CA Advanced Authentication

アップグレード ガイド

8.0

ca technologies

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。

目次

第 1 章: CA Advanced Authentication のアップグレード

このガイドでは、CA Advanced Authentication をアップグレードする方法について説明します。

このセクションには、以下のトピックが含まれています。

アップグレード元のバージョン

以下のいずれかのリリースからリリース 8.0 にアップグレードできます。

- *（Strong Authentication）* 6.2.9 または 7.x
- （Risk Authentication） 2.2.9 または 3.x

  重要: ここに記載されている Strong Authentication および Risk Authentication のリリースがない場合、必要なパッチを適用してこれらのリリースのいずれかにアップグレードする必要があります。 その後、アップグレードを続行します。

パッチ アップグレードについては、該当するリリース ノートを参照してください。

注:

- 古い Java SDK クライアントは、Strong Authentication サーバの新しいインストールでも動作します。クライアント コードを変更する必要は*ありません*。
- 古い WSDL は、Strong Authentication サーバの新しいインストールでも動作します。 クライアント コードを変更する必要は*ありません*。

アップグレードに必要なデータベース権限

以下の表に、アップグレードに関連して実行する必要があるデータベース権限のリストを示します。

Database Type	アップグレード権限	実行時権限
Oracle	CREATE TABLE	CREATE TABLE
	CREATE ANY INDEX	DML 権限
	CREATE ANY SEQUENCE	
	CREATE TABLESPACE （*レポートの場合*）	
	CREATE PROCEDURE	
	UNLIMITED TABLESPACE （*レポートの場合、オプション*）	
	DROP TABLESPACE	
	ALTER ANY TABLE	
	ALTER TABLESPACE	
	DML 権限 （CREATE SESSION 権限を含む）	
MS SQL Server **注**: UserID には ddladmin のデータベース ロールも設定されている必要があります。	CREATE TABLE	CREATE TABLE
	CREATE INDEX	DML 権限
	CREATE PROCEDURE	
	EXECUTE PROCEDURE	
	REFERENCES	
	ALTER TABLE	
	DML 権限	
IBM DB2	CREATE TABLE	CREATE TABLE
	CREATE INDEX	DML 権限
	CREATE SEQUENCE	
	CREATE TABLESPACE	
	CREATE TABLESPACE with AUTORESIZE = yes （*レポートの場合、オプション*）	

Database Type	アップグレード権限	実行時権限
	CREATE PROCEDURE (SQL - ネイティブ)	
	ALTER TABLE	
	DML 権限	

Windows 上の Strong Authentication をアップグレードする方法

8.0 リリースにアップグレードするには、以下の手順に従います。

1. アップグレード前のタスクの実行 (P. 10)
2. リリース 8.0 へのアップグレードの準備 (P. 12)
3. 共通コンポーネント用のリリース 8.0 へのデータベースの移行 (P. 13)
4. Strong Authentication コンポーネント用のリリース 8.0 へのデータベースの移行 (P. 16)
5. Strong Authentication の既存のリリースのアンインストール (共有) (P. 18)
6. 既存の Strong Authentication が単一システムまたは分散システムに展開されているかどうかに応じて、以下のいずれかのセクションで説明されている手順を実行します。
   - 単一システムへの Strong Authentication の再インストール (P. 20)
   - 分散システムへの Strong Authentication の再インストール (P. 21)
7. アップグレード中、Strong Authentication サーバの起動時に警告が表示される場合、およびトランザクションが失敗する場合は、「*(エラーの場合のみ) 初期設定への復帰*」に示されている手順を実行します。
8. アップグレード後のタスクの実行 (共有) (P. 22)

アップグレード前のタスクの実行

このセクションでは、アップグレード前に実行する手順について説明します。

重要: Strong Authentication が分散システムに展開されている場合は、Strong Authentication サーバがインストールされているシステムでアップグレードを実行します。

次の手順に従ってください:

1. 以下のサーバをシャットダウンします。
   - Strong Authentication サーバ
   - CA Advanced Authentication およびユーザ データ サービスが展開されているアプリケーション サーバ。
2. システムに JDK がインストールされていることを確認します。 JDK のバージョンについては、「*プラットフォーム サポート マトリックス* https://support.ca.com/phpdocs/7/8190/adv_authentication_platform_support_matrix.pdf?intcmp=searchresultclick&resultnum=5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。
3. アップグレード プロセスの間、データベースが利用可能であることを確認します。
4. アップグレードを実行するデータベースでレプリケーションが設定されていないことを確認します。アップグレードの前にデータベース レプリケーションを無効にします。
5. 新しいディレクトリに既存の ARCOT_HOME ディレクトリの内容をコピーします。

   注: ここでは、ARCOT_HOME は、既存の Strong Authentication のインストールで作成されたディレクトリ構造全体を含むベース ディレクトリを指します。 通常、リリース 6.0 より前のリリースでは、ARCOT_HOME は *<install_location>*¥Common Files¥Arcot Shared¥ を指します。 リリース 6.x 以降は、ARCOT_HOME は *<install location>*¥Arcot Systems を指します。

   新しいディレクトリに %ARCOT_HOME% のすべての内容をコピーします。 このディレクトリは ARCOT_HOME_BACKUP として参照されます。
6. テキスト エディタで %ARCOT_HOME%¥conf¥arcotcommon.ini ファイルを開き、以下の手順に従います。

a. プライマリ データベースの詳細が正しいことを確認します。 アップグレード ツールは、このファイルに設定されているデータベースを使用します。

b. バックアップ データベースを設定している場合は、以下のプロパティがある行をコメントアウトして、バックアップ データベースを無効にします。 これらのプロパティは、arcotcommon.ini ファイルの arcot¥db¥backupdb セクションにあります。

- URL.1
- AppServerConnectionPoolName.1
- Username.1

a. 現在のバージョンが 6.2.9 である場合は、arcotcommon.ini ファイルに以下のセクションを含めます。

- [arcot/crypto/device]
- HSMDevice=S/W

a. arcotcommon.ini ファイルを保存して閉じます。

7. IBM DB2 でリリース 6.0 からアップグレードする場合は、SYSTEM TEMPORARY テーブルスペースのページ サイズを 16K 以上に設定します。 詳細については、データベース ベンダーのドキュメントを参照してください。

8. Strong Authentication スキーマを含むデータベースをバックアップします。

9. DBA に相談して、データベース ボリューム要件に応じてデータベースを設定します。

10. Strong Authentication をアップグレードするための十分なデータベース権限があることを確認します。

11. 以前のリリースから LDAP リポジトリにユーザの詳細を保存している場合は、LDAP サーバがアップグレード プロセスの間、利用可能であることを確認します。

12. %ARCOT_HOME% 環境変数が、Strong Authentication がインストールされているディレクトリに設定されていることを確認します。

13. この Strong Authentication インストールにプラグインを登録している場合は、Strong Authentication スタートアップ ログを保存します。 このファイルは %ARCOT_HOME%¥logs¥ ディレクトリにあり、プラグインの詳細が含まれています。 アップグレード後、プラグインを再コンパイルします。

アップグレードの準備

このセクションでは、Strong Authentication のアップグレードを開始する前に実行するタスクについて説明します。

次の手順に従ってください:

1. 以下の場所で入手可能な Microsoft Visual C++ 2010 SP1 再頒布可能パッケージをダウンロードします。

   http://www.microsoft.com/en-us/download/details.aspx?id=8328

2. アプリケーション サーバ接続プールが既存の Strong Authentication 展開で使用されている場合は、以下の手順に従って securestore.enc ファイル内のデータベースの詳細を更新します。

   a. コマンド プロンプト ウィンドウを開きます。

   b. DBUtil が使用可能な以下の場所に作業ディレクトリを変更します。
   `%ARCOT_HOME%¥tools¥win`

   c. プライマリ データベースに対して以下のコマンドを実行します。
   `DBUtil -pi <DB_username> <DB_password>`

3. SSL を使用するようにデータベース通信を設定する場合は、以下の手順に従って securestore.enc ファイル内のデータベースの詳細を更新します。

   a. コマンド プロンプト ウィンドウを開きます。

   b. DBUtil が使用可能な以下の場所に作業ディレクトリを変更します。
   `%ARCOT_HOME%¥tools¥win`

   c. データベースで SSL 通信が有効な場合は、以下のようにトラスト ストア パスワードを設定します。
   `DBUtil -pi TrustStorePath.1 <truststore-password>`

共通コンポーネント データベースの移行

Strong Authentication が使用する共通コンポーネント データベースを移行するには、以下の手順に従います。

次の手順に従ってください:

1. アップグレードするシステム上の一時的な場所にアップグレード ディレクトリをコピーします。

   このフォルダには、この移行パスに適用可能な以下の ZIP ファイルが含まれます。

   - ca-common-upgrade-1.0.x-2.0.zip
   - ca-strongaauth-upgrade-6.2.9-or-7.x-8.0 .zip

   重要: ! Risk Authentication がすでに 8.0 にアップグレードされている場合、または現在の Strong Authentication のバージョンが 7.x である場合、または現在の Risk Authentication のバージョンが 3.x である場合は、手順 2 ～ 12 を無視します。

2. 以下のディレクトリに ca-common-upgrade-1.0.x-2.0.zip ファイルをコピーします。
   %ARCOT_HOME%
3. このディレクトリで、ca-common-upgrade-1.0.x-2.0.zip ファイルの内容を抽出します。
4. %ARCOT_HOME%¥tools¥common¥**upgrade¥** ディレクトリに移動します。

   このディレクトリで、arcot-common-db-upgrade zip ファイルの内容を抽出します。
5. 以下の方法で、同じ名前のデータベースに対応するデータベース jar ファイルを %ARCOT_HOME%¥tools¥common¥upgrade¥**lib¥** ディレクトリにコピーします。

   - **Oracle データベース：** ojdbc.jar
   - **Microsoft SQL Server：** sqljdbc.jar
   - **IBM DB2 UDB：** db2jcc.jar

   注: Oracle データベースと IBM DB2 UDB の場合は、使用しているデータベースに適用可能な JDBC JAR バージョンを使用します。 Microsoft SQL Server の場合は、sqljdbc4.0 （SQL Server 用の Microsoft JDBC ドライバ 4.0）を使用します。

6. 既存のインストールで使用されている JAVA_HOME を見つけます。アップグレード ツールを実行する場合は、同じ JAVA_HOME または最近のサポートされているバージョンの JAVA_HOME を使用することを確認します。
7. ArcotAccessKeyProvider.dll 共有ライブラリがアプリケーション サーバで設定されていることを確認します。 このファイルを <*アプリケーション サーバで使用する JAVA_HOME*>¥jre¥bin¥ フォルダにコピーします。
8. PATH 変数に、ArcotAccessKeyProvider.dll がコピーされるディレクトリを含めます。
9. コマンド プロンプト ウィンドウを開きます。
10. 作業ディレクトリを以下に変更します。
    `%ARCOT_HOME%¥tools¥common¥upgrade¥`
11. 以下のコマンドを使用して、arcot-common-upgrade-framework.jar ファイルを実行します。
    `java [JVM_Options] -jar arcot-common-upgrade-framework.jar [--log-file <log-file-name>] [--log-level <log-level>][--commit-batch-size <batch_size>] [--product-name common][--prompt][--mst]`

    以下の表に、この JAR でサポートされているオプションの説明を示します。

オプション	説明
JVM-Options	以下の JVM オプションは、LDAP 組織が設定されている場合のみ必要です。 ■ **-Xmx1024m**： 最大ヒープ サイズを 1 GB に設定します。 100,000 人を超えるユーザが設定済みの LDAP に存在する場合は、ヒープ サイズを 2,048 MB （2 GB）に増やすことを強く推奨します。 ■ **-Dcom.arcot.ldap.migration.timeout=<duration>**： LDAP 組織の移行が失敗としてマークされるまでの時間（分単位）。 100,000 人のユーザの LDAP 移行のタイムアウトは、約 240 分（4 時間）です。 ただし、使用しているハードウェア構成のタイプによって異なります。このパラメータのデフォルト値は 240 分です。

オプション	説明
log-file	ログ ファイルへのパスを指定します。 ■ 値を指定しない場合、arcot_common_upgrade.log ファイルは %ARCOT_HOME%¥logs¥ ディレクトリに作成されます。 ■ 絶対パスを指定すると、ログ ファイルは指定した場所に作成されます。 ■ ファイル名を指定すると、ログ ファイルは指定したファイル名で %ARCOT_HOME% に作成されます。
-log-level	ログ レベルを指定します。 値を指定しない場合、アップグレード ログ レベルは INFO に設定されます。
commit-batch-size	COMMIT ステートメントが発行される前に、データベースに発行されるトランザクションの数を指定します。
product-name	移行する必要がある製品の名前を指定します。 デフォルト値は common です。
prompt	各段階が正常に完了した後に、先に進むかどうかを確認するためのプロンプトを表示します。 後でツールを実行して、停止した場所から続行することを選択できます。 このオプションを指定しない場合、アップグレード ツールは、アップグレード プロセスが完了するまでプロンプトを表示せずに実行されます。
mst	Monitoring Sleep Time（スリープ時間のモニタ）を意味します。このオプションを指定すると、アップグレード ツールは、指定した期間（分単位）スリープした後にアップグレード中の進捗状況を示す診断メッセージを出力します。デフォルト値は 2 分です。

12. ログ ファイル（デフォルト ファイルは、%ARCOT_HOME%¥logs¥arcot_common_upgrade.log）を確認して、共通データベースのアップグレードが成功したことを確認します。

アップグレード ツールは検証情報も出力します。

重要: データベースの移行中にエラーが発生した場合は、以前に作成したデータベース バックアップをリストアしてください。データベースが正しくリストアされたことを確認した後、この手順全体を再試行します。

Strong Authentication データベースの移行

共通コンポーネント用のデータベースをアップグレードした後、Strong Authentication コンポーネント用のデータベースをアップグレードします。

次の手順に従ってください:

1. %ARCOT_HOME% ディレクトリで、ca-strongaauth-upgrade-6.x-or-7.x-8.0.zip を解凍します。
2. コマンド プロンプト ウィンドウを開きます。
3. 作業ディレクトリを以下のディレクトリに変更します。
   `%ARCOT_HOME%¥ca-strongaauth-upgrade-6.x-or-7.x-8.0¥tools¥win32¥`
4. 以下のコマンドを実行します。
   `wfupgrade.exe -migrate`

   このコマンドは、6.x、7.x、または 8.0 の設定データを、以前のデータベース テーブルから 8.0 のテーブルに移行します。

   wfupgrade ツールは、%ARCOT_HOME%¥logs¥ ディレクトリに ca-strongaauth-8.0-upgrade.log ファイルを生成します。

   重要: wfupgrade アップグレード ツールは、Strong Authentication サーバがインストールされているシステムから実行してください。
5. テキスト エディタでログ ファイルを開き、FATAL または WARNING メッセージが含まれていないことを確認します。

   重要: 移行中にエラーが発生した場合は、以前に作成したデータベース バックアップをリストアしてください。データベースが正しくリストアされたことを確認した後、データベースの移行手順を再試行します。

サーバ接続プールの設定の更新

アプリケーション サーバ接続プールが使用されている場合、またはデータベースとの接続で SSL が設定されている場合は、以下の手順を実行します。

次の手順に従ってください:

1. 既存の展開でアプリケーション サーバ接続プールが使用されている場合は、以下の手順に従って、securestore.enc ファイル内のデータベースの詳細を更新します。
   a. DBUtil が使用可能な以下の場所に作業ディレクトリを変更します。
      `%ARCOT_HOME%¥tools¥win`
   b. プライマリ データベースに対して以下のコマンドを実行します。
      `DBUtil -pi <DB_username> <DB_password>`
2. データベースとの接続で SSL が設定されている場合は、以下の手順に従って、securestore.enc ファイル内のデータベースの詳細を更新します。
   a. DBUtil が使用可能な以下の場所に作業ディレクトリを変更します。
      `%ARCOT_HOME%¥tools¥win`
   b. データベースで SSL 通信が有効になっている場合は、トラスト ストア パスワードを以下のように設定します。
      `DBUtil -pi TrustStorePath.1 <truststore-password>`

Strong Authentication コンポーネントの既存のリリースのアンインストール

Strong Authentication の既存のリリースをアンインストールし、アプリケーション サーバにインストールされている CA Advanced Authentication および UDS を展開解除します。

注: このセクションで示されている手順がアンインストール オプションと一致しない場合は、Strong Authentication の既存リリースのインストール ガイドに記載されているアンインストール手順に従ってください。

次の手順に従ってください:

1. 以下の手順に従って、既存の Strong Authentication をアンインストールします。
   a. Strong Authentication サーバを停止します。
   b. 次の手順に従って DSN エントリを削除します。
      a. ［コントロール パネル］-［管理ツール］に移動します。
      b. ［データ ソース (ODBC)］を開きます。
      c. ［システム DSN］タブをクリックします。
      d. 目的の DSN を選択し、［削除］をクリックします。
   c. 該当する INI ファイルがエディタで開かれていないことを確認します。
   d. %ARCOT_HOME%¥Uninstall_Arcot WebFort¥ ディレクトリに移動します。
   e. Uninstall Arcot WebFort.exe ファイルをダブルクリックします。
   f. ［Complete Uninstall］を選択します。
   g. ［Done］をクリックしてアンインストールを完了します。
2. <install_location>¥Arcot Systems¥ フォルダを削除します。
3. アプリケーション サーバから以下の Web アプリケーションをアンインストールします。
   - arcotadmin： 管理コンソール
   - arcotuds： ユーザ データ サービス
   - webfort-7.1.01-sample-application： サンプル アプリケーション

   注: Strong Authentication の分散システム展開の場合は、特定のアプリケーションを展開したシステム上でこれらのファイルを探します。

4. アプリケーション サーバから CA Advanced Authentication およびユーザ データ サービス WAR ファイルを展開解除します。

   アプリケーション サーバのキャッシュをクリアします。

5. Zero G Registry フォルダが削除されていることを確認します。 この非表示フォルダは、インストール時に %ARCOT_HOME% フォルダの親フォルダに作成されます。

Strong Authentication の再インストール

Strong Authentication を単一システムに展開しているか、または分散システムに展開しているかに応じて、以下のいずれかのセクションで説明されているタスクを実行します。

- 単一システムへの Strong Authentication の展開
- 分散システムへの Strong Authentication の展開

単一システムに Strong Authentication を再インストールする方法

単一システムに Strong Authentication を再インストールするには、以下の手順に従います。

重要: 以下のセクションの情報は、Strong Authentication の新規インストールに適用されます。

アップグレード操作中に事前に移行したデータベースを使用します。 古いリリースがインストールされているのと同じ場所に Strong Authentication をインストールします。 別の場所にインストールすると、Strong Authentication サーバが起動 *しません*。

次の手順に従ってください：

1. Complete インストールの実行
2. データベースのセットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication の確認
6. Strong Authentication サーバの起動
7. インストールの確認

   注: サーバの起動中、またはインストールの確認中に警告が表示される場合、およびトランザクションが失敗する場合、アップグレードは正常に実行されていません。 「アップグレード時の問題のトラブルシューティング」に記載されている情報を使用します。 それでも解決できない場合は、「初期設定への復帰」の手順に従って初期設定に戻すことができます。
8. ユーザ データ サービスの展開
9. サンプル アプリケーションの展開
10. サンプル アプリケーションの使用
11. CA Adapter 2.2.7 用の追加設定の実行
12. インストール後のチェックリスト

分散システムに Strong Authentication を再インストールする方法

分散システムに Strong Authentication を再インストールするには、以下のセクションで説明されているタスクを実行します。

重要:

これらのセクションの情報は、分散システムへの Strong Authentication を展開、および Windows への Strong Authentication のインストールに適用されます。

アップグレード中に事前に移行したデータベースを使用します。 古いリリースがインストールされているのと同じ場所に Strong Authentication をインストールします。別の場所にインストールすると、Strong Authentication サーバが起動しません。

次の手順に従ってください：

1. 1 つ目のシステムへのインストール
2. データベースのセットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication の確認
6. CA Advanced Authentication へのログイン
7. Strong Authentication サーバの起動
8. インストールの確認
9. ユーザ データ サービスの展開
10. 2 つ目のシステムへのインストール
11. サンプル アプリケーションの展開
12. Strong Authentication サーバとの通信用サンプル アプリケーションの設定
13. サンプル アプリケーションの使用
14. CA Adapter 2.2.7 用の追加設定の実行

アップグレード後のタスクの実行

以下のアップグレード後のタスクを実行します。

- バックアップ データベースを無効にした場合は、%ARCOT_HOME%¥conf¥arcotcommon.ini ファイルの arcot/db/backupdb セクションを編集して有効にし、バックアップ データベースとプライマリ データベースを同期します。アップグレードの前にデータベース レプリケーションを無効にした場合は、アップグレード後、バックアップ データベースのレプリケーションを有効にします。
- アップグレードの前にこの Strong Authentication インストールにプラグインを登録していた場合は、プラグインを再コンパイルします。 再コンパイルしたファイルの名前が以前と同じであることを確認します。アップグレードの前に保存した Strong Authentication スタートアップ ログを使用して、プラグインの詳細を確認します。
- Strong Authentication のマルチバイト文字または国際化のサポートを必要とし、使用しているデータベースが現在マルチバイト データをサポートしていない場合は、マルチバイト データをサポートする文字セットにデータベースを移行します。 詳細については、「*CA Strong Authentication インストールおよび展開ガイド (Microsoft Windows 用)*」の「データベース サーバの設定」を参照してください。

アップグレード パスが 6.x または 7.x から始まる場合は、CA Advanced Authentication を使用して、以下の設定を行います。

- 以前のすべての認証設定に対して、グローバル レベルで新しい認証ポリシーを作成します。

  詳細については、「CA Strong Authentication Administration Guide」の「Managing Global Strong Authentication Configurations」の章の「Configuring Policies and Profiles」を参照してください。
- RADIUS 設定を新規作成します。

  詳細については、「*CA Strong Authentication 管理ガイド*」の「RADIUS のための Strong Authentication の設定」を参照してください。
- 以下の Strong Authentication サーバ インスタンス設定をセットアップします。
  - データベース接続の設定
  - ログ ファイルの設定

詳細については、「*CA Strong Authentication 管理ガイド*」の「サーバ インスタンスのセットアップ」を参照してください。

- プロトコルごとのスレッド設定をセットアップします。

  詳細については、「*CA Strong Authentication 管理ガイド*」の「通信プロトコルの設定」を参照してください。

- ASSP 設定を作成します。

  詳細については、「*CA Strong Authentication 管理ガイド*」の「グローバルな Strong Authentication 設定の管理」の章の「ASSP の設定」を参照してください。

- （オプション） CA AuthID の猶予期間を設定します。 設定するには、CA AuthID ポリシーの［**認証の成功を許可**］フィールドを設定します。

  詳細については、「*CA Strong Authentication 管理ガイド*」の「ポリシーおよびプロファイルの設定」を参照してください。

- （オプション） Q&A 認証情報の呼び出し元検証を有効にします。 有効にするには、Q&A ポリシーの［**コール元検証の有効化**］フィールドを設定します。

  詳細については、「*CA Strong Authentication 管理ガイド*」の「ポリシーおよびプロファイルの設定」を参照してください。

UNIX 上の Strong Authentication をアップグレードする方法

以下のプロセスでは、UNIX 上の Strong Authentication をアップグレードする方法について説明します。

1. アップグレード前のタスクの実行 (P. 24)
2. 共通コンポーネント データベースの移行 (P. 26)
3. Strong Authentication データベースの移行 (P. 29)
4. 移行後のタスクの実行
5. サーバ接続プールの設定の更新 (P. 30)
6. 既存リリースのアンインストール (P. 31)
7. Strong Authentication の再インストール (P. 32)
   - 単一システムへの Strong Authentication の再インストール
   - 分散システムへの Strong Authentication の再インストール
8. アップグレード後のタスクの実行 (P. 35)

アップグレード前のタスクの実行

このセクションでは、アップグレード前の手順を示します。

重要: Strong Authentication が分散システムに展開されている場合は、Strong Authentication サーバがインストールされているシステムでアップグレードを実行します。

次の手順に従ってください:

1. 以下のサーバをシャットダウンします。
   - Strong Authentication サーバ
   - CA Advanced Authentication およびユーザ データ サービスが展開されているアプリケーション サーバ。
2. システムに JDK がインストールされていることを確認します。 JDK のバージョンについては、「*プラットフォーム サポート マトリックス* https://support.ca.com/phpdocs/7/8190/adv_authentication_platform_support_matrix.pdf?intcmp=searchresultclick&resultnum=5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。
3. アップグレード プロセスの間、データベースが利用可能であることを確認します。
4. アップグレードを実行するデータベースでレプリケーションが設定されていないことを確認します。アップグレードの前にデータベース レプリケーションを無効にします。
5. 新しいディレクトリに既存の ARCOT_HOME ディレクトリの内容をコピーします。

   ARCOT_HOME は、ディレクトリ構造全体のベース ディレクトリを表しています。 **例：** ARCOT_HOME は *<install_location>*/arcot/ を指しています。

   新しいディレクトリに $ARCOT_HOME のすべての内容をコピーします。このディレクトリは ARCOT_HOME_BACKUP として参照されます。

6. テキスト エディタで $ARCOT_HOME/conf/arcotcommon.ini ファイルを開き、以下の手順に従います。

   a. プライマリ データベースの詳細が正しいことを確認します。 アップグレード ツールは、このファイルに設定されているデータベースを使用します。

   b. バックアップ データベースを設定している場合は、以下のプロパティがある行をコメントアウトして、バックアップ データベースを無効にします。 これらのプロパティは、arcotcommon.ini ファイルの arcot/db/backupdb セクションにあります。

      - URL.1
      - AppServerConnectionPoolName.1
      - Username.1

   c. 現在のバージョンが 6.2.9 である場合は、arcotcommon.ini ファイルに以下のセクションを含めます。

      ```
      [arcot/crypto/device]
      HSMDevice=S/W
      ```

7. IBM DB2 でリリース 6.0 からアップグレードする場合は、SYSTEM TEMPORARY テーブルスペースのページ サイズを 16K 以上に設定します。 詳細については、データベース ベンダーのドキュメントを参照してください。

8. Strong Authentication スキーマを含むデータベースをバックアップします。

9. DBA に相談して、データベース ボリューム要件に応じてデータベースを設定します。

10. Strong Authentication をアップグレードするための十分なデータベース権限があることを確認します。

11. 以前のリリースの LDAP リポジトリにユーザの詳細を保存している場合は、LDAP サーバがアップグレード プロセスの間、利用可能であることを確認します。

12. $ARCOT_HOME 環境変数が、Strong Authentication がインストールされているディレクトリに設定されていることを確認します。

13. このインストールにプラグインを登録している場合は、スタートアップ ログを保存します。 このファイルは $ARCOT_HOME/logs/ ディレクトリにあり、プラグインの詳細が含まれています。アップグレード後、プラグインを再コンパイルします。

共通コンポーネント データベースの移行

Strong Authentication が使用する共通コンポーネント データベースを移行するには、以下の手順に従います。

次の手順に従ってください:

1. アップグレードするシステム上の一時的な場所にアップグレード ディレクトリをコピーします。

   このフォルダには、この移行パスに適用可能な以下の ZIP ファイルが含まれます。

   - ca-common-upgrade-1.0.x-2.0.zip
   - ca-strongaauth-upgrade-6.2.9-or-7.x-8.0 .zip

   重要: Risk Authentication がすでに 8.0 にアップグレードされている場合、または現在の Strong Authentication のバージョンが 7.x である場合、または現在の Risk Authentication のバージョンが 3.x である場合は、手順 2 ～ 12 を無視します。

2. ca-common-upgrade-1.0.x-2.0.zip ファイルを $ARCOT_HOME ディレクトリにコピーします。
3. このディレクトリで、ca-common-upgrade-1.0.x-2.0.zip ファイルの内容を抽出します。
4. 以下のディレクトリに移動します。
   `%ARCOT_HOME%/tools/common/upgrade/`

   このディレクトリで、arcot-common-db-upgrade zip ファイルの内容を抽出します。
5. 以下に示されているファイル名の、各データベース用のデータベース jar ファイルを、**%ARCOT_HOME%/tools/common/upgrade/lib/** ディレクトリにコピーします。

   - **Oracle データベース：** ojdbc.jar
   - **Microsoft SQL Server：** sqljdbc.jar
   - **IBM DB2 UDB：** db2jcc.jar

   注: Oracle データベースと IBM DB2 UDB の場合は、使用しているデータベースに適用可能な JDBC JAR バージョンを使用します。 Microsoft SQL Server の場合は、sqljdbc4.0 （SQL Server 用の Microsoft JDBC ドライバ 4.0）を使用します。

6. libArcotAccessKeyProvider.so ファイルを *<アプリケーション サーバで使用する JAVA_HOME>*/jre/sbin にコピーします。 例： Strong Authentication リリース 6.x では、libArcotAccessKeyProvider.so ファイルは *<ARCOT_HOME>*/java/ext/*<プラットフォーム名>/<32bit または 64bit>* にあります。
7. $ARCOT_HOME/java/lib/arcot-crypto-util.jar ファイルを以下の場所にコピーします。

   コピー先：
   `JAVA_HOME-used-by-App-Server/jre/lib/ext`
8. LD_LIBRARY_PATH を、libArcotAccessKeyProvider.so をコピーしたディレクトリに設定してエクスポートします。
9. 作業ディレクトリを以下に変更します。
   `$ARCOT_HOME/tools/common/upgrade/`
10. 以下のコマンドを使用して、arcot-common-upgrade-framework.jar ファイルを実行します。
    `java [JVM_Options] -jar arcot-common-upgrade-framework.jar [--log-file <log-file-name>] [--log-level <log-level>][--commit-batch-size <batch_size>] [--product-name common][--prompt][--mst]`

    以下の表に、この JAR でサポートされているオプションの説明を示します。

オプション	説明
JVM-Options	以下の JVM オプションは、LDAP 組織が設定されている場合のみ必要です。 ■ **-Xmx1024m**： 最大ヒープ サイズを 1 GB に設定します。 100,000 人を超えるユーザが設定済みの LDAP に存在する場合は、ヒープ サイズを 2,048 MB （2 GB）に増やすことを強く推奨します。 ■ **-Dcom.arcot.ldap.migration.timeout=<duration>**： LDAP 組織の移行が失敗としてマークされるまでの時間（分単位）。 100,000 人のユーザの LDAP 移行のタイムアウトは、約 240 分（4 時間）です。 ただし、使用しているハードウェア構成のタイプによって異なります。このパラメータのデフォルト値は 240 分です。

オプション	説明
log-file	ログ ファイルへのパスを指定します。 ■ 値を指定しない場合、arcot_common_upgrade.log ファイルは %ARCOT_HOME%¥logs¥ ディレクトリに作成されます。 ■ 絶対パスを指定すると、ログ ファイルは指定した場所に作成されます。 ■ ファイル名を指定すると、ログ ファイルは指定したファイル名で %ARCOT_HOME% に作成されます。
-log-level	ログ レベルを指定します。 値を指定しない場合、アップグレード ログ レベルは INFO に設定されます。
commit-batch-size	COMMIT ステートメントが発行される前に、データベースに発行されるトランザクションの数を指定します。
product-name	移行する必要がある製品の名前を指定します。 デフォルト値は common です。
prompt	各段階が正常に完了した後に、先に進むかどうかを確認するためのプロンプトを表示します。 後でツールを実行して、停止した場所から続行することを選択できます。 このオプションを指定しない場合、アップグレード ツールは、アップグレード プロセスが完了するまでプロンプトを表示せずに実行されます。
mst	Monitoring Sleep Time（スリープ時間のモニタ）を意味します。このオプションを指定すると、アップグレード ツールは、指定した期間（分単位）スリープした後にアップグレード中の進捗状況を示す診断メッセージを出力します。デフォルト値は 2 分です。

12. $ARCOT_HOME/logs/arcot_common_upgrade.log ログ ファイルを確認して、共通データベースの移行が成功したことを確認します。

    重要: データベースの移行中に、手順を間違って実行してしまったためにエラーが発生した場合は、以前に作成したデータベース バックアップをリストアしてください。データベースが正しくリストアされたことを確認した後、データベースの移行手順を再試行します。

Strong Authentication データベースの移行

共通コンポーネント用のデータベースをアップグレードした後、Strong Authentication コンポーネント用のデータベースをアップグレードします。

次の手順に従ってください:

1. $ARCOT_HOME ディレクトリで、
   ca-strongaauth-upgrade-6.2.9-or-7.x-8.0.zip を解凍します。
2. 作業ディレクトリを以下のディレクトリに変更します。
   `$ARCOT_HOME/ca-strongaauth-upgrade-6.2.9-or-7.x-8.0.zip/tools/<platform_name>`
3. $ARCOT_HOME/sbin に移動し、以下のコマンドを実行します。

   ```
   source arwfenv
   ```

4. 以下のコマンドを実行します。
   `./wfupgrade -migrate`

   このコマンドは、6.x、7.x、または 8.0 の設定データを、以前のデータベース テーブルから 8.0 のテーブルに移行します。

   wfupgrade ツールは、$ARCOT_HOME/logs/ ディレクトリに ca-strongaauth-8.0-upgrade.log ファイルを生成します。

   重要: wfupgrade アップグレード ツールは、サーバがインストールされているシステムから実行してください。
5. テキスト エディタでログ ファイルを開き、FATAL および WARNING メッセージが含まれていないことを確認します。

サーバ接続プールの設定の更新

アプリケーション サーバ接続プールが使用されている場合、またはデータベースとの接続で SSL が設定されている場合は、以下の手順を実行します。

次の手順に従ってください:

1. 既存の展開でアプリケーション サーバ接続プールが使用されている場合は、以下の手順に従って、securestore.enc ファイル内のデータベースの詳細を更新します。
   a. DBUtil が使用可能な以下の場所に作業ディレクトリを変更します。
      `$ARCOT_HOME/tools/linux`
   b. プライマリ データベースに対して以下のコマンドを実行します。
      `DBUtil -pi <DB_username> <DB_password>`
2. データベースとの接続で SSL が設定されている場合は、以下の手順に従って、securestore.enc ファイル内のデータベースの詳細を更新します。
   a. DBUtil が使用可能な以下の場所に作業ディレクトリを変更します。
      `$ARCOT_HOME/tools/linux`
   b. データベースで SSL 通信が有効になっている場合は、トラスト ストア パスワードを以下のように設定します。
      `DBUtil -pi TrustStorePath.1 <truststore-password>`

既存リリースのアンインストール

Strong Authentication の既存のリリースをアンインストールし、アプリケーション サーバにインストールされている CA Advanced Authentication および UDS を展開解除します。

注: このセクションで示されている手順がアンインストール オプションと一致しない場合は、Strong Authentication の既存リリースのインストール ガイドに記載されているアンインストール手順に従ってください。

次の手順に従ってください：

1. 以下の手順に従って、既存リリースのアンインストールを実行します。
   a. 以下のコンポーネントをシャットダウンします。
      - Strong Authentication サーバ
      - ほかのコンポーネントが展開されているすべてのアプリケーション サーバ
   b. CA Advanced Authentication が閉じていることを確認します。
   c. INI ファイルおよび設定関連のその他のファイルがすべて閉じられていることを確認します。
   d. 以下のディレクトリに移動します。
      `$ARCOT_HOME/arcot/Uninstall_Arcot WebFort/`
   e. 以下のコマンドを使用して、インストーラを実行します。
      `sh Uninstall Arcot WebFort`

      アンインストール オプションを指定するように促すメッセージが表示されます。
   f. 「1」を入力して、すべての機能とコンポーネントを削除することを指定します。
   g. Enter キーを押して確定します。
   h. Enter キーを押して、アンインストールを完了します。
   i. $ARCOT_HOME ディレクトリに残っているファイルをすべて削除します。

2. アプリケーション サーバから CA Advanced Authentication およびユーザ データ サービス Web アプリケーションを展開解除し、アプリケーション サーバを正常にシャットダウンします。次に、アプリケーション サーバのキャッシュをリフレッシュします。
3. .com.zerog.registry.xml ファイルが削除されたことを確認します。 この隠しファイルはインストール時に作成されます。このファイルの場所は、Strong Authentication のインストールに使用したユーザ アカウントによって異なります。
   - root ユーザとして Strong Authentication をインストールした場合、このファイルは /var ディレクトリにあります。
   - その他のユーザとして Strong Authentication をインストールした場合、このファイルはそのユーザの HOME ディレクトリにあります。

Strong Authentication の再インストール

使用した展開モデルに応じて、以下のいずれかのセクションで説明されているタスクを実行します。

- 単一システムへの Strong Authentication の再インストール
- 分散システムへの Strong Authentication の再インストール

単一システムに Strong Authentication を再インストールする方法

単一システムに Strong Authentication を再インストールするには、以下の手順に従います。

重要: 以下のセクションの情報は、Strong Authentication の新規インストールに適用されます。

アップグレード操作中に事前に移行したデータベースを使用します。 古いリリースがインストールされているのと同じ場所に Strong Authentication をインストールします。 別の場所にインストールすると、Strong Authentication サーバが起動 *しません*。

次の手順に従ってください：

1. Complete インストールの実行
2. データベースのセットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication の確認
6. Strong Authentication サーバの起動
7. インストールの確認

   注: サーバの起動中、またはインストールの確認中に警告が表示される場合、およびトランザクションが失敗する場合、アップグレードは正常に実行されていません。 「アップグレード時の問題のトラブルシューティング」に記載されている情報を使用します。 それでも解決できない場合は、「初期設定への復帰」の手順に従って初期設定に戻すことができます。
8. ユーザ データ サービスの展開
9. サンプル アプリケーションの展開
10. サンプル アプリケーションの使用
11. CA Adapter 2.2.7 用の追加設定の実行
12. インストール後のチェックリスト

分散システムに Strong Authentication を再インストールする方法

分散システムに Strong Authentication を再インストールするには、以下のセクションで説明されているタスクを実行します。

重要:

これらのセクションの情報は、分散システムへの Strong Authentication を展開、および Windows への Strong Authentication のインストールに適用されます。

アップグレード中に事前に移行したデータベースを使用します。 古いリリースがインストールされているのと同じ場所に Strong Authentication をインストールします。別の場所にインストールすると、Strong Authentication サーバが起動しません。

次の手順に従ってください：

1. 1 つ目のシステムへのインストール
2. データベースのセットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication の確認
6. CA Advanced Authentication へのログイン
7. Strong Authentication サーバの起動
8. インストールの確認
9. ユーザ データ サービスの展開
10. 2 つ目のシステムへのインストール
11. サンプル アプリケーションの展開
12. Strong Authentication サーバとの通信用サンプル アプリケーションの設定
13. サンプル アプリケーションの使用
14. CA Adapter 2.2.7 用の追加設定の実行

アップグレード後のタスクの実行

以下のアップグレード後のタスクを実行します。

- バックアップ データベースを無効にした場合は、$ARCOT_HOME/conf/arcotcommon.ini ファイルの arcot/db/backupdb セクションを編集して有効にし、バックアップ データベースとプライマリ データベースを同期します。 アップグレードの前にデータベース レプリケーションを無効にした場合は、アップグレードの後にレプリケーションを有効にします。
- アップグレードの前にこのインストールにプラグインを登録していた場合は、プラグインを再コンパイルします。 再コンパイルしたファイルの名前が以前と同じであることを確認します。 アップグレードの前に保存したスタートアップ ログを使用して、プラグインの詳細を確認します。
- マルチバイト文字または国際化のサポートを必要とし、使用しているデータベースが現在マルチバイト データをサポートしていない場合は、マルチバイト データをサポートする文字セットにデータベースを移行します。 詳細については、「CA Strong Authentication インストールおよび展開ガイド（UNIX プラットフォーム用）」の「データベース サーバの設定」を参照してください。

6.x、7.x、または 8.0 からのアップグレード パスである場合は、CA Advanced Authentication を使用して以下の設定を行います。

1. 以前のすべての認証設定に対して、グローバル レベルで新しい認証ポリシーを作成します。
2. RADIUS 設定を再作成します。
3. 以下のサーバ インスタンス設定をセットアップします。
   - データベース接続の設定
   - ログ ファイルの設定
4. プロトコルごとのスレッド設定をセットアップします。
5. ASSP 設定を作成します。
6. （オプション） CA AuthID の猶予期間を設定します。 設定するには、CA AuthID ポリシーの［**認証の成功を許可**］フィールドを設定します。
7. （オプション） Q&A 認証情報の呼び出し元検証を有効にします。 有効にするには、Q&A ポリシーの［**コール元検証の有効化**］フィールドを設定します。

Windows 上の Risk Authentication をアップグレードする方法

Windows 上の Risk Authentication をリリース 8.0 にアップグレードするには、以下のタスクを実行します。

次の手順に従ってください：

1. アップグレード前のタスクの実行 (P. 37)
2. アップグレードの準備 (P. 42)
3. 共通コンポーネント データベースの移行 (P. 43)
4. Risk Authentication データベースの移行 (P. 47)
5. Risk Authentication の既存のリリースのアンインストール (P. 48)
6. Risk Authentication の再インストール (P. 49)
7. サーバの起動時に警告が表示される場合、およびトランザクションが失敗する場合は、「（エラーの場合のみ）初期設定への復帰」の手順を実行します。
8. アップグレード後のタスクの実行 (P. 52)
9. 廃止されたルールと新規ルールの置き換え (P. 53)
10. アップグレード後の設定の変更

アップグレード前のタスクの実行

アップグレード手順を開始する前に、以下のアップグレード前のタスクを実行します。

重要: CA Advanced Authentication がインストールされているシステムでアップグレード手順を実行します。

- アップグレード操作に使用するアカウントが Administrators グループに属していることを確認します。
- リリース 8.0 以降では、スコアが 0 のルールは ALLOW アドバイスを実行しなくなりました。代わりに、スコア 0 は SILENT を意味しています。ルールは実行されますが、スコアリングには使用されません。 アップグレード前のデフォルトのスコアが 0 であった場合、アップグレード時にデフォルトのスコアが 1 に変更されます。

  注: ルールのスコアの変更については、「CA Risk Authentication 管理ガイド」を参照してください。
- 2.x 以前のリリースで作成したカスタム アドオン ルール タイプは、アップグレード時に移行されません。 XML ファイルをインポートすることによりカスタム アドオン ルール タイプを作成する機能は廃止されました。 Risk Authentication 展開にカスタム アドオン ルール タイプが含まれている場合、アップグレードの前に削除します。
- 既存ルールの短縮名または名前が新しく導入またはアップグレードで変更するルールの短縮名または名前と同じ場合は、アップグレードが失敗します。 既存ルールの名前が新しいルールの名前と同じである場合も、同じ問題が発生します。 この問題を回避するには、以下の手順に従います。

  1. CA Advanced Authentication を使用して、既存ルールの短縮名と新しく導入またはアップグレードで変更するルールの短縮名を比較します。

     以下の表に、新しく導入されるルールまたはアップグレードで変更されるルールを示します。

ルール名	Rule Mnemonic
Unknown DeviceID	UNKNOWNDEVICEID
Device MFP Not Match	MFPMISMATCH
User Not Associated with DeviceID	USERDEVICENOTASSOCIATED
Unknown User	UNKNOWNUSER

2. 既存ルールの短縮名と新規ルールの短縮名が一致する場合は、既存ルールを削除した後、再度作成してください。 ルールを再作成する間、そのルールには別の短縮名を付けてください。 2 つの異なるルールに同じルール名を付けることは可能です。 しかし、混同しないように既存ルールの名前を変更することをお勧めします。

   注: ルールの削除および作成については、「CA Risk Authentication 管理ガイド」を参照してください。

- リリース 8.0 では、ルール、ルール セット、またはその他のルール設定で、別のルール、ルール セット、またはその他のルール設定を参照できます。別のルール、ルール セット、またはその他のルール設定を参照するルール、ルール セット、またはその他のルール設定に対して、以下の手順を実行します。

  a. GA または OA として CA Advanced Authentication にログインします。

  b. GA としてログインして、システム ルール セットに対してこの手順を実行する場合は、［サービスおよびサーバの設定］タブをクリックします。

  c. GA または OA としてログインして単一の組織に対してこの手順を実行する場合は、以下の手順に従います。

     - ［組織］タブをアクティブにします。
     - ［組織の管理］で、［組織の検索］リンクをクリックします。
     - ［組織の検索］ページの［検索］ボタンをクリックします。
     - 組織の名前をクリックします。
     - ［設定］タブをクリックします。

  d. サイド バー メニューの［ルール管理］に移動します。

  e. 別のルール、ルール セット、またはその他のルール設定を参照するルール、ルール セット、またはその他のルール設定のリンクをクリックします。

  f. ［独自のルールを使用］を選択します。

  g. 既存のルール セットから［コピー］を選択します。

  h. ［ルールセット名］リストから、このルール、ルール セット、またはその他のルール設定が参照しているルール セットを選択します。

  i. ［保存］をクリックします。

  j. 変更を運用環境に移行します。

     注: 変更の運用環境への移行、およびキャッシュのリフレッシュの詳細については、「CA Risk Authentication 管理ガイド」を参照してください。

- アップグレード プロセスは、オフライン モードでのみサポートされます。 以下のサービスをシャットダウンします。
  - Risk Authentication サーバ
  - ケース管理キュー サーバ
  - CA Advanced Authentication およびユーザ データ サービスが展開されているすべてのアプリケーション サーバ
- CA Advanced Authentication を閉じます。
- テキスト エディタで %ARCOT_HOME%¥conf¥arcotcommon.ini ファイルを開き、以下の手順に従います。
  a. プライマリ データベースの詳細が正しいことを確認します。

  注: アップグレード ツールは、このファイルに設定されているデータベースを使用します。

  b. バックアップ データベースを設定している場合、arcotcommon.ini ファイルの arcot/db/backupdb セクションで、以下のプロパティが含まれる行をコメントアウトして、バックアップ データベースを無効にします。
  - URL.1
  - AppServerConnectionPoolName.1
  - Username.1

  a. バージョン 2.2.9 用に、arcotcommon.ini ファイルに以下のセクションを含めます。
  - [arcot/crypto/device]
  - HSMDevice=S/W

  a. arcotcommon.ini ファイルを保存して閉じます。

- アップグレードするシステムに JDK 以降がインストールされていることを確認します。
- アップグレードを実行するデータベースが、アップグレード プロセスの間、利用可能であることを確認します。
- アップグレードを実行するデータベースで、レプリケーションが無効であることを確認します。
- Risk Authentication スキーマを含むデータベースをバックアップします。
- Risk Authentication のマルチバイト文字または国際化のサポートを必要とし、使用しているデータベースが現在マルチバイト データをサポートしていない場合は、マルチバイト データをサポートする文字セットにデータベースを移行します。 詳細については、「CA Risk Authentication インストールおよび展開ガイド(Microsoft Windows 用)」の「データベース サーバの設定」の章を参照してください。
- アップグレード ツールを実行する前に、データ ボリュームに基づいて、ロールバック セグメント サイズなどの要件を検討します。
- Risk Authentication のアップグレードに必要なデータベース権限があることを確認します。 すべての権限のリストについては、Risk Authentication 8.0 へのアップグレードの前提条件を参照してください。
- 以前のリリースの LDAP リポジトリにユーザの詳細を保存している場合は、LDAP サーバがアップグレード プロセスの間、利用可能であることを確認します。
- ARCOT_HOME 環境変数が、Risk Authentication がインストールされているディレクトリに設定されていることを確認します。
- 新しいディレクトリに既存の ARCOT_HOME ディレクトリの内容をコピーします。

  ARCOT_HOME は、既存の Risk Authentication のインストールで作成されたディレクトリ構造全体を含むベース ディレクトリを指します。 ARCOT_HOME の例： *install_location*/arcot/。

  ARCOT_HOME_BACKUP は、既存の ARCOT_HOME ディレクトリの内容をコピーするバックアップ ディレクトリを指します。

  注: アップグレード中にエラーが発生した場合には、ARCOT_HOME_BACKUP ディレクトリを使用して初期設定に戻します。

アップグレードの準備

アプリケーション サーバ接続プールが使用されている場合、またはデータベースとの接続で SSL が設定されている場合は、以下の手順を実行します。

次の手順に従ってください:

1. アプリケーション サーバ接続プールが既存の Risk Authentication 展開で使用されている場合は、%ARCOT_HOME%¥tools¥win ディレクトリに移動し、プライマリ データベースに対して以下のコマンドを実行して securestore.enc ファイルを更新します。
   `DBUtil -pi <DB_username> <DB_password>`

   注: データベース接続プールが使用されているかどうかを確認するには、%ARCOT_HOME%¥conf¥arcotcommon.ini ファイルを開きます。AppServerConnectionPoolName パラメータの値を確認します。

2. データベースとの接続に SSL が設定されている場合は、%ARCOT_HOME%¥tools¥win ディレクトリに移動し、DBUtil を使用して、以下のようにトラスト ストア パスワードを設定します。
   `DBUtil -pi TrustStorePath.1 <truststore-password>`

   注: SSL が設定されているかどうかを確認するには、arcotcommon.ini ファイル内の TrustStorePath パラメータの値を確認します。

共通コンポーネント データベースの移行

共通コンポーネント用のデータベースを移行するには、以下の手順に従います。

次の手順に従ってください:

1. アップグレードするシステム上の一時的な場所にアップグレード ディレクトリをコピーします。

   このディレクトリには、この移行パスに適用可能な以下の ZIP ファイルが含まれます。

   - ca-common-upgrade-1.0.*x*-2.0.zip.
   - ca-riskauth-upgrade-2.2.9-or-3.x-8.0.zip

   重要: Strong Authentication が 8.0 にアップグレードされている場合、または現在の Strong Authentication のバージョンが 7.x である場合、または現在の Risk Authentication のバージョンが 3.x である場合は、手順 2 ～ 10 を無視します。

2. ARCOT_HOME ディレクトリに ca-common-upgrade-1.0.*x*-2.0.zip ファイルをコピーします。
3. このディレクトリで、ca-common-upgrade-1.0.*x*-2.0.zip ファイルの内容を抽出します。

   注: いずれかの既存ファイルを上書きするようにプロンプトが表示された場合は、［**Yes**］をクリックします。

4. 以下のディレクトリに移動します。
   `%ARCOT_HOME%¥tools¥common¥upgrade`
5. このディレクトリ内の arcot-common-db-upgrade.zip ファイルの内容を抽出します。
6. データベースと互換性のある JDBC JAR をダウンロードします。

   - Oracle： ojdbc.jar
   - SQL Server： sqljdbc.jar

   %ARCOT_HOME%¥tools¥common¥upgrade¥**lib** ディレクトリに JAR をコピーします。

7. 既存のインストールで使用されている JAVA_HOME を見つけます。 同じ JAVA_HOME を使用してアップグレード ツールを実行していることを確認します。

8. ArcotAccessKeyProvider.dll 共有ライブラリがアプリケーション サーバで設定されていることを確認します。 このファイルを <アプリケーション サーバで使用する JAVA_HOME>¥jre¥bin¥ フォルダにコピーします。
9. 作業ディレクトリを以下に変更します。
   `%ARCOT_HOME%¥tools¥common¥upgrade¥`
10. 以下のコマンドを使用して、arcot-common-upgrade-framework.jar ファイルを実行します。
    `java [JVM_Options] -jar arcot-common-upgrade-framework.jar [--log-file <log-file-name>] [--log-level <log-level>][--commit-batch-size <batch_size>] [--product-name common] [--prompt][--mst]`

    以下の表に、この JAR ファイルでサポートされているオプションの説明を示します。

オプション	説明
JVM-Options	以下の JVM オプションは、LDAP 組織が設定されている場合のみ必要です。 ■ -Xmx<*heap_memory_size_in_MB*>M： 最大ヒープ サイズを 1 GB に設定します。 100,000 人を超えるユーザが設定済みの LDAP に存在する場合は、ヒープ サイズを 2,048 MB （2 GB）に増やすことを強く推奨します。 -Dcom.arcot.ldap.migration.timeout=<*duration*>： LDAP 組織の移行では、LDAP サーバからすべてのユーザを取得し、Risk Authentication データベースに移行します。このパラメータは、LDAP サーバからすべてのユーザを取得するための最大時間 (分単位) を設定します。この時間を超えると、LDAP 組織の移行は失敗としてマークされます。 100,000 人のユーザの LDAP 移行のタイムアウトは、約 240 分（4 時間）です。 ただし、タイムアウト値は、使用しているハードウェア構成のタイプによって異なります。このパラメータのデフォルト値は 240 分です。 **注**: Java コマンド実行可能ファイルが、この手順で識別された JAVA_HOME に属することを確認します。 7.JAVA_HOME が設定されない場合は、%JAVA_HOME%¥bin を含むように PATH 環境変数を変更します。

オプション	説明
log-file	ログ ファイルへのパスを指定します。 ■ 値を指定しない場合、arcot_common_upgrade.log ファイルは %ARCOT_HOM%¥logs¥ ディレクトリに作成されます。 ■ 絶対パスを指定すると、ログ ファイルは指定した場所に作成されます。 ■ ファイル名を指定すると、ログ ファイルは指定したファイル名で %ARCOT_HOME%¥logs¥ に作成されます。
log-level	ログ レベルを指定します。 値を指定しない場合、アップグレード ログ レベルは INFO に設定されます。
commit-batch-size	COMMIT ステートメントが発行される前に、データベースに発行されるトランザクションの数を指定します。
product-name	アップグレードが実行される製品の名前を指定します。 製品名を指定しないと、製品名は共通であると見なされます。 以下の値が使用可能です。 ■ common： 共通コンポーネントを示します。 ■ Risk Authentication： Risk Authentication を示します。 **注**: Risk Authentication をアップグレードする前に、共通コンポーネントをアップグレードしてください。
prompt	アップグレード プロセスの各段階の正常完了後に、先に進むかどうかを確認するためのプロンプトを表示します。 アップグレード プロセスで、以下の段階が実行されます。 ■ アップグレード前: データベース スキーマの移行のために、さまざまな DDL および DML 操作が実行されます。 ■ アップグレード： 新しいスキーマにデータが移行されます。 ■ アップグレード後： アップグレード後に実行する必要があるクリーンアップまたはフォローアップ アクションが含まれます。 ■ 検証： アップグレードが成功したかどうかを確認します。 このオプションでは、後でアップグレード ツールを実行して、停止した場所から続行することを選択できます。 このオプションを指定しない場合、アップグレード ツールは、アップグレード プロセスが完了するまでプロンプトを表示せずに実行されます。

オプション	説明
mst	Monitoring Sleep Time（スリープ時間のモニタ）を意味します。このオプションを指定すると、アップグレード ツールは、指定した期間（分単位）スリープした後にアップグレード中の進捗状況を示す診断メッセージを出力します。デフォルト値は 2 分です。

注: リリース 1.0.x からアップグレードする場合は、%ARCOT_HOME%¥logs¥arcot_common_upgrade.log ファイル内で以下の行を確認します。

```
Upgrade for common from version 1.0.x to version 2.0 run successfully.
```

ログ内にこの行が存在する場合、データベースが正常にアップグレードされたことが確認されます。

Risk Authentication データベースの移行

共通コンポーネント用のデータベースを移行した後、Risk Authentication コンポーネント用のデータベースを移行します。

次の手順に従ってください:

1. ARCOT_HOME ディレクトリの ca-riskauth-upgrade-2.2.9-or-3.x-8.0 ファイルの内容を抽出します。
2. 以下のディレクトリに移動します。
   `%ARCOT_HOME%¥tools¥common¥upgrade`
3. 以下のコマンドを実行します。
   `java -jar arcot-common-upgrade-framework.jar --product-name riskfort`

   コマンド オプションの説明については、「共通コンポーネント データベースの移行 (P. 43)」の表を参照してください。
4. アップグレード元のリリースに応じて、%ARCOT_HOME%¥logs¥ ディレクトリ内の arcot_common_upgrade.log ファイル内で、以下のいずれかの行を探します。
   `Upgrade for Risk Authentication from version <your-Risk Authentication-release> to version 8.0 run successfully.`

   注: リリース 3.0 からアップグレードする場合は、以下の行を探します。

   `Upgrade for Risk Authentication from version 3.0 to version 8.0 run successfully.`

   ログ内にこの行が存在する場合、データベースが正常にアップグレードされたことが確認されます。

Risk Authentication の既存のリリースのアンインストール

Risk Authentication の既存のリリースをアンインストールするには、以下の手順に従います。 また、アプリケーション サーバにインストールされている Risk Authentication コンポーネント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. 以下の手順を実行して、Risk Authentication の既存のリリースをアンインストールします。
   a. 以下のコンポーネントをシャットダウンします。
      - Risk Authentication サーバ
      - ケース管理キュー サーバ
      - Risk Authentication のその他のコンポーネントが展開されているすべてのアプリケーション サーバ
   b. CA Advanced Authentication が開いていないことを確認します。
   c. INI ファイル、および Risk Authentication の設定関連のその他のファイルがすべて閉じられていることを確認します。
   d. arcot¥ ディレクトリに移動します。
   e. %ARCOT_HOME%%¥Uninstall_Arcot RiskFort ディレクトリに移動します。
   f. Uninstall Arcot RiskFort.exe ファイルをダブルクリックします。
   g. ［Complete Uninstall］を選択します。
   h. ARCOT_HOME ディレクトリに残っているファイルをすべて削除します。
2. アプリケーション サーバから、CA Advanced Authentication、ユーザ データ サービス、およびサンプル アプリケーション Web アプリケーションを展開解除します。詳細については、アプリケーション サーバのドキュメントを参照してください。

Risk Authentication の再インストール

Risk Authentication を単一システムに展開しているか、または分散システムに展開しているかに応じて、以下のいずれかのセクションで説明されているタスクを実行します。

- 単一システムへの Risk Authentication の再インストール (P. 50)
- 分散システムへの Risk Authentication の再インストール (P. 51)

単一システムに Risk Authentication を再インストールする方法

単一システムに Risk Authentication を再インストールするには、以下のセクションで説明されているタスクを実行します。 アップグレード操作中に事前に移行したデータベースを使用します。

重要: この情報は、Risk Authentication の新規インストール、*単一システムへの Risk Authentication の展開*、および *Windows への Risk Authentication のインストール*に適用されます。

1. Risk Authentication をインストールします。

   注: Risk Authentication のインストール時には、%ARCOT_HOME%¥conf¥ ディレクトリ内の arcotcommon.ini と同じプライマリおよびバックアップ データベース詳細を指定してください。

2. データベースのセットアップを確認します。
3. アプリケーション サーバを準備します。
4. CA Advanced Authentication を展開します。
5. CA Advanced Authentication にログインします。

   重要: MA パスワードは、インストール中に実行したブートストラップ プロセス中にリセットされるため、デフォルト パスワードではなく現在の MA パスワードを使用してください。

6. Risk Authentication サーバを起動します。
7. ケース管理キュー サーバを起動します。
8. インストールを確認します。

   注: サーバの起動中に警告が表示される場合、およびトランザクションが失敗する場合、アップグレードは正常に実行されていません。「（エラーの場合のみ）初期設定への復帰」の手順に従って、初期設定に戻すことができます。

9. ユーザ データ サービスを展開します。
10. サンプル アプリケーションを展開します。

分散システムに Risk Authentication を再インストールする方法

分散システムに Risk Authentication を再インストールするには、以下のタスクを実行します。 アップグレード操作中に事前に移行したデータベースを使用します。

注: これらのセクションの情報は、Risk Authentication の新規インストール、*分散システムへの Risk Authentication の展開*、および *Windows への Risk Authentication のインストール*に適用されます。

1. 1 つ目のシステムへの Risk Authentication のインストール
2. データベースのセットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication へのログイン
6. Risk Authentication サーバの起動
7. ケース管理キュー サーバの起動
8. インストールの確認
9. ユーザ データ サービスの展開
10. 2 つ目のシステムへのインストール
11. 2 つ目のシステムへのサンプル アプリケーションの展開
12. Risk Authentication サーバとの通信用サンプル アプリケーションの設定

アップグレード後のタスクの実行

このセクションでは、アップグレード後に実行する必要があるタスクについて説明します。

次の手順に従ってください:

1. アップグレードの前にデータベース レプリケーションを無効にした場合は、Risk Authentication 8.0 へのアップグレード後に、バックアップ データベースのレプリケーションを有効にする必要があります。
2. Risk Authentication 2.2.7 で以下のポートに SSL が設定されていることを確認します。
   - Risk Authentication サーバ インスタンスの Server Management プロトコル用のポート： 7980
   - ケース管理キュー サーバ インスタンスの Case Management Queuing Administration プロトコル用のポート： 7780
3. 以下の手順に従って、SSL を再設定します。
   - CA Advanced Authentication と Risk Authentication サーバ間： ポート 7980
   - CA Advanced Authentication とケース管理キュー サーバ間： ポート 7780

   注: インスタンス管理やプロトコル設定などのほとんどの管理タスクは、Risk Authentication 8.0 の CA Advanced Authentication でこれらのポートを使用して実行されるため、この設定が必要です。

   CA Advanced Authentication と Risk Authentication サーバまたはケース管理キュー サーバ間の SSL の設定手順については、「CA Risk Authentication 管理ガイド」の「SSL の設定」の章を参照してください。
4. ［その他の設定］画面で組織の基準通貨コードを設定します。

   注: 組織に固有の基準通貨コードの設定の詳細については、「CA Risk Authentication 管理ガイド」の「グローバル設定の管理」の章を参照してください。
5. スコアが 0 の何らかのルールがあり、これらのルールをスコアリングに使用する場合には、1 または 2 のように、ゼロ以外の値にスコアを変更します。

廃止されたルールと新規ルールの置き換え

リリース 8.0 では、4 つの事前定義済みルールが廃止されました。 廃止されたこれらのルールに対して、代替ルールが導入されました。 以下の表に、廃止されたルールと新規ルール、およびルールの短縮名を示します。

廃止されたルール名とルールの短縮名	新規ルール名とルールの短縮名
DeviceID Known （DEVICEIDCHECK）	Unknown DeviceID （UNKNOWNDEVICEID）
Device MFP Match （SIGMATCH）	Device MFP Not Match （MFPMISMATCH）
User Associated with DeviceID （USERDEVICEASSOCIATED）	User Not Associated with DeviceID （USERDEVICENOTASSOCIATED）
User Known （USERKNOWN）	Unknown User （UNKNOWNUSER）

重要: これらのルールは廃止されましたが、引き続き使用可能であり、アップグレード後に使用できます。 ルール式に必要な変更を加えて、廃止されたルールを、対応する新しいルールで置き換えることを推奨します。

廃止された 4 つのルールのいずれかに対して、ルールが No に評価される場合、ルールは一致したと考えられます。 その後、それはスコアリングに使用されます。 対照的に、その他の事前定義済みの各ルールは、Yes に評価されると一致したと考えられます。

リリース 8.0 で導入された 4 つの新規ルールのいずれかに対して、ルールが Yes に評価される場合、ルールは一致したと考えられます。このように、4 つの新しいルールはその他の事前定義済みルールと一致しています。

以下の表に、廃止されたルールと新規ルールの違いを強調する例を示します。

サンプル ユース ケース	廃止されたルール	廃止されたルールの結果	新規ルール	新規ルールの結果
ユーザが Risk Authentication データベースに存在しない。	USERKNOWN	いいえ	UNKNOWNUSER	はい

DeviceID が Risk Authentication データベースに存在しない。	DEVICEIDCHECK	いいえ	UNKNOWNDEVICEID	はい
MFP が Risk Authentication データベースに存在しない。	SIGMATCH	いいえ	MFPMISMATCH	はい
ユーザが DeviceID と関連付けられていない。	USERDEVICEASSOCIATED	いいえ	USERDEVICENOTASSOCIATED	はい

次の手順に従ってください：

1. CA Advanced Authentication にログインします。
2. すべての組織およびルール セット用のルール設定レポートで、［ルール式］列に一覧表示された短縮名のいずれかが、廃止された短縮名のリストに属するかどうかを確認します。
3. ルールが廃止された短縮名を使用する場合で、廃止された短縮名を使用したくない場合には、対応する新しい短縮名を使用します。

   ルール式を変更する方法

   a. GA または OA として CA Advanced Authentication にログインします。
   b. GA としてログインして、システム ルール セットに対してこの手順を実行する場合は、［サービスおよびサーバの設定］をクリックします。
   c. GA または OA としてログインして単一の組織に対してこの手順を実行する場合は、以下の手順に従います。
      - ［組織］タブをアクティブにします。
      - ［組織の管理］に移動し、［組織の検索］リンクをクリックします。
      - ［組織の検索］ページの［検索］ボタンをクリックします。
      - 組織の名前をクリックします。
      - ［設定］タブをクリックします。
   d. サイド バー メニューの［ルール管理］に移動します。
   e. ［ルールおよびスコアリング管理］リンクをクリックします。
   f. ［ルールセットを選択してください］リストからルール セットを選択します。
   g. 変更するルールをクリックします。
   h. テキスト フィールドで作成中のルールに必要な変更を行います。
   i. 変更を保存し、［ルール ビルダ］ページを閉じます。
4. 変更したルールを運用環境に移行し、次にキャッシュをリフレッシュします。

   注: 運用環境へのルールの移行およびキャッシュのリフレッシュの詳細については、「CA Risk Authentication 管理ガイド」を参照してください。

UNIX 上の Risk Authentication をアップグレードする方法

UNIX 上の Risk Authentication をリリース 8.0 にアップグレードするには、以下のタスクを実行します。

次の手順に従ってください：

1. アップグレード前のタスクの実行 (P. 57)
2. 共通コンポーネント データベースの移行 (P. 62)
3. Risk Authentication データベースの移行 (P. 66)
4. Risk Authentication の既存のリリースのアンインストール (P. 67)
5. Risk Authentication の再インストール (P. 68)
6. サーバの起動時に警告が表示される場合、およびトランザクションが失敗する場合は、「*初期設定への復帰*」の手順を実行します。
7. アップグレード後のタスクの実行 (P. 71)
8. 廃止されたルールと新規ルールの置き換え (P. 72)
9. アップグレード後の設定の変更

アップグレード前のタスク

アップグレード手順を開始する前に、以下のアップグレード前のタスクを実行します。

重要: CA Advanced Authentication がインストールされているシステムでアップグレード手順を実行します。

- アップグレード操作に使用するアカウントが Administrators グループに属していることを確認します。
- リリース 8.0 以降では、スコアが 0 のルールは ALLOW アドバイスを実行しなくなりました。代わりに、スコア 0 は SILENT を意味しています。ルールは実行されますが、スコアリングには使用されません。 アップグレード前のデフォルトのスコアが 0 であった場合、アップグレード時にデフォルトのスコアが 1 に変更されます。

  注: ルールのスコアの変更については、「CA Risk Authentication 管理ガイド」を参照してください。
- 2.x 以前のリリースで作成したカスタム アドオン ルール タイプは、アップグレード時に移行されません。 XML ファイルをインポートすることによりカスタム アドオン ルール タイプを作成する機能は廃止されました。 Risk Authentication 展開にカスタム アドオン ルール タイプが含まれている場合、アップグレードの前に削除します。
- 既存ルールの短縮名または名前が新しく導入またはアップグレードで変更するルールの短縮名または名前と同じ場合は、アップグレードが失敗します。 既存ルールの名前が新しいルールの名前と同じである場合も、同じ問題が発生します。 この問題を回避するには、以下の手順に従います。

  1. CA Advanced Authentication を使用して、既存ルールの短縮名と新しく導入またはアップグレードで変更するルールの短縮名を比較します。

     以下の表に、新しく導入されるルールまたはアップグレードで変更されるルールを示します。

ルール名	Rule Mnemonic
Unknown DeviceID	UNKNOWNDEVICEID
Device MFP Not Match	MFPMISMATCH
User Not Associated with DeviceID	USERDEVICENOTASSOCIATED
Unknown User	UNKNOWNUSER

2. 既存ルールの短縮名と新規ルールの短縮名が一致する場合は、既存ルールを削除した後、再度作成してください。 ルールを再作成する間、そのルールには別の短縮名を付けてください。 2 つの異なるルールに同じルール名を付けることは可能です。 しかし、混同しないように既存ルールの名前を変更することをお勧めします。

   注: ルールの削除および作成については、「CA Risk Authentication 管理ガイド」を参照してください。

- リリース 8.0 では、ルール、ルール セット、またはその他のルール設定で、別のルール、ルール セット、またはその他のルール設定を参照できます。別のルール、ルール セット、またはその他のルール設定を参照するルール、ルール セット、またはその他のルール設定に対して、以下の手順を実行します。

  a. GA または OA として CA Advanced Authentication にログインします。

  b. GA としてログインして、システム ルール セットに対してこの手順を実行する場合は、［サービスおよびサーバの設定］タブをクリックします。

  c. GA または OA としてログインして単一の組織に対してこの手順を実行する場合は、以下の手順に従います。

     - ［組織］タブをアクティブにします。
     - ［組織の管理］で、［組織の検索］リンクをクリックします。
     - ［組織の検索］ページの［検索］ボタンをクリックします。
     - 組織の名前をクリックします。
     - ［設定］タブをクリックします。

  d. サイド バー メニューの［ルール管理］に移動します。

  e. 別のルール、ルール セット、またはその他のルール設定を参照するルール、ルール セット、またはその他のルール設定のリンクをクリックします。

  f. ［独自のルールを使用］を選択します。

  g. 既存のルール セットから［コピー］を選択します。

  h. ［ルールセット名］リストから、このルール、ルール セット、またはその他のルール設定が参照しているルール セットを選択します。

  i. ［保存］をクリックします。

  j. 変更を運用環境に移行します。

     注: 変更の運用環境への移行、およびキャッシュのリフレッシュの詳細については、「CA Risk Authentication 管理ガイド」を参照してください。

- アップグレード プロセスは、オフライン モードでのみサポートされます。 以下のサービスをシャットダウンします。
  - Risk Authentication サーバ
  - ケース管理キュー サーバ
  - CA Advanced Authentication およびユーザ データ サービスが展開されているすべてのアプリケーション サーバ
- CA Advanced Authentication を閉じます。
- テキスト エディタで $ARCOT_HOME/conf/arcotcommon.ini ファイルを開き、以下の手順に従います。
  a. プライマリ データベースの詳細が正しいことを確認します。 アップグレード ツールは、このファイルに設定されているデータベースを使用します。
  b. バックアップ データベースを設定している場合、arcotcommon.ini ファイルの arcot/db/backupdb セクションで、以下のプロパティが含まれる行をコメントアウトして、バックアップ データベースを無効にします。
     - URL.1
     - AppServerConnectionPoolName.1
     - Username.1
  c. バージョン 2.2.9 用に、arcotcommon.ini ファイルに以下のセクションを含めます。
     ```
     [arcot/crypto/device]
     HSMDevice=S/W
     ```
  d. arcotcommon.ini ファイルを保存して閉じます。
- システムに JDK がインストールされていることを確認します。
- アップグレードを実行するデータベースが、アップグレード プロセスの間、利用可能であることを確認します。
- アップグレードを実行するデータベースで、レプリケーションが無効であることを確認します。
- Risk Authentication スキーマを含むデータベースをバックアップします。

- Risk Authentication のマルチバイト文字または国際化のサポートを必要とし、使用しているデータベースが現在マルチバイト データをサポートしていない場合は、マルチバイト データをサポートする文字セットにデータベースを移行します。 詳細については、「*データベース サーバの設定*」を参照してください。
- アップグレード ツールを実行する前に、データ ボリュームに基づいて、ロールバック セグメント サイズなどの要件を検討します。
- Risk Authentication をアップグレードするデータベース権限があることを確認します。 すべての権限のリストについては、「アップグレードに必要なデータベース権限」を参照してください。
- 以前のリリースの LDAP リポジトリにユーザの詳細を保存している場合は、LDAP サーバがアップグレード プロセスの間、利用可能であることを確認します。
- ARCOT_HOME 環境変数が、Risk Authentication がインストールされているディレクトリに設定されていることを確認します。
- 新しいディレクトリに既存の ARCOT_HOME ディレクトリの内容をコピーします。

  ここでは、ARCOT_HOME は、既存の Risk Authentication のインストールで作成されたディレクトリ構造全体を含むベース ディレクトリを指します。 通常、ARCOT_HOME は *install_location*/arcot/ です。

  ARCOT_HOME_BACKUP は、既存の ARCOT_HOME ディレクトリの内容をコピーするバックアップ ディレクトリを指します。アップグレード中にエラーが発生した場合には、ARCOT_HOME_BACKUP ディレクトリを使用して初期設定に戻します。

共通コンポーネント データベースの移行

共通コンポーネント用のデータベースを移行するには、以下の手順に従います。

次の手順に従ってください:

1. アップグレードするシステム上の一時的な場所にアップグレード ディレクトリをコピーします。

   このディレクトリには、この移行パスに適用可能な以下の ZIP ファイルが含まれます。

   - ca-common-upgrade-1.0.*x*-2.0.zip
   - ca-riskauth-upgrade-2.2.9-or-3.x-8.0.zip

   重要: Strong Authentication が 8.0 にアップグレードされている場合、または現在の Strong Authentication のバージョンが 7.x である場合、または現在の Risk Authentication のバージョンが 3.x である場合は、手順 2 ～ 11 を無視します。

2. ARCOT_HOME ディレクトリに ca-common-upgrade-1.0.*x*-2.0.zip ファイルをコピーします。
3. このディレクトリで、ca-common-upgrade-1.0.*x*-2.0.zip ファイルの内容を抽出します。

   注: いずれかの既存ファイルを上書きするようにプロンプトが表示された場合は、［**Yes**］をクリックします。

4. 以下のディレクトリに移動します。
   `$ARCOT_HOME/tools/common/upgrade/`
5. このディレクトリ内の arcot-common-db-upgrade.zip ファイルの内容を抽出します。
6. データベースと互換性のある JDBC JAR をダウンロードします。

   - Oracle： ojdbc.jar
   - SQL Server： sqljdbc.jar

   $ARCOT_HOME/tools/common/upgrade/**lib** ディレクトリに JAR をコピーします。

7. 既存のインストールで使用されている JAVA_HOME を見つけます。 同じ JAVA_HOME を使用してアップグレード ツールを実行していることを確認します。

8. libArcotAccessKeyProvider.so ファイルを <アプリケーション サーバで使用する JAVA_HOME>/jre/sbin にコピーします。例: Risk Authentication では、libArcotAccessKeyProvider.so ファイルは <ARCOT_HOME>/java/ext/<プラットフォーム名>/<32bit または 64 bit> にあります。
9. LD_LIBRARY_PATH を、libArcotAccessKeyProvider.so があるディレクトリに設定してエクスポートします。
10. 作業ディレクトリを以下に変更します。
    `$ARCOT_HOME/tools/common/upgrade/`
11. 以下のコマンドを使用して、arcot-common-upgrade-framework.jar ファイルを実行します。
    `java [JVM_Options] -jar arcot-common-upgrade-framework.jar [--log-file <log-file-name>] [--log-level <log-level>][--commit-batch-size <batch_size>] [--product-name common] [--prompt][--mst]`

    以下の表に、この JAR ファイルでサポートされているオプションの説明を示します。

オプション	説明
JVM-Options	以下の JVM オプションは、LDAP 組織が設定されている場合のみ必要です。 ■ -Xmx<*heap_memory_size_in_MB*>M： 最大ヒープ サイズを 1 GB に設定します。 100,000 人を超えるユーザが設定済みの LDAP に存在する場合は、ヒープ サイズを 2,048 MB （2 GB）に増やすことを強く推奨します。 -Dcom.arcot.ldap.migration.timeout=<*duration*>： LDAP 組織の移行では、LDAP サーバからすべてのユーザを取得し、Risk Authentication データベースに移行します。このパラメータは、LDAP サーバからすべてのユーザを取得するための最大時間 (分単位) を設定します。この時間を超えると、LDAP 組織の移行は失敗としてマークされます。 100,000 人のユーザの LDAP 移行のタイムアウトは、約 240 分（4 時間）です。 ただし、タイムアウト値は、使用しているハードウェア構成のタイプによって異なります。このパラメータのデフォルト値は 240 分です。 **注**: Java コマンド実行可能ファイルが、この手順で識別された JAVA_HOME に属することを確認します。 7.JAVA_HOME が設定されない場合は、$JAVA_HOME/sbin を含むように PATH 環境変数を変更します。

オプション	説明
log-file	ログ ファイルへのパスを指定します。 ■ 値を指定しない場合、arcot_common_upgrade.log ファイルは $ARCOT_HOME/logs/ ディレクトリに作成されます。 ■ 絶対パスを指定すると、ログ ファイルは指定した場所に作成されます。 ■ ファイル名を指定すると、ログ ファイルは指定したファイル名で $ARCOT_HOME/logs/ に作成されます。
log-level	ログ レベルを指定します。 値を指定しない場合、アップグレード ログ レベルは INFO に設定されます。
commit-batch-size	COMMIT ステートメントが発行される前に、データベースに発行されるトランザクションの数を指定します。
product-name	アップグレードが実行される製品の名前を指定します。 製品名を指定しないと、製品名は共通であると見なされます。 以下の値が使用可能です。 ■ common： 共通コンポーネントを示します。 ■ Risk Authentication： Risk Authentication を示します。 **注**: Risk Authentication をアップグレードする前に、共通コンポーネントをアップグレードしてください。
prompt	アップグレード プロセスの各段階の正常完了後に、先に進むかどうかを確認するためのプロンプトを表示します。 アップグレード プロセスで、以下の段階が実行されます。 ■ アップグレード前: データベース スキーマの移行のために、さまざまな DDL および DML 操作が実行されます。 ■ アップグレード： 新しいスキーマにデータが移行されます。 ■ アップグレード後： アップグレード後に実行する必要があるクリーンアップまたはフォローアップ アクションが含まれます。 ■ 検証： アップグレードが成功したかどうかを確認します。 このオプションでは、後でアップグレード ツールを実行して、停止した場所から続行することを選択できます。 このオプションを指定しない場合、アップグレード ツールは、アップグレード プロセスが完了するまでプロンプトを表示せずに実行されます。

オプション	説明
mst	Monitoring Sleep Time（スリープ時間のモニタ）を意味します。このオプションを指定すると、アップグレード ツールは、指定した期間（分単位）スリープした後にアップグレード中の進捗状況を示す診断メッセージを出力します。デフォルト値は 2 分です。

注: リリース 1.0.x からアップグレードする場合は、$ARCOT_HOME/logs/arcot_common_upgrade.log ファイル内で以下の行を確認します。

```
Upgrade for common from version 1.0.x to version 2.0 run successfully.
```

ログ内にこの行が存在する場合、データベースが正常にアップグレードされたことが確認されます。

Risk Authentication データベースの移行

共通コンポーネント用のデータベースを移行した後、Risk Authentication コンポーネント用のデータベースを移行します。

次の手順に従ってください:

1. ARCOT_HOME ディレクトリの ca-riskauth-upgrade-2.2.9-or-3.x-8.0 ファイルの内容を抽出します。
2. 以下のディレクトリに移動します。
   `&ARCOT_HOME/tools/common/upgrade`
3. 以下のコマンドを実行します。
   ```
   java -jar arcot-common-upgrade-framework.jar --product-name
   riskfort
   ```
   コマンド オプションの説明については、「共通コンポーネント データベースの移行 (P. 62)」の表を参照してください。
4. アップグレード元のリリースに応じて、$ARCOT_HOME/logs/ ディレクトリ内の arcot_common_upgrade.log ファイル内で、以下のいずれかの行を探します。
   `Upgrade for Risk Authentication from version <your-Risk Authentication-release> to version 8.0 run successfully.`

   注: リリース 3.0 からアップグレードする場合は、以下の行を探します。

   `Upgrade for Risk Authentication from version 3.0 to version 8.0 run successfully.`

   ログ内にこの行が存在する場合、データベースが正常にアップグレードされたことが確認されます。

Risk Authentication の既存のリリースのアンインストール

Risk Authentication の既存のリリースをアンインストールするには、以下の手順に従います。 また、アプリケーション サーバにインストールされている Risk Authentication コンポーネント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. 以下の手順を実行して、Risk Authentication の既存のリリースをアンインストールします。
   a. 以下のコンポーネントをシャットダウンします。
      - Risk Authentication サーバ
      - ケース管理キュー サーバ
      - Risk Authentication のその他のコンポーネントが展開されているすべてのアプリケーション サーバ
   b. CA Advanced Authentication が開いていないことを確認します。
   c. INI ファイル、および Risk Authentication の設定関連のその他のファイルがすべて閉じられていることを確認します。
   d. arcot/ ディレクトリに移動します。
   e. $ARCOT_HOME/Uninstall_Arcot RiskFort/ ディレクトリに移動します。
   f. Uninstall Arcot RiskFort.exe ファイルをダブルクリックします。
   g. ［Complete Uninstall］を選択します。
   h. ARCOT_HOME ディレクトリに残っているファイルをすべて削除します。
2. アプリケーション サーバから、CA Advanced Authentication、ユーザ データ サービス、およびサンプル アプリケーション Web アプリケーションを展開解除します。詳細については、アプリケーション サーバのドキュメントを参照してください。

Risk Authentication の再インストール

Risk Authentication を単一システムに展開しているか、または分散システムに展開しているかに応じて、以下のいずれかのセクションで説明されているタスクを実行します。

- 単一システムへの Risk Authentication の再インストール
- 分散システムへの Risk Authentication の再インストール

単一システムに Risk Authentication を再インストールする方法

単一システムに Risk Authentication を再インストールするには、以下のセクションで説明されているタスクを実行します。 アップグレード操作中に事前に移行したデータベースを使用します。

重要: この情報は、Risk Authentication の新規インストール、*単一システムへの Risk Authentication の展開*、および *Windows への Risk Authentication のインストール*に適用されます。

1. Risk Authentication をインストールします。

   注: Risk Authentication のインストール時には、%ARCOT_HOME%¥conf¥ ディレクトリ内の arcotcommon.ini と同じプライマリおよびバックアップ データベース詳細を指定してください。

2. データベースのセットアップを確認します。
3. アプリケーション サーバを準備します。
4. CA Advanced Authentication を展開します。
5. CA Advanced Authentication にログインします。

   重要: MA パスワードは、インストール中に実行したブートストラップ プロセス中にリセットされるため、デフォルト パスワードではなく現在の MA パスワードを使用してください。

6. Risk Authentication サーバを起動します。
7. ケース管理キュー サーバを起動します。
8. インストールを確認します。

   注: サーバの起動中に警告が表示される場合、およびトランザクションが失敗する場合、アップグレードは正常に実行されていません。「（エラーの場合のみ）初期設定への復帰」の手順に従って、初期設定に戻すことができます。

9. ユーザ データ サービスを展開します。
10. サンプル アプリケーションを展開します。

分散システムに Risk Authentication を再インストールする方法

分散システムに Risk Authentication を再インストールするには、以下のタスクを実行します。 アップグレード操作中に事前に移行したデータベースを使用します。

注: これらのセクションの情報は、Risk Authentication の新規インストール、*分散システムへの Risk Authentication の展開*、および *Windows への Risk Authentication のインストール*に適用されます。

1. 1 つ目のシステムへの Risk Authentication のインストール
2. データベースのセットアップの確認
3. アプリケーション サーバの準備
4. CA Advanced Authentication の展開
5. CA Advanced Authentication へのログイン
6. Risk Authentication サーバの起動
7. ケース管理キュー サーバの起動
8. インストールの確認
9. ユーザ データ サービスの展開
10. 2 つ目のシステムへのインストール
11. 2 つ目のシステムへのサンプル アプリケーションの展開
12. Risk Authentication サーバとの通信用サンプル アプリケーションの設定

アップグレード後のタスクの実行

このセクションでは、アップグレード後に実行する必要があるタスクについて説明します。

次の手順に従ってください:

1. アップグレードの前にデータベース レプリケーションを無効にした場合は、Risk Authentication 8.0 へのアップグレード後に、バックアップ データベースのレプリケーションを有効にする必要があります。
2. Risk Authentication 2.2.7 で以下のポートに SSL が設定されていることを確認します。
   - Risk Authentication サーバ インスタンスの Server Management プロトコル用のポート： 7980
   - ケース管理キュー サーバ インスタンスの Case Management Queuing Administration プロトコル用のポート： 7780
3. 以下の手順に従って、SSL を再設定します。
   - CA Advanced Authentication と Risk Authentication サーバ間： ポート 7980
   - CA Advanced Authentication とケース管理キュー サーバ間： ポート 7780

   注: インスタンス管理やプロトコル設定などのほとんどの管理タスクは、Risk Authentication 8.0 の CA Advanced Authentication でこれらのポートを使用して実行されるため、この設定が必要です。

   CA Advanced Authentication と Risk Authentication サーバまたはケース管理キュー サーバ間の SSL の設定手順については、「CA Risk Authentication 管理ガイド」の「SSL の設定」の章を参照してください。
4. ［その他の設定］画面で組織の基準通貨コードを設定します。

   注: 組織に固有の基準通貨コードの設定の詳細については、「CA Risk Authentication 管理ガイド」の「グローバル設定の管理」の章を参照してください。
5. スコアが 0 の何らかのルールがあり、これらのルールをスコアリングに使用する場合には、1 または 2 のように、ゼロ以外の値にスコアを変更します。

廃止されたルールと新規ルールの置き換え

リリース 8.0 では、4 つの事前定義済みルールが廃止されました。 廃止されたこれらのルールに対して、代替ルールが導入されました。 以下の表に、廃止されたルールと新規ルール、およびルールの短縮名を示します。

廃止されたルール名とルールの短縮名	新規ルール名とルールの短縮名
DeviceID Known （DEVICEIDCHECK）	Unknown DeviceID （UNKNOWNDEVICEID）
Device MFP Match （SIGMATCH）	Device MFP Not Match （MFPMISMATCH）
User Associated with DeviceID （USERDEVICEASSOCIATED）	User Not Associated with DeviceID （USERDEVICENOTASSOCIATED）
User Known （USERKNOWN）	Unknown User （UNKNOWNUSER）

重要: これらのルールは廃止されましたが、引き続き使用可能であり、アップグレード後に使用できます。 ルール式に必要な変更を加えて、廃止されたルールを、対応する新しいルールで置き換えることを推奨します。

廃止された 4 つのルールのいずれかに対して、ルールが No に評価される場合、ルールは一致したと考えられます。 その後、それはスコアリングに使用されます。 対照的に、その他の事前定義済みの各ルールは、Yes に評価されると一致したと考えられます。

リリース 8.0 で導入された 4 つの新規ルールのいずれかに対して、ルールが Yes に評価される場合、ルールは一致したと考えられます。このように、4 つの新しいルールはその他の事前定義済みルールと一致しています。

以下の表に、廃止されたルールと新規ルールの違いを強調する例を示します。

サンプル ユース ケース	廃止されたルール	廃止されたルールの結果	新規ルール	新規ルールの結果
ユーザが Risk Authentication データベースに存在しない。	USERKNOWN	いいえ	UNKNOWNUSER	はい

DeviceID が Risk Authentication データベースに存在しない。	DEVICEIDCHECK	いいえ	UNKNOWNDEVICEID	はい
MFP が Risk Authentication データベースに存在しない。	SIGMATCH	いいえ	MFPMISMATCH	はい
ユーザが DeviceID と関連付けられていない。	USERDEVICEASSOCIATED	いいえ	USERDEVICENOTASSOCIATED	はい

次の手順に従ってください：

1. CA Advanced Authentication にログインします。
2. すべての組織およびルール セット用のルール設定レポートで、［ルール式］列に一覧表示された短縮名のいずれかが、廃止された短縮名のリストに属するかどうかを確認します。
3. ルールが廃止された短縮名を使用する場合で、廃止された短縮名を使用したくない場合には、対応する新しい短縮名を使用します。

   ルール式を変更する方法

   a. GA または OA として CA Advanced Authentication にログインします。
   b. GA としてログインして、システム ルール セットに対してこの手順を実行する場合は、［サービスおよびサーバの設定］をクリックします。
   c. GA または OA としてログインして単一の組織に対してこの手順を実行する場合は、以下の手順に従います。
      - ［組織］タブをアクティブにします。
      - ［組織の管理］に移動し、［組織の検索］リンクをクリックします。
      - ［組織の検索］ページの［検索］ボタンをクリックします。
      - 組織の名前をクリックします。
      - ［設定］タブをクリックします。
   d. サイド バー メニューの［ルール管理］に移動します。
   e. ［ルールおよびスコアリング管理］リンクをクリックします。
   f. ［ルールセットを選択してください］リストからルール セットを選択します。
   g. 変更するルールをクリックします。
   h. テキスト フィールドで作成中のルールに必要な変更を行います。
   i. 変更を保存し、［ルール ビルダ］ページを閉じます。
4. 変更したルールを運用環境に移行し、次にキャッシュをリフレッシュします。

   注: 運用環境へのルールの移行およびキャッシュのリフレッシュの詳細については、「CA Risk Authentication 管理ガイド」を参照してください。

アップグレードの問題のトラブルシューティング

このセクションでは、アップグレード時に発生する可能性があるエラーを解決するために適用できるトラブルシューティング手順について説明します。

問題:

アップグレード ツールが以下のエラーで失敗します。

```
Error Occured: IO exception while
parsing, %ARCOT_HOME%¥tools¥common¥upgrade¥xml¥arcot-common-upgrade-meta-data.xml
```

このエラーは、アップグレード ツールが arcot-common-upgrade-meta-data.xml ファイルを検出できないことが原因で発生します。

解決方法:

arcot-common-upgrade-meta-data.xml ファイルが %ARCOT_HOME%¥tools¥common¥upgrade¥xml に存在するかどうかを確認します。このエラーは通常、［**Extract To Here**］オプションを使用して、arcot-common-db-upgrade.zip ファイルを抽出していない場合に発生します。

問題:

アップグレード ツールが以下のエラーで失敗します。

```
Internal Error: Could not initialize upgrade tool. Error:: Cannot load JDBC driver class 'oracle.jdbc.driver.OracleDriver' Error Occured: Upgrade Initialization Error:oracle.jdbc.driver.OracleDriver
```

このエラーは、アップグレード ツールがデータベースに接続するための JDBC ライブラリを検出できないことが原因で発生します。

解決方法:

JDBC ライブラリが %ARCOT_HOME%¥tools¥common¥upgrade¥lib ディレクトリにコピーされているかどうかを確認します。

JDBC ライブラリがすでにコピーされている場合は、JDBC jar ファイルの名前が正しく指定されているかどうかを確認します（Arcot の共通コンポーネント用のリリース 6.0 へのデータベース移行手順に従います）。 また、データベースに対応する JDBC JAR ファイルが、arcotcommon.ini ファイルで DbType パラメータに対して設定されているかどうかを確認します。

問題:

アップグレード ツールが以下のエラーで失敗します。
"FATAL: ARCOT_HOME Environment Variable Not Set"

注: %ARCOT_HOME% が設定されていません。

解決方法:

%ARCOT_HOME% 環境変数を設定して、アップグレード ツールを実行します。

問題:

アップグレード ツールが以下のエラーで失敗します。
Error Occured: Upgrade Initialization Error:Could not create DBService instance"

解決方法:

arcotcommon.ini ファイルおよび securestore.enc ファイルで、ユーザ名とパスワードが正しく設定されているかどうかを確認します。

問題:

アップグレード ツールが以下のエラーで失敗します。
Error Occured: Upgrade Initialization Error:Io exception: The Network Adapter could not establish the connection"

解決方法:

JDBC の URL が正しいかどうか、および正しいデータベースを指しているかどうかを確認します。 データベースが動作していることを確認してください。

問題:

アップグレード ツールが以下のエラーで失敗します。
`javax.crypto.BadPaddingException: Given final block not properly padded`

データの暗号化に使用されたキー ラベルと復号化に使用されたキーが異なっています。

解決方法:

データベース内のデータを暗号化するために使用されたマスタ キー ラベルが、データを復号化するためにアップグレード ツールで使用されているキー ラベルと同じであることを確認します。 マスタ キー ラベルは、%ARCOT_HOME%/conf フォルダの securestore.enc ファイルに格納されています。

問題:

アップグレード ツールが以下のエラーまたは同様のエラーで失敗します。
`"java.sql.SQLException: ORA-20010: -1031-ORA-01031: insufficient privileges"`

arcotcommon.ini ファイルに設定されているデータベース ユーザに、データベース アップグレードを実行する十分なデータベース権限がありません。

解決方法:

アップグレードを実行している管理者に、必要なデータベース権限があることを確認します。 インストール時の権限はアップグレードにも適用できます。

問題:

アップグレード ツールが以下のエラーまたは同様のエラーで失敗します。
"ORA-01536: space quota exceeded for tablespace"

arcotcommon.ini ファイルに設定されているデータベース ユーザが、テーブルスペース内のスペース クォータを使い果たしました。

解決方法:

DBA は、ユーザのクォータを増やす必要があります。アップグレード前のデータを再インポートした後で、アップグレード ツールを再起動する必要があります。

問題:

アップグレード プロセス後、管理コンソールを起動できず、以下のエラーが返される。
ERROR : taglib.tiles.InsertTag : ServletException in '/WEB-INF/jsp/dynamic/navbar_GA.jsp': File "/WEB-INF/jsp/dynamic/navbar_GA.jsp"

管理コンソールが展開されているアプリケーション サーバの Work フォルダに、以前の管理コンソールのバージョンのキャッシュがまだ含まれています。

解決方法:

管理コンソールが展開されているアプリケーション サーバの Work フォルダをクリアして、アプリケーション サーバを再起動します。

問題:

アップグレード プロセス後、LDAP リポジトリに属する管理者が管理コンソールにログインできません。

管理者が LDAP 内で無効になっている可能性があります。

解決方法:

管理者が LDAP 内で無効になっていないことを確認します。 無効になっている管理者は、管理コンソールにログインできません。

問題:

アップグレード プロセス後、IBM DB2 データベース用の AuthMinder サーバ固有のレポートを生成できず、以下のエラーが表示される。
`DB2 SQL Error: SQLCODE=-1585, SQLSTATE=54048, SQLERRMC=null`

SYSTEM TEMPORARY テーブルスペースのページ サイズがデフォルト値の 4K に設定されている可能性があります。この値は、4K を超える列を含むレポート クエリには不十分です。

解決方法:

SYSTEM TEMPORARY テーブルスペースのページ サイズを 16K 以上に設定します。 詳細については、データベース ベンダーのドキュメントを参照してください。

（エラーの場合のみ）初期設定への復帰

サーバの起動時に警告が表示される場合、およびトランザクションが失敗する場合には、初期設定に戻したい場合があります。

次の手順に従ってください：

1. Risk Authentication 8.0 をアンインストールします。

   詳細については、「Risk Authentication のアンインストール」の章を参照してください。

2. 戻る対象の Risk Authentication リリースをインストールします。 たとえば、6.*x* または 7.*x* などです。

   注: インストール手順については、対応するリリースに付属している「*Risk Authentication* インストールおよび展開ガイド」を参照してください。

3. ARCOT_HOME_BACKUP ディレクトリがある場所に移動します。
4. 現在の ARCOT_HOME に ARCOT_HOME_BACKUP の内容をコピーします。
5. <*アプリケーション サーバで使用する JAVA_HOME*>/jre/bin 内の libArcotAccessKeyProvider.so ファイルをバックアップ ファイルで置き換えます。
6. CA Advanced Authentication や UDS などの Web コンポーネントを展開します。
7. アップグレード手順を開始する前に作成したバックアップからデータベースをリストアします。
8. Risk Authentication サーバおよびケース管理キュー サーバを起動します。
9. インストールをテストします。