワイルドカード文字を使用する代わりに、[サブジェクト代替名（Subject Alterative Name）] フィールドでワイルドカード文字を使用する必要があります。[サブジェクト代替名（Subject Alternative Name）] フィールドには、ドメイン名（DNS 名）を確認するように指定された拡張子が保持されます。詳細については、RFC 6125 と RFC 2128 を参照してください。

ISE-PIC での証明書階層

管理ISE-PICポータルには、すべての証明書の証明書階層または信頼書信頼チェーンが表示されます。証明書階層には、証明書、すべての中間 CA 証明書、およびルート証明書が含まれています。たとえば、管理ISE-PICポータルからシステム証明書を表示すると、デフォルトの対応するシステム証明書の詳細が表示されます。証明書階層は、証明書の上部に表示されます。詳細を表示するには、その階層で証明書をクリックします。自己署名証明書には階層または信頼チェーンがありません。

証明書のリストウィンドウで、[ステータス（Status）] 列に次のアイコンのいずれかが表示されます。

- 緑色のアイコン：有効な証明書（有効な信頼チェーン）を示します。
- 赤色のアイコン：エラーを示します（たとえば、信頼証明書の欠落または期限切れ）。
- 黄色のアイコン：証明書が期限切れ間近であることを警告し、更新処理を求めます。

システム証明書

Cisco ISE-PIC システム証明書は、展開内のその他のノードおよびクライアントアプリケーションに対して Cisco ISE-PIC ノードを識別するサーバー証明書です。システム証明書にアクセスするには、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[システム証明書（System Certificates）]** を選択します。システム証明書の用途は次のとおりです。

- Cisco ISE-PIC 展開でノード間通信に使用されます。これらの証明書の[使用方法（Usage）]領域で[管理（Admin）]チェックボックスをオンにします。
- pxGrid コントローラとの通信に使用されます。これらの証明書の [使用方法（Usage）] 領域の [pxGrid] チェックボックスをオンにします。

Cisco ISE-PIC 展開の各ノードに有効なシステム証明書をインストールします。デフォルトでは、インストール時に Cisco ISE-PIC ノードに 2 つの自己署名証明書と、内部 Cisco ISE CA により署名された 1 つの証明書が作成されます。

- [管理（Admin）] および [pxGrid] を使用するための自己署名サーバー証明書（キー サイズは 2048 で 1 年間有効です）。
- SAML ID プロバイダとの安全な通信に使用できる自己署名 SAML サーバー証明書（キー サイズは 2048 で 1 年間有効です）。
- pxGrid クライアントとの安全な通信に使用できる内部 Cisco ISE CA 署名付きサーバー証明書（キー サイズは 4096 で 1 年間有効です）。

展開をセットアップし、セカンダリノードを登録すると、pxGrid コントローラ用の証明書が自動的にプライマリノードの CA 署名付き証明書に置き換わります。したがってすべての pxGrid 証明書が同一 PKI トラスト階層の一部となります。

お使いのリリースでサポートされているキーと暗号については、該当バージョンの『 Cisco Identity Services Engine ネットワークコンポーネントの互換性 』ガイドを参照してください。

セキュリティを強化するために、自己署名証明書を CA 署名付き証明書で置き換えることを推奨します。CA 署名付き証明書を取得するには、以下を行う必要があります。

1. 証明書署名要求の作成と認証局への送信 （101 ページ）
2. 信頼できる証明書ストアへのルート証明書のインポート （98 ページ）
3. 証明書署名要求への CA 署名付き証明書のバインド （101 ページ）

システム証明書の表示

[システム証明書（System Certificate）] ウィンドウに、Cisco ISE-PIC に追加されたすべてのシステム証明書のリストが表示されます。

ステップ 1 **[証明書（Certificates）] > [システム証明書（Certificates）]** を選択します。

ステップ 2 [システム証明書（System Certificates）] ウィンドウには、次の列が表示されます。

- [フレンドリ名（Friendly Name）]：証明書の名前。
- [使用方法（Usage）]：この証明書が使用されるサービス。
- [ポータルグループタグ（Portal group tag）]：ポータルを使用するように指定された証明書に対してのみ適用できます。このフィールドはポータルに使用する必要がある証明書を指定します。
- [発行先（Issued To）]：証明書のサブジェクトの共通名。
- [発行元（Issued By）]：証明書発行者の共通名
- [有効期限の開始（Valid From）]：証明書の作成日付（「Not Before」証明書属性）。
- [期限日（Expiration Date）]：証明書の有効期限（「Not After」証明書属性）。有効期限の横に次のアイコンが表示されます。
  - 緑色のアイコン：期限切れまで 91 日以上。
  - 青色のアイコン：期限切れまで 90 日以内。
  - 黄色のアイコン：期限切れまで 60 日以内。
  - オレンジ色のアイコン：期限切れまで 30 日以内。
  - 赤色のアイコン： 期限切れ。

システム証明書のインポート

管理者ポータルから、任意の Cisco ISE-PIC ノードのシステム証明書をインポートできます。

（注） プライマリ PAN 上の管理者ロール証明書の証明書を変更すると、他のすべてのノード上のサービスが再起動されます。プライマリ PAN の再起動が完了すると、システムによって一度に 1 つのノードが再起動されます。

始める前に

- クライアントブラウザで実行しているシステムに、システム証明書と秘密キーファイルがあることを確認します。
- インポートするシステム証明書が外部 CA によって署名されている場合は、関連するルート CA および中間 CA の証明書を信頼できる証明書ストアにインポートします（**[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**）。

- インポートするシステム証明書に、CA フラグが true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、およびkeyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。
[証明書インポートウィザード（Certificate Import Wizard）] ウィンドウが表示されます。

ステップ 3 インポートする証明書の値を入力します。

ステップ 4 **[送信（Submit）]** をクリックします。

自己署名証明書の生成

自己署名証明書を生成することで、新しいローカル証明書を追加します。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境にCisco ISE-PICを展開することを計画している場合は、可能な限り CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

（注） 自己署名証明書を使用しており、Cisco ISE-PIC ノードのホスト名を変更する場合は、 Cisco ISE-PIC ノードにログインし、古いホスト名が使用されている自己署名証明書を削除してから、新しい自己署名証明書を生成します。そうしないと、Cisco ISE-PIC は古いホスト名が使用された自己署名証明書を引き続き使用します。

システム証明書の編集

このウィンドウを使用して、システム証明書を編集し、自己署名証明書を更新します。ワイルドカード証明書を編集すると、変更が展開内のすべてのノードに複製されます。ワイルドカード証明書を削除した場合、そのワイルドカード証明書は展開内のすべてのノードから削除されます。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 自己署名証明書を更新するには、**[更新期間（Renewal Period）]** チェックボックスをオンにして、有効期限 TTL（存続可能時間）を日、週、月、または年単位で入力します。ドロップダウンリストから必要な値を選択します。

ステップ 4 [保存（Save）] をクリックします。

[管理者（Admin）] チェックボックスがオンになっている場合、Cisco ISE-PICノードのアプリケーションサーバーが再起動します。

（注） Chrome 65 以上を使用して Cisco ISE を起動すると、URL が正しくリダイレクトされたにもかかわらず、BYOD ポータルまたはゲストポータルがブラウザで起動に失敗することがあります。これは、すべての [サブジェクトの別名（Subject Alternative Name）] フィールドに証明書を必要とする、Google で導入された新しいセキュリティ機能が原因です。Cisco ISE リリース 2.4 以降の場合、[サブジェクトの別名（Subject Alternative Name）] フィールドを入力する必要があります。

Chrome 65 以上で起動するには、次の手順に従います。

1. [サブジェクトの別名（Subject Alternative Name）] フィールドに入力することで、Cisco ISE GUI から新しい自己署名証明書を生成します。DNS と IP アドレスの両方を入力する必要があります。

2. Cisco ISE サービスが再起動します。

3. Chrome ブラウザでポータルにリダイレクトされます。

4. ブラウザで [証明書の表示（View Certificate）] > [詳細（Details）] > [コピー（Copy）] の順に選択し、base-64 エンコードを選択して、証明書をコピーします。

5. 高信頼パスで証明書をインストールします。

6. Chrome ブラウザを終了し、ポータルのリダイレクトを試みます。

（注） Win RS4 または RS5 のオペレーティングシステムでブラウザ Firefox 64 以降のリリースのワイヤレス BYOD セットアップを設定する場合は、証明書の例外を追加することができない場合があります。この現象は Firefox 64 以降のリリースの新規インストール時に発生することがあります。以前のバージョンから Firefox 64 以降にアップグレードした場合は発生しません。次の手順では、このような場合でも証明書の例外を追加することができます。

1. BYOD フローのシングル PEAP またはデュアル PEAP または TLS を設定します。
2. Windows のすべてのオプションで CP ポリシーを設定します。
3. エンドクライアント Windows RS4 または Windows RS5 で、Dot1.x または MAB SSID に接続します。
4. ゲストポータルまたは BYOD ポータルにリダイレクトするには、FF64 ブラウザに 何らか URL を入力します。
5. **[例外を追加（Add Exception）] > [証明書を追加できない（Unable to add certificate）]** をクリックし、フローを続行します。

回避策として、Firefox 64 の証明書を手動で追加します。Firefox 64 のブラウザで、**[オプション（Options）] > [プライバシー&設定（Privacy & Settings）] > [証明書の表示（View Certificates）] > [サーバー（Servers）] > [例外の追加（Add Exception）]** を選択します。

システム証明書の削除

今後使用しないシステム証明書を削除できます。

システム証明書ストアから複数の証明書を一度に削除できますが、管理認証に使用する証明書を少なくとも 1 つ所有する必要があります。また、管理または pxGrid コントローラに使用される証明書は削除できません。ただし、サービスがディセーブルの場合は、pxGrid 証明書を削除できます。

ワイルドカード証明書を削除することを選択した場合、証明書は展開内のすべての Cisco ISE ノードから削除されます。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]**を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

システム証明書のエクスポート

システム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

ステップ 1 **[証明書（Certificates）] > [システム証明書（System Certificates）]**を選択します。の順に選択します。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、**[エクスポート（Export）]** をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント　値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他の Cisco ISE ノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE-PIC ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）] をクリックして、クライアント ブラウザを実行しているファイル システムに証明書を保存します。

証明書のみをエクスポートする場合、証明書はPEM形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書はPEM形式の証明書と暗号化された秘密キーファイルを含む.zip ファイルとしてエクスポートされます。

信頼できる証明書ストア

信頼できる証明書ストアには、信頼に使用される、Simple Certificate Enrollment Protocol（SCEP）用の X.509 証明書が含まれています。

X.509 証明書が有効なのは、指定された特定の日付までのみです。信頼できる証明書が期限切れになった場合、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、システム証明書の有効期間の残りについて通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限のステータスアイコンが、[システム証明書（System Certificates）] ウィンドウに表示されます。
- 有効期限メッセージは、Cisco ISE システム診断レポート（**[操作（Operations）] > [レポート（Reports）] > [レポート（Reports）] > [診断（Diagnostics）] > [システム診断（System Diagnostic）]**）に表示されます

- 有効期限のアラームは、有効期限の 90 日前、60 日前、および 30 日前に生成され、有効期限前の最後の 30 日間には毎日生成されます。

失効した証明書が自己署名証明書の場合は、この証明書を編集して有効期限を延長できます。CA 署名付き証明書の場合は、CA から新しい証明書を取得するのに十分な期間を確保する必要があります。

Cisco ISE は、次の目的で信頼できる証明書を使用します。

- エンドポイントによる認証と、証明書ベースの管理者認証を使用してISE-PICアクセスする Cisco ISE 管理者による認証に使用するクライアント証明書を確認するため。
- 展開内の Cisco ISE-PIC ノード間のセキュアな通信を可能にするため。信頼できる証明書ストアには、展開内の各ノードのシステム証明書との信頼を確立するために必要な CA 証明書のチェーンが含まれている必要があります。
  - 自己署名証明書をシステム証明書に使用する場合は、各ノードの自己署名証明書を PAN の信頼できる証明書ストアに配置する必要があります。
  - CA署名付き証明書をシステム証明書に使用する場合は、CAルート証明書と信頼チェーン内のすべての中間証明書も PAN の信頼できる証明書ストアに配置する必要があります。

（注）
- Cisco ISE にインポートされる X.509 証明書は、PEM 形式か、または識別符号化規則形式である必要があります。証明書チェーン（システム証明書およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。
- ゲストポータルに公開ワイルドカード証明書を割り当て、ルート CA 証明書を使用してサブ CA をインポートする場合、Cisco ISE サービスが再起動されるまで証明書チェーンは送信されません。

インストール時に、自動的に生成された信頼できる証明書が、信頼できる証明書ストアに取り込まれます。ルート証明書（Cisco Root CA）は、製造業者（Cisco CA Manufacturing）証明書に署名します。

信頼できる証明書の命名の制約

CTL の信頼できる証明書には名前の制約の拡張が含まれている場合があります。この拡張は、証明書チェーンの後続のすべての証明書のサブジェクト名とサブジェクト代替名フィールドの値の名前空間を定義します。Cisco ISE は、ルート証明書で指定された制約を検査しません。

Cisco ISE は、次の名前の制約をサポートしています。

- ディレクトリ名

ディレクトリ名の制約は、サブジェクトのディレクトリ名またはサブジェクトの別名フィールドのプレフィクスです。次に例を示します。

- 正しいサブジェクト プレフィクス：

  CA 証明書の名前の制約：Permitted: O=Cisco

  クライアント証明書のサブジェクト：O=Cisco,CN=Salomon

- 不正なサブジェクト プレフィクス：

  CA 証明書の名前の制約：Permitted: O=Cisco

  クライアント証明書のサブジェクト：CN=Salomon,O=Cisco

- DNS
- E メール
- URI（URI の制約は、http://、https://、ftp://、または ldap:// のような URI プレフィクスで始まる必要があります）。

Cisco ISE は、次の名前の制約をサポートしていません。

- IPアドレス
- OtherName

信頼できる証明書にサポートされていない制約が含まれており、検証中の証明書に該当のフィールドが含まれていない場合は、Cisco ISE がサポートされない制約を検証できないため、その証明書は拒否されます。

信頼できる証明書内の名前の制約の定義例を次に示します。

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                 DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100

                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

受け入れ可能なクライアント証明書のサブジェクトは、次のように上記の定義に一致します。

```
          Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

信頼できる証明書の表示

[信頼できる証明書（Trusted Certificates）] ウィンドウに、Cisco ISE-PIC で使用可能なすべての信頼できる証明書が一覧表示されます。

ステップ 1 すべての証明書を表示するには、**[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択しますを選択します。表示される [信頼できる証明書（Trusted Certificates）] ウィンドウにはすべての信頼できる証明書のリストが表示されます。

ステップ 2 [信頼できる証明書（Trusted Certificate）] のチェックボックスをオンにし、[編集（Edit）]、[表示（View）]、[エクスポート（Export）]、または [削除（Delete）] をクリックして必要なタスクを実行します。

信頼できる証明書ストアの証明書のステータス変更

証明書のステータスが有効になっている必要があります。これにより、Cisco ISE-PIC が信頼の確立にこの証明書を使用できるようになります。証明書が信頼できる証明書ストアにインポートされると、この証明書は自動的に有効になります。

信頼できる証明書ストアへの証明書の追加

[信頼できる証明書ストア（Trusted Certificate Store）] ウィンドウでは、Cisco ISE-PIC に CA 証明書を追加できます。

始める前に

- 追加する証明書は、ブラウザを実行しているコンピュータのファイルシステムにある必要があります。証明書は PEM または DER 形式である必要があります。
- 管理者認証または EAP 認証に証明書を使用するには、基本的な制約を証明書内に定義し、CA フラグを true に設定します。

信頼できる証明書の編集

証明書を信頼できる証明書ストアに追加したら、[編集（Edit）] のオプションを使用して、その証明書をさらに編集できます。

ステップ 1 **[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 3 （オプション）[フレンドリ名（Friendly Name）] フィールドに証明書の名前を入力します。フレンドリ名を指定しない場合、デフォルト名は次の形式で生成されます。

common-name#issuer#nnnnn

ステップ 4 [信頼先（Trusted For）] 領域で必要なチェックボックスをオンにして、証明書の用途を定義します。

ステップ 5 （オプション）[説明（Description）] フィールドに、証明書の説明を入力します。

ステップ 6 [保存（Save）] をクリックします。

信頼できる証明書の削除

今後使用しない信頼できる証明書を削除できます。ただし、Cisco ISE-PIC 内部 CA 証明書は削除しないでください。Cisco ISE-PIC 内部 CA 証明書を削除できるのは、展開全体の Cisco ISE-PIC ルート証明書チェーンを置き換える場合のみです。

ステップ 1 **[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 削除する証明書の隣にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。

警告メッセージが表示されます。Cisco ISE-PIC 内部 CA 証明書を削除するには、次のいずれかのオプションをクリックします。

- [削除（Delete）]：Cisco ISE-PIC 内部 CA 証明書を削除する場合。Cisco ISE-PIC 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークに参加できません。エンドポイントをネットワークで再度有効にするには、信頼できる証明書ストアに同じ Cisco ISE-PIC 内部 CA 証明書をインポートします。
- [削除および取消（Delete & Revoke）]：Cisco ISE-PIC 内部 CA 証明書を削除して取り消します。Cisco ISE-PIC 内部 CA によって署名されたすべてのエンドポイント証明書は無効になり、エンドポイントはネットワークにアクセスできません。この操作は取り消すことができません。展開全体の Cisco ISE-PIC ルート証明書チェーンを置き換える必要があります。

ステップ 3 [はい（Yes）] をクリックして、証明書を削除します。

信頼できる証明書ストアからの証明書のエクスポート

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

（注） 内部 CA から証明書をエクスポートし、そのエクスポートされた証明書を使用してバックアップから復元する場合は、CLI コマンド **application configure ise** を使用する必要があります。Cisco ISE CA 証明書およびキーのエクスポート （115 ページ）を参照してください。

ステップ 1 **[証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]**

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 3 選択した証明書は、クライアントブラウザを実行しているファイルシステムに PEM 形式でダウンロードされます。

信頼できる証明書ストアへのルート証明書のインポート

ルート CA 証明書および中間 CA 証明書をインポートするとき、信頼できる CA 証明書を使用する対象のサービスを指定できます。

外部ルート CA 証明書をインポートするときに、次のタスクのステップ 5 で、[管理者認証に基づく証明書への信頼（Trust for certificate based admin authentication）] オプションを有効にします。

始める前に

証明書署名要求に署名し、デジタルで署名された CA 証明書を返した CA のルート証明書と他の中間証明書が必要です。

ステップ 1 **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [証明書ストアへの新しい証明書のインポート（Import a new Certificate into the Certificate Store）] ウィンドウで、[ファイルの選択（Choose File）] をクリックし、CA によって署名され、返されたルート CA 証明書を選択します。

ステップ 4 **[フレンドリ名（Friendly Name）]**を入力します。

[フレンドリ名（Friendly Name）]を入力しないと、Cisco ISE-PIC により、このフィールドには、*common-name#issuer#nnnnn* 形式（、*nnnnn* は一意の番号）で名前が自動的に入力されます。後で証明書を編集して、[フレンドリ名（Friendly Name）] を変更できます。

ステップ 5 この信頼できる証明書を使用するサービスの横にあるチェックボックスをオンにします。

ステップ 6 （任意）[説明（Description）] フィールドに証明書の説明を入力します。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

信頼できる証明書ストアに中間 CA 証明書をインポートします（該当する場合）。

証明書チェーンのインポート

証明書ストアから受信した証明書チェーンを含む単一のファイルから、複数の証明書をインポートすることができます。ファイル内のすべての証明書は PEM の形式であり、証明書は次の順序に並べられている必要があります。

- ファイル内の最後の証明書は、CAによって発行されたクライアント証明書またはサーバー証明書である必要があります。
- 前にあるすべての証明書は、ルート CA 証明書と、発行された証明書の署名のチェーンにあるすべて中間 CA 証明書である必要があります。

証明書チェーンのインポートは、次の 2 ステップのプロセスです。

1. Cisco ISE 管理ポータルで信頼できる証明書ストアに証明書チェーンファイルをインポートします。この操作により、最後の 1 つを除き、すべての証明書がファイルから信頼できる証明書ストアにインポートされます。
2. CA 署名付き証明書のバインド操作を使用して証明書チェーン ファイルをインポートします。この操作により、最後の証明書がローカル証明書としてファイルからインポートされます。

信頼できる証明書のインポート設定

表 *18 :* 信頼できる証明書のインポート設定

フィールド名	説明
証明書ファイル（**Certificate file**）	[参照（Browse）] をクリックして、ブラウザを実行しているコンピュータから証明書ファイルを選択します。
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。名前を指定しない場合は、Cisco ISE-PIC により <common name>#<issuer>#<nnnnn> の形式で自動的に名前が作成されます。ここで、<nnnnn> は固有の 5 桁の数値です。
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書を（他の ISE-PIC ノードまたは LDAP サーバーから）サーバー証明書の検証に使用する場合は、このチェックボックスをオンにします。

フィールド名	説明
クライアント認証および syslog 用に信頼する（**Trust for client authentication and Syslog**）	（[ISE-PIC 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した ISE-PIC に接続するエンドポイントの認証 • syslog サーバーの信頼
シスコ サービスの認証用に信頼する（**Trust for authentication of Cisco Services**）	フィードサービスなどの外部シスコ サービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書の拡張の検証（**Validate Certificate Extensions**）	（[クライアント認証用に信頼する（Trust for client authentication）] オプションと [証明書拡張の検証を有効にする（Enable Validation of Certificate Extensions）] オプションの両方をオンにした場合のみ）「keyUsage」拡張が存在し、「keyCertSign」ビットが設定されていることと、CA フラグが true に設定された基本制約拡張が存在することを確認します。
説明（**Description**）	任意で説明を入力します。

関連トピック

信頼できる証明書ストア （93 ページ）
証明書チェーンのインポート （99 ページ）
信頼できる証明書ストアへのルート証明書のインポート （98 ページ）

証明書署名要求

CA が署名付き証明書を発行するには、証明書署名要求を作成して CA に送信する必要があります。

作成した証明書署名要求のリストは、**[証明書署名要求（Certificate-Signing Requests）]** ウィンドウに表示されます。**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[証明書署名要求（Certificate-Signing Requests）]** を選択します。CA から署名を取得するには、証明書署名要求をエクスポートし、その証明書を CA に送信する必要があります。証明書は CA によって署名され、返されます。

Cisco ISE の管理ポータルから証明書を一元的に管理できます。展開内のすべてのノードの証明書署名要求を作成し、それらをエクスポートできます。その後、証明書署名要求を CA に送

信し、CA から署名付き証明書を取得し、CA によって返されたルートおよび中間 CA 証明書を信頼できる証明書ストアにインポートし、証明書署名要求に CA 署名付き証明書をバインドする必要があります。

証明書署名要求の作成と認証局への送信

証明書署名要求（CSR）を生成して、展開内のノードの CA 署名付き証明書を取得できます。展開内の特定のノードまたは展開内のすべてのノード用の証明書署名要求（CSR）を生成できます。

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 **[証明書署名要求（CSR）の生成（Generate Certificate-Signing Requests (CSR)）]** をクリックして、証明書署名要求を生成します。

ステップ 3 証明書署名要求を生成するための値を入力します。表示されるウィンドウの各フィールドについては、信頼できる証明書の設定 （111 ページ）を参照してください。

ステップ 4 （オプション）ダウンロードする署名要求のチェックボックスをオンにし、**[エクスポート（Export）]** をクリックして要求をダウンロードします。

ステップ 5 「 **-----BEGIN CERTIFICATE REQUEST-----** 」から「 **-----END CERTIFICATE REQUEST-----** 」までのすべてのテキストをコピーし、選択した CA の証明書要求に要求の内容を貼り付けます。

ステップ 6 署名済みの証明書をダウンロードします。

CA によっては、署名付き証明書が電子メールで送信される場合があります。署名付き証明書は、zip ファイルの形式で、Cisco ISE-PIC の信頼できる証明書ストアに追加する必要がある、新規発行の証明書と CA のパブリック署名証明書が含まれています。デジタル署名された CA 証明書、ルート CA 証明書、および他の中間 CA 証明書（該当する場合）をクライアントブラウザを実行するローカルシステムにダウンロードできます。

証明書署名要求への CA 署名付き証明書のバインド

CA がデジタル署名付き証明書を返してから、その証明書を証明書署名要求にバインドする必要があります。Cisco ISE 管理者ポータルから展開内のすべてのノードに対してバインド操作を実行できます。

始める前に

- デジタル署名付き証明書、および関連するルート中間 CA 証明書を CA から受け取る必要があります。
- 信頼できる証明書ストアに関連するルート CA 証明書と中間 CA 証明書をインポートします（**[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]**。を選択します）。

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 CA 署名付き証明書とバインドする必要がある証明書署名要求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 **[証明書のバインド（Bind Certificate）]** をクリックします。

ステップ 4 表示される [CA 署名付き証明書（Bind CA Signed Certificate）] ウィンドウで、**[ファイルの選択（Choose File）]** をクリックし、CA 署名付き証明書を選択します。

ステップ 5 [フレンドリ名（Friendly Name）] フィールドに値を入力します。

ステップ 6 Cisco ISE-PIC に証明書の拡張の検証を許可する場合は、[証明書の拡張の検証（Validate Certificate Extensions）] チェックボックスをオンにします。

[証明書の拡張の検証（Validate Certificate Extensions）] オプションが有効になっており、インポートする証明書に CA フラグが True に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在すること、および keyEncipherment ビットと keyAgreement ビットのいずれかまたは両方が設定されていることを確認します。

（注） Cisco ISE では、EAP-TLS クライアント証明書にデジタル署名のキー使用拡張を使用する必要があります。

ステップ 7 （オプション）[使用方法（Usage）] 領域で、この証明書が使用されるサービスをオンにします。

この情報は、証明書署名要求の生成時に [使用方法（Usage）] オプションを有効にした場合は自動入力されます。また、後で証明書を編集して使用方法を指定することもできます。

プライマリ PAN で使用方法が **[管理者（Admin）]** の証明書を変更すると、他のすべてのノードでサービスが再起動します。プライマリ PAN 再起動後にシステムは一度に 1 つのノードを再起動します。

ステップ 8 **[送信（Submit）]** をクリックして証明書署名要求を CA 署名付き証明書とバインドします。

この証明書の使用方法が Cisco ISE-PIC ノード間通信用としてマークされている場合は、Cisco ISE-PIC ノードのアプリケーションサーバーが再起動します。

このプロセスを繰り返して、証明書署名要求と展開内の他のノード上の CA 署名付き証明書をバインドします。

次のタスク

信頼できる証明書ストアへのルート証明書のインポート （98 ページ）

証明書署名要求のエクスポート

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書署名要求がローカルファイルシステムにダウンロードされます。

証明書署名要求の設定

Cisco ISE-PIC では、1 つの要求で、管理者ポータルから展開内のノードの証明書署名要求を生成することができます。また、展開内の単一ノードか、またはノードのどちらの証明書署名要求を生成するのかを選択することもできます。単一ノードの証明書署名要求を生成する場合、ISE は証明書サブジェクトの [CN=] フィールドの特定ノードの完全修飾ドメイン名（FQDN）を自動的に置き換えます。証明書の [サブジェクト代替名（Subject Alternative Name (SAN)）] フィールドにエントリを含めることを選択した場合、他の SAN 属性に加えて ISE-PIC ノードの FQDN を入力する必要があります。展開内の両方のノードの証明書署名要求を生成することを選択した場合は、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] チェックボックスをオンにして、[SAN] フィールド（DNS 名）にワイルドカード表記で FQDN を入力します（*.amer.example.com など）。EAP 認証に証明書を使用する場合は、[CN=] フィールドにワイルドカード値を入力しないでください。

ワイルドカード証明書を使用することにより、各 Cisco ISE-PIC ノードに固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値を入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、展開内のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE-PIC ノードに固有のサーバー証明書を割り当てる場合よりも安全性が低いと見なされます。

表 *19 :* 証明書署名要求の設定

フィールド	使用上のガイドライン
証明書の用途（**Certificate(s) will be used for**）	

フィールド	使用上のガイドライン
	証明書を使用するサービスを選択します。 **Cisco ISE ID 証明書** • [複数使用（Multi-Use）]：複数のサービス（管理者、EAP-TLS 認証、pxGrid）に使用されます。複数使用の証明書は、クライアントとサーバー両方のキーの用途を使用します。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [管理者（Admin）]：サーバー認証に使用されます（管理者ポータルとの通信および展開内の ISE-PIC ノード間の通信を保護するため）。署名 CA の証明書テンプレートは、Web サーバー証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1） • [pxGrid]：クライアント認証とサーバー認証の両方に使用されます（pxGrid クライアントとサーバー間の通信を保護するため）。署名 CA の証明書テンプレートは、コンピュータまたはマシン証明書テンプレートと呼ばれます。このテンプレートには、次のプロパティがあります。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1）および TLS Web クライアント認証（1.3.6.1.5.5.7.3.2） • [SAML]：SAML ID プロバイダ（IdP）とのセキュア通信に使用するサーバー証明書。SAML での使用を目的とした証明書は、管理者認証や EAP 認証などのその他のサービスのために使用することはできません。 • [キーの用途（Key Usage）]：デジタル署名（署名） • [キーの拡張用途（Extended Key Usage）]：TLS Web サーバー認証（1.3.6.1.5.5.7.3.1）

フィールド	使用上のガイドライン
	（注） 拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用しないことをお勧めします。拡張キーの使用状況属性に任意の目的のオブジェクト識別子のための 2.5.29.37.0 の値が含まれている証明書を使用する場合、証明書は無効と見なされ、次のエラー メッセージが表示されます。 `source=local ; type=fatal ; message="unsupported certificate"` **Cisco ISE 認証局証明書** • [ISE ルート CA（ISE Root CA）]：（内部 CA サービスにのみ適用可能）プライマリ PAN のルート CA および PSN の下位 CA を含む内部 CA 証明書チェーン全体を再生成するために使用されます。 • [ISE 中間 CA（ISE Intermediate）]：（ISE-PIC が外部 PKI の中間 CA として機能する場合に内部 CA サービスにのみ適用可能）プライマリ PAN の中間 CA 証明書および PSN の下位 CA 証明書の生成に使用されます。署名 CA の証明書テンプレートは、下位認証局と呼ばれます。このテンプレートには、次のプロパティがあります。 • [基本制約（Basic Constraints）]：重要、認証局 • [キーの用途（Key Usage）]：証明書の署名、デジタル署名 • [キーの拡張用途（Extended Key Usage）]：OCSP 署名（1.3.6.1.5.5.7.3.9） • [ISE OCSP 応答側証明書の更新（Renew ISE OCSP Responder Certificates）]：（内部 CA サービスにのみ適用可能）展開全体の ISE-PIC OCSP 応答側証明書の更新に使用されます（証明書署名要求ではありません）。セキュリティ上の理由から、ISE-PIC OCSP 応答側証明書を 6 ヵ月ごとに更新することを推奨します。
ワイルドカード証明書の許可（Allow Wildcard Certificates）	証明書の [SAN] フィールドの CN/DNS 名にワイルドカード文字（*）を使用するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、展開内のすべてのノードが自動的に選択されます。左端のラベルの位置にアスタリスク（*）ワイルドカード文字を使用する必要があります。ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、セキュリティ上の問題が発生する可能性があります。

フィールド	使用上のガイドライン
これらのノードの CSR の生成（Generate CSRs for these Nodes）	証明書を生成するノードの隣のチェックボックスをオンにします。展開内の選択されたノードの CSR を生成するには、[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオフにします。
共通名（Common Name）（CN）	デフォルトでは、共通名は証明書署名要求を生成する ISE-PIC ノードの FQDN です。$FQDN$ は ISE-PIC ノードの FQDN を意味します。展開内の複数ノードの証明書署名要求を生成すると、証明書署名要求の [共通名（Common Name）] フィールドは各 ISE ノードの FQDN に置き換えられます。
組織ユニット（Organization Unit）（OU）	組織ユニット名。Engineering など。
組織（Organization）（O）	組織名。Cisco など。
都市（City）（L）	（省略不可）都市名。San Jose など。
州（State）（ST）	（省略不可）州名。California など。
国（Country）（C）	国名。2 文字の ISO 国番号を入力する必要があります。US など。
サブジェクト代替名（Subject Alternative Name）（SAN）	証明書に関連付けられている IP アドレス、DNS 名、Uniform Resource Identifier（URI）、またはディレクトリ名。 • [DNS 名（DNS Name）]：DNS 名を選択した場合は、ISE-PIC ノードの完全修飾ドメイン名を入力します。[ワイルドカード証明書の許可（Allow Wildcard Certificates）] オプションをオンにした場合は、ワイルドカード表記（ドメイン名の前にアスタリスクとピリオドを入力）を指定します。*.amer.example.com など。 • [IP アドレス（IP Address）]：証明書に関連付けられる ISE-PIC ノードの IP アドレス。 • [ユニフォーム リソース識別子（Uniform Resource Identifier）]：証明書に関連付ける URI。 • [ディレクトリ名（Directory Name）]：RFC 2253 に従って定義される識別名（DN）の文字列表現。DN 間はカンマ（,）で区切ります。「dnQualifier」RDN の場合は、カンマをエスケープし、区切り文字としてバックスラッシュ カンマ「\,」を使用します。たとえば、CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL などです。

フィールド	使用上のガイドライン
キータイプ（**Key Type**）	RSA または ECDSA の公開キーの作成に使用するアルゴリズムを指定します。
キーの長さ（**Key Length**）	公開キーのビット サイズを指定します。 RSA には、次のオプションを使用できます。 • 512 • 1024 • 2048 • 4096 ECDSA には、次のオプションを使用できます。 • 256 • 384 （注） RSA および ECDSA の公開キーは、同じセキュリティ レベルで異なるキー長を持つことがあります。 パブリック CA の署名付き証明書を取得する場合は 2048 以上を選択します。
署名するダイジェスト（**Digest to Sign With**）	ハッシュ アルゴリズム SHA-1 または SHA-256 を選択します。
証明書ポリシー（**Certificate Policies**）	証明書が従うべき証明書ポリシーの OID または OID のリストを入力します。OID を区切るには、カンマまたはスペースを使用します。

Cisco ISE CA サービス

証明書は、自己署名したり、外部の認証局（CA）がデジタルで署名したりできます。ISE-PIC は、pxGrid 証明書にデジタル署名を行う pxGrid の外部認証局（CA）として機能できます。CA 署名付きデジタル証明書は、業界標準であり、よりセキュアです。ISE-PIC CA には次の機能があります。

- 証明書の発行：ネットワークに接続するエンドポイントの証明書署名要求（CSR）を検証し、署名します。
- キー管理：キーと証明書を生成し、セキュアに保存します。
- 証明書ストレージ：ユーザーやデバイスに発行された証明書を保存します。

- Online Certificate Status Protocol（OCSP）サポート：OCSP 応答側に証明書の有効性を確認する手段を提供します。

CA サービスがプライマリ管理ノードで無効になっている場合でも、CA サービスはセカンダリ管理ノードの CLI で実行中として表示されます。理想的には、CA サービスは無効として表示される必要があります。これは、Cisco ISE の既知の問題です。

楕円曲線暗号化証明書のサポート

Cisco ISE-PIC CA サービスが、楕円曲線暗号化（ECC）アルゴリズムに基づく証明書をサポートするようになりました。ECC は、より小さいキー サイズを使用している場合でも、他の暗号化アルゴリズムよりも高いセキュリティとパフォーマンスを提供します。

次の表では、ECC および RSA のキー サイズとセキュリティ強度を比較しています。

ECC のキー サイズ（ビット単位）	**RSA のキー サイズ（ビット単位）**
160	1024
224	2048
256	3072
384	7680
521	15360

キー サイズが小さいため、暗号化が迅速になります。

Cisco ISE-PIC では、次の ECC 曲線タイプがサポートされています。曲線タイプまたはキー サイズが大きくなると、セキュリティが強化されます。

- P-192
- P-256
- P-384
- P-521

ISE-PIC は、証明書の EC 部分の明示的なパラメータをサポートしていません。明示的なパラメータで証明書をインポートしようとすると、「証明書の検証に失敗しました」というエラーが表示されます。名前付き ECParameters のみがサポートされています。

証明書プロビジョニング ポータルから ECC 証明書を生成することができます。

Cisco ISE-PIC 認証局証明書

[認証局（CA）証明書（Certificate Authority (CA) Certificates）] ページには、内部 Cisco ISE-PIC CA に関連するすべての証明書が表示されます。これらの証明書は、このページにノード方式で表示されます。ノードを展開して、その特定のノードの ISE-PIC CA 証明書をすべて表示することができます。プライマリおよびセカンダリ管理ノードには、ルート CA、ノード CA、

下位 CA、OCSP レスポンダ証明書があります。展開内の他のノードには、エンドポイント下位 CA および OCSP 証明書があります。

Cisco ISE-PIC CA サービスを有効にすると、すべてのノードでこれらの証明書が自動的に生成され、インストールされます。また、ISE-PIC ルート CA チェーン全体を置き換えると、すべてのノードでこれらの証明書が自動的に再生成され、インストールされます。手動による介入は必要ありません。

Cisco ISE-PIC CA 証明書は **Certificate Services** <**エンドポイント サブ *CA*/ノード *CA*/ルート *CA*/*OCSP* レスポンダ**>-<ノードのホスト名>#証明書番号という命名規則に従います。

[CA 証明書（CA Certificates）] ページで Cisco ISE-PIC CA 証明書を編集、インポート、エクスポート、削除、表示できます。

Cisco ISE-PIC CA 証明書の編集

証明書を Cisco ISE-PIC CA 証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 の順に選択します。

ステップ 3 編集する証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

ステップ 4 必要に応じて編集可能なフィールドを変更します。フィールドの説明については、信頼できる証明書の設定 （111 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックして、証明書ストアに対して行った変更を保存します。

Cisco ISE CA 証明書のエクスポート

Cisco ISE ルート CA およびノード CA 証明書をエクスポートするには、次の手順を実行します。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）]** の順に選択します。

ステップ 2 ISE-PIC GUI で [メニュー（Menu）] アイコン（☰）をクリックして、 の順に選択します。

ステップ 3 エクスポートする証明書の隣にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 4 クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

Cisco ISE-PIC CA 証明書のインポート

クライアントが別の展開の Cisco ISE-PIC CA によって発行された証明書を使用してネットワークへの認証を試みる場合、Cisco ISE-PIC ルート CA、ノード CA、エンドポイント サブ CA 証明書をその展開から Cisco ISE-PIC の信頼できる証明書ストアにインポートする必要があります。

始める前に

- ISE-PIC ルート CA、ノード CA、エンドポイント サブ CA 証明書を、エンドポイント証明書が署名されている展開からエクスポートし、ブラウザが実行されているコンピュータのファイル システムに保存します。

ステップ 1 **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** を選択します。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 必要に応じてフィールドの値を設定します。詳細については、信頼できる証明書のインポート設定 （99 ページ）を参照してください。

クライアント証明書ベースの認証が有効である場合は、Cisco ISE-PIC により展開内の各ノードのアプリケーション サーバーが再起動されます（最初に PAN のアプリケーション サーバーが再起動されます）。

信頼できる証明書の設定

次の表では、信頼できる証明書の [編集（Edit）] ウィンドウのフィールドについて説明します。このウィンドウで CA 証明書の属性を編集します。このページへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[証明書（Certificates）]** > **[信頼できる証明書（Trusted Certificates）]** です。編集する信頼できる証明書の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

表 *20* : 信頼できる証明書の編集設定

フィールド名	使用上のガイドライン
証明書発行元（Certificate Issuer）	
フレンドリ名（**Friendly Name**）	証明書のフレンドリ名を入力します。これはオプションのフィールドです。フレンドリ名を入力しない場合は、次の形式でデフォルト名が生成されます。 *common-name#issuer#nnnnn*

フィールド名	使用上のガイドライン
ステータス（**Status**）	ドロップダウンリストから [有効（Enabled）] または [無効（Disabled）] を選択します。証明書が無効になっている場合、Cisco ISE は信頼の確立に証明書を使用しません。
説明（**Description**）	（任意）説明を入力します。
使用方法（Usage）	
ISE 内の認証用に信頼する（Trust for authentication within ISE）	この証明書で（他の Cisco ISE ノードまたは LDAP サーバーからの）サーバー証明書を確認する場合は、このチェックボックスをオンにします。
クライアント認証および syslog 用に信頼する（Trust for client authentication and Syslog）	（[ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスをオンにした場合に限り適用可能）この証明書を使用して次を行う場合は、このチェックボックスをオンにします。 • EAP プロトコルを使用した Cisco ISE に接続するエンドポイントを認証します。 • syslog サーバーを信頼します。
シスコ サービスの認証用に信頼する（Trust for authentication of Cisco Services）	フィードサービスなどの外部シスコサービスを信頼するためにこの証明書を使用する場合は、このチェックボックスをオンにします。
証明書ステータスの検証（Certificate Status Validation）	Cisco ISE は、特定の CA が発行するクライアントまたはサーバー証明書の失効ステータスをチェックする 2 とおりの方法をサポートしています。1 つめの方法は、Online Certificate Status Protocol（OCSP）を使用して証明書を検証することです（OCSP は、CA によって保持される OCSP サービスに要求を行います）。2 つめの方法は、Cisco ISE に CA からダウンロードした証明書失効リスト（CRL）と照合して証明書を検証することです。どちらの方法も、OCSP を最初に使用してステータスを判断できないときに限り CRL を使用する場合に使用できます。

フィールド名	使用上のガイドライン
OCSP サービスに対して検証する（Validate Against OCSP Service）	OCSP サービスに対して証明書を検証するには、このチェックボックスをオンにします。このボックスをオンにするには、まず OCSP サービスを作成する必要があります。
OCSP が不明なステータスを返した場合は要求を拒否する（Reject the request if OCSP returns UNKNOWN status）	証明書ステータスが OCSP サービスによって判断されなかった場合に要求を拒否するには、このチェックボックスをオンにします。このチェックボックスをオンにした場合、OCSP サービスによって不明なステータス値が返されると、Cisco ISE は現在評価しているクライアントまたはサーバー証明書を拒否します。
OCSP応答側が到達不能な場合は要求を拒否する（Reject the request if OCSP Responder is unreachable）	OCSP 応答側が到達不能な場合に Cisco ISE が要求を拒否するには、このチェックボックスをオンにします。
CRL のダウンロード（Download CRL）	Cisco ISE で CRL をダウンロードするには、このチェックボックスをオンにします。
CRL 配信 URL（CRL Distribution URL）	CA から CRL をダウンロードするための URL を入力します。認証局証明書で指定されている場合、このフィールドは自動的に読み込まれます。URL は「http」、「https」、または「ldap」で始まる必要があります。
CRL の取得（Retrieve CRL）	CRL は、自動的または定期的にダウンロードできます。ダウンロードの時間間隔を設定します。
ダウンロードが失敗した場合は待機する（If download failed, wait）	Cisco ISE が CRL を再度ダウンロードするまでに Cisco ISE に必要な試行を待機する必要がある時間間隔を設定します。
CRL を受信しない場合 CRL 検証をバイパスする（Bypass CRL Verification if CRL is not Received）	このチェックボックスをオンにした場合、クライアント要求は CRL が受信される前に受け入れられます。このチェックボックスをオフにした場合、選択した CA によって署名された証明書を使用するすべてのクライアント要求は、Cisco ISE によって CRL ファイルが受信されるまで拒否されます。

フィールド名	使用上のガイドライン
CRL がまだ有効でないか、または期限切れの場合は無視する（Ignore that CRL is not yet valid or expired）	Cisco ISE で開始日と期限日を無視し、まだアクティブでないかまたは期限切れの CRL を引き続き使用し、CRL の内容に基づいて EAP-TLS 認証を許可または拒否する場合は、このチェックボックスをオンにします。 Cisco ISE で [有効日（Effective Date）] フィールドの開始日と [次の更新（Next Update）] フィールドの期限日を CRL ファイルでチェックする場合は、このチェックボックスをオフにします。CRLがまだアクティブではないか、または期限切れの場合、その CA によって署名された証明書を使用するすべての認証は拒否されます。

関連トピック

信頼できる証明書ストア （93 ページ）
信頼できる証明書の編集 （96 ページ）

Cisco ISE-PIC CA 証明書およびキーのバックアップと復元

PAN に障害が発生し、セカンダリ管理ノードを外部 PKI のルート CA または中間 CA として機能させるために昇格する場合に備え、Cisco ISE-PIC CA 証明書およびキーをセキュアにバックアップして、セカンダリ管理ノードにこれらを復元できるようにする必要があります。Cisco ISE-PIC 設定のバックアップには、CA 証明書とキーは含まれていません。CA 証明書およびキーをリポジトリにエクスポートおよびインポートするには、代わりにコマンドライン インターフェイス（CLI）を使用する必要があります。**application configure ise** コマンドには、CA 証明書およびキーのバックアップと復元のためのエクスポートおよびインポートのオプションが含まれています。

信頼できる証明書ストアからの次の証明書が、セカンダリ管理ノードで復元されます。

- Cisco ISE ルート CA 証明書
- Cisco ISE サブ CA 証明書
- Cisco ISE エンドポイント RA 証明書
- Cisco ISE OCSP 応答側証明書

次の場合、Cisco ISE CA 証明書およびキーのバックアップおよび復元が必要となります。

- 展開内にセカンダリ管理ノードが存在する
- Cisco ISE-PIC CA ルート チェーン全体を置き換える
- 外部 PKI の下位 CA として機能するように Cisco ISE-PIC ルート CA を設定する

- 設定のバックアップからデータを復元する。この場合、最初に Cisco ISE-PIC CA ルートチェーンを再生成し、次に ISE CA 証明書およびキーのバックアップと復元を行う必要があります。

（注） 展開で Cisco ISE の内部 CA を置き換えるたびに、完全な証明書チェーンを取得するように ISE メッセージング サービスも更新する必要があります。

Cisco ISE CA 証明書およびキーのエクスポート

CA 証明書およびキーを PAN からエクスポートし、セカンダリ管理ノードでインポートする必要があります。このオプションでは、PAN がダウンした場合にセカンダリ管理ノードでエンドポイントの証明書を発行および管理し、セカンダリ管理ノードを PAN に昇格させることができます。

始める前に

CA 証明書およびキーを格納するためのリポジトリを作成したことを確認します。

ステップ 1 Cisco ISE CLI から、**application configure ise** コマンドを入力します。

ステップ 2 7 を入力して、証明書およびキーをエクスポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 暗号キーを入力します。

エクスポートされた証明書のリスト、件名、発行者、およびシリアル番号とともに成功メッセージが表示されます。

例：

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE-PIC CA 証明書およびキーのインポート

セカンダリ管理ノードを登録したら、PAN から CA 証明書およびキーをエクスポートし、セカンダリ管理ノードにインポートします。

ステップ 1 Cisco ISE-PIC CLI から、**application configure ise** コマンドを入力します。

ステップ 2 8 を入力して、CA 証明書およびキーをインポートします。

ステップ 3 リポジトリの名前を入力します。

ステップ 4 インポートするファイルの名前を入力します。ファイル名は **ise_ca_key_pairs_of_<vm hostname>** 形式である必要があります。

ステップ 5 ファイルを復号化するための暗号キーを入力します。

処理が正常に完了したことを知らせるメッセージが表示されます。

例：

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

（注） エクスポートされたキーファイルの暗号化は、Cisco ISE リリース 2.6 で導入されました。Cisco ISE リリース 2.4 以前のバージョンからのキーのエクスポート、および Cisco ISE リリース 2.6 以降のバージョンでのキーのインポートは成功しません。

ルート CA および下位 CA の生成

展開をセットアップする場合、Cisco ISE-PIC は、ノードでルート CA を生成します。ただし、ノードのドメイン名またはホスト名を変更する場合は、プライマリ PAN でルート CA、PSN で下位 CA をそれぞれ再生成する必要があります。

ステップ 1 **[証明書（Certificates）]** > **[証明書署名要求（Certificate Signing Requests）]** を選択します。 を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用先（Certificate(s) will be used for）] ドロップダウン リストから ISE ルート CA を選択します。

ステップ 4 [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate chain）] をクリックします。

ルート CA と下位 CA 証明書が、展開内のすべてのノードに対して生成されます。

外部 PKI の下位 CA としての Cisco ISE-PIC ルート CA の設定

外部 PKI の下位 CA として機能する PAN のルート CA が必要な場合は、ISE-PIC中間 CA 証明書署名要求を生成して、外部 CA に送信し、ルートおよび CA 署名付き証明書を入手して、ルート CA 証明書を信頼できる証明書ストアにインポートし、CA 署名付き証明書を CSR にバインドします。この場合、外部 CA はルート CA、ノード は外部 CA の下位 CA、PSN はノード の下位 CA です。

ステップ 1 **[証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）]** を選択します。

ステップ 2 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests (CSR)）] をクリックします。

ステップ 3 [証明書の使用目的（Certificate(s) will be used for）] ドロップダウン リストから [ISE 中間 CA（ISE Intermediate CA）] を選択します。

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 CSR をエクスポートし、外部 CA に送信して、CA 署名付き証明書を取得します。

ステップ 6 信頼できる証明書ストアに外部 CA のルート CA 証明書をインポートします。

ステップ 7 CSR に CA 署名付き証明書をバインドします。

OCSP サービス

Online Certificate Status Protocol（OCSP）は、x.509 デジタル証明書のステータスのチェックに使用されるプロトコルです。このプロトコルは証明書失効リスト（CRL）に代わるものであり、CRL の処理が必要となる問題に対処します。

Cisco ISE には HTTP を介して OCSP サーバーと通信し、認証で証明書のステータスを検証する機能があります。OCSP のコンフィギュレーションは、Cisco ISE で設定されるいずれかの認証局（CA）証明書から参照できる再利用可能な設定オブジェクトで設定されます。

CRL 検証と OCSP 検証の両方または一方を CA ごとに設定できます。両方を選択すると、Cisco ISE では最初に OCSP を介した検証が実行されます。プライマリ OCSP サーバーとセカンダリ OCSP サーバーの両方で通信の問題が検出された場合、または特定の証明書に対して不明のステータスが返された場合、Cisco ISE は CRL チェックの実行に切り替えます。

Cisco ISE CA サービスの Online Certificate Status Protocol レスポンダ

Cisco ISE CA OCSP 応答側は、OCSP クライアントと通信するサーバーです。Cisco ISE CA の OCSP クライアントには、Cisco ISE の内部 OCSP クライアントと適応型セキュリティ アプライアンス（ASA）の OCSP クライアントがあります。OCSP クライアントは、RFC 2560、5019 で定義されている OCSP 要求/応答構造を使用して、OCSP 応答側と通信する必要があります。

Cisco ISE CA は、OCSP 応答側に証明書を発行します。OCSP 応答側は、着信要求をポート 2560 でリッスンします。このポートは、OCSP トラフィックのみを許可するように設定されています。

OCSP 応答側は RFC 2560、5019 で規定された構造に従って要求を受け入れます。OCSP 要求ではナンス拡張がサポートされます。OCSP 応答側は証明書のステータスを取得し、OCSP 応答を作成して署名します。OCSP 応答は、OCSP 応答側ではキャッシュされませんが、クライアントでは最大 24 時間 OCSP 応答をキャッシュすることができます。OCSP クライアントでは、OCSP 応答の署名を検証する必要があります。

PAN 上の自己署名 CA 証明書（ISE が外部 CA の中間 CA として機能する場合は、中間 CA 証明書）によって、OCSP 応答側証明書が発行されます。PAN 上のこの CA 証明書によって、PAN および PSN の OCSP 証明書が発行されます。この自己署名 CA 証明書は、展開全体に対するルート証明書でもあります。展開全体のすべての OCSP 証明書が、これらの証明書を使用して署名された応答を ISE で検証するために、信頼できる証明書ストアに格納されます。

（注） Cisco ISE は OCSP レスポンダサーバーから thisUpdate 値を受信します。この値は、最後の証明書失効からの時間を示します。thisUpdate 値が 7 日より大きい場合、Cisco ISE で OCSP 証明書の検証が失敗します。

OCSP 証明書のステータスの値

OCSP サービスでは、所定の証明書要求に対して次の値が返されます。

- [良好（Good）]：ステータスの問い合わせへの肯定的な応答を示します。証明書が失効していないこと、および状態が次の時間間隔（存続可能時間）値までは良好であることを示します。
- [失効（Revoked）]：証明書は失効しています。
- [不明（Unknown）]：証明書のステータスは不明です。この OCSP 応答側の CA で証明書が発行されなかった場合、OCSP サービスはこの値を返します。
- [エラー（ERROR）]：OCSP 要求に対する応答を受信しませんでした。

OCSP ハイ アベイラビリティ

Cisco ISE では CA ごとに最大 2 つの OCSP サーバーを設定でき、それらのサーバーはプライマリおよびセカンダリ OCSP サーバーと呼ばれます。各 OCSP サーバー設定には、次のパラメータが含まれます。

- [URL]：OCSP サーバーの URL。
- [ナンス（Nonce）]：要求で送信される乱数。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
- [応答の検証（Validate Response）]：Cisco ISE は OCSP サーバーから受信した応答の署名を検証します。

Cisco ISE がプライマリ OCSP サーバーと通信しているときに、タイムアウト（5 秒）が発生した場合、Cisco ISE はセカンダリ OCSP サーバーに切り替えます。

Cisco ISE はプライマリ サーバーの再使用を試行する前に、設定可能な期間セカンダリ OCSP サーバーを使用します。

OCSP の障害

3 つの一般的な OCSP 障害のシナリオは次のとおりです。

- OCSP キャッシュまたは OCSP クライアント側（Cisco ISE）の失敗による障害。
- 失敗した OCSP 応答側のシナリオ。例：

  最初のプライマリ OCSP 応答側が応答せず、セカンダリ OCSP 応答側が Cisco ISE OCSP 要求に応答します。

  Cisco ISE OCSP 要求からエラーまたは応答が受信されません。

  OCSP 応答側が、Cisco ISE OCSP 要求への応答を提供しないか、失敗の OCSP 応答のステータスを返している可能性があります。OCSP 応答のステータス値は次のようになります。

  - tryLater
  - signRequired
  - unauthorized
  - internalError
  - malformedRequest

    OCSP 要求には、多数の日時チェック、署名の有効性チェックなどがあります。詳細については、エラー状態を含むすべての可能性のある状態について説明している『*RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』を参照してください。

- 失敗した OCSP レポート

OCSP クライアント プロファイルの追加

[OCSP クライアント プロファイル（OCSP Client Profile）] ページを使用して、Cisco ISE に新しい OCSP クライアント プロファイルを追加できます。

始める前に

認証局（CA）が非標準ポート（80 または 443 以外）で OCSP サービスを実行している場合は、そのポートで Cisco ISE と CA 間の通信を可能にするためにスイッチで ACL を設定する必要があります。次に例を示します。

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP* ポート番号 >

ステップ 1 **[証明書（Certificates）]** > **[OCSP クライアントプロファイル（OCSP Client Profile）]** を選択します。

ステップ 2 OCSP クライアント プロファイルを追加するための値を入力します。

ステップ 3 **[送信（Submit）]** をクリックします。

OCSP 統計情報カウンタ

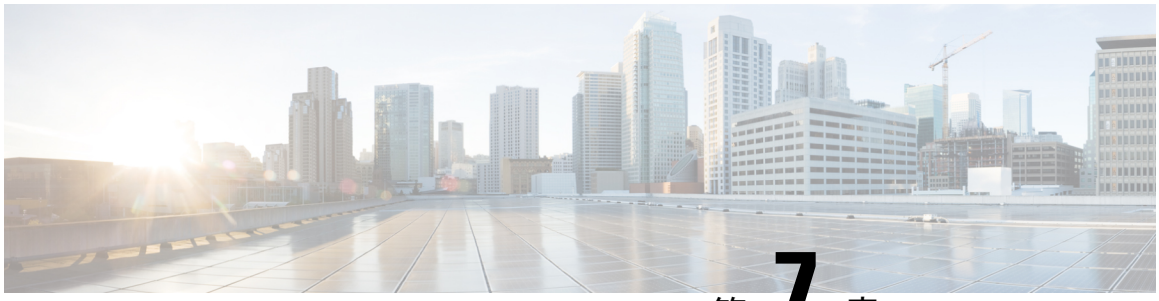
Cisco ISE では、OCSP カウンタを使用して、OCSP サーバーのデータと正常性をロギングおよびモニターリングします。ロギングは 5 分ごとに実行されます。Cisco ISE はモニターリング ノードに syslog メッセージを送信し、それはローカル ストアに保持されます。ローカル ストアには過去 5 分のデータが含まれています。Cisco ISE が syslog メッセージを送信した後、カウンタは次の間隔について再計算されます。つまり、5 分後に、新しい 5 分間の間隔が再度開始されます。

次の表に、OCSP syslog メッセージとその説明を示します。

表 *21 : OCSP Syslog* メッセージ

メッセージ	説明
OCSPPrimaryNotResponsiveCount	応答のないプライマリ要求の数
OCSPSecondaryNotResponsiveCount	応答のないセカンダリ要求の数
OCSPPrimaryCertsGoodCount	プライマリ OCSP サーバーを使用して返された所定の CA の「良好な」証明書の数
OCSPSecondaryCertsGoodCount	プライマリ OCSP サーバーを使用して返された所定の CA の「良好な」ステータスの数
OCSPPrimaryCertsRevokedCount	プライマリ OCSP サーバーを使用して返された所定の CA の「失効した」ステータスの数

メッセージ	説明
OCSPSecondaryCertsRevokedCount	セカンダリ OCSP サーバーを使用して返された所定の CA の「失効した」ステータスの数
OCSPPrimaryCertsUnknownCount	プライマリ OCSP サーバーを使用して返された所定の CA の「不明の」ステータスの数
OCSPSecondaryCertsUnknownCount	セカンダリ OCSP サーバーを使用して返された所定の CA の「不明の」ステータスの数
OCSPPrimaryCertsFoundCount	プライマリの送信元からのキャッシュ内に見つかった証明書の数
OCSPSecondaryCertsFoundCount	セカンダリの送信元からのキャッシュ内に見つかった証明書の数
ClearCacheInvokedCount	一定間隔の後にキャッシュのクリアがトリガーされた回数
OCSPCertsCleanedUpCount	t間隔の後にクリーンアップされたキャッシュエントリの数
NumOfCertsFoundInCache	キャッシュから実行された要求の数
OCSPCacheCertsCount	OCSP キャッシュ内に見つかった証明書の数



第 7 章

管理 ISE-PIC

ISE-PIC ノードの管理

セカンダリ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ャルを入力します。

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。ノートが登録されると、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ャルを入力します。

（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に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。

次のタスク

セカンダリノードでパッチをインストールする必要がある場合は、ノードが動作中であることを確認し、プロセスを繰り返して残りのノードにパッチをインストールします。

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。これを行うには、GUI で [管理者（Administrator）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch management）] ウィンドウを選択します。

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）]** を選択します。

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 5 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。

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 （135 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

表 22：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。

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 （133 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.file* 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の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。

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の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。

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 [作成（Create）][スケジュール（Schedule）]をクリックして、設定または操作バックアップをスケジュールします。

ステップ 3 必要に応じてバックアップをスケジュールするための値を入力します。

ステップ 4 [保存（Save）] をクリックして、バックアップをスケジュールします。

ステップ 5 次のいずれかの操作を実行します。

- [リポジトリの選択（Select Repository）] ドロップダウンリストから、必要なリポジトリを選択します。
- [リポジトリの追加（Add Repository）] リンク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 6 [更新（Refresh）] リンクをクリックして、スケジュール バックアップのリストを表示します。

作成できる設定または操作バックアップのスケジュールは 1 回に 1 つだけです。スケジュール バックアップは有効化または無効化できますが、削除はできません。

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

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。（[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

restore	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。
filename	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、tar.gpg という拡張子を付ける必要があります（myfile.tar.gpg など）。
repository	バックアップを含むリポジトリを指定します。
repository-name	バックアップを復元するリポジトリの名前。
encryption-key	（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。
hash	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 文字までで指定します。
plain	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 文字までで指定します。
encryption-key name	暗号キーを入力します。

include-adeos	（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
backup	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。
backup-logs	システム ログをバックアップします。
repository	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。
show repository	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。
show backup history	システムのバックアップ履歴を表示します。
show backup status	バックアップ操作のステータスを表示します。
show restore status	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）] > [システム（System）] > [展開（Deployment）]** を選択します。

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

ステップ 3 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 4 [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アドレスとホストネームを使用します。

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すが、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. N1A で Cisco ISE-PIC 管理者ポータルにログインし、**[管理（Administration）] > [展開（Deployment）]** を選択して、次の操作を行う必要があります。

   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。**[管理（Administration）] > [展開（Deployment）]** 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。

パージオプションは、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。

[運用データの消去（Operational Data Purging）] ウィンドウには、[データベース使用率（Database Utilization）] および [データを今すぐ消去（Purge Data Now）] 領域があります。このウィンドウへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]** の順に選択します。[データベースの使用状況（Database Utilization）] 領域には、使用可能なデータベース容量の合計が表示されます。ステータス バーをマウス オーバーすると、利用可能なディスク容量と、データベースに既存データが保存されている日数が表示されます。データは毎朝午前 4 時に消去されます。また、保存日数を指定して、消去前にデータをリポジトリにエクスポートするように設定できます。[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、リポジトリを選択して作成し、[暗号キー（Encryption Key）] を指定します。

関連トピック

古い運用データの消去 （150 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 Base 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。

フル アップグレードを実行するには、まず ISE-PIC アップグレード ライセンスをノードにインストールし、次のいずれかの操作を行います。

- アップグレードした ISE-PIC ノードを既存の ISE 展開に追加する。
- Base ライセンス以上のライセンスをインストールする。

（注） 完全なCisco ISE展開にアップグレードすると、以前のISE-PICインストール環境にロールバックすることはできません。

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 （5 ページ）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

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。

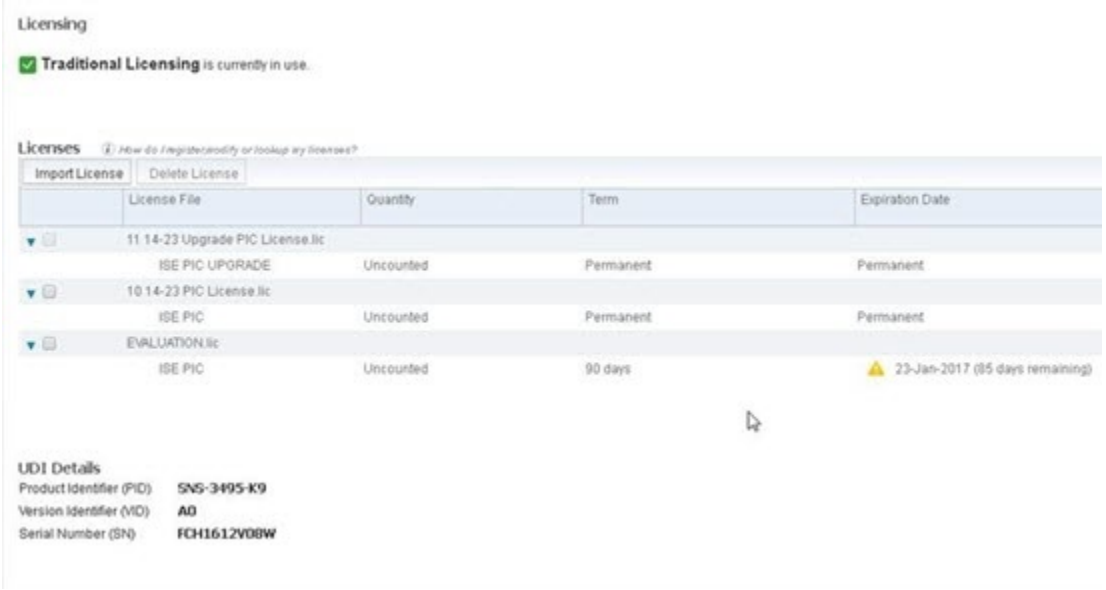
ステップ 2 **[管理（Administration）] > [ライセンス（Licensing）]** を選択します。

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。
[ライセンス（License）] テーブルが更新され、アップグレードライセンスが表示されます。



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 Base 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。

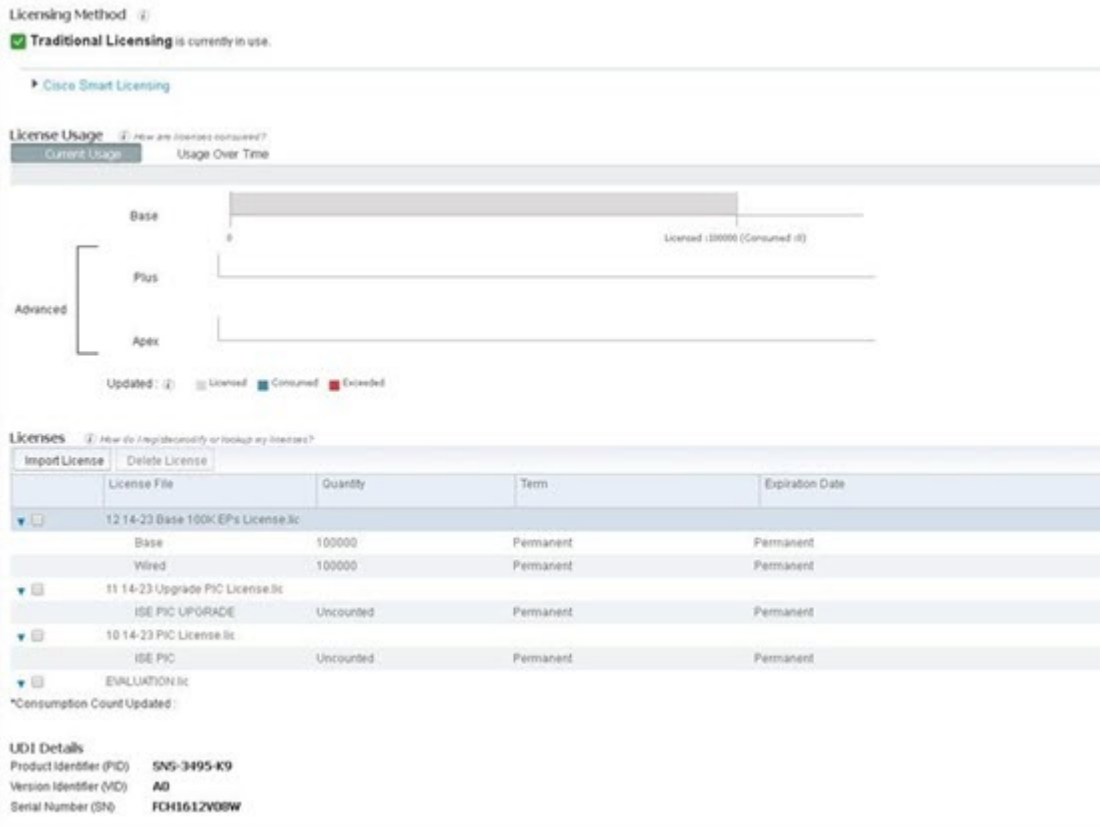
ステップ 7 [ファイルの選択（Choose File）] をクリックし、シスコの担当者から受け取ったライセンスを参照して、[OK] をクリックします。

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。

[ライセンス（License）] テーブルが更新され、Base ライセンスが表示されます。



数分後にログイン画面が表示されます。再度ログインし、Base 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。

（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 （155 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 *23 : 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	• ERS API 要求の作成、読み取り、更新、および削除	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ド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。

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

電子メールの目的	電子メールを送信するノード
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。

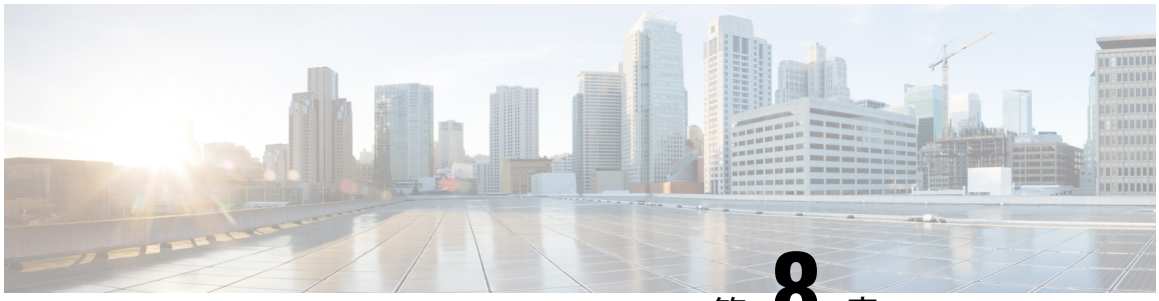
すべてのタイプの外部 RESTful サービス要求はプライマリ ISE ノードに限り有効です。セカンダリ ノードは読み取りアクセス（GET 要求）に対応します。

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。



第 8 章

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

モニターリングおよびトラブルシューティング サービスは、すべての Cisco ISE-PIC 実行時サービスに対する包括的なアイデンティティ ソリューションであり、次のコンポーネントを使用します。

- モニターリング：ネットワーク上のアクセス アクティビティの状態を表す意味のあるデータのリアルタイム表示を提供します。これを把握することにより、操作の状態を簡単に解釈し、作用することができます。
- トラブルシューティング：ネットワーク上のアクセスの問題を解決するための状況に応じたガイダンスを提供します。また、ユーザーの懸念に対応してタイムリーに解決策を提供できます。
- レポート：トレンドを分析し、システム パフォーマンスおよびネットワーク アクティビティをモニターするために使用できる、標準レポートのカタログを提供します。レポートをさまざまな方法でカスタマイズし、今後使用するために保存できます。レコードの検索時には、[ID（Identity）]、[エンドポイント ID（Endpoint ID）]、および [ノード（Node）] フィールドにワイルドカードと複数の値を使用できます。

モニターリング、トラブルシューティング、およびレポーティングの各ツールを使用して ISE-PIC を管理する方法についてはこのセクションで説明します。

ライブ セッション

次の表では、[ライブセッション（Live Sessions）] ウィンドウのフィールドについて説明します。このウィンドウにはライブセッションが表示されます。メインメニューバーから [ライブセッション（Live Sessions）] を選択します。

表 *24 :* ライブ セッション

フィールド名	説明
開始（**Initiated**）	セッション開始時のタイムスタンプを表示します。
更新済み（**Updated**）	何らかの変更のためにセッションが最後に更新された時点のタイムスタンプを表示します。
アカウント セッション時間（**Account Session Time**）	ユーザー セッションの期間（秒単位）を表示します。
セッション ステータス（**Session Status**）	エンドポイント デバイスの現在のステータスを表示します。
アクション（**Action**）	[アクション（Actions）] アイコンをクリックして [アクション（Actions）] ポップアップ ウィンドウを開きます。次を実行できます。 • セッションのクリア • 現行ユーザーのセッション ステータスの確認
エンドポイント ID（**Endpoint ID**）	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
ID（**Identity**）	エンドポイント デバイスのユーザー名を表示します。
IPアドレス（**IP Address**）	エンドポイントデバイスの IP アドレスを表示します。
サーバー（**Server**）	ログを生成した PIC ノードを示します。
認証方式（**Auth Method**）	パスワード認証プロトコル（PAP）、チャレンジ ハンドシェイク認証プロトコル（CHAP）、IEE 802.1x、dot1x など、RADIUS プロトコルによって使用される認証方式を表示します。

フィールド名	説明
セッション送信元（**Session Source**）	RADIUS セッションまたは PassiveID セッションのいずれであるかを示します。
ユーザードメイン名（**User Domain Name**）	ユーザーの登録済み DNS 名を示します。
ユーザーNetBIOS名（**User NetBIOS Name**）	ユーザーの NetBIOS 名を示します。
プロバイダ（**Provider**）	エンドポイント イベントはさまざまな syslog ソースから学習されます。これらの syslog ソースはプロバイダと呼ばれます。 • Windows Management Instrumentation（WMI）：WMI は、オペレーティング システム、デバイス、アプリケーション、およびサービスに関する管理情報にアクセスするための共通インターフェイスとオブジェクト モデルを提供する Windows サービスです。 • エージェント：クライアントまたは別のプログラムの代わりにクライアントで実行されるプログラム。 • syslog：クライアントがイベント メッセージを送信するロギング サーバー。 • REST：クライアントはターミナル サーバーで認証されます。この syslog ソースの場合、[TS エージェント ID（TS Agent ID）]、[開始送信元ポート（Source Port Start）]、[終了送信元ポート（Source Port End）]、[最初の送信元ポート（Source First Port）] の値が表示されます。 • SPAN：ネットワーク情報は SPAN プローブを使用して検出されます。 • DHCP：DHCP イベント。 • エンドポイント（Endpoint） 異なるプロバイダからの 2 つのイベントがエンドポイント セッションから学習されると、ライブ セッション ページにこれらのプロバイダがカンマ区切り値として表示されます。
MAC アドレス（**MAC Address**）	クライアントの MAC アドレスを表示します。

フィールド名	説明
エンドポイント チェック時刻（**Endpoint Check Time**）	エンドポイント プローブによってエンドポイントが最後にチェックされた時刻を表示します。
エンドポイント チェック結果（**Endpoint Check Result**）	エンドポイント プローブの結果が表示されます。設定可能な値は次のとおりです。 • [到達不要（Unreachable）] • [ユーザー ログアウト（User Logout）] • [アクティブ ユーザー（Active User）]
送信元ポートの開始（**Source Port Start**）	（RESTプロバイダの場合にのみ値が表示されます。）ポート範囲の最初のポートの番号を示します。
送信元ポートの終了（**Source Port End**）	（RESTプロバイダの場合にのみ値が表示されます。）ポート範囲の最後のポート番号を示します。
最初の送信元ポート（**Source First Port**）	（RESTプロバイダの場合にのみ値が表示されます。）ターミナルサーバー（TS）エージェントにより割り当てられた最初のポートを示します。 ターミナルサーバー（TS）は、複数のエンドポイントがモデムまたはネットワークインターフェイスなしで接続でき、複数エンドポイントがLANネットワークに接続できるようにするサーバーまたはネットワークデバイスです。複数のエンドポイントに同一 IP アドレスが割り当てられている場合は、特定ユーザーの IP アドレスを識別することが困難になります。このため、特定ユーザーを識別する目的でTSエージェントがサーバーにインストールされ、各ユーザーにポート範囲が割り当てられます。これにより、IP アドレス - ポート - ユーザーのマッピングが作成されます。
TS エージェント ID（**TS Agent ID**）	（RESTプロバイダの場合にのみ値が表示されます。）エンドポイントにインストールされているターミナルサーバー（TS）エージェントの一意の ID を表示します。

フィールド名	説明
AD ユーザー解決 ID（AD User Resolved Identities）	（AD ユーザーの場合にのみ値が表示されます。）一致したアカウントの候補が表示されます。
AD ユーザー解決 DN（AD User Resolved DNs）	（AD ユーザーの場合にのみ値が表示されます。）AD ユーザーの識別名（例：CN=chris,CN=Users,DC=R1,DC=com）を表示します。

使用可能なレポート

次の表に、事前設定済みレポートをカテゴリ別に分類して示します。また、レポートの機能およびロギング カテゴリについても説明します。

レポート名	説明	ロギング カテゴリ
IDC レポート		
AD コネクタ操作	AD コネクタ操作レポートは、ISE-PIC サーバーのパスワードの更新、Kerberos チケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など、AD コネクタが実行する操作のログを提供します。 AD の障害がいくつか発生している場合、このレポートで詳細を確認して考えられる原因を特定できます。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択し、[AD コネクタ（AD Connector）] を選択します。
管理者ログイン	管理者ログイン レポートには、GUI ベースの管理者ログイン イベントと成功した CLI ログイン イベントに関する情報が提供されます。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。

レポート名	説明	ロギング カテゴリ
変更設定監査	変更設定監査レポートは、指定した期間内の設定変更の詳細を提供します。機能をトラブルシューティングする必要がある場合、このレポートは、最新の設定変更が問題の原因となったかどうかを決定するのに役立ちます。	**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。
現在のアクティブなセッション	現在アクティブなセッション レポートを使用すると、指定の期間内のその時点でネットワーク上に存在していた者に関する詳細を含むレポートをエクスポートできます。 ユーザーがネットワークにアクセスできない場合、セッションが認証または終了されているかどうか、またはセッションに別の問題があるかどうかを確認できます。	**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギング カテゴリ（Logging Categories）]** を選択し、ロギング カテゴリ [アカウンティング（Accounting）] および [RADIUS アカウンティング（RADIUS Accounting）] を選択します。

レポート名	説明	ロギング カテゴリ
正常性の概要	正常性の概要レポートは、ダッシュボードのような詳細を提供します。ただし、ダッシュボードは過去 24 時間のデータしか表示しませんが、このレポートを使用するとより多くの履歴データを確認できます。 データの一貫したパターンを調べるためにこのデータを評価できます。たとえば、大多数の従業員が就業時間を開始するときに、非常に高い CPU 使用率が予想されます。これらのトレンドの不整合がわかれば、潜在的な問題を識別できます。 [CPU 使用率（CPU Usage）] テーブルには、各種 ISE-PIC 機能の CPU 使用率（%）が表示されます。**show cpu usage** CLI コマンドの出力がこのテーブルに表示されるため、これらの値を、展開内で発生している問題と関連付け、原因を特定することができます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択し、ロギング カテゴリ [管理監査および操作監査（Administrative and Operational Audit）]、[システム診断（System Diagnostics）]、[システム統計情報（System Statistics）] を選択します。
操作監査	操作監査レポートは、次のような操作の変更に関する詳細を提供します。バックアップの実行、ISE-PIC ノードの登録、またはアプリケーションの再起動。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。

レポート名	説明	ロギング カテゴリ
PassiveID	Passive ID レポートを使用すると、ドメイン コントローラへの WMI 接続の状態をモニターし、関連する統計情報（受信した通知の数、1 秒あたりのユーザー ログイン/ログアウト回数など）を収集することができます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギング カテゴリ（Logging Categories）]** を選択し、[ID マッピング（Identity Mapping）] を選択します。
pxGrid 管理者の監査	pxGrid 管理者の監査レポートは、クライアントの登録、クライアントの登録解除、クライアントの承認、トピックの作成、トピックの削除、パブリッシャとサブスクライバの追加、およびパブリッシャとサブスクライバの削除など、pxGrid の管理処理の詳細を提供します。 すべてのレコードに、ノードで処理を実行した管理者の名前が示されます。 管理者およびメッセージの基準に基づいて、pxGrid 管理者の監査レポートをフィルタできます。	—

レポート名	説明	ロギング カテゴリ
システム診断	システム診断レポートは ISE-PIC ノードのステータスの詳細を提供します。ISE-PIC ノードが登録できない場合、このレポートを確認して問題をトラブルシューティングすることができます。 このレポートでは、最初に複数の診断ロギング カテゴリを有効にする必要があります。これらのログを収集すると、ISE-PIC のパフォーマンスに悪影響を及ぼすことがあります。したがって、これらのカテゴリはデフォルトで有効ではなく、データを収集するのに十分な時間だけ有効にする必要があります。そうでない場合は、30 分後に自動的に無効になります。	**[管理（Administration）]>[ロギング（Logging）]>[ロギングカテゴリ（Logging Categories）]** を選択し、次のロギング カテゴリを選択します：[内部操作診断（Internal Operations Diagnostics）]、[分散管理（Distributed Management）]、および [管理者の認証と許可（Administrator Authentication and Authorization）]。
ユーザー変更パスワードの監査	ユーザー変更パスワードの監査レポートは、従業員のパスワード変更に関する検証を表示します。	**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[ロギング カテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。

Cisco ISE-PIC のアラーム

アラームは、ネットワークの状態を通知し、[アラーム（Alarms）] ダッシュレットに表示されます。アラームには、[クリティカル（Critical）]、[警告（Warning）]、および [情報（Information）] の 3 つのアラームシビラティ（重大度）があります。データ消去イベントなど、システム アクティビティの情報も提供されます。システム アクティビティについてどのように通知するかを設定したり、それらを完全に無効にしたりできます。また、特定のアラームのしきい値を設定できます。

大半のアラームには関連付けられているスケジュールがなく、イベント発生後即時に送信されます。その時点で最新の 15,000 件のアラームのみが保持されます。

イベントが繰り返し発生した場合、同じアラームは約1時間抑制されます。イベントが繰り返し発生する間は、トリガーに応じて、アラームが再び表示されるのに約1時間かかる場合があります。

次の表に、すべての Cisco ISE-PIC アラームおよびその説明と解決方法を示します。

表 *25 : Cisco ISE-PIC* のアラーム

アラーム名	アラームの説明	アラームの解決方法
管理および操作の監査の管理		
展開のアップグレードの失敗（Deployment Upgrade Failure）	ISE PIC ノードでアップグレードに失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE.ログを確認します。
アップグレード バンドルのダウンロードの失敗（Upgrade Bundle Download failure）	アップグレードバンドルのダウンロードが ISE-PIC ノードで失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE.ログを確認します。
CRL で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。
OCSP で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続（Secure LDAP connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。
CRL で失効した証明書が見つかったことによるセキュア syslog 接続の再接続（Secure syslog connection reconnect due to CRL found revoked certificate）	CRL チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。

アラーム名	アラームの説明	アラームの解決方法
OCSP で失効した証明書が見つかったことによるセキュアな syslog 接続の再接続（Secure syslog connection reconnect due to OCSP found revoked certificate）	OCSP チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	OCSP設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。
管理者アカウントがロック/無効（Administrator account Locked/Disabled）	パスワードの失効または不正なログイン試行のために、管理者アカウントがロックされているか、または無効になっています。詳細については、管理者パスワード ポリシーを参照してください。	管理者パスワードは、GUI または CLI を使用して、他の管理者によってリセットできます。
ERS が非推奨の URL を検出（ERS identified deprecated URL）	ERS が非推奨の URL を検出しました。	要求された URL が非推奨であるため、使用しないでください。
ERS が古い URL を検出（ERS identified out-dated URL）	ERS が古い URL を検出しました。	要求された URL が古いため、新しいものを使用してください。この URL は今後のリリースで削除されません。
ERS 要求 Content-Type ヘッダーが最新ではありません。	ERS 要求 Content-Type ヘッダーが最新ではありません。	要求 Content-Type ヘッダーで指定された要求のリソース バージョンが最新ではありません。これはリソース スキーマが変更されたことを意味します。いくつかの属性が追加または削除された可能性があります。古いスキーマをこのまま処理するために、ERS エンジンでデフォルト値が使用されます。
ERS XML 入力が XSS またはインジェクション攻撃の原因です（ERS XML input is a suspect for XSS or Injection attack）	ERS XML 入力が XSS またはインジェクション攻撃の原因になっています。	XML 入力を確認してください。

アラーム名	アラームの説明	アラームの解決方法
バックアップに失敗（Backup Failed）	Cisco ISE-PIC のバックアップ操作に失敗しました。	Cisco ISE-PIC とリポジトリ間のネットワーク接続を確認します。次の点を確認します。 • リポジトリに使用するクレデンシャルが正しいこと。 • リポジトリに十分なディスク領域があること。 • リポジトリ ユーザーが書き込み特権を持っていること。
CA サーバーがダウン（CA Server is down）	CA サーバーがダウンしています。	CA サービスが CA サーバーで稼働中であることを確認します。
CA サーバーが稼働中（CA Server is Up）	CA サーバーは稼働中です。	CA サーバーが稼働中であることを管理者に通知します。
証明書の有効期限（Certificate Expiration）	この証明書はまもなく有効期限が切れます。これが失効すると、Cisco ISE-PIC がクライアントとのセキュアな通信を確立しないようにします。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE-PIC を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書が失効（Certificate Revoked）	管理者は、内部 CA がエンドポイントに発行した証明書を取り消しました。	ISE-PIC フローに従って最初から新しい証明書を使用してプロビジョニングします。
証明書プロビジョニング初期化エラー（Certificate Provisioning Initialization Error）	証明書プロビジョニングの初期化に失敗しました。	複数の証明書でサブジェクトの CN（CommonName）属性が同じ値になっており、証明書チェーンを構築できません。システム内のすべての証明書を確認します。

アラーム名	アラームの説明	アラームの解決方法
証明書の複製に失敗（Certificate Replication Failed）	セカンダリ ノードへの証明書の複製に失敗しました。	証明書がセカンダリ ノードで無効であるか、他の永続的なエラー状態があります。セカンダリ ノードに矛盾する証明書が存在しないかどうかを確認します。見つかった場合は、セカンダリノードに存在するその証明書を削除し、プライマリの新しい証明書をエクスポートしてから削除し、その後インポートすることによって複製を再試行します。
証明書の複製に一時的に失敗（Certificate Replication Temporarily Failed）	セカンダリ ノードへの証明書の複製に一時的に失敗しました。	証明書は、ネットワークの停止などの一時的な条件によりセカンダリ ノードに複製されませんでした。複製は、成功するまで再試行されます。
証明書が失効（Certificate Expired）	この証明書の期限が切れています。Cisco ISE-PIC がクライアントとのセキュアな通信を確立しないようにします。ノードツーノード通信も影響を受ける場合があります。	証明書を交換します。信頼できる証明書の場合、発行元の認証局（CA）にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE-PIC を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書要求転送に失敗（Certificate Request Forwarding Failed）	証明書要求転送に失敗しました。	受信する証明書要求が送信者からの属性に一致することを確認します。
設定が変更（Configuration Changed）	Cisco ISE 設定が更新されています。このアラームは、ユーザーとエンドポイントに設定変更があってもトリガーされません。	設定変更が想定どおりであるかどうかを確認します。

アラーム名	アラームの説明	アラームの解決方法
CRL の取得に失敗（CRL Retrieval Failed）	サーバーから CRL を取得できません。これは、指定した CRL が使用できない場合に発生することがあります。	ダウンロード URL が正しく、サービスに使用可能であることを確認します。
DNS 解決に失敗（DNS Resolution Failure）	ノードで DNS 解決に失敗しました。	コマンド **ip name-server** で設定した DNS サーバーが到達可能であることを確認してください。 「CNAME <hostname of the node> に対する DNS 解決が失敗しました（DNS Resolution failed for CNAME <hostname of the node>）」というアラームが表示された場合は、各 Cisco ISE ノードの A レコードとともに CNAME RR を作成できることを確認します。
ファームウェアの更新が必要（Firmware Update Required）	このホスト上でファームウェアの更新が必要です。	Cisco Technical Assistance Center（TAC） に問い合わせてファームウェアアップデートを入手してください。
仮想マシン リソースが不十分（Insufficient Virtual Machine Resources）	このホストでは、CPU、RAM、ディスク容量、IOPS などの仮想マシン（VM）リソースが不十分です。	Cisco ISE Hardware Installation Guide に指定されている VM ホストの最小要件を確認します。
NTP サービスの障害（NTP Service Failure）	NTP サービスがこのノードでダウンしています。	これは、NTP サーバーと Cisco ISE-PIC ノードとの間に大きな時間差（1,000 秒を超える）があるために発生することがあります。NTP サーバーが正しく動作していることを確認し、**ntp server <servername>** CLI コマンドを使用して NTP サービスを再起動して、時間を同期します。

アラーム名	アラームの説明	アラームの解決方法
NTP 同期に失敗（NTP Sync Failure）	このノードに構成されているすべての NTP サーバーが到達不能です。	CLI で **show ntp** コマンドを実行してトラブルシューティングを行います。Cisco ISE-PIC から NTP サーバーに到達可能であることを確認します。NTP 認証が設定されている場合、キー ID と値がサーバーの対応する値に一致することを確認します。
スケジュールされた設定バックアップなし（No Configuration Backup Scheduled）	Cisco ISE-PIC 設定バックアップがスケジュールされていません。	設定バックアップのスケジュールを作成します。
操作 DB 消去に失敗（Operations DB Purge Failed）	操作データベースから古いデータを消去できません。このことは、M&T ノードがビジー状態である場合に発生する可能性があります。	[データ消去の監査（Data Purging Audit）] レポートをチェックし、used_space が threshold_space を下回ることを確認します。CLI を使用して M&T ノードにログインし、消去操作を手動で実行します。
複製に失敗（Replication Failed）	セカンダリ ノードは複製されたメッセージを消費できませんでした。	Cisco ISE-PIC の GUI にログインし、展開ページから手動同期を実行します。影響を受ける Cisco ISE-PIC ノードを登録解除してから登録します。
復元に失敗（Restore Failed）	Cisco ISE-PIC の復元操作に失敗しました。	Cisco ISE-PIC とリポジトリ間のネットワーク接続を確認します。リポジトリに使用するクレデンシャルが正しいことを確認します。バックアップファイルが破損していないことを確認します。CLI で **reset-config** コマンドを実行して、正常な既知の最終バックアップを復元します。
パッチに失敗（Patch Failure）	パッチ プロセスがサーバーで失敗しました。	サーバーにパッチ プロセスを再インストールします。
パッチに成功（Patch Success）	パッチ プロセスがサーバーで成功しました。	-

アラーム名	アラームの説明	アラームの解決方法
複製が停止（Replication Stopped）	ISE-PIC ノードがプライマリ ノードから設定データを複製できませんでした。	Cisco ISE-PIC の GUI にログインして [Deployment（展開）] ページから手動同期を実行するか、または影響を受けた Cisco ISE-PIC ノードを登録解除してから必須フィールドで再登録します。
エンドポイント証明書が期限切れ（Endpoint certificates expired）	エンドポイント証明書が日次スケジュール ジョブで期限切れとマークされました。	エンドポイント デバイスを再登録して新しいエンドポイント証明書を取得してください。
エンドポイント証明書が消去（Endpoint certificates purged）	期限切れのエンドポイント証明書が日次スケジュール ジョブによって消去されました。	アクションは必要ありません。これは、管理者が開始したクリーンアップ操作です。
複製低速エラー（Slow Replication Error）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速情報（Slow Replication Info）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速警告（Slow Replication Warning）	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
EST サービスの停止	EST サービスが停止しています。	CA および EST サービスが稼働しており、証明書サービスのエンドポイント サブ CA 証明書チェーンが完了したことを確認します。
EST サービスの稼働	EST サービスが稼働しています。	EST サービスが稼働中であることを管理者に通知します。
Smart Call Home の通信障害	Smart Call Home メッセージが正常に送信されませんでした。	Cisco ISE-PIC と Cisco システムの間でネットワーク接続があることを確認します。
テレメトリ メッセージの障害	テレメトリ メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。

アラーム名	アラームの説明	アラームの解決方法
ISE サービス		
AD コネクタを再起動する必要があります（AD Connector had to be restarted）	AD コネクタが突然シャットダウンし、再起動が必要となりました。	この問題が連続して発生する場合は、Cisco TAC にお問い合わせください。
Active Directory フォレストが使用不可（Active Directory forest is unavailable）	Active Directory フォレスト GC（グローバル カタログ）が使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
認証ドメインが使用不可（Authentication domain is unavailable）	認証ドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ID マッピングの認証非アクティビティ（ID Map. Authentication Inactivity）	ユーザー認証イベントが過去 15 分に ID マッピング サービスによって収集されませんでした。	これがユーザー認証が想定される時間（たとえば、勤務時間）である場合は、Active Directory ドメイン コントローラへの接続を確認します。
設定されたネーム サーバーがダウン（Configured nameserver is down）	設定されたネーム サーバーがダウンしているか、使用できません。	DNS 設定とネットワーク接続を確認します。
AD：マシン TGT のリフレッシュに失敗（AD: Machine TGT refresh failed）	ISE-PIC サーバー TGT（チケット認可チケット）の更新に失敗しました。これは AD 接続とサービスに使用されます。	Cisco ISE-PIC のマシンアカウントが存在し、有効であることを確認します。また、クロックスキュー、複製、Kerberos 設定やネットワークエラーも確認します。
AD：ISE アカウント パスワードの更新に失敗（AD: ISE account password update failed）	ISE-PIC サーバーは、AD のマシンアカウントパスワードを更新できませんでした。	Cisco ISE-PIC のマシンアカウントパスワードが変更されていないこと、およびマシンアカウントが無効でなく制限もされていないことを確認します。KDC への接続を確認します。
参加しているドメインが使用不可（Joined domain is unavailable）	参加しているドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。

アラーム名	アラームの説明	アラームの解決方法
ID ストアが使用不可（Identity Store Unavailable）	Cisco ISE-PIC のポリシーサービスノードは設定された ID ストアに到達できません。	Cisco ISE-PIC と ID ストア間のネットワーク接続を確認します。
AD：ISE のマシンアカウントにグループを取得するために必要な権限がない	Cisco ISE-PIC のマシンアカウントにグループを取得するために必要な権限がありません。	Cisco ISE-PIC のマシンアカウントに Active Directory のユーザーグループを取得する権限があるかどうかを確認します。
システムの状態		
ディスク I/O 使用率が高い（High Disk I/O Utilization）	Cisco ISE-PIC システムは、ディスク I/O 使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。
ディスク領域の使用率が高い（High Disk Space Utilization）	Cisco ISE-PIC システムは、ディスク領域の使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。
負荷平均が高い（High Load Average）	Cisco ISE-PIC システムは、負荷平均が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。

アラーム名	アラームの説明	アラームの解決方法
メモリ使用率が高い（High Memory Utilization）	Cisco ISE-PIC システムは、メモリ使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。
操作DBの使用率が高い（High Operations DB Usage）	ノードをモニタする Cisco ISE-PIC は、syslog データの量が想定よりも多くなっています。	操作データの消去設定ウィンドウを確認して削減します。
ヘルス ステータスが使用不可	モニタリングノードは Cisco ISE-PIC ノードからヘルス ステータスを受信しませんでした。	Cisco ISE-PIC ノードが稼働中であることを確認します。Cisco ISE-PIC ノードがモニタリングノードと通信できることを確認します。
プロセスがダウン（Process Down）	Cisco ISE-PIC プロセスの 1 つが動作していません。	Cisco ISE-PIC アプリケーションを再起動します。
OCSP トランザクションしきい値に到達（OCSP Transaction Threshold Reached）	OCSP トランザクションしきい値に到達しました。このアラームは、内部 OCSP サービスが大量のトラフィックに到達するとトリガーされます。	システムに十分なリソースがあるかどうかを確認してください。
ライセンシング		
PIC ライセンスの期限切れ（PIC License Expired）	Cisco ISE-PIC ノードにインストールされたライセンスの期限が切れました。	シスコ アカウント チームに問い合わせて、新しいライセンスを購入してください。
PIC ライセンスが 30 日以内に期限が切れます（PIC License expiring within 30 Days）	Cisco ISE-PIC ノードにインストールされたライセンスが 30 日後に期限切れになります。	ISE-PIC ライセンスの延長については、シスコの営業チームにお問い合わせください。
PIC のライセンスが 60 日以内に期限が切れます（License expiring within 60 Days）	Cisco ISE-PIC ノードにインストールされたライセンスが 60 日後に期限切れになります。	ISE-PIC ライセンスの延長については、シスコの営業チームにお問い合わせください。
PIC のライセンスが 90 日以内に期限が切れます（License expiring within 90 Days）	Cisco ISE-PIC ノードにインストールされたライセンスが 90 日後に期限切れになります。	ISE-PIC ライセンスの延長については、シスコの営業チームにお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
システム エラー		
ログ収集エラー（Log Collection Error）	コレクタプロセスをモニターする Cisco ISE-PIC がポリシーサービスノードから生成された監査ログを保持できません。	これは、ポリシー サービス ノードの実際の機能に影響を与えません。その他の解決のために TAC に連絡してください。
スケジュールされているレポートのエクスポートに失敗（Scheduled Report Export Failure）	設定されたリポジトリにエクスポートされたレポート（CSV ファイル）をコピーできません。	設定されたリポジトリを確認します。それが削除されていた場合は、再度追加します。それが使用できないか、またはそれに到達できない場合は、リポジトリを再設定して有効にします。

アラームは、Cisco ISE-PIC にユーザーまたはエンドポイントを追加する場合にはトリガーされません。

アラーム設定

次の表では、[アラーム設定（Alarm Settings）] ウィンドウ（**[設定（Settings）]** > **[アラーム設定（Alarm Settings）]**）のフィールドについて説明します。

フィールド名	説明
アラーム タイプ（Alarm Type）	アラームタイプ。
アラーム名（Alarm Name）	アラームの名前。
説明（Description）	アラームの説明。
推奨されるアクション（Suggested Actions）	アラームがトリガーされたときに実行されるアクション。
ステータス（Status）	アラームルールの有効化または無効化。

フィールド名	説明
重大度	アラームの重大度レベルを選択します。有効なオプションは次のとおりです。 • [重大（Critical）]：重大なエラーの条件を示します。 • [警告（Warning）]：正常ではあるものの重要な状態を示します。これがデフォルトの条件です。 • [情報（Info）]：情報メッセージを示します。
syslog メッセージを送信（Send Syslog Message）	Cisco ISE-PIC で生成される各システムアラームの syslog メッセージを送信します。
複数の電子メールアドレスをカンマで区切って入力	電子メールアドレスまたは ISE-PIC 管理者名あるいはその両方のリスト。
電子メールのメモ（0 ～ 4,000 文字）	システムアラームに関連付けるカスタムテキストメッセージ。

カスタム アラームの追加

シスコ ISE-PIC には、5 つのデフォルトのアラームタイプ（設定変更、高ディスク I/O 使用率、高ディスク容量使用率、高メモリ使用率、ISE 認証非アクティブ）があります。シスコ定義のシステムアラームは [アラーム設定（Alarms Settings）] ページ（[設定（Settings）] > [アラーム設定（Alarms Settings）]）に表示されます。システム アラームだけを編集できます。

既存のシステム アラームの他に、既存のアラーム タイプでカスタム アラームを追加、編集、削除できます。

各アラーム タイプで最大 5 つのアラームを作成でき、アラームの合計数は 200 に制限されます。

アラームを追加するには、次の手順を実行します。

ステップ 1 [設定（Settings）] > [アラーム設定（Alarm Settings）] を選択します。

ステップ 2 [アラームの設定（Alarm Configuration）] タブで、[追加（Add）] をクリックします。

ステップ 3 次の必須詳細情報を入力します。詳細については、「アラーム設定」の項を参照してください。

アラームタイプに基づいて、追加の属性が [アラームの設定（Alarm Configuration）] ページに表示されます。たとえば、設定変更アラームには、[オブジェクト名（Object Name）]、[オブジェクトタイプ（Object Types）] および [管理者名（Admin Name）] フィールドが表示されます。さまざまな基準で同じアラームの複数のインスタンスを追加できます。

ステップ 4 **[送信（Submit）]** をクリックします。

着信トラフィックを検証する TCP ダンプユーティリティ

パケットをスニッフィング する TCP ダンプユーティリティを使用して、予定していたパケットがノードに到達したかどうかを確認できます。たとえば、レポートに示されている着信認証またはログがない場合、着信トラフィックがないのではないか、または着信トラフィックが Cisco ISE に到達できないのではないかと疑われる場合があります。このような場合、検証するためにこのツールを実行できます。

TCP ダンプオプションを設定し、ネットワークトラフィックからデータを収集して、ネットワークの問題をトラブルシューティングできます。

⚠

注意 TCP ダンプを起動すると、以前のダンプ ファイルは自動的に削除されます。以前のダンプ ファイルを保存するには、新しい TCP ダンプ セッションを開始する前に、「TCP ダンプ ファイルの保存」の項の説明に従ってタスクを実行します。

ネットワーク トラフィックのモニターリングでの TCP ダンプの使用

始める前に

[TCP ダンプ（TCP Dump）] ウィンドウの [ネットワーク インターフェイス（Network Interface）] ドロップダウンリストには、IPv4 または IPv6 アドレスが設定されているネットワーク インターフェイス カード（NIC）のみが表示されます。VMware のデフォルトでは、すべての NIC が接続されるため、すべての NIC に IPv6 アドレスが設定されて、[ネットワーク インターフェイス（Network Interface）] ドロップダウンリストに表示されます。

ステップ 1 **[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般ツール（General Tools）]** > **[TCP ダンプ（TCP Dump）]** を選択します。

ステップ 2 [ホスト名（Host Name）] ドロップダウンリストから、TCP ダンプユーティリティのソースを選択します。

ステップ 3 [ネットワーク インターフェイス（Network Interface）] ドロップダウンリストから、モニターするインターフェイスを選択します。

ステップ 4 [無差別モード（Promiscuous Mode）] トグルボタンをクリックして、[オン（On）] または [オフ（Off）] にします。デフォルトは [オン（On）] です。

無差別モードは、ネットワーク インターフェイスがシステムの CPU にすべてのトラフィックを渡すデフォルト パケット スニッフィング モードです。この設定のままにすることを推奨します。

ステップ 5 [フィルタ（Filter）] フィールドに、フィルタ処理のもとになるブール式を入力します。

サポートされている標準 TCP ダンプフィルタ式は、次のとおりです。

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

ステップ 6 [開始（Start）] をクリックして、ネットワークのモニターリングを開始します。

ステップ 7 十分な量のデータが収集された後で [停止（Stop）] をクリックするか、最大パケット数（500,000）が累積されてプロセスが自動的に終了するまで待機します。

（注） Cisco ISE は、1500 より大きいフレーム（ジャンボ フレーム）の MTU をサポートしません。

TCP ダンプ ファイルの保存

始める前に

「ネットワークトラフィックのモニタリングでの TCP ダンプの使用」の項の説明に従って、タスクを完了しておく必要があります。

（注） Cisco ISE CLI を使用して TCP ダンプにアクセスすることもできます。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。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [TCP ダンプ（TCP Dump）]** を選択します。

ステップ 2 [フォーマット（Format）] ドロップダウンリストからオプションを選択します。[可読（Human Readable）] がデフォルトです。

ステップ 3 [ダウンロード（Download）] をクリックし、目的の場所に移動して、[保存（Save）] をクリックします。

ステップ 4 （任意）以前のダンプファイルを保存せずに削除するには、[削除（Delete）] をクリックします。

TCP ダンプの設定

次の表では、ネットワーク インターフェイスのパケットの内容をモニターし、ネットワークで問題が発生したときにはトラブルシューティングするために使用する **tcpdump** ユーティリティ ページのフィールドについて説明します。このページへのナビゲーション パスは、**[トラブルシューティング（Troubleshoot）]** です。

表 *26 : TCP* ダンプの設定

オプション	使用上のガイドライン
ステータス	• [停止済み（Stopped）] : tcpdump ユーティリティは実行されていません。 • [開始（Start）] : tcpdump ユーティリティによるネットワークのモニタリングを開始する場合にクリックします。 • [停止（Stop）] : tcpdump ユーティリティを停止する場合にクリックします。
ホスト名（Host Name）	モニターするホストの名前をドロップダウン リストから選択します。
ネットワーク インターフェイス（Network Interface）	モニターするネットワーク インターフェイスの名前をドロップダウン リストから選択します。 （注） IPv4 アドレスまたは IPv6 アドレスを持つすべてのネットワーク インターフェイス カード（NIC）を Cisco ISE 管理者ポータルに表示されるように設定する必要があります。
無差別モード（Promiscuous Mode）	• [オン（On）] : 無差別モードを有効にする場合にクリックします（デフォルト）。 • [オフ（Off）] : 無差別モードを無効にする場合にクリックします。 無差別モードがデフォルトのパケット スニッフィング モードです。有効に設定しておくことを推奨します。このモードでは、ネットワーク インターフェイスはすべてのトラフィックをシステムの CPU に渡します。
フィルタ	フィルタリング基準として使用するブール式を入力します。サポートされている標準 tcpdump フィルタ式 : ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123

オプション	使用上のガイドライン
フォーマット（Format）	tcpdump ファイルのフォーマットを選択します。

ダンプ ファイル（Dump File）	最後のダンプ ファイルに記録された、次のようなデータを表示します。
	Last created on Wed Apr 27 20:42:38 UTC 2011 by admin
	`File size: 3,744 bytes`
	`Format: Raw Packet Data`
	`Host Name: Positron`
	`Network Interface: GigabitEthernet 0`
	`Promiscuous Mode: On`
	• [ダウンロード（Download）]：最新のダンプ ファイルをダウンロードする場合にクリックします。
	• [削除（Delete）]：最新のダンプ ファイルを削除する場合にクリックします。

ロギング メカニズム

Cisco ISE-PIC ロギング メカニズム

syslog の消去の設定

このプロセスを使用して、ローカル ログ格納期間を設定し、特定の期間後にローカル ログを削除します。

Smart Call Home

Smart Call Home（SCH）は、ネットワーク内の Cisco ISE-PIC デバイスを監視し、重大なイベントに関して電子メールで知らせます。電子メールには、環境情報と修復に関するアドバイスが記載されたリアルタイムのアラートが含まれています。

- [シスコアカウント（Cisco Account）]：SCH からの電子メールを受信できるようにシスコアカウントを入力します。この ID は、お客様に影響する重大な問題が SCH によって発見された場合の連絡にも使用される場合があります。
- [トランスポートゲートウェイ（Transport Gateway）]：セキュリティを強化するために、Cisco ISE とシスコの外部テレメトリ サーバーの間でプロキシを使用することができます。

そうする場合は、このオプションをオンにして、プロキシ サーバーの FQDN を入力します。

シスコでは、Cisco.com からダウンロードできるトランスポート ゲートウェイ用のソフトウェアを提供しています。このソフトウェアは、Linux サーバー上で実行されます。RHEL サーバーでの Transport Gateway ソフトウェアの導入方法については、『Smart Call Home Deployment Guide』を参照してください。

SCH 機能の有効化については、Smart Call Home サービスの登録（188 ページ）を参照してください。

Smart Call Home プロファイル

Smart Call Home プロファイルは、デバイスでモニターされるイベントのタイプを決定します。Cisco ISE-PIC には、次のデフォルト プロファイルがあります。

- ciscotac-1：匿名レポートのために使用されます
- isesch-1：Smart Call Home 機能のために使用されます

匿名レポートのために使用されるデフォルト プロファイル（ciscotac-1）を編集することはできません。

Anonymous Reporting

Cisco ISE-PIC は、ユーザーの展開に関する非機密情報を安全に収集します。このデータは、Cisco ISE-PIC の使用状況をより詳しく把握し、製品と製品が提供するさまざまなサービスを向上させる目的で収集されます。

デフォルトでは、anonymous reporting は有効になっています。anonymous reporting を使用不可にするには、ISE-PIC 管理者ポータル**[設定（Settings）] > [Smart Call Home]**で行うことができます。

Smart Call Home サービスの登録

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

ステップ 2 次のいずれかを実行します。

- SCH のすべての機能をオンにする（Turn on full SCH capability）
- デフォルト SCH テレメトリ設定を保持して匿名データのみを送信する（Keep the default SCH telemetry settings and send only anonymous data）
- すべて無効にする（Disable everything）

ステップ 3 （[SCH のすべての機能をオンにする（Turn on full SCH capability）] オプションを選択した場合のみ）[登録ステータス（Registration Status）] エリアに電子メール アドレスを入力します。

ステップ 4 （オプション）[Transport Gateway] チェックボックスをオンにして、Transport Gateway の URL を入力します。

ステップ 5 [保存（Save）] をクリックします。

SCH のすべての機能を有効にしている場合は、アクティベーション リンクが記載された電子メールを受信します。アクティベーション リンクをクリックして記載されている指示に従い、登録を完了します。

Active Directory のトラブルシューティング

Active Directory と Cisco ISE-PIC の統合の前提条件

この項では、Cisco ISE-PIC と統合する Active Directory を設定するために必要な手動での作業手順について説明します。ただしほとんどの場合、Cisco ISE-PIC が Active Directory を自動的に設定するようにできます。次に、Cisco ISE-PIC と Active Directory を統合するための前提条件を示します。

- AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。
- Cisco ISE-PIC サーバーと Active Directory 間の時間を同期するために Network Time Protocol（NTP）サーバー設定を使用します。Cisco ISE-PIC CLI で NTP を設定できます。
- Cisco ISE-PIC の参加先ドメインでは、少なくとも 1 つのグローバル カタログ サーバーが動作し、Cisco ISE-PIC からアクセス可能である必要があります。

さまざまな操作の実行に必要な Active Directory アカウント権限

参加操作	脱退処理	Cisco ISE-PIC マシン アカウント
参加操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE-PIC マシンアカウントがあるかどうかの確認） • ドメインに Cisco ISE-PIC マシン アカウントを作成する権限（マシン アカウントが存在しない場合） • 新しいマシン アカウントに属性を設定する権限（Cisco ISE-PIC マシン アカウント パスワード、SPN、dnsHostname など）	脱退操作には、次のアカウント権限が必要です。 • Active Directory を検索する権限（Cisco ISE-PIC マシンアカウントがあるかどうかの確認） • ドメインから Cisco ISE-PIC マシンアカウントを削除する権限 強制脱退（パスワードなしの脱退）を実行する場合、ドメインからマシン アカウントは削除されません。	Active Directory 接続と通信する Cisco ISE-PIC マシン アカウントには、次の権限が必要です。 • パスワードを変更する。 • 接続されるユーザーおよびマシンに対応するユーザーおよびマシンオブジェクトを読み取る権限 • 情報を取得するために Active Directory をクエリする権限（信頼ドメイン、代替の UPN サフィックスなど） • tokenGroups 属性を読み取る権限 Active Directory でマシン アカウントを事前に作成できます。SAM の名前が Cisco ISE-PIC アプライアンスのホスト名と一致する場合は、参加操作中に検索して再利用します。 複数の参加操作が実行される場合、参加ごとに複数のマシン アカウントが Cisco ISE-PIC 内で保持されます。

（注） 参加操作または脱退操作に使用するクレデンシャルは Cisco ISE-PIC に保存されません。新規作成された Cisco ISE-PIC マシンアカウントのログイン情報のみが保存されます。

Microsoft Active Directory のセキュリティポリシー「**ネットワーク アクセス：SAM へのリモートの呼び出しを許可するクライアントを制限する**」が改訂されました。このため、Cisco ISE は 15 日ごとにマシンアカウントのパスワードを更新できない場合があります。マシンアカウントのパスワードが更新されない場合、Cisco ISE は Microsoft Active Directory を介してユーザー

を認証しません。このイベントを通知するために、Cisco ISE ダッシュボードに [AD：ISE アカウントパスワードの更新に失敗（AD: ISE account password update failed）] アラームが表示されます。

（注） この問題は、Windows Server 2016 Active Directory 以降および Windows 10 バージョン 1607 の制限により発生します。この制限を克服するには、Windows Server 2016 Active Directory 以降または Windows 10 バージョン 1607 を Cisco ISE と統合する場合、レジストリ：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam のレジストリ値を non-zero から空白に設定して、すべてにアクセスを提供する必要があります。これにより、Cisco ISE がそのマシンのアカウントパスワードを更新できるようになります。

セキュリティポリシーにより、ユーザーはローカル セキュリティ アカウント マネージャ（SAM）データベース内と Microsoft Active Directory 内のユーザーとグループを列挙できます。Cisco ISE がマシンアカウントのパスワードを更新できるようにするには、Microsoft Active Directory の設定が正しいことを確認します。影響を受ける Windows オペレーティングシステムと Windows Server のバージョン、ネットワークにおけるこのセキュリティポリシーの意味、必要な変更の詳細については、以下を参照してください。

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

通信用に開放するネットワークポート

プロトコル	ポート（リモートローカル）	ターゲット	注記
DNS（TCP/UDP）	49152 以上の乱数	DNS サーバー/AD ドメイン コントローラ	—
MSRPC	445	ドメインコントローラ	—
Kerberos（TCP/UDP）	88	ドメインコントローラ	MS AD/KDC
LDAP（TCP/UDP）	389	ドメインコントローラ	—
LDAP（GC）	3268	グローバル カタログ サーバー	—
NTP	123	NTP サーバー/ドメイン コントローラ	—
IPC	80	セカンダリ ISE-PIC ノードの場合	—

Active Directory でISE-PIC

ISE-PIC では、Active Directory ドメイン コントローラによって生成される Active Directory ログイン監査イベントを利用して、ユーザー ログイン情報を収集します。ISE ユーザーが接続を行い、ユーザー ログイン情報を取得することができるように、Active Directory サーバーを適切に設定する必要があります。ここでは、ISE-PIC をサポートするように Active Directory ドメイン コントローラを設定する方法（Active Directory 側からの設定）について説明します。

をサポートするように Active Directory ドメインコントローラを設定するには（Active Directory 側からの設定）、次の手順に従います：

（注） すべてのドメインのすべてのドメインコントローラを設定する必要があります。

1. ISE-PIC から Active Directory の参加ポイントとドメイン コントローラを設定します。Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE-PIC ノードの参加 （22 ページ）および#unique_218を参照してください。
2. ドメイン コントローラごとに WMI を設定します。#unique_219を参照してください。
3. Active Directory で次の操作を実行します。
   - パッシブ ID サービス の Active Directory の設定 （192 ページ）
4. （オプション）Active Directory で ISE により実行された自動設定のトラブルシューティングを行うには、次の操作を実行します。
   - Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定 （197 ページ）
   - ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限 （197 ページ）
   - ドメイン コントローラで DCOM を使用するための権限 （199 ページ）
   - WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （201 ページ）
   - AD ドメインコントローラのセキュリティイベントログへのアクセス権の付与 （202 ページ）

パッシブ ID サービス の Active Directory の設定

ISE-PIC 、ユーザー ログイン情報を収集するため、Active Directory ドメイン コントローラにより生成される Active Directory ログイン監査イベントが使用されます。ISE-PIC は Active Directory に接続し、ユーザー ログイン情報を取得します。

次の手順は、Active Directory ドメイン コントローラから実行する必要があります。

ステップ 1 該当する Microsoft のパッチが Active Directory ドメイン コントローラにインストールされていることを確認します。

- Windows Server 2008 には次のパッチが必要です。
  - http://support.microsoft.com/kb/958124

    このパッチは Microsoft の WMI のメモリリークを修正し、ISE がドメインコントローラとの正常な接続を確立できないようにします。

  - http://support.microsoft.com/kb/973995

    このパッチは、Microsoft WMI の別のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザー ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。

- Windows Server 2008 R2 では、（SP1 がインストールされていない場合）次のパッチが必要です。
  - http://support.microsoft.com/kb/981314

    このパッチは、Microsoft WMI のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザー ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。

  - http://support.microsoft.com/kb/2617858

    このパッチは、Windows Server 2008 R2 での予期しない起動やログイン プロセスの遅れを解消します。

- Windows プラットフォームの WMI 関連問題には、次のリンクにリストされているパッチが必要です。
  - http://support.microsoft.com/kb/2591403

  これらのホットフィックスは、WMI サービスおよび関連コンポーネントの動作と機能に関連付けられます。

ステップ 2 Active Directory がユーザー ログイン イベントを Windows セキュリティ ログに記録するのを確認します。

[監査ポリシー（Audit Policy ）]の設定（[グループポリシー管理（Group Policy Management）] の設定の一部）が、正常なログインによって Windows セキュリティログに必要なイベントが生成されるように設定されていることを確認します（これはデフォルトの Windows 設定ですが、この設定が適切であることを明示的に確認する必要があります）。

ステップ 3 ISE-PIC が Active Directory に接続するための十分な権限を持つ Active Directory ユーザーを設定する必要があります。次の手順では、管理ドメイン グループのユーザー、または管理ドメイン グループではないユーザーに対して権限を定義する方法を示します。

- Active Directory ユーザーが Domain Admin グループのメンバーである場合に必要な権限
- Active Directory ユーザーが Domain Admin グループのメンバーでない場合に必要な権限

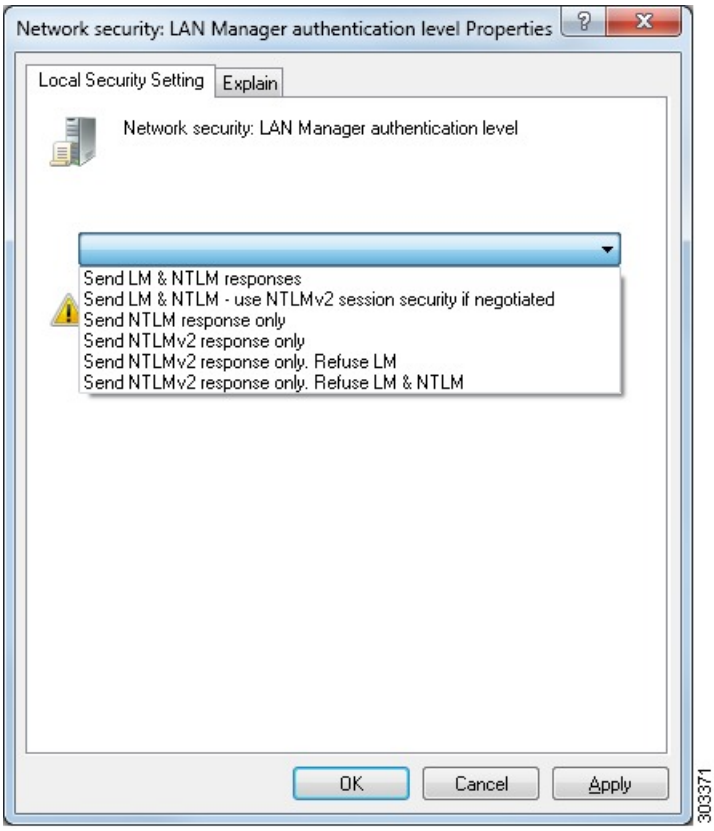
ステップ 4 ISE-PIC によって使用される Active Directory ユーザーは、NT Lan Manager（NTLM）v1 または v2 のいずれかによって認証を受けることができます。ISE-PIC と Active Directory ドメイン コントローラ間の正常な認証済み接続を確実に行うために、Active Directory NTLM の設定が ISE-PIC NTLM の設定と合っていることを確認する必要があります。次の表に、すべての Microsoft NTLM オプションと、サポート対象の ISE-PIC NTLM アクションを示します。ISE-PIC が NTLMv2 に設定される場合、記載されている 6 つのオプションがすべてサポートされます。NTLMv1 をサポートするように ISE-PIC が設定されている場合、最初の 5 つのオプションだけがサポートされます。

表 *27 : ISE-PIC* と *AD NTLM* のバージョン設定に基づいてサポートされる認証タイプ

ISE-PICISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション（NTLMv1 NTLMv2）	**NTLMv1**	**NTLMv2**
LM & NTLM応答を送信接続を許可接続を許可（Send LM & NTLM responses connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
LM & NTLMを送信：ネゴシエートされた接続が許可された場合にNTLMv2セッションセキュリティを使用接続を許可（Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLM応答を送信接続を許可（Send NTLM response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみNTLMv2応答を送信接続を許可（Send NTLMv2 response only connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます
NTLMv2応答のみを送信（Send NTLMv2 response only）。LMを拒否接続を許可接続を許可（Refuse LM connection is allowed connection is allowed）	接続が受け入れられます	接続が受け入れられます

ISE-PICISE NTLM の設定オプションおよび Active Directory（AD）NTLM の設定オプション（NTLMv1 NTLMv2）	NTLMv1	NTLMv2
NTLMv2応答のみを送信（Send NTLMv2 response only）。LM & NTLMを拒否接続を拒否接続を許可（Refuse LM & NTLM connection is refused connection is allowed）	接続は拒否されます	接続が受け入れられます

図 *10 : MS NTLM* 認証タイプのオプション



ステップ 5 Active Directory ドメイン コントローラで `dllhost.exe` へのトラフィックを許可するファイアウォール ルールを作成していることを確認します。

ファイアウォールをオフにするか、または次のポートへの特定の IP（ISE-PIC IP アドレス）のアクセスを許可することができます。

- TCP 135：一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 137：NetBIOS 名前解決

- UDP 138：NetBIOS データグラム サービス
- TCP 139：NetBIOS セッション サービス
- TCP 445：SMB

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dllhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォール ルールを、特定の IP アドレス（ISE-PIC IP）に割り当てることができます。

Windows 監査ポリシーの設定

監査ポリシー（**グループ ポリシー管理**設定の一部）が正常なログインを許可していることを確認します。これには、AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントを生成する必要があります。これはデフォルトの Windows 設定ですが、この設定が正しいことを確認する必要があります。

ステップ 1 **[スタート]** > **[Programs]** > **[Administrative Tools]** > **[Group Policy Management]** を選択します。

ステップ 2 [Domains] で関連するドメインに移動し、ナビゲーション ツリーを展開します。

ステップ 3 [Default Domain Controller Policy] を選択し、右クリックして、[編集] を選択します。

グループ ポリシー管理エディターが表示されます。

ステップ 4 **[デフォルトのドメイン コントローラ ポリシー（Default Domain Controllers Policy）]** > **[コンピュータ設定（Computer Configuration）]** > **[ポリシー（Policies）]** > **[Windows 設定（Windows Settings）]** > **[セキュリティ設定（Security Settings）]** の順に選択します。

- Windows Server 2003 または Windows Server 2008（R2 以外）の場合は **[ローカル ポリシー（Local Policies）]** > **[監査ポリシー（Audit Policy）]** の順に選択します。2 つのポリシー項目（[Audit Account Logon Events] と [Audit Logon Events]）で、対応する [Policy Setting] に [Success] 状態が直接的または間接的に含まれていることを確認します。[Success] 状況を間接的に含めるには、[Policy Setting] に [Not Defined] を設定します。この場合、上位ドメインから有効値が継承されるため、[Success] 状態を明示的に含めるようにその上位ドメインの [Policy Setting] を設定する必要があります。
- Windows Server 2008 R2 および Windows 2012 の場合、**[Advanced Audit Policy Configuration]** > **[Audit Policies]** > **[Account Logon]** を選択します。2 つのポリシー項目（[Audit Kerberos Authentication Service] と [Audit Kerberos Service Ticket Operations]）に対応する [Policy Setting] に、前述のように [Success] 状態が直接または間接的に含まれていることを確認します。

（注） Active Directory ドメイン コントローラの設定で RC4 暗号が無効になっている場合を除き、Cisco ISE は Active Directory との通信に Kerberos プロトコルで RC4 暗号を使用します。Active Directory で [ネットワークセキュリティ：Kerberosで許可される暗号タイプを設定（Network Security: Configure Encryption Types Allowed for Kerberos）] オプションを使用すると、Kerberos プロトコルで許可される暗号タイプを設定できます。

ステップ 5 [監査ポリシー] の項目設定が変更されている場合は、`gpupdate /force` を実行して新しい設定を強制的に有効にする必要があります。

Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows Server 2012 および Windows Server 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティングシステムの特定のレジストリ キーを完全に制御することはできません。Microsoft Active Directory の管理者は、Microsoft Active Directory ユーザーに次のレジストリキーに対する完全制御権限を提供する必要があります。

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

次の Microsoft Active Directory バージョンでは、レジストリを変更する必要はありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、まず Microsoft Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーアイコンを右クリックし、[所有者（Owner）] タブを選択します。

ステップ 2 [アクセス許可（Permissions）] をクリックします。

ステップ 3 [詳細設定（Advanced）] をクリックします。

ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限

Windows 2012 R2 の場合は、Microsoft AD ユーザーに次のレジストリキーに対する完全制御権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell で次のコマンドを使用して、レジストリキーに完全な権限が付与されているかどうかを確認します。

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

Microsoft AD ユーザーがドメイン管理者グループではなく、ドメインユーザーグループに所属している場合は、次の権限が必要です。

- ISE-PIC がドメインコントローラに接続できるようにするには、レジストリキーを追加します。
- ドメイン コントローラで DCOM を使用するための権限 （199 ページ）
- WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 （201 ページ）

これらの権限は、次のバージョンの Microsoft AD でのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ドメインコントローラへの ISE-PIC の接続を許可するためにレジストリキーを追加

ISE-PIC がドメインユーザーとして接続し、ログイン認証イベントを取得できるようにするには、ドメインコントローラにいくつかのレジストリ キーを手動で追加する必要があります。エージェントはドメインコントローラまたはドメイン内のマシンには必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate キーの値には、2 つのスペースが含まれていることを確認します。レジストリを手動で更新する場合は、2 つのスペースのみを含める必要があり、引用符は含めないでください。レジストリを手動で更新する際は、AppID、DllSurrogate、およびその値に引用符が含まれていないことを確認してください。

前述のスクリプトに示すように、ファイルの末尾の空の行を含めて、空の行は保持します。

Windows コマンドプロンプトで次のコマンドを使用して、レジストリキーが作成され、正しい値が設定されているかどうかを確認します。

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

ドメイン コントローラで DCOM を使用するための権限

ISE-PIC パッシブ ID サービスに使用される Microsoft Active Directory ユーザーには、ドメイン コントローラ サーバーで DCOM を使用する権限が必要です。**dcomcnfg** コマンドラインツールを使用して権限を設定します。

ステップ 1 コマンド ラインから **dcomcnfg** ツールを実行します。

ステップ 2 [コンポーネントサービス（Component Services）] を展開します。

ステップ 3 **[コンピュータ（Computers）]** > **[マイコンピュータ（My Computer）]** を展開します。

ステップ 4 メニューバーで [アクション（Action）] を選択し、[プロパティ（Properties）] をクリックして [COM セキュリティ（COM Security）] をクリックします。

ステップ 5 Cisco ISE がアクセスと起動の両方に使用するアカウントには許可権限が必要です。4 つのオプション（[アクセス権限Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対する [制限の編集（Edit Limits）] と [デフォルトの編集（Edit Default）]）のすべてに Microsoft Active Directory ユーザーを追加します。

ステップ 6 [アクセス権限（Access Permissions）] と [起動およびアクティブ化の権限（Launch and Activation Permissions）] の両方に対してローカルアクセスとリモートアクセスをすべて許可します。

図 *11 : [*アクセス権限（***Access Permissions***）*]* に対するローカルアクアセスとリモートアクセス

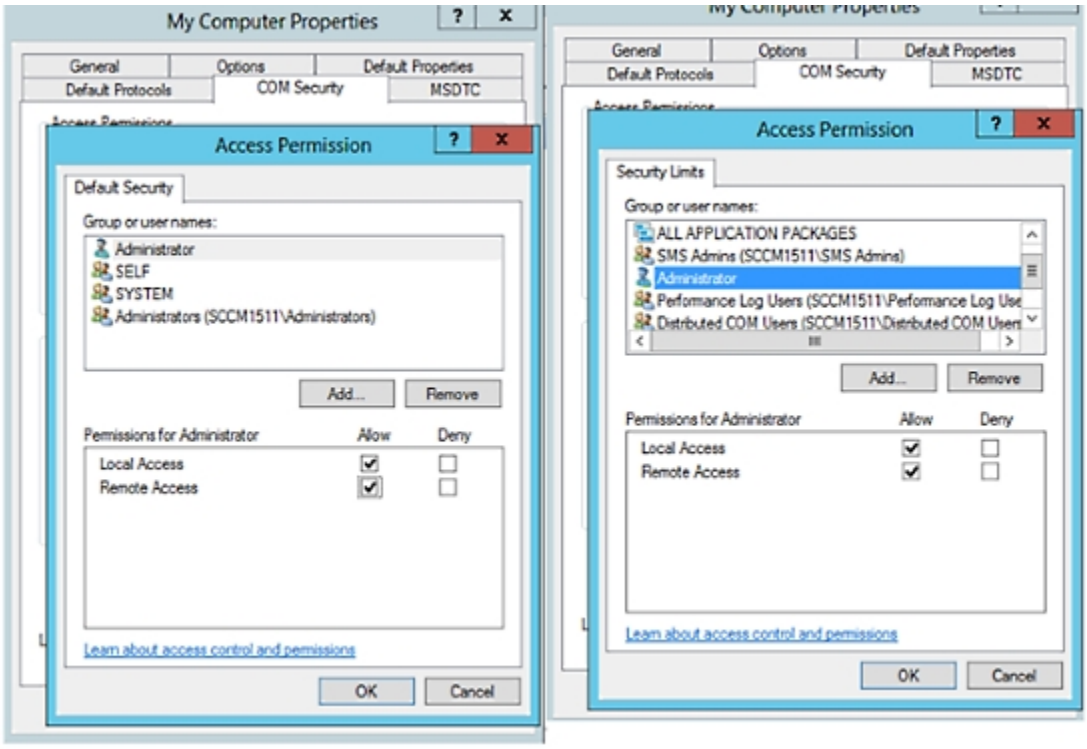
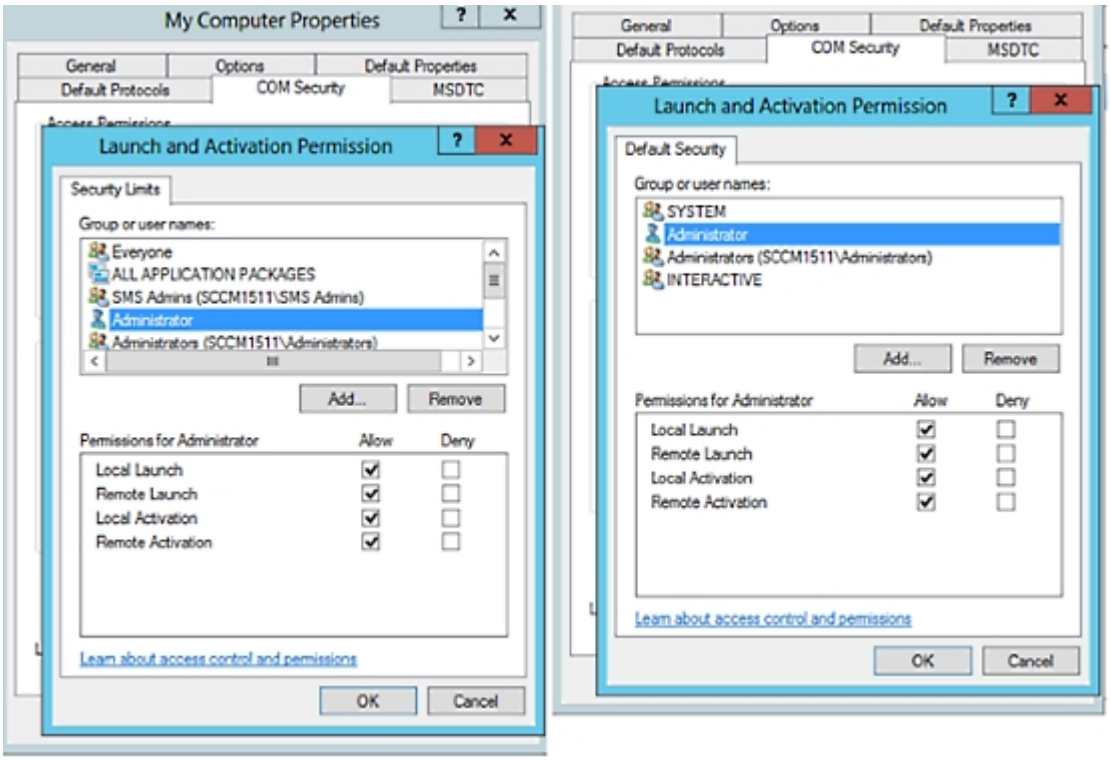


図 *12 : [*起動およびアクティブ化の権限（***Launch and Activation Permissions***）*]* のローカルアクセスとリモートアクセス



WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Microsoft Active Directory ユーザーには実行メソッドおよびリモートの有効化のための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

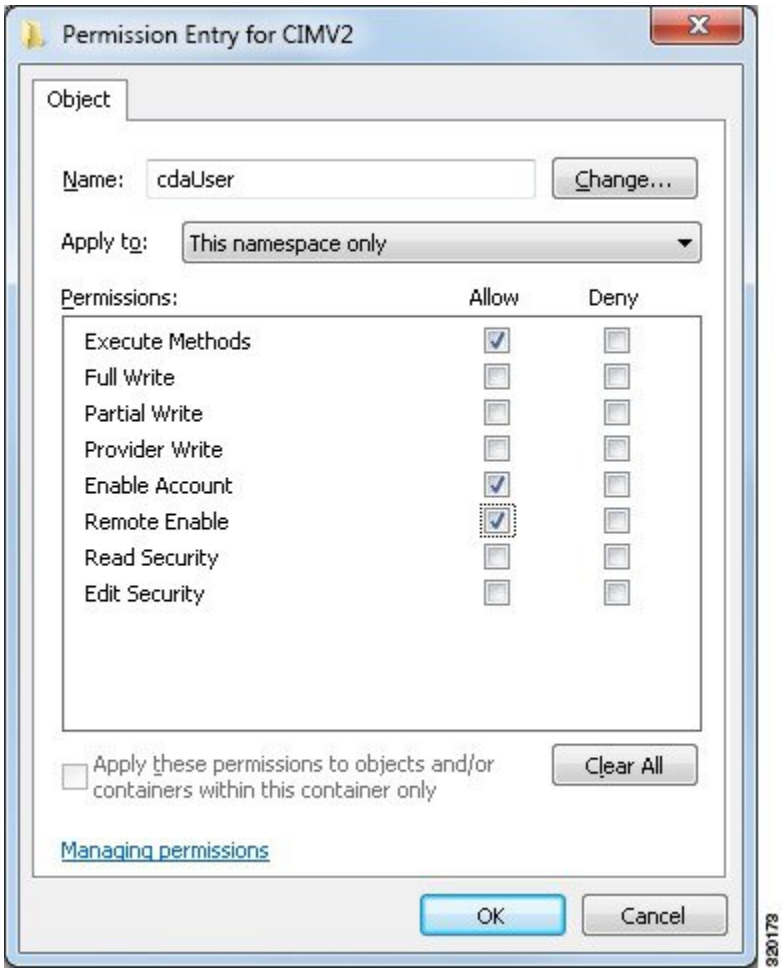
ステップ 1 **[スタート（Start）]** > **[実行（Run）]** を選択し、`wmimgmt.msc` と入力します。

ステップ 2 **[WMI Control]** を右クリックし、**[プロパティ（Properties）]** をクリックします。

ステップ 3 **[セキュリティ（Security）]** タブで、**[ルート（Root）]** を展開し、**[CIMV2]** を選択します。

ステップ 4 [セキュリティ（Security）] をクリックします。

ステップ 5 次のイメージに示すように、Microsoft Active Directory ユーザーを追加し、必要な権限を設定します。



AD ドメインコントローラのセキュリティイベントログへのアクセス権の付与

Windows 2008 以降では、ISE-PIC ID マッピング ユーザーを Event Log Reader と呼ばれるグループに追加することで、AD ドメイン コントローラのログへのアクセス権を付与できます。

Windows のすべての旧バージョンでは、次に示すようにレジストリ キーを編集する必要があります。

ステップ 1 セキュリティ イベント ログへのアクセス権を委任するには、アカウントの SID を検索します。

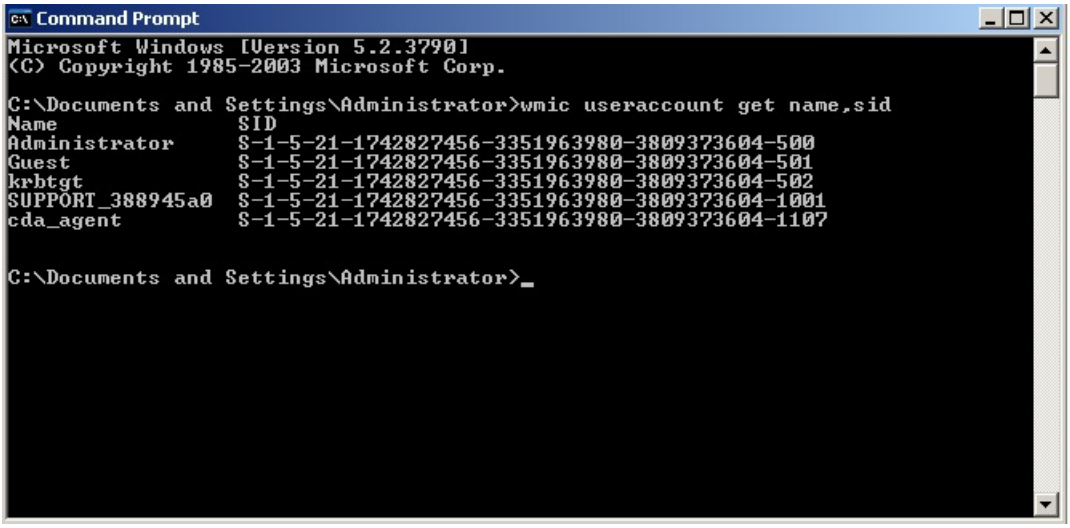
ステップ 2 すべての SID アカウントを表示するには、次の図に示すように、コマンド ラインから次のコマンドを使用します。

```
wmic useraccount get name,sid
```

特定のユーザー名とドメインに対して、次のコマンドを使用することもできます。

```
wmic useraccount where name="iseUser" get domain,name,sid
```

図 *13* : すべての *SID* アカウントの表示



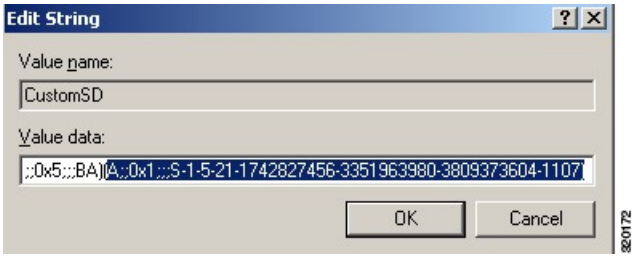
ステップ 3 SID を見つけ、レジストリ エディタを開き、次の場所を参照します。

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

ステップ 4 [セキュ リティ（Security）] をクリックし、[CustomDS] をダブルクリックします。

たとえば、ise_agent アカウント（`SID : S-1-5-21-1742827456-3351963980-3809373604-1107`）への読み取りアクセスを許可するには、「`(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`」と入力します。

図 *14 : CustomSD* 文字列の編集



ステップ 5 ドメイン コントローラ上で WMI サービスを再起動します。次の 2 とおりの方法で WMI サービスを再起動できます。

a) CLI から次のコマンドを実行します。

net stop winmgmt

net start winmgmt

b) `Services.msc` を実行します。これにより、Windows サービス管理ツールが開きます。Windows サービス管理ウィンドウで、「**Windows Management Instrumentation**」サービスを検索し、右クリックして [再起動] を選択します。

その他のトラブルシューティング情報の入手

Cisco ISE-PIC を使用すると、管理者ポータルから、サポートおよびトラブルシューティング情報をダウンロードできます。サポートバンドルを使用して、Cisco Technical Assistance Center（TAC）が Cisco ISE-PIC の問題をトラブルシューティングするための診断情報を準備できます。

（注） サポート バンドルおよびデバッグ ログにより、高度なトラブルシューティング情報が TAC に提供されます。サポート バンドルおよびデバッグ ログは解釈が困難です。Cisco ISE-PIC で提供されるさまざまなレポートおよびトラブルシューティング ツールを使用して、ネットワークで直面している問題を診断およびトラブルシューティングできます。

Cisco ISE-PIC のサポート バンドル

サポートバンドルに含めるログを設定できます。たとえば、特定のサービスのログをデバッグログに含めるように設定できます。また、日付に基づいてログをフィルタリングできます。

ダウンロードできるログは、次のように分類されます。

- 完全な設定データベース：Cisco ISE-PIC 設定データベースは、可読の XML 形式です。問題をトラブルシューティングする場合、このデータベース設定を別の Cisco ISE ノードにインポートして、シナリオを再現できます。
- デバッグログ：ブートストラップ、アプリケーション設定、ランタイム、展開、公開キーインフラストラクチャ（PKI）情報、およびモニタリングとレポートがキャプチャされます。

  デバッグ ログによって、特定の Cisco ISE コンポーネントのトラブルシューティング情報が提供されます。デバッグログを有効にするには、「Logging」の第 11 章を参照してください。デバッグ ログを有効にしない場合、情報メッセージ（INFO）はすべてサポート バンドルに含まれます。詳細については、Cisco ISE-PIC デバッグ ログ （206 ページ）を参照してください。
- ローカルログ：Cisco ISE で実行されるさまざまなプロセスからの syslog メッセージが含まれています。
- コアファイル：クラッシュの原因の特定に役立つ重要な情報が含まれています。これらのログは、アプリケーションがクラッシュしたためアプリケーションにヒープダンプが含まれている場合に作成されます。
- モニターリングおよびレポートログ：アラートおよびレポートに関する情報が含まれています。
- システムログ：Cisco Application Deployment Engine（ADE）関連の情報が含まれています。

- ポリシー設定：Cisco ISE で設定されたポリシーが人間が読み取れる形式で含まれています。

これらのログは、Cisco ISE CLI から **backup-logs** コマンドを使用してダウンロードできます。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。

これらのログを管理者ポータルからダウンロードすることを選択した場合、次の操作を実行できます。

- デバッグログやシステムログなどのログタイプに基づいて、ログのサブセットのみをダウンロードします。
- 選択したログ タイプの最新の「*n*」個のファイルのみをダウンロードします。このオプションによって、サポート バンドルのサイズとダウンロードにかかる時間を制御できます。

モニターリングログによって、モニターリング、レポート、およびトラブルシューティング機能に関する情報が提供されます。ログのダウンロードの詳細については、Cisco ISE-PIC ログ ファイルのダウンロード （205 ページ）を参照してください。

サポート バンドル

サポート バンドルは、単純な tar.gpg ファイルとしてローカル コンピュータにダウンロードできます。サポート バンドルは、日付とタイム スタンプを使用して、ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg という形式で名前が付けられます。ブラウザに、適切な場所にサポートバンドルを保存するように要求するプロンプトが表示されます。サポートバンドルの内容を抽出し、README.TXT ファイルを表示できます。このファイルには、サポートバンドルの内容と、ISE データベースがサポートバンドルに含まれている場合はその内容をインポートする方法が示されています。

Cisco ISE-PIC ログ ファイルのダウンロード

ネットワークでの問題のトラブルシューティング時に、Cisco ISE-PIC ログ ファイルをダウンロードして、詳細情報を確認できます。

インストールとアップグレードに関する問題のトラブルシューティングを行うには、ADE-OS やその他のログファイルを含む、システムログをダウンロードすることもできます。

始める前に

- デバッグログとデバッグログレベルを設定する必要があります。

ステップ 1 **[管理（Administration）]** > **[ロギング（Logging）]** > **[ログのダウンロード（Download Logs）]** > **[アプライアンスノードリスト（Appliance node list）]** を選択します。

ステップ 2 サポート バンドルをダウンロードするノードをクリックします。

ステップ 3 [サポートバンドル（Support Bundle）] タブでは、サポートバンドルに入力するパラメータを選択します。

すべてのログを含めると、サポート バンドルが大きくなりすぎて、ダウンロードに時間がかかります。ダウンロード プロセスを最適化するには、最新の *n* ファイルのみをダウンロードするように選択します。

ステップ 4 サポートバンドルを生成する [開始日（From date）] と [終了日（To date）] を入力します。

ステップ 5 次のいずれかを実行します。

- [公開キー暗号化（Public Key Encryption）]：トラブルシューティング用に Cisco TAC にサポートバンドルを提供する場合は、このオプションを選択します。
- [共有キー暗号化（Shared Key Encryption）]：オンプレミスでローカルに問題をトラブルシューティングする場合は、このオプションを選択します。このオプションを選択すると、サポート バンドル用の暗号キーを入力する必要があります。

ステップ 6 [サポート バンドルの作成（Create Support Bundle）] をクリックします。

ステップ 7 [ダウンロード（Download）] をクリックして、新しく作成されたサポート バンドルをダウンロードします。

サポート バンドルは、アプリケーション ブラウザを実行しているクライアント システムにダウンロードされる tar.gpg ファイルです。

次のタスク

特定のコンポーネントのデバッグログをダウンロードします。

Cisco ISE-PIC デバッグ ログ

デバッグ ログには、さまざまな Cisco ISE-PIC コンポーネントのトラブルシューティング情報が含まれています。デバッグログには、過去30日間に生成された重大なアラームと警告アラーム、過去7日間に生成された情報アラームが含まれています。問題を報告しているときに、これらのデバッグ ログを有効にして、問題の診断と解決のためにこれらのログを送信するよう求められる場合があります。

（注） 高負荷のデバッグログ（モニタリングデバッグログなど）を有効にすると、高負荷に関するアラームが生成されます。

デバッグ ログの入手

ステップ 1 デバッグログを入手するコンポーネントを設定します。

ステップ 2 デバッグ ログをダウンロードします。

Cisco ISE-PIC コンポーネントおよび対応するデバッグログ

（注） 次のリストに、ISE で使用可能なすべてのコンポーネントを示します。この表には ISE-PIC に関連していないコンポーネントも含まれています。

表 *28 :* コンポーネントおよび対応するデバッグ ログ

コンポーネント	デバッグ ログ
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
ライセンス	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
クライアント	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
ゲスト アクセス管理	guest.log
ゲスト アクセス	guest.log
MyDevices	guest.log

コンポーネント	デバッグ ログ
ポータル（Portal）	guest.log
ポータル セッション マネージャ	guest.log
ポータル Web アクション	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
ポスチャ	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

デバッグ ログのダウンロード

ステップ 1 **[管理（Administration）] > [ロギング（Logging）] > [ログのダウンロード（Download Logs）]** を選択します。

ステップ 2 [アプライアンスノードリスト（Appliance node list）] で、デバッグログをダウンロードするノードをクリックします。

ステップ 3 [デバッグ ログ（Debug Logs）] タブをクリックします。

デバッグ ログ タイプとデバッグ ログのリストが表示されます。このリストは、デバッグ ログの設定に基づいています。

ステップ 4 ダウンロードするログ ファイルをクリックし、クライアント ブラウザを実行しているシステムに保存します。

必要に応じて、このプロセスを繰り返して他のログ ファイルをダウンロードできます。次に、[デバッグログ（Debug Logs）] ウィンドウからダウンロードできるその他のデバッグログを示します。

- isebootstrap.log：ブートストラップ ログ メッセージを提供します
- monit.log：ウォッチドッグメッセージを提供します
- pki.log：サードパーティの暗号ライブラリログを提供します。
- iseLocalStore.log：ローカルストアファイルに関するログを提供します
- ad_agent.log：Microsoft Active Directory サードパーティ ライブラリ ログを提供します
- catalina.log：サードパーティログを提供します

その他の参考資料

次のリンクには、Cisco ISE で作業するときに使用できる追加のリソースが含まれています。
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコサービスにアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

シスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

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。