CA SiteMinder Federation Standalone

インストールおよびアップグレード ガイド

r12.52 SP1

ca technologies

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- SiteMinder

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

マニュアルの変更点

以下の更新は、SiteMinder の以前のリリース内に見つかった問題の結果として、12.52 のドキュメントに対して行われました。

- SiteMinder コネクタ ライブラリに関する考慮事項 (P. 22) -- このトピックでは、CA SiteMinder® Federation Standalone が SiteMinder と連係できるように、ポリシー サーバにコピーする正しいライブラリについて説明します。 CQ 177513 を解決。
- Java Cryptographic Extension （JCE）用の必要なパッチ (P. 9) -- このアイテムは、Java によって提供される暗号化アルゴリズムを使用するために更新が必要なファイルを詳しく説明します。 CQ 174929 を解決。
- 既存の SAML パートナーシップに同じバックチャネル ユーザ名がないことを確認 (P. 70) -- 既存のパートナーシップに同じ SSO プロファイル内の同じ受信バックチャネル ユーザ名を使用できないというアップグレード要件について説明するトピックが追加されました。 CQ 177179 を解決。
- システムおよびインストールの前提条件 (P. 9)、UNIX システム上の CA SiteMinder® Federation Standalone のインストール (P. 19)、UNIX システム上の設定ウィザードの実行 (P. 48) -- さまざまなインストールおよび設定の問題が修正されました。 CQ 176815 を解決（STAR イシュー番号： 21189977 および 1+21182925;1）
- Windows 上のフェデレーション スタンドアロン 12.52 へのアップグレード (P. 72)、および UNIX 上のフェデレーション スタンドアロン 12.52 へのアップグレード (P. 75) -- AssertionGeneratorFramework.properties ファイルを更新する手順が追加されました。 これにより、CQ 176623 が解決されました。
- 設定のエクスポート (P. 85) -- 設定をエクスポートする前に、パートナーシップを非アクティブにして SSL を無効にする手順が削除されました。 これらの手順は不要です。 CQ 165316 を解決。

目次

第 1 章: CA SiteMinder® Federation Standalone のインストール

システムおよびインストールの前提条件

CA SiteMinder® Federation Standalone の最小システム要件は以下のとおりです。

メモリ

2 GB （最小）

ディスク容量

最小 3 GB （1 GB のディスク容量、2 GB の一時ファイル場所）

ブラウザ

Windows Internet Explorer、 Mozilla FireFox

対応オペレーティング システム

Windows、Solaris、 Linux

特定のバージョンに関する詳細については、**エラー! ハイパーリンクの参照に誤りがあります。**サイトの「CA SiteMinder® Federation Standalone プラットフォーム サポート マトリクス」を参照してください。

インストールの前提条件

インストールを成功させるには、以下の前提条件を満たす必要があります。

注: 特定のプラットフォームに関する詳細については、「CA SiteMinder® Federation Standalone リリース ノート」を確認してください。

Oracle または SQL Server データベース

ポリシー、キー、およびセッション ストアでサーバ データベースが使用されます。データベースをインストールし、データベース インスタンスに名前を付けます。 このインスタンス名は、後で設定ウィザードを実行するときに使用されます。

重要: 複数のサーバで 1 つのデータベース インスタンスを共有できますが、そのデータベース インスタンスはお使いのフェデレーション環境の専用にする必要があります。 SiteMinder サーバなど、他のアプリケーション用のサーバとデータベース インスタンスを共有しないでください。システムは専用データベース インスタンスを必要としますが、専用データベース サーバを必要としません。

データベース管理者には、データベースにテーブルを作成し、データベースにデータを入力する権限を与える必要があります。

特定のバージョンに関する詳細については、**エラー! ハイパーリンクの参照に誤りがあります。** サイトのプラットフォーム サポート マトリックスを参照してください。

Java

- サポートされる JDK が必要です。 特定のバージョンに関する詳細については、**エラー! ハイパーリンクの参照に誤りがあります。** サイトのプラットフォーム サポート マトリックスを参照してください。
- 現在の Java Cryptography Extension （JCE）の Unlimited Strength Jurisdiction パッチは、Java の暗号化アルゴリズムを使用するのに必要です。 使用しているプラットフォーム用の JCE パッケージを見つけるには、Oracle の Web サイトを参照してください。

  システム上の以下のファイルにパッチを適用します。

  - local_policy.jar
  - US_export_policy.jar

  これらのファイルは、以下のディレクトリにあります。

  Windows： *jre_home*¥lib¥security

  UNIX： *jre_home*/lib/security

  jre_home

  この変数は、Java Runtime Environment がインストールされる場所を指定します。

JavaScript

Javascript を有効にする必要があります。

Windows

管理者としてインストールを実行し、管理者としてフェデレーション サービスを停止および開始します。

Solaris および Linux

- root ユーザとして CA SiteMinder® Federation Standalone をインストールしないでください。 root ユーザとしてインストールを試行すると、インストールは失敗し、エラー メッセージが表示されます。代わりに、CA SiteMinder® Federation Standalone をインストールするためのユーザ アカウントを作成します。
- 1024 より下のポートを使用し、UNIX プラットフォームで CA SiteMinder® Federation Standalone を実行することは回避してください。この推奨事項にはデフォルト Apache HTTP ポート（80）とデフォルト Apache SSL ポート（443）が含まれます。

- 64 ビットのシステムでインストールする場合でも、インストール プログラムは 32 ビットのシステム ライブラリを必要とします。 インストールを実行する前に 32 ビットのライブラリを 64 ビットのシステムにインストールします。

  Linux システムで、32 ビットのライブラリをインストールした後に **updatedb** コマンドを実行します。 updatedb コマンドを実行すると、オペレーティング システムが新しいライブラリを認識します。

- xterminal で GUI モード インストールを実行するために X11 （32 ビット）ライブラリ パッケージをインストールします。 これらのパッケージは必須です。

Linux *のみ*

- **Linux 固有の Java 要件：**
  - JDK の必要なバージョンがシステム パスに存在することを確認します。
  - 必要なバージョン以外の Java のバージョンがインストールされていないことを確認します。（OpenJDK が、Red Hat と共にインストールされていることがあります。） OpenJDK が存在する場合は、削除するために以下のコマンドを実行してください。

    ```
    yum erase openjdk
    ```

  - Java ベースの GUI を実行するには、libXsts などの必須パッケージがシステムに必要です。 デフォルトでは通常、必須パッケージはシステムに備わっています。

- **/dev/urandom と /dev/random の間で必要なシンボリック リンク**

  再起動により、/dev/urandom と /dev/random の間に必要なシンボリック リンクが削除される場合があります。 このシンボリック リンクがないと、CA SiteMinder® Federation Standalone サービスを開始できない可能性があります。

  シンボリック リンクを回復させるには、以下のコマンドを入力します。

  ```
  rm dev/random;ln -s /dev/urandom /dev/random
  ```

- **ファイアウォール**

  ファイアウォールは無効である必要があります。

  ファイアウォールを無効にするには、以下のコマンドを実行します。

  ```
  /etc/init.d/iptables stop
  chkconfig iptables off
  ```

- ライブラリの依存関係
  - mlocate.86_64
  - glibc.i686
  - libstdc++.i686
  - compat-expat1.i686
  - libuuid.i686
  - ksh.86_64
  - X-Windows の場合：
    - libXext.i686
    - libXi.686
    - libXtst.686

CA SiteMinder® Federation Standalone のインストールの実行

CA SiteMinder® Federation Standalone をインストールするには次のプロセスを完了します。

1. インストール ウィザードで要求される情報を集めます。
2. 使用するインストール モードを決定します。
3. インストール プログラムを実行します。

重要: 次のインストール制限に注意してください。

- ポリシー サーバまたは Secure Proxy Server （SPS）がすでにインストールされているシステムに CA SiteMinder® Federation Standalone をインストールしないでください。 これらのその他のコンポーネントを備えたシステムに CA SiteMinder® Federation Standalone をインストールすると、既存の SiteMinder インストールにマイナスの影響を与える可能性があります。
- Apache Web サーバまたは Apache Tomcat サーバがすでに配置されているシステムに本製品をインストールしないでください。

インストールに必要な情報

CA SiteMinder® Federation Standalone をインストールする前に、次の情報を用意します。 情報はインストール中に要求されます。

インストールした JDK へのパス

CA SiteMinder® Federation Standalone をインストールする前に、JDK をインストールし、その場所を記録します。

CA SiteMinder® Federation Standalone 管理者パスワード

CA SiteMinder® Federation Standalone のインストール中にパスワードの入力が要求されます。 このパスワードは、CA SiteMinder® Federation Standalone UI にログインする際に使用するものです。

注: CA SiteMinder® Federation Standalone 管理者パスワードには英語（ASCII）文字のみを含めることができます。

FIPS モード

次の FIPS 操作モードのいずれかで CA SiteMinder® Federation Standalone をインストールできます。

FIPS_COMPAT

FIPS_COMPAT（互換性）モードは、インストール中のデフォルトの FIPS 操作モードです。FIPS_COMPAT モードでは、フェデレーション システムは、サポートされている FIPS 準拠アルゴリズムと共に非 FIPS アルゴリズムの現在のセットも引き続きサポートします。

FIPS_COMPAT モードは、旧バージョンのフェデレーションと互換性があります。 この互換性により、r12.52 SP1 よりも前のバージョンの環境が r12.52 SP1 と相互運用できるようになります。また、FIPS_COMPAT は、現在のフェデレーション実装で使用可能なセキュリティの程度に満足しているすべてのライアントにとっても適切です。

組織が FIPS の使用を必要としない場合、CA SiteMinder® Federation Standalone を FIPS_COMPAT モードでインストールします。追加設定は必要ありません。

FIPS_ONLY

FIPS_ONLY モードでは、環境は FIPS 準拠アルゴリズムのみを使用して機密データを暗号化します。

FIPS 互換アルゴリズムのみを使用する新しいインストールの場合、CA SiteMinder® Federation Standalone を FIPS_ONLY モードでインストールします。

重要: FIPS モードを変更するたびに CA SiteMinder® Federation Standalone を再起動します。

使用するインストール モードの決定

以下のいずれかのモードを使用し、Windows または UNIX プラットフォームに CA SiteMinder® Federation Standalone をインストールできます。

- GUI モード -- グラフィカル ユーザ インターフェース インストールを有効にします。
- コンソール モード -- コマンド ライン インストールを有効にします。
- 無人モード -- ユーザの介在を必要としないファイル ベースのインストールを有効にします。 他のシステムで無人モードを使用する前に、1 つのシステムで 1 つの GUI またはコンソール モード インストールを完了する必要があります。

r12.52 SP1 用のインストール実行可能ファイル

次の表は、CA SiteMinder® Federation Standalone のインストール実行可能ファイルを識別したものです。 この表はプラットフォーム別に整理されています。

Platform	インストール実行ファイル
Linux	ca-fedmgr-r12.52 SP1-rhel30.bin
Solaris	ca-fedmgr-r12.52 SP1-sol.bin
Windows	ca-fedmgr-r12.52 SP1-win32.exe

サポートされているオペレーティング システムの詳細については、テクニカル サポート サイトで「CA SiteMinder® Federation Standalone プラットフォーム サポート マトリクス」を参照してください。

Windows システムでの CA SiteMinder® Federation Standalone のインストール

これらの手順は Windows システムで GUI およびコンソール モードでインストールするための手順です。 2 つのモードの手順は同じですが、コンソール モードについては以下に示す例外があります。

- 対応する数を入力してオプションを選択するように指示される場合があります。
- 各手順の後に ENTER キーを押してプロセスを続行します。
- 各モードのプロンプトにより、順を追ってプロセスをガイドします。
- 「BACK」を入力すると前の手順に戻ることができます。

重要: 次のインストール制限に注意してください。

- ポリシー サーバまたは Secure Proxy Server （SPS）がすでにインストールされているシステムに CA SiteMinder® Federation Standalone をインストールしないでください。 これらのその他のコンポーネントを備えたシステムに CA SiteMinder® Federation Standalone をインストールすると、既存の SiteMinder インストールにマイナスの影響を与える可能性があります。
- Apache Web サーバまたは Apache Tomcat サーバがすでに配置されているシステムに本製品をインストールしないでください。

インストール キットを見つける方法

1. テクニカル サポート サイトに移動します。
2. サイトにログオンします。
3. ［Download Center］をクリックします。

必要とするインストール キットの［Download Center］を検索し、ローカル システムにそれをダウンロードします。

Windows で CA SiteMinder® Federation Standalone をインストールする方法

1. 実行しているすべてのアプリケーションを終了し、アンチウイルス ソフトウェアを停止します。
2. インストールを実行します。

   インストールの実行方法は、ローカル管理者としてログインした場合と、ネットワーク ユーザとしてログインした場合で異なります。ネットワーク ユーザの場合、インストールを実行するには Administrators グループに属する必要があります。

   - **GUI モード**

     ローカル管理者： *installation_executable* をダブルクリックします

     ネットワーク ユーザ: *installation_executable* を右クリックし、［管理者として実行］を選択します
   - **コンソール モード：** コマンド ウィンドウを開き、「*installation_executable* -i console」を入力します

   CA SiteMinder® Federation Standalone インストール ウィザードが起動します。

   注: インストール実行可能ファイルのリストを表示します。
3. インストールに先立って収集した情報を使用し、各インストール ダイアログ ボックスのプロンプトに応答します。

   ［ライセンス契約］ダイアログ ボックスの契約を読みます。契約を受け入れるか、拒否するには、契約の終わりまでスクロールする必要があります。
4. インストール概要のインストール設定を確認し、［インストール］をクリックするか（GUI モード）、「Y」を入力して（コンソール モード）インストールします。

   インストールが実行されます。

   インストール中に問題が発生した場合、インストール ログ ファイルの CA_Federation_Standalone_Install_*date_time*.log （ディレクトリ *federation_install_dir*¥install_config_info にあります）を確認します。
5. インストールが完了したら、システムを再起動します。

システムの再起動後、設定ウィザードが続行されます。

UNIX システムへの CA SiteMinder® Federation Standalone のインストール

これらの手順は UNIX システムで GUI およびコンソール モードでインストールするための手順です。 2 つのモードの手順は同じですが、コンソール モードについては以下に示す例外があります。

- 該当する数を入力し、オプションを選択するように指示されます。
- 各手順の後に ENTER キーを押してプロセスを続行します。
- 各モードのプロンプトにより、順を追ってプロセスをガイドします。
- 「BACK」を入力すると前の手順に戻ることができます。

注: CA SiteMinder® Federation Standalone をインストールする予定の UNIX システムで IPv6 アドレスが使用される場合、コンソール モードでのみインストールを実行します。 GUI モードでインストールを試行すると、サードパーティ制限により、インストール プログラムはデフォルトのコンソール モードになります。

重要: 次のインストール制限に注意してください。

- ポリシー サーバまたは Secure Proxy Server （SPS）がすでにインストールされているシステムに CA SiteMinder® Federation Standalone をインストールしないでください。 これらのその他のコンポーネントを備えたシステムに CA SiteMinder® Federation Standalone をインストールすると、既存の SiteMinder インストールにマイナスの影響を与える可能性があります。
- Apache Web サーバまたは Apache Tomcat サーバがすでに配置されているシステムに本製品をインストールしないでください。
- root ユーザとして CA SiteMinder® Federation Standalone をインストールしないでください。 root ユーザとしてインストールを試行すると、インストールは失敗し、エラー メッセージが表示されます。代わりに、CA SiteMinder® Federation Standalone をインストールするためのユーザ アカウントを作成します。
- 1024 より下のポートを使用し、UNIX プラットフォームで CA SiteMinder® Federation Standalone を実行することは回避してください。この推奨事項にはデフォルト Apache HTTP ポート（80）とデフォルト Apache SSL ポート（443）が含まれます。
- Linux では、KornShell （ksh）を使用してインストールを実行します。

インストール キットを見つける方法

1. テクニカル サポート サイトに移動します。
2. サイトにログオンします。
3. ［Download Center］をクリックします。
4. 必要とするインストール キットの［Download Center］を検索し、ローカル システムにそれをダウンロードします。

CA SiteMinder® Federation Standalone を UNIX システムにインストールする方法

1. 実行しているすべてのアプリケーションを終了し、アンチウイルス ソフトウェアを停止します。
2. 必要な権限がない場合、次のように chmod コマンドを実行し、インストール ファイルに実行可能許可を追加します。

   Linux： chmod +x ca-fedmgr-r12.52 SP1-rhel30.bin
3. コマンド ウィンドウに次のいずれかのコマンドを入力します。
   - **GUI モード：** *./installation_executable*
   - **コンソール モード：** *./installation_executable* -i console

   CA SiteMinder® Federation Standalone インストール ウィザードが起動します。

   注: インストール実行可能ファイルのリストがこのガイドにあります。
4. インストールに先立って収集した情報を利用し、インストール プロンプトに応答します。

   ［ライセンス契約］ダイアログ ボックスの契約を読みます。契約を受け入れるか、拒否するには、契約の終わりまで表示します。
5. インストール設定を確認し、［インストール］をクリックするか（GUI モード）、「Y」を入力して（コンソール モード）インストールします。

   CA SiteMinder® Federation Standalone インストール プログラムが実行されます。

   インストール中に問題が発生した場合、インストール ログ ファイルの CA_Federation_Standalone_Install_date_time.log （ディレクトリ *federation_install_dir*/install_config_info にあります）を確認します。

インストールが完了すると、設定ウィザードが続行されます。

Solaris 10 セキュリティ プロパティ ファイルは変更を必要とします

デフォルト セキュリティ プロバイダ設定が配置されている場合、CA SiteMinder® Federation Standalone は Solaris 10 システムで暗号化と復号化を正しく実行できません。

この問題を解決するには、java.security プロパティ ファイルで PKCS11 プロバイダ（sun.security.pkcs11.SunPKCS11）の前に Sun プロバイダ（sun.security.provider.Sun）を配置します。このファイルは JDK インストールの lib/security ディレクトリにあります。

java.security ファイルを次のように変更します。

security.provider.1=sun.security.provider.Sun

security.provider.2=sun.security.pkcs11.SunPKCS11
${java.home}/lib/security/sunpkcs11-solaris.cfg

security.provider.3=sun.security.rsa.SunRsaSign

security.provider.4=com.sun.net.ssl.internal.ssl.Provider

security.provider.5=com.sun.crypto.provider.SunJCE

security.provider.6=sun.security.jgss.SunProvider

security.provider.7=com.sun.security.sasl.Provider

SiteMinder コネクタ ライブラリに関する考慮事項

CA SiteMinder® Federation Standalone インストールには、SiteMinder コネクタが含まれているため、フェデレーション製品が SiteMinder で保護されたアプリケーションとユーザ ID 情報を共有できるようになります。 コネクタはプロキシまたはスタンドアロンの展開モードで使用できます。

smauthconnectors.zip ファイルは、コネクタと連係するために製品インストールに含まれています。 ライブラリをアーカイブから抽出すると、コネクタ ライブラリの以下の 2 つのバージョンが抽出されます。

Windows

smauthsmconnector.dll

smauthsmconnectorI18n.dll

Solaris/Linux

libsmauthsmconnector.so

libsmauthsmconnectorI18n.so

smauthsmconnector.dll および libsmauthsmconnector.so ファイルは、12.52 より前のライブラリです。 smauthsmconnectorI18n.dll および libsmauthsmconnectorI18n.so は、新しいライブラリで、国際的な文字を処理できます。

CA SiteMinder® Federation Standalone と SiteMinder が共に動作するには、適切なライブラリを SiteMinder ポリシー サーバにコピーします。 ライブラリは以下のいずれかのポリシー サーバ ディレクトリに属します。

- **Windows**： *policy_server_home*¥siteminder¥bin
- **Solaris/Linux**： *policy_server_home*/siteminder/lib

コピーするライブラリにはいくつかの考慮事項があります。

新しいフェデレーション インストールの場合は、以下のガイドラインに従います。

- r12.51 より前のポリシー サーバとの接続をセットアップするには、12.52 より前のライブラリをポリシー サーバにコピーします。 新しいライブラリは使用しないでください。

  国際的な文字を処理する必要がある r12.51 ポリシー サーバとの接続をセットアップするには、新しいライブラリをポリシー サーバにコピーします。 ライブラリの名前を 12.52 より前の名前（smauthsmconnector.dll または libsmauthsmconnector.so）に変更します。

- r12.52 またはそれより新しいポリシー サーバとの接続をセットアップするには、ライブラリをコピーする必要はありません。 r12.52 以降のポリシー サーバの場合、オペレーティング環境に対して関連ライブラリがインストールされています。

12.52 より前の既存の設定によって国際的な文字を扱うには、以下のガイドラインに従います。

- r12.51 より前のポリシー サーバの場合、新しいライブラリは使用できません。 国際化は、r12.51 より前の展開では管理できません。
- r12.51 ポリシー サーバの場合、既存のライブラリをバックアップして新しいライブラリをコピーします。

  次の手順に従ってください：

  a. ポリシー サーバを停止します。

  b. 既存のライブラリのバックアップ コピーを作成し、一意の名前（smauthsmconnector_bkup.dll など）を付けます。

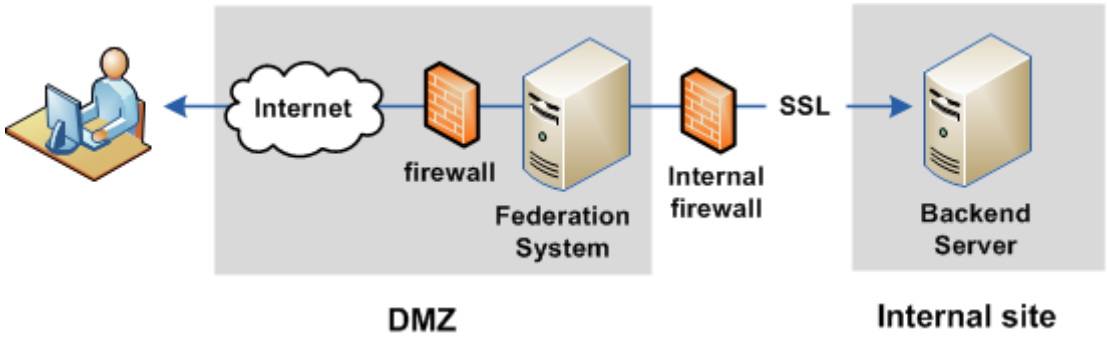
  c. 新しいライブラリをポリシー サーバにコピーします。

  d. 名前を 12.52 より前の名前（smauthsmconnector.dll または libsmauthsmconnector.so）に戻します。

  e. ポリシー サーバを再起動します。

フェデレーション システムとバックエンド サーバ間の SSL の有効化

フェデレーション ネットワークでは、フェデレーション システムは SSL 接続を介してバックエンド サーバと通信できます。 次の図はネットワークの構成を示したものです。



次の手順に従ってください:

1. SSL のバックエンド サーバを設定します。

   手順については、サーバのドキュメントを参照してください。

2. フェデレーション システムで、サーバ証明書を署名した CA 証明書を ca-bundle.cert ファイルに追加します。 このサーバ証明書は、SSL を有効にするためにバックエンド サーバで使用した証明書です。

   ca-bundle.cert ファイルは、ディレクトリ *federation_install_dir*¥secure-proxy¥SSL¥certs にあります。

   federation_install_dir は、本製品がインストールされた場所です。

   バックエンド サーバの管理者からのこの証明書を取得します。

Windows または UNIX プラットフォームでのフェデレーション システムの再インストール

既存のインストールの上に CA SiteMinder® Federation Standalone の同じバージョンを再インストールできます。 再インストールすることで、失われたアプリケーション ファイルをリストアするか、デフォルト インストール設定をリストアできます。

注: 本製品をアンインストールせずに再インストールできます。

次の手順に従ってください:

1. UNIX プラットフォームでは、環境スクリプトの ca_federation_env.ksh を用意します。
2. 初回インストールに使用したのと同じプログラムを使用し、インストール プログラムを再度実行します。
3. システムの再起動を求められたら再起動します。
4. 設定ウィザードを再実行します (P. 26)。

   再インストールの後に設定ウィザードを再実行します。 この手順は、元のインストールと設定に使用したのと同じ設定を使用するかどうかに関係なく必要です。
5. システムの再起動を求められたら再起動します。

注: 再インストールしたフェデレーション システムに Windows 認証のエージェントをインストールした場合、エージェントを再設定します。再設定しないと、正しく作動しません。

再インストールが完了します。

CA SiteMinder® Federation Standalone 設定ウィザードの実行

フェデレーション製品をインストールした後、設定ウィザードを実行します。

設定ウィザードでは、ポリシー ストアとして使用されるデータベース、フェデレーション サーバのポート、Apache Web サーバ設定をセットアップします。

設定ウィザードはいつでも再実行し、既存の設定を変更できますが、既存の設定が破棄されることに注意してください。 設定を保持するには、それをバックアップします。

注: SSL が有効になっている Windows システムを再設定する場合は、システムを再設定する前に SSL 設定を非アクティブ化します。再設定が完了したら、SSL を再度アクティブにします。

以下の設定プロセスを実行します。

1. 設定ウィザードで要求される情報を集めます。
2. 設定ウィザードを実行します。

設定前に展開モードを決定します

設定ウィザードを実行するとき、次のいずれかの展開モードを選択します。

- プロキシ モード
- スタンドアロン モード

展開モードは、依存パーティとしてフェデレーション システムにどのようにリクエストを処理させるかによって決めます。 依存パーティとは、モードがフェデレーションの実装方法に最も影響を与えるフェデレーション通信の側です。

展開モードを変更するには、設定ウィザードを再実行します。

各モードは、ユーザが選択した SAML 互換フェデレーション製品と連動できます。CA SiteMinder® Federation Standalone は任意で SiteMinder コネクタと連動し、既存の SiteMinder 展開と統合することもできます。

プロキシ モード

プロキシ モード展開では、DMZ でフェデレーション システムを使用し、フェデレーション アプリケーションをホストするバックエンド Web サーバに要求を転送します。 これらのバックエンド システムはファイアウォールの後ろに置かれ、直接アクセスすることはできません。

プロキシ モードには以下の長所があります。

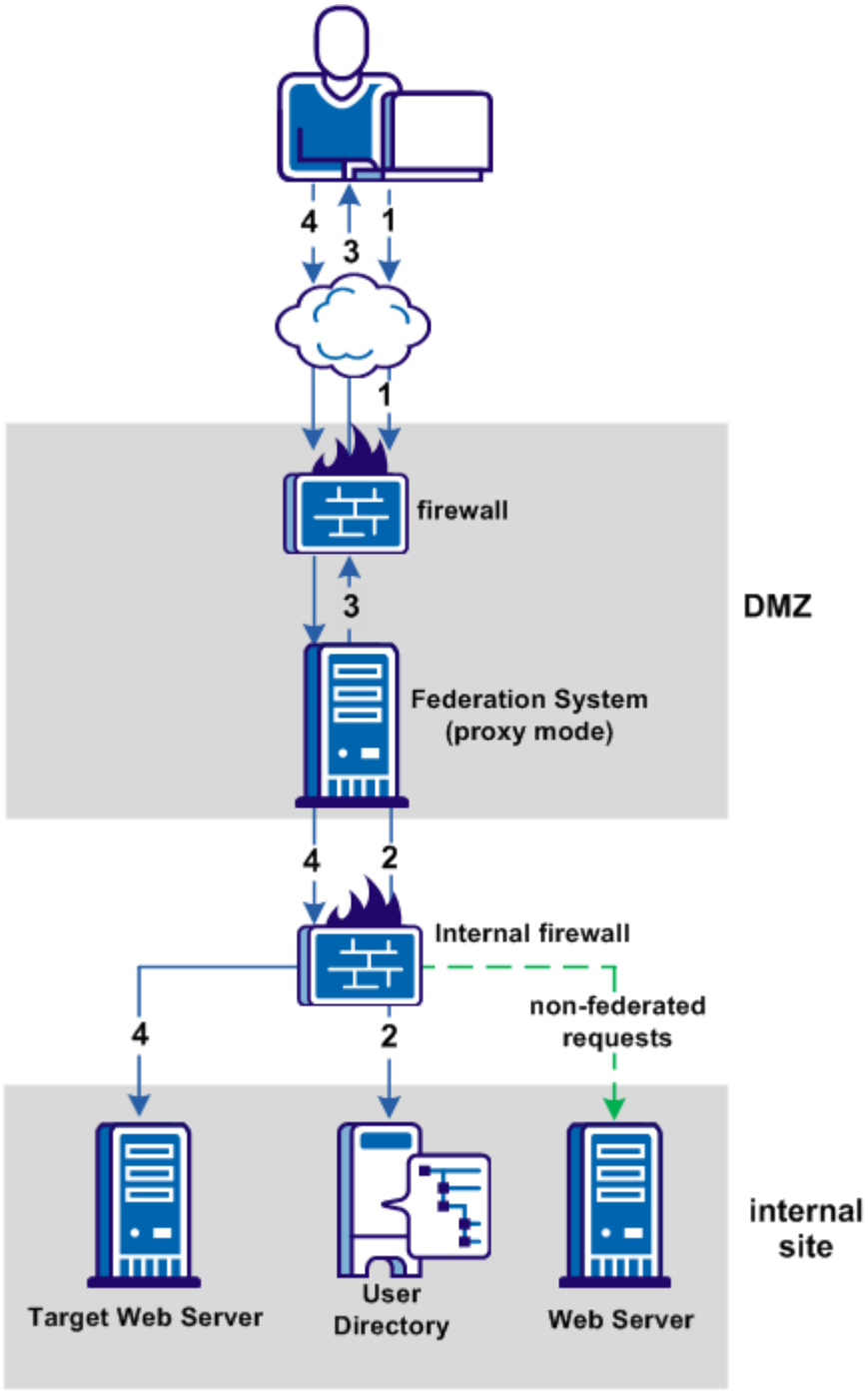
- ネットワークへのアクセス ポイントを 1 つ提供します。
- フェデレーション システムで、HTTP ヘッダを利用し、SAML アサーションからバックエンド アプリケーションに ID 属性を提供することを可能にします。 その後、もっとパーソナライズされたユーザ操作性を提供するようにアプリケーションをカスタマイズできます。

注: HTTP ヘッダ プレフィックスを設定することで、無許可のユーザによる変更から HTTP ヘッダを保護できます。 プロキシ モードでの HTTP ヘッダの保護に関しては、さらに多くの詳細があります。

プロキシ モードでは、フェデレーション システムはすべての要求をバックエンド ネットワークに渡します。 バックエンド Web サーバのすべてのリソースが SiteMinder または別のアクセス制御製品によって保護されていることを確認してください。

たとえば、バックエンド Web サーバは、ファイアウォールの後ろの非保護のリソースと同様に、フェデレーション アプリケーションもホストする場合があります。 管理者がフェデレーション アプリケーションを公開する場合、非保護のリソースも公開されます。これは、フェデレーション システムは認可を確認せずにバックエンド Web サーバへのフル アクセスを許可するためです。 このとき、非フェデレーション リソースが URL アドレス可能であるものと想定されます。

以下の図では、依存パーティの観点から典型的なプロキシ モード展開を示したものです。



前の図は、依存パーティでの次の通信フローを示したものです。

1. ユーザは、フェデレーション リソースに最初の要求を行います。
2. アサーションのデータに基づいて、フェデレーション システムは内部サイトのユーザ ディレクトリに問い合わせてユーザを認証し、ユーザを特定するプロセスを完了します。
3. 認証に成功した後、リダイレクト応答がユーザのブラウザに返されます。
4. フェデレーション システムは代理としてターゲット Web サーバにリクエストを渡します。ユーザはリソースにアクセスします。

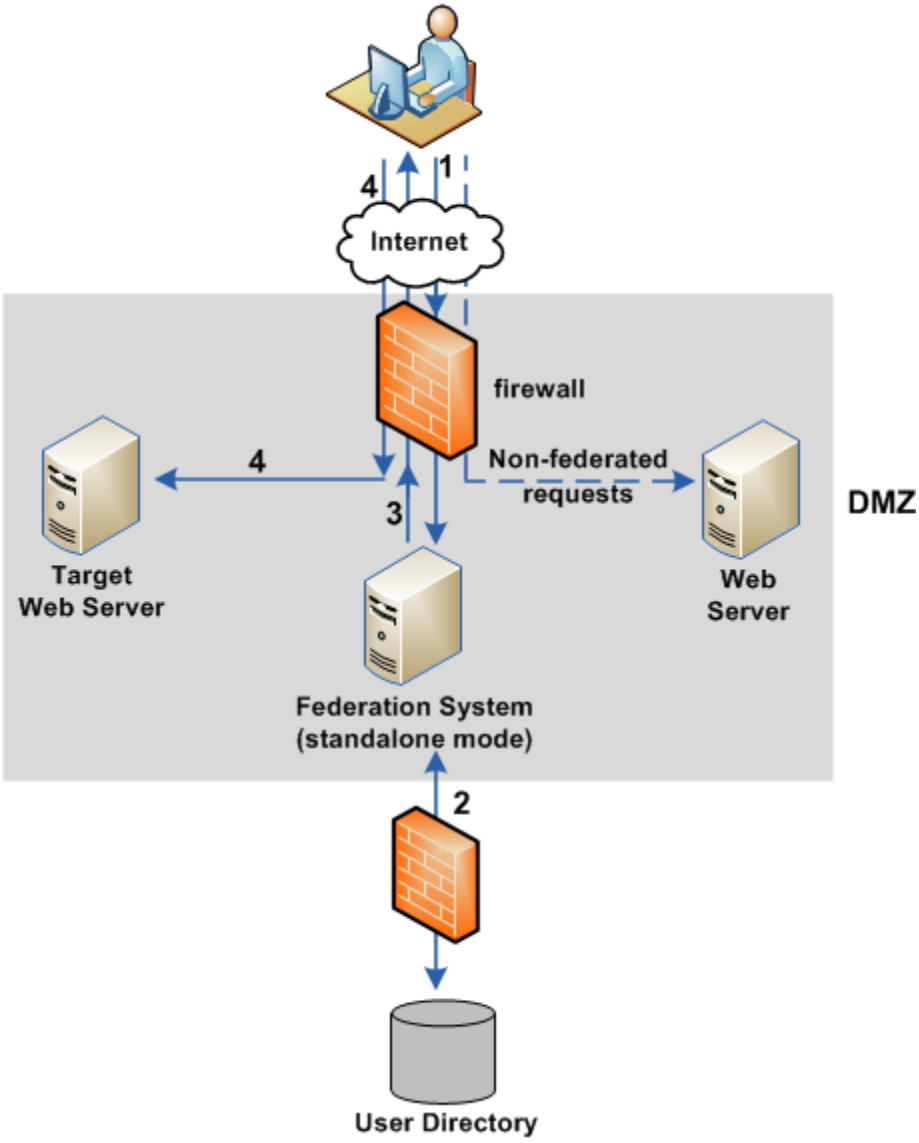
スタンドアロン モード

スタンドアロン モード展開では、CA SiteMinder® Federation Standalone はフェデレーション リクエストのみを処理し、ターゲット Web サーバにこれらのリクエストをリダイレクトします。 非フェデレーション リクエストは、CA SiteMinder® Federation Standalone には関係なく、適切な Web サーバに直接送信されます。

スタンドアロン モードの利点は、それがフェデレーション トラフィックを CA SiteMinder® Federation Standalone に限定し、他のコンテンツの処理の負荷を他の Web サーバに分散することです。 また、サイトは、既存のインフラストラクチャを中断せずに、そのネットワークにフェデレーションを追加できます。

スタンドアロン モードでは、HTTP ヘッダを応答に追加するプロキシが Web サーバとブラウザの間にないため、アサーションからユーザ属性を渡すことができません。

次の図は、依存パーティの観点から典型的なスタンドアロン モード展開を示したものです。



前の図は、依存パーティでの次の通信フローを示したものです。

1. あるユーザがフェデレーション リソースを要求します。
2. アサーションのデータに基づき、CA SiteMinder® Federation Standalone はユーザを認証します。その際、ユーザ ディレクトリと通信し、ユーザを特定するプロセスを完了します。
3. CA SiteMinder® Federation Standalone はユーザのブラウザにリダイレクト応答を返します。
4. ブラウザは、CA SiteMinder® Federation Standalone を通過せずに、ユーザをターゲット Web サーバのターゲット リソースにリダイレクトします。

SiteMinder のある CA SiteMinder® Federation Standalone 展開

CA SiteMinder® Federation Standalone には SiteMinder コネクタが組み込まれており、SiteMinder により保護されるアプリケーションとユーザ識別情報を共有できます。CA SiteMinder® Federation Standalone と SiteMinder のこの統合はシングル サインオンを促進します。SiteMinder コネクタはプロキシまたはスタンドアロン展開モードで使用できます。

一部のパートナーシップがコネクタを使用する間、他のパートナーシップがコネクタを使用しないように、パートナーシップ単位で SiteMinder コネクタを有効にします。 グローバル SiteMinder コネクタ オブジェクトは 1 つだけ存在します。 あるパートナーシップのコネクタを有効にすると、そのパートナーシップはグローバル コネクタ設定を使用します。

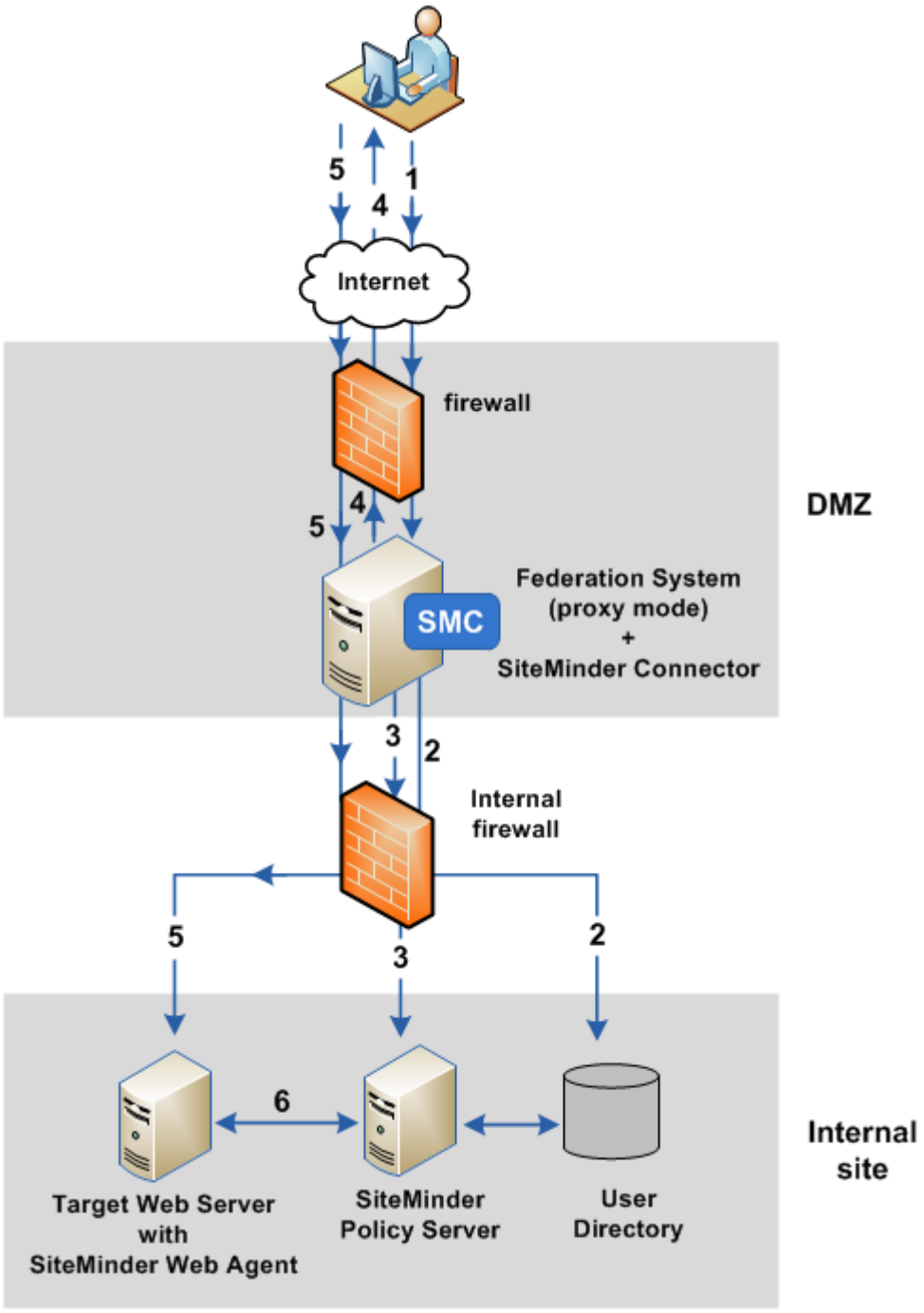
重要: SiteMinder コネクタは、独立 SiteMinder インストールに接続するために使用されます。 SiteMinder ポリシー サーバまたは Secure Proxy Server（SPS）がすでにインストールされているシステムに CA SiteMinder® Federation Standalone をインストールしないでください。

SiteMinder コネクタの使用に関する詳細については、「CA SiteMinder® Federation Standalone ガイド」を参照してください。

依存パーティに SiteMinder コネクタを置くプロキシ モード

CA SiteMinder® Federation Standalone がプロキシ モードで SiteMinder と通信する場合でも、すべてのリクエストは CA SiteMinder® Federation Standalone を通過します。ただし、ユーザが SiteMinder 保護のリソースを要求したときに再チャレンジされないように、CA SiteMinder® Federation Standalone はポリシー サーバと SiteMinder セッションを確立する必要があります。 リクエストは SiteMinder Web エージェントにより保護されるターゲット Web サーバにリダイレクトされます。

以下の図は、SiteMinder コネクタを使用したプロキシ モード アーキテクチャを示したものです。 これは依存パーティの観点からみた図です。



前の図は、依存パーティでの次の通信フローを示したものです。

1. ユーザはフェデレーション リソースを要求し、依存パーティのアサーション コンシューマ サービスにリダイレクトされます。
2. アサーションで受信したデータに基づき、CA SiteMinder® Federation Standalone はユーザを認証します。その際、ユーザ ディレクトリと通信し、ユーザを特定するプロセスを完了します。
3. SiteMinder コネクタは CA SiteMinder® Federation Standalone の一部であり、SiteMinder ポリシー サーバでカスタム認証方式に問い合わせます。ポリシー サーバにより SiteMinder セッション チケットが作成され、CA SiteMinder® Federation Standalone に送信されます。 CA SiteMinder® Federation Standalone は次に、そのチケットを含むセッション Cookie を作成します。SiteMinder セッションを確立することで、後にターゲット リソースにアクセスしたときにユーザが再チャレンジされることがありません。
4. CA SiteMinder® Federation Standalone はユーザのブラウザにリダイレクト応答を返します。
5. ブラウザはユーザを CA SiteMinder® Federation Standalone にリダイレクトします。CA SiteMinder® Federation Standalone は、SiteMinder Web エージェントによって保護され、ターゲット リソースのある Web サーバに代理としてリクエストを送信します。
6. SiteMinder Web エージェントとポリシー サーバは認証プロセスを実行します。

   認証が成功すると、ユーザのブラウザにターゲット リソースが提示されます。

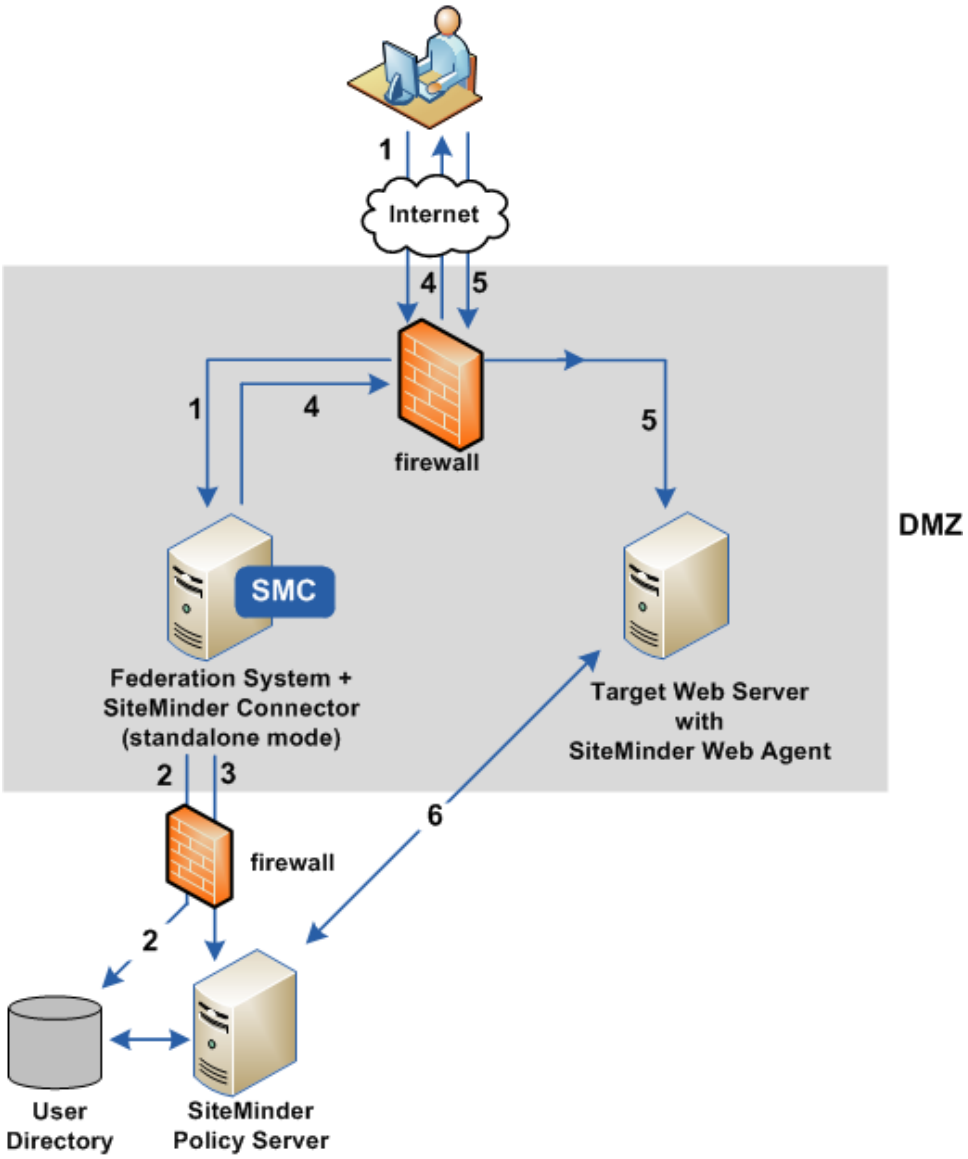
依存パーティに SiteMinder コネクタを置くスタンドアロン モード

CA SiteMinder® Federation Standalone がスタンドアロン モードで既存の SiteMinder 環境と通信する場合、CA SiteMinder® Federation Standalone はフェデレーション リクエストのみを処理します。

SiteMinder と連動するには、ユーザが SiteMinder 保護のリソースを要求するときに再チャレンジされないように、CA SiteMinder® Federation Standalone はポリシー サーバと SiteMinder セッションを確立する必要があります。フェデレーション リクエストは最終的に、SiteMinder Web エージェントにより保護されるターゲット Web サーバにリダイレクトされます。

注: CA SiteMinder® Federation Standalone と SiteMinder Web エージェントは、スタンドアロン モードで同じ Cookie ドメインを共有する必要があります。

次の図は、SiteMinder コネクタを使用するスタンドアロン モード アーキテクチャを示したものです。 これは依存パーティから観察される図です。



前の図は、依存パーティでの次の通信フローを示したものです。

1. ユーザはフェデレーション リソースを要求し、依存パーティのアサーション コンシューマ サービスにリダイレクトされます。
2. アサーションのデータに基づき、CA SiteMinder® Federation Standalone はユーザを認証します。その際、ユーザ ディレクトリと通信し、ユーザを特定するプロセスを完了します。
3. SiteMinder コネクタは CA SiteMinder® Federation Standalone の一部であり、SiteMinder ポリシー サーバでカスタム認証方式に問い合わせます。ポリシー サーバにより SiteMinder セッション チケットが作成され、CA SiteMinder® Federation Standalone に送信されます。 CA SiteMinder® Federation Standalone は次に、そのチケットを含むセッション Cookie を作成します。SiteMinder セッションを確立することで、後にターゲット リソースにアクセスしたときにユーザが再チャレンジされることがありません。
4. CA SiteMinder® Federation Standalone はユーザのブラウザにリダイレクト応答を返します。
5. ブラウザは、SiteMinder Web エージェントによって保護され、ターゲット リソースのある Web サーバにユーザをリダイレクトします。
6. SiteMinder Web エージェントとポリシー サーバは認証プロセスを完了します。

   認証が成功すると、ユーザのブラウザにターゲット リソースが提示されます。

アサーティング パーティに SiteMinder コネクタを置く展開

アサーティング パーティで CA SiteMinder® Federation Standalone に SiteMinder コネクタを設定すると、SiteMinder 使用してユーザを認証できます。 認証に成功したら、アサーションを発行する CA SiteMinder® Federation Standalone にユーザをリダイレクトする必要があります。

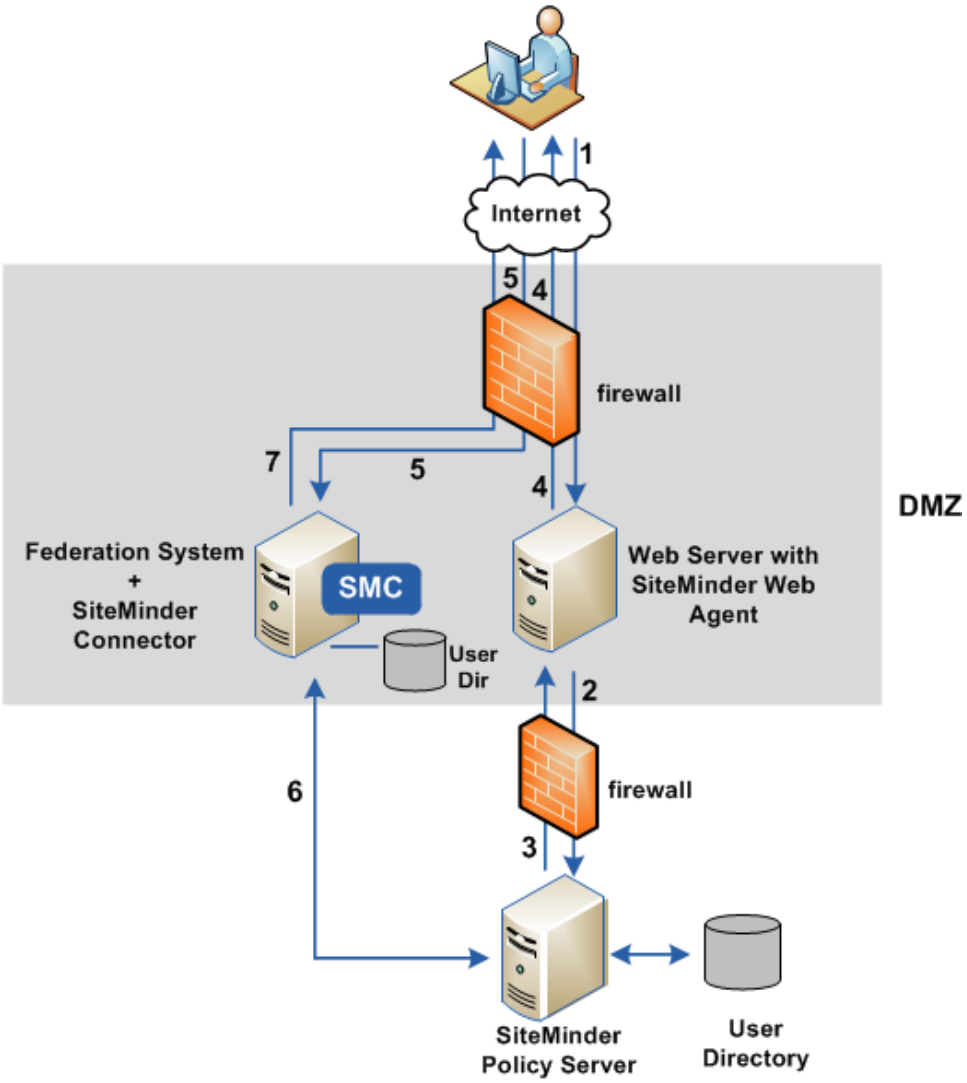
アサーティング パーティで SiteMinder はユーザを認証し、SMSESSION Cookie を発行します。 ユーザが CA SiteMinder® Federation Standalone に送信されたときに SMSESSION Cookie が存在すると、FEDSESSION Cookie の作成がトリガされます。 この場合、展開モード（プロキシまたはスタンドアロン）は関連しません。

注: CA SiteMinder® Federation Standalone がスタンドアロン モードで作動している場合、CA SiteMinder® Federation Standalone と SiteMinder Web エージェントは同じ Cookie ドメインを共有する必要があります。

SiteMinder を置く展開の場合、ユーザは最初に SiteMinder にアクセスして本物であることを証明する必要があります。 認証に成功したら、SiteMinder によって保護された Web リソースは CA SiteMinder® Federation Standalone にユーザを送信する必要があります。 SiteMinder コネクタを置く展開は「委任認証」と呼ばれる CA SiteMinder® Federation Standalone 機能とは異なります。委任認証の場合、SiteMinder のような Web アクセス管理システムでユーザ認証の処理を許可します。 委任認証と、委任認証のない SiteMinder コネクタ展開の違いは、委任認証の場合、ユーザが SiteMinder で認証を開始する必要がないということです。

委任認証では、CA SiteMinder® Federation Standalone が認証リクエストを開始し、ユーザを SiteMinder にリダイレクトします。この機能が正しく設定されていれば、リダイレクトは自動的に行われます。 ユーザの認証が成功した後に CA SiteMinder® Federation Standalone にユーザをリダイレクトするには、SiteMinder が保護するリソースを、CA SiteMinder® Federation Standalone にユーザをリダイレクトするメカニズムで設定する必要があります。 リダイレクトには、保護されているリソースが受信したすべてのデータを含める必要があります。 たとえば、SiteMinder に保護されたリソースが初回認証リクエストからいくつかのクエリ パラメータを受信した場合、そのリソースは同じクエリ パラメータを持つ CA SiteMinder® Federation Standalone にユーザをリダイレクトする必要があります。

次の図は、アサーティング パーティで SiteMinder コネクタを使用するアーキテクチャを示したものです。



前の図は、アサーティング パーティでの次の通信フローを示したものです。

1. ユーザはフェデレーション リソースをリクエストします。それにより、アサーティング パーティで SiteMinder Web エージェントへの認証リクエストがトリガにされます。
2. 認証リクエストは SiteMinder ポリシー サーバに転送されます。

3. ポリシー サーバはユーザを認証し、SiteMinder セッション チケットを生成します。チケットは SiteMinder Web エージェントに返され、このチケットを含む SMSESSION Cookie が作成されます。
4. Web エージェントは CA SiteMinder® Federation Standalone へのリダイレクト レスポンスとともに SMSESSION Cookie をユーザのブラウザに渡します。
5. ユーザのブラウザが SMSESSION Cookie とともに CA SiteMinder® Federation Standalone にリダイレクトされます。
6. CA SiteMinder® Federation Standalone は SiteMinder ポリシー サーバに問い合わせ、SMESSION Cookie を検証します。
7. SMSESSION Cookie の検証が成功すると、CA SiteMinder® Federation Standalone セッションが作成されます。 CA SiteMinder® Federation Standalone はその後、依存パーティ（ターゲット リソースが存在する）への残りのフェデレーション通信を処理します。

設定ウィザードに必要な情報

設定ウィザードを実行する前に、次の情報を用意します。

データベース タイプ

ポリシー ストアに使用する予定のデータベース タイプ（SQL または Oracle）を指定します。

データベース情報

CA SiteMinder® Federation Standalone が使用するデータベースを識別します。

データベース サーバ

データベースがインストールされているサーバのホスト名または IP アドレスを指定します。データベースはデータ ストア リポジトリです。

動作環境とデータベース タイプに基づき、次を入力できます。

Windows （Oracle および SQL） ： IPv4 アドレス、IPv6 アドレス、ホスト名

UNIX （Oracle） ： IPv4 アドレス、ホスト名

UNIX （SQL） ： IPv4 アドレス、IPv6 アドレス、ホスト名

重要: このフィールドでは、IPv6 アドレスのまわりに角かっこを使用しないでください。 角かっこの省略はこの設定にのみ適用されます。 例： 3ff3:1900:4545:3:200:f8ff:fe25:67 （角かっこはありません）

SQL データベースの名前付きインスタンスを使用する場合は、動作環境に合わせて次の値を入力します。

Windows: *server_name¥named_instance*

例： server01-w3s-t1¥federation1

この例では、「server01-w3s-t1」がサーバ名で、「federation1」がインスタンス名です。

UNIX: *server_name*

SQL の名前付きインスタンスではなく、データベース サーバ名をこのフィールドに指定します。 さらに、データベース ポート フィールドに SQL の名前付きインスタンスのポート番号を入力します。

例： server01-w3s-t1

データベース名

データベース インスタンスに名前を付けます。

制限

SQL： データベース名

Oracle： CA SiteMinder® Federation Standalone がデータベース テーブルを作成し、管理するテーブルスペースに CONNECT と RESOURCE のロールを持つ Oracle ユーザの名前。

データベース ポート

データベースがリスニングするポートを識別します。 データベースがデフォルト ポートで実行されていない場合、ポート番号を変更します。 たとえば、データベース サーバに SQL の名前付きインスタンスを指定した場合、このデータベース インスタンスにポートを入力します。

デフォルト

SQL： 1433

Oracle： 1521

Database ユーザ名

スーパーの管理権限でデータベースにアクセスし、データベース テーブルを作成し、管理する管理者に名前を付けます。

ユーザ名には、スラッシュ（/）を除き、あらゆる印刷可能文字を含めることができます。 データベースへの接続が失敗するので、スラッシュは Oracle データベースに使用できません。

データベース パスワード

データベース管理者アカウントのパスワードを指定します。 パスワードには、スラッシュ（/）を除き、あらゆる印刷可能文字を含めることができます。 データベースへの接続が失敗するので、スラッシュは Oracle データベースに使用できません。

CA SiteMinder® Federation Standalone サーバ ポート

CA SiteMinder® Federation Standalone がリスニングする TCP ポート番号を指定します。

デフォルト： 44442

制限： 44443、44444、44445 以外の数値。 ポート番号 44443、44444、44445 は許可されません。

展開モード

環境で CA SiteMinder® Federation Standalone を実装する方法を決定します。

展開モード オプションは次のとおりです。

プロキシ モード

プロキシ モード展開では、CA SiteMinder® Federation Standalone はすべてのバックエンド リソースへの主要エントリ ポイントになります。

次の場合にこのモードを選択します。

- ネットワークへのアクセス ポイントを 1 つとします。
- バックエンド アプリケーションでは、パーソナライズされたユーザ操作性を提供するために、SAML アサーションからの属性を必要とします。 SAML アサーション属性はヘッダとして提供できます。

注: HTTP ヘッダ プレフィックスを設定することで、無許可のユーザによる変更から HTTP ヘッダを保護できます。 プロキシ モードでの HTTP ヘッダの保護に関しては、さらに多くの詳細があります。

スタンドアロン モード

スタンドアロン モード展開では、CA SiteMinder® Federation Standalone は SiteMinder Web エージェントまたはサードパーティ Web サーバと共に展開されます。 この場合、CA SiteMinder® Federation Standalone はフェデレーション リクエストのみを処理します。Web サーバは他のすべてのリクエストを処理します。

フェデレーション トラフィックを CA SiteMinder® Federation Standalone に制限し、通常の Web トラフィックの処理を他の Web サーバに担わせる場合にこのモードを選択します。

スタンドアロン モードでは、HTTP ヘッダを使用してアサーションからユーザ属性をパスすることはできません。応答に HTTP ヘッダを追加できません。 Web サーバとブラウザの間には、この変更を行うためのメカニズムがありません。

サーバ ホスト名（プロキシ モードのみ）

CA SiteMinder® Federation Standalone がフェデレーション リソースのリクエストを転送するバックエンド サーバの完全修飾ドメイン名を識別します。

Apache 設定

CA SiteMinder® Federation Standalone は受信リクエストの HTTP リスナとしてオープン ソース Apache Web サーバを使用します。

サーバ名

CA SiteMinder® Federation Standalone 展開の完全修飾ドメイン名を識別します。このサーバ名は、CA SiteMinder® Federation Standalone がインストールされているシステムに必ずしもマップしません。それを仮想ホストと考えることができます。

管理者の電子メール アドレス

データベース管理者の電子メール アドレスを指定します。

CA SiteMinder® Federation Standalone とともにインストールされた Apache サーバはこの設定を必要とします。 問題が発生する場合、Apache サーバはそのデフォルト エラー メッセージで管理者の電子メール アドレスを使用します。 電子メール アドレスは ServerAdmin ディレクティブにより設定され、任意の有効な電子メール アドレスになります。

注: このアドレスに転送されるイベントは、Apache サーバのサーバ固有のエラーと警告です。 メッセージはフェデレーションに関連しません。

Apache HTTP ポート

HTTP リクエストをリスニングするポートを指定します。

デフォルト： 80

注: 別の Web サーバにポート 80 を使用している場合は、Apache Web サーバのデフォルト ポートを変更します。

Apache SSL ポート

SSL リクエストをリスニングする Apache のポートを指定します。

デフォルト： 443

注: 別の Web サーバにポート 443 を使用している場合、Apache Web サーバのデフォルト SSL ポートを変更します。

管理 UI HTTP ポート

CA SiteMinder® Federation Standalone が UI HTTP リクエストをリスニングするポートを指定します。

このポートを変更する場合、それが内部用となり、インターネットからアクセスできなくする必要があることに注意してください。

デフォルト： 8888

管理 UI SSL ポート

CA SiteMinder® Federation Standalone が UI SSL リクエストをリスニングポートを指定します。

このポートを変更する場合、それが内部用となり、インターネットからアクセスできなくする必要があることに注意してください。

デフォルト： 8889

重要: ポート番号は次の設定で一意にする必要があります。

- CA SiteMinder® Federation Standalone サーバ ポート
- Apache HTTP ポート
- Apache SSL ポート
- 管理 UI HTTP ポート
- 管理 UI SSL ポート

設定実行可能ファイル

次の表は、CA SiteMinder® Federation Standalone の設定実行可能ファイルを識別したものです。 この表はプラットフォーム別に整理されています。

プラットフォーム	設定実行可能ファイル
Linux	ca-Federation-config.sh
Solaris	ca-Federation-config.sh
Windows	ca-federation-config.exe

サポートされているオペレーティング システムの詳細については、テクニカル サポート サイトで「CA SiteMinder® Federation Standalone プラットフォーム サポート マトリクス」を参照してください。

Windows での設定ウィザードの実行

設定ウィザードを実行する前に、CA SiteMinder® Federation Standalone をインストールし、設定ウィザードで要求される情報をすべて集めます。 CA SiteMinder® Federation Standalone を再インストールするときは常に設定ウィザードを実行します。

これらの手順は Windows システムで GUI およびコンソール モードで設定するための手順です。2 つのモードの手順は同じですが、コンソール モードについては以下に示す例外があります。

- オプションを選択するには、該当する数を入力します。
- 各手順の後に ENTER キーを押してプロセスを続行します。
- 「BACK」を入力すると前の手順に戻ることができます。

各モードのプロンプトにより、順を追ってプロセスをガイドします。

次の手順に従ってください:

1. 設定ウィザードを実行します。

   ウィザードの実行方法は、ローカル管理者としてログインした場合と、ネットワーク ユーザとしてログインした場合で異なります。 ネットワーク ユーザの場合、ウィザードを実行するには Administrators グループに属する必要があります。

   - **GUI モード**

     ローカル管理者： ［スタート］メニューのショートカットを選択するか、［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［CA SiteMinder® Federation Standalone 設定ウィザード］の順に選択します。

     ネットワーク ユーザ： ［スタート］メニューのショートカットを右クリックするか、［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］の順に選択し、［CA SiteMinder® Federation Standalone 設定ウィザード］を右クリックして［管理者として実行］を選択します。

   - **コンソール モード：** コマンド ウィンドウを開き、*federation_install_dir*¥install_config_info に移動し、次のコマンドを入力します。

     ca-federation-config.exe -i -console

     正しい場所からのこのコマンドを実行します。パスは自動的に設定されません。

2. ウィザードを実行する前に、集めた情報を使用して設定ウィザードのプロンプトに答えます。

3. 設定を確認し、［インストール］をクリックするか（GUI モード）、「Y」を入力して（コンソール モード）設定を実行します。

   CA SiteMinder® Federation Standalone 設定が実行されます。

   設定中に問題が発生した場合、設定ログファイル CA_SiteMinder_Federation_Standalone_Configuration.log（*federation_install_dir*¥install_config_info 内）を確認します。

4. CA SiteMinder® Federation Standalone システムを再起動します。

CA SiteMinder® Federation Standalone のインストールと設定が完了します。

重要: 設定を変更する、たとえば、展開モードを切り替えるには、設定ウィザードを再実行します。 ウィザードを再実行するとき、CA SiteMinder® Federation Standalone サービスが実行されている必要があります。 設定ウィザードはいつでも再実行できます。ただし、そのたびに既存の設定が破棄されます。 設定ウィザードを再実行する前に、既存の設定をバックアップし、SSL 接続を保持します。

UNIX システムで設定ウィザードを実行します

設定ウィザードを実行する前に、CA SiteMinder® Federation Standalone をインストールし、設定ウィザードで要求される情報をすべて集めます。 CA SiteMinder® Federation Standalone を再インストールするときは常に設定ウィザードを実行します。

重要: CA SiteMinder® Federation Standalone を再インストールする場合、設定ウィザードを再実行します。 設定ウィザードを再実行する前に、既存の設定をバックアップし、SSL とデータベースの接続を保持します。ODBC ユーザ ディレクトリを使用している場合、system_odbc.ini ファイルもバックアップします。 このファイルはディレクトリ *federation_install_dir*/siteminder/db/ にあります。

これらの手順は UNIX システムで GUI およびコンソール モードでインストールするための手順です。 2 つのモードの手順は同じですが、コンソール モードについては以下に示す例外があります。

- オプションを選択するには、該当する数を入力します。
- 各手順の後に ENTER キーを押してプロセスを続行します。
- 「BACK」を入力すると前の手順に戻ることができます。

各モードのプロンプトにより、順を追ってプロセスをガイドします。

注: CA SiteMinder® Federation Standalone を設定する予定の UNIX システムで IPv6 アドレスが使用される場合、コンソール モードでのみ設定ウィザードを実行します。 GUI モードを使用しようとすると、サードパーティ制限により、プログラムはデフォルトのコンソール モードになります。

重要: root ユーザとして設定ウィザードを実行しないでください。 root として実行しようとすると、ウィザードが終了し、エラー メッセージが表示されます。 インストールを実行したユーザと同じユーザとして設定ウィザードを実行します。

設定ウィザードを実行する方法

1. コンソール ウィンドウを開きます。
2. ディレクトリ *federation_install_dir* に移動します。
3. 環境スクリプト ca_federation_env.ksh を用意します。
4. コマンド ウィンドウ（Linux の場合は ksh ウィンドウを使用）に次のいずれかのコマンドを入力します。
   - **GUI モード：** ./ca-Federation-config.sh
   - **コンソール モード：** ./ca-Federation-config.sh -i console

   設定ウィザードが起動します。
5. ウィザードを実行する前に集めた情報を使用し、設定ウィザードのプロンプトに答えます。

6. 設定を確認し、［インストール］をクリックするか（GUI モード）、「Y」を入力して（コンソール モード）インストールします。

   CA SiteMinder® Federation Standalone が設定されます。

   設定中に問題が発生した場合、設定ログファイル CA_Federation_Manager_ConfigLog.log（*federation_install_dir*/install_config_info 内）を確認します。

   CA SiteMinder® Federation Standalone のインストールと設定が完了します。

7. 次のスクリプトを実行し、CA SiteMinder® Federation Standalone を開始します。

   federation_install_dir/fedmanager.sh start

重要: 設定を変更する、たとえば、展開モードを切り替えるには、設定ウィザードを再実行します。 ウィザードを再実行するとき、CA SiteMinder® Federation Standalone サービスが実行されている必要があります。 設定ウィザードはいつでも再実行できます。ただし、そのたびに既存の設定が破棄されます。 設定ウィザードを再実行する前に、既存の設定をバックアップし、SSL 接続を保持します。

CA SiteMinder® Federation Standalone の仮想ホスト設定

CA SiteMinder® Federation Standalone には複数の仮想ホストを定義できます。 仮想ホストを利用すれば、アサーティング パーティと依存パーティを同じシステムにインストールできるので、仮想ホストはテスト目的に役立ちます。 複数の仮想ホストを定義することで、個別のホスト名とドメインを検索サービスに利用し、SAML 2.0 IdP Discovery プロファイルを設定することもできます。

複数の仮想ホストを定義するには、CA SiteMinder® Federation Standalone で次のように設定します。

- server.conf ファイルのホスト名パラメータにホストを追加します。server.conf ファイルは次のディレクトリにあります。

  federation_install_dir¥secure-proxy¥proxy-engine¥conf.

- CA SiteMinder® Federation Standalone UI にアクセスする起点となるシステム、またはフェデレーション トランザクションを実行するシステムと同じシステムで CA SiteMinder® Federation Standalone が作動している場合は、httpd.conf ファイルを更新します。 httpd.conf ファイルはディレクトリ *federation_install_dir*¥secure-proxy¥httpd¥conf にあります。

  注: SSL が埋め込み Web サーバで有効になっている場合、httpd-ssl.conf ファイルで次の変更も行います。 httpd-ssl ファイルはディレクトリ *federation_install_dir*¥secure-proxy¥httpd¥conf¥extra にあります。

  利用しているシステム タイプに基づき、httpd.conf ファイルを次のように更新します。

  - IPV4 ベースのシステムの場合、LISTEN ディレクティブを次のように追加します。

    LISTEN 127.0.0.1:*port*

  - IPv4 と IPv6 がサポートされているたデュアル スタック システムの場合、LISTEN ディレクティブを次のように追加します。

    LISTEN 127.0.0.1:*port*

    LISTEN [::1]:*port*

  - IPv6 システムの場合、LISTEN ディレクティブを次のように追加します。

    LISTEN [::1]:*port*

  さらに、システムの hosts ファイルで、ループバック アドレス エントリを更新し、新しいホスト名がそのエントリに追加されるようにします。 値は次のようになります。

  - IPv4: 127.0.0.1
  - IPv6: [::1]

無人 CA SiteMinder® Federation Standalone インストール

CA SiteMinder® Federation Standalone をインストールする方法の 1 つは無人インストールです。 無人インストールでは、ユーザの介在なしで製品をインストールできます。

無人インストールを実行するには、有人インストールを最初に実行する必要があります。手動インストールでは、「*ca-federation-installer.properties*」という名前のファイルが作成されます。それにはパラメータ、パス、および手動インストール中に入力されたパスワードがすべて含まれています。無人インストールを実行するとき、このプロパティ ファイルが通常手動で入力する設定を提供します。

デフォルト プロパティ ファイルを使用して初回インストールと同じ設定でインストールを実行するか、そのファイルをテンプレートとして使用し、環境に合わせて変更します。 プロパティ ファイルを変更するときは注意が必要です。そのコンテンツは大文字と小文字を区別します。

重要: 最初に CA SiteMinder® Federation Standalone をインストールしたシステムと同じプラットフォームのシステムでのみ無人インストールを実行できます。たとえば、Solaris システムに製品をインストールし、その後、そのプロパティ ファイルを使用して Windows システムで無人インストールを実行することはできません。

インストール プロパティ ファイルの設定

ca-federation-installer.properties ファイルを使用し、ネットワーク内のその他のシステムにインストール セットアップを伝達します。

重要: プロパティ ファイルを生成するには、最初に有人インストールを実行する必要があります。

このプロパティ ファイルを利用し、次を実行します。

- ファイルのインストール パラメータを定義します。
- ネットワーク内のシステムで、CA SiteMinder® Federation Standalone をインストールするシステムにプロパティ ファイルとインストール実行可能ファイルをコピーします。

ca-federation-installer.properties ファイルが次の場所に作成されます。

Windows： *federation_install_dir*¥install-config-info

UNIX： *federation_install_dir*/install-config-info

ファイルのデフォルト パラメータとパスは、初回インストール中に入力された情報を反映します。

インストール プロパティ ファイルを変更する方法

1. ca-federation-installer.properties ファイルを開き、ファイルのパラメータを変更します。

   注: プロパティ ファイルは大文字と小文字を区別します。

2. ファイルを保存します。

パラメータは以下のとおりです。

パラメータ	定義
DEFAULT_PRODUCT_INSTALL_TYPE	インストールの種類（新規インストール、アップグレード、再インストール）を定義します。 **デフォルト：** INSTALL
DEFAULT_INSTALL_DIR	デフォルト（Windows）：C:¥¥Program Files¥¥CA¥¥FederationManager （ダブル バック スラッシュに注意してください。） デフォルト（UNIX）：システムのアカウント 例：/home/myacct/CA/FederationManager
サーバ固有のエントリ	
DEFAULT_JRE_ROOT	<JRE> の場所を示します。
JDK_ROOT	<JDK> の場所を示します。

パラメータ	定義
#FEDADMIN_PW	CA SiteMinder® Federation Standalone のパスワードを定義します。これはコメントを外す必要があります。パスワードはクリア テキストで提供する必要があります。 セキュリティを強化するには、ENCRYPTED_FEDADMIN_PASSWORD 設定を使用します。 **注**: CA SiteMinder® Federation Standalone 管理者パスワードには英語（ASCII）文字のみを含めることができます。
ENCRYPTED_FEDADMIN_PASSWORD	CA SiteMinder® Federation Standalone パスワードは暗号化された形式で表示されます。セキュリティを強化するために、この暗号化されたパスワードを使用することをお勧めします。 すべてのシステムで同じ管理者パスワードを使用する場合、このパスワードを所定の場所に残し、FEDADMIN_PW プロパティのコメントを外しません。
FIPS モード設定	
FED_FIPS_VALUE	FIPS 140-2 操作モードを指定します。 **制限：** ■ ONLY ■ COMPAT
LGPL ライセンス設定	
ACCEPT_LGPL_EULA	LGPL ライセンスを受諾するかどうかを示します。 ディレクトリ *federation_install_dir*/install_config_info でライセンス（httpclient-EULA.txt）を確認します ライセンスを受諾するには、この変数を「YES」に設定します。 **デフォルト：** NO

無人 CA SiteMinder® Federation Standalone インストールの実行

無人インストールを実行し、ユーザの介在なしで CA SiteMinder® Federation Standalone をインストールできます。

注: 無人インストールを実行する前に、手動インストールを実行し、ca-Federation-installer.properties ファイルを作成します。このファイルは別のシステムで無人インストールを実行するために必要です。 インストールに合わせてこのファイルを変更できます。

次の手順に従ってください:

1. CA SiteMinder® Federation Standalone がすでにインストールされているシステムから、一時ロケーションに次の 2 つのファイルをコピーします。
   - インストール実行可能ファイルまたはバイナリ
   - ca-Federation-installer.properties ファイル
2. インストールおよびプロパティのファイルをコピーした場所から次のコマンドを実行します。

   installation_executable -f ca-federation-installer.properties -i silent

インストールは無人モードで開始し、プロパティ ファイルのパラメータを使用して CA SiteMinder® Federation Standalone をインストールします。

注: Windows の無人インストールを確認するには、インストール ログ ファイル CA_Federation_Standalone_Install_date_time.log（ディレクトリ *federation_install_dir*¥install_config_info 内）を参照します。

無人 CA SiteMinder® Federation Standalone 設定

CA SiteMinder® Federation Standalone を設定する方法の 1 つは無人設定です。 無人設定では、ユーザの介在なしで CA SiteMinder® Federation Standalone を設定できます。

無人設定を実行するには、最初にマシンで CA SiteMinder® Federation Standalone を手動で設定する必要があります。 手動設定で *ca-federation-config.properties* という名前のファイルが作成されます。これを利用して個々のマシンで無人設定を実行します。 デフォルトでは、ca-federation-config.properties には初回設定からの設定が含まれます。

ca-federation-config.properties ファイルにはパラメータ、パス、および初回設定中に入力されたパスワードがすべて含まれます。 ユーザが無人設定を実行すると、このプロパティ ファイルが通常は手動で入力する設定を提供します。

デフォルト プロパティ ファイルを使用して初回設定と同じ設定で設定を実行するか、そのファイルをテンプレートとして使用し、環境に合わせて変更します。

あるネットワークの複数のシステムでプロパティ ファイルを使用する場合、APACHE_SERVER_NAME 設定を無人設定を実行する各システムで一意の値に設定します。 複数のシステムでサーバ名が同じ場合、競合を引き起こす可能性があります。

重要: 最初に CA SiteMinder® Federation Standalone をインストールしたシステムと同じプラットフォームのシステムでのみ無人設定を実行できます。 たとえば、Solaris システムで製品を設定し、その後、そのプロパティ ファイルを使用して Linux システムで無人設定を実行することはできません。

設定プロパティ ファイルの設定

無人設定では ca-federation-config.properties ファイルを使用し、ネットワークの別のシステムに CA SiteMinder® Federation Standalone 設定を伝達します。

このプロパティ ファイルを利用し、次を実行します。

- ファイルの設定パラメータを定義します。
- ネットワーク内のシステムで、CA SiteMinder® Federation Standalone を設定するシステムにプロパティ ファイルと設定実行可能ファイルをコピーします。

ca-federation-config.properties ファイルは次の場所にインストールされます。

Windows： *federation_install_dir*¥install-config-info

UNIX： *federation_install_dir*/install-config-info

ファイルのデフォルト パラメータとパスは、初回設定中に入力された情報を反映します。

重要: 設定プロパティ ファイルは大文字と小文字を区別します。

設定プロパティ ファイルを変更する方法

1. ca-federation-config.properties ファイルを開き、ファイルのパラメータを変更します。
2. ファイルを保存します。

パラメータは以下のとおりです。

パラメータ	説明
データベース情報	
PARAM_DBTYPE	データベースのタイプ（SQL または Oracle）を示します。
PARAM_UID	データベース管理者ユーザ名を表示します。
#PARAM_PWD	クリア テキストで、UI へのログインに使用される CA SiteMinder® Federation Standalone 管理者パスワードを識別します。 値を入力する前にこの行のコメントを外します。 セキュリティを強化するには、ENCRYPTED_PARAM_PWD 設定を使用します。
ENCRYPTED_PARAM_PWD	暗号化された CA SiteMinder® Federation Standalone 管理者パスワードを指定します。 セキュリティを強化するために、この暗号化されたパスワードを使用することをお勧めします。
PARAM_DB_SERVER	データベース サーバの IP アドレスを識別します。

パラメータ	説明
PARAM_DB_PORT	データベースがリスニングするポートを表示します。 **デフォルト設定：** ■ SQL： 1433 ■ Oracle： 1521
MSSQL 固有	
PARAM_DB	MS-SQL 固有パラメータ。 SQL データベースに名前を付けます。
Oracle 固有	
ORACLE_SID	Oracle 固有パラメータ。 Oracle データベースの**サービス名**（SID ではありません）を指定します。
RECONFIGURE	CA SiteMinder® Federation Standalone が既存のデータベーススキーマを使用するか、新しいスキーマを作成するかを示します。 **制限：** 真（既存のスキーマを使用する）、偽（新しいスキーマを作成する）
サーバ ポート	
PARAM_PORT	CA SiteMinder® Federation Standalone がリスニングするポートを定義します。 **デフォルト：** 44442 **重要**: このポートに値 44445 を割り当てないでください。
展開モード	
DEPLOYMENT_MODE	CA SiteMinder® Federation Standalone 展開モードを指定します。 **制限：** ■ プロキシ（大文字 P） ■ スタンドアロン（大文字 S）

パラメータ	説明
PROXY_HOST_NAME	（プロキシ モードのみ） CA SiteMinder® Federation Standalone がフェデレーション リソースのリクエストを転送するバックエンド サーバの完全修飾ドメイン名を識別します。 構文 *server_name.domain:port* を使用してこの設定を定義します。 例： myserver.mycompany.ca.com： 5555 複数の CA SiteMinder® Federation Standalone システムでこのプロパティ ファイルを使用し、これらのシステムが同じプロキシを使用する場合は、このホスト名を各システムで同じ値に設定します。 CA SiteMinder® Federation Standalone とプロキシ ホストは同じドメインにある必要があります。
Apache サーバ情報	
APACHE_SERVER_NAME	Apache Web サーバの名前を指定します。 あるネットワークの複数のシステムでプロパティ ファイルを使用する場合、この値を無人設定を実行する各システムで一意の名前に設定します。 複数のシステムでサーバ名が同じ場合、競合を引き起こす可能性があります。
APACHE_ADMIN_EMAIL	CA SiteMinder® Federation Standalone 管理者の電子メール アドレスを示します。 この設定は、CA SiteMinder® Federation Standalone の一部としてインストールされた Apache サーバで必要になります。 問題が発生する場合、Apache はそのデフォルト エラー メッセージで管理者の電子メール アドレスを使用します。 電子メール アドレスは ServerAdmin ディレクティブにより設定され、任意の有効な電子メール アドレスになります。 このアドレスに転送されるイベントは、Apache サーバのサーバ固有のエラーと警告です。 メッセージはフェデレーションに関連しません。 **デフォルト：** admin@mycompany.com
APACHE_HTTP_PORT	Apache Web サーバがリスニングするデフォルト ポートを指定します。 **デフォルト：** 80
APACHE_SSL_PORT	Apache Web サーバがリスニングするデフォルト SSL ポートを指定します。 **デフォルト：** 443

パラメータ	説明
UI_HTTP_PORT	Administrative UI がリスニングするデフォルト HTTP ポートを指定します。 **デフォルト：** 8888
UI_SSL_PORT	Administrative UI がリスニングするデフォルト SSL ポートを指定します。 **デフォルト：** 8889

重要: ポート番号は次の設定で一意にする必要があります。

- CA SiteMinder® Federation Standalone サーバ ポート
- Apache HTTP ポート
- Apache SSL ポート
- 管理 UI HTTP ポート
- 管理 UI SSL ポート

無人設定の実行

ユーザの操作なしで CA SiteMinder® Federation Standalone を設定できます。

注: 先にシステムを手動で設定し、ca-Federation-config.properties ファイルを作成しておく必要があります。 このファイルは、ネットワークに合わせて変更できます。

次の手順に従ってください:

1. CA SiteMinder® Federation Standalone がすでにインストールされているシステムから、一時ロケーションに次の 2 つのファイルをコピーします。
   - 設定実行可能ファイルまたはバイナリ (P. 45)
   - ca-Federation-config.properties

2. インストールおよびプロパティのファイルをコピーした場所から次のコマンドを実行します。

   configuration_executable -f ca-federation-config.properties -i silent

   プロパティ ファイルのパラメータを設定に使用し、設定が無人モードで開始します。

3. Windows の場合、設定の完了後にシステムを再起動します。

   注: Windows の無人インストールを確認するには、インストール ログ ファイル CA_Federation_Standalone_Install_date_time.log (ディレクトリ *federation_install_dir*¥install_config_info 内) を参照します。

Administrative UI へのログイン

Administrative UI でフェデレーション システムを設定できます。

重要: Administrative UI に一度にログオンできるのは 1 人の管理者のみです。 また、管理者は 1 つのブラウザ インスタンスのみを開くことができます。

次の手順に従ってください:

1. ブラウザで Java Script が有効になっていることを確認します。これは、Administrative UI を開くために必須です。
2. 使用するプラットフォームの手順に従います。

   Windows

   ［スタート］-［すべてのプログラム］-［CA］-［Federation Standalone］-［Federation Standalone 管理 UI］を選択します。

   UNIX

   Web ブラウザを開き、次の URL を入力します：
   http://*fed_server:ui_port*/ca/federation/adminui

   fed_server:ui_port

   CA SiteMinder® Federation Standalone がインストールされているサーバの完全修飾ドメイン名（Administrative UI 用ポートを含む）を指定します。 デフォルトのポートは 8888 です。

   例：

   http://fed1.ca.com:8888/ca/federation/adminui

   ログイン ウィンドウが表示されます。
3. ユーザ名とパスワードを入力し、［サイン イン］をクリックします。

   重要: ユーザ名は常に「**admin**」です。 これは変更できません。 管理者パスワードはインストール中に設定されます。

Administrative UI が起動します。

第 2 章: CA SiteMinder® Federation Standalone をアンインストールします

Windows からのフェデレーション システムのアンインストール

不要になった場合は、システムから CA SiteMinder® Federation Standalone をアンインストールします。

次の手順に従ってください:

1. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［CA SiteMinder® Federation Standalone のアンインストール］を選択します。

   アンインストール ウィザードが実行されます。
2. ウィザードの指示に従います。
3. アンインストールが完了したら、*federation_install_dir* に移動し、必要に応じて、Federation Manager フォルダとそのすべてのサブフォルダを削除します。
4. システムを再起動します。

本製品がアンインストールされます。

UNIX システムから CA SiteMinder® Federation Standalone をアンインストールする

不要になった場合は、システムから CA SiteMinder® Federation Standalone をアンインストールします。

次の手順に従ってください:

1. コマンド ウィンドウを開きます。
2. ディレクトリ *federation_install_dir* に移動します。
3. 環境スクリプト ca_federation_env.ksh を用意します。
4. 次のコマンドを入力し、アンインストール スクリプトを実行します。

   ./ca-Federation-uninstall.sh
5. 必要に応じて、ディレクトリ *federation_install_dir* に移動し、CA SiteMinder® Federation Standalone フォルダとすべてのサブフォルダを削除します。

本製品がアンインストールされます。

第 3 章: 12.x システムを CA SiteMinder® Federation Standalone r12.52 SP1 にアップグレードします

このセクションには、以下のトピックが含まれています。

CA SiteMinder® Federation Standalone のアップグレードと移行のパス

アップグレードとは、既存の 12.x バージョンを実行するシステムで CA SiteMinder® Federation Standalone の新しいバージョンに更新することです。アップグレードを行うには、既存のシステムで、新しいバージョンの本製品をサポートするオペレーティング システム、データベース、JDK を実行している必要があります。

移行とは、新しい r12.52 SP1 インストールをするシステムに既存のシステムの設定を複製することです。 新しいフェデレーション システムは、サポートされるデータベース バージョンと通信する必要があります。

注:

- r12.52 SP1 環境に移行するとき、サポートされるデータベースを追加する必要があります。 環境において、r12.52 SP1 によってサポートされないデータベースを使用している場合、サポートされるデータベース サーバをインストールし、新しいデータベースにデータを移します。 最後に、r12.52 SP1 に移行します。
- r12.52 SP1 にアップグレードするとき、Windows 認証のフェデレーション エージェントがインストールされている場合、エージェントをフェデレーション システムと同じバージョンにアップグレードします。 アップグレードしないと、エージェントは正しく動作しません。

特定のバージョンに関する詳細については、**エラー! ハイパーリンクの参照に誤りがあります。** サイトのプラットフォーム サポート マトリックスを参照してください。

これらの利用可能なパスに基づき、r12.52 SP1 にアップグレードまたは移行できます。

Windows

既存のフェデレーション バージョン	データベースは r12.52 SP1 で動作しますか	アップグレードまたは移行
すべての SP を含む r12.0	いいえ	r12.52 SP1 に移行します
すべての SP を含む r12.1	いいえ	r12.52 SP1 に移行します
r12.1 SP3	はい	r12.52 SP1 にアップグレードします

Solaris/Linux

既存のフェデレーション バージョン	データベースは r12.52 SP1 で動作しますか	アップグレードまたは移行
すべての SP を含む r12.0	いいえ	r12.52 SP1 に移行します
すべての SP を含む r12.1	いいえ	r12.52 SP1 に移行します
r12.1 SP3	はい	r12.52 SP1 にアップグレードします

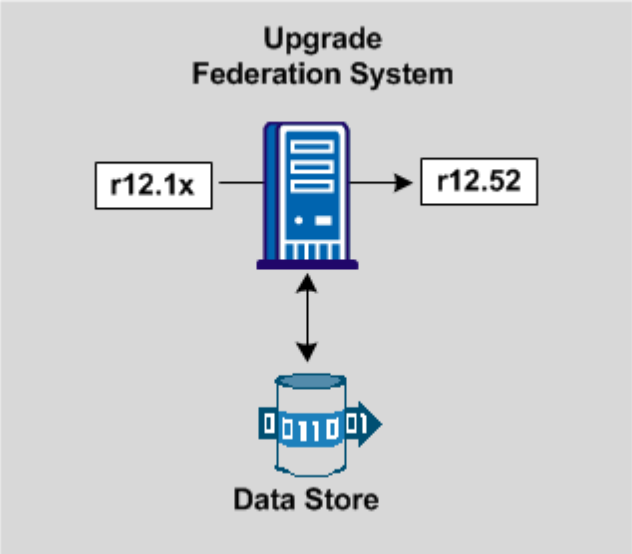
FIPS 移行

CA SiteMinder® Federation Standalone は非 FIPS から FIPS のみの環境への移行をサポートします。ただし、移行プロセスは複雑です。非 FIPS から FIPS のみの環境に移行する場合、最初に r12.52 SP1 へのアップグレードを完了します。 アップグレードに成功したら、FIPS 移行プロセスに従います。

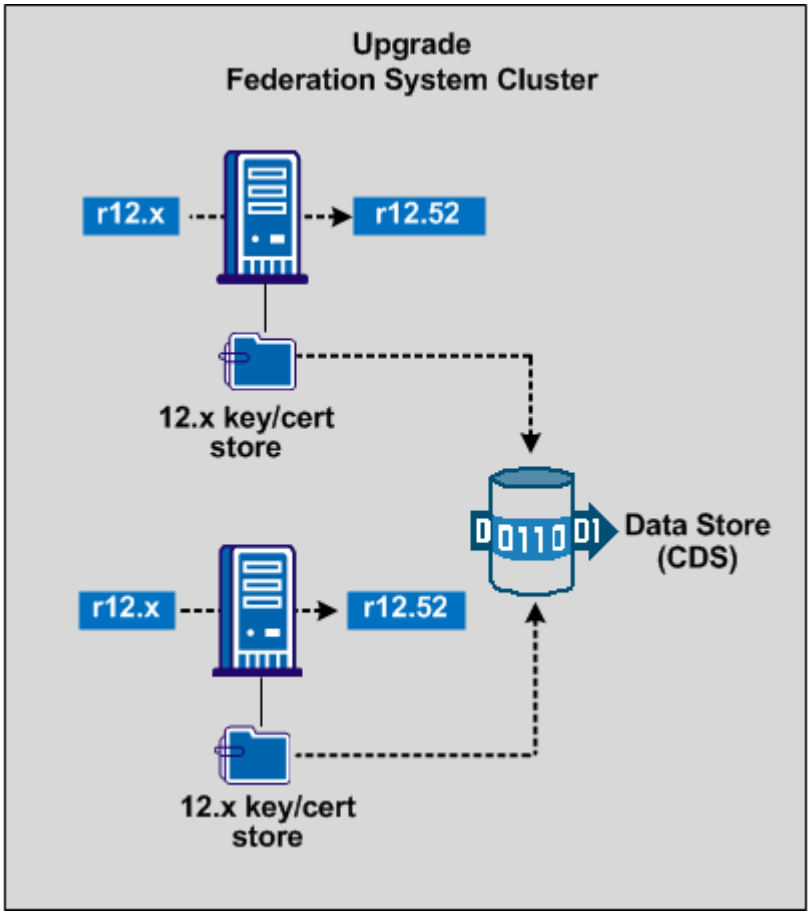
CA SiteMinder® Federation Standalone r12.52 SP1 にアップグレードする方法

Windows と UNIX （Solaris と Linux）システムで CA SiteMinder® Federation Standalone を r12.52 SP1 にアップグレードできます。 既存のシステムで、r12.52 SP1 をサポートするオペレーティング プラットフォームとデータベースを実行している必要があります。

次の図は、単一のシステムのアップグレード パスを示したものです。



次の図は、クラスタ化された環境のアップグレードを示したものです。



CA SiteMinder® Federation Standalone クラスタをセットアップし、フェールオーバをサポートできます。 既存の r12.x クラスタから新しいクラスタにアップグレードするには、非クラスタ アップグレードと同様の手順に従います。 現在のオペレーティング プラットフォームが r12.52 SP1 をサポートすると仮定する場合、既存のクラスタの各システムを r12.52 SP1 にアップグレードします。

クラスタ内のシステムは 1 つのデータ ストアを共有します。 アップグレードを検出する、r12.52 SP1 インストール プログラムを実行すると、キーと証明書の情報が証明書データ ストア（CDS）に自動的に移動されます。 CDS はメイン データ ストアと連結されます。

アップグレードのプロセスは次のようになります。

1. 複数のキー データベースを同期します（クラスタをアップグレードしている場合に限り）。
2. パートナーシップに一意のバックチャネル ユーザ名があることを確認します。
3. データ ストアとキー ストアを含む、既存の設定をバックアップします。
4. インストール プログラムを実行し、r12.52 SP1 にアップグレードします。 このインストールではアップグレードを検出できます。

各手順の詳細は以下のセクションにあります。

キー データベースの同期

12.5 以前のシステムでは、smkeydatabase と呼ばれるキー ストアに秘密鍵および証明書のデータが格納されました。このデータは、証明書データ ストアに格納されるようになりました。このデータ ストアは従来のデータ ストアと併存します。 証明書データ ストアは、環境の各フェデレーション システムがローカル smkeydatabase にアクセスするという要件に取って代わります。

アップグレードの一部として、インストーラは自動的にローカル smkeydatabase をバックアップし、証明書データ ストアにコンテンツをすべて移行しようとします。 このプロセスでは、移行を開始する前に smkeydatabase と CDS が比較されます。 比較の目的は、データの不整合を特定することです。たとえは、複数の証明書に同じエイリアスがマッピングされている場合、移行が失敗する可能性があります。

クラスタ環境で、smkeydatabase の複数のインスタンスがあります。r12.52 SP1 にアップグレードまたは移行する前に、smkeydatabase インスタンスをすべて同期し、情報を整合します。 データベースを同期することで、各インスタンスを CDS に移行しても不整合が発生しません。

Administrative UI の［証明書およびキー］タブからの smkeydatabase インスタンスにあるあらゆるデータ不整合を解決します。 次のデータがキー データベース インスタンス全体で一貫していることを確認します。

- 各 CA 証明書は、インスタンス全体で、証明書破棄リストを一貫して参照する必要があります。
- **例：** CA 証明書は、LDAP ディレクトリ サービス内の証明書破棄リストを一貫して参照します。
- defaultentpriseprivatekey エイリアスは、すべてのインスタンスで、同じ秘密鍵/証明書のペアを表します。
- 同じエイリアスは、同じ証明書またはキー/証明書のペアにマップされます。
- 同じ CA 証明書は、同じ証明書破棄リストにマップされます。
- 破棄された、または有効期限が切れた証明書は存在しません。
- すべての CRL 情報が有効です。

重要: データの不整合をすべて解決したら、移行がすべて完了するまで smkeydatabase インスタンスを変更しないでください。

既存のパートナーシップに一意のバックチャネル ユーザ名があることを確認する

HTTP-Artifact シングル サインオン トランザクション中に、アサーティング パーティは保護されたバック チャネルを介して依存パーティにアサーションを返します。 バック チャネルへのアクセスを認証するためにエンティティを要求できます。 バック チャネル用の認証方式として基本認証を選択している場合は、ユーザ名が必要です。

アップグレードする前に、同じ SAML プロファイル内のフェデレーション パートナーシップが、それぞれ一意のユーザ名を受信バック チャネルに使用していることを確認します。 複数の SAML 2.0 または SAML 1.x パートナーシップでは、受信バック チャネル ユーザ名を共有できません。

注: SAML 1.x と SAML 2.0 のパートナーシップでは受信バック チャネル ユーザ名を共有できますが、推奨されません。

受信バック チャネル ユーザ名を共有する同じプロトコルのパートナーシップがある場合は、アップグレードする前に以下の手順に従います。

1. パートナーシップの 1 つを非アクティブにします。
2. そのパートナーシップで定義されているバック チャネル ユーザ名を変更します。
3. リモート パートナーに変更を伝えます。

パートナーシップを再度アクティブ化します。

既存の設定のバックアップ

設定とキー データベースをバックアップしておくと、システムの復旧または移行に役立ちます。

設定をバックアップするには、キー データベースをコピーし、設定データをエクスポートします。 製品に付属する XPSExport ツールを使用して、設定データを XML ファイルにエクスポートできます。

重要: フェデレーション トランザクションはエクスポート プロセス中は続行できません。

設定をバックアップする方法

1. キー データベースをコピーし、安全な場所に保存します。 キー データベースは次のディレクトリにあります。

   federation_install_dir/siteminder/smkeydatabase

2. コマンド ウィンドウから次のコマンドを入力し、CA SiteMinder® Federation Standalone 設定をエクスポートします。

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   エクスポートの結果の出力ファイルに名前を付けます。 XPSExport からの出力は、XML 形式であるため、ファイル名は拡張子 **.xml** で終わる必要があります。

   passphrase

   機密データを暗号化するのに必要なパスフレーズを指定します。 パスフレーズは、8 文字以上で、1 つ以上の数字、1 つ以上の大文字、および 1 つ以上の小文字を含んでいる必要があります。 パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。

   注: パスフレーズを直接入力しない場合、コマンドからそれを省くことができます。 そうすると、XPSExport はパスフレーズの入力およびパスフレーズの確認を求め、画面に表示されません。

これでキー データベースのコピーと、暗号化された設定データを含む XML ファイルが用意できました。

Windows での CA SiteMinder® Federation Standalone r12.52 SP1 のアップグレード

CA SiteMinder® Federation Standalone をサポートするオペレーティング プラットフォームを実行する Windows システムで、同じオペレーティング プラットフォームで CA SiteMinder® Federation Standalone r12.52 SP1 に直接アップグレードできます。

r12.52 SP1 でサポートされていないオペレーティング システムで既存のシステムを実行している場合は、設定を移行 (P. 79)します。直接アップグレードすることはできません。

注: アップグレード前にパートナーシップを非アクティブ化する必要はありません。

r12.52 SP1 CA SiteMinder® Federation Standalone インストーラ実行可能ファイルを実行し、アップグレードします。このアップグレードでは、前の CA SiteMinder® Federation Standalone 設定が保持されます。

重要: 次のインストール制限に注意してください。

- ポリシー サーバまたは Secure Proxy Server （SPS）がすでにインストールされているシステムに CA SiteMinder® Federation Standalone をインストールしないでください。 これらのその他のコンポーネントを備えたシステムに CA SiteMinder® Federation Standalone をインストールすると、既存の SiteMinder インストールにマイナスの影響を与える可能性があります。
- Apache Web サーバまたは Apache Tomcat サーバがすでに配置されているシステムに本製品をインストールしないでください。

インストーラが smkeydatabase ファイルを検出した場合、インストーラは次の手順を実行します。

- smkeydatabase をバックアップする。
- 証明書データ ストアへのコンテンツの移行を試行する。

重要: smkeydatabase 移行が失敗した場合、システムを元の環境に戻さないでください。証明書データを必要とするすべてのトランザクションが失敗するためです。

インストール キットを見つける方法

1. CA テクニカル サポート サイトにログオンします。
2. ［Download Center］をクリックします。
3. ダウンロード センターで必要なインストール キットを検索します。

Windows で CA SiteMinder® Federation Standalone をアップグレードする方法

1. 実行中のすべてのアプリケーションを終了します。
2. インストール プログラムの実行を予定しているフォルダに移動します。
3. インストール実行可能ファイルをフォルダにコピーします。

   注: インストール実行可能ファイルのリストを表示します。

4. *installation_executable* をダブルクリックします。

   インストール ウィザードが起動されます。

5. インストールを進めます。
6. インストール設定を確認し、［インストール］をクリックします。
7. インストール プログラムが実行され、システムがアップグレードされます。

   システムの再起動を求められたら再起動します。

8. AssertionGeneratorFramework.properties ファイルの名前を変更し、アップグレードによって作成された新しいファイルが使用されるようにします。

   a. *federation_install_dir*¥siteminder¥config¥properties に移動します。

   b. 既存の AssertionGeneratorFramework.properties ファイルが保持されるように名前を変更します（例：AssertionGeneratorFramework.properties.old）。

   c. AssertionGeneratorFramework.properties.new ファイル（アップグレードによって作成）から .new 拡張子を削除します。

9. アップグレードが完了したら、正しいファイルがロードされるように、ブラウザですべての一時ファイルを消去します。

注: SiteMinder コネクタが有効な環境からアップグレードする場合、コネクタを使用するパートナーシップは何も変更しなくても引き続き動作します。 アップグレードの完了後、パートナーシップごとにコネクタを有効または無効にできます。 アップグレードの前にコネクタが有効ではなかった場合は、コネクタを有効にして、特定のパートナーシップで使用するように設定します。

アップグレード エラーが発生した場合の措置

データベース アップグレードに失敗した場合、CA SiteMinder® Federation Standalone はエラー メッセージを表示し、policy_store_upgrade スクリプトを実行するように通知します。 アップグレード スクリプト（policy_store_upgrade.bat）は *federation_install_dir*/install_config_info にあります。

インストール中に他の問題が発生した場合は、インストール ログ ファイル CA_Federation_Standalone_Install_*date_time*.log とアップグレード ログ ファイル CA_Federation_policy_store_upgrade.log を確認します。 いずれのファイルもディレクトリ *federation_install_dir*/install_config_info にあります。

UNIX での CA SiteMinder® Federation Standalone r12.52 SP1 のアップグレード

UNIX システムで、同じオペレーティング プラットフォームと同じデータベースで CA SiteMinder® Federation Standalone r12.52 SP1 に直接アップグレードできます。

r12.52 SP1 でサポートされていないオペレーティング システムで既存のシステムを実行している場合は、設定を移行 (P. 79)します。直接アップグレードすることはできません。

r12.52 SP1 CA SiteMinder® Federation Standalone インストーラを実行します。このアップグレードでは、前の設定が保持されます。

インストーラが smkeydatabase ファイルを検出した場合、インストーラは次の手順を実行します。

- smkeydatabase をバックアップする。
- 証明書データ ストアへのコンテンツの移行を試行する。

重要: smkeydatabase 移行が失敗した場合、システムを元の環境に戻さないでください。証明書データを必要とするすべてのトランザクションが失敗するためです。

これらの手順は UNIX システムで GUI およびコンソール モードでインストールするための手順です。 2 つのモードの手順は同じですが、コンソール モードについては以下に示す例外があります。

- 対応する数を入力してオプションを選択するように指示される場合があります。
- 各手順の後に ENTER キーを押してプロセスを続行します。
- 各モードのプロンプトにより、順を追ってプロセスをガイドします。
- 「BACK」を入力すると前の手順に戻ることができます。

重要: 次のインストール制限に注意してください。

- ポリシー サーバまたは Secure Proxy Server （SPS）がすでにインストールされているシステムに CA SiteMinder® Federation Standalone をインストールしないでください。 これらのその他のコンポーネントを備えたシステムに CA SiteMinder® Federation Standalone をインストールすると、既存の SiteMinder インストールにマイナスの影響を与える可能性があります。
- Apache Web サーバまたは Apache Tomcat サーバがすでに配置されているシステムに本製品をインストールしないでください。

r12.52 SP1 CA SiteMinder® Federation Standalone インストーラを実行し、CA SiteMinder® Federation Standalone をアップグレードします。 プラットフォームに合わせてインストーラを選択します。

サポート サイトでインストール キットを見つける方法

1. CA テクニカル サポート サイトにログオンします。
2. ［Download Center］をクリックします。
3. ダウンロード センターで必要なインストール キットを検索します。

CA SiteMinder® Federation Standalone をアップグレードする方法

重要: root ユーザとしてアップグレードを実行しないでください。 root としてインストールを試行すると、インストールは失敗し、エラー メッセージが表示されます。 代わりに、CA SiteMinder® Federation Standalone をインストールするための新しいユーザ アカウントを作成します。

1. 実行中のすべてのアプリケーションを終了します。

   注: アップグレード前にパートナーシップを非アクティブ化する必要はありません。

2. 必要に応じて、たとえば、chmod コマンドを実行し、インストール ファイルに実行権限を追加します。

   chmod +x *ca-fed-executable*-sol.bin

3. インストール プログラムの実行を予定しているフォルダに移動します。

4. フォルダにインストール バイナリをコピーします。

5. コマンド ウィンドウに次のいずれかのコマンドを入力します。

   - **GUI モード：** ./*installation_binary*
   - **コンソール モード：** ./*installation_binary* -i console

   例（GUI モード）： ./*ca-fed-executable*-sol.bin

   インストール ウィザードが起動されます。

6. インストールを進めます。

7. インストール設定を確認し、［インストール］をクリックするか（GUI モード）、「Y」を入力して（コンソール モード）インストールします。

   CA SiteMinder® Federation Standalone インストール プログラムが実行され、サービスが再起動します。

8. AssertionGeneratorFramework.properties ファイルの名前を変更し、アップグレードによって作成された新しいファイルが使用されるようにします。
   a. *federation_install_dir*¥siteminder¥config¥properties に移動します。
   b. 既存の AssertionGeneratorFramework.properties ファイルが保持されるように名前を変更します（例：AssertionGeneratorFramework.properties.old）。
   c. AssertionGeneratorFramework.properties.new ファイル（アップグレードによって作成）から .new 拡張子を削除します。
9. アップグレードが完了したら、正しい CA SiteMinder® Federation Standalone ファイルがロードされるように、ブラウザの一時ファイルをすべてクリアします。

注: SiteMinder コネクタが有効な環境からアップグレードする場合、コネクタを使用するパートナーシップは何も変更しなくても引き続き動作します。 アップグレードの完了後、パートナーシップごとにコネクタを有効または無効にできます。 アップグレードの前にコネクタが有効ではなかった場合は、コネクタを有効にして、特定のパートナーシップで使用するように設定します。

アップグレード エラーが発生した場合の措置

データベース アップグレードに失敗した場合、CA SiteMinder® Federation Standalone はメッセージを表示し、policy_store_upgrade スクリプトを実行するように通知します。 アップグレード スクリプト（policy_store_upgrade.sh）は *federation_install_dir*/install_config_info にあります。

インストール中に他の問題が発生した場合は、インストール ログ ファイル CA_Federation_Standalone_Install_*date_time*.log とアップグレード ログ ファイル CA_Federation_policy_store_upgrade.log を確認します。 いずれのファイルもディレクトリ *federation_install_dir*/install_config_info にあります。

重要: smkeydatabase 移行が失敗した場合、システムを元の環境に戻さないでください。証明書データを必要とするすべてのトランザクションが失敗するためです。

第 4 章: CA SiteMinder® Federation Standalone r12.52 SP1 への移行

このセクションには、以下のトピックが含まれています。

CA SiteMinder® Federation Standalone のアップグレードと移行のパス

アップグレードとは、既存の 12.x バージョンを実行するシステムで CA SiteMinder® Federation Standalone の新しいバージョンに更新することです。アップグレードを行うには、既存のシステムで、新しいバージョンの本製品をサポートするオペレーティング システム、データベース、JDK を実行している必要があります。

移行とは、新しい r12.52 SP1 インストールをするシステムに既存のシステムの設定を複製することです。 新しいフェデレーション システムは、サポートされるデータベース バージョンと通信する必要があります。

注:

- r12.52 SP1 環境に移行するとき、サポートされるデータベースを追加する必要があります。 環境において、r12.52 SP1 によってサポートされないデータベースを使用している場合、サポートされるデータベース サーバをインストールし、新しいデータベースにデータを移します。 最後に、r12.52 SP1 に移行します。
- r12.52 SP1 にアップグレードするとき、Windows 認証のフェデレーション エージェントがインストールされている場合、エージェントをフェデレーション システムと同じバージョンにアップグレードします。 アップグレードしないと、エージェントは正しく動作しません。

特定のバージョンに関する詳細については、**エラー! ハイパーリンクの参照に誤りがあります。** サイトのプラットフォーム サポート マトリックスを参照してください。

これらの利用可能なパスに基づき、r12.52 SP1 にアップグレードまたは移行できます。

Windows

既存のフェデレーション バージョン	データベースは r12.52 SP1 で動作しますか	アップグレードまたは移行
すべての SP を含む r12.0	いいえ	r12.52 SP1 に移行します
すべての SP を含む r12.1	いいえ	r12.52 SP1 に移行します
r12.1 SP3	はい	r12.52 SP1 にアップグレードします

Solaris/Linux

既存のフェデレーション バージョン	データベースは r12.52 SP1 で動作しますか	アップグレードまたは移行
すべての SP を含む r12.0	いいえ	r12.52 SP1 に移行します
すべての SP を含む r12.1	いいえ	r12.52 SP1 に移行します
r12.1 SP3	はい	r12.52 SP1 にアップグレードします

FIPS 移行

CA SiteMinder® Federation Standalone は非 FIPS から FIPS のみの環境への移行をサポートします。ただし、移行プロセスは複雑です。非 FIPS から FIPS のみの環境に移行する場合、最初に r12.52 SP1 へのアップグレードを完了します。 アップグレードに成功したら、FIPS 移行プロセスに従います。

r12.52 SP1 に移行する方法

r12.52 SP1 以前の展開はオペレーティング プラットフォームで実行できます。または r12.52 SP1 がサポートしないデータベースを使用できます。そのため、r12.52 SP1 以前の環境から r12.52 SP1 に移行できます。

新しいシステムに CA SiteMinder® Federation Standalone 設定を移行し、設定を複製します。 既存の設定をコピーすることで、新しいシステムで設定プロセス全体を繰り返す必要がなくなります。

次のタスクを完了し、r12.52 SP1 システムに移行します。

重要: 説明の通りに正確にインポート手順に従います。コピー手順が完了するまで、CA SiteMinder® Federation Standalone UI の［Certs & Keys］タブにアクセスしないでください。

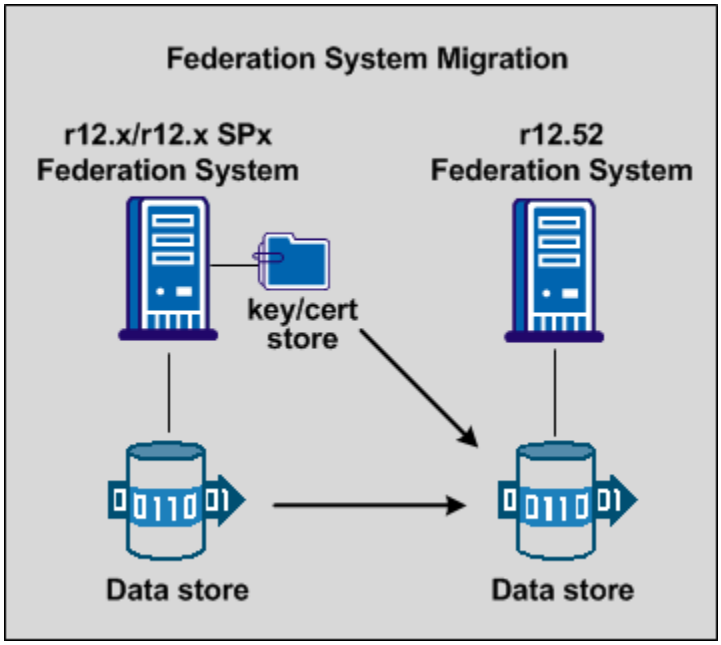
1. 複数のキー データベースを同期します（クラスタの移行に対して）（P. 69）
2. 既存の設定を XML ファイルにエクスポートします（P. 85）。
3. 新しいシステムでインストール プログラムを実行します。（P. 86）
4. 既存の設定を新しいシステムにインポートします（P. 87）。
5. キー データベースを証明書データ ストアに移行します（P. 89）。
6. SSL キーと証明書データを移行します（P. 92）。

データがすべて移行されたら、パートナーシップを再アクティブ化します。

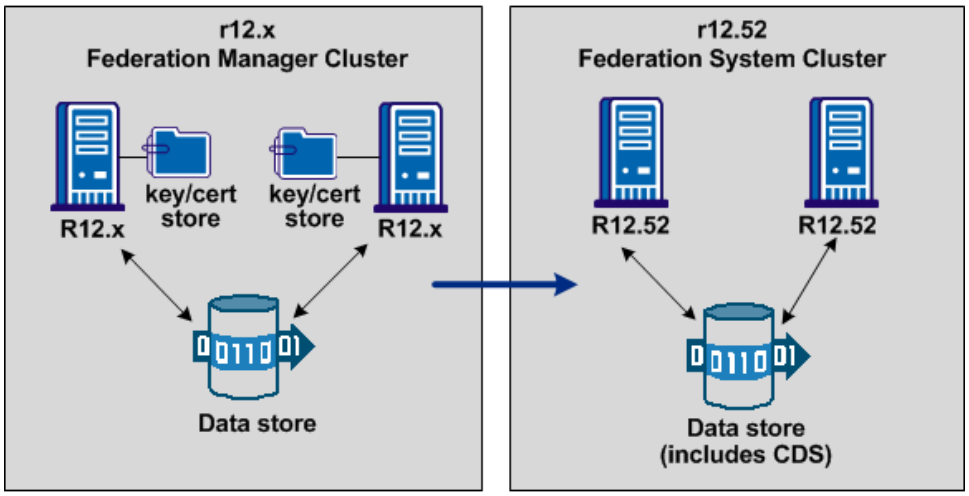
注: XPSExport と XPSImport のツールは製品に付属します。

重要: 移行は実稼働環境ではなく、テスト環境で実行することをお勧めします。

次の図は、単一のシステムからの移行パスを示したものです。



次の図は、クラスタ環境の移行パスを示したものです。



クラスタをセットアップし、フェールオーバをサポートできます。 非クラスタ移行と同様の手順を使用し、既存の r12.x クラスタから新しいクラスタに移行できます。 クラスタを移行するには、既存のクラスタで各システムの新しい r12.52 SP1 システムをセットアップします。クラスタ内のシステムは 1 つのデータ ストアを共有します。 新しい r12.52 SP1 データストアにすべてのデータを移行します。

次の手順に従ってください:

1. XML ファイルに設定をエクスポートし、キー データベースをコピーします。 エクスポートされたファイルは、バックアップ設定として機能できます。
2. キー データベース インスタンスを同期します
3. 新しい各システムで CA SiteMinder® Federation Standalone をインストールし、設定します。
4. 新しい各システムを設定します。 元のシステムに使用される設定と同じ設定を新しいシステムに使用します。 新しいシステムの次の設定が一致する必要があります。
   - **展開モード**

     新しいシステムに同じ展開モード（プロキシまたはスタンドアロン）を使用します。
   - **SiteMinder コネクタ**

     SiteMinder が元のシステムで有効な場合、新しいシステムでも有効にする必要があります。
   - **ポート番号**

     設定ウィザードを実行するとき、元のシステムで使用された同じポートを新しいシステムに指定します。
   - **仮想ホスト名**

     元のシステムが仮想ホストを使用した場合、新しいシステムで同じ仮想ホスト名を使用します。 さらに、新しいシステムのホストファイルに適切なデータを入力します。
5. エクスポートした設定を元のシステムから新しいシステムにインポートします。

このプロセスの詳細は次のセクションにあります。

キー データベースの同期

12.5 以前のシステムでは、smkeydatabase と呼ばれるキー ストアに秘密鍵および証明書のデータが格納されました。このデータは、証明書データ ストアに格納されるようになりました。このデータ ストアは従来のデータ ストアと併存します。 証明書データ ストアは、環境の各フェデレーション システムがローカル smkeydatabase にアクセスするという要件に取って代わります。

アップグレードの一部として、インストーラは自動的にローカル smkeydatabase をバックアップし、証明書データ ストアにコンテンツをすべて移行しようとします。 このプロセスでは、移行を開始する前に smkeydatabase と CDS が比較されます。 比較の目的は、データの不整合を特定することです。たとえは、複数の証明書に同じエイリアスがマッピングされている場合、移行が失敗する可能性があります。

クラスタ環境で、smkeydatabase の複数のインスタンスがあります。r12.52 SP1 にアップグレードまたは移行する前に、smkeydatabase インスタンスをすべて同期し、情報を整合します。 データベースを同期することで、各インスタンスを CDS に移行しても不整合が発生しません。

Administrative UI の［証明書およびキー］タブからの smkeydatabase インスタンスにあるあらゆるデータ不整合を解決します。 次のデータがキー データベース インスタンス全体で一貫していることを確認します。

- 各 CA 証明書は、インスタンス全体で、証明書破棄リストを一貫して参照する必要があります。
- **例：** CA 証明書は、LDAP ディレクトリ サービス内の証明書破棄リストを一貫して参照します。
- defaultentpriseprivatekey エイリアスは、すべてのインスタンスで、同じ秘密鍵/証明書のペアを表します。
- 同じエイリアスは、同じ証明書またはキー/証明書のペアにマップされます。
- 同じ CA 証明書は、同じ証明書破棄リストにマップされます。
- 破棄された、または有効期限が切れた証明書は存在しません。
- すべての CRL 情報が有効です。

重要: データの不整合をすべて解決したら、移行がすべて完了するまで smkeydatabase インスタンスを変更しないでください。

XML ファイルに設定をエクスポートします

新しいシステムに r12.5 以前の設定を複製できるように、XML ファイルに既存のシステムの設定をエクスポートします。XPSExport ツールを使用し、このタスクを完了します。

CA SiteMinder® Federation Standalone に付属する XPSExport ツールを利用すると、XML ファイルにデータ ストアのすべてのデータをエクスポートできます。

重要: 設定バックアップが進行中の場合、フェデレーション トランザクションは失敗します。

設定をエクスポートするには

1. キー データベース ディレクトリをコピーし、それを安全な場所に保存します。 キー データベースは次のディレクトリにあります。

   federation_install_dir/siteminder/smkeydatabase

   移行プロセス中にこのディレクトリを別のシステムにコピーします。

2. コマンド ウィンドウから以下のコマンドを入力して、設定をエクスポートします。

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   エクスポートの結果の出力ファイルに名前を付けます。 XPSExport からの出力は XML 形式になります。そのため、ファイル名は拡張 **.xml** で終了する必要があります。

passphrase

機密データを暗号化するのに必要なパスフレーズを指定します。パスフレーズは、8 文字以上で、1 つ以上の数字、1 つ以上の大文字、および 1 つ以上の小文字を含んでいる必要があります。 パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。

注: パスフレーズを直接入力しない場合、コマンドからそれを省くことができます。 そうすると、XPSExport はパスフレーズの入力およびパスフレーズの確認を求め、画面に表示されません。

これで暗号化された設定データを含む XML ファイルが与えられます。これを利用し、別のシステムで設定を複製できます。

3. 正常に設定をバックアップした後、インストール プログラムを実行 (P. 86) します。

CA SiteMinder® Federation Standalone インストール プログラムを実行します

設定を移行する前に、新しいシステムでインストール プログラムを実行します。

次の手順に従ってください:

1. 元のシステムのインストールに使用された同じ設定を新しいインストールに使用し、製品をインストールします。
2. フェデレーション データ オブジェクトをインポートするための新しいデータベース インスタンスをセットアップします。

   重要: 既存のデータベースを使用しないでください。 使用すると、インポートは失敗します。
3. 入力を求められたら、新しいデータベース インスタンスを指定して、設定ウィザードを実行します。

   元のシステムに使用された同じ設定をこの新しい設定に使用します。これらの設定には以下のものが含まれます。

   - 展開モード
   - ポート番号
   - 仮想ホスト名
   - SiteMinder コネクタ

新しいシステムに既存設定をインポートします

1. XPSImport コマンドを使用し、設定データをすべてインポートします。構文は以下のとおりです。

   XPSImport *export_file_name* -passphrase *passphrase*

   export_file_name

   元の設定のエクスポートの結果の XML ファイルに名前を付けます。ファイル名は拡張 **.xml** で終了する必要があります。

   passphrase

   機密データを復号化するために必要なパスフレーズを指定します。このパスフレーズは、ファイルにエクスポートするデータを暗号化したときと同じパスフレーズにする必要があります。 XML ファイルを最初に作成した管理者からパスフレーズを取得します。

   パスフレーズは、8 文字以上で、1 つ以上の数字、1 つ以上の大文字、および 1 つ以上の小文字を含んでいる必要があります。 パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。

2. プラットフォームに応じて CA SiteMinder® Federation Standalone サービスを停止します。

   - Windows

     CA SiteMinder® Federation Standalone 停止ショートカットを使用します。 ローカル管理者ではなく、ネットワーク ユーザとしてログインした場合は、ショートカットを右クリックし、［管理者として実行］を選択します。

     ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの停止］を選択します。

   - UNIX

     a. コマンド ウィンドウを開きます。

     b. スクリプト *federation_install_dir*/fedmanager.sh stop を実行します。

   注: root ユーザとしてサービスを停止したり開始したりしないでください。

3. ユーザ ストアとして ODBC データベース（SQL または Oracle）を使用する環境の場合、データベースにデータ ソース名を指定する必要があります。

   Windows の場合：

   a. 管理ツール コントロール パネルからデータ ソース（ODBC）に移動します。

   b. 新しいデータ ソース エントリを追加し、そのエントリにデータ ソース名を指定します。

   データ ソースの追加に関しては、Windows ドキュメントを参照します。

   UNIX の場合：

   system_odbc.ini ファイルを変更し、データベースのデータ ソース名（DSN）を追加します。この DSN により、移行の前に、使用されるデータベースの名前が付けられます。この DSN エントリは、CA SiteMinder® Federation Standalone システムがデータベースに接続し、トランザクションを完了するために必要です。

   a. ディレクトリ *federation_install_dir*/siteminder/db に移動します。

   b. テキスト エディタで system_odbc.ini ファイルを開きます。

   c. DSN を追加します。

   d. ファイルを保存します。

   注: 同じ system_odbc.ini ファイルで SQL と Oracle のデータ ソースを追加できます。

4. 元のシステムの CA SiteMinder® Federation Standalone 設定と同じ設定を使用し、設定ウィザードを再実行します。 これらの設定には以下のものが含まれます。

   - 展開モード
   - ポート番号
   - 仮想ホスト名
   - SiteMinder コネクタ

   重要: Apache Tomcat http.conf ファイルまたは SPS server.conf ファイルを手動で変更した場合は、新しいシステムでそれらのファイルに同じ変更を加えます。

5. 次のいずれかのタスクを実行し、SSL キーと証明書を移行します。
   - 新しいシステムに SSL キーと証明書を移行します。 SSL 移行手順に従います。 SSL データを移行することで、新しいキーまたは証明書を購入せずに済みます。
   - 新しいキー/証明書リクエストを生成してから、証明書に署名させます。SSL 証明書はインポートされた設定ファイルに含まれていません。

データがすべて移行されたら、パートナーシップを再アクティブ化します。

証明書データ ストアにキー データベースを移行します

環境に 1 つ以上のキー データベース (smkeydatabase) が含まれる場合は、r12.52 SP1 証明書データ ストアにコンテンツを移行します。

注: SSL キーと証明書を移行するには、SSL 移行手順 (P. 92)を確認します。

証明書データ ストアはキー データベースを置換します。 使用する環境で 1 つ以上の smkeydatabases を展開する場合は、以下の点を考慮します。

- 証明書データ ストアはデータ サーバと連結されます。 単一の証明書データ ストアによって、各ホスト システム上の個別の smkeydatabase インスタンスが不要になります。
- アップグレードの一部として、すべての smkeydatabase コンテンツが自動的にバックアップされ、証明書データ ストアに移行されます。
- フェデレーション システムは証明書データ ストアとのみ通信できます。 smkeydatabase は、互換モードでは動作しません。

  重要: smkeydatabase の移行が失敗した場合、フェデレーション システムを環境に戻さないでください。 移行が失敗した後でシステムを戻すと、証明書データを必要とするトランザクションはすべて失敗します。
- 移行を開始する前に smkeydatabase インスタンスをすべて同期します。すべてのインスタンスを同期することによって、データの衝突を防ぎます。 データの衝突が発生すると、移行が正常に実行されません。
- すべてのフェデレーション システムがビューを共有して同じデータベース サーバを参照し、同じキー、証明書、証明書破棄リスト（CRL）にアクセスします。

- 証明書データ ストアの目的は、smkeydatabase の目的と変わりません。このストアによって以下が SiteMinder 環境で利用可能になります。
  - 認証機関（CA）の証明書
  - 公開キーおよび秘密キー
  - 証明書破棄リスト
- CRL が LDAP ディレクトリ サービスに格納される場合、以下の点を考慮します。
  - フェデレーション システムでは、CRL の発行元と、対応するルート証明書の発行元が同一の CA である必要がなくなりました。
  - フェデレーション システムはこの確認を実行しなくなりました。この動作はテキスト ベースの CRL の要件と一致しています。

CDS にデータを移動するための移行ユーティリティの実行

CDS にキー データベースを移行するための考慮事項を確認したら、smmigratecds という名前の移行ユーティリティを実行します。

次の手順に従ってください:

1. 必ずすべての r12.x smkeydatabases を同期 (P. 69)します。
2. r12.x ホスト システムにログインし、次の場所に移動します。

   federation_install_dir¥siteminder¥config¥properties

   federation_install_dir

   CA SiteMinder® Federation Standalone インストール パスを指定します。
3. 以下のファイルをコピーします。

   smkeydatabase.properties
4. r12.52 SP1 ホスト システムにログインし、次の手順を完了します。
   a. 以下の場所に移動します。

      federation_install_dir¥siteminder¥config¥properties
   b. smkeydatabase プロパティ ファイルの r12.52 SP1 バージョンの名前を以下の値に変更します。

      newsmkeydatabase.properties
   c. プロパティ ファイルの r12.x バージョンをディレクトリに追加します。

d. テキスト エディタで r12.52 SP1 および r12.x のプロパティ ファイルを開きます。

e. r12.x バージョンのデータベースのパスを編集して、r12.52 SP1 バージョンのパスに一致させます。

Windows の例

```
DBLocation=C:¥CA¥FederationStandalone¥siteminder¥smkeydatabase
```

Solaris/Linux の例

```
DBLocation=export/fed/CA/FederationStandalone/siteminder/smkeydatabase
```

f. r12.x プロパティ ファイルを保存し、r12.52 SP1 プロパティ ファイルを閉じます。

g. CA SiteMinder® Federation Standalone インストールのルートで次のディレクトリを作成します。

```
smkeydatabase
```

Windows の例：

```
C:¥Program Files¥CA¥FederationStandaloe¥siteminder¥smkeydatabase
```

Solaris/Linux の例

```
export/fed/CA/FederationStandalone/siteminder/smkeydatabase
```

5. r12.x ホスト システムに戻り、smkeydatabase ディレクトリの内容をコピーします。

6. r12.52 SP1 ホスト システムに戻り、次の手順を完了します。

a. 作成した r12.52 SP1 smkeydatabase ディレクトリに、r12.x smkeydatabase ディレクトリの内容を追加します。

b. 次のコマンドを入力し、証明書データ ストアに smkeydatabase を移行します。

```
smmigratecds
```

c. 移行が成功したら、smkeydatabase プロパティ ファイルおよび smkeydatabase ディレクトリを削除します。

これで移行は完了です。

キー データベースの移行に失敗した場合、CDS に手動で移行できます。

詳細情報:

キー データベース移行をトラブルシューティングする (P. 127)

SSL キーと証明書の移行(任意)

CA SiteMinder® Federation Standalone r12.52 SP1 については、埋め込み Apache と Tomcat サーバの SSL キーと証明書ファイルが暗号化されます。リリース 12.0 と 12.0 SP1 については、これらのファイルは暗号化されません。 暗号化ファイルの新しいキー/証明書ペアを購入しないようにするには、CA SiteMinder® Federation Standalone r12.0/r12.0 SP1 から r12.52 SP1 に既存のキーまたは証明書ファイルを移行します。 また、それらを移行せず、バックアップ目的でこれらのファイルをエクスポートできます。

重要: r12.1 の前のシステムについては、埋め込み Tomcat サーバは自己署名証明書を使用します。この自己署名証明書を r12.52 SP1 への移行に使用することはできません。 署名付き証明書を購入し、署名付き証明書で Tomcat SSL 設定をアップグレードします。

Apache については、r12.0 以降、SSL 接続のファイルを移行できます。Tomcat については、r12.1 以降からのみファイルを移行できます。12.0 では、自己署名証明書が Tomcat キー ストアをセキュリティ保護したためです。 r12.1 以降、フェデレーション製品では認証機関による証明書の署名が必要です。

SSL キーと証明書ファイルの移行は次の状況で役立ちます。

- 既存のシステムをアップグレードする代わりに、新しいシステムで CA SiteMinder® Federation Standalone の別のバージョンに移動します。 既存のシステムから新しいシステムに SSL キーと証明書を移行します。
- クラスタのあるシステムから別のシステムに SSL キーと証明書を移行します。移行することで、キーと証明書を再利用できます。たとえば、ロード バランサが SSL リクエストをクラスタのフェデレーション システムに渡す場合、各システムが同じキーと証明書を使用する必要があります。 そのため、あるシステムから別のシステムにキーと証明書を移行します。

注: 12.0 システムを r12.52 SP1 にアップグレードする場合、インストーラは自動的に Apache と Tomcat SSL のキーと証明書ファイルを暗号化ファイルにアップグレードします。 これが移行に自動的に適用されることはありません。

証明書と秘密鍵ファイルは次のようになります。

Apache

- server.key ファイルには秘密鍵が含まれます。
- server.cert ファイルにはサーバ証明書が含まれます。

Tomcat

- r12.0 については、tomcat.keystore ファイルには自己署名証明書が含まれます。 r12.x については、tomcat.keystore ファイルには CA 署名証明書と秘密鍵のペアが含まれます。

これらのファイルを移行またはエクスポートするには、migratessl という名前の SSL ユーティリティを使用します。 移行ユーティリティは、Windows システムの場合はバッチ ファイルとして、UNIX システムの場合はシェル スクリプトとして CA SiteMinder® Federation Standalone r12.52 SP1 に付属します。 ツールは *federation_install_dir*/bin フォルダにあります。

SSL ファイルを移行するプロセスは次のようになります。

1. 既存のフェデレーション システムから r12.52 SP1 システムの任意の場所にキーと証明書のファイルをコピーします。
2. キーと証明書のファイルをコピーした場所に migratessl ツールをコピーします。
3. 署名付き証明書を移行する場合、SSL 証明書に署名した認証機関証明書をエクスポートします。移行を続行する前に、CA 証明書をインポートします。

注: この移行プロセスをスキップし、新しいキー/証明書リクエストを出し、証明書に署名することもできます。 SSL 証明書はインポートされた設定ファイルに含まれていません。

r12 System からキーと証明書をコピーします

SSL 移行ツールを使用するには、移行またはエクスポートを計画している CA SiteMinder® Federation Standalone システムのキーと証明書ファイルを最初に収集し、コピーします。

SSL キーと証明書ファイルをコピーする方法

1. 既存の CA SiteMinder® Federation Standalone システムでファイルの場所を確認します。

   Apache SSL キーと証明書ファイルは次の場所にあります。

   - *federation_install_dir*/secure-proxy/SSL/keys/server.key
   - *federation_install_dir*/secure-proxy/SSL/certs/server.crt

   Tomcat SSL キー ストア ファイルは次の場所にあります。

   - *federation_install_dir*/secure-proxy/SSL/keys/tomcat.keystore
2. 新しい CA SiteMinder® Federation Standalone マシンの任意の場所にキーと証明書のファイルをコピーします。

キー/証明書ファイルと同じフォルダに SSL 移行ツールをコピーします

SSL 移行ツールは、CA SiteMinder® Federation Standalone 12.1 SP3 で展開するソフトウェアを必要とします。CA SiteMinder® Federation Standalone 12.1 SP3 製品がインストールされているマシンでツールを実行します。 特に、ツールは移行するファイルをコピーした同じフォルダに置く必要があります。

SSL ユーティリティ ツールをコピーする方法

1. r12.52 SP1 システムの *federation_install_dir*/bin に移動します。
2. キーと証明書のファイルをコピーした、r12.52 SP1 システムの場所に migratessl ファイル（.bat または .sh）をコピーします。

SSL キーおよび証明書の移行またはエクスポート

migratessl ユーティリティを実行することにより、SSL キーまたは証明書ファイルの移行を実行します。

次の手順に従ってください:

1. 移行している SSL 証明書に最初に署名した認証機関証明書をインポートします。
   a. 移行元のシステムで、CA SiteMinder® Federation Standalone UI を使用して CA 証明書をエクスポートします。
   b. 移行先の新しいシステムで、CA SiteMinder® Federation Standalone UI を使用して CA 証明書をインポートします。
2. 既存のキーまたは証明書ファイルをコピーした新しいシステムで、コマンド ウィンドウを開きます。
3. コンポーネントをコピーしたフォルダに移動します。
4. 必要なコマンド引数と共に migratessl コマンドを指定します。 すべてのオプションについては、移行ツール コマンド引数 (P. 96) のリストを参照してください。

   例

   - Apache SSL 接続用の SSL server.key を移行するには、以下を入力します。

```
migratessl.bat -op migrate -keytype Apache
-sourcefile server.key -certfile server.crt
-sourcever 12.0 -sourceos Windows -oldpwd admin1
-newpwd admin2 -issueralias trustedca
```

- Tomcat SSL 接続用のキー/証明書ファイルを移行するには、以下を入力します。

```
migratessl.sh -op migrate -keytype Tomcat
-sourcefile tomcat.keystore -sourcever 12.1
-sourceos UNIX -issueralias trustedca
-oldpwd admin1 -newpwd admin2
```

- Tomcat SSL 接続用のキー/証明書ファイルをエクスポートするには、以下を入力します。

```
migratessl.sh -op export -keytype Tomcat
-sourcefile tomcat.keystore -sourcever 12.1
-sourceos UNIX  -dest ca/federationmgr/secure-proxy/
SSL/keys/ -oldpwd admin1 -newpwd admin2
```

設定移行全体の一部として SSL キーおよび証明書を移行している場合は、パートナーシップを再アクティブ化することによって移行プロセスを完了します。

SSL 移行ツール コマンド引数

migratessl ツールはコマンド ラインで呼び出されます。 コマンドを入力する場合

- 各コマンド引数（Help フラグを除く）の後に値を 1 つだけ付けます。
- ディレクトリ パスなどのスペースがある値は、二重引用符で囲みます。

コマンド引数	意味
-op	Migrate または Export デフォルト： Migrate Apache のエクスポートの場合、-certfile 引数を指定した場合、ツールは server.key ファイルおよび server.crt ファイルをエクスポートします。 Tomcat の場合、ツールは PKCS#12 キー/証明書ファイルの tomcat.p12 ファイルをエクスポートします。
-keytype	Apache または Tomcat デフォルト： Apache
-sourcefile	SSL キー（Apache）または、キーと証明書を格納するキー ストア（Tomcat）を含むファイルの名前。
-certfile	Apache SSL サーバ証明書を含むファイルの名前（Apache のみ）。

-sourcever	12.0、12.1 など、キーまたは証明書が生成された CA SiteMinder® Federation Standalone のバージョン。 デフォルト： 12.0
-sourceos	キーが生成された環境のオペレーティング システム（Windows または UNIX）。 **注**: Linux のサポートは r12.1 SP3 で導入されたため、Linux オプションはありません。 デフォルト： ツールが実行されているマシンの OS。
-dest	出力ファイルのフォルダのパス。 移行の場合、このオプションは無視されます。 エクスポートの場合のデフォルト： 現在のフォルダ **重要**: 宛先フォルダを指定しない場合、移行しているファイルが上書きされます。
-issueralias	移行している証明書を署名した CA 証明書のエイリアス。 このエイリアスで CA 証明書を宛先の CA SiteMinder® Federation Standalone システムにインポートします （Migrate の場合にのみ使用され、Export の場合は無視されます）。
-oldpwd	キーのソースであるシステムの CA SiteMinder® Federation Standalone 管理パスワード。
-newpwd	キーの移動先のシステムの CA SiteMinder® Federation Standalone 管理パスワード。
-h	これらの使用手順を表示します。
-help	これらの使用手順を表示します。
-?	これらの使用手順を表示します。

SSL および SiteMinder コネクタを再設定する（オプション）

前の設定で SSL または SiteMinder コネクタを使用した場合は、移行を完了した後、これらの手順を完了します。

1. Administrative UI にログインします。

   重要: この手順全体が完了するまで、Administrative UI の［証明書 & キー］タブにアクセスしないでください。

2. （オプション）コネクタが元のシステムで有効だった場合、これらの手順に従って、新しいシステム上でコネクタを設定し有効にできます。

   a. ［インフラストラクチャ］タブをクリックし、［展開設定］を選択します。

   b. 元の設定からの同じ値を使用して、コネクタ設定を再設定します。

   c. ［ホストの登録］をクリックして、ポリシー サーバにフェデレーション システムを再登録します。

   注: 新しいシステムでコネクタを設定して有効にした場合、すべてのパートナーシップはデフォルトでそのコネクタを使用します。 個々のパートナーシップのコネクタを無効にするには、特定のパートナーシップを編集します。

3. （オプション）SSL が Artifact バック チャネル、または元のシステムの Administrative UI に対して有効だった場合は、新しいシステムで SSL を再設定します。 フェデレーション トランザクションを処理する前に SSL を有効にします。

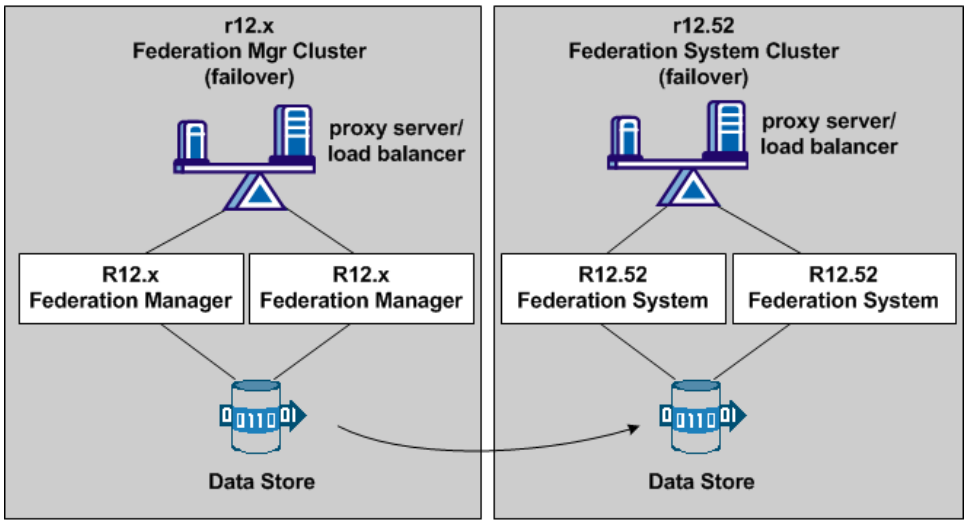
   埋め込み Web サーバの場合は、既存の SSL キーと証明書を移行するか、新しいキー/証明書リクエストを生成します。 最後に証明書に署名します。 SSL 証明書はインポートされた設定ファイルに含まれていません。

これで新しいシステムは元のシステムと同じ設定で作動します。

フェールオーバ展開を移行する方法

r12.52 SP1 フェールオーバ展開に既存の r12x フェールオーバ展開を移行できます。

次の図は、フェールオーバをサポートするクラスタ化された環境を示したものです。



r12.52 SP1 にフェールオーバ展開を移行するには、次の手順を行います。

1. 新しい r12.52 SP1 システムに既存の設定をコピーします。
2. プロキシ サーバまたはロード バランサを更新し、適切な URL を新しい r12.52 SP1 システムに渡します。

r12.52 SP1 に r12 フェールオーバ展開を移行します

r12.52 SP1 CA SiteMinder® Federation Standalone 展開に既存の r12.x フェールオーバ展開を移行できます。

フェールオーバ設定を移行する方法

1. 展開の各マシンに r12.52 SP1 をインストールします。
2. 最初のアップグレードされたマシンで設定ウィザードを実行し、前の設定に使用された情報と同じ情報を入力します。

   既存の設定を確認するには、r12.x システムにあるファイル *federation_install_dir*¥install_config_info¥ca-Federation-Config.properties を参照します。
3. 2 番目のマシンで r12.52 SP1 設定ウィザードを実行します。 以下の情報を入力します。
   a. 最初のマシンからのデータベース情報。
   b. ca-Federation-Config.properties ファイルからの他のすべてのエントリ。
4. CA SiteMinder® Federation Standalone UI にログインします。
5. ［インフラストラクチャ］タブで［システム設定］を選択します。

   ［システムの設定］ダイアログ ボックスが表示されます。
6. UI の［グローバル ベース URL］を変更し、フェデレーション ネットワークにプロキシ サーバまたはロード バランサのホストとポートを含めます。 この URL を適切に設定することで、パートナーシップの作成に使用されるすべてのメタデータのデフォルト URL が正しくなります。
7. プロキシ エンジンのデフォルト ベース URL を変更し、フェデレーション ネットワークにプロキシ サーバまたはロード バランサのホストとポートを含めます。 この URL を適切に設定することで、パートナーシップの作成に使用されるすべてのメタデータのデフォルト URL が正しくなります。

   ベース URL は server.conf ファイルに定義されます。

   server.conf ファイルを変更するには、以下の操作を実行します。
   a. *federation_mgr_home*/secure-proxy/proxy-engine/conf に移動します。
   b. エディタで server.conf ファイルを開きます。

c. ［# デフォルト仮想ホスト］セクションに移動します。

d. 以下のように、完全修飾ホスト名を使用して**ホスト名**設定にベース URL を追加します。

```
<VirtualHost name="default">
hostnames="defaultbaseurl.ca.com:80, newbaseurl.ca.com:80"
</VirtualHost>
```

注: 各エントリをカンマで区切ることにより、ホスト名設定に複数の *host_name:port* エントリを指定します。

8. r12x システムでフェールオーバの SSL を有効にしている場合、SSL 移行手順 (P. 92)にあるように、r12.52 SP1 のプライマリおよびセカンダリ システムに SSL 設定を移行する必要があります。

これでいずれの CA SiteMinder® Federation Standalone システムも同じデータベース サーバを指します。プロキシ サーバまたはロード バランサからのフェールオーバに対して設定できます。

プロキシ サーバまたはロード バランサでフェールオーバをセットアップする

このガイドでは、プロキシ サーバまたはロード バランサの管理者がそのシステムにフェールオーバをセットアップする方法を知っていると想定しています。

プロキシ サーバ/ロード バランサのマシンで

1. プロキシ サーバ設定については、プライマリ ホストとして 1 つのフェデレーション システムを識別し、セカンダリ ホストとしてもう 1 つのフェデレーション システムを識別します。

   マシンの負荷分散を設定しないでください。

2. 次の URL をフェデレーション マシンに渡すようにサーバを設定します。
   - /affwebservices/*
   - /siteminderagent/*

展開モード(スタンドアロンまたはプロキシ)によっては、フェデレーション システムを介して他のトラフィックを送信できます。

これでプロキシ サーバまたはロード バランサはフェデレーション システムにフェールオーバできます。

第 5 章: フェデレーション システムの移行による FIPS 暗号化の使用

FIPS_Only モードに移行する前に、次の問題に注意します。

- SiteMinder コネクタを有効化し、FIPS_ONLY モードでフェデレーション製品を展開する場合、バックエンド SiteMinder システムがバージョン r12x であり、FIPS_ONLY モードで作動している必要があります。

  SiteMinder システムが r6.0 SP5 の場合、このシステムは FIPS 互換の操作をサポートしません。そのため、フェデレーション システムは FIPS_ONLY モードで動作できません。

- r12.1 より前の CA SiteMinder® Federation Standalone リリースは、秘密鍵を生成する FIPS 承認済み暗号化アルゴリズムをサポートしません。これらのリリースは秘密鍵を生成するシグネチャ アルゴリズムとして MD5 のみをサポートします。MD5 は認められた FIPS アルゴリズムではありません。

  シグネチャ アルゴリズムとして MD5 のみを使用する秘密鍵がある場合、パートナーシップの両方のサイトで次のアクションを実行します。

  - 新しい秘密鍵を生成します
  - 新しい証明書を取得します
  - 新しい公開鍵で必要なすべてのパートナーシップを更新します。

このセクションには、以下のトピックが含まれています。

考慮するべき FIPS 移行問題 (P. 104)
FIPS_COMPAT モードから FIPS_Only モードに移行する方法 (P. 104)

考慮するべき FIPS 移行問題

FIPS_Only モードに移行する前に、次の問題に注意します。

- SiteMinder コネクタを有効化し、FIPS_ONLY モードでフェデレーション製品を展開する場合、バックエンド SiteMinder システムがバージョン r12x であり、FIPS_ONLY モードで作動している必要があります。

  SiteMinder システムが r6.0 SP5 の場合、このシステムは FIPS 互換の操作をサポートしません。そのため、CA SiteMinder® Federation Standalone は FIPS_ONLY モードで作動できません。

- r12.1 より前の CA SiteMinder® Federation Standalone リリースは、秘密鍵を生成する FIPS 承認済み暗号化アルゴリズムをサポートしません。これらのリリースは秘密鍵を生成するシグネチャ アルゴリズムとして MD5 のみをサポートします。MD5 は認められた FIPS アルゴリズムではありません。

  シグネチャ アルゴリズムとして MD5 のみを使用する秘密鍵がある場合、パートナーシップの両方のサイトで次のアクションを実行します。

  - 新しい秘密鍵を生成します
  - 新しい証明書を取得します
  - 新しい公開鍵で必要なすべてのパートナーシップを更新します。

FIPS_COMPAT モードから FIPS_Only モードに移行する方法

FIPS が提供する強固な暗号化アルゴリズムを使用して機密データの安全を守ることで、機密漏洩からデータを守り、フェデレーション システムを全体的により安全にします。

機密データの安全を守る FIPS 互換の暗号化アルゴリズムのみを使用し、運用するフェデレーション システムを移行できます。

次の FIPS 操作モードのいずれかで CA SiteMinder® Federation Standalone をインストールできます。

FIPS_COMPAT

FIPS_COMPAT（互換性）モードは、インストール中のデフォルトの FIPS 操作モードです。FIPS_COMPAT モードでは、フェデレーション システムは、サポートされている FIPS 準拠アルゴリズムと共に非 FIPS アルゴリズムの現在のセットも引き続きサポートします。

FIPS_COMPAT モードは、旧バージョンのフェデレーションと互換性があります。 この互換性により、r12.52 SP1 よりも前のバージョンの環境が r12.52 SP1 と相互運用できるようになります。また、FIPS_COMPAT は、現在のフェデレーション実装で使用可能なセキュリティの程度に満足しているすべてのライアントにとっても適切です。

組織が FIPS の使用を必要としない場合、CA SiteMinder® Federation Standalone を FIPS_COMPAT モードでインストールします。追加設定は必要ありません。

FIPS_ONLY

FIPS_ONLY モードでは、環境は FIPS 準拠アルゴリズムのみを使用して機密データを暗号化します。

FIPS 互換アルゴリズムのみを使用する新しいインストールの場合、CA SiteMinder® Federation Standalone を FIPS_ONLY モードでインストールします。

製品は FIPS_COMPAT モードからの一方向の移行パスのみを許可します。このモードは MIGRATE モードを通過して FIPS_ONLY モードに移行するためのデフォルト モードです。 FIPS_MIGRATE モードでは、FIPS_COMPAT モードで実行されているフェデレーション環境を FIPS_ONLY モードに移行させることができます。 MIGRATE モードでは、フェデレーション システムは FIPS_ONLY モードに環境を移行する際に、既存のデータ用の既存の暗号化アルゴリズムを継続して使用します。 ただし、暗号化を必要とする新しいデータは FIPS 互換のアルゴリズムのみを使用して暗号化されます。

重要: FIPS_ONLY モードで作動している環境は、古いバージョンのフェデレーション API を使用するカスタム ソフトウェアを含む以前のバージョンのフェデレーションとの下位互換性がなく、相互運用できません。r12.52 SP1 以前の SDK でカスタム ソフトウェアを構築している場合、r12.52 SP1 SDK を利用してこのソフトウェアを再コンパイルし、FIPS_ONLY モードに必要なサポートを得ます。

フェデレーション システムを FIPS_ONLY モードに移行するには：

1. 既存の設定をバックアップします。
2. OPENSSL_FIPS 環境変数を設定します。
3. ポリシー エンジンを FIPS_MIGRATE に設定します。
4. ポリシー ストア キーを再暗号化します。
5. ポリシー ストア管理者パスワードを再暗号化します。
6. SiteMinder スーパーユーザ パスワードを再暗号化します。
7. クライアントの共有秘密鍵を再暗号化します。
8. ポリシーとキー ストア データを再暗号化します。
9. Administrative UI を FIPS_ONLY モードに設定します。
10. 埋め込みセキュア プロキシ エンジンを FIPS_ONLY モードに設定します。
11. 埋め込みポリシー エンジンを FIPS_ONLY モードに設定します。

重要: FIPS_ONLY モードに移行すると、FIPS ではない承認済み証明書で設定されたパートナーシップは動作を停止し、その結果、パートナーシップは動作を停止します。FIPS_ONLY 動作に移行する前に FIPS 互換アルゴリズムを使用し、パートナーシップ データを暗号化します。

次のセクションで、各手順を詳細に説明します。

SSL 設定を非アクティブ化します

［FIPS のみ］モードに移行する最初の手順は、［埋め込み Web サーバ］または［管理 UI］セクションの SSL を非アクティブ化することです。そもそも SSL をアクティブ化しなかった場合は、この手順をスキップします。

SSL を非アクティブ化するには

1. ［SSL 設定］ダイアログ ボックスで開始します。
2. アクティブなサービスがあれば、それを非アクティブ化します。 それを行うには、［埋め込み Web サーバ］および/または［管理 UI］セクションの［非アクティブ化］をクリックします。

   SSL を無効にするかどうかを尋ねる確認プロンプトが表示されます。
3. ［はい］をクリックして非アクティブ化を完了します。

4. オペレーティング環境に応じて、フェデレーション サービスを再起動します。

   - **Windows**

     以下のように、停止および開始ショートカットを使用します。ローカル管理者ではなく、ネットワーク ユーザとしてログインした場合は、ショートカットを右クリックし、［管理者として実行］を選択します。

     a. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの停止］

     b. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの開始］

   - **UNIX**

     a. コマンド ウィンドウを開きます。

     b. 以下のスクリプトを実行します。

     federation_install_dir/fedmanager.sh stop

     federation_install_dir/fedmanager.sh start

   注: root ユーザとしてサービスを停止したり開始したりしないでください。

SSL 接続がアクティブではなくなり、［SSL 設定ステータス］設定が［**サーバ証明書は CA によって署名され、SSL の準備ができています**］に変わります。 ユーザが SSL を再度有効にできるように、証明書およびキー ファイルは残ります。

既存設定をバックアップします

システム回復、アップグレード、移行の一部として既存の設定をリストアできます。

設定をリストアするには、キー データベースをコピーし、設定データをエクスポートします。 製品に付属する XPSExport ツールを使用して、設定データを XML ファイルにエクスポートできます。

重要: 設定のリストア中は、フェデレーション トランザクションは失敗します。

設定をエクスポートする方法

1. キー データベースをコピーし、安全な場所に保存します。 キー データベースは次のディレクトリにあります。

   federation_mgr_home/siteminder/smkeydatabase

2. コマンド ウィンドウから以下のコマンドを入力して、設定をエクスポートします。

   XPSExport *export_file_name* -xa -passphrase *passphrase*

   export_file_name

   エクスポートの結果の出力ファイルに名前を付けます。 XPSExport からの出力は、XML 形式であるため、ファイル名は拡張子 **.xml** で終わる必要があります。

   passphrase

   機密データを暗号化するのに必要なパスフレーズを指定します。 パスフレーズは、8 文字以上で、1 つ以上の数字、1 つ以上の大文字、および 1 つ以上の小文字を含んでいる必要があります。 パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。

   注: パスフレーズを直接入力しない場合、コマンドからそれを省くことができます。 そうすると、XPSExport はパスフレーズの入力およびパスフレーズの確認を求め、画面に表示されません。

これで暗号化された設定データを含む XML ファイルが用意できました。 XML ファイルを使用し、設定をリストアします。

OPENSSL_FIPS 環境変数を設定します

OPENSSL_FIPS 環境変数を設定し、FIPS モードを有効にします。 COMPAT モードから FIPS のみモードに移行する場合に限り、この変数を 1 回設定します。

次の手順に従ってください:

Windows

1. Windows システム プロパティにアクセスします
2. 環境変数にアクセスします。
3. 次のように環境変数を追加します。

   変数名

   OPENSSL_FIPS

   変数値

   1
4. 新しい変数を保存します。

UNIX

1. federation_install_dir に移動します。
2. 環境スクリプト ca_federation_env.ksh を編集します。
3. スクリプトに次のエントリを追加します。

   ```
   OPENSSL_FIPS=1;export OPENSSL_FIPS=1
   ```
4. 環境スクリプトの ca_federation_env.ksh を実行し、環境変数を設定します。
5. UNIX システムのみで、*federation_install_dir*/bin/migratessltofips.sh スクリプトを実行します。

   このスクリプトを実行すると、SSL 証明書と関連付けられた秘密鍵が正しく暗号化されます。

ポリシー エンジンを FIPS_MIGRATE モードに設定する

FIPS_Only モードに移行する最初の手順は、FIPS_MIGRATE モードでポリシー エンジンを設定することです。

次の手順に従ってください:

1. CA SiteMinder® Federation Standalone が COMPAT モードになっていることを確認します。 COMPAT モードになっていない場合、CA SiteMinder® Federation Standalone を再インストールし、COMPAT モードで実行されるように設定します。
2. コマンド プロンプトから、次のように setFIPSmigration コマンドを実行します。

   Windows

   「setFIPSmigration」を入力します

   UNIX

   a. *federation_install_dir*/siteminder/bin に移動します。
   b. 「setFIPSmigration.ksh」を入力します
   c. 環境スクリプトの ca_federation_env.ksh を実行し、環境変数を設定します。

   移行プロセスが開始します。

3. 以下のいずれかを実行します。

   Windows

   CA SiteMinder® Federation Standalone システムを再起動します。

   UNIX

   コマンド ウィンドウからの次のスクリプトを実行し、CA SiteMinder® Federation Standalone サービスを再起動します。

   a. *federation_install_dir*/fedmanager.sh stop

   b. *federation_install_dir*/fedmanager.sh start

   注: root ユーザとしてサービスを停止したり開始したりしないでください。 root 以外のユーザである必要があります。

4. smps.log ファイルを調べ、ポリシー エンジンが MIGRATE モードになっていることを確認します。

   ログ ファイルの場所は *federation_install_dir*/logs/server/smps.log です。

これでポリシー エンジンは FIPS_MIGRATE モードで作動しています。

ポリシー ストア暗号化キーを再暗号化します

移行プロセスの次の手順は、ポリシー ストア暗号化キーを再暗号化することです。

ポリシー ストア キーを再暗号化する方法

1. CA SiteMinder® Federation Standalone Web キットをまだダウンロードしていない場合は、テクニカル サポート サイトに移動し、動作環境に合ったキットをダウンロードします。
2. *federation_install_dir*/siteminder/bin に smreg をコピーします。
3. コマンド プロンプト ウィンドウを開きます。

4. コマンド プロンプトから、以下のコマンドを入力します。

   smreg -cf MIGRATE -key *admin_password*

   admin_password

   インストール時に入力した CA SiteMinder® Federation Standalone 管理者パスワードを指定します。

5. ディレクトリ *federation_install_dir*¥siteminder¥bin にある EncryptionKey.txt ファイルを開きます。

   その中に新しい暗号化キーがあります。それには、AES など、FIPS 互換のアルゴリズムによるプレフィックスが付いています。

再暗号化が完了します。

データベース管理者パスワードを再暗号化します

移行プロセスでは、データベース管理者パスワードを再暗号化する必要があります。

パスワードを再暗号化する方法

1. コマンド プロンプトから、次のように fedconfig ユーティリティを実行します。

   Windows

   federation_install_dir/bin に移動し、「fedconfig.bat」を入力します。

   UNIX

   a. federation_install_dir に移動します。

   b. 環境スクリプトの ca_federation_env.ksh を実行し、環境変数を設定します。

   c. /bin ディレクトリに移動します。

   d. 「fedconfig.sh」を入力します。

   fedconfig ユーティリティにより、ユーティリティ オプションが一覧表示されます。

2. 「5」を入力し、データベース管理者パスワードを変更します。

3. 「C」を入力し、CA SiteMinder® Federation Standalone 設定ウィザードの実行時に入力したパスワードを入力します。

4. パスワード入力を確認します。
5. 「0」を入力し、パスワードを保存して終了します。

パスワードを正常に変更しました。

スーパーユーザ パスワードの再暗号化

FIPS_Only モードに移行するには、CA SiteMinder® Federation Standalone スーパーユーザ パスワードを再暗号化します。

スーパーユーザ パスワードを再暗号化する方法

1. CA SiteMinder® Federation Standalone Web キットをまだダウンロードしていない場合は、テクニカル サポート サイトに移動し、動作環境に合ったキットをダウンロードします。
2. *federation_install_dir*/siteminder/bin に smreg をコピーします。
3. 以下のコマンドを入力します。

   smreg -cf MIGRATE -su *admin_password*

   admin_password

   インストール時に入力した CA SiteMinder® Federation Standalone 管理者パスワードを指定します。
4. siteminder¥bin から smreg を削除します。

   注: smreg を削除すると、前のパスワードを知らない限り、パスワードを変更できなくなります。

スーパーユーザ パスワードが設定されます。

プロキシ エンジン エージェントの共有秘密鍵を再暗号化します

移行するには、プロキシ エンジン Web エージェントの共有秘密鍵を再暗号化します。

共有秘密鍵を再暗号化するには

1. コマンド プロンプト ウィンドウを開きます。
2. *federation-mgr_home*¥secure-proxy¥proxy-engine¥conf¥defaultagent¥SmHost.conf にある SmHost.conf ファイルに移動します。

3. 設定の一部に対して、SmHost.conf ファイルの値を利用し、次のコマンドを入力します。

   smreghost -i *policy_server_ip_address,port,port,port* -u a*dmin_user_name* -p *admini_password* -hn *host_name* -hc *host_config_object* -f *host_config_file_path* -o -cf MIGRATE

   policy_server_ip_address, port, port, port

   ポリシー エンジンの IP アドレスとポート番号を指定します。SmHost.conf ファイルでアドレスを探します。デフォルト ポートは 44441、44442、44443 です。

   デフォルト以外のポートを使用している場合、ポート番号のみを指定する必要があります。デフォルト以外のポートについては、3 つのポートすべてに同じ番号または別の番号を使用できます。

   admin_user_name

   管理者名を指定します。smreghost ユーティリティを使用するときは、この値に「**siteminder**」を入力します。

   admin_password

   インストール時に指定した CA SiteMinder® Federation Standalone 管理者のパスワードを指定します。

   hostname

   ポリシー エンジンでホスト登録に使用される信頼されたホストの名前を指定します。 このパラメータには一意の値を入力します。SmHost.conf ファイルでそのホスト名を使用しないでください。そのホスト名はポリシー ストアにすでに存在します。

   host_config_object

   ポリシー エンジンで使用されるホスト設定オブジェクトの名前を示します。 SmHost.conf ファイルでホスト名の値を探します。

   host_config_file_path

   SmHost.conf ファイルの場所を指定します。

   例

   ```
   smreghost -i localhost -u siteminder -p mypassword
   -hn lfed-localhost20090511024942 -hc fed-localhost20090511024942
   -f "C:¥Program Files¥CA¥FederationManager¥secure-proxy¥proxy-engine
   ¥conf¥defaultagent¥SmHost.conf" -o -cf MIGRATE
   ```

   このコマンドを実行すると、共有秘密鍵の再暗号化が完了します。

4. 次のディレクトリにある SmHost.conf ファイルに移動します。

   federation-mgr_home¥secure-proxy¥proxy-engine¥conf¥defaultagent¥SmHost.conf

5. SmHost.conf ファイルを開き、その中に共有秘密鍵があることと、それに {AES} など、FIPS の承認済みアルゴリズム プレフィックスが付いていることを確認します。

共有秘密鍵の再暗号化が完了します。

ポリシー ストアとキー ストア データの再暗号化

FIPS 互換の暗号化アルゴリズムが使用されるように、ポリシーとキー ストア データを再暗号化します。

ポリシーとキー ストア データを再暗号化するには

1. コマンド プロンプト ウィンドウを開きます。
2. 次のコマンドを入力し、キー データをエクスポートします

   smkeyexport -d*admin_name* -w*admin_password* -o*export_file* -l -v -t -cf

   admin_name

   管理者名を指定します。smkeyexport ユーティリティを使用するときは、この値に「siteminder」を入力する必要があります。

   admin_password

   パスワード CA SiteMinder® Federation Standalone 管理者を指定します。

   export_file

   エクスポートの結果として作成されるファイルの名前を指定します。 このファイルは .smdif 拡張子で終わる必要があります。

3. 次のコマンドを入力し、ポリシー ストア データをエクスポートします。

   XPSExport *export_file* -xa –xs –xc -passphrase *passphrase* -v -e *file_name* -l *log_file*

   export_file

   エクスポートの結果の出力ファイルに名前を付けます。 XPSExport からの出力は XML 形式になります。そのため、ファイル名は拡張 **.xml** で終了する必要があります。

passphrase

機密データを暗号化するのに必要なパスフレーズを指定します。パスフレーズは、8 文字以上で、1 つ以上の数字、1 つ以上の大文字、および 1 つ以上の小文字を含んでいる必要があります。 パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。

注: パスフレーズを直接入力しない場合は、コマンドにそれを指定しないでください。 そうすると、XPSExport によってパスフレーズの入力およびパスフレーズの確認を促すメッセージが表示され、画面に表示されません。

file_name

CA SiteMinder® Federation Standalone がエラー メッセージを書き込むエラー ファイルの名前を指定します。

log_file

CA SiteMinder® Federation Standalone がエクスポートの結果を書き込むログ ファイルの名前を指定します。 このファイルには任意の名前を設定できます。ただし、拡張子 .log が推奨されます。

ファイルへの完全パスを入力するか、ファイル名のみを入力できます。 ファイル名のみを入力する場合、CA SiteMinder® Federation Standalone は XPSExport コマンドを実行している場所にファイルを作成します。 このパラメータに入力する名前は、ポリシー ストア データをインポートするときに入力する log_path 値とは別の名前にする必要があります。

4. 次のコマンドを入力し、新規または既存のキー ストアへキー データをインポートします。

   注: キー ストアとしてポリシー ストアを使用する場合があります。

   smkeyimport -i*export_file* -da*dmin_name* -w*admin_password* -l -v -t -cf

   export_file

   元のストアのエクスポートの結果として作成される XML ファイルの名前を指定します。

   admin_name

   管理者名を指定します。smkeyimport ユーティリティを使用するときは、この値に「siteminder」を入力する必要があります。

   admin_password

   パスワード CA SiteMinder® Federation Standalone 管理者を指定します。

5. 次のコマンドを入力し、新規または既存のポリシー ストアにポリシー ストア データをインポートします。

   XPSImport –fo *export_file* -passphrase *passphrase* -vT -vI -vW -vE -vF -l *log_path*

   export_file

   元の設定のエクスポートの結果の XML ファイルに名前を付けます。

   passphrase

   機密データを復号化するために必要なパスフレーズを指定します。パスフレーズは、前の手順で XPSExport コマンドを実行したときに指定したパスフレーズと同じにする必要があります。

   log_path

   CA SiteMinder® Federation Standalone がインポートの結果を書き込むログ ファイルの場所と名前を指定します。 このファイルには任意の名前を設定できます。ただし、拡張子 .log が推奨されます。

CA SiteMinder® Federation Standalone UI を FIPS_Only モードに設定します

FIPS 互換アルゴリズムを使用するために必要なすべてのデータを再暗号化した後、すべてのパートナーシップと SSL 設定が FIPS 互換であることを確認します。

次の手順に従ってください:

1. オペレーティング環境に応じて、フェデレーション サービスを再起動します。
   - **Windows**

     以下のように、停止および開始ショートカットを使用します。ローカル管理者ではなく、ネットワーク ユーザとしてログインした場合は、ショートカットを右クリックし、［管理者として実行］を選択します。

     a. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの停止］

     b. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの開始］
   - **UNIX**

     a. コマンド ウィンドウを開きます。

     b. 以下のスクリプトを実行します。

     federation_install_dir/fedmanager.sh stop

     federation_install_dir/fedmanager.sh start

     注: root ユーザとしてサービスを停止したり開始したりしないでください。
2. Administrative UI にログインします。
3. ［インフラストラクチャ］、［展開設定］に移動します。

   ［展開の設定］ダイアログ ボックスが表示されます。

4. ［展開設定］セクションの［確認］ボタンがアクティブになっていること、メッセージ［システムは、FIPS 専用モードへの移行準備ができています］が［はい］に設定されていることを確認します。

   これらの 2 つの条件が満たされない場合、パートナーシップまたは SSL 設定の 1 つまたは複数が FIPS 有効になりません。パートナーシップは次の理由のために FIPS 有効ではありません。

   - ［アプリケーション統合］ダイアログ ボックスの［リダイレクト モード］設定を Agent for Open Files と PBE アルゴリズムに設定しています。

     Agent for Open Files と PBE 暗号化アルゴリズムを使用するように［リダイレクト モード］設定を構成した場合、モードは FIPS 互換になりません。

   - プロビジョニングの配信タイプをオープン形式の Cookie と PBE アルゴリズムに設定しています。

     Agent for Open Files と PBE 暗号化アルゴリズムを使用するようにプロビジョニング配信タイプを設定した場合、その配信メカニズムは FIPS 互換になりません。

   - 代理認証のグローバル オープン形式 Cookie 設定を PBE アルゴリズムに設定しています。

     PBE 暗号化アルゴリズムを使用するように［展開設定］ダイアログ ボックスのオープン形式の Cookie を構成した場合、Cookie は FIPS 互換になりません。

   これらの問題を修正するには、次を実行します。

   - FIPS ではないパートナーシップがある場合、そのようなパートナーシップを非アクティブ化するか、そのようなすべてのパートナーシップで FIPS 承認済み証明書と暗号化アルゴリズムが使用されることを確認します。
   - SSL 設定が FIPS 承認ではない場合は、SSL を非アクティブ化し、FIPS 承認済み証明書を使用してそれを再設定します。

5. ［確認］をクリックし、UI を FIPS_ONLY モードに移行します。

これで Administrative UI は FIPS_ONLY モードで作動します。

セキュア プロキシ エンジンを FIPS_Only モードに設定します

移行プロセスの一部として、セキュア プロキシ エンジンを FIPS_Only モードに設定します。

セキュア プロキシ エンジンを FIPS_Only に設定するには

1. コマンド ウィンドウを開きます。
2. *federation-manager_home*¥secure-proxy¥proxy-engine¥conf¥defaultagent¥SmHost.conf に移動します。
3. テキスト エディタで SmHost.conf ファイルを開きます。
4. fipsmode 設定を MIGRATE から ONLY に変更します。

   例： fipsmode="ONLY"

これでプロキシ エンジンは FIPS_Only モードで作動します。

ポリシー エンジンを FIPS_Only モードに設定します

移行プロセスの最後の手順は、ポリシー エンジンを FIPS_Only モードに設定することです。

次の手順に従ってください:

1. （Solaris のみ） CA SiteMinder® Federation Standalone 環境スクリプトの ca_federation_env.ksh を用意し、適切な環境変数を設定します。
2. コマンド プロンプトから、次のように setFIPSmigration コマンドを実行します。

   Windows

   「setFIPSonly」を入力します

   UNIX

   a. *federation_install_dir*¥secure-proxy に移動します。
   b. 「setFIPSonly.ksh」を入力します。
   c. 環境スクリプトの ca_federation_env.ksh を実行し、環境変数を設定します。

   コマンドが成功すると、「FIPS_ONLY」という言葉がコマンド プロンプトに表示されます。

3. 以下のいずれかを実行します。

   Windows

   フェデレーション システムを再起動します。

   UNIX

   コマンド ウィンドウからの次のスクリプトを実行し、フェデレーション サービスを再起動します。

   a. *federation_install_dir*/fedmanager.sh stop

   b. *federation_install_dir*/fedmanager.sh start

4. ポリシー エンジンが FIPS_ONLY モードで作動していることを確認します。ディレクトリ *federation_install_dir*¥logs¥server で smps ログを確認します。

FIPS 互換の SSL 証明書を取得します（任意）

CA SiteMinder® Federation Standalone を FIPS_Only モードに移行すると、フェデレーション システムが SSL 設定に使用するサーバ証明書が FIPS 互換になっている必要があります。システムが SSL に使用しているサーバ証明書が MD5 形式の場合、FIPS 互換である SHA1 アルゴリズムを使用する新しい証明書を取得します。

SSL 証明書を更新する必要があるかどうか判断する方法

1. 現在の SSL 証明書の FIPS ステータスを確認します。

   これらは埋め込み Web サーバと Administrative UI の証明書です。

2. FIPS ステータスが False の場合、新しい証明書をリクエストします。
3. 新しい FIPS 互換のサーバ証明書をアップロードします。

この手順については後述のセクションで説明します。

SSL 証明書の FIPS ステータスを確認します

埋め込み Web サーバと管理 UI の SSL 証明書の FIPS ステータスを確認します。 新しい FIPS 承認済み証明書を必要とするかどうか判断します。

SSL 証明書のステータスを確認する方法

1. Administrative UI にログインします。
2. ［インフラストラクチャ］、［SSL 設定］に移動します。

   ［SSL 設定］ダイアログ ボックスが表示されます。
3. 埋め込み Web サーバと管理 UI の［FIPS 承認済み］フィールドを確認します。 以下のいずれかを実行します。
   - ［FIPS 承認済み］ステータスが True の場合、何のアクションも必要ありません。
   - ステータスが False の場合、次の手順に基づき、FIPS 承認済み証明書を取得します。

FIPS 互換サーバ証明書をリクエストします

埋め込み Web サーバまたは管理 UI の［FIPS 承認済み］設定が False の場合、新しい FIPS 互換証明書をリクエストします。 両方のコンポーネントが新しい証明書を必要とする場合、コンポーネント別にリクエストを生成し、リクエスト プロセス全体を完了します。

FIPS 互換のサーバ証明書をリクエストする方法

1. Administrative UI にログインします。
2. ［インフラストラクチャ］、［SSL 設定］に移動します。

   ［SSL 設定］ダイアログ ボックスが表示されます。
3. 新しい証明書を必要とするコンポーネントの適切なセクションにある［リクエスト］をクリックします。

   ［証明書のリクエスト］ダイアログ ボックスが表示されます。
4. ［証明書のリクエスト］ダイアログ ボックスのフィールドに入力します。

   証明書が FIPS 承認になるように、SHA-1 署名アルゴリズムによる証明書を要求するように求められます。別のアルゴリズムを使用するように求められない限り、一部の CA では MD5 がデフォルトで使用されます。

5. ［保存］をクリックします。

   PKCS#10 形式のファイルが保存されます。

6. 認証機関にファイルをサブミットし、新しい証明書を受け取ります。リクエストをサブミットするための適切な手順については、認証機関に問い合わせてください。

   CA は、署名された証明書を含む応答を送信します。

7. 次の手順に基づき、キー ストアに新しい証明書をアップロードします。
8. 必要に応じて、別のリクエストにこの手順を繰り返します。

FIPS 互換証明書をアップロードします

新しい証明書を取得したら、それょキー ストアにアップロードします。複数の証明書をリクエストした場合、各証明書を別々にアップロードします。

新しい証明書をアップロードする方法

1. ［インフラストラクチャ］、［SSL 設定］に移動します。

   ［SSL 設定］ダイアログ ボックスが表示されます。

2. ［署名された証明書レスポンス］フィールドの隣の［参照］をクリックし、新しい署名されたレスポンス ファイルを探します。

   注: SSL は複数のペアをサポートしないので、SSL 機能にはキーと証明書のペアを 1 つだけ必要とします。

3. ［CA 証明書］フィールドで、プルダウン メニューから SSL 証明書を署名した CA を選択します。

   CA 証明書がキー ストアにない場合は、SSL 証明書リクエストを署名するために使用した CA 証明書のコピーをインポートします。

4. ［インポート］をクリックして証明書をインポートし、インポート手順を完了します。
5. ［適用］をクリックし、CA SiteMinder® Federation Standalone にサーバ証明書をアップロードします。

   確認メッセージが表示されます。そして、［SSL 設定］は証明書が現在更新されたことを反映して変更されます。

6. ［アクティブ化］をクリックし、SSL 設定を再起動します。

   ［FIPS 承認済み］ステータスが True であり、証明書が FIPS 互換であることを示している必要があります。

7. オペレーティング環境に応じて、フェデレーション サービスを再起動します。

   - **Windows**

     以下のように、停止および開始ショートカットを使用します。ローカル管理者ではなく、ネットワーク ユーザとしてログインした場合は、ショートカットを右クリックし、［管理者として実行］を選択します。

     a. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの停止］

     b. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの開始］

   - **UNIX**

     a. コマンド ウィンドウを開きます。

     b. 以下のスクリプトを実行します。

     federation_home/fedmanager.sh stop

     federation_home/fedmanager.sh start

     注: root ユーザとしてサービスを停止したり開始したりしないでください。

これで SSL 設定のサーバ証明書が FIPS 互換になりました。

第 6 章: CA SiteMinder® Federation Standalone をトラブルシューティングする

このセクションには、以下のトピックが含まれています。

インストールに関するトラブルシューティング

インストールと設定で問題が発生した場合、次の情報が解決に役立つ可能性があります。

CA SiteMinder® Federation Standalone ライセンスの取得、またはソフトウェアのダウンロードにともなうトラブル

症状:

CA SiteMinder® Federation Standalone ライセンスの取得や CA SiteMinder® Federation Standalone ソフトウェアのダウンロードで問題が発生しています。

解決方法:

サポートが必要な場合、セールス アカウント マネージャに問い合わせます。

CA SiteMinder® Federation Standalone UI またはコンポーネント サービスが起動しません

症状:

CA SiteMinder® Federation Standalone UI が起動しません。

解決方法:

1. URL のポートとホスト名が正しいことを確認します。
2. オペレーティング環境に応じて、フェデレーション サービスを再起動します。
   - **Windows**

     以下のように、停止および開始ショートカットを使用します。ローカル管理者ではなく、ネットワーク ユーザとしてログインした場合は、ショートカットを右クリックし、［管理者として実行］を選択します。

     a. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの停止］

     b. ［スタート］、［すべてのプログラム］、［CA］、［Federation Standalone］、［サービスの開始］

   - **UNIX**

     a. コマンド ウィンドウを開きます。

     b. 以下のスクリプトを実行します。

     federation_install_dir/fedmanager.sh stop

     federation_install_dir/fedmanager.sh start

注: root ユーザとしてサービスを停止したり開始したりしないでください。

設定マネージャを実行しているときにインストールが失敗します

症状:

設定マネージャを実行すると、CA SiteMinder® Federation Standalone インストールがハングアップまたは失敗します。

解決方法:

データベース サーバ情報が求められたら、完全修飾ホスト名の代わりに、データベース サーバの IP アドレスを入力します。 IP アドレスを使用することで、インストールと設定が正常に完了します。

キー データベース移行をトラブルシューティングする

次のセクションでは、証明書データ ストアにキー データベースを移行する際に発生する問題を解決する方法について詳細に説明します。

SiteMinder キー データベースの移行の状況がわからない

症状：

CA SiteMinder® Federation Standalone がアップグレードされたことはわかっています。ただし、証明書データ ストアに smkeydatabase が問題なく移行されたか不確かです。

解決方法：

smkeydatabase 移行ユーティリティ（smmigratecds）を使用して、移行が成功したことを確認します。

注: このユーティリティのデフォルトの場所は *federation_install_dir*¥siteminder¥bin です。

federation_install_dir

CA SiteMinder® Federation Standalone インストール パスを指定します。

次の手順に従ってください:

1. smkeydatabase が連結されているホスト システムにログインします。
2. 以下のいずれかを実行します。
   - （Windows）コマンド プロンプトを開き、以下のコマンドを実行します。

     ```
     smmigratecds.bat –isComplete
     ```

     -isComplete

     前の移行が成功したことを確認します。
   - （UNIX）シェルを開き、以下のコマンドを実行します。

     ```
     smmigratecds.sh –isComplete
     ```

移行が成功していた場合、システムで移行がすでに成功したことを示すメッセージが表示されます。 移行が失敗していた場合、システムで移行を実行する必要があることを示すメッセージが表示されます。

移行失敗のエラーが表示される

症状:

smkeydatabase 移行が失敗したことを示すメッセージが表示されました。

解決方法:

移行ユーティリティ（smmigratecds）により、smkeydatabase のコンテンツが証明書データ ストアと比較され、1 つ以上のデータ不整合が検出されています。 データ不整合の一例として、別の証明書への同じエイリアスのマッピングがあります。

これらの不整合があると移行は成功しません。

次の手順に従ってください:

1. smkeydatabase 移行ログ（smkeydatabaseMigration.log）を使用して、問題を特定します。

   smmigratecds ユーティリティを実行する場合、ログ ファイルを指定できます。

   ログ ファイルのデフォルトの場所は *federation_install_dir*/siteminder/log です。

   federation_install_dir は CA SiteMinder® Federation Standalone のインストール ディレクトリです。

2. アクセス レガシー キー ストア フラグ（–accessLegacyKS） を含む smkeytool ユーティリティを使用して、smkeydatabase にアクセスします。

3. 移行失敗の原因となったデータ不整合を解決します。

   注: 詳細については、smkeytool を使用する方法を確認してください。

4. キー データベースを手動で移行します。

証明書データ ストアのエラーが表示される

症状：

証明書データ ストアが設定されていないことを示すメッセージが表示されました。

解決方法：

次の手順に従ってください:

1. CA SiteMinder® Federation Standalone ホスト システムにログインします。
2. 以下のコマンドを実行します。

   ```
   XPSDDInstall CDSObjects.xdd
   ```

   ポリシー ストア スキーマが拡張されて、証明書データ ストアをサポートします。

3. 以下のいずれかを実行します。
   - （Windows）コマンド プロンプトを開き、以下のコマンドを実行します。

     ```
     smmigratecds.bat –validateInstall
     ```

     validateInstall

     証明書データ ストアが正しくインストールされているかどうかを確認します。
   - （UNIX）シェルを開き、以下のコマンドを実行します。

     ```
     smmigratecds.sh -validateInstall
     ```

     証明書データ ストアが正しく設定される場合、インストールが有効であることを示すメッセージが表示されます。 証明書データ ストア のインストールが失敗した場合、インストールが有効ではないことを示すメッセージが表示されます。
4. キー データベースを手動で移行します。

手動による SiteMinder キー データベースの移行

症状:

smkeydatabase 証明書データを証明書データ ストアに手動で移行する場合は、以下のようにします。

解決方法:

smkeydatabase 移行ユーティリティ（smmigratecds）を使用します。

次の手順に従ってください:

1. 必ずすべての smkeydatabases インスタンスを同期します。
2. smkeydatabase が連結されているフェデレーション ホスト システムにログインします。

3. 証明書データ ストアが正しく設定されていることを確認するために、以下のいずれかの手順を実行します。

   - （Windows）コマンド プロンプトを開き、以下のコマンドを実行します。

     ```
     smmigratecds.bat –validateInstall
     ```

     -validateInstall

     証明書データ ストアが正しくインストールされているかを検証します。

   - （UNIX）シェルを開き、以下のコマンドを実行します。

     ```
     smmigratecds.sh -validateInstall
     ```

4. smkeydatabase のコンテンツを証明書データ ストアと比較します。 コンテンツの比較によって、移行の成功を妨げるデータの不整合が特定されます。

   オペレーティング プラットフォームの手順に従います。

   - （Windows）以下のコマンドを入力します。

     ```
     smmigratecds.bat –validate -log log_file
     ```

     -validate

     smkeydatabase のコンテンツを証明書データ ストアと比較します。

     -log

     検証結果がログに送信されます。

     log_file

     ログ ファイルの名前と、それがユーティリティによって送信される送信先を指定します。

     例： -log "C:¥FederationStandalone¥logs"

   - （UNIX）以下のコマンドを入力します。

     ```
     smmigratecds.sh -validate -log log_file
     ```

5. （オプション）データの不整合が存在する場合は、ログ ファイルを使って問題を特定します。

6. 以下のいずれかの手順を実行して、移行を開始します。
   - （Windows）以下のコマンドを入力します。

     ```
     smmigratecds.bat -migrate -log log_file -p
     unencrypted_password
     ```

   - （UNIX）以下のコマンドを入力します。

     ```
     smmigratecds.sh -migrate -log log_file -p unencrypted_password
     ```

   コマンド引数は次のアクションを示します。

   -migrate

   smkeydatabase を証明書データ ストアに移行します。

   -log

   移行の実行結果がログに送信されます。

   log_file

   ログ ファイルの名前と、それがユーティリティによって送信される送信先を指定します。

   例：

   -log "C:¥Progam Files¥Sample¥Logs"

   -log export/fed/Sample/Logs"

   -p

   （オプション）。 smkeydatabase パスワードの暗号化されていない値を指定します。smkeydatabase.properties ファイルに格納されたパスワードを復号化できない場合のあらゆる問題を回避するためにこの引数を使用します。

   unencrypted_password

   smkeydatabase の暗号化されていないパスワードを指定します。

7. （オプション）移行が失敗した場合は、ログ ファイルを使用して原因を特定します。

XML 署名ラッピング攻撃から守る

悪意のあるユーザは、署名を無効にせずにドキュメント署名のコンテンツを変更することにより、XML シグネチャ ラッピング攻撃を実行できます。

フェデレーション トランザクションが失敗する場合は、smtracedefault.log ファイルと fwstrace.log ファイルを確認します。 これらのログ ファイルに署名検証失敗が含まれている場合があります。 署名検証の失敗は、次の理由で発生する可能性があります。

- 重複した ID 要素が XML ドキュメントに存在します。重複した ID 属性は許可されません。 署名はこの重複した ID を参照します。
- 署名ラッピングの脆弱性がログ記録されます。たとえば、署名は想定される親要素を参照しません。

署名の脆弱性から守るには：

1. 次のいずれかの場所にある xsw.properties ファイルに移動します。
   - smtracedefualt.log ファイルにエラー メッセージがある場合、*federation_install_dir*/siteminder/config/properties に移動します。
   - fwstrace.log ファイルにエラー メッセージがある場合、*federation_install_dir*/secure-proxy/tomcat/webapps/affwebservices/web-INF/classes に移動します。
2. xsw.properties ファイルに次の設定を追加し、各々を true に設定します。

   DisableXSWCheck=true

   DisableUniqueIDCheck=true
3. ファイルを保存します。

既存システムで JDK をアップグレードします

既存の CA SiteMinder® Federation Standalone システムで JDK をアップグレードする場合、CA SiteMinder® Federation Standalone インストール プログラムを再実行し、アップグレードされた JDK バージョンを指します。

第 7 章: キー ツール参照

キー ツール ユーティリティ（smkeytool）は CDS 移行問題を解決するためにのみ使用します。 他のすべての証明書管理については、CA SiteMinder® Federation Standalone Administrative UI を使用します。

キー ツール ユーティリティ（smkeytool）：

- r12.52 SP1 へのアップグレード/移行時にレガシー smkeydatabase にアクセスできます。証明書データ ストアへの移行が失敗した場合、その原因となっているデータ不整合をすべて解決するために、アクセス レガシー キー ストア フラグ（-accessLegacyKS）を使用します。
- インストールされている場所は以下のとおりです。

  *federation_install_dir/siteminder/*bin

  federation_install_dir

  本製品のインストール パスを指定します。

次の手順に従ってください:

1. コマンド ラインまたはシェルを開きます。
2. 以下のいずれかのコマンドを実行します。
   - （Windows） smkeytool.bat -*option* [-*arguments*]
   - （UNIX） smkeytool.sh -*option* [-*arguments*]

このセクションには、以下のトピックが含まれています。

秘密キーと証明書のペアの追加

addPrivKey オプションを使用して、秘密キー/証明書ペアのみを証明書データ ストアにインポートします。 以下の点を考慮します。

- データ ストア内には、複数の秘密キー/証明書ペアを格納できますが、SiteMinder がサポートするのはストア内の RSA キーのみです。
- 秘密キー/証明書のペアのみが、暗号化されたフォームで格納されます。
- 証明書を作成する側のポリシー サーバで、以下を行います。
  - 単一の秘密キー/証明書のペアを使用して SAML アサーションに署名します。
  - 証明書を使用して、証明書を使用する側から受け取る暗号化 SAML アサーションを復号します。

  通常、キーは証明書データ ストアで見つかる最初の秘密キー/証明書ペアです。

- 証明書メタデータは、インポートする前に証明書ファイルから削除します。「--BEGIN CERTIFICATE --」というマーカで始まり、「--END CERTIFICATE --」というマーカで終わるデータのみをインポートします。以下のマーカを必ず含めるようにしてください。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-alias *alias*

必須です。 データベース内の秘密キー/証明書のペアにエイリアスを割り当てます。 エイリアスは、英数文字のみを含む一意の文字列である必要があります。

-certfile *cert_file*

秘密キー/証明書ペアに関連付けられている証明書の場所のフル パスを指定します。 PKCS1、PKCS5、および PKCS8 の各形式のキーに必須です。

-keyfile *private_key_file*

秘密キー ファイルの場所へのフル パスを指定します。PKCS1、PKCS5、および PKCS8 の各形式のキーに必須です。

-keycertfile *key_cert_file*

秘密キーおよび証明書ペアのデータを含む PKCS12 ファイルの場所へのフル パスを指定します。 PKCS12 形式のキーに必須です。

-password *password*

（オプション）秘密キー/証明書ペアが作成された場合、そのペアの暗号化に使用されたパスワードを指定します。 キー/証明書ペアが証明書データ ストアに書き込まれる前に、そのペアを復号するためにこのパスワードを提供します。

注: このパスワードは証明書データ ストアには格納されません。

キー/証明書ペアが復号され、証明書データ ストアに格納された後、SiteMinder はそのペアをそれ自体のパスワードを使用して再び暗号化します。

証明書の追加

addCert オプションを使用して、公開証明書または信頼された CA 証明書を証明書データ ストアに追加します。

以下の点を考慮します。

- 証明書は、秘密キー/証明書ペアと関連付けられる証明書です。 ただし、証明書のみが証明書データ ストアに追加されます。
- 証明書を認証機関（CA）として信頼する場合、この証明書は常に CA 証明書として処理されます。
- X.509 証明書形式については、V1、V2 および V3 バージョンが SiteMinder ではサポートされています。 エンコード形式については、DER および PEM の各形式が SiteMinder ではサポートされています。
- CA 証明書を追加するときは、Web エージェントを再起動してください。
- 証明書メタデータは、インポートする前に証明書ファイルから削除します。 「--BEGIN CERTIFICATE --」というマーカで始まり、「--END CERTIFICATE --」というマーカで終わるデータのみをインポートします。以下のマーカを必ず含めるようにしてください。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-alias *alias*

必須です。証明書データ ストアの秘密キーと関連付けられた証明書のエイリアスを指定します。

制限： 英数文字のみを含む一意の文字列。

-infile *cert_file*

必須です。新しく追加された証明書の場所へのフル パスを指定します。

- trustcacert

任意です。 追加されるユーザ プロバイダ証明書が CA 証明書であることを確認します。 ユーティリティにより、証明書にデジタル署名拡張子があり、証明書に同じ IssuerDN 値および SubjectDN 値があることが確認されます。

-noprompt

（オプション）証明書の追加の確認を求めるメッセージは表示されません。

破棄情報の追加

addRevocationInfo オプションを使用して、CRL の場所を指定します。 証明書データ ストアは、CRL の場所を参照します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-issueralias *issuer_alias*

必須です。 CRL を発行する認証機関のエイリアスを指定します。

例： -issueralias verisignCA

-type (*ldapcrl* | *filecrl*)

必須です。 CRL が LDAP ベースかファイル ベースかを指定します。

-location *location*

必須です。 CRL の場所を指定します。

- （ファイル ベース）ファイルのフル パスを指定します。

  例： -location c:¥crls¥siteminder_root_ca.crl

- （LDAP ディレクトリ サービス）LDAP サーバ ノードのフル パスを指定します。

  例： -location "http://localhost:880/sn=siteminderroot, dc=crls,dc=com"

破棄情報の削除

deleteRevocationInfo オプションを使用して、証明書データ ストアから CRL を削除します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-issueralias *issuer_alias*

CRL を発行する認証機関の名前を指定します。

-noprompt

（オプション） CRL の削除の確認を求めるメッセージは表示されません。

証明書データの削除

removeAllCertificateData オプションを使用して、証明書データ ストアから証明書データをすべて削除します。

このオプションに対する引数を以下に示します。

-noprompt

（オプション）証明書データの削除の確認を求めるメッセージは表示されません。

証明書の削除

削除オプションを使用して、証明書データ ストアから証明書を削除します。 証明書に秘密キーが関連付けられている場合は、そのキーも削除されます。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-alias <*alias*>

（必須）削除する証明書のエイリアスを指定します。

-noprompt

（オプション）証明書の削除の確認を求めるメッセージは表示されません。

証明書または秘密キーのエクスポート

エクスポート オプションを使用して、証明書または秘密キーをファイルにエクスポートします。

以下の点を考慮します。

- 証明書データは、PEM エンコーディングを使用してエクスポートされます。
- 秘密キー データは、DER エンコードによる PKCS8 形式でエクスポートされます。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-alias *alias*

（必須）エクスポートする証明書またはキーを特定します。

-outfile *out_file*

（必須）データがエクスポートされるファイルへのフル パスを指定します。

-type (key|cert)

（オプション）証明書またはキーのどちらをエクスポートするかを指定します。

デフォルト： 証明書。

-password *password*

秘密キーをエクスポートする場合のみ必須です。エクスポート時に秘密キーの暗号化に使用するパスワードを指定します。公開キーを保持する証明書をエクスポートする場合、パスワードは不要です。これは、証明書はクリア テキストでエクスポートされるためです。

証明書データ ストアにこの秘密キーを追加するには、このパスワードで addPrivKey オプションを使用します。

エイリアスの検索

findAlias オプションを使用して、証明書データ ストアの証明書と関連付けられるエイリアスを検索します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-infile *cert_file*

（必須）検索対象のエイリアスに関連付けられている証明書ファイルへのフル パスを指定します。

-password *password*

パスワードで保護されている P12 ファイルが証明書ファイルとして指定されている場合にのみ必須。

デフォルトの CA 証明書のインポート

importDefaultCACerts オプションを使用して、SiteMinder に含まれるデフォルトの信頼された認証機関の証明書をすべて、証明書データ ストアにインポートします。

このオプションに対する引数を以下に示します。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

すべての証明書のメタデータ リスト

listCerts オプションを使用して、証明書データ ストアに格納されたすべての証明書のメタデータの一部を表示します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-alias *alias*

（オプション）指定した別名に関連付けられている証明書およびキーのメタデータ情報をリストで表示します。

このオプションは、ワイルドカード文字としてアスタリスク（*）をサポートしています。 ワイルドカードの使い方は以下のとおりです。

- エイリアス値の先頭または終わりに挿入する。
- エイリアス値の先頭と終わりに挿入する。

コマンド シェルがワイルドカード文字を解釈しないように、アスタリスクは引用符で囲んでください。

破棄情報リスト

listRevocationInfo オプションを使用して、証明書データ ストア内の証明書廃棄リストの一覧を表示します。 以下の項目が表示されます。

- CRL 名。
- CRL はファイル ベースか LDAP ベースかを指定します。
- CRL の場所。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-issueralias *issuer_alias*

（オプション）CRL を発行する認証機関の名前。

このオプションは、ワイルドカード文字としてアスタリスク（*）をサポートしています。 ワイルドカードの使い方は以下のとおりです。

- エイリアス値の先頭または終わりに挿入する。
- エイリアス値の先頭と終わりに挿入する。

コマンド シェルがワイルドカード文字を解釈しないように、アスタリスクは引用符で囲んでください。

証明書メタデータの表示

printCert オプションを使用して、指定された証明書のメタデータの一部を表示します。 このコマンドは、証明書プロパティの表示が難しいシステムで有効です。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-infile *cert_file*

必須です。 証明書ファイルの場所。

-password *password*

パスワードで保護されている P12 ファイルが証明書ファイルとして指定されている場合にのみパスワードが必須です。

エイリアス名の変更

renameAlias オプションを使用して、証明書と関連付けられるエイリアスの名前を変更します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-alias *current_alias*

（必須）証明書と関連付けられるエイリアスを指定します。

-newalias *new_alias*

（必須）新規エイリアスを指定します。

制限： 英数文字のみを含む一意の文字列である必要があります。

証明書の検証

validateCert オプションを使用して、証明書を廃棄するかどうかを決定します。

このオプションに対する引数には、以下が含まれます。

-accessLegacyKS

オプションがレガシー smkeydatabase に適用されることを指定します。この引数を指定しない場合、オプションは r12.52 SP1 証明書データ ストアに適用されます。

-alias *alias*

（必須）証明書データ ストアの秘密キーと関連付けられた証明書のエイリアスを指定します。

制限： 英数文字のみを含む一意の文字列である必要があります。

-infile *crl_file*

（オプション）ユーティリティで、検証する証明書を検索する CRL を指定します。