



アップグレード後のタスク

- [アップグレード後のタスク \(1 ページ\)](#)

アップグレード後のタスク

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。ポリシー変更の詳細については、[新規ポリシー モデル](#)を参照してください。

これらのタスクの詳細については、「[Administrators Guide for your version of ISE](#)」を参照してください。

- **VM 設定の確認**

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。

ESXi 5.x サーバ (5.1 U2 以上) で ISE を実行する場合は、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。

- **ブラウザのセットアップ**

アップグレード後、Cisco ISE 管理者用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。また、リリースノートに記載されているサポート対象のブラウザを使用していることを確認します。 <https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html>

- **Active Directory の再結合**

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 ノードを再度結合する必要があります。結合

が完了した後に、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。

- 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。
- Cisco ISE への管理アクセスに対して証明書ベースの認証を有効にしている、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、アップグレード後に ISE ログインページを起動できません。これは、アップグレード中に Active Directory との結合が失われるためです。Active Directory との結合を復元するには、Cisco ISE CLI に接続し、次のコマンドを使用してセーフモードで ISE アプリケーションを開始します。

application start ise safe

Cisco ISE がセーフモードで起動したら、次のタスクを実行します。

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。

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、管理者ガイドの「[Administrator Access to Cisco ISE](#)」を参照してください。

2. Cisco ISE と Active Directory を結合します。

Active Directory との結合の詳細については、次の項目を参照してください。

[Configure Active Directory as an External Identity Source](#)

• Active Directory で使用される証明書属性

Cisco ISE は、SAM と CN のいずれか、または両方の属性を使用してユーザを識別します。Cisco ISE リリース 2.2 パッチ 5 以降、および 2.3 パッチ 2 以降は、sAMAccountName 属性をデフォルトの属性として使用します。これ以前のリリースでは、SAM と CN の両方の属性がデフォルトで検索されていました。この動作はリリース 2.2 パッチ 5 以降と 2.3 パッチ 2 以降で、[CSCv#21978](#) バグ修正の一部として変更されました。これらのリリースでは、sAMAccountName 属性のみがデフォルトの属性として使用されます。

実際の環境で必要に応じて、SAM と CN のいずれか、または両方を使用するように Cisco ISE を設定できます。SAM および CN が使用される場合、sAMAccountName 属性の値が一意でないと、Cisco ISE は CN 属性値も比較します。

Active Directory アイデンティティ検索の属性を設定するには、次の手順を実行します。

1. [管理 (Administration)] > [IDの管理 (Identity Management)] > [外部IDソース (External Identity Sources)] > [Active Directory] を選択します。[Active Directory] ウィンドウで、[拡張ツール (Advanced Tools)] をクリックし、[高度な調整 (Advanced Tuning)] を選択します。次の詳細を入力します。

- [ISEノード (ISE Node)] : Active Directory に接続される ISE ノードを選択します。
- [名前 (Name)] : 変更するレジストリ キーを入力します。Active Directory 検索属性を変更するには、
REGISTRY\Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
と入力します。
- 値 : ユーザを識別するために ISE で使用する属性を入力します。
 - SAM : クエリで SAM のみを使用します (このオプションがデフォルトです)。
 - CN : クエリで CN のみを使用します。
 - SAMCN : クエリで CN と SAM を使用します。
- コメント : 変更内容を記述します (たとえば「デフォルト動作を SAM および CN に変更」)。

2. [値の更新 (Update Value)] をクリックしてレジストリを更新します。

ポップアップウィンドウが表示されます。メッセージを読み取り、変更を受け入れます。ISE の AD コネクタ サービスが再起動します。

• 逆引き DNS ルックアップ

すべての DNS サーバに分散展開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デプロイメント配置関連の問題が発生する可能性があります。

• PAN での証明書の復元

分散展開をアップグレードすると、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。

- 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。
- 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。

証明書がストアにない場合は、認証エラーが発生し、次のエラーが表示される可能性があります :

- Unknown CA in chain during a BYOD flow
- OCSP unknown error during a BYOD flow

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。

回避策として、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昇格した後に、管理者用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)。

- 証明書とキーをセカンダリ管理ノードで復元する

セカンダリ管理ノードを使用している場合は、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。この操作により、プライマリ 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。

証明書とキーのバックアップおよび復元に関する詳細については、次の項目を参照してください。

[Backup and Restore of Cisco ISE CA Certificates and Keys](#)

- 脅威中心型 NAC

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。

- SNMP 送信元ポリシー サービス ノード設定

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。SNMP 設定を再設定する必要があります。

詳細については、以下を参照してください。

「[Network Device Definition Settings](#)」の「SNMP Settings」を参照してください。

- プロファイラ フィード サービス

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：

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。
2. [今すぐ更新 (Update Now)] をクリックします。

- クライアント プロビジョニング

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ブリカント 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。

ISE でのクライアントプロビジョニングリソースの更新：

• オンライン更新

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。
2. [追加 (Add)]をクリックします。
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。
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。
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。

• オフライン更新

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。
2. [追加 (Add)]をクリックします。
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。
4. [カテゴリ (Category)]ドロップダウンから、[シスコが提供するパッケージ (Cisco Provided Packages)]を選択します。

• 暗号スイート

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。アップグレード後に Cisco ISE がレガシー デバイスを認証できるようにするには、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。

1. 管理者用ポータルから、[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[結果 (Results)]>[認証 (Authentication)]>[許可されているプロトコル (Allowed Protocols)]を選択します。
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。
3. [送信 (Submit)]をクリックします。

サポート対象の暗号スイートの完全なリストについては、次のマニュアルを参照してください。

Cisco Identity Services Engine のリリース ノート

Cisco Identity Services Engine Network Component Compatibility

• モニタリングおよびトラブルシューティング

- 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。
- 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。

• MnT バックアップの復元

更新前に作成した MnT データの運用データ バックアップを使用して、バックアップを復元します。

詳細については、以下を参照してください。

詳細については、『Cisco ISE Administrator Guide』の「[Backup and Restore Operations](#)」を参照してください。

• Trustsec NAD に対するポリシーの更新

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3 インターフェイスにポリシーをダウンロードします。

1. no cts role-based enforcement
2. cts role-based enforcement

• サプリカント プロビジョニング ウィザードの更新

新しいリリースにアップグレードする場合、またはパッチを適用する場合、サプリカント プロビジョニング ウィザード (SPW) は更新されません。SPW を手動で更新し、新しい SPW を参照する新しいネイティブ サプリカント プロファイルと新しいクライアント プロビジョニング ポリシーを作成する必要があります。新しい SPW は ISE ダウンロード ページで使用できます。