# アップグレード後の作業

展開のアップグレード後に、この章にリストされているタスクを実行します。



## アップグレード後の作業

Cisco ISE リリース 2.3 以降では、すべてのネットワーク アクセス ポリシーとポリシー セットを置き換える、新しい拡張された [ポリシーセット（Policy Sets）] ページが提供されます。以前のリリースからリリース 2.3 以降にアップグレードすると、すべてのネットワーク アクセス ポリシーの設定（認証および承認の条件、ルール、ポリシー、プロファイル、および例外を含む）が ISE GUI の新しい [ポリシーセット（Policy Sets）] 領域に移行されます。変更に関する詳細については、『*Release Notes for Cisco Identity Services Engine, Release 2.3*』の「*Upgrade Considerations and Requirements*」の項を参照してください。

次のタスクの詳細については、『*Cisco Identity Services Engine Administrator Guide*』を参照してください。

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
|---|---|
| VMware 仮想マシンのゲスト オペレーティング システムが Red Hat Enterprise Linux（RHEL）7 に設定され、ネットワーク アダプタが E1000 または VMXNET3 に設定されていることを確認します。<br>（注） ESXi 5.x サーバ（5.1 U2 以上）でリリース 2.3 にアップグレードする場合は、RHEL 7 をゲスト OS として選択する前に、VMware ハードウェア バージョンを 9 にアップグレードする必要があります。 | — |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
|---|---|
| アップグレード後、Cisco ISE 管理者ポータルにアクセスする前に、ブラウザのキャッシュをクリアしていることを確認し、ブラウザを閉じて、新しいブラウザセッションを開きます。サポート対象のブラウザは次のとおりです。<br>• Mozilla Firefox バージョン：<br>◦ 52.1.2 ESR<br>◦ 53.0.3 以上<br>• Google Chrome の最新バージョン<br>• Microsoft Internet Explorer 10.*x* および 11.*x* | — |
| リリース 2.3 へのアップグレード後、[ゲストポータル（Guest Portals）] および [ゲストタイプ（Guest Types）] ページは最初は空のように表示されます。この問題は、使用されなかったか、まだアクティブになっている、リリース 1.2 で作成された最初のログインからのゲストタイプのアカウントがある場合に発生します。アップグレード後、システムが初期化されると、これらのアカウントは移行に時間がかかります。<br>一定時間後（1.2 で作成した「最初のログインからの」ゲストアカウントの数による）、データが正常に移行されたら、[ゲスト ポータル（Guest Portals）] および [ゲスト タイプ（Guest Types）] ページを更新して情報を表示できます。<br>これらのアカウントが不要になった場合は、スポンサーポータルから手動で削除することができます。 | — |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| | 外部 ID ソースとしての Active Directory の設定 |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| 外部アイデンティティ ソースとして使用している Active Directory との接続が失われた場合は、Active Directory とすべての Cisco ISE ノードを再度結合します。再結合した後に、外部アイデンティティ ソースのコールフローを実行して、確実に接続します。<br>• アップグレード後に、Active Directory 管理者アカウントを使用して Cisco ISE ユーザ インターフェイスにログインした場合、アップグレード時に Active Directory の結合が失われるため、ログインが失敗します。Cisco ISE にログインし、Active Directory と結合するには、内部管理者アカウントを使用する必要があります。<br>• アップグレード前に Cisco ISE への管理アクセスに対して証明書ベースの認証をイネーブルにしていて（[管理（Administration）] > [管理者アクセス（Admin Access）]）、Active Directory をアイデンティティ ソースとして使用している場合、アップグレード時に Active Directory 結合が失われるため、アップグレード後に ISE ログイン ページを起動できません。この問題が発生した場合、次のコマンドを使用して、Cisco ISE CLI から、セーフ モードで ISE アプリケーションを起動します。<br>**application start ise safe**<br>このコマンドにより、Cisco ISE ノードはセーフ モードで起動します。次の作業を実行します。<br>1 内部管理者アカウントを使用して Cisco ISE ユーザ インターフェイスにログインします。<br>パスワードを忘れた場合または管理者アカウントがロックされている場合は、管理者パスワードをリセットする方法について、『Cisco Identity Services Engine Hardware Installation Guide Cisco Identity Services Engine Hardware | |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
|---|---|
| Installation Guide』を参照してください。<br>2 Cisco ISE と Active Directory を結合します。 | |
| DNS サーバに分散配置されているすべての Cisco ISE ノードに対して逆引き DNS ルックアップが設定されていることを確認します。そうしないと、アップグレード後に配置関連の問題が発生する可能性があります。 | — |
| 脅威中心型 NAC（TC-NAC）サービスを有効にしている場合は、アップグレード後に、TC-NAC アダプタが機能しない可能性があります。ISE GUI の [脅威中心型 NAC（Threat-Centric NAC）] ページからアダプタを再起動する必要があります。アダプタを再起動するには、アダプタを選択して [再起動（Restart）] をクリックします。 | — |
| プライマリ管理ノードから Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ管理ノードで復元します。これにより、PAN に障害が発生し、セカンダリ管理ノードをプライマリ管理ノードに昇格する場合に、セカンダリ管理ノードが外部 PKI ルート CA または下位 CA として動作するようになります。 | Cisco ISE CA 証明書およびキーのバックアップと復元 |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| 分散展開をアップグレードした後に、次の両方の条件が満たされた場合は、プライマリ管理ノードのルート CA 証明書は信頼できる証明書ストアに追加されません。<br>• セカンダリ管理ノード（古い展開のプライマリ管理ノード）は新しい展開でプライマリ管理ノードに昇格されている<br>• セッション サービスはセカンダリ ノードでディセーブルになっている<br>これにより、次のエラーで認証が失敗する可能性があります。<br>• Unknown CA in chain during a BYOD flow<br>• OCSP unknown error during a BYOD flow<br>これらのメッセージは、失敗した認証の [ライブ ログ（Live Logs）] ページの [詳細（More Details）] リンクをクリックすると表示されます。<br>回避策として、展開をアップグレードし、新しい展開でプライマリ管理ノードになるようにセカンダリ管理ノードをプロモートした後に、管理者ポータルから新しい ISE ルート CA 証明書チェーンを作成します（[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換（Replace ISE Root CA certificate chain）] の順に選択）。 | PAN および PSN でのルート CA および下位 CA の生成 |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| Cisco ISE は、シスコ以外の一部のネットワーク アクセス デバイス（NAD）をサポートしています。<br><br>リリース 2.0 以前にシスコ以外の NAD を展開し、それらを使用するようにポリシールールや RADIUS ディクショナリを作成した場合、これらは通常どおりに機能し続けます。<br><br>リリース 2.0 以降のリリースでは、MAB、dot1x、認可変更（CoA）、URL リダイレクト（ゲスト、フロー、ポスチャなどへのフローを可能にする）などのさまざまな機能をサポートできるように、シスコ以外のデバイスに適用できる事前定義されたネットワーク デバイス プロファイルがいくつか用意されています。<br><br>ネットワーク デバイス プロファイルを表示するには、管理者用ポータルから、[管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス プロファイル（Network Device Profile）] の順に選択します。<br><br>ネットワーク デバイス プロファイルを NAD に適用するには、次の手順を実行します。<br><br>1 [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] の順に選択します。<br><br>2 NAD を編集して、適切なプロファイルを選択します。<br><br>NAD の一覧をエクスポートし、プロファイルを追加、NAD を再インポートすることによって、簡単にネットワーク デバイス プロファイルを多くの NAD に同時に適用できます。 | Cisco ISE でのサードパーティ ネットワーク アクセス デバイスのサポート |
| 外部アイデンティティ ソースとして RSA SecurID サーバを使用する場合は、RSA のノード秘密をリセットします。 | RSA ノード秘密リセット |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
|---|---|
| ポスチャ サービスをイネーブルにした場合は、アップグレード後にプライマリ管理ノードからポスチャの更新を実行します。 | Cisco ISE へのポスチャ更新のダウンロード |
| SNMP の設定で、手動で [元のポリシー サービス ノード（Originating Policy Services Node）] の値を設定した場合、この設定はアップグレード中に失われます。この値を再設定する必要があります。 | 「Network Device Definition Settings」の「SNMP Settings」を参照してください。 |
| アップグレード後にプロファイラ フィード サービス更新して、最新OUIがインストールされているようにします。 | Cisco ISE 管理者用ポータルから：<br>1 [管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）] の順に選択します。プロファイラ フィード サービスが有効にされていることを確認します。<br>2 [今すぐ更新（Update Now）] をクリックします。 |

| タスクの説明 | 追加情報/『**Cisco ISE Administrator Guide**』の関連セクションのリンク |
| --- | --- |
| | — |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| アップグレード後に Cisco Temporal Agent を設定するには、次のいずれかのアップデートを実行します。<br>• オンライン更新<br>1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] を選択して、クライアントプロビジョニングリソースを設定します。<br>2 [追加（Add）] をクリックします。<br>3 [Cisco サイトからのエージェント リソース（Agent Resources From Cisco Site）] を選択します。<br>4 [リモート リソースのダウンロード（Download Remote Resources）] ウィンドウで、Cisco Temporal Agent リソースを選択します。<br>5 [保存（Save）] をクリックして、ダウンロードしたリソースが [リソース（Resources）] ページに表示されていることを確認します。<br>• オフライン更新<br>1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] を選択して、クライアントプロビジョニングリソースを設定します。<br>2 [追加（Add）] をクリックします。<br>3 [ローカルディスクからのエージェント リソース（Agent Resources from Local Disk）] を選択します。<br>4 [カテゴリ（Category）] ドロップダウン | |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| から、[シスコが提供するパッケージ（Cisco Provided Packages）] を選択します。 | |
| クライアント プロビジョニング ポリシーで使用されているネイティブのサプリカント プロファイルをチェックして、ワイヤレス SSID が正しいことを確認します。iOSデバイスの場合、接続対象ネットワークが非表示の場合は、[iOSの設定（iOS Settings）] エリアで [ターゲットネットワーク非表示時にイネーブルにする（Enable if target network is hidden）] チェックボックスをオンにします。 | — |

| タスクの説明 | 追加情報/『**Cisco ISE Administrator Guide**』の関連セクションのリンク |
| --- | --- |
| | — |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| Cisco ISE リリース 2.3 は、次の暗号方式をサポートしています。TLS バージョン 1.0、1.1 および 1.2 がサポートされます。<br>EAP-TLS、PEAP、EAP-FAST、EAP-TTLS の場合：<br>• ECDHE-RSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES128-GCM-SHA256<br>• ECDHE-RSA-AES256-SHA384<br>• ECDHE-RSA-AES128-SHA256<br>• ECDHE-RSA-AES256-SHA<br>• ECDHE-RSA-AES128-SHA<br>• AES256-SHA256<br>• AES128-SHA256<br>• AES256-SHA<br>• AES128-SHA<br>• DES-CBC3-SHA<br>[弱い暗号方式を EAP に許可する（Allow weak ciphers for EAP）] チェックボックスをオンにすると、次の暗号方式がサポートされます。<br>• RC4-SHA<br>• RC4-MD5<br>EAP-FAST 匿名プロビジョニングの場合：<br>ADH_WITH_AES_128_SHA<br>（注） これらの廃止予定の暗号方式を Cisco ISE に対する認証に使用する古い IP フォンなどのレガシー デバイスがある場合、これらのデバイスは従来の暗号方式を使用するため、認証は失敗します。Cisco ISE がそのようなレガシー デバイスを認証できるようにするには、リリース 2.2 にアップグレードした後、次のように許可されているプロトコルの設定を更新してください。<br>1 管理者用ポータルから、[ポリシー | |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
| --- | --- |
| （Policy）]>[ポリシー要素（Policy Elements）] > [認証（Authentication）]>[許可されているプロトコル（Allowed Protocols）] を選択します。<br>2 許可されているプロトコル サービスを編集し、[弱い暗号方式をEAPに許可する（Allow weak ciphers for EAP）]チェックボックスをオンにします。<br>3 [送信（Submit）] をクリックします。<br>サポートされている暗号スイートの完全なリストについては、『Cisco Identity Services Engine Network Component Compatibility, Release 2.2』を参照してください。 | |
| 電子メール設定、お気に入りレポート、データ削除設定を再設定します。 | 『Cisco ISE Administrator Guide』の「Monitoring and Troubleshooting section」を参照してください。 |
| 必要とする特定のアラームのしきい値またはフィルタを確認します。すべてのアラームは、アップグレード後にデフォルトでイネーブルになります。 | |
| 必要に応じてレポートをカスタマイズします。古い展開でレポートをカスタマイズした場合は、加えた変更が、アップグレードプロセスによって上書きされます。 | |

| タスクの説明 | 追加情報/『Cisco ISE Administrator Guide』の関連セクションのリンク |
|---|---|
| RSA キーを使用して SFTP リポジトリを作成した場合、セカンダリ管理ノードをそれ以降のリリースにアップグレードすると、RSA キーはプライマリ管理ノードから生成されるため、SFTP リポジトリはアクセス不能になります。<br>アップグレード後、SFTP リポジトリにアクセスするには、次のいずれかを実行します。<br>• 新しいプライマリ管理ノードから RSA キーを再生成します。<br>• アップグレード後、新しいセカンダリ管理ノードをプライマリ管理ノードに昇格させます。 | 詳細については、『Cisco ISE Administrator Guide』の「Create Repositories」の項を参照してください。 |
| 次のコマンドを次の順序で実行して、システムの Cisco TrustSec 対応レイヤー 3 インターフェイスにポリシーをダウンロードする必要があります。<br>**1** no cts role-based enforcement<br>**2** cts role-based enforcement | — |

アップグレード後の作業