Cisco ISE の管理

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。

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

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

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

関連トピック

管理者ログイン ブラウザのサポート （2 ページ）

管理者ログイン ブラウザのサポート

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

- Mozilla Firefox 61 以前のバージョン
- Google Chrome 67 以前のバージョン
- Microsoft Internet Explorer 10.*x* および 11.*x*

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

ISE コミュニティ リソース

ISE Pages Fail to Fully Load When Adblock Plus is Used

ログインの試行に失敗した後の管理者のロックアウト

管理者ユーザ ID に対して誤ったパスワードを入力した回数が所定の数に達すると、ユーザは「ロックアウト」されて管理者ポータルからシステムにアクセスできなくなり、ログエントリが [サーバ管理者ログイン（Server Administrator Logins）] レポートに記録され、その管理者 ID のクレデンシャルは一時停止されます。一時停止を解除するには、その管理者 ID に関連付けられたパスワードをリセットする必要があります。手順については、『*Cisco Identity Services Engine Hardware Installation Guide*』の「Performing Post-Installation Tasks」の章を参照してください。管理者アカウントを無効にするのに必要な試行失敗回数は、「ユーザアカウントのカスタム属性およびパスワード ポリシー」の項で説明しているガイドラインに従って設定できます。管理者ユーザ アカウントがロックアウトされると、関連付けられた管理者ユーザに電子メールが送信されます。

無効になったシステム管理者のステータスは、Active Directory ユーザを含むすべてのスーパー管理者が有効にできます。

Cisco ISE でのプロキシ設定の指定

既存のネットワーク トポロジにおいて、外部リソース（たとえば、クライアント プロビジョニングやポスチャ関連のリソースが存在するリモート ダウンロード サイト）にアクセスする

ために、Cisco ISE に対してプロキシを使用することが要求されている場合は、管理者ポータルを使用してプロキシのプロパティを指定できます。

プロキシ設定は次の Cisco ISE 機能に影響します。

- パートナー モバイル管理
- エンドポイント プロファイラ フィード サービスの更新
- エンドポイント ポスチャの更新
- エンドポイント ポスチャ エージェント リソースのダウンロード
- CRL（証明書失効リスト）のダウンロード
- ゲスト通知

Cisco ISE プロキシ設定はプロキシ サーバの基本認証をサポートします。NT LAN Manager（NTLM）認証はサポートされていません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）]** を選択します。

ステップ 2 プロキシの IP アドレスまたは DNS 解決可能ホスト名を入力し、Cisco ISE との間のプロキシ トラフィックを通過させるポートを [プロキシ ホスト サーバ：ポート（Proxy host server : port）] で指定します。

ステップ 3 必要に応じて、[パスワード必須（Password required）] チェックボックスをオンにします。

ステップ 4 [ユーザ名（User Name）] および [パスワード（Password）] フィールドに、プロキシ サーバへの認証に使用するユーザ名とパスワードを入力します。

ステップ 5 [次のホストとドメインに対するプロキシをバイパス（Bypass proxy for these hosts and domain）] に、バイパスするホストまたはドメインの IP アドレスまたはアドレス範囲を入力します。

ステップ 6 [保存（Save）] をクリックします。

管理者ポータルで使用されるポート

管理者ポータルは HTTP ポート 80 および HTTPS ポート 443 を使用するように設定され、これらの設定は変更できません。Cisco ISE はまた、あらゆるエンドユーザ ポータルが同じポートを使用することを禁止して、管理者ポータルへのリスクを減らすようになっています。

外部 RESTful サービス API の有効化

外部 RESTful サービス API は HTTPS プロトコルおよび REST 方法論に基づいており、ポート 9060 を使用します。

外部 RESTful サービス API は、基本認証をサポートしています。認証クレデンシャルは、暗号化され、要求ヘッダーの一部となっています。

JAVA、curl Linux コマンド、Python などの REST クライアントやその他のクライアントを使用して、外部 RESTful サービス API コールを呼び出すことができます。

ISE 管理者は、外部 RESTful サービス API を使用して操作を実行するための特権をユーザに割り当てる必要があります。外部 RESTful サービス API（ゲスト API を除く）を使用して操作を実行するには、次の管理者グループのいずれかにユーザを割り当て、Cisco ISE の内部データベース（内部管理者ユーザ）に保存されているクレデンシャルに対して認証する必要があります。

- 外部 RESTful サービス管理者：すべての ERS API へのフル アクセス（GET、POST、DELETE、PUT）。このユーザは、ERS API 要求を作成、読み取り、更新、および削除できます。
- 外部 RESTful サービス オペレータ：読み取り専用アクセス（GET 要求のみ）。

（注） ネットワーク管理者ユーザは、すべての ERS API にアクセスできます。

外部 RESTful サービス API は、デフォルトではイネーブルになっていません。それらをイネーブルにする前に外部 RESTful サービス API コールを呼び出そうとすると、エラー応答を受信します。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。

ステップ 1 [管理（Administration）] > [設定（Settings）] > [ERS 設定（ERS Settings）] の順に選択します。

ステップ 2 プライマリ管理ノードの [読み取り/書き込み用に ERS をイネーブル化（Enable ERS for Read/Write）] を選択します。

ステップ 3 セカンダリ ノードがある場合は、[その他すべてのノードの読み取り用に ERS をイネーブル化（Enable ERS for Read for All Other Nodes）] を選択します。

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 4 次のオプションのいずれかを選択します。

- [セキュリティ強化に CSRF チェックを使用（Use CSRF Check for Enhanced Security）]：このオプションを有効にすると、ERS クライアントは Cisco ISE から Cross-Site Request Forgery（CSRF）トークンを取得する GET 要求を送信し、Cisco ISE に送信される要求に CSRF トークンを含める必要があります。Cisco ISE は、ERS クライアントからの要求を受信すると、CSRF トークンを検証します。Cisco ISE は、トークンが有効な場合にのみ要求を処理します。このオプションは、ISE 2.3 以前のクライアントには適用されません。
- [ERS 要求に対して CSRF を無効にする（Disable CSRF for ERS Request）]：このオプションを有効にすると、CSRF 検証は実行されません。このオプションは、ISE 2.3 以前のクライアントに使用できます。

ステップ 5 [送信（Submit）] をクリックします。

すべての REST 操作が監査され、ログがシステム ログに記録されます。外部 RESTful サービス API にはデバッグ ロギング カテゴリがあります。このカテゴリは、Cisco ISE GUI のデバッグ ログ ページからイネーブルにすることができます。

関連トピック

外部 RESTful サービス SDK （5 ページ）

外部 RESTful サービス SDK

外部 RESTful サービス SDK を使用して、独自ツールの構築を開始できます。次の URL から外部 RESTful サービス SDK にアクセスできます。https://<ISE-ADMIN-NODE>:9060/ers/sdk 外部 RESTful サービス SDK には、外部 RESTful サービス管理ユーザのみがアクセスできます。

SDK は、次のコンポーネントで構成されています。

- クイック リファレンス API マニュアル
- すべての利用可能な API 操作の完全なリスト
- ダウンロード可能なスキーマ ファイル
- ダウンロード可能な Java のサンプル アプリケーション
- cURL スクリプト形式の使用例
- python スクリプト形式の使用例
- Chrome POSTMAN の使用方法

システム時刻と NTP サーバ設定の指定

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

シスコは、すべての Cisco ISE ノードを協定世界時（UTC）の時間帯に設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。この手順では、展開内にあるさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。

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

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

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

プライマリおよびセカンダリの両方の Cisco ISE ノードがある場合は、セカンダリ ノードのユーザ インターフェイスにログインし、展開内の各 Cisco ISE ノードのシステム時間と NTP サーバ設定を個別に設定する必要があります。

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

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

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

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

a) [追加（Add）] をクリックします。

b) [キー ID（Key ID）] と [キー値（Key Value）] に必要な値を入力します。そのキーが信頼できる場合は、[信頼できるキー（Trusted Key）] オプションをオンにし、[OK] をクリックします。[キー ID（Key ID）] フィールドは 1 ～ 65535 の数値をサポートし、[キー値（Key Value）] フィールドは最大 15 文字の英数字をサポートします。

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

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

ステップ 6 [保存（Save）] をクリックします。

システムの時間帯の変更

一度設定すると、管理者ポータルからの時間帯の編集はできません。時間帯設定を変更するには、Cisco ISE CLI で次のコマンドを入力します。

clock timezone タイムゾーン

（注） Cisco ISE は、タイム ゾーン名と出力の省略形に POSIX スタイルの記号を使用します。そのため、グリニッジの西にあるゾーンはプラス記号を持ち、グリニッジの東にあるゾーンはマイナス記号を持ちます。たとえば、TZ='Etc/GMT+4' はグリニッジ標準時（UT）の 4 時間遅れに対応します。

注意 インストール後に Cisco ISE アプライアンスでタイム ゾーンを変更するには、ISE サービスをその特定のノードで再起動する必要があります。そのため、メンテナンス ウィンドウ内でこのような変更を行うことを推奨します。また、単一 ISE 展開内のすべてのノードが同じタイム ゾーンに設定されていることが重要です。複数の ISE ノードが異なる地理的な場所やタイム ゾーンにある場合は、すべての ISE ノードで UTC などのグローバルなタイム ゾーンを使用する必要があります。

clock timezone コマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

通知をサポートするための SMTP サーバの設定

アラームの電子メール通知を送信したり、スポンサーがゲストにログイン クレデンシャルやパスワードのリセット指示の電子メール通知を送信できるようにしたり、ゲストがアカウント登録に成功した後、自動的にログイン クレデンシャルを受信したり、ゲスト アカウントの期限が切れる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）サーバを設定します。

電子メールを送信する ISE ノード

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

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

ステップ 1 **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTP サーバ（SMTP Server）]** を選択します。

ステップ 2 **[設定（Settings）] > [SMTPサーバ（SMTP Server）]** を選択します。

ステップ 3 [SMTPサーバ（SMTP Server）] フィールドにアウトバウンド SMTP サーバのホスト名を入力します。この SMTP ホスト サーバは Cisco ISE サーバ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 4 次のオプションのいずれかを選択します。

- スポンサーの電子メールアドレスからゲスト通知メールを送信するには、[スポンサーの電子メールアドレスを使用（Use email address from Sponsor）] を選択して、[通知の有効化（Enable Notifications）] を選択します。
- すべてのゲスト通知の送信元となる電子メールアドレスを指定するには、[デフォルトの電子メールアドレスを使用（Use Default email address）] を選択して、それを [デフォルトの電子メールアドレス（Default email address）] フィールドに入力します。

ステップ 5 [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。

Cisco ISE 展開のアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスはさらに簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。アップグレード前およびアップグレード後のタスクのリストについては、『*Cisco Identity Services Engine Upgrade Guide*』を参照してください。

[アップグレードの概要（Upgrade Overview）] ページには、展開内のすべてのノード、そのノードで有効なペルソナ、インストールされている ISE のバージョン、およびノードのステータス（ノードがアクティブか非アクティブか）がリストされます。ノードがアクティブな状態である場合にのみアップグレードを開始できます。

さまざまなタイプの展開

- スタンドアロン ノード：管理、ポリシー サービスおよびモニタリングのペルソナを担当する単一の Cisco ISE ノード
- マルチノード展開：複数の ISE ノードによる分散展開。分散展開をアップグレードする手順については、次の参照先で説明しています。

ISE コミュニティ リソース

ネットワークが ISE 展開への準備ができているかどうかを評価する方法については、ISE Deployment Assistant（IDA）を参照してください。

分散展開のアップグレード

管理者ポータルから Cisco ISE 展開のすべてのノードをアップグレードできます。

（注） GUI ベースのアップグレードは、リリース 2.0 以降からそれよりも新しいリリースにアップグレードする場合、または Cisco ISE 2.0 以降の限定提供リリースを一般提供リリースにアップグレードする場合にのみ適用できます。

始める前に

アップグレードする前に、次の作業が完了していることを確認します。

- ISE の設定および運用データのバックアップを取得します。
- システム ログのバックアップを取得します。
- スケジュールしたバックアップを無効にします。展開のアップグレードが完了したら、バックアップ スケジュールを再設定します。
- 証明書および秘密キーをエクスポートします。
- リポジトリを設定します。アップグレードバンドルをダウンロードし、このリポジトリに格納します。
- Active Directory の参加クレデンシャルと RSA SecurID ノード秘密のメモを取ります（該当する場合）。この情報は、アップグレード後に Active Directory または RSA SecurID サーバに接続するために必要です。
- アップグレードのパフォーマンスを向上させるために、運用データを消去します。

ステップ 1 管理者ポータルの [アップグレード（Upgrade）] タブをクリックします。

ステップ 2 [続行（Proceed）] をクリックします。

[レビューチェックリスト（Review Checklist）] ウィンドウが表示されます。表示された手順を確認してください。

ステップ 3 [チェックリストを確認済み（I have reviewed the checklist）] チェックボックスをオンにし、[続行（Continue）] をクリックします。

[バンドルのノードへのダウンロード（Download Bundle to Nodes）] ウィンドウが表示されます。

ステップ 4 リポジトリからノードにアップグレード バンドルをダウンロードします。

a) アップグレード バンドルをダウンロードするノードの隣のチェックボックスをオンにします。

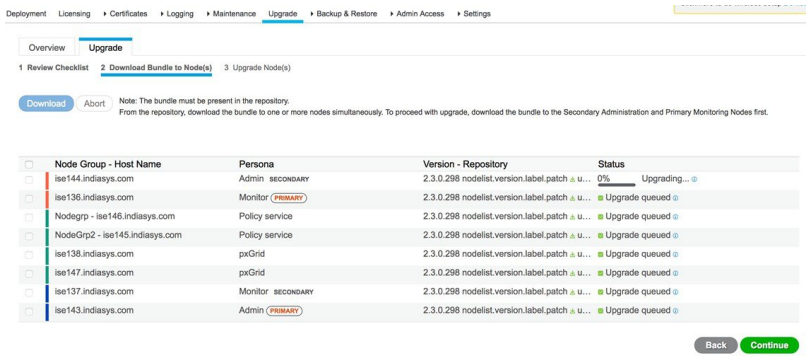
b) [ダウンロード（Download）] をクリックします。

[リポジトリおよびバンドルの選択（Select Repository and Bundle）] ウィンドウが表示されます。

c) リポジトリを選択します。

異なるノードで同じリポジトリまたは異なるリポジトリを選択できますが、すべてのノードで同じアップグレード バンドルを選択する必要があります。

図 *1*：各ノードの選択したリポジトリを表示するアップグレード ウィンドウ



d) アップグレードに使用するバンドルの隣にあるチェックボックスをオンにします。

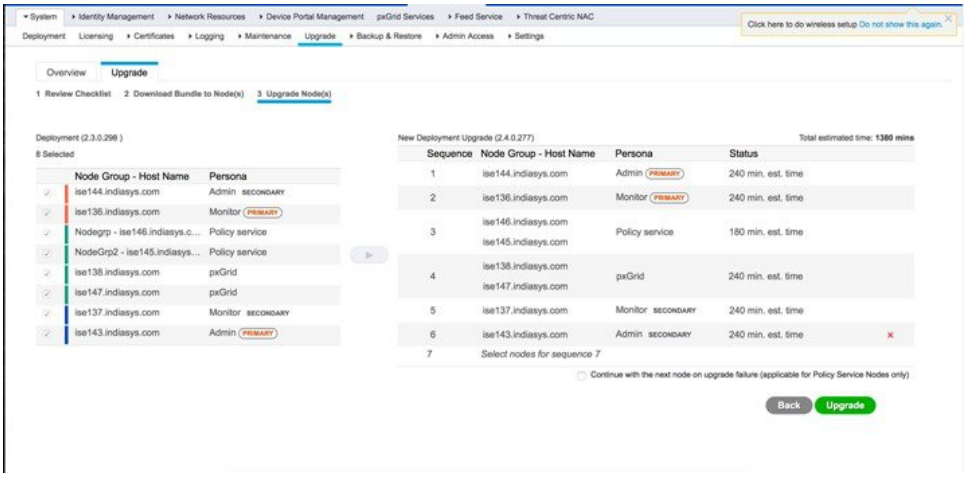
e) [確認（Confirm）] をクリックします。

バンドルがノードにダウンロードされると、ノードステータスが[アップグレードの準備が整いました（Ready for Upgrade）] に変わります。

ステップ 5 [続行（Continue）] をクリックします。

[ノードのアップグレード（Upgrade Nodes）] ウィンドウが表示されます。

図 *2*：現在の展開と新しい展開を表示するアップグレード ウィンドウ



ステップ 6 アップグレード順序を選択します。

ノードを新しい展開に移動すると、アップグレードの推定所要時間が [ノードのアップグレード（Upgrade Nodes）] ウィンドウに表示されます。この情報を使用して、アップグレードを計画し、ダウンタイムを最小化できます。管理ノードとモニタリング ノードのペアおよび複数のポリシー サービス ノードがある場合は、以下の手順に従います。

a) デフォルトでは、セカンダリ管理ノードは、アップグレード順序の最初にリストされています。アップグレード後に、このノードは新しい展開でプライマリ管理ノードになります。
b) プライマリ モニタリング ノードは、次に新しい展開にアップグレードされるノードです。
c) ポリシー サービス ノードを選択し、新しい展開に移動します。ポリシー サービス ノードをアップグレードする順序を変更できます。

   ポリシーサービス ノードは、順番にまたは並行してアップグレードできます。ポリシーサービス ノードのセットを選択し、並行してアップグレードできます。

d) セカンダリ モニタリング ノードを選択し、新しい展開に移動します。
e) 最後に、プライマリ管理ノードを選択し、新しい展開に移動します。

管理ノードがモニタリング ペルソナも担当する場合は、次の表に示す手順に従ってください。

現在の展開内のノード ペルソナ	アップグレードの順序
セカンダリ管理/プライマリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/セカンダリ モニタリング ノード	**1.** セカンダリ管理/プライマリ モニタリング ノード **2.** ポリシー サービス ノード **3.** プライマリ管理/セカンダリ モニタリング ノード
セカンダリ管理/セカンダリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/プライマリ モニタリング ノード	**1.** セカンダリ管理/セカンダリ モニタリング ノード **2.** ポリシー サービス ノード **3.** プライマリ管理/プライマリ モニタリング ノード
セカンダリ管理ノード、プライマリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/セカンダリ モニタリング ノード	**1.** セカンダリ管理ノード **2.** プライマリ モニタリング ノード **3.** ポリシー サービス ノード **4.** プライマリ管理/セカンダリ モニタリング ノード
セカンダリ管理ノード、セカンダリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/プライマリ モニタリング ノード	**1.** セカンダリ管理ノード **2.** セカンダリ モニタリング ノード **3.** ポリシー サービス ノード **4.** プライマリ管理/プライマリ モニタリング ノード
セカンダリ管理/プライマリ モニタリング ノード、ポリシー サービス ノード、セカンダリ モニタリング ノード、プライマリ管理ノード	**1.** セカンダリ管理/プライマリ モニタリング ノード **2.** ポリシー サービス ノード **3.** セカンダリ モニタリング ノード **4.** プライマリ管理ノード

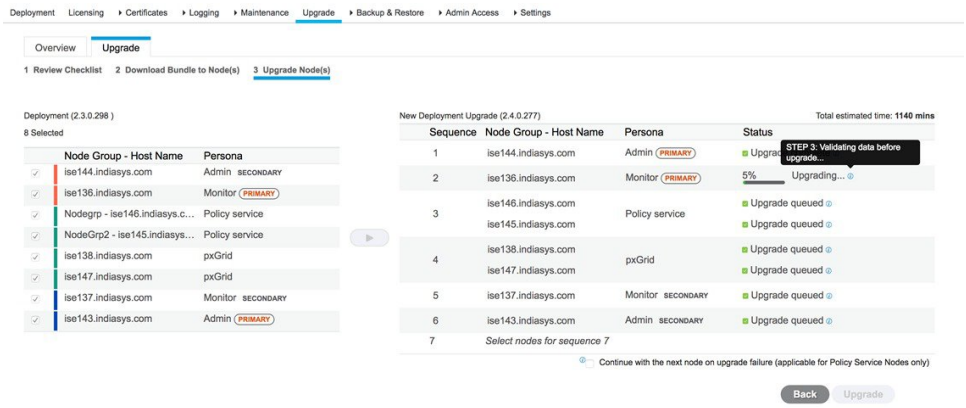
現在の展開内のノード ペルソナ	アップグレードの順序
セカンダリ管理/セカンダリ モニタリング ノード、ポリシー サービス ノード、プライマリ モニタリング ノード、プライマリ管理ノード	1. セカンダリ管理/セカンダリ モニタリング ノード 2. ポリシー サービス ノード 3. プライマリ モニタリング ノード 4. プライマリ管理ノード

ステップ 7 アップグレードがアップグレード順序のいずれかのポリシーサービス ノードで失敗した場合でもアップグレードを続行するには、[失敗時でもアップグレードを続行する（Continue with upgrade on failure）] チェックボックスをオンにします。

このオプションは、セカンダリ管理ノードおよびプライマリ モニタリング ノードには適用されません。これらのノードのいずれかに障害が発生すると、アップグレード プロセスはロールバックされます。ポリシーサービス ノードのいずれかが失敗すると、セカンダリ モニタリング ノードおよびプライマリ管理ノードはアップグレードされず、古い展開内に残ります。

ステップ 8 [アップグレード（Upgrade）] をクリックして、展開のアップグレードを開始します。

図 *3:* アップグレードの進行状況を表示する *[*アップグレード（*Upgrade*）*]* ウィンドウ



各ノードのアップグレードの進行状況が表示されます。正常に完了すると、ノードのステータスが [アップグレード完了（Upgrade Complete）] に変わります。

（注） 管理者ポータルからノードをアップグレードするときに、ステータスが長時間変化しない場合（80% のままの場合）は、CLI からアップグレード ログをチェックするか、コンソールからアップグレードのステータスをチェックできます。アップグレードの進行状況を表示するには、CLI にログインするか、Cisco ISE ノードのコンソールを表示します。**show logging application** コマンドを使用すると、*upgrade-uibackend-cliconsole.log* および *upgrade-postosupgrade-yyyymmdd-xxxxxx.log* を表示できます。

（注） 新しい展開のプライマリ管理ノードでポスチャ データの更新処理が実行している場合、プライマリ管理ノードにノードを登録できません。ポスチャ更新プロセスが終了するまで待つか（約20分かかることがあります）、またはアップグレードまたはノードの新しい展開への登録中に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] ページから、ポスチャの自動更新機能を無効にすることができます。

Cisco ISE ソフトウェア パッチ

Cisco ISE ソフトウェア パッチは通常累積されます。Cisco ISE 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 サーバ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。

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。

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 Reference Guide*』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。

関連トピック

ソフトウェア パッチ インストールのガイドライン （14 ページ）
ソフトウェア パッチのインストール （14 ページ）
ソフトウェア パッチ インストールのガイドライン （14 ページ）
ソフトウェア パッチ ロールバックのガイドライン （16 ページ）
ソフトウェア パッチのインストール （14 ページ）
ソフトウェア パッチのロールバック （15 ページ）

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 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 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。

Cisco ISE 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 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 サーバ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。

分散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 によってそのパッチが展開内のプライマリ ノードとすべてのセカンダリ 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 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。ただし、何らかの理由でセカンダリ ノードのいずれかでインストールに失敗した場合は、処理が続行され、展開内の次のセカンダリ ノードでインストールが実行されます。

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 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 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 パッチのインストール

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。
- **[管理（Administration）] > [システム（System）] > [展開（Deployment）] > [PANのフェールオーバー（PAN Failover）]** に移動し、[PANの自動フェールオーバーを有効にする（Enable PAN Auto Failover）] チェックボックスがオフになっていることを確認します。このタスクの期間中は、PAN の自動フェールオーバー設定を無効にする必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）] >** [インストール（Install）] を選択します。

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 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）] > [システム（System）] > [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 セカンダリ ノードに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

1 つ以上のセカンダリ 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。

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 によってそのパッチが展開内のプライマリ ノードとすべてのセカンダリ ノードにロールバックされます。

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [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 **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択します。

ステップ 5 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 6 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 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。

関連トピック

ソフトウェア パッチ ロールバックのガイドライン （16 ページ）

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 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。ただし、いずれかのセカンダリ ノードでパッチのロールバックが失敗しても、展開内の次のセカンダリ ノードからのパッチのロールバックは継続されます。

Cisco ISE 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。

パッチのインストールおよびロールバックの変更の表示

インストールされているパッチに関連するレポートを表示するには、次の手順を実行します。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** ページで、パッチをインストールまたはロールバックできます。展開内の各ノードで特定のパッチのステータス（[インストール済み（installed）]、[処理中（in-progress）]、[未インストール（not installed）]）を確認できます。このためには、特定のパッチを選択し、[ノード ステータスを表示（Show Node Status）] ボタンをクリックします。

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [監査（Audit）] > [操作監査（Operations Audit）]** を選択します。デフォルトでは、過去 7 日間のレコードが表示されます。

ステップ 2 [フィルタ（Filter）] ドロップダウンをクリックして [クイックフィルタ（Quick Filter）] または [高度なフィルタ（Advanced Filter）] を選択し、必要なキーワード（例：patch install iniated）を使用して、インストール済みのパッチを示すレポートを生成します。

FIPS モードのサポート

ISE FIPS 140 モードでは、FIPS 140-2 モードに対して Cisco FIPS オブジェクト モジュールの暗号化モジュールを初期化します。Cisco Identity Services Engine には、FIPS 140-2 の検証済み暗号化モジュールが組み込まれています。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。

FIPS モードを有効にすると、Cisco ISE 管理者インターフェイスのページの右上隅のノード名の左側に FIPS モード アイコンが表示されます。

Cisco ISE は、FIPS 140-2 標準でサポートされないプロトコルまたは証明書の使用を検出すると、準拠していないプロトコルまたは証明書の名前とともに警告を表示し、FIPS モードは有効になりません。必ず FIPS に準拠したプロトコルのみを選択し、FIPS モードを有効にする前に FIPS に非準拠の証明書を交換してください。

FIPS 標準では特定のアルゴリズムの使用について制限が設けられています。Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードが有効になると、FIPS 非準拠アルゴリズムを使用する機能はすべて失敗します。

Cisco ISE にインストールされている証明書で使用されている暗号化方式が FIPS でサポートされていない場合には、証明書を再発行する必要があります。

FIPS モードを有効にすると、次の機能が影響を受けます。

- IEEE 802.1X 環境
  - EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）
  - EAP-Transport Layer Security（EAP-TLS）
  - PEAP
  - RADIUS

（注） EAP-Message Digest 5（EAP-MD5）、Lightweight Extensible Authentication Protocol（LEAP）、PAP など、その他のプロトコルは FIPS 140-2 標準と互換性がなく、FIPS モードが有効な場合は無効になります。ゲスト アクセスの従来の方法であるローカル Web 認証（LWA）は PAP を使用しているため、FIPS モードが有効な場合は機能しません。ただし、MAC 認証バイパス（MAB）の許可されているプロトコルでホスト ルックアップが使用されている場合、中央 Web 認証（CWA）のゲスト アクセスは機能します。

- Lightweight Directory Access Protocol（LDAP）over Secure Sockets Layer（SSL）
- Cisco ISE による FIPS 140-2 準拠の有効化の手段として、RADIUS の共有秘密とキー管理が使用されます。FIPS モードが有効になると、FIPS 非準拠アルゴリズムを使用する機能はすべて失敗します。

ゲストでは、FIPS モードはサポートされていません。また FIPS モードを有効にすると、Cisco ISE のゲスト ログイン機能に必要な Password Authentication Protocol（PAP）および Challenge Handshake Authentication Protocol（CHAP）プロトコルが自動的に無効になります。

FIPS モードを有効にすると、展開内のすべてのノードが自動的に再起動されます。Cisco ISE はローリング再起動を実行します。具体的には、最初にプライマリ PAN を再起動し、その後でセカンダリ ノードを 1 つずつ再起動します。そのため、設定を変更する前にダウンタイムを計画することをお勧めします。

ヒント　データベース移行プロセスを行う場合は、移行が完了してから FIPS モードを有効にすることを推奨します。

Cisco ISE での FIPS モードの有効化

FIPS モードを有効にする場合：

ステップ 1　**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [FIPSモード（FIPS Mode）]** の順に選択します。

ステップ 2　[FIPSモード（FIPS Mode）] ドロップダウン リストで [有効（Enabled）] オプションを選択します。

ステップ 3　[保存（Save）] をクリックして、マシンを再起動します。

次のタスク

FIPS モードを有効にしたら、次の FIPS 140-2 準拠機能を有効にして設定します。

- 自己署名証明書の生成
- 証明書署名要求の作成と認証局への CSR の送信
- 『』の「ネットワーク デバイス定義の設定」のセクションを参照してください。
- ネットワーク デバイス定義の設定で RADIUS 認証を設定します。

また、Common Access Card（CAC）機能を使用して管理者アカウントの許可を有効にすることもできます。許可のために CAC 機能を使用することは、厳密には FIPS 140-2 の要件ではありませんが、セキュア アクセスの手法としてよく知られており、多くの環境で FIPS 140-2 準拠を強化するために使用されています。

管理者 CAC 認証のための Cisco ISE の設定

始める前に

設定を始める前に、次の手順を実行してください。

- （任意）FIPS モードを有効にします。FIPS モードは証明書ベースの認証には必要ありませんが、この 2 つのセキュリティ手段は多くの場合、組み合わせて使用されます。Cisco ISE を FIPS 140-2 準拠の環境に展開する予定があり、CAC 証明書ベース許可も使用する場合は、必ず FIPS モードを有効にするとともに、適切な秘密キーと暗号化/復号化設定を最初に指定してください。
- Cisco ISE のドメイン ネーム サーバ（DNS）が Active Directory に設定されていることを確認します。
- Active Directory のユーザとユーザ グループ メンバーシップが、管理者証明書ごとに定義されていることを確認します。

Cisco ISE による管理者の認証と許可を、ブラウザから送信された CAC ベースのクライアント証明書に基づいて実行できるようにするには、次の設定が完了していることを確認してください。

- 外部 ID ソース（次の例では Active Directory）
- 管理者が属する Active Directory のユーザ グループ
- ユーザのアイデンティティを証明書の中で見つける方法
- Active Directory ユーザ グループから Cisco ISE RBAC 権限へのマッピング
- クライアント証明書に署名する認証局（信頼）証明書
- クライアント証明書がすでに CA によって失効させられたかどうかを判断する方法

Cisco ISE にログインする場合、クレデンシャルを認証するために Common Access Card（CAC）を使用できます。

ステップ 1 FIPS モードを有効にします。FIPS モードを有効にすると、システムを再起動するように促されます。CA 証明書もインポートする場合は、再起動を遅らせることができます。

ステップ 2 Cisco ISE の Active Directory ID ソースを設定し、Active Directory にすべての Cisco ISE ノードを追加します。

ステップ 3 ガイドラインに従って証明書認証プロファイルを設定します。

[プリンシパル名 X.509 属性（Principal Name X.509 Attribute）] フィールドでは、証明書内で管理者ユーザ名が格納されている属性を選択します。（CAC カードの場合は、カード上の署名証明書が通常は Active Directory でのユーザの検索に使用されます。プリンシパル名は、この証明書の「サブジェクトの別名（Subject Alternative Name）」拡張情報の中にあります。具体的には、この拡張情報の「別の名前（Other Name）」というフィールドです。したがって、ここで選択する属性は「Subject Alternative Name - Other Name」となります。）

ユーザの AD レコードにユーザの証明書が格納されている場合に、ブラウザから受信した証明書を AD の証明書と比較するには、[証明書のバイナリ比較（Binary Certificate Comparison）] チェックボックスをオンにして、以前に指定した Active Directory インスタンス名を選択します。

ステップ 4 パスワードベースの admin 認証用の Active Directory を有効にします。Cisco ISE に接続し結合された Active Directory インスタンス名を選択します。

（注） その他の設定が完了するまでは、パスワードベースの認証を使用します。この手順の最後に、認証タイプをクライアント証明書ベースに変更できます。

ステップ 5 外部管理者グループを作成して、Active Directory グループにマッピングします。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理グループ（Admin Groups）]** を選択します。外部システム管理者グループを作成します。

ステップ 6 外部管理グループに RBAC 権限を割り当てる管理者許可ポリシーを設定します。

注意 外部スーパー管理者グループを作成して Active Directory グループにマッピングし、スーパー管理者権限を持つ管理者許可ポリシー（メニュー アクセスおよびデータ アクセス）を設定し、Active Directory グループに少なくとも 1 人のユーザを作成することを強く推奨します。このマッピングにより、クライアント証明書ベースの認証が有効になると、少なくとも 1 人の外部管理者がスーパー管理者権限を持つことが保証されます。これができないと、Cisco ISE 管理者が管理者ポータルの重要な機能から締め出される状況になる可能性があります。

ステップ 7 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書ストア（Certificate Store）]** を選択して、認証局証明書を Cisco ISE 証明書信頼ストアにインポートします。

Cisco ISE がクライアント証明書を受け入れるには、そのクライアント証明書の信頼チェーンの CA 証明書が Cisco ISE 証明書ストアの中にあることが条件となります。Cisco ISE 証明書ストアには適切な CA 証明書をインポートする必要があります。

a) [参照（Browse）] をクリックして証明書を選択します。
b) [クライアント認証を信頼（Trust for client authentication）] チェックボックスをオンにします。
c) [送信（Submit）] をクリックします。

Cisco ISE は、証明書をインポートしたら展開内のすべてのノードを再起動することを促します。すべての証明書をインポートするまで、再起動を遅らせることができます。ただし、すべての証明書をインポートしたら、次に進む前に Cisco ISE を再起動する必要があります。

ステップ 8 失効ステータス確認のための認証局証明書を設定します。

a) **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [OSCP サービス（OSCP Services）]** を選択します。
b) OSCP サーバの名前、説明（任意）、サーバの URL を入力します。
c) **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書ストア（Certificate Store）]** を選択します。
d) クライアント証明書に署名できる CA 証明書のそれぞれについて、その CA の失効ステータス チェックを行う方法を指定する必要があります。リストから CA 証明書を選択して [編集（Edit）] をクリックします。編集ページで、OCSP または CRL 検証の一方あるいは両方を選択します。OCSP を選択した

場合は、CA に使用する OCSP サービスを選択します。CRL を選択した場合は、CRL Distribution URL などの設定パラメータを指定します。

ステップ 9 クライアント証明書ベースの認証を有効にします。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authentication）]** を選択します。

a) [認証方式（Authentication Method）] タブの [クライアント証明書ベース（Client Certificate Based）] 認証タイプを選択します。
b) 設定済みの証明書認証プロファイルを選択します。
c) Active Directory のインスタンス名を選択します。
d) [保存（Save）] をクリックします。

ここで、パスワード ベースの認証からクライアント証明書ベースの認証に切り替えます。設定済みの証明書認証プロファイルにより、管理者による証明書の認証方法を指定します。管理者は外部 ID ソースを使用して許可されます。この例では、Active Directory です。

Active Directory での管理者の検索には、証明書認証プロファイルからのプリンシパル名属性が使用されます。

Cisco ISE は、管理者 CAC 認証に設定されています。

関連トピック

サポートされる Common Access Card 標準 （21 ページ）
Cisco ISE での共通アクセス カードの動作 （21 ページ）

サポートされる Common Access Card 標準

Cisco ISE は、Common Access Card（CAC）認証デバイスを使用して自身を認証する米国政府ユーザをサポートします。CAC は特定の従業員を識別する一連の X.509 クライアント証明書を含む電子チップの認識票です。CAC によるアクセスには、カードを挿入し PIN を入力するカードリーダーが必要です。カードからの証明書が Windows の証明書ストアに転送されます。Windows の証明書ストアは、Cisco ISE などのローカル ブラウザで実行されているアプリケーションで使用可能です。

Windows Internet Explorer バージョン 8 または 9 を Windows 7 オペレーティング システムで使用している場合は、ActiveIdentity の ActivClient バージョン 6.2.0.133 をインストールする必要があります。このミドルウェアは、Cisco ISE を CAC とともに相互運用するためのサードパーティ製品です。ActiveIdentity セキュリティ クライアント製品の詳細については、ActivID ActivClient Security Software Datasheet を参照してください。

Cisco ISE での共通アクセス カードの動作

管理者ポータルは、クライアント証明書を使用してのみ Cisco ISE との認証が許可されるように設定できます。ユーザ ID とパスワードなどのクレデンシャル ベースの認証はできません。クライアント証明書認証では、共通アクセス カード（CAC）カードを挿入して PIN を入力してから、ブラウザのアドレス フィールドに Cisco ISE 管理者ポータルの URL を入力します。ブラウザによって証明書が Cisco ISE に転送され、Cisco ISE はログイン セッションを証明書の内容に基づいて認証および許可します。このプロセスが完了すると、[Cisco ISE モニタリング

およびトラブルシューティング（Cisco ISE Monitoring and Troubleshooting）] ホーム ページに表示され、適切な RBAC 権限が与えられます。

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

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

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

次に例を示します。

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

セキュア syslog 送信のための Cisco ISE の設定

Cisco ISE ノード間で、およびモニタリング ノードに対して、TLS 保護されたセキュア syslog のみを送信するように Cisco ISE を設定するには、次の手順を実行します。

始める前に

- 展開内のすべての Cisco ISE ノードに適切なサーバ証明書が設定されていることを確認します。 FIPS 140-2 準拠にセットアップする場合は、証明書キーは 2,048 ビット以上のキーサイズが必要です。
- 管理者ポータルの FIPS モードを有効にします。
- デフォルト ネットワーク アクセス認証ポリシーが、あらゆるバージョンの SSL プロトコルを許可しないことを確認します。FIPS 認定アルゴリズムとともに、FIPS モードで TLS プロトコルを使用します。
- 展開内のすべてのノードがプライマリ PAN に登録されていることを確認します。また、展開の少なくとも 1 つのノードに、セキュア syslog レシーバ（TLS サーバ）としての動作が有効になっているモニタリング ペルソナが含まれることも確認します。

ステップ 1 セキュア syslog リモート ロギング ターゲットを設定します。

ステップ 2 セキュア syslog リモート ロギング ターゲットに監査可能なイベントを送信するロギング カテゴリを有効にします。

ステップ 3 TCP syslog および UDP syslog コレクタを無効にします。TLS 保護された syslog コレクタのみを有効にします。

関連トピック

セキュア syslog リモート ロギング ターゲットの設定 （23 ページ）
セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化 （24 ページ）
TCP syslog および UDP syslog コレクタの無効化 （24 ページ）

セキュア syslog リモート ロギング ターゲットの設定

Cisco ISE システム ログは、さまざまな目的のために、ログ コレクタによって収集され保存されます。セキュア syslog ターゲットを設定するためには、ログ コレクタとして Cisco ISE モニタリング ノードを選択する必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 **[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 セキュア syslog サーバの名前を入力します。

ステップ 5 [ターゲット タイプ（Target Type）] ドロップダウン リストからセキュア syslog を選択します。

ステップ 6 [ステータス（Status）] ドロップダウン リストで [有効化（Enabled）] を選択します。

ステップ 7 展開の Cisco ISE モニタリング ノードの IP アドレスを入力します。

ステップ 8 ポート番号として 6514 を入力します。セキュア syslog レシーバは TCP ポート 6514 をリッスンします。

ステップ 9 syslog ファシリティ コードを選択します。デフォルトは LOCAL6 です。

ステップ 10 [サーバ ダウンの場合はバッファ メッセージ（Buffer Messages When Server is Down）] チェックボックスをオンにします。このオプションがオンの場合、Cisco ISE は、セキュア syslog レシーバが到達不能な場合にはログを格納し、セキュア syslog レシーバを定期的に検査し、セキュア syslog レシーバが起動すると転送します。

a) バッファ サイズを入力します。
b) 定期的にセキュア syslog レシーバを検査するように、Cisco ISE の再接続タイムアウトを秒単位で入力します。

ステップ 11 Cisco ISE がセキュア syslog サーバに提示する CA 証明書を選択します。

ステップ 12 [サーバ証明書有効性を無視（Ignore Server Certificate validation）] チェックボックスをオフにします。このオプションをオンにしてはいけません。

ステップ 13 [送信（Submit）] をクリックします。

セキュア syslog ターゲットに監査可能なイベントを送信するためのロギング カテゴリの有効化

Cisco ISE によってセキュア syslog ターゲットに監査可能なイベントが送信されるようにするには、ロギング カテゴリを有効にする必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択します。

ステップ 3 AAA 監査ロギング カテゴリの横にあるオプション ボタンをクリックし、次に [編集（Edit）] をクリックします。

ステップ 4 [ログ重大度レベル（Log Severity Level）] ドロップダウン リストから [警告（WARN）] を選択します。

ステップ 5 作成済みのセキュア syslog リモート ロギング ターゲットを、選択したボックスに移動します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 次のロギング カテゴリを有効にする場合は、この手順を繰り返し行います。

- 管理および操作の監査（Administrative and Operational Audit）
- ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）

TCP syslog および UDP syslog コレクタの無効化

Cisco ISE が ISE ノード間でセキュアな syslog のみを送信するには、TCP および UDP syslog コレクタを無効にして、セキュアな syslog コレクタのみを有効にする必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）]** を選択します。

ステップ 3 TCP または UDP syslog コレクタの横にあるオプション ボタンをクリックします。

ステップ 4 [編集（Edit）] をクリックします。

ステップ 5 [ステータス（Status）] ドロップダウン リストから [無効化（Disabled）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 すべての TCP または UDP syslog コレクタが無効になるまで、このプロセスを繰り返します。

デフォルトのセキュア syslog コレクタ

Cisco ISE には、MnT ノード用のデフォルトのセキュア syslog コレクタがあります。デフォルトでは、これらのデフォルト セキュア syslog コレクタにはロギング カテゴリはマッピングされません。デフォルト セキュア syslog コレクタの名前は次のとおりです。

- プライマリ MnT ノード：SecureSyslogCollector
- セカンダリ MnT ノード：SecureSyslogCollector2

[リモート ロギング ターゲット（Remote Logging Targets）] ページ（[管理（Administration）] > [システム（System）] > [ロギング（Logging）]）でこの情報を確認できます。デフォルトの syslog コレクタは削除できません。また、デフォルト syslog コレクタの [名前（Name）]、[ターゲット タイプ（Target Type）]、[IP/ホスト アドレス（IP/Host address）]、および [ポート（Port）] フィールドは更新できません。

Cisco ISE の新規インストール中に、システムから「デフォルトの自己署名サーバ証明書（Default Self-signed Server Certificate）」が信頼ストアに追加され、「クライアン認証および syslog 用の信頼（Trust for Client authentication and Syslog）」目的で使用されるものとしてマークされます。これにより、この証明書はセキュア syslog に使用できるようになります。展開を設定する場合または証明書を更新する場合には、関連する証明書をセキュア syslog ターゲットに割り当てる必要があります。

アップグレード中に、ポート 6514 で MnT ノードを指し示している既存のセキュア syslog ターゲットがある場合、同じ名前と設定が維持されますが、アップグレード完了後にこれらの syslog ターゲットを削除すること、および [名前（Name）]、[ターゲット タイプ（Target Type）]、[IP/ホスト アドレス（IP/Host address）]、および [ポート（Port）] フィールドを編集することはできません。アップグレードの時点でこのようなターゲットが存在しない場合、新規インストールの場合と同様にデフォルト セキュア syslog ターゲットが作成されますが、証明書のマッピングは行われません。これらの syslog ターゲットに関連証明書を割り当てることができます。どの証明書にもマッピングされていないセキュア syslog ターゲットをロギング カテゴリにマッピングしようとすると、次のメッセージが表示されます。

log_target_name □□□□□□□□□□□□□□□Please configure the certificate for log_target_name□

オフライン メンテナンス

メンテナンス時間が 1 時間未満の場合、ISE ノードをオフラインにしてメンテナンス作業を行います。ノードをオンラインに戻すと、メンテナンス時間内に行われたすべての変更が PAN により自動的に同期されます。変更が自動的に同期されない場合は、PAN を使用して手動で同期できます。

メンテナンス時間が 1 時間を超える場合は、メンテナンスの時点でノードを登録解除し、ノードを展開に再び追加するときにノードを再登録します。

処理があまり行われていない時間帯にメンテナンスをスケジュールすることが推奨されます。

（注）

1. キューに格納されているメッセージの数が 1,000,000 を超える場合、または ISE ノードが 6 時間を超えてオフラインになっている場合には、データの複製の問題が発生している可能性があります。
2. プライマリ MnT ノードでメンテナンスを行う予定の場合は、メンテナンスアクティビティを実行する前に、MnT ノードの操作バックアップを作成しておくことを推奨します。