CA Strong Authentication

管理ガイド

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: 管理コンソールの概要

CA Advanced Authentication 管理コンソール（以下、「管理コンソール」と呼びます）は、操作およびシステムを管理するための Web ベースのツールで、CA Advanced Authentication を管理するための一貫性のある、統一されたインターフェースを提供します。

管理コンソールは、真の *マルチテナント* アーキテクチャを備えており、コンソールの単一のインスタンスを使用して、企業内の複数の組織または事業単位を管理することを可能にします。 このモデルを使用すると、各組織または事業単位は、自身の設定を使用して個別にセットアップできます。また、管理コンソールは、システム レベルから設定データを継承し、必要に応じて、各組織の特定の設定を構築する機能を提供します。

このガイドでは、管理コンソールを使用して CA Strong Authentication をセットアップおよび管理する方法について説明します。 また、CA Strong Authentication でサポートしている Windows および UNIX ベースの両方のプラットフォームについて説明します。

ここでは、管理コンソールのインターフェースおよびサポートされる管理者階層について説明します。

注: 推奨するデスクトップ画面の解像度は、管理コンソールへのアクセスに使用するシステムの最適な解像度です。

重要: このドキュメントでは、コード オブジェクトやその他の製品の一部に Arcot、WebFort、RiskFort、WebFort、RiskMinder、AuthMinder という用語が使用されています。 ArcotID は、現在、CA Auth ID と呼ばれています。また、このガイドには標準的なフォーマットのガイドラインに従っていないトピックが一部あります。

管理コンソールについて

管理コンソールはブラウザ ベースのグラフィカル ユーザ インターフェースです。 管理コンソールを使用すると、展開しているすべての CA Strong Authentication インスタンスを管理できます。*インスタンス*は、システムにインストールされている CA Strong Authentication サーバを表します。

管理コンソールでは、CA Strong Authentication サーバの設定、ユーザおよび管理ロールの作成を行います。また、以下の管理操作および設定タスクを実行します。

- サーバ インスタンスの設定およびリフレッシュ
- サーバとその他の CA Strong Authentication コンポーネント間の通信パラメータの設定
- 組織、管理者、LDAP にマップされた組織、およびユーザとその認証情報の管理
- プラグインの設定
- 認証ポリシーの設定
- 認証情報プロファイルの設定
- 管理、トランザクション、および設定の各レポートの生成

実行を許可されているタスクが、管理コンソール 上のさまざまなタブを介して表示されます。 これらのタスクは、所属するユーザ グループ（またはロール）、およびロールに付与された管理者権限に基づきます。

サポートされるロール

*ロール*を使用すると、ユーザ、または同様の責任を共有するユーザ セットに、どの操作および権限を割り当てるかを指定できます。ユーザがロールに割り当てられると、そのロールに関連付けられている*タスク*と呼ばれる一連の機能をユーザは利用できるようになります。 その結果、管理者はシステム内の各ユーザに割り当てるタスクを細かく制御できます。

管理コンソールを使用すると、管理階層のセットアップ、および権限の管理者への割り当てを柔軟に行うことができます。 それぞれに異なる管理権限を持つ、複数のレベルの管理者を作成できます。 また、他のユーザに管理タスクを委任できる管理者を作成することもできます。

管理コンソールは、以下のタイプのロールをサポートします。

- ユーザ (P. 17)
- デフォルトの管理ロール (P. 19)
- カスタム ロール (P. 25)

ユーザ

オンライン アプリケーション システムのすべてのエンド ユーザは、管理コンソール内でユーザと呼ばれます。 このユーザは、Active Directory などの LDAP リポジトリまたは CA Strong Authentication データベースに存在できます。

ユーザが LDAP システムにすでに存在する場合、LDAP 属性を CA Strong Authentication でサポートされる属性にマップします。 詳細については、「LDAP リポジトリでの組織の作成 (P. 192)」を参照してください。

CA Strong Authentication データベースにユーザを登録するには、リポジトリ タイプが Arcot データベースである組織を選択します。詳細については、「LDAP リポジトリでの組織の作成 (P. 192)」を参照してください。

管理ロールのスコープ

管理コンソールの管理ロールの*スコープ*は、以下で構成されます。

- 特定のロールが割り当てられた管理者が管理できるすべての組織。
- ロールに関連付けられた権限。

スコープに関する注意事項

管理ロールを作成する際には、以下の点に注意する必要があります。

- マスタ管理者 (P. 21) のスコープは、*すべての組織*です。また、この管理者は、既存または今後作成される *すべての*組織を管理します。
- 管理者（グローバル管理者 (P. 23)、組織管理者 (P. 24)、またはユーザ管理者 (P. 25)）は、管理者が属する組織にスコープがある場合、自分より少ない権限を持つピアおよびロールを管理できます。

  たとえばグローバル管理者は、ほかのグローバル管理者、組織管理者、およびユーザ管理者を管理できます。 ただし、マスタ管理者は管理 *できません*。
- グローバル管理者 (P. 23) ロールのスコープを、「すべての組織」に設定することが *できます*。その場合、既存のすべての組織に加えて、将来作成される組織もこのロールで管理できます。
- 組織管理者 (P. 24)、またはユーザ管理者 (P. 25) は、特定の組織のみを管理するように制限できます。
- 管理者がカスタム ロール (P. 25) を使用して作成された場合、派生した管理者は親のレベルと同じレベルに属します。

  たとえば、グローバル管理者から MyGlobalAdmin 管理者が派生した場合、MyGlobalAdmin は、グローバル管理者と認識されます。 これは、MyGlobalAdmin に組織管理者またはユーザ管理者より少ない権限を割り当てた場合も同じです。

  注: *組織管理者*および*ユーザ管理者*ロールは、すべての組織のスコープを使用して定義 *しないでください*。

デフォルトの管理ロール

マスタ管理者 (P. 21)と呼ばれる組み込みの管理者は、高いレベルの設定を実行できます。CA Advanced Authentication システムを管理したり、ビジネス データにアクセスするために、ユーザに管理ロールを割り当てることができます。 管理ロールは、通常、職務権限プロファイル、およびこれらの権限が適用可能なスコープに基づく一連の権限で構成されます。 管理者権限を持つユーザは、管理者ユーザと呼ばれます。

注: 各管理ロールで利用可能な権限の全体的なリストについては、「管理権限の要約 (P. 381)」を参照してください。

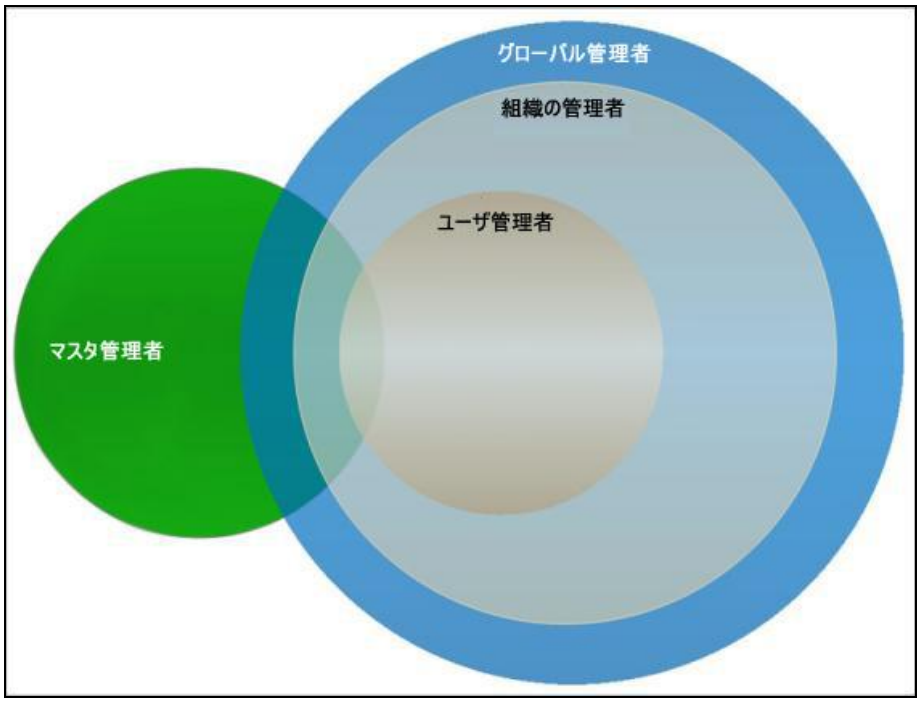
管理コンソールでは、以下の事前定義済み管理ロールがサポートされます。

- MA （マスタ管理者） (P. 21)
- GA （グローバル管理者） (P. 23)
- OA （組織の管理者） (P. 24)
- UA （ユーザ管理者） (P. 25)

また、カスタム ロール (P. 25)も作成できます。

注: 管理者もシステムのユーザと見なされます。

以下の図に、管理ロールと、管理ロールで使用可能な権限の関係を示します。 また、この図の後のセクションでは、サポートされている管理者レベルを詳しく説明します。



注: 権限は階層的に分配されているため、管理者が固定された境界を越えて機能にアクセスすることはできません。 各レベルには、事前定義済み権限またはロールがあります。

MA（マスタ管理者）

MA （Master Administrator、マスタ管理者）は、システムのスーパーユーザです。MA にはシステム全体に対して無制限のアクセス権があります。MA のスコープはすべての組織です。このため、既存の組織、自身で作成する組織、または今後作成されるいずれの組織も管理できます。

MA は、以下の操作を行うことができます。

- インストールの後にシステムを初期化（ブートストラップ）する。
- UDS 接続パラメータを設定する。
- 管理コンソールおよびユーザ データ サービス用に、組織に対するグローバル設定やキャッシュ リフレッシュ設定を設定する。
- カスタム ロケールを設定する。
- デフォルトの組織を設定する。
- Web サービスの認証および許可を有効にする。
- CA Strong Authentication サーバの通信パラメータを設定する。
- CA Strong Authentication サーバ インスタンスを設定および管理する。
- CA Strong Authentication サーバのプロトコルを設定する。
- 管理コンソールおよびサーバのコンポーネントの認証メカニズム、およびその他の設定を設定する。
- カスタム プラグインを使用して CA Strong Authentication の機能を拡張する場合に、プラグインを登録する。

  注: プラグインを登録する方法の詳細については、「プラグインの登録と更新 (P. 92)」を参照してください。 プラグインの設定の詳細については、「プラグインの設定」を参照してください。
- 組織を作成および管理する。
- 必要に応じて、管理者ロール（グローバル管理者、組織の管理者、またはユーザ管理者）を作成し、管理する。
- カスタム ロール (P. 25) を作成および管理する。
- インスタンス統計を生成する。

管理コンソールが正常にインストールされたら、最初に MA としてログインします。 インストール直後の MA アカウント（*masteradmin*）には、デフォルト パスワード（master1234!）が設定されています。 初めてログインした後、このパスワードを変更することをお勧めします。

データを追跡および分析するために、MA はすべての管理者アクティビティの包括的なレポートを生成できます。　また、システム内のほかの管理者のアクティビティのレポートも生成できます。 さらに、すべての組織のレポートおよびすべてのサーバ設定のレポートも生成できます。

マスタ管理者のパスワードのリセット

誤ったパスワードを複数回入力したために MA アカウントのパスワードがロックされた場合は、以下の手順に従います。

arcot-masteradmin-password-reset-2.0.sql スクリプトを実行して、パスワードをリセットします。 このスクリプトは *<INSTALL_HOME>¥dbscripts¥<database>¥* フォルダにあります。 スクリプトを実行した後、MA はデフォルト パスワードを使用して管理コンソールにログインし、パスワードをリセットする必要があります。

GA（グローバル管理者）

GA （Global Administrator、グローバル管理者）は、管理階層の 2 番目のレベルに位置します。これらの管理者が実行できる MA のタスクはごくわずかです。

デフォルトでは、GA はシステム内のすべての組織に対するスコープを持っています。GA に特定の組織のみを管理させるには、GA アカウントの作成時に指定する必要があります。

GA は、以下の操作を行うことができます。

- 必要に応じて、他のグローバル管理者、組織の管理者、ユーザ管理者を作成し、管理する。
- 管理コンソールの認証ポリシーを設定する。
- 管理コンソールのキャッシュ リフレッシュ設定を設定する。
- 必要に応じて、組織を作成し、管理する。

  注: これには組織の詳細の編集が含まれます。
- 必要に応じて、ユーザを作成し、管理する。
- ASSP（Adobe 署名サービス プロトコル I) および SAML（Secure Assertion Markup Language）を設定する。
- ユーザ認証情報を管理する。
- サポートされる認証メカニズム用の CA Strong Authentication プロファイルおよびポリシーを設定する。
- 設定を全体または 1 つの組織に割り当てる。
- 登録したプラグインを設定する。
- RADIUS クライアントおよび RADIUS プロキシ サーバを設定する。

利用可能な情報を追跡し、分析するために、GA は、管理権限の範囲内の組織に対する管理アクティビティ、設定、および認証情報管理のすべてのレポートを生成し、表示できます。 また、割り当てられているすべての組織、ユーザ管理者、およびユーザ のレポートを表示できます。

OA（組織の管理者）

OA （Organization Administrator、組織の管理者）は、管理階層の 3 番目のレベルに位置します。OA は、MA または GA によって割り当てられた組織、および組織に属するユーザの管理に関連するすべてのタスクを実行できます。

OA は、以下の操作を行うことができます。

- 必要に応じて、ほかの組織管理者またはユーザ管理者を作成し、管理する。
- 権限の範囲内の組織に属するユーザを作成し、管理する。
- 権限の範囲内の組織を管理する。
- 権限の範囲内の組織のキャッシュをリフレッシュする。
- 組織の認証ポリシーを設定する。
- 組織固有の設定を管理（更新）する。

OA を作成する際には、管理のスコープを指定します。 指定しない場合、いずれの組織も管理できません。

OA は、管理権限の範囲内の組織のための管理アクティビティ、設定、およびトランザクションの各レポートを生成し、表示できます。 また、割り当てられているすべてのユーザ管理者およびユーザ のレポートを表示できます。

UA（ユーザ管理者）

UA （User Administrator、ユーザ管理者）ロールは、管理階層の最下位のレベルに位置します。 UA は、MA または GA のいずれかによって割り当てられた組織のユーザ管理に関連するすべてのタスクを実行できます。 これには以下が含まれます。

- 必要に応じて、ほかの UA を管理する。
- 必要に応じて、エンド ユーザを作成し、管理する。

  注: これにはユーザの詳細の編集が含まれます。
- ユーザ認証情報を管理する。

UA を作成する際には、管理のスコープを指定します。 指定しない場合、いずれの組織も管理できません。

UA は、管理権限の範囲内の組織のユーザと UA アクティビティの各レポートを生成し、表示できます。

カスタム ロール

MA は、以下のいずれかの事前定義済みの親ロールから権限のサブセットを継承する新しい管理ロールを作成することもできます。

- GA （グローバル管理者）（P. 23）
- OA （組織の管理者）（P. 24）
- UA （ユーザ管理者）（P. 25）

これらのロールは*カスタム ロール*と呼ばれ、親ロールに関連付けられているデフォルト権限のいくつかを*無効にする*ことによって作成されます。たとえば、GA の*組織の作成権限*を無効にする場合、この権限を無効にすることによってカスタム ロールを作成できます。

作成したカスタム ロールは、管理ロールの作成または更新時にロール オプションとして利用できます。 カスタム ロールは、作成するだけではなく更新および削除も行えます。

第 2 章: はじめに

この章では、CA Strong Authentication を正常にインストールし、管理コンソールを展開した後で、*マスタ管理者*として管理コンソールにログインし、システムを初期化するための手順について説明します。

注: CA Strong Authentication のインストール、管理コンソールの展開、およびブートストラップの詳細については、「CA Strong Authentication インストール ガイド」を参照してください。

管理コンソールへのアクセス

デフォルトの MA（マスタ管理者）ロールは、初めて管理コンソールにログインするために使用します。

次の手順に従ってください:

1. Web ブラウザを使用して、管理コンソールにアクセスするための URL を入力します。 デフォルトのアドレスは以下のとおりです。

   http://<hostname>:<app_server_port>/arcotadmin/masteradminlogin.htm

   ホスト名

   管理コンソールを展開したシステムのホスト名または IP アドレスを指定します。

   app_server_port

   管理コンソールがリスンするポートを指定します。

2. ［*パスワード*］フィールドに、ブートストラップ ウィザードで設定したパスワードを指定し、［*ログイン*］をクリックします。

管理コンソール使用時のセキュリティに関する推奨事項

管理コンソールにアクセスするときには、以下のベスト プラクティスを確認してください。

- ほかのアプリケーションとブラウザ セッションを共有しない。
- 管理コンソールを操作しながらほかのサイトを開かない。
- ブラウザの別のタブでほかのサイトを開かない。
- 管理コンソールに対して厳しいパスワード制限を実施する。
- 管理コンソールの使用後は必ずログアウトする。
- セッションの終了後にブラウザ ウィンドウを閉じる。
- ユーザが実行する必要のあるタスクに従って適切な役割をユーザに割り当てる。

パスワードとプロファイル情報の変更

［マイ プロファイル］ページを使用して、現在のパスワードと、今後実行する管理者関連のすべてのタスクがデフォルトで反映されている基本設定を変更します。

必ず MA としてログインしてください。

次の手順に従ってください:

1. 管理コンソールのヘッダにある［*マスタ管理者*］リンクをクリックします。
2. ［*パスワードの変更*］セクションで、以下を指定します。
   a. *現在のパスワード*
   b. *新規パスワード*
   c. *［パスワードの確認］*フィールドに、新しいパスワードを再入力します。
3. *［管理者基本設定］*セクションで、以下を指定します。
   a. 優先組織を有効にするかどうか。

      この組織は、今後実行するすべての管理者関連のタスクの［*組織*］フィールドで、デフォルトで選択されます。たとえば管理者やユーザを検索する場合、デフォルトでは、優先組織内で管理者が検索されます。
   b. ［*組織*］フィールドでデフォルトで選択される*優先組織*。
   c. 優先される*日付/時刻形式*。

      この日付/時刻形式は、*最終ログオン*のタイム スタンプおよび管理コンソール内のほかのすべてのタイム スタンプで今後使用されます。 さらに、レポート データ（トランザクション日付など）ではこの日付/時刻形式を使用します。
   d. 管理コンソールのログインで優先される*ロケール*。

      ロケールを設定する方法の詳細については、「カスタム ロケールの設定 (P. 43)」を参照してください。 CA Strong Authentication ではデフォルトで英語（米国）を使用します。
   e. 優先される*タイム ゾーン*。

このタイム ゾーンは、*最終ログイン*のタイム スタンプおよび管理コンソール内のほかのすべてのタイム スタンプで今後使用されます。 さらに、レポート データ（トランザクション日付など）やその他の日付およびタイム スタンプで、このタイム ゾーンが使用されます。

*タイム ゾーン*のデフォルトは［*GMT*］です。

4. *［保存］*をクリックします。

管理コンソールの設定

CA Strong Authentication 固有の設定を行う前に、管理コンソールのグローバル設定を行うことをお勧めします。

注: 以下のすべての管理コンソール設定では、MA としてログインしていることを確認してください。

UDS 接続の更新

ユーザ データ サービス (*UDS*) は、組織によって展開されたサードパーティのデータ リポジトリ（LDAP ディレクトリ サーバなど）へのアクセスを可能にするためのユーザ仮想化レイヤです。 CA Strong Authentication および管理コンソールは、UDS を使用して既存のデータにシームレスにアクセスしたり、エンド ユーザの情報を活用したりすることができます。標準の CA Strong Authentication SQL データベース テーブルにデータを複製する必要はありません。

CA Strong Authentication はリレーショナル データベース（RDBMS）から、または LDAP サーバから直接ユーザ データにアクセスできます。

- リレーショナル データベースを使用する場合は、インストール後の設定の一環として CA Strong Authentication スキーマをデータベースにシードする必要があります。
- LDAP ディレクトリ サーバを使用していて、このサーバに CA Strong Authentication サーバと管理コンソールからシームレスにアクセスしたい場合は、インストール後の設定の一環として UDS を展開する必要があります。

デフォルトの UDS 接続設定を更新するには、［ユーザ データ サービス接続設定］ページを使用します。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。

   ［*UDS 接続設定*］ページが表示されます。
3. ［*ユーザ データ サービス接続 設定*］セクションで、以下の表に示すパラメータを指定します。 このページのほとんどのパラメータは必須です。

   プロトコル

   管理コンソールを使用して UDS サービスに接続するプロトコル。使用可能なオプションは、以下のとおりです。

   - TCP
   - 一方向 SSL
   - 双方向 SSL

デフォルト値： TCP

ホスト

UDS を使用できるシステムの IP アドレスまたはホスト名。 デフォルト値の localhost は機能しません。

デフォルト値： localhost

ポート

UDS が使用可能なポート。

デフォルト値： 8080

アプリケーション コンテキスト ルート

アプリケーション サーバに UDS を展開するときに指定したアプリケーション コンテキスト。

デフォルト値： arcotuds

読み取りタイムアウト（ミリ秒）

UDS からのレスポンスを待機する最大時間（ミリ秒）。

デフォルト値： 10000

アイドル タイムアウト（ミリ秒）

リクエストに応答しないアイドル接続が閉じる前の時間（ミリ秒）。

デフォルト値： 30000

サーバ ルート証明書

UDS サーバの CA 証明書ファイルのパス。 このファイルは PEM 形式である必要があります。

クライアント証明書

管理コンソールの CA 証明書ファイルのパス。このファイルは PEM 形式である必要があります。

クライアント秘密キー

CA の秘密キーが含まれるファイルの場所。 パスは絶対パス、または ARCOT_HOME への相対パスのいずれにもできます。

最小接続数

CA Strong Authentication サーバと UDS サーバの間で作成される接続の最小数。

デフォルト値： 4

最大接続数

CA Strong Authentication サーバと UDS サーバ間で作成できる接続の最大数。

デフォルト値： 32

接続タイムアウト(ミリ秒)

UDS サービスが到達不能になるまでのミリ秒単位の最大時間。

デフォルト値： 30000

4. *[保存]* をクリックします。
5. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ (P. 36)」を参照してください。

UDS パラメータの更新

UDS パラメータを更新するには、［UDS 設定］ページを使用します。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. サイドバー メニューの［*UDS 設定*］セクションで、［*UDS 設定*］リンクをクリックして、対応するページを表示します。
4. このページで、以下の表で説明するパラメータを指定します。 このページのパラメータはすべて必須です。

検索設定

検索結果の最大数

Administration Console 内でのすべての検索操作に対して返されるレコードの最大数。

デフォルト値： 500

LDAP Configuration

注: これらのフィールドは管理コンソールを使用して編集できません。 これらのパラメータの設定の詳細については、「CA Strong Authentication インストール ガイド」の「LDAP 接続プールの有効化」を参照してください。

LDAP 接続プールの初期サイズ

プール内に作成される UDS と LDAP 間の接続の初期数。

LDAP 接続プールの最大サイズ

UDS と LDAP 間で許可される接続の最大数。

LDAP 接続プールの推奨サイズ

UDS と LDAP 間の推奨される接続数。

LDAP 接続プールのタイムアウト（ミリ秒）

新しい接続がリクエストされたとき、UDS が LDAP からのレスポンスを待機する時間。

認証トークンの設定

パージ間隔（秒）

トークンが失効した後に、認証トークンがデータベースから消去される前の最大間隔。

デフォルト値： 3600

有効期間（秒）

発行済み認証トークンが失効する前の最大期間（デフォルトは 1 日）。

デフォルト値： 86400

5. *［保存］*をクリックします。
6. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法の詳細については、「キャッシュのリフレッシュ（P. 36）」を参照してください。

キャッシュのリフレッシュ

管理コンソールは特定のデータをキャッシュします。これにより、頻繁にアクセスされるコンソール ページおよび UDS データを高速に処理します。通常、組織およびロールはキャッシュされます。 CA Strong Authentication はシステム レベルおよび組織レベルでキャッシュされるデータを保持します。

システム レベルでキャッシュされるデータ

以下のデータがシステム レベルでキャッシュされます。

- **すべてのシステム レベル設定**
  - UDS 設定および UDS 接続
  - LDAP 接続プールの詳細
  - グローバル キー ラベル
  - アカウント タイプの詳細
  - カスタム ロール
- **グローバル データ**
  - 暗号化セット
  - ローカライゼーションの設定
  - 電子メールと電話のタイプ
  - 認証および許可の設定
- **すべての組織に適用可能なリソース**
  - すべての組織に適用可能なグローバル アカウント タイプ

組織レベルでキャッシュされるデータ

以下のデータが組織レベルでキャッシュされます。

- **個別の組織に適用可能なデータ**
  - 暗号化セット、ローカライゼーション設定、および電子メールと電話のタイプなどのグローバル データを参照しない設定
- **組織のセットに適用可能なリソース**
  - 組織に固有のアカウント タイプ

重要: システム レベルと組織レベルの両方での変更が関係するデータの設定を変更するときには、先にシステム キャッシュがリフレッシュされ、次に組織のキャッシュがリフレッシュされます。 変更時にこの順序でキャッシュのリフレッシュが行われることにより、整合性のない動作が生じる場合があります。

キャッシュのリフレッシュ順序に関する例

アカウント タイプの詳細およびグローバル アカウント タイプはシステム レベルでキャッシュされます。 アカウント タイプを作成する場合は、それがグローバルか組織に固有かどうかに関係なく、システム キャッシュをリフレッシュします。 また、アカウント タイプが組織固有の場合は、スコープ内のすべての組織のキャッシュをリフレッシュする必要があります。 アカウント タイプの詳細については、「アカウント タイプの設定 (P. 45)」を参照してください。

必要な権限

MA と GA は、管理コンソールのキャッシュおよび CA Strong Authentication サーバのすべてのインスタンスをリフレッシュできます。 MA、GA、および OA は、そのスコープ内の組織のキャッシュをリフレッシュできます。

キャッシュのリフレッシュ

変更を有効にするために、影響を受けるサーバ インスタンスのキャッシュをリフレッシュします。 CA Strong Authentication には、管理者が管理コンソールからすべてのサーバ インスタンスのキャッシュをリフレッシュできる*統合キャッシュ リフレッシュ*機能があります。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。

   サイド バー メニューの［*システム設定*］セクションで、［*キャッシュのリフレッシュ*］リンクをクリックして、対応するページを表示します。
3. 以下のいずれか、または両方を選択します。

- 管理コンソール、ユーザ データ サービス（展開されている場合）、およびすべての CA Strong Authentication サーバ インスタンスのキャッシュ設定をリフレッシュするには、［*システム設定をリフレッシュ*］を選択します。
- ［*組織キャッシュのリフレッシュ*］を選択し、権限の範囲内のすべての組織のキャッシュ設定をリフレッシュします。

4. ［OK］をクリックします。

キャッシュ リフレッシュ リクエストのステータスの表示

管理コンソールでは、キャッシュ リフレッシュ リクエストの詳細を表示できます。［キャッシュ リフレッシュ ステータスの確認］ページでは、キャッシュ リフレッシュ リクエストを、その一意の識別子またはリクエストのステータスに基づいて表示できます。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. サイド バー メニューの［*システム設定*］セクションで、［*キャッシュ リフレッシュ ステータスの確認*］リンクをクリックして、対応するページを表示します。

4. 以下のフィールドのいずれかを使用して、キャッシュ リフレッシュ リクエストの詳細を指定します。

Request ID

キャッシュ リフレッシュ リクエストの一意の識別子の定義

ステータス

キャッシュ リフレッシュ リクエストの詳細を表示したいステータスを選択します。キャッシュ リフレッシュ リクエストのステータスは以下のいずれかになります。

- すべて： 受信したすべてのキャッシュ リフレッシュ リクエストを一覧表示します。
- 進行中： 現在処理中のキャッシュ リフレッシュ リクエストをすべて一覧表示します。
- 失敗： 失敗したキャッシュ リフレッシュ リクエストを一覧表示します。
- 成功： 正常に処理されたキャッシュ リフレッシュ リクエストを一覧表示します。

5. ［*検索*］をクリックして、キャッシュ リフレッシュ リクエストを表示します。

検索結果には以下の項目が一覧表示されます。

- キャッシュ リフレッシュ リクエストの一意の識別子
- リクエストを受信した時間
- キャッシュ リフレッシュ リクエストによって影響を受けた組織
- イベント タイプ
- キャッシュ リフレッシュ リクエストによって影響を受けた CA Strong Authentication のコンポーネント

  Resource

  リフレッシュされた CA Strong Authentication のリソースを指定します。 以下の値が使用可能です。

  - AdminConsole

    管理コンソールとユーザ データ サービスの場合

  - WebFort

    CA Strong Authentication サーバの場合

サーバ インスタンス ID

リフレッシュされたサーバ インスタンスの一意の識別子を指定します。

- 管理コンソールとユーザ データ サーバの場合は、この値は arcotcommon.ini ファイルに設定された InstanceID パラメータから取得されます。
- CA Strong Authentication サーバの場合は、CA Strong Authentication サーバのインスタンス名です。デフォルトでは、ホスト名と一意の識別子の組み合わせです。

サーバ インスタンス名

リフレッシュされた CA Strong Authentication コンポーネントのインスタンス名を指定します。 以下の値が使用可能です。

- Arcot 管理コンソール
- ユーザ データ サービス
- CA Strong Authentication サーバ インスタンスの名前。デフォルトでは、ホスト名と一意の識別子の組み合わせです。

ホスト名

リフレッシュされたコンポーネントがインストールされているシステムの名前を指定します。

ステータス

キャッシュ リフレッシュ リクエストのステータスを指定します。

属性の暗号化の設定

デフォルトでは、CA Strong Authentication は、インストール時にシードしたデータベース テーブルにプレーンな形式でユーザ関連データを格納します。

注: データを暗号化するには、［属性暗号化設定］ページを使用して、暗号化するユーザ属性を選択します。 暗号化された形式で格納できる属性のリストについては、「マルチバイト文字および暗号化されるパラメータ (P. 325)」を参照してください。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをアクティブにします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。

   サイド バー メニューの［**システム設定**］セクションで、［*属性暗号化設定*］リンクをクリックして、対応するページを表示します。

   注: ユーザ識別子属性を暗号化することを選択する場合は、一意にユーザを識別する際に使用する以下の属性もすべて暗号化されます。

   - ユーザ ID
   - アカウント ID
   - アカウント ID 属性
3. ［*暗号化する属性の選択*］セクションで、［*暗号化用に利用可能な属性*］から暗号化する属性を選択し、［*暗号化用に選択した属性*］に指定します。

   ［>］ボタンをクリックして、選択した属性を目的のリストに移動します。 ［>>］ボタンをクリックして、すべての属性を目的のリストに移動することもできます。

   注: 一度に複数の属性を選択するには、*Ctrl* キーを押したまま選択します。

   ［*暗号化用に選択した属性*］リストには、暗号化された形式で格納される属性がすべて表示されます。
4. ［*データ マスキング設定*］セクションで、以下の表に示すパラメータを指定します。

   Type

ドロップダウン リストから、暗号化を設定した属性をマスクするかマスク解除するオプションを選択します。

開始位置からの文字数

実際のデータ文字列の開始位置からのマスクまたはマスク解除する文字の数。

終了位置からの文字数

実際のデータ文字列の終了位置からのマスクまたはマスク解除する文字の数。

マスキング文字

実際のデータをマスクする（非表示にする）ために使用する文字。

たとえば、暗号化するように設定されたユーザ名をマスクする場合、［*開始位置からの文字数*］、［*終了位置からの文字数*］、［マスキング文字］を 2、2、x に指定すると、ユーザ名「mparker」が「xxarkxx」とマスクされます。マスク解除する場合は逆になります。

5. ［保存］をクリックし、加えた変更を保存します。
6. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ（P. 36）」を参照してください。

カスタム ロケールの設定

CA Strong Authentication は*ローカライゼーション*をサポートしています。［ローカライズ設定］ページでサポートされているロケールを設定できます。

注: カスタム ロケールを設定する前に、言語を［*利用可能*］リストで選択できるように追加することができます。「CA Strong Authentication インストール ガイド」の「ローカライゼーションの準備」を参照してください。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. サイド バー メニューの［*システム設定*］セクションで、［*ローカライズ設定*］リンクをクリックして、対応するページを表示します。
4. ［*サポートされるロケールの設定*］セクションで、追加するロケールを［*利用可能*］リストから選択して［*選択済み*］リストに移動させます。

   ［>］ボタンをクリックして、選択したロケールを目的のリストに移動します。［>>］ボタンをクリックして、すべてのロケールを目的のリストに移動することもできます。

   注: 一度に複数のロケールを選択するには、*Ctrl* キーを押したまま選択します。
5. ［*デフォルト ロケールの設定*］セクションで、ドロップダウン リストから*デフォルト ロケール*を選択します。
6. ［*デフォルトの日付/時刻形式の設定*］セクションで、使用する*日付/時刻形式*を指定します。

   注: 管理者は、［マイ プロファイル］ページでロケールおよび日付/時刻形式を変更できます。
7. ［**保存**］をクリックして変更内容を保存します。
8. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ (P. 36)」を参照してください。

デフォルトの組織の設定

管理コンソールを展開すると、デフォルトで、MA アカウントと共に組織が作成されます。 この既定の組織は「*デフォルトの組織（DEFAULTORG）*」と呼ばれます。

単一の組織システムでは、新しい組織を作成する必要がないため、デフォルトの組織は有用です。 「デフォルトの組織」の設定を行い、「表示名」を変更し（基本組織情報の更新 (P. 202)を参照）、管理目的で続けて使用できます。 ただし、複数組織システムの場合には、「デフォルトの組織」の表示名を変更して設定を指定し、これをデフォルトとして続けて使用できます。または、新しい組織を作成し、「デフォルトの組織」に設定できます。

注: 通常、組織を指定*せずに*何らかの操作を実行すると、「デフォルトの組織」に対して実行されます。 たとえば、組織を指定せずに管理者を作成した場合は、「デフォルトの組織」内に作成されます。

［デフォルト組織の設定］ページでは、デフォルトの組織として使用する組織を選択できます。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. 左側のペインで、［*UDS 設定*］セクションにある［*デフォルト組織の設定*］リンクをクリックして、［デフォルト組織の設定］ページを表示します。
4. ［*デフォルトの組織*］で、［*組織名*］リストからデフォルトの組織として設定する組織を選択します。
5. ［*保存*］をクリックします。

   「デフォルトの組織が設定されました」というメッセージが表示されます。
6. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ (P. 36)」を参照してください。

アカウント タイプの設定

システムで CA Strong Authentication ユーザはすべて一意のユーザ名によって識別されます。 CA Strong Authentication *アカウント*または*アカウント ID* は、ユーザを識別するためにユーザ名に加えて使用されます。 ユーザは 1 つ以上のアカウントまたはアカウント ID を持つことができます。またアカウントまたはアカウント ID を持たないことも可能です。

たとえば、顧客の ID を使用する金融機関について考えてみます。

注: 特定の組織の 2 人のユーザが同じアカウント ID を持つことはできません。 以下の組み合わせは常に一意です。

- 組織名、アカウント タイプ、およびアカウント ID
- 組織名およびユーザ名

新しいアカウント タイプの作成

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. サイド バー メニューの［*UDS 設定*］セクションで、［*アカウント タイプの設定*］リンクをクリックして、対応するページを表示します。
4. （これが初めて追加するアカウント タイプである場合）［*新規アカウント タイプの追加*］セクションで以下の操作を行います。
   a. アカウント タイプの*名前*を入力します。
   b. アカウント タイプの*表示名*を入力します。
   c. 必要に応じて、［+］記号をクリックして［*カスタム属性*］セクションを展開し、このアカウント タイプに対して追加するカスタム属性の*名前*と*値*を指定します。
5. *割当先組織*のセクションで、以下を実行します。
   - このアカウント タイプを、既存のすべての組織および今後作成されるすべての組織に対して使用する場合は、*すべてに適用*することを選択します。

     注: このようなアカウントは、組織レベルで［*アカウント タイプの設定*］ページの［*グローバル アカウント*］の下に表示されます。

または

- アカウント タイプを割り当てる組織を［*利用可能*］リストから選択して［*選択済み*］リストに移動させます。

  注: このようなアカウントは、組織レベルの［*アカウント タイプの設定*］ページで*組織固有アカウント*として表示されます。

  ［>］ボタンをクリックして、選択した組織を目的のリストに移動します。 ［>>］ボタンをクリックして、すべての組織を目的のリストに移動することもできます。

  注: 一度に複数の組織を選択するには、*Ctrl* キーを押したまま選択します。

6. ［*作成*］をクリックします。
7. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ (P. 36)」を参照してください。

アカウント タイプの削除

既存のアカウント タイプを削除するには、削除したいアカウント タイプを［*アカウント タイプの選択*］ドロップダウン リストから選択し、［*削除*］をクリックします。

注: アカウント タイプを変更または削除した後は、展開したすべての CA Strong Authentication サーバ インスタンスをリフレッシュします。 システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ (P. 36)」を参照してください。

注: アカウント タイプに対してユーザ アカウントを作成した場合、そのアカウント タイプを削除することは*できません*。

電子メールと電話のタイプの設定

CA Strong Authentication では、ユーザと管理者を作成する際に、複数の電子メール アドレスと電話番号を指定することができます。MA はグローバル レベルで複数の電子メールと電話のタイプを設定でき、これは自動的にすべての組織で利用できるようになります。 また MA は、特定の電子メールと電話のタイプを必須として、その他のものをオプションとして指定することができます。 組織内にユーザと管理者を作成するときには、MA が設定した電子メールと電話のタイプに値を入力するように促されます。組織を作成する際には、別の電子メールと電話のタイプを設定して、グローバル設定を無効にすることもできます。

注: 組織レベルで設定された電子メールと電話のタイプの属性によってグローバル レベルで設定された値は無効になり、組織レベルの属性が優先して使用されます。

電子メールと電話のタイプの設定例

MA が、すべての組織で使用する必要があるとして以下の電子メールと電話のタイプを設定したと仮定します。

- （必須）電子メール タイプ： Work Email
- （オプション）電子メール タイプ： Personal Email
- （必須）電話タイプ： Work Phone
- （オプション）電話タイプ： Home Phone

GA がグローバル設定を使用する組織 *Org1* の管理者を作成するとき、GA は Work Email および Work Phone に対して値を指定する*必要があります*。必要に応じて、GA はその他の電子メールと電話のタイプを追加できますが、電子メールと電話のタイプに対するグローバル設定を削除することはできません。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. 左側のナビゲーション ウィンドウで、［*UDS 設定*］セクションにある［*電子メール/電話番号タイプの設定*］リンクをクリックして、対応するページを表示します。
4. ［*電子メール タイプの設定*］セクションで、以下のように指定します。

- 複数の電子メール タイプが設定されている場合、電子メール タイプの*優先度*。 上向きまたは下向きのアイコンを使用して優先度を変更します。 優先度は、複数の電子メール タイプが設定されているときに、電子メール タイプが画面に表示される順序を定義します。
- 設定する電子メールの*タイプ*。たとえば、業務用、個人用など。
- 電子メール タイプの*表示名*。
- 電子メール タイプが*必須*かどうか。

5. ［*電話タイプの設定*］セクションで、以下のように指定します。
   - 複数の電話タイプが設定されている場合、電話タイプの*優先度*。上向きまたは下向きのアイコンを使用して優先度を変更します。 優先度は、複数の電話タイプが設定されているときに、電話タイプが画面に表示される順序を定義します。
   - 設定する電話番号の*タイプ*。たとえば、自宅用、業務用など。
   - *電話タイプ*の表示名。
   - 電話タイプが*必須*かどうか。

   注: ［**+**］アイコンをクリックすると、電子メールと電話のタイプを追加できます。
6. *［保存］*をクリックします。
7. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ（P. 36）」を参照してください。

基本認証設定の指定

基本ユーザ パスワード、*LDAP ユーザ パスワード*、または *WebFort パスワード*メカニズムのいずれかを使用して、管理者は認証されます。 組織の作成時に選択したオプションがメカニズムとして使用されます。

- ［*基本ユーザ パスワード*］オプションを選択した場合は、デフォルトの認証設定を使用するか、または「基本認証パスワード ポリシーの設定 (P. 50)」の説明に従って新しい設定を行うかを選択できます。
- ［*LDAP ユーザ パスワード*］オプションを選択した場合は、LDAP に格納されたパスワードを管理者がログインに使用します。 認証ポリシーは LDAP システムで定義します。
- ［*WebFort パスワード*］オプションを選択した場合、まず CA Strong Authentication サーバに接続情報を指定します。

基本認証パスワード ポリシーの設定

基本認証方式では、ユーザ ID を使用して管理コンソールにログインします。

［基本認証ポリシー］ページを使用して、パスワード長、使用可能な特殊文字の数、ユーザのシステムへのアクセスをロックするまでに許可されるログインの失敗回数などの制限を実施することでパスワード ポリシーを強化することができます。

次の手順に従ってください:

1. *［サービスおよびサーバの設定］*タブをアクティブにします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. 左側のペインで、［*認証*］セクションにある［*基本認証ポリシー*］リンクをクリックして、対応するページを表示します。
4. ［*パスワード ポリシー設定*］セクションで、以下の表に示すパラメータを指定します。 このページのパラメータはすべて必須です。

   パスワードの最小文字数

   パスワードに含める必要のある最小文字数。値は 6 ～ 32 文字で設定できます。

   デフォルト値： 6

   パスワード最大長

   パスワードに含めることのできる最大文字数。値は 6 ～ 32 文字で設定できます。

   デフォルト値： 25

   失敗の最大試行回数

   管理者がパスワードを不正確に指定しても良い連続回数。この回数を超えると認証情報がロックされます。 3 ～ 10 の値を設定できます。

   デフォルト値： 5

   数字の最小文字数

   パスワードに含める必要のある数字（0 ～ 9）の最小数。 値は 0 ～ 32 文字で設定できます。

   デフォルト値： 1

パスワード履歴数

再使用できない以前のパスワードの数。

デフォルト値： 3

有効期間

パスワードが有効な最大日数。 パスワードが期限切れにならないようにする場合は、［無期限にする］オプションを選択します。

デフォルト値： 180 日

マルチバイト文字を許可

パラメータをマルチバイト文字形式で格納する場合は、このオプションを有効にします。 **注**: このオプションを選択した場合は、以下の 3 つのフィールドが無効になります。

デフォルト値： 無効

アルファベット文字の最小文字数

パスワードに含める必要のあるアルファベット文字（a-z および A-Z）の最小数。 値は 0 ～ 32 文字で設定できます。

デフォルト値： 4

特殊文字の最小文字数

パスワードに含める必要のある使用可能な特殊文字の最小文字数。 値は 0 ～ 32 文字で設定できます。

デフォルト値： 1

使用できる特殊文字（オプション）

パスワードに含めることができる特殊文字のリスト。

デフォルト値： !@#$%^&*()_+

5. ［保存］をクリックして、このページに対して行った変更を保存します。

マスタ管理者認証ポリシーの設定

マスタ管理者は*基本認証*方式を使用します。

MA のパスワード ポリシーを強化することができます。たとえば、パスワード長、使用可能な特殊文字の数、システムへの MA アクセスがロックされるまでに許可されるログイン失敗回数などの制限を実施します。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. 左側のペインで、［*認証*］セクションにある［*マスタ管理者認証ポリシー*］リンクをクリックして、対応するページを表示します。
4. ［*パスワード ポリシー設定*］セクションで、以下の表に示すパラメータを指定します。 このページのパラメータはすべて必須です。

パスワードの最小文字数

パスワードに含める必要のある最小文字数。値は 6 ～ 32 文字で設定できます。

デフォルト値： 6

パスワード最大長

パスワードに含めることのできる最大文字数。値は 6 ～ 32 文字で設定できます。

デフォルト値： 25

失敗の最大試行回数

管理者がパスワードを不正確に指定しても良い連続回数。この回数を超えると認証情報がロックされます。 3 ～ 10 の値を設定できます。

デフォルト値： 5

数字の最小文字数

パスワードに含める必要のある数字（0 ～ 9）の最小数。 値は 0 ～ 32 文字で設定できます。

デフォルト値： 1

パスワード履歴数

再使用できない以前のパスワードの最大数。

デフォルト値： 3

有効期間

パスワードが有効な最大日数。

デフォルト値： 180 日

マルチバイト文字を許可

パラメータをマルチバイト文字形式で格納する場合は、このオプションを有効にします。

注: このオプションを選択した場合、以下の 3 つのフィールドは無効になります。

デフォルト値： 無効

アルファベット文字の最小文字数

パスワードに含める必要のあるアルファベット文字（a-z および A-Z）の最小数。 値は 0 ～ 32 文字で設定できます。

デフォルト値： 4

特殊文字の最小文字数

パスワードに含める必要のある使用可能な特殊文字の最小文字数。値は 0 ～ 32 文字で設定できます。

デフォルト値： 1

使用できる特殊文字（オプション）

パスワードに含めることができる特殊文字のリスト。

デフォルト値： !@#$%^&*()_+

5. ［保存］をクリックします。

Web サービス認証および許可の有効化

CA Strong Authentication は、認証情報の発行、ユーザ認証、および管理操作をプログラムによって実行する Web サービスを提供します。 認証および許可を有効にすることで、これらの Web サービスの呼び出しを安全に保護できます。管理コンソールを使用して、認証と許可を有効にする Web サービスを選択できます。

注: 詳細については、「*CA Strong Authentication Web サービス開発者ガイド*」の「Web サービス セキュリティの管理」を参照してください。

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. タブのサブメニューで［*管理コンソール*］オプションをクリックします。
3. サイド バー メニューの［*Web サービス*］セクションで、［*認証と許可*］リンクをクリックして、対応するページを表示します。
4. ［Web サービス］セクションで、Web サービスを［無効］リストから選択して［有効］リストに移動させます。

   ［>］ボタンをクリックして、選択した Web サービスを目的のリストに移動します。 ［>>］ボタンをクリックして、すべての Web サービスを目的のリストに移動することもできます。

   注: 一度に複数の Web サービスを選択するには、Ctrl キーを押したまま選択します。
5. ［保存］をクリックします。
6. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。システム キャッシュをリフレッシュする方法については、「キャッシュのリフレッシュ（P. 36）」を参照してください。

次の手順: 迅速な管理

ここまでは、管理コンソールの概念について説明してきました。このセクションでは、展開を管理するための準備手順について簡単に説明します。

デフォルトの展開

通常、CA Strong Authentication の最も単純な実装では、小規模なユーザ基盤に強力な認証を内部的に提供します。 この実装では、単一のシステム上にすべての CA Strong Authentication コンポーネントおよび Web アプリケーションが構成されます。 データベースは、CA Strong Authentication がインストールされているのと同じシステム上、または異なるシステム上のどちらにあってもかまいません。

このタイプの展開については、「*CA Strong Authentication インストール ガイド*」の「*展開の計画*」を参照してください。

以下の表に、この展開タイプの典型的な特徴を示します。

特徴	詳細
展開タイプ	■ 開発、概念実証、初期テスト、または初期パイロット ■ 中小規模企業（SMB） ■ 企業内の地方展開
地理的な拡張	通常、1 つの場所に制限
展開の必要条件	実装と管理の容易さ

小規模な展開の場合、ほとんどの設定にデフォルトを使用して、すぐに実行できます。 単一組織のシステムであるため、デフォルトの組織を使用できます。デフォルトの組織は、新しい組織をセットアップせずにシステムを初期化する場合に自動的に作成されます。 結果として、OA も必要としない場合があります。 必要なのは、必須の GA および UA を作成することのみです。

ユーザに対する強力な認証をセットアップし、管理を開始する手順の簡単な概要を以下に示します。

1. CA Strong Authentication が正しくインストールおよび設定されており、管理コンソールとユーザ データ サービスの WAR ファイルが展開されていることを確認します。

   注: CA Strong Authentication のインストール、WAR ファイルの展開、およびその他のインストール後のタスクの実行の詳細については、「*CA Strong Authentication インストール ガイド*」の「単一システムへの CA Strong Authentication の展開」を参照してください。

2. MA として管理コンソールにログインし、ブートストラップ ウィザードの手順に従ってシステムを初期化します。

   注: 詳細については、「*CA Strong Authentication インストール ガイド*」の「*システムのブートストラップ*」を参照してください。

3. 必須の GA および UA を作成します。

   詳細については、「管理者の作成 (P. 221)」を参照してください。

4. 適切な認証情報プロファイルおよび認証ポリシー (P. 99)を作成し、これらの設定を割り当てます。

   詳細については、「グローバル CA Strong Authentication 設定の管理 (P. 99)」を参照してください。

5. CA Strong Authentication にユーザを登録します。

   詳細については、「ユーザの作成 (P. 260)」を参照してください。

システム（「CA Strong Authentication サーバ インスタンスの管理 (P. 67)」）、管理者（「管理者の管理 (P. 221)」）、およびユーザ（「ユーザと認証情報の管理 (P. 259)」）を管理できます。

複雑な展開

複雑で高可用性の環境において CA Strong Authentication を実装する大企業に対しては、この実装を使用します。 この展開は、大きなユーザ ベースおよびシステムを管理する管理者に対して強い認証を提供します。 この展開タイプでは、CA Strong Authentication コンポーネントは複数のサーバ上にインストールされます。 この展開により、高いセキュリティ、パフォーマンス、および可用性が実現されます。また、複数のアプリケーションが強力な認証機能を使用できるようにすることも目的の 1 つです。

このタイプの展開については、「CA Strong Authentication インストール ガイド」の「*展開の計画*」を参照してください。

以下の表に、この展開タイプの典型的な特徴を示します。

特徴	詳細
展開タイプ	■ 中規模から大規模なビジネスへの複雑な展開 ■ 企業展開 ■ ステージング展開
地理的な拡張	グローバルな展開
展開の必要条件	■ 実装と管理の容易さ ■ グローバルな可用性 ■ 高可用性

ユーザに対して強い認証をセットアップし、管理を開始する手順の簡単な概要を、以下に説明します。

1. CA Strong Authentication が正しくインストールおよび設定されており、管理コンソールとユーザ データ サービスの WAR ファイルが展開されていることを確認します。

   注: CA Strong Authentication のインストール、WAR ファイルの展開、およびその他のインストール後のタスクの実行の詳細については、「*CA Strong Authentication インストール ガイド*」を参照してください。

2. MA として管理コンソールにログインし（「管理コンソールへのアクセス (P. 28)」を参照）、ブートストラップ ウィザードの手順に従ってシステムを初期化します。

   詳細については、「*CA Strong Authentication インストール ガイド*」の「*システムのブートストラップ*」を参照してください。

3. 管理コンソールを設定します。これには、UDS 設定、組織のグローバル設定、管理コンソールのキャッシュ設定、および管理コンソールにログインするための基本的なユーザ名-パスワード認証が含まれます。

   詳細については、「管理コンソールの設定 (P. 30)」を参照してください。

4. 別のシステムで CA Strong Authentication サーバ インスタンスをセットアップします。

   詳細については、「サーバ インスタンスのセットアップ (P. 72)」を参照してください。

5. 管理コンソール、SDK、および Web サービスと CA Strong Authentication サーバとの間の通信で使用されるプロトコルを設定します。

   詳細については、「通信プロトコルの設定 (P. 83)」を参照してください。

6. 組織を計画し、作成します。 組織アーキテクチャはフラットで、作成する組織は、企業内の事業単位にマッピングできます。

   詳細については、「組織の作成とアクティブ化 (P. 186)」を参照してください。

7. 必要に応じて、管理者（「管理者の作成 (P. 221)」を参照）とカスタム ロール（「カスタム ロールの操作 (P. 61)」を参照）を計画し、作成します。

8. 適切な認証情報プロファイル (P. 105)および認証ポリシーを作成し、これらの設定を割り当てます。

詳細については、「グローバルな CA Strong Authentication 設定の管理 (P. 99)」を参照してください。

9. CA Strong Authentication にユーザを登録します。

   詳細については、「ユーザの作成 (P. 260)」を参照してください。

10. 必要に応じて、SAML トークン設定、RADIUS クライアント、および ASSP 設定を設定します。

    詳細については、「組織情報の更新 (P. 202)」を参照してください。

11. 必要に応じて、CA Strong Authentication サーバとそのクライアントとの間の SSL ベースの通信を設定します。

    詳細については、「信頼ストアの作成 (P. 82)」を参照してください。

12. 必要に応じて、その他の設定（トークンの有効性およびチャレンジ有効性の設定など）を設定します。

    詳細については、「その他の設定 (P. 94)」を参照してください。

13. CA Strong Authentication の機能を拡張するためにプラグインを使用することを計画している場合は、これらを登録し、設定します。

    注: プラグインを登録する方法の詳細については「プラグインの登録と更新 (P. 92)」、プラグインを設定する方法については「プラグインの設定 (P. 179)」を参照してください。

システム（「CA Strong Authentication サーバ インスタンスの (221P.)管理」）、管 (67P.)理者（「管理者の管理 (P. 259)」）、およびユーザ（「ユーザと認証情報の管理」）を管理できます。

第 3 章: カスタム ロールの操作

CA Strong Authentication には、事前定義された権限に関連付けられたビルトイン ロールが付属しています。 このトピックの詳細については、「サポートされるロール」を参照してください。CA Strong Authentication では、これらの事前定義されたロールを以下のような場合に操作できる機能も提供しています。

- デフォルトのロールが組織の要件を満たしていない場合。
- CA Strong Authentication によって提供されるものとは異なるロール情報を管理する必要がある場合。

重要: この章で説明されているロール管理タスクは、マスタ管理者のみが実行できます。

この章では、重要な利点である、CA Strong Authentication でカスタム ロールを作成して適用する機能について説明します。 この章では以下について説明します。

- カスタム ロールについて
- カスタム ロールの作成
- カスタム ロール情報の更新
- カスタム ロールの削除
- 管理権限の要約

カスタム ロールについて

MA は、以下のいずれかの事前定義された親ロールから権限のサブセットを継承する*新しい管理ロール*を作成できます（「管理コンソールの概要」を参照）。

- GA （グローバル管理者）
- OA （組織の管理者）
- UA （ユーザ管理者）（P. 25）

これらのロールは*カスタム ロール*と呼ばれ、親ロールに関連付けられているデフォルト権限のいくつかを*無効にする*ことによって作成されます。たとえば、GA の組織を作成する権限を無効にする必要がある場合、この権限を無効にし、同じものを GA に割り当てることにより、カスタム ロールを作成できます。

カスタム ロールを作成すると、管理者を作成または更新する際にロール オプションとして利用可能になります。 カスタム ロールは、作成するだけではなく更新および削除も行えます。 カスタム ロールの管理の詳細については、この章の以下のセクションを参照してください。

カスタム ロールについて

以下の項目を確認します。

- MA *のみ*がカスタム ロールを作成できます。
- カスタム ロールは、単一のロールの権限のサブセットのみを継承できます。 カスタム ロールは、2 つの異なるロールから権限を継承することは *できません*。

  たとえば、ユーザの管理（UA 権限）および組織の作成（OA 権限）を行う権限を持つカスタム UA ロールは作成できません。
- 親ロールに割り当てられていない権限は、カスタム ロールにも割り当てることはできません。

  たとえば、事前定義された OA ロールに組織の作成権限がない場合は、この OA ロールに基づいたカスタム ロールもその権限を持つことができません。
- カスタム ロールを作成する際、1 つ以上の権限に相当するタスクは、それらの権限の少なくとも 1 つがまだ利用可能な場合に限り、継続して表示されます。

  たとえば、アクティブ化、非アクティブ化、および削除の権限が無効な場合でも、更新の権限がまだ利用できる場合、「組織の検索」リンクが表示されます。
- 新たに作成したカスタム ロールは、サーバのキャッシュをリフレッシュした*後にのみ*、管理コンソールのほかのインスタンスで利用できます（「サーバ インスタンスのリフレッシュ」を参照）。

カスタム ロールの作成

この手順では、カスタム ロールを作成する方法について説明します。

次の手順に従ってください:

1. ［*ユーザと管理者*］タブをクリックします。
2. ［*ロールの管理*］リンクをクリックすると、［カスタム ロールの作成］ページが表示されます。
3. ［*ロール詳細*］セクションで、以下の情報を指定します。

   ロール名

   新規ロールを識別する一意の名前を定義します。 この名前は、この新規ロールを認証および許可するために CA Strong Authentication によって内部的に使用されます。

   ロール表示名

   管理コンソールのほかのすべてのページおよびレポートに表示されるロールの説明的な名前を定義します。

   Role Description

   ロールの説明を指定します。

   ロール元

   このカスタム ロールの派生元の既存のロールを定義します。
4. ［*権限の設定*］セクションで以下の情報を指定します。
   a. ［*利用可能な権限*］リストで、カスタム ロールに対して*無効*にするすべての権限を選択します。

      このリストには、［**ロール元**］フィールドで選択した管理ロールで利用可能なすべての権限が表示されます。

   b. ［**>**］ボタンをクリックすると、選択した権限が［*利用不可の権限*］リストに移動されます。
5. ［*作成*］をクリックすると、カスタム ロールが作成されます。
6. キャッシュをリフレッシュします。 詳細については、「キャッシュのリフレッシュ」を参照してください。

カスタム ロール情報の更新

既存のカスタム ロール定義を更新するには、この手順に従います。

次の手順に従ってください:

1. ［*ユーザと管理者*］タブをクリックします。
2. サブメニューから、［*ロールの管理*］リンクをクリックします。
3. ［タスク］メニューから、［*カスタム ロールの更新*］リンクをクリックします。

   ［カスタム ロールの更新］ページが表示されます。
4. 更新する*ロール名*を選択します。
5. ［*ロール詳細*］セクションの 1 つまたはすべてのフィールドで必要な変更を行います。
6. ［*権限の設定*］セクションで、以下のいずれかの手順を実行します。
   a. ［*利用可能な権限*］リストで、このロールに対して*無効*にするすべての権限を選択します。

      このリストには、［*ロール元*］フィールドで選択した管理ロールで利用可能なすべての権限が表示されます。

      ［*利用不可の権限*］リストで、このロールに対して*有効*にする権限を選択します。

      このリストには、［*ロール元*］フィールドで選択した管理ロールで利用できないすべての権限が表示されます。

      注: *Ctrl* キーを押したままにすると、一度に複数の権限を選択できます。
   b. ［**>**］ボタンをクリックすると、選択した権限が［*利用不可の権限*］リストに移動されます。
7. ［*更新*］をクリックします。
8. キャッシュをリフレッシュします。詳細については、「キャッシュのリフレッシュ」を参照してください。

カスタム ロールの削除

既存のカスタム ロールを削除するには、この手順を使用します。

重要: 管理者に現在割り当てられるカスタム ロールを削除することはできません。 そのようなロールを削除する必要がある場合は、［管理者の更新］ページを使用して、まずこのロールを割り当てられているすべての管理者のロールを変更します。その後で、このセクションの手順に従います。

次の手順に従ってください：

1. ［*ユーザと管理者*］タブをアクティブにします。
2. サブメニューから、［*ロールの管理*］リンクをクリックします。
3. ［タスク］メニューから、［*カスタム ロールの削除*］リンクをクリックします。

   ［カスタム ロールの削除］ページが表示されます。
4. ［*ロール詳細*］セクションで、削除する必要のあるカスタム ロールを［*ロール名*］リストから選択します。
5. ［*削除*］をクリックします。

   注: カスタム ロールは、管理者のいずれかに割り当てられている場合は削除 できません。
6. キャッシュをリフレッシュします。 詳細については、「キャッシュのリフレッシュ」を参照してください。

第 4 章: CA Strong Authentication サーバ インスタンスの管理

CA Strong Authentication サーバをインストールして設定した各システムは、*インスタンス*と呼ばれます。

重要: この章で説明されているすべての設定およびタスクは、マスタ管理者のみが実行できます

マスタ管理者は、各 CA Strong Authentication インスタンスをローカルまたはリモートで管理できます。 サーバ インスタンスを管理する前に、接続パラメータを設定してインスタンスに接続する必要があります （手順の詳細については、「CA Strong Authentication 接続の設定 (P. 68)」を参照してください。）

1 つのインスタンスの接続パラメータを設定した後、ほかの CA Strong Authentication サーバ インスタンスを管理できます。

CA Strong Authentication サーバ インスタンスを管理するために、MA としてログインしていることを確認します。

注: 「システム管理者ユーティリティ (P. 275)」で説明されているように、これらのタスクの一部はシステム ツールを使用して実行できます。

CA Strong Authentication 接続の設定

CA Strong Authentication サーバの複数のインスタンスをインストールできます。ただし、管理コンソールを使用して接続を詳細に設定できるのは、1 つのインスタンスのみです。この設定されたインスタンスは、マルチインスタンス管理や、管理コンソールを使用して実行する設定の作成や認証情報の発行などの操作を 1 つのインスタンスから他のインスタンスにフェイルオーバするために、ほかのインスタンスのデータを取得します。

注: 単一システムの展開では、ほとんどの場合、インスタンスを設定する必要はありません。デフォルト値を使用して、すぐに動作するようになります。

双方向 SSL トランスポート モードを設定して、［Webfort 接続］で WebSphere アプリケーション サーバ上の CA Strong Authentication サーバ インスタンスに接続すると、「SDK failed to initialize. Configuration is invalid」というエラー メッセージが表示されます。 IBM の Web サイトから Unrestricted JCE ポリシー ファイルの local_policy.jar および US_export_policy.jar をダウンロードし、以下の場所へコピーする必要があります。

- <WebSphere_JAVA_HOME>¥lib¥security（security ディレクトリが存在しない場合は作成してください。）
- <WebSphere_JAVA_HOME>¥jre¥lib¥security

次の手順に従ってください:

1. ［*サービスおよびサーバの設定*］タブをクリックします。
2. サブメニューで *CA Strong Authentication* オプションが選択されていることを確認します。
3. 対応するページがまだ表示されていない場合は、タスク ペインの［*CA Strong Authentication 接続*］をクリックすると表示されます。
4. 以下の表の情報を使用して、［CA Strong Authentication 接続］ページのフィールドを編集します。

   AuthMinder サーバの IP アドレス

   必要な CA Strong Authentication サーバ インスタンスをインストールしたシステムの IP アドレスを定義します。

   注: CA Strong Authentication コンポーネントをインストールしたシステムが、ホスト名を使用してネットワーク上で相互にアクセスできることを確認します。

   デフォルト： localhost

   ポート

   Server Management Web Services プロトコル サービスが公開されるポートを定義します。

   注: このフィールドは Server Management Web Services プロトコルにのみ有効です。このプロトコルはほかの CA Strong Authentication インスタンスの情報を取得する必要があるためです。

   デフォルト： 9743

Transport

対応するコンポーネント（サーバ管理 Web サービス、管理 Web サービス、トランザクション Web サービス、および認証ネイティブ）のトランスポート モードを指定して、指定した CA Strong Authentication サーバ インスタンスに接続します。

サポートされている値は以下のとおりです。

SSL（1 方向）：一方向の SSL（Secure Sockets Layer）を転送時にデータを暗号化および復号化するために使用します。

SSL （双方向）： 双方向の SSL を転送時にデータを暗号化および復号化するために使用します。

TCP： TCP （Transmission Control Protocol）モードを転送時にデータを暗号化および復号化するために使用します。

デフォルト： TCP

サーバ CA 証明書（PEM）

対応するフィールドの参照ボタンをクリックすると、サーバ証明書チェーンがアップロードされます。

注: このフィールドは、［トランスポート］フィールドで［SSL（1 方向）］または［SSL （双方向）］が選択されている場合に使用可能です。

PKCS#12 内のクライアント証明書 - キーのペア

対応するフィールドの参照ボタンを使用して、クライアント証明書の公開キーと秘密キーのペアをアップロードします。

注: このフィールドは、［トランスポート］フィールドで［SSL（双方向）］が選択されている場合に使用可能です。

クライアント PKCS#12 パスワード

P12 ファイルに対応するパスワード。

注: このフィールドは、［トランスポート］フィールドで［SSL（双方向）］が選択されている場合に使用可能です。

［詳細設定］セクション

Maximum Active Connections

クライアントと CA Strong Authentication サーバ間で維持できるアクティブな接続の最大数。

デフォルト： 32

最大アイドル接続数

CA Strong Authentication サーバで維持できるアイドル状態の接続の最大数。

デフォルト： 8

最大待機時間（ミリ秒）

接続がタイムアウトする前に、使用可能になるまでクライアントが待機する必要がある（使用可能な接続がない場合）最大時間（ミリ秒）。

デフォルト： -1

最小削除待機時間（ミリ秒）

接続がアイドル接続エビクター（ある場合）によって削除されるまでの、プール内で接続がアイドルになる可能性のある最小時間（ミリ秒）。

デフォルト： 300000

削除実行間隔（ミリ秒）

プールをチェックしてアイドル接続を削除するまで待機する時間（ミリ秒）。

デフォルト： 600000

Connection Timeout

CA Strong Authentication サーバが到達できないと考えられるまでの最大時間（ミリ秒）。

デフォルト： 10000

読み取りタイムアウト

CA Strong Authentication サーバからのレスポンスに許容される最大時間（ミリ秒）。

デフォルト： 30000

5. ［**保存**］をクリックすると、設定した設定が保存されます。

注: 新しい CA Strong Authentication サーバ インスタンスを追加する場合、インスタンスに固有の設定を行う前に、このページの［*保存*］をクリックする必要があります。 これにより、管理コンソールに新しく追加されたすべてのインスタンスの詳細が登録され、新しく追加されたインスタンスに対してインスタンス管理機能が円滑に動作するようになります。

サーバ インスタンスのセットアップ

［CA Strong Authentication インスタンス］ページには、同じ CA Strong Authentication データベースを管理コンソールとして共有する、設定されたすべての CA Strong Authentication サーバ インスタンスがリスト表示されます。 ［AuthMinder 接続］ページを使用して以前に設定したサーバ インスタンスにより、他のすべてのインスタンスに関する必要な情報がポーリングにより収集され、管理コンソールに渡されます。その後、これらの情報が 管理コンソールによりこのページに表示されます。

CA Strong Authentication サーバのインスタンスを展開した後に、インスタンスの詳細の更新が必要になることがあります。［CA Strong Authentication インスタンス］ページでは、サーバ キャッシュのリフレッシュ、および指定したインスタンスのシャットダウンを行うことができます。 ただし、インスタンス固有の属性、データベース接続パラメータ、ログ ファイルの詳細情報、または統計データ ログ パラメータを変更するには、インスタンス名をクリックし、インスタンスのページで必要な変更を行います。

典型的なインスタンス管理操作には、次があります。

- サーバ インスタンスのリフレッシュ (P. 72)
- インスタンス名の変更 (P. 74)
- CA Strong Authentication サーバ ログ記録設定の管理 (P. 75)
- データベース パラメータの設定 (P. 77)
- インスタンス タイム スタンプの詳細の読み取り (P. 79)
- サーバ インスタンスのシャットダウン (P. 79)
- サーバ インスタンスの再起動 (P. 81)

注: このセクションで説明されている操作のほとんどは、arwfutil コマンド ライン ツールによっても実行できます。詳細については、「arwfutil : ユーティリティ ツール (P. 286)」を参照してください。

サーバ インスタンスのリフレッシュ

管理コンソールまたは arwfutil ツール (P. 286)を使用して、CA Strong Authentication サーバ インスタンスをリフレッシュできます。

管理コンソールを使用したリフレッシュ

［インスタンス管理］ページでインスタンスを選択することにより、特定の CA Strong Authentication サーバ インスタンスをリフレッシュできます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. ［インスタンス設定］セクションの［インスタンス管理］リンクをクリックすると、［AuthMinder インスタンス］ページが表示されます。
3. ［選択］列で、ステータスを変更するサーバ インスタンスを選択します。
4. ［リフレッシュ］をクリックすると、選択したインスタンスがリフレッシュされます。

arwfutil ツールを使用したリフレッシュ

次の手順に従ってください:

1. arwfutil ツールを使用できるシステムにログインします。
2. 以下のディレクトリに移動します。
   - **Windows の場合**
     `<install_location>¥Arcot Systems¥bin¥`
   - **UNIX ベースのプラットフォームの場合**
     `<install_location>/arcot/sbin/`
3. 以下のようにツールを実行します。
   - **Windows の場合**
     `arwfutil cr`
   - **UNIX ベースのプラットフォームの場合**
     `./arwfutil cr`

インスタンス名の変更

インスタンスが実行されているホストおよび最初のスタートアップ時のタイム スタンプに基づいて、CA Strong Authentication サーバは、各インスタンスの一意の名前を生成します。 この名前はレポートで使用され、監査ログに記録されます。 インスタンスの容易に識別できるようにするには、各インスタンスに適切な名前を指定します。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［インスタンス設定］セクションの［インスタンス管理］リンクをクリックすると、インスタンス ページが表示されます。
4. ［インスタンス名］列で設定するインスタンスのリンクをクリックします。

   ［インスタンス名 : <selected_instance>］ページが表示されます。
5. ［インスタンス属性］セクションで、［インスタンス名の変更］チェック ボックスをオンにします。
6. ［新規インスタンス名］フィールドに新しい名前を入力します。
7. ［保存］をクリックすると、変更内容が保存されます。
8. 変更を行った CA Strong Authentication サーバ インスタンスをリフレッシュします。 手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

CA Strong Authentication サーバ ログ記録設定の管理

CA Strong Authentication では広範なログ記録機能が用意されており、以下のログ ファイルがあります。

- CA Strong Authentication ログ ファイル（arcotwebfort.log）
- CA Strong Authentication スタートアップ ログ ファイル（arcotwebfortstartup.log）
- 管理コンソール ログ ファイル（arcotadmin.log）
- UDS ログ ファイル（arcotuds.log）

  注: これらのログ ファイルの場所、これらのファイルに記録される重大度レベル、およびこれらのログ ファイルの形式に関する詳細については、「(P. 311)CA Strong Authentication のログ」を参照してください。

インスタンス固有のページを使用することによって、インスタンス用の CA Strong Authentication ログ ファイルのログ記録設定を個別に管理できます。

次の手順に従ってください:

注: 管理コンソールを使用して CA Strong Authentication 統計ログ ファイルの設定を管理する方法の詳細については、「インスタンス タイム スタンプの詳細の読み取り (P. 79)」を参照してください。

1. メイン メニューの［*サービスおよびサーバの設定*］タブをクリックします。
2. サブメニューの［*CA Strong Authentication*］タブがアクティブであることを確認します。
3. ［*インスタンス設定*］セクションの［*インスタンス管理*］リンクをクリックすると、インスタンス ページが表示されます。
4. ［**インスタンス名**］列で設定するインスタンスのリンクをクリックします。

   ［インスタンス名 : <*selected_instance*>］ページが表示されます。
5. 必要に応じて、**ログ設定**セクションのフィールドを編集します。 以下の表に、このセクションのフィールドの説明を示します。

   トランザクション ログ ディレクトリ

   ログ ファイルが作成されるディレクトリを指定します。

絶対パスまたは ARCOT_HOME への相対パスのいずれかを入力できます。

ロールオーバー開始サイズ（バイト単位）

ログ ファイルの最大サイズを入力します。

ログ ファイルがこのサイズに到達すると、ログの内容はバックアップ ファイルに移動されます。

トランザクション ログ バックアップ ディレクトリ

バックアップ ファイルが格納されるディレクトリを指定します。

絶対パスまたは ARCOT_HOME への相対パスのいずれかを入力できます。

［Log Level］

ログ記録される情報の詳細レベルを指定します。 以下の値を指定できます。

- FATAL
- 注意
- INFO
- DETAIL

GMT でのタイム スタンプのログ記録

CA Strong Authentication サーバ インスタンスですべてのメッセージを GMT タイム ゾーン形式でログ記録する場合は、このチェックボックスをオンにします。

トレース ログの有効化

CA Strong Authentication サーバ インスタンスですべてのトランザクションのファンクション フローのログを生成する場合は、このチェック ボックスをオンにします。

これはフロー問題をデバッグする場合に役立ちます。

6. *［保存］*をクリックします。
7. 変更を行った CA Strong Authentication サーバ インスタンスをリフレッシュします。 手順の詳細については、「サーバ インスタンスのリフレッシュ（P. 72）」を参照してください。

データベース パラメータの設定

CA Strong Authentication は、接続プールを使用して、サーバがデータベースにアクセスするたびに新規データベース接続を確立するオーバーヘッドを回避します。 インスタンス固有のページを使用することによって、個別のインスタンスにこれらの接続プーリング パラメータを設定できます。 ［インスタンス統計］ページに表示されるデータは、このページで設定されるパラメータによって異なります。

次の手順に従ってください:

1. メイン メニューの［*サービスおよびサーバの設定*］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［インスタンス設定］セクションの［インスタンス管理］リンクをクリックすると、インスタンス ページが表示されます。
4. ［インスタンス名］列で設定するインスタンスのリンクをクリックします。

   ［インスタンス名 : <selected_instance>］ページが表示されます。

5. 必要に応じて［データベース構成］セクション内のフィールドを編集します。以下の表に、このセクションのフィールドの説明を示します。

最小接続数

サーバの起動時に、CA Strong Authentication サーバとデータベースとの間のサポートされる接続の最小数を定義します。

最大接続数

CA Strong Authentication サーバとデータベースとの間のサポートされる接続の最大数を定義します。

注: この値は、MaxConnections パラメータより優先されるため、データベースがサポートする最大接続数に応じてこの値を設定する必要があります。 詳細については、データベース ベンダーのマニュアルを参照してください。

接続数の増分

既存の接続に対して一度に追加する接続の数を定義します。

重要: 接続の総数は、接続の最大数を超えることはできません。

モニタ スレッド スリープ時間（秒）

モニタリング スレッドがすべてのデータベースに対して継続してハートビート チェックを行う間隔を指定します。

障害がある場合のモニタ スレッド スリープ時間（秒）

データベース接続に障害が発生した場合に、データベース モニタ スレッドが接続プールの健全性をチェックする間隔を指定します。

クエリ詳細のログ

すべてのデータベース クエリの詳細をログ記録する場合は、このチェック ボックスをオンにします。

データベース接続のモニタ

データベース モニタ スレッドで、プールを事前にチェックするには、このチェック ボックスをオンにします。

プライマリに自動的に戻す

フェイルオーバ状態後にプライマリ データベースが再度利用可能になった場合、CA Strong Authentication サーバがバックアップ データベースからプライマリ データベースに切り替わるようにするには、このチェック ボックスをオンにします。

6. ［**保存**］をクリックします
7. 変更を行った CA Strong Authentication サーバ インスタンスをリフレッシュします。この実行の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

インスタンス タイム スタンプの詳細の読み取り

インスタンス固有のページには、［**サーバ タイム スタンプ詳細**］セクションに各サーバ インスタンスのタイム スタンプの詳細が表示されます。 以下の表に、これらの詳細を示します。

最終スタートアップ時刻

サーバ インスタンスが前回再起動されたときのタイム スタンプです。

前回のサーバ シャットダウン時刻

サーバ インスタンスが前回シャットダウンされたときのタイム スタンプです。

前回のリフレッシュ時刻

サーバ インスタンスが前回リフレッシュされたときのタイム スタンプです。

サーバ稼働時間

サーバ インスタンスが実行されている期間です。

サーバ インスタンスのシャットダウン

管理コンソールまたは arwfutil ツールを使用して、CA Strong Authentication サーバ インスタンスをシャットダウンできます。

管理コンソールを使用したシャットダウン

［インスタンス管理］ページでインスタンスを選択することにより、特定の CA Strong Authentication サーバ インスタンスをシャットダウンできます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. ［インスタンス設定］セクションの［インスタンス管理］リンクをクリックすると、インスタンス ページが表示されます。
3. ［選択］列で、ステータスを変更するサーバ インスタンスを選択します。
4. ［シャットダウン］をクリックすると、選択したインスタンスがシャットダウンされます。

arwfutil ツールを使用したシャットダウン

次の手順に従ってください:

1. arwfutil ツールを使用できるシステムにログインします。
2. 以下のディレクトリに移動します。
   - **Windows の場合**
     `<install_location>¥Arcot Systems¥bin¥`
   - **UNIX ベースのプラットフォームの場合**
     `<install_location>/arcot/sbin/`
3. 以下のようにツールを実行します。
   - **Windows の場合**
     `arwfutil sd`
   - **UNIX ベースのプラットフォームの場合**
     `./arwfutil sd`

サーバ インスタンスの再起動

CA Strong Authentication サーバ インスタンスをシャットダウンするには、このセクションで説明されている手順に従います。

Windows の場合

次の手順に従ってください:

1. インスタンスが停止されているコンピュータにログインします。
2. デスクトップの［**スタート**］ボタンをクリックします。
3. ［**設定**］-［**コントロール パネル**］-［**管理ツール**］-［**サービス**］に移動します。
4. 表示されるサービスのリストから［**Arcot WebFort Authentication Service**］を選択します。
5. ［**開始**］をクリックすると、サービスが開始されます。

UNIX ベースのプラットフォームの場合

次の手順に従ってください:

1. インスタンスが停止されているシステムにログインします。
2. 以下のディレクトリに移動します。
   `<install_location>/arcot/bin/`
3. 以下のコマンドを実行します。
   `./webfortserver start`

トラスト ストアの作成

トラスト ストアを作成して、SSL ベースの通信の実行中に、CA Strong Authentication サーバ インスタンスに対して CA Strong Authentication コンポーネントまたはその他のクライアントを認証することができます。 *トラスト ストア*には、CA Strong Authentication サーバによって信頼される CA ルート証明書が含まれます。

各 CA Strong Authentication サーバ インスタンスは、個別のトラスト ストアを使用することにより、異なる証明書を使用できるように設定できます。［トラステッド認証機関］ページを使用することにより、信頼ストアを作成し、新しいルート証明書を信頼ストアに追加できます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［インスタンス設定］セクションの［トラステッド認証機関］リンクをクリックすると、［トラステッド認証機関］ページが表示されます。
4. ［名前］フィールドに、作成する信頼ストアの名前を入力します。
5. 対応する参照ボタンをクリックすると、信頼された CA のルート証明書が PEM 形式でアップロードされます。［さらに追加］をクリックすると、証明書をアップロードするための他のフィールドが表示されます。
6. 必要な証明書がすべてアップロードされたら、［保存］をクリックします。

通信プロトコルの設定

認証情報管理、認証、管理の目的で、CA Strong Authentication サーバ インスタンスと通信するために管理コンソール、SDK、および Web サービスが使用するプロトコルを設定できます。

以下の表では、［プロトコル設定］ページに表示されるプロトコルについて説明し、それらのデフォルト ポート番号を示します。

プロトコル	デフォルト ポート番号	Description
Administration Web Services	9745	このプロトコルは、SAML、ASSP、プロファイル、およびポリシー設定を管理するために使用されます。
ASSP	9741	Adobe 署名サービス プロトコル（ASSP）は、PDF ドキュメントのサーバ側デジタル署名用にユーザを認証するために、Adobe Reader および Adobe Acrobat で使用されます。
RADIUS	1812	CA Strong Authentication の機能を拡張して、RADIUS（Remote Authentication Dial In User Service）プロトコルをサポートするために使用される RADIUS リスナ プロトコルです。 **注**: RADIUS をサポートするように設定すると、CA Strong Authentication サーバは RADIUS サーバとして動作します。
Server Management Web Services	9743	管理コンソールおよび arwfutil ツールは、このプロトコルを使用して、サーバ管理アクティビティ用の CA Strong Authentication サーバ インスタンスと通信します。
Transaction HTTP	9746	このプロトコルは HTTP データを受信します。 CA Auth ID OTP プロビジョニングおよび CA Auth ID PKI キー バッグ管理操作に使用します。 **注**: ほかの汎用 CA Strong Authentication 操作には公開されません。
Transaction Native	9742	これは、発行と認証用のバイナリ CA Strong Authentication プロトコルです。このプロトコルは、発行および認証 Java SDK によって使用されます。

プロトコル	デフォルト ポート番号	Description
Transaction Web Services	9744	このプロトコルは、認証および発行 Web サービスによって送信される Web サービス リクエストを受信します。

次の手順に従ってください:

注:［インスタンス統計］ページ（「インスタンス統計のモニタリング (P. 88)」を参照）に表示されるデータは、このページで設定されるパラメータによって異なります。

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。

   ［インスタンス設定］セクションの［プロトコル管理］リンクをクリックすると、［プロトコル設定］ページが表示されます。
3. プロトコルを設定するサーバ インスタンスを選択します。
4. ［プロトコルのリスト］セクションで、設定するプロトコルをクリックします。

   特定のプロトコルを設定するためのページが表示されます
5. 必要に応じて、ページ上でフィールドを編集します。 以下の表に、これらのフィールドの説明を示します。

   ［Protocol Status］

   プロトコルが有効または無効のいずれであるかを示します。

   プロトコル ステータスの変更

   このオプションを選択して［アクション］リストを有効にし、新しいステータスを［アクション］ドロップダウン リストから選択します。

   注: Server Management プロトコルは無効にできません。 そのため、これらのオプションはこのプロトコルに対して表示されません。

   ポート

   プロトコル サービスが利用可能なポート番号を定義します。

   最大リクエスト サイズ（KB）

   CA Strong Authentication サーバに送信できるリクエストの最大サイズを定義します。 入力サイズがこの値を超える場合、リクエストは CA Strong Authentication サーバによって処理されません。

   注: デフォルトでは、入力リクエスト サイズに制限はありません。

   最小値

クライアントと CA Strong Authentication サーバが維持できるスレッドの最小数を定義します。

最大スレッド数

クライアントと CA Strong Authentication サーバとの間に存在できるスレッドの最大数を指定します。

注: **以下のフィールドは RADIUS プロトコルには適用できません。**

スレッドしきい値

最大スレッド数をパーセンテージで指定します。 最大スレッド数のしきい値のパーセンテージを超えたリクエストは、リクエストを処理した直後に閉じられます。

たとえば、デフォルトでは最大スレッド数は 128 で、スレッドしきい値は 90% です。これは、115 を超えて確立されたスレッドは処理された後ただちに閉じられることを示します。

クライアント アイドル タイムアウト（秒）

CA Strong Authentication サーバが接続を閉じるまでにクライアントからのリクエストを待機する間隔（秒）を指定します。

接続キープ アライブ

リクエストが処理された後もクライアントが接続を維持するようにしたい場合は、このオプションを有効にします。

接続期間が［クライアント アイドル タイムアウト（秒）］の期間と等しい場合は、接続が閉じられます。

Transport

データ転送のモードを指定します。

サポートされている値は以下のとおりです。

SSL（1 方向）：一方向の SSL（Secure Sockets Layer）を転送時にデータを暗号化および復号化するために使用します。

SSL （双方向） ： 双方向の SSL を転送時にデータを暗号化および復号化するために使用します。

注: このオプションは、トラスト ストアを設定した場合にのみ使用可能です。

TCP： TCP （Transmission Control Protocol）モードを転送時にデータを暗号化および復号化するために使用します。

HSM 内のキー

SSL 通信用の秘密キーが HSM デバイスに格納されている場合は、このチェック ボックスをオンにします。 CA Strong Authentication サーバ は、提供された証明書チェーンに基づいて秘密キーを検索します。

証明書チェーン（PEM 形式）

対応するフィールドの参照ボタンをクリックすると、サーバ証明書チェーンがアップロードされます。

注: このフィールドは、［HSM 内のキー］オプションを選択したときのみ使用可能です。

キー ペアを含む P12 ファイル

P12 ファイルに対応するパスワード。

P12 ファイル パスワード　　クライアント ストアの選択

信頼された CA のルート証明書が含まれる信頼ストアを選択します。

トラスト ストアを設定する方法の詳細については、「信頼ストアの作成 (P. 82)」を参照してください。

注: このフィールドは双方向の SSL 通信の場合にのみ使用可能です。

6. ［保存］をクリックします。

注: 各プロトコルは個別に設定してください。

7. 変更を行った CA Strong Authentication サーバ インスタンスを再起動します。手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

インスタンス統計のモニタリング

管理コンソールの［AuthMinder 統計］ページを使用すると、各サーバ インスタンスの CA Strong Authentication データベースの接続ステータスおよび詳細、UDS、および設定した CA Strong Authentication プロトコルを監視できます。 前記のセクションで説明されているさまざまなパラメータを調整して、パフォーマンスを向上させることができます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［インスタンス設定］セクションの［インスタンス統計］リンクをクリックすると、［AuthMinder 統計］ページが表示されます。
4. 詳細を監視するインスタンスを［インスタンスの選択］リストから選択します。

   以下のインスタンス詳細が表示されます。

   - データベース接続 (P. 88)
   - サーバ プロトコル (P. 89)
   - スレッド統計 (P. 90)
   - ユーザ データ サービス接続 (P. 91)

データベース接続の設定

以下の表に、データベース接続の設定情報を示します。

フィールド	Description
接続詳細	
データ ソース	選択した CA Strong Authentication サーバ インスタンスのために設定したデータ ソース名（DSN）です。
Type	サーバ インスタンスが使用しているデータベースがプライマリまたはバックアップのいずれであるかを示します。
最小接続数	CA Strong Authentication サーバ インスタンスに設定されているデータベース接続の最小数を示します。

フィールド	Description
最大接続数	CA Strong Authentication サーバ インスタンスに設定されているデータベース接続の最大数を示します。
現在の状況	
ステータス	プールがアクティブか非アクティブかを示します。
使用接続数	サーバ インスタンスによって現在使用されているデータベース接続の数を示します。
Connections Idle	サーバ インスタンスによって現在使用されていないデータベース接続の数を示します。
プール サイズ	接続プールで現在利用可能なデータベース接続の総数を示します。
失敗したクエリ数	指定した条件に一致するレコードを返さなかったクエリの数を示します。

サーバ プロトコル

以下の表に、設定されている各 CA Strong Authentication プロトコルのリクエスト、レスポンス、および処理の詳細を示します。

フィールド	Description
処理数	
Name	設定されているプロトコルの名前を指定します。
要求数	サーバ インスタンスによって処理されたリクエストの数です。
レスポンス	サーバ インスタンスによって送信されたレスポンスの数です。
成功	サーバ インスタンスによって正常に処理されたリクエストの数です。
Failed	サーバ インスタンスが処理に失敗したリクエストの数です。
内部エラー	内部エラーにより発生したエラーの数です。 内部エラーは、たとえば、データベースに到達できない、トークンが生成されない、トランザクション ID が生成されない、または、モジュールが正しくロードされない、などの理由で発生することがあります。
処理時間（ミリ秒）	

フィールド	Description
最小値	リクエストを処理するためにサーバ インスタンスによって費やされた最小時間です。
最大値	リクエストを処理するためにサーバ インスタンスによって費やされた最大時間です。
合計（秒）	リクエストを処理するためにサーバ インスタンスによって費やされた総時間です。
平均	リクエストを処理するためにサーバ インスタンスによって費やされた平均時間です。
最終リクエスト	最後のリクエストを処理するためにサーバ インスタンスによって費やされた時間です。
タイムスタンプ	
最後に受信したリクエスト	最後のリクエストがサーバ インスタンスによって受信されたときのタイム スタンプです。
最後に送信した応答	最後のレスポンスがサーバ インスタンスによって送信されたときのタイム スタンプです。

スレッド統計

以下の表に、プロトコルごとのスレッドの詳細を示します。 プロトコルごとの設定された値と現在の状態を示します。

フィールド	Description
設定済みデータ	
Name	CA Strong Authentication サーバと通信するためにクライアントによって使用されるプロトコルの名前。
最小値	リストされているプロトコルに設定されているスレッドの最小数。
最大値	リストされているプロトコルに許可されているスレッドの最大数。
しきい値	リストされているプロトコルの最大スレッド数のしきい値。 デフォルトでは、この値は 115 です。
現在の状況	

フィールド	Description
現在	リストされているプロトコルと CA Strong Authentication サーバとの間で確立されたアクティブなスレッドの現在の数。

ユーザ データ サービス接続

以下の表に、CA Strong Authentication サーバ インスタンスと UDS との間の接続の詳細を示します。

フィールド	Description
処理時間（ミリ秒）	
最小値	サーバ インスタンスによって送信されたリクエストを処理するために UDS によって費やされた最小時間です。
最大値	サーバ インスタンスによって送信されたリクエストを処理するために UDS によって費やされた最大時間です。
合計（秒）	サーバ インスタンスからのリクエストをすべて処理するために UDS によって費やされた総時間です。
平均	サーバ インスタンスからのリクエストを処理するために UDS によって費やされた平均時間です。
コール総数	CA Strong Authentication サーバから UDS に送信されたリクエストの総数です。
接続詳細 このセクションは、Web サービスの認証および許可、LDAP 認証などの処理を行う UDS Web サービスに CA Strong Authentication サーバから送信されたリクエストに関するものです。	
最小接続数	サーバ インスタンスと UDS との間に存在する接続の最小数です。
最大接続数	サーバ インスタンスと UDS との間に存在する接続の最大数です。
アクティブ接続数	サーバ インスタンスと UDS との間のアクティブな接続の数です。
非アクティブ接続数	サーバ インスタンスと UDS との間のアイドル接続の数です。
Web サービス タイムアウト	UDS からのレスポンスが受信される前にタイムアウトとなったリクエストの総数です。

プラグインの登録と更新

*プラグイン*は、サーバ側のカスタム コンポーネントで、プラグインを使用すると、CA Strong Authentication サーバの機能を拡張できます。 プラグインは CA Strong Authentication サーバ プロセスによってロードされ、カスタム イベント ハンドラ ライブラリとして実装されます。

プラグインを開発したら、イベントの発行済みセットに登録します。これにより、指定されたイベントが発生すると、プラグインが呼び出されるようになります。 登録には、［プラグインの登録］ページを使用します。 このページは、既存のプラグインを更新するためにも使用できます。 この画面を使用して設定したプラグ関連の設定は、システムで設定されているすべての組織で利用可能で、特定のインスタンスに限定できません。

プラグインの登録

次の手順に従ってください:

1. メイン メニューの［*サービスおよびサーバの設定*］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［拡張設定］セクションの［プラグイン登録］リンクをクリックすると、［プラグインの登録］ページが表示されます。
4. ［作成］オプションを選択します。
5. ［名前］にプラグインの名前を指定します。
6. ［ハンドラ パス］にプラグインのライブラリ ファイルへのパスを指定します。 ハンドラ ファイルには、開発したプラグイン ライブラリが含まれており、CA Strong Authentication からアクセスできる必要があります。

   UNIX で、このファイルが LD_LIBRARY_PATH によって指定されたパスで利用できる場合、ハンドラ ファイルへの絶対パスを指定する必要はありません。 単に拡張子のないファイル名を指定できます。 ただし、ハンドラ ファイルが LD_LIBRARY_PATH 変数によって指定されたパスで利用できない場合、ハンドラ ファイルへの絶対パスを指定する必要があります。
7. ［設定テンプレート］の隣にある参照ボタンをクリックし、プラグイン設定テンプレート ファイルの場所に移動します。

   設定テンプレート ファイルは、プラグインを設定するために使用されるデータの型、およびプラグインによって使用されるパラメータのデフォルト値を定義します。 この情報も、管理コンソールのプラグイン設定画面を表示するために使用されます。
8. プラグインに関連付けるイベントを［利用可能なイベント］リストから選択し、［>］ボタンをクリックすると、それらのイベントが［サポート対象イベント］リストに追加されます。

   注: ［利用可能なイベント］リストには、CA Strong Authentication で利用可能なすべてのイベントが表示され、［サポート対象イベント］リストには、登録中の新しいプラグインで利用可能なイベントが表示されます。
9. ［登録］をクリックすると、CA Strong Authentication の すべてのインスタンスがプラグインに登録されます。

10. 展開されているすべての CA Strong Authentication サーバ インスタンスを再起動します。この方法の詳細については、「サーバ インスタンスのリフレッシュ（P. 72）」を参照してください。

その他の設定

［その他の設定］を編集すると、以下の設定を変更できます。

- OTT（ワンタイム トークン）の長さとその有効性
- 認証トークンの有効性
- 認証メカニズムを有効にするか無効にするか

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［その他の設定］セクションの［その他の設定］リンクをクリックすると、対応するページが表示されます。
4. 必要に応じて、ページ上でフィールドを編集します。 以下の表に、このページのフィールドの説明を示します。

General

ワンタイム トークン長

認証が成功した後にユーザに発行される OTT （ワンタイム トークン）の長さを指定します。

デフォルト： 6

トークン有効期間（秒）

CA Strong Authentication によって発行される OTT の有効期間を指定します。

デフォルト： 300

認証トークン有効期間（秒）

CA Strong Authentication によって発行される認証トークンの有効期間を指定します。

デフォルト： 300

認証メカニズム ステータスの変更

CA Auth ID

CA Strong Authentication が CA Auth ID PKI 認証機能を提供するかどうかを指定します。

デフォルト： 有効

Q&A

CA Strong Authentication が Q&A 認証機能を提供するかどうかを指定します。

デフォルト： 有効

Password

CA Strong Authentication が基本的なパスワード認証機能を提供するかどうかを指定します。

デフォルト： 有効

OTP/アクティベーション コード

CA Strong Authentication が OTP ベースの認証をサポートするかどうかを指定します。

デフォルト： 有効

OATH OTP トークン

CA Strong Authentication が OATH OTP トークン ベースの認証をサポートするかどうかを指定します。

デフォルト： 有効

Kerberos

CA Strong Authentication が Kerberos ベースの認証をサポートするかどうかを指定します。

注: Kerberos 認証方式は ASSP （Adobe 署名サービス プロトコル）に対してのみサポートされています（「ASSP の設定 (P. 170)」を参照）。

デフォルト： 有効

CA Mobile OTP （ArcotOTP-OATH） CA Mobile OTP （ArcotOTP-OATH）

CA Strong Authentication が OATH 互換の ArcotOTP 認証情報をサポートするかどうかを指定します。

デフォルト： 有効

<arotp>

CA Strong Authentication が EMV 互換の ArcotOTP 認証情報をサポートするかどうかを指定します。

デフォルト： 有効

5. ［*更新*］をクリックすると、変更が保存されます。
6. ［*一般*］設定を変更したら、展開したすべての CA Strong Authentication サーバ インスタンスをリフレッシュします。ただし、認証メカニズム ステータスを変更している場合は、CA Strong Authentication サーバを再起動する必要があります。手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

第 5 章: グローバルな CA Strong Authentication 設定の管理

以下の 2 つのレベルで CA Strong Authentication 設定を管理できます。

- グローバル（すべての組織に適用可能）
- 組織レベル（個別の組織に適用可能）

システム レベルでグローバル設定を設定したとき、システム内のすべての組織はその設定を継承できます。 また、これらのグローバル設定は組織レベルの設定を優先させることができ、設定が行われた特定の組織にのみ適用することができます。 グローバル レベルまたは組織レベルでの設定の変更は、自動的に適用 *されません*。

重要: この章で説明される設定およびタスクはすべて、グローバル管理者のみが実行できます。

注: これらの設定は、それを設定する GA の権限の範囲内のすべての組織に適用可能です。個別の組織を設定するには、GA（グローバル管理者）、または対象組織の OA （組織管理者）としてログインします。 詳細については、「組織情報の更新 (P. 202)」を参照してください。

これらのタスクに加えて、GA は、グローバル レベルで基本認証ポリシーを設定することもできます。手順の詳細については、「基本認証パスワード ポリシーの設定 (P. 50)」を参照してください。

AuthMinder プロファイルおよびポリシーの理解

CA Strong Authentication の各エンド ユーザは、少なくとも 1 つの認証情報（CA Auth ID、Q&A、パスワード、OTP など）と関連付けられ、アプリケーションにログインするためにそれを使用する必要があります。 クレデンシャルを使用してエンド ユーザがログインするたびに、その認証は対応するポリシーによって制御されます。

認証情報プロファイル

多くのエンドユーザを CA Strong Authentication に登録する場合、同じ認証情報テンプレートがそのまま適用できることがあります。 そのような場合、CA Strong Authentication では、すぐに使える認証設定（*認証情報プロファイル*）を柔軟に作成できます。この認証情報プロファイルは、複数の組織の間で共有でき、そのため複数のユーザに適用できます。その結果、認証情報プロファイルを使用することにより、認証情報発行の管理が簡単になります。

認証情報 プロファイルでは、発行設定プロパティと、有効期間、キーの強度、パスワードの強度に関連する詳細などの認証情報属性を指定します。

CA Strong Authentication には、CA Mobile OTP（ArcotOTP-EMV）*以外の*各認証情報のデフォルト プロファイルが付属しています。 また、認証情報のすべてのタイプに複数のプロファイルを作成し、それぞれ一意の名前を付けることができます。 その後、1 つのプロファイルをデフォルトとして設定できます。 CA Strong Authentication では、ユーザへの認証情報の発行時に、これらの設定済みプロファイルを利用します。

認証ポリシー

CA Strong Authentication は複数の認証メカニズムをサポートします。 エンドユーザが CA Strong Authentication に対する認証を試行するたびに、認証処理は、*認証ポリシー*と呼ばれるルール（または確認）のセットによって制御されます。 たとえば、これらのルールは、認証情報がロック アウトされるまでに許可される失敗した認証試行の数と、認証前のユーザ ステータスを追跡するように設定できます。

CA Strong Authentication では、以下のタイプのトークンを生成できます。

- **ネイティブ トークン：** 有効期限が切れる前に複数回使用できる CA Strong Authentication のトークンです。
- **ワンタイム トークン：** 有効期限が切れる前に 1 回*しか*使用できません。
- **SAML トークン：** 他の任意の認証システムによって解釈可能です。 CA Strong Authentication は、SAML （Secure Assertion Markup Language）のバージョン 1.1 および 2.0 をサポートしています。

認証情報プロファイルと同様に、CA Strong Authentication には各認証情報のデフォルト ポリシーが付属しています。 また、認証情報のすべてのタイプに複数のプロファイルを作成し、それぞれ一意の名前を付けることができます。 1 つのプロファイルをデフォルトとして設定できます。

グローバル管理者としてのログイン

最初のグローバル管理者（GA）は MA が作成する必要があります。 GA としてログインし、引き続き設定を続行するには、MA からログイン認証情報の詳細を取得します。GA は、CA Strong Authentication パスワードを使用 (P. 102)して、または基本ユーザ パスワードを使用 (P. 104)してログインできます。

CA Strong Authentication パスワードの使用

MA が CA Strong Authentication パスワード認証情報を持つユーザのアカウントを作成した場合、そのユーザは、ID およびアクティベーション コード（ワンタイム パスワード）があることを確認してください。アクティベーション コードは、初めてログインするときにパスワードとして使用します。

次の手順に従ってください:

1. Web ブラウザを使用して、管理コンソールにアクセスするための URL を入力します。 管理コンソールのデフォルト URL は次のとおりです。

   http://<*hostname*>:<*app_server_port*>/arcotadmin/adminlogin.htm

2. ログインする組織名を指定します。

   重要: 組織の表示名を入力しないでください。組織の一意の ID を入力する必要があります（組織名によって定義）。たとえば、デフォルトの組織（表示名は CA）にログインする場合、この組織の（デフォルト）一意の ID である「defaultorg」を入力します。 ここで CA を指定しないでください。

3. ［ログイン］をクリックします。
4. ［ユーザ名］フィールドでユーザ ID を指定し、受け取った対応するアクティベーション コードを［パスワード］フィールドに入力して、［ログイン］をクリックします。
5. 初めてログインする場合は、パスワードを変更するように求められます。
6. ［新規パスワード］、［パスワードの確認］を指定し、次に［ログイン］をクリックします。

   ログイン ページにリダイレクトされます。

7. 再度パスワードを指定し、［ログイン］をクリックします。

   管理コンソールのランディング ページが表示されます。

パスワードを忘れた場合のフロー

次の手順に従ってください:

1. Web ブラウザを使用して、管理コンソールにアクセスするための URL を入力します。管理コンソールのデフォルト URL は以下のとおりです。

   http://<*hostname*>:<*app_server_port*>/arcotadmin/adminlogin.htm

2. ［組織名］にログインする組織名を入力し、［ログイン］をクリックします。
3. ユーザ名を入力します。
4. ［パスワードを忘れた場合 ］リンクをクリックします。
5. ［ユーザ名］フィールドにユーザ ID を指定し、［ログイン］をクリックします。

   プロファイル情報に設定された質問（この Q&A 情報を設定する方法については「管理者のプロファイル情報の変更 (P. 225)」を参照してください）を表示するページが表示されます。
6. 表示された質問に対応する回答を指定し、［ログイン］をクリックします。

   ［パスワードのリセット］ページが表示されます。
7. ［新規パスワード］および［パスワードの確認］の各フィールドに新しいパスワードを入力します。
8. ［ログイン］をクリックします。

   ［ログイン］ページが表示されます。
9. 再度パスワードを指定し、［ログイン］をクリックします。

   管理コンソールのランディング ページが表示されます。

基本ユーザ パスワードを使用したログイン

基本ユーザ パスワード認証情報を使用して GA として管理コンソールにログインする方法

次の手順に従ってください:

1. Web ブラウザを使用して、管理コンソールにアクセスするための URL を入力します。 管理コンソールのデフォルト URL は次のとおりです。

   http://<*hostname*>:<*app_server_port*>/arcotadmin/adminlogin.htm

2. ログインする組織名を入力します。

   重要: 組織の表示名を入力しないでください。組織の一意の ID を入力する必要があります（組織名によって定義）。たとえば、デフォルトの組織（表示名は CA）にログインする場合、この組織の（デフォルト）一意の ID である「defaultorg」を入力します。 ここで CA を指定しないでください。

3. ［ログイン］をクリックします。

   注: このページには、［パスワードを忘れた場合］リンクは表示されません。 このリンクは、WebFort パスワード認証情報を使用してログインするときに利用できます。

4. ［ユーザ名］フィールドにユーザ ID を指定し、［パスワード］フィールリドに対応するパスワードを入力して、［ログイン］をクリックします。

   初めてログインする場合は、パスワードを変更するように求められます。

5. ［新規パスワード］、［パスワードの確認］を指定し、次に［ログイン］をクリックします。

   ログイン ページにリダイレクトされます。

6. 再度**パスワード**を指定し、［**ログイン**］をクリックします。

   管理コンソールのランディング ページが表示されます。

プロファイルとポリシーの設定

このセクションでは、CA Advanced Authentication によってサポートされている認証情報のプロファイルおよびポリシーの設定について説明します。

重要: *(JBoss EAP 6.2 アプリケーション サーバの場合)* ポリシーの数が 500 を超える場合、または管理コンソールで単一のリクエストのリクエストパラメータにおいて例外が発生する場合は、*<JBOSS_HOME>¥standalone¥configuration* フォルダにある standalone.xml 内の <extensions> タグの後に*以下のシステム プロパティ*を追加します。

```
<system-properties>

    <property name="org.apache.tomcat.util.http.Parameters.MAX_COUNT"
value="2000"/>

</system-properties>
```

CA Auth ID PKI の設定

このセクションでは、以下の手順について説明します。

- CA Auth ID PKI 認証情報プロファイルの設定 (P. 106)
- CA Auth ID PKI 認証ポリシーの設定 (P. 110)

注: このセクションのすべてのタスクを実行するには、グローバル管理者（MA）としてログインしていることを確認します。

CA Auth ID PKI 認証情報プロファイルの設定

以下の属性を定義するために CA Auth ID PKI プロファイルを使用できます。

- **キー長**： CA Auth ID PKI の Cryptographic Camouflage アルゴリズムで使用されるキーのサイズ（ビット単位）です。
- **有効期間**： CA Auth ID PKI 認証情報が有効な期間です。
- **パスワード強度**：パスワードの長さとそれに含まれるアルファベット、数字、および特殊文字の数の組み合わせによって決定される、パスワードの有効性です。

CA Auth ID PKI プロファイルを設定し、それを 1 つ以上の組織に割り当てることによって、それらの組織のユーザに発行される CA Auth ID PKI の特性を制御できます。

次の手順に従ってください:

1. メイン メニューの［*サービスおよびサーバの設定*］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［CA Auth ID］セクションの［発行］リンクをクリックすると、［CA Auth ID プロファイル］ページが表示されます。
4. 必要に応じて、［プロファイル設定］セクションのフィールドに入力します。
   - **プロファイル設定**

   作成

   新規プロファイルを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規プロファイルの設定名を指定します。

   更新

   既存のプロファイルを更新する場合は、［設定の選択］リストから更新するプロファイルを選択します。

   設定のコピー

   既存のプロファイルから設定をコピーしてプロファイルを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするプロファイルを選択します。

キー長(ビット)

暗号化に使用されるキーのサイズ(ビット単位)を指定します。デフォルト値は 1024 ビットです。

有効期間の開始日

発行された CA Auth ID PKI 認証情報が有効になる日付を指定します。

有効期間は、CA Auth ID PKI が作成された日付から開始することもできますし、特定の日付を指定することもできます。

有効期間の終了日

CA Auth ID PKI が期限切れになる日付を指定します。

認証情報の有効期間を指定することもできますし、特定の日付を指定することもできます。

- **パスワード強度**

最小文字数

パスワードに含むことができる最小文字数を指定します。 値は 4 ～ 64 文字で設定できます。

最大文字数

パスワードに含むことができる最大文字数を指定します。 値は 4 ～ 64 文字で設定できます。

アルファベット文字の最小文字数

パスワードに含むことができるアルファベット文字(a ～ z および A ～ Z)の最小文字数を指定します。

この値は、[最小文字数]フィールドで指定した値以下にする必要があります。

数字の最小文字数

パスワードに含むことができる数字(0 ～ 9)の最小文字数を指定します。

特殊文字の最小文字数

パスワードに含むことができる特殊文字の最小文字数を指定します。 デフォルトでは、ASCII （0 ～ 31）文字を除く特殊文字はすべて許可されています。

5. ［**詳細設定**］セクションを展開します。
6. ［**追加属性**］セクションで、CA Auth ID PKI 認証情報に対して**名前**と**値**のペアの形式で渡す追加情報（符号のない属性）を指定します。

   たとえば、エンド ユーザのシステムなどの特定のデバイスに CA Auth ID PKI をロックする場合は、このセクションを使用して、以下に示す追加情報を送信します。

   devlock_required

   値： yes

   devlock_type

   値： hd

   注: ここで指定できる追加情報の詳細については、「*CA Auth ID クライアント リファレンス ガイド*」を参照してください。

   より多くの属性を指定する必要がある場合は、［**さらに追加**］をクリックすると、一度に 1 つの追加フィールドが表示されます。
7. ［**カスタム属性**］セクションで、**名前**と**値**のペアの形式で追加情報を指定します。 たとえば、プラグインで使用できる組織情報などです。
8. ［**ユーザ検証**］セクションで以下を設定します。
   - 現在の認証情報に関する以下の操作に対するユーザ ステータスを確認するには、［**アクティブなユーザ**］チェック ボックスをオンにします。
     - 認証情報の作成
     - 認証情報の再発行
     - 認証情報のリセット
     - 認証情報の有効期間のリセット
   - ユーザ属性が特定の値と一致するかどうか確認する場合は、［**ユーザ属性**］オプションを選択します。 以下のユーザ属性に対する値を設定できます。
     - ユーザが作成された日付
     - ユーザ詳細が変更された日付
     - 電子メール アドレス

- First name
- ミドル ネーム
- Last name
- ユーザ ステータス
- 電話番号
- 一意のユーザ識別子

注: ユーザ属性確認機能は、組織レベルで設定を実行している場合にのみ利用可能です。

9. ［**複数認証情報オプション**］セクションで、［**使用タイプ**］フィールドに CA Auth ID PKI を使用する目的を識別するための説明を入力します。たとえば、ユーザは、ネットワークへのリモート ログインを実行するために一時認証情報を持つことができます。この認証情報用の使用タイプは「*temporary*」とすることができます。
10. ［**履歴の検証**］セクションでは、古い CA Auth ID PKI パスワードを再利用しないようユーザに強制することができます。以下のフィルタ オプションのいずれかを選択できます。
    - **過去 <N> 個のパスワード**： 現在の CA Auth ID PKI パスワードが、過去の *<n>* 個のパスワードと異なる必要がある場合は、このオプションを選択します。
    - **パスワード対象期間**： 現在の CA Auth ID PKI パスワードが、指定された期間に使用されたパスワードと異なる必要がある場合は、このオプションを選択します。
11. ［**保存**］をクリックして、CA Auth ID PKI プロファイルを作成または更新します。
12. 展開された CA Strong Authentication インスタンスをすべてリフレッシュします。 手順の詳細については、「サーバ インスタンスのリフレッシュ（P. 72）」を参照してください。

CA Auth ID PKI 認証ポリシーの設定

CA Auth ID PKI ポリシーを使用して、CA Auth ID PKI ベースの認証に関連する以下の属性を指定できます。

- **ユーザ ステータス：** ユーザのステータスです。アクティブまたは非アクティブのいずれかです。

  注: ユーザ ステータスの確認を有効にすると、非アクティブ状態のユーザの認証は失敗します。

- **ロックアウト条件：** 許可される試行の失敗数です。この数を超えると、ユーザの認証情報がロック アウトされます。
- **ロック解除条件：** ロックされた CA Auth ID PKI 認証情報を使用して再度ログイン可能になるまでの時間数です。 この機能は、認証情報 リセットのリクエスト数を大きく減らすことができます。
- **期限切れの CA Auth ID PKI の使用：** ユーザが期限切れの CA Auth ID PKI 認証情報を使用して認証に成功できる日数です。
- **期限切れ警告設定：** ユーザの CA Auth ID PKI 認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

注: これらのオプションは慎重に使用してください。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［ArcotID］セクションの［認証］リンクをクリックすると、［CA Auth ID 認証ポリシー］ページが表示されます。
4. 必要に応じて、［ポリシー設定］セクションのフィールドに入力します。

   - **ポリシー設定**

   作成

   新規ポリシーを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規ポリシーの設定名を指定します。

更新

既存のポリシーを更新する場合は、表示される［設定の選択］リストから更新するポリシーを選択します。

設定のコピー

既存のポリシーから設定をコピーしてポリシーを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするポリシーを選択します。

認証情報ロックアウト

許可される試行の失敗数を指定します。この数を超えると、ユーザの認証情報がロックされます。

認証前にユーザ ステータスを確認

認証の前にユーザのステータスがアクティブかどうかを確認する場合は、このオプションを選択します。

5. ［+］記号をクリックして［**詳細設定**］セクションを展開します。
6. 必要に応じて、このセクションのフィールドに入力します。

- **詳細設定**

警告を発行

ユーザの CA Auth ID PKI 認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

期限切れ認証によるログイン猶予日数

正常にログインするためにユーザが期限切れの CA Auth ID PKI 認証情報を使用できる日数を指定します。

認証情報の自動ロック解除を有効化

ロックされた認証情報が、［ロック解除までの時間］フィールドに指定した時間の後に自動的にロック解除されるようにする場合は、このチェック ボックスをオンにします。

このフィールドは、［認証情報ロックアウト］フィールドで対応する値を指定する場合のみ有効です。

注: 認証情報は、ロック解除期間の後に自動的にロック解除されません。 認証情報をロック解除するには、ロック解除期間の後に認証に使用して成功させる必要があります。

ロック解除までの時間

ロックされた認証情報が認証に再使用できるようになるまでの時間数を指定します。

チャレンジ有効期間(秒)

CA Auth ID PKI チャレンジの有効期間を指定します。

- **複数認証情報オプション**

検証用の使用タイプ

ユーザが特定の CA Auth ID PKI を使用して認証する場合は、このフィールドにその使用タイプの名前を入力します。

使用タイプを指定しないと、デフォルトの CA Auth ID PKI 認証ポリシーで指定された使用タイプが使用されます。

7. ［保存］をクリックします。
8. 展開された CA Strong Authentication インスタンスをすべてリフレッシュします。 手順の詳細については、「サーバインスタンスのリフレッシュ (P. 72)」を参照してください。

QnA の設定

このセクションでは、以下の手順について説明します。

- Q&A 発行プロファイルの設定 (P. 113)
- Q&A 認証ポリシーの設定 (P. 117)

Q&A 発行プロファイルの設定

Q&A プロファイルを使用して、Q&A 認証情報に関連する以下の属性を指定できます。

- **質問の数：**
  - 発行時にユーザが設定する必要がある、質問と回答の最小数です。
  - 発行時にユーザが設定できる、質問と回答の最大数です。
- **有効期間：** Q&A 認証情報が有効な期間です。
- **回答で大文字と小文字を区別：** ユーザが入力した回答で大文字と小文字を区別する必要があるかどうかを決定します。
- **質問バンク：** ユーザは、Q&A 認証情報をセットアップするため、質問バンクのあらかじめ設定済みの質問を使用します。

Q&A プロファイルを設定し、それを 1 つ以上の組織に割り当てることによって、それらの組織のユーザに発行される Q&A 認証情報の特性を制御できます。 Q&A 認証情報プロファイルを作成するには、［質問および回答プロファイル］ページを使用します。

次の手順に従ってください:

1. メイン メニューの［*サービスおよびサーバの設定*］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［Q&A］セクションの［発行］リンクをクリックすると、［質問および回答プロファイル］ページが表示されます。
4. 必要に応じて、［プロファイル設定］セクションのフィールドに入力します。
   - **プロファイル設定**

   作成

   新規プロファイルを作成する場合は、以下の手順に従います。
   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規プロファイルの設定名を指定します。

   更新

既存のプロファイルを更新する場合は、表示される［設定の選択］リストから更新するプロファイルを選択します。

設定のコピー

既存のプロファイルから設定をコピーしてプロファイルを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするプロファイルを選択します。

質問と回答の最小数

ユーザが設定する必要がある質問と回答の最小数を指定します。

たとえば、このフィールドに「3」を設定し、［質問と回答の最大数］フィールドに「5」を設定する場合、設定した 5 つの質問のうち、認証時に少なくとも 3 つに正解する必要があります。

質問と回答の最大数

ユーザが設定できる質問と回答の最大数を指定します。

回答で大文字と小文字を区別

ユーザが指定する回答が、Q&A の設定に使用した大文字または小文字と一致する必要があるかどうかを指定します。

有効期間の開始日

発行された QnA 認証情報が有効になる日付を設定します。

有効期間は、QnA が作成された日付から開始することもできますし、特定の日付を指定することもできます。

有効期間の終了日

Q&A 認証情報が期限切れになる日付を設定します。

認証情報の有効期間を指定することもできますし、特定の日付を指定することもできます。

5. **［+］**記号をクリックして［**詳細設定**］セクションを展開します。
6. ［**カスタム属性**］セクションで、**名前**と**値**のペアの形式で追加情報を指定します。 たとえば、プラグインで使用できる組織情報などです。
7. ［**ユーザ検証**］セクションで以下を設定します。

- 現在の認証情報に関する以下の操作に対するユーザ ステータスを確認するには、［**アクティブなユーザ**］チェック ボックスをオンにします。
  - 認証情報の作成
  - 認証情報の再発行
  - 認証情報のリセット
  - 認証情報の有効期間のリセット
- ユーザ属性が特定の値と一致するかどうか確認する場合は、［**ユーザ属性**］オプションを選択します。 以下のユーザ属性に対する値を設定できます。
  - ユーザが作成された日付
  - ユーザ詳細が変更された日付
  - 電子メール アドレス
  - First name
  - ミドル ネーム
  - Last name
  - ユーザ ステータス
  - 電話番号
  - 一意のユーザ識別子

  注: ユーザ属性確認機能は、組織レベルで設定を実行している場合にのみ利用可能です。

8. ［QnA 発行用の質問バンク］セクションで以下を設定します。
   - ［質問リターン モード］で、ユーザが回答を設定するためにどのような質問を選択する必要があるかを指定します。 サポートされているモードは以下のとおりです。
     - 固定 - 設定されている質問のセットから決まった質問を選択し、ユーザに提示します。
     - ランダム - 設定されている質問のセットから質問をランダムに選択し、ユーザに提示します。
   - ［質問バンク］テーブルで質問を入力します。これらはグローバル レベルで設定されます。 これらの質問は組織レベルで上書きできます。

9. ［複数認証情報オプション］セクションで、［使用タイプ］フィールドに QnA を使用する目的を識別するための説明を入力します。たとえば、ユーザは、ネットワークへのリモート ログインを実行するために一時認証情報を持つことができます。この認証情報用の使用タイプは「temporary」とすることができます。
10. ［保存］をクリックし、QnA プロファイルを作成または更新します。
11. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ（P. 72）」を参照してください。

Q&A 認証ポリシーの設定

Q&A ベースの認証に関連する以下の属性を指定するために Q&A ポリシーを使用できます。

- **ユーザ ステータス**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。

  注: ユーザ ステータスの確認を有効にすると、非アクティブ状態のユーザの認証は失敗します。

- **質問の数**：
  - CA Strong Authentication では、認証処理中にユーザに質問を行う必要があります。
  - そのため、正しい回答が認証時に必要です。
- **コール元検証**：回答がサードパーティによって確認されてから結果が CA Strong Authentication サーバに送信されます。
- **ロックアウトの条件：** 許可される試行の失敗数です。この数を超えると、ユーザの認証情報がロック アウトされます。
- **ロック解除の条件：** ロックされた Q&A 認証情報がログインに再使用できるようになるまでの時間数です。
- **質問選択モード**：質問は、ランダムまたは交互に選択されます。つまり、［**質問セットの変更**］オプションに基づいて、新しい質問セットが質問されます。
- **質問セットの変更**: 各試行の後で、または認証成功の後で質問セットが変更されます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［QnA］セクションの［認証］リンクをクリックすると、［QnA 認証ポリシー名］ページが表示されます。
4. 必要に応じて、［ポリシー設定］セクションのフィールドに入力します。
   - **ポリシー設定**

   作成

新規ポリシーを作成する場合は、以下の手順に従います。

- ［作成］オプションを選択します。
- 表示されるフィールドに、新規ポリシーの設定名を指定します。

更新

既存のポリシーを更新する場合は、表示される［設定の選択］リストから更新するポリシーを選択します。

設定のコピー

既存のポリシーから設定をコピーしてポリシーを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするポリシーを選択します。

チャレンジの質問数

ユーザが認証中に回答を求められる質問の数を設定します。

必要な正解数

認証に成功するためにユーザが提示する必要がある正しい回答の数を指定します。

たとえば、このフィールドに「3」を設定し、［チャレンジの質問数］フィールドに「5」を設定する場合、ユーザは 5 つの質問のうち少なくとも 3 つに正解する必要があります。

コール元検証の有効化

このオプションを有効にすると、認証中に回答が CSR （Customer Support Representatives、テクニカル サポート担当者）または同様の機関によって収集され確認されます。また、確認結果は CA Strong Authentication サーバに送信されます。

認証情報ロックアウト

許可される試行の失敗数を指定します。この数を超えると、ユーザの認証情報がロックされます。

認証前にユーザ ステータスを確認

認証の前にユーザのステータスがアクティブかどうかを確認する場合は、このオプションを選択します。

5. ［+］記号をクリックして［**詳細設定**］セクションを展開します。

6. 必要に応じて、このセクションのフィールドに入力します。

   - **詳細設定**

警告を発行

ユーザの認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

期限切れ認証によるログイン猶予日数

正常にログインするためにユーザが期限切れの認証情報を使用できる日数を指定します。

認証情報の自動ロック解除を有効化

ロックされた認証情報が、次のフィールドに指定した時間の後に自動的にロック解除されるようにする場合は、このチェック ボックスをオンにします。

このフィールドは、［認証情報ロックアウト］フィールドで対応する値を指定する場合のみ有効です。

注: 認証情報は、ロック解除期間の後に自動的にロック解除されません。 認証情報をロック解除するには、ロック解除期間の後に認証に使用して成功させる必要があります。

ロック解除までの時間

ロックされた認証情報が認証に再使用できるようになるまでの時間数を指定します。

質問選択モード

提示される質問が選択される方法を指定します。 サポートされている値は以下のとおりです。

- ランダム - 質問は、設定されたセットからランダムに選択されます。
- 別の質問 - 設定されているセットから新しい質問のセットが選択されます。つまり、前回の認証メッセージで尋ねられた質問はスキップされます。

質問セットの変更

CA Strong Authentication サーバが質問の新しいセットを選択して提示する必要がある時期を指定します。 サポートされるオプションは以下のとおりです。

- 認証成功時のみ - ユーザ認証が成功した場合のみ、質問選択モードに基づいて新しい質問セットが選択されます。
- 各試行ごと - 認証が試行されるたびに、認証結果に関係なく、質問選択モードに基づいて新しい質問セットが選択されます。

チャレンジ有効期間（秒）

Q&A チャレンジの有効期間を指定します。

- **複数認証情報オプション**

検証用の使用タイプ

ユーザが特定の Q&A 認証情報を使用して認証する場合は、このフィールドにその使用タイプの名前を入力します。

使用タイプを指定しないと、デフォルトの QnA 認証ポリシーで指定された使用タイプが使用されます。

7. ［保存］をクリックします。
8. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ（P. 72）」を参照してください。

パスワードの設定

このセクションでは、以下の手順について説明します。

- パスワード発行プロファイルの設定（P. 121）
- パスワード認証ポリシーの設定（P. 125）

パスワード発行プロファイルの設定

パスワード認証情報に関連する以下の属性を指定するために、パスワードプロファイルを使用できます。

- **パスワード強度**：パスワードの長さとそれに含まれるアルファベット、数字、および特殊文字の数によって決定される、パスワードの有効性です。
- **有効期間：** パスワード認証情報が有効な期間です。
- **パスワードの自動生成**： CA Strong Authentication サーバによってパスワードが作成されます。
- **使用数**： パスワードを使用可能な回数です。
- **使用タイプおよびパスワードの一意性：** 使用要件に基づいて、ユーザは複数のパスワード認証情報を持つことができます。 たとえば、一時的なパスワードと永続的なパスワードなどです。 これらのパスワードは同じにすることも、一意にすることもできます。

パスワード プロファイルを設定し、それを 1 つ以上の組織に割り当てることによって、それらの組織のユーザに発行されるパスワード認証情報の特性を制御できます。 パスワード認証情報プロファイルを作成するには、［パスワード プロファイル］ページを使用します。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［パスワード］セクションの［発行］リンクをクリックすると、［パスワード プロファイル］ページが表示されます。
4. 必要に応じて、［プロファイル設定］セクションのフィールドに入力します。
   - **プロファイル設定**

   作成

   新規プロファイルを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規プロファイルの設定名を指定します。

更新

既存のプロファイルを更新する場合は、［設定の選択］リストから更新するプロファイルを選択します。

設定のコピー

既存のプロファイルから設定をコピーしてプロファイルを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするプロファイルを選択します。

有効期間の開始日

発行されたパスワード認証情報が有効になる日付を設定します。

有効期間は、この認証情報が作成された日付から開始することも、カスタムの日付を指定することもできます。

有効期間の終了日

パスワードが期限切れになる日付を設定します。

期限切れになる日付を設定するには、以下のオプションのいずれかを選択できます。

- 期間の指定
- カスタム日付の指定

パスワードが期限切れにならないようにするには、［無期限にする］オプションを選択します。

- **パスワード強度オプション**

最小文字数

パスワードに含むことができる最小文字数を指定します。 値は 4 ～ 64 文字で設定できます。

デフォルト値は 6 です。

最大文字数

パスワードに含むことができる最大文字数を指定します。 値は 4 ～ 64 文字で設定できます。

デフォルト値は 10 です。

アルファベット文字の最小文字数

パスワードに含むことができるアルファベット文字（a ～ z および A ～ Z）の最小文字数を指定します。

この値は、［最小文字数］フィールドで指定した値以下にする必要があります。

数字の最小文字数

パスワードに含むことができる数字（0 ～ 9）の最小文字数を指定します。 値は 0 ～ 32 文字で設定できます。

特殊文字の最小文字数

パスワードに含むことができる特殊文字の最小文字数を指定します。 デフォルトでは、ASCII （0 ～ 31）文字を除く特殊文字はすべて許可されています。

5. ［**+**］記号をクリックして［**詳細設定**］セクションを展開します。
6. ［**カスタム属性**］セクションで、**名前**と**値**のペアの形式で追加情報を指定します。 たとえば、プラグインで使用できる組織情報などです。
7. ［**ユーザ検証**］セクションで以下を設定します。
   - 現在の認証情報に関する以下の操作に対するユーザ ステータスを確認するには、［**アクティブなユーザ**］チェック ボックスをオンにします。
     - 認証情報の作成
     - 認証情報の再発行
     - 認証情報のリセット
     - 認証情報の有効期間のリセット
   - ユーザ属性が特定の値と一致するかどうか確認する場合は、［**ユーザ属性**］オプションを選択します。 以下のユーザ属性に対する値を設定できます。
     - ユーザが作成された日付
     - ユーザ詳細が変更された日付
     - 電子メール アドレス
     - First name
     - ミドル ネーム
     - Last name
     - ユーザ ステータス

- 電話番号
- 一意のユーザ識別子

注: ユーザ属性確認機能は、組織レベルで設定を実行している場合にのみ利用可能です。

8. ［**追加パスワード オプション**］セクションで以下を設定します。
   - CA Strong Authentication サーバがユーザ パスワードを生成するようにするには、［**パスワードの自動生成**］チェック ボックスをオンにします。ユーザがパスワードを忘れ、サーバが新しいパスワードを自動生成可能で、ユーザが次回のログインにこの新しいパスワードを使用できる場合に、この機能を使用できます。
   - ［**使用数**］オプションでは、有効期限が切れるまでパスワードを有効にする場合は［**無制限**］を選択します。 パスワードの使用回数を制限する場合は、2 番目のオプション内に回数を入力します。
9. ［**複数認証情報オプション**］セクションで以下を設定します。
   - ［**使用タイプ**］フィールドにパスワードの使用目的を識別する説明を入力します。 たとえば、ユーザは、ネットワークへのリモート ログインを実行するために一時パスワードを持つことができます。このパスワード用の使用タイプは「temporary」とすることができます。
   - 使用タイプが異なるパスワードを一意とする必要がある場合は、［**使用タイプ内でパスワードが一意**］チェック ボックスを有効にします。
10. ［**履歴の検証**］セクションでは、古いパスワードを再利用しないようユーザに強制することができます。以下のフィルタ オプションのいずれかを選択できます。
    - **過去 <N> 個のパスワード**： 現在のパスワードが、過去の <n> 個のパスワードと異なる必要がある場合は、このオプションを選択します。
    - **パスワード対象期間**： 現在のパスワードが、指定された期間に使用されたパスワードと異なる必要がある場合は、このオプションを選択します。
11. ［保存］をクリックします。
12. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。 手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

パスワード認証ポリシーの設定

パスワード ベースの認証に関連する以下の属性を定義するためにパスワード ポリシーを使用できます。

- **ユーザ ステータス**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。

  注: ユーザ ステータスの確認を有効にすると、非アクティブ状態のユーザの認証は失敗します。

- **ロックアウトの条件：** 許可される試行の失敗数です。この数を超えると、ユーザの認証情報がロック アウトされます。
- **ロック解除の条件：** ロックされたユーザ パスワード 認証情報が再度ログインで使用可能になるまでの時間数です。
- **部分パスワード オプション：**チャレンジのためのパスワードの文字数。

  CA Strong Authentication サーバが部分パスワード認証リクエストを受信すると、ユーザはパスワード中の異なる位置の文字を入力するように求められます。 たとえば、パスワードが welcome1 で、［**チャレンジで使用するパスワード文字数**］フィールドが 4 に設定される場合を考えます。 チャレンジとして「2、4、7 の位置のチャレンジを入力」と表示された場合、 「ece」と入力すると、認証は成功します。

- **複数パスワード オプション：**特定の使用タイプを持つ、パスワードのいずれかまたはパスワードを入力することが許可されているかどうかを指定します。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［パスワード］セクションの［認証］リンクをクリックすると、［パスワード認証ポリシー］ページが表示されます。
4. 必要に応じて、［ポリシー設定］セクションのフィールドに入力します。

   - **ポリシー設定**

   作成

   新規ポリシーを作成する場合は、以下の手順に従います。

- ［作成］オプションを選択します。
- 表示されるフィールドに、新規ポリシーの設定名を指定します。

更新

既存のポリシーを更新する場合は、表示される［設定の選択］リストから更新するポリシーを選択します。

設定のコピー

既存のポリシーから設定をコピーしてポリシーを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするポリシーを選択します。

認証情報ロックアウト

許可される試行の失敗数を指定します。この数を超えると、ユーザの認証情報がロックされます。

認証前にユーザ ステータスを確認

認証の前にユーザがアクティブかどうかを確認する場合は、このオプションを選択します。

5. ［+］記号をクリックして［**詳細設定**］セクションを展開します。
6. 必要に応じて、このセクションのフィールドに入力します。

- 追加パスワード オプション

警告を発行

ユーザの認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

期限切れ認証によるログイン猶予日数

正常にログインするためにユーザが期限切れの認証情報を使用できる日数を指定します。

認証情報の自動ロック解除を有効化

認証情報が、次のフィールドに指定した時間の後に自動的にロック解除されるようにする場合は、このオプションを選択にします。

このフィールドは、［認証情報ロックアウト］フィールドで対応する値を指定する場合のみ有効です。

注: 認証情報は、ロック解除期間の後に自動的にロック解除されません。 認証情報をロック解除するには、ロック解除期間の後に認証に使用して成功させる必要があります。

ロック解除までの時間

ロックされた認証情報が認証に再使用できるようになるまでの時間数を指定します。

チャレンジ有効期間（秒）

パスワード チャレンジの有効期間を指定します。

- **部分パスワード オプション**

チャレンジで使用するパスワード文字数

提示される必要があるパスワード文字の総数を指定します。 CA Strong Authentication サーバによって提示されるランダムな位置の数はこの値と等しくなります。

- **代替処理オプション**

代替処理オプション

CA Strong Authentication サーバ はプロキシとして機能し、以下の条件に基づいて、認証リクエストをほかの認証サーバへ渡します。

- 見つからないユーザ： 認証しようとするユーザが CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。
- 見つからない認証情報: ユーザが認証に使用しようとしている認証情報が CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。

この機能を有効にする方法の詳細については、「RADIUS プロキシ サーバとしての CA Strong Authentication の設定」を参照してください。

- **複数認証情報オプション**

検証用の使用タイプ

複数のパスワードのいずれかを使用して認証する場合は、［任意の使用タイプ］オプションを選択します。 たとえば、ユーザが、使用タイプが「permanent」である「welcome123」と使用タイプが「temporary」である「hello123」という 2 つのパスワードを持っている場合、いずれかのパスワードを提供すると、ユーザが認証されます。

ユーザが特定のパスワードを使用して認証する場合は、［使用タイプ］フィールドにその使用タイプの名前を入力します。

7. ［保存］をクリックします。
8. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。 手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

OTP の設定

このセクションでは、以下の手順について説明します。

- OTP 発行プロファイルの設定 (P. 129)
- OTP 認証ポリシーの設定 (P. 132)

OTP 発行プロファイルの設定

OTP プロファイルを使用して、ワンタイム パスワード認証情報に関連する以下の属性を定義できます。

- **OTP 長**： OTP のタイプ（数字または英数字）および長さです。
- **有効期間**： OTP が有効な期間です。
- **使用数**： OTP を認証に再使用できる回数です。

OTP プロファイルを設定し、それを 1 つ以上の組織に割り当てることによって、それらの組織のユーザに発行される OTP 認証情報の特性を制御できます。 OTP 認証情報プロファイルを作成するには、［ワン タイム パスワード プロファイル］ページを使用します。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［OTP］セクションの［発行］リンクをクリックすると、［ワン タイム パスワード プロファイル］ページが表示されます。
4. 必要に応じて、［プロファイル設定］セクションのフィールドに入力します。

   プロファイル設定

   作成

   新規プロファイルを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規プロファイルの設定名を指定します。

   更新

   既存のプロファイルを更新する場合は、表示される［設定の選択］リストから更新するプロファイルを選択します。

   設定のコピー

   既存のプロファイルから設定をコピーしてプロファイルを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするプロファイルを選択します。

Type

ユーザに数値または英数字の OTP を発行するかどうかを指定します。

デフォルト値は［数値］です。

長さ

OTP の長さを設定します。

OTP の最小長は 5（デフォルト値でもあります）であり、最大長は 32 文字です。

有効期間

発行された OTP 認証情報の有効期間を設定します。

秒単位、分単位、時間単位、および日単位で指定でき、月単位および年単位でも指定できます。

複数回の使用を許可

OTP を 2 回以上使用する場合は、このチェック ボックスをオンにします。

用途

［複数回の使用を許可］チェック ボックスをオンにした場合は、OTP が使用可能な合計回数を指定します。

5. ［**+**］記号をクリックして［**詳細設定**］セクションを展開します。
6. ［**カスタム属性**］セクションで、**名前**と**値**のペアの形式で追加情報を指定します。 たとえば、プラグインで使用できる組織情報などです。
7. ［**ユーザ検証**］セクションで以下を設定します。
   - 現在の認証情報に関する以下の操作に対するユーザ ステータスを確認するには、［**アクティブなユーザ**］チェック ボックスをオンにします。
     - 認証情報の作成
     - 認証情報の再発行
     - 認証情報のリセット

- 認証情報の有効期間のリセット

- ユーザ属性が特定の値と一致するかどうか確認する場合は、［**ユーザ属性**］オプションを選択します。 以下のユーザ属性に対する値を設定できます。
  - ユーザが作成された日付
  - ユーザ詳細が変更された日付
  - 電子メール アドレス
  - First name
  - ミドル ネーム
  - Last name
  - ユーザ ステータス
  - 電話番号
  - 一意のユーザ識別子

  注: ユーザ属性確認機能は、組織レベルで設定を実行している場合にのみ利用可能です。

8. ［**複数認証情報オプション**］セクションで、［**使用タイプ**］フィールドに OTP を使用する目的を識別するための説明を入力します。たとえば、ユーザは、ネットワークへのリモート ログインを実行するために一時認証情報を持つことができます。この認証情報用の使用タイプは「*temporary*」とすることができます。
9. ［保存］をクリックします。
10. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。 手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

OTP 認証ポリシーの設定

OTP ベースの認証に関連する以下の属性を定義するために OTP ポリシーを使用できます。

- **ユーザ ステータス**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。

  注: ユーザ ステータスの確認を有効にすると、非アクティブ状態のユーザの認証は失敗するようになります。

- **ロック アウト条件：** 失敗した試行の数です。この数を超えると、ユーザの認証情報がロックされます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［OTP］セクションの［認証］リンクをクリックすると、［OTP 認証ポリシー名］ページが表示されます。
4. 必要に応じて、［ポリシー設定］セクションのフィールドに入力します。

   ポリシー設定

   作成

   新規ポリシーを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規ポリシーの設定名を指定します。

   更新

   既存のポリシーを更新する場合は、表示される［設定の選択］リストから更新するポリシーを選択します。

   設定のコピー

   既存のポリシーから設定をコピーしてポリシーを作成する場合は、このオプションを有効にします。

   注: スコープがあるほかの組織に属する設定からコピーすることもできます。

   利用可能な設定

設定をコピーするポリシーを選択します。

認証情報ロックアウト

失敗した試行の数を指定します。この数を超えると、OTP がロックされます。

認証前にユーザ ステータスを確認

認証の前にユーザのステータスがアクティブかどうかを確認する場合は、このオプションを選択します。

5. ［+］記号をクリックして［**詳細設定**］セクションを展開します。
6. 必要に応じて、このセクションのフィールドに入力します。 以下の表に、このセクションのフィールドの説明を示します。

詳細設定

警告を発行

ユーザの認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

期限切れ認証によるログイン猶予日数

正常にログインするためにユーザが期限切れの認証情報を使用できる日数を指定します。

認証情報の自動ロック解除を有効化

認証情報が、次のフィールドに指定した時間の後に自動的にロック解除されるようにする場合は、このオプションを選択にします。

このフィールドは、［認証情報ロックアウト］フィールドで対応する値を指定する場合のみ有効です。

注: 認証情報は、ロック解除期間の後に自動的にロック解除されません。 認証情報をロック解除するには、ロック解除期間の後に認証に使用して成功させる必要があります。

ロック解除までの時間

ロックされた認証情報が認証に再使用できるようになるまでの時間数を指定します。

代替処理オプション

代替処理オプション

CA Strong Authentication サーバはプロキシとして機能し、以下の条件に基づいて、認証リクエストをほかの認証サーバへ渡します。

- 見つからないユーザ： 認証しようとするユーザが CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。
- 見つからない認証情報: ユーザが認証に使用しようとしている認証情報が CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。

この機能を有効にする方法の詳細については、「RADIUS プロキシサーバとしての CA Strong Authentication の設定」を参照してください。

複数認証情報オプション

検証用の使用タイプ

ユーザが特定の OTP 認証情報を使用して認証する場合は、このフィールドにその使用タイプの名前を入力します。

使用タイプを指定しないと、デフォルトの OTP 認証ポリシーで指定された使用タイプが使用されます。

7. ［保存］をクリックします。
8. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ（P. 72）」を参照してください。

OATH OTP 設定の設定

このセクションでは、以下の手順について説明します。

- OATH OTP 発行プロファイルの設定（P. 135）
- OATH OTP 認証ポリシーの設定（P. 138）
- OATH OTP トークンの管理（P. 143）

OATH OTP 発行プロファイルの設定

OATH ワンタイム パスワード（OATH OTP トークン）認証情報に関連する以下の属性を指定するために OATH OTP プロファイルを使用できます。

- **有効期間**： OATH OTP トークン が有効な期間です。

OATH OTP トークン プロファイルを設定し、それを 1 つ以上の組織に割り当てることによって、それらの組織のユーザに発行される OATH OTP 認証情報の特性を制御できます。OATH OTP トークン 認証情報プロファイルを作成するには、［OATH OTP プロファイル］ページを使用します。

次の手順に従ってください:

1. メイン メニューの［**サービスおよびサーバの設定**］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［**OATH OTP トークン**］セクションの［発行］リンクをクリックすると、［OATH ワンタイム パスワード プロファイル］ページが表示されます。
4. 必要に応じて、［**プロファイル設定**］セクションのフィールドに入力します。

   プロファイル設定

   作成

   新規プロファイルを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規プロファイルの設定名を指定します。

   更新

   既存のプロファイルを更新するには、表示される［設定の選択］リストから更新するプロファイルを選択します。

   設定のコピー

   既存のプロファイルから設定をコピーしてプロファイルを作成する場合は、このオプションを有効にします。

   注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするプロファイルを選択します。

有効期間の開始日

発行された OATH OTP トークン 認証情報が有効になる日付を設定します。

有効期間は、この認証情報が作成された日付から開始することも、カスタムの日付を指定することもできます。

有効期間の終了日

OATH OTP トークン が期限切れになる日付を設定します。

期限切れになる日付を設定するには、以下のオプションのいずれかを選択できます。

- 期間の指定
- カスタム日付の指定
- OATH OTP トークン が期限切れにならないようにするには、［無期限にする］オプションを選択します。

5. ［+］記号をクリックして［**詳細設定**］セクションを展開します。
6. ［**カスタム属性**］セクションで、**名前**と**値**のペアの形式で追加情報を指定します。 たとえば、プラグインで使用できる組織情報などです。
7. ［**ユーザ検証**］セクションで以下を設定します。
   - 現在の認証情報に関する以下の操作に対するユーザ ステータスを確認するには、［**アクティブなユーザ**］チェック ボックスをオンにします。
     - 認証情報の作成
     - 認証情報の再発行
     - 認証情報のリセット
     - 認証情報の有効期間のリセット

- ユーザ属性が特定の値と一致するかどうか確認する場合は、［**ユーザ属性**］オプションを選択します。 以下のユーザ属性に対する値を設定できます。
  - ユーザが作成された日付
  - ユーザ詳細が変更された日付
  - 電子メール アドレス
  - First name
  - ミドル ネーム
  - Last name
  - ユーザ ステータス
  - 電話番号
  - 一意のユーザ識別子

  注: ユーザ属性確認機能は、組織レベルで設定を実行している場合にのみ利用可能です。

8. ［**複数認証情報オプション**］セクションで、［**使用タイプ**］フィールドに OATH OTP トークン を使用する目的を識別するための説明を入力します。 たとえば、ユーザは、ネットワークへのリモート ログインを実行するために一時認証情報を持つことができます。 この認証情報用の使用タイプは「*temporary*」とすることができます。
9. ［**保存**］をクリックします。
10. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。 手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

OATH OTP 認証ポリシーの設定

OATH OTP トークン ベースの認証に関連する以下の属性を指定するために OATH OTP 認証ポリシーを使用できます。

- **ユーザ ステータス**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。

  注: ユーザ ステータスの確認を有効にすると、非アクティブ状態のユーザの認証は失敗します。

- **ロックアウトの条件：** 許可される試行の失敗数です。この数を超えると、ユーザの認証情報がロックされます。
- **ロック解除の条件：** ロックされた認証情報が再使用できるようになるまでの時間数です。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［OATH OTP トークン］セクションの［認証］リンクをクリックすると、［OATH OTP トークン 認証ポリシー］ページが表示されます。
4. 必要に応じて、［ポリシー設定］セクションのフィールドに入力します。

   ポリシー設定

   作成

   新規ポリシーを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規ポリシーの設定名を指定します。

更新

既存のポリシーを更新する場合は、表示される［設定の選択］リストから更新するポリシーを選択します。

設定のコピー

既存のポリシーから設定をコピーしてポリシーを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするポリシーを選択します。

認証ルック アヘッド数

ユーザが入力した OATH OTP を確認するために、CA Strong Authentication サーバの OATH OTP カウンタが増加される回数を指定します。ユーザが入力した OATH OTP は、現在のカウント - 認証ルック バック数 ～ 現在のカウント + 認証ルック アヘッド数の範囲でサーバ上で生成されるすべての OATH OTP と比較され、ユーザが入力した OATH OTP-EMV が一致した場合、そのユーザは認証されます。

注: クライアントとサーバの OATH OTP が一致する場合、そのカウントはサーバ上の現在のカウントとして設定されます。

認証ルック バック数

ユーザが入力した OATH OTP を確認するために、CA Strong Authentication サーバの OATH OTP カウンタが減少される回数を指定します。

ユーザが入力した OATH OTP は、現在のカウント - 認証ルック バック数 ～ 現在のカウント + 認証ルック アヘッド数の範囲でサーバ上で生成されるすべての OATH OTP と比較され、ユーザが入力した OATH OTP-EMV が一致した場合、そのユーザは認証されます。

注: クライアントとサーバの OATH OTP が一致する場合、そのカウントはサーバ上の現在のカウントとして設定されます。

同期ルック アヘッド数

クライアント デバイス上の OATH OTP カウンタと同期するために、CA Strong Authentication サーバ上の OATH OTP カウンタが増加される回数を指定します。

クライアントとサーバの OATH OTP が同期を取るために、ユーザが 2 つの連続した OATH OTP を提供する必要があります。これらの OATH OTP が、検索範囲（カウント - 同期ルック バック数 ～ 現在のカウント + 同期ルック アヘッド数）にあるサーバの連続した OATH OTP と一致する場合、サーバのカウンタは、ユーザが入力した 2 番目の OATH OTP に対応するカウントに同期されます。

同期ルック バック数

クライアント デバイス上の OATH OTP カウンタと同期するために、CA Strong Authentication サーバ上の OATH OTP カウンタが減少される回数を指定します。

クライアントとサーバの OATH OTP が同期を取るために、ユーザが 2 つの連続した OATH OTP を提供する必要があります。これらの OATH OTP が、検索範囲（カウント - 同期ルック バック数 ～ 現在のカウント + 同期ルック アヘッド数）にあるサーバの連続した OATH OTP と一致する場合、サーバのカウンタは、ユーザが入力した 2 番目の OATH OTP に対応するカウントに同期されます。

認証情報ロックアウト

失敗した試行の数を指定します。この数を超えると、OATH OTP がロックされます。

認証前にユーザ ステータスを確認

認証の前にユーザのステータスがアクティブかどうかを確認する場合は、このオプションを選択します。

5. ［+］記号をクリックして［**詳細設定**］セクションを展開します。
6. 必要に応じて、このセクションのフィールドに入力します。

詳細設定

警告を発行

ユーザの認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

期限切れ認証によるログイン猶予日数

正常にログインするためにユーザが期限切れの認証情報を使用できる日数を指定します。

認証情報の自動ロック解除を有効化

認証情報が、次のフィールドに指定した時間の後に自動的にロック解除されるようにする場合は、このオプションを選択にします。

このフィールドは、［認証情報ロックアウト］フィールドで対応する値を指定する場合のみ有効です。

注: 認証情報は、ロック解除期間の後に自動的にロック解除されません。 認証情報をロック解除するには、ロック解除期間の後に認証に使用して成功させる必要があります。

ロック解除までの時間

ロックされた認証情報が認証に再使用できるようになるまでの時間数を指定します。

代替処理オプション

CA Strong Authentication サーバ はプロキシとして機能し、以下の条件に基づいて、認証リクエストをほかの認証サーバへ渡します。

- 見つからないユーザ： 認証しようとするユーザが CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。
- 見つからない認証情報: ユーザが認証に使用しようとしている認証情報が CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。

この機能を有効にする方法の詳細については、「RADIUS プロキシサーバとしての CA Strong Authentication の設定」を参照してください。

検証用の使用タイプ

ユーザが特定の OATH OTP 認証情報を使用して認証する場合は、このフィールドにその使用タイプの名前を入力します。

使用タイプを指定しないと、デフォルトの OATH OTP 認証ポリシーで指定された使用タイプが使用されます。

7. ［保存］をクリックします。
8. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

OATH OTP トークンの管理

管理コンソールを使用して、OATH トークンをバルク アップロードしたり、グローバル レベルまたは組織レベルで割り当てられている OATH トークンを一括して取得したりすることができます。

このセクションでは、以下の手順について説明します。

- OATH OTP トークンの取得
- OATH OTP トークンのアップロード

OATH OTP トークンの取得

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［OATH OTP］セクションの［トークン管理］リンクをクリックすると、［OATH OTP トークン管理］ページが表示されます。
4. 必要に応じて、［OATH トークンの取得］セクションのフィールドに入力します。

   トークン ステータス

   ステータスを選択してトークンを取得します。 以下のステータスを指定できます。

   - 空き: トークンがユーザに割り当てられていないことを示します。
   - 割り当て済み: トークンがユーザに割り当てられていることを示します。
   - 放棄: トークンが割り当てられたユーザが、現在ではトークンとの関連付けがなくなったことを示します。

     たとえば、新しいトークンを取得した従業員、または組織を退職した従業員などが該当します。

     放棄されたトークンは、別のユーザに割り当てることができます。
   - 失敗: アップロード操作に失敗したトークンを示します。

   一括請求 ID

OATH トークンが作成されたバッチを示す識別子です。

トークン ID

トークンの一意の識別子を指定します。

検索条件にワイルドカード文字を含めることもできます。たとえば、アスタリスク（*）、ピリオド（.）、バックスラッシュ（¥）などです。 以下の例で説明するような文字を使用できます。

データベースに以下のようなトークンがある場合を考えます。

- 12
- 123
- 1234
- 123*4

トークン ID として「12*」と入力すると、上記のトークンがすべて取得されます。 トークン ID として「12.」と入力すると、トークン 123 が取得されます。「123¥*4」と入力すると、トークン 123*4 が取得されます。

グローバル レベルで使用可能なフェッチ トークン

グローバル レベルで割り当てられているトークンを取得する場合は、このオプションを選択します。

組織に割り当てられたフェッチ トークン

トークンが割り当てられている組織を選択します。 選択した組織に割り当てられているトークンが取得されます。

5. ［**取得**］をクリックして、トークンを取得します。

OATH OTP トークンのアップロード

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［OATH OTP］セクションの［トークン管理］リンクをクリックすると、［OATH OTP トークン管理］ページが表示されます。
4. OATH OTP トークンが含まれる XML ファイルに対応する［参照］ボタンをクリックして、CA Strong Authentication サーバによって発行される必要がある OTP 用のキー コンテナを定義する XML ファイルをアップロードします。

   注: CA Strong Authentication には、OATH トークンをユーザにアップロードするためのサンプル XML ファイルとして、oath-token-upload.xml が用意されています。 このファイルによって、事前定義済みユーザ用の OATH トークンを作成します。 これは以下の場所にあります。

   Windows の場合: *<install_location>*¥Arcot Systems¥samples¥xml¥webfort

   UNIX の場合: *<install_location>*/arcot/samples/xml/webfort
5. ［アップロード］をクリックします。

ArcotID OTP（OATH 準拠）の設定

CA Auth ID OTP（OATH 準拠）発行プロファイルの設定

CA Auth ID OTP-OATH プロファイルは、OATH 標準に準拠している CA Auth ID OTP に関連する以下の属性を指定するために指定できます。

- **長さ**： CA Auth ID OTP の長さです。
- **有効期間**： CA Auth ID OTP が有効な期間です。

CA Auth ID OTP-OATH プロファイルを設定し、それを 1 つ以上の組織に割り当てることによって、それらの組織のユーザに発行される CA Auth ID OTP 認証情報の特性を制御できます。 CA MobileOTP 認証情報プロファイルを作成するには、［CA MobileOTP プロファイル］ページを使用します。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［ArcotOTP-OATH］セクションの［発行］リンクをクリックすると、［ArcotOTP-OATH プロファイル名］ページが表示されます。
4. 必要に応じて、［プロファイル設定］セクションのフィールドに入力します。

   作成

   新規プロファイルを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規プロファイルの設定名を指定します。

   更新

   既存のプロファイルを更新する場合は、表示される［設定の選択］リストから更新するプロファイルを選択します。

   設定のコピー

   既存のプロファイルから設定をコピーしてプロファイルを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするプロファイルを選択します。

トークン タイプ

ユーザのために作成される必要がある CA Auth ID OTP のタイプを選択します。 HOTP はカウンタ ベースのトークンであり、TOTP は時間ベースのトークンです。

長さ

CA Auth ID OTP の長さを設定します。

CA Auth ID OTP の最小長は 6（デフォルト値でもあります）であり、最大長は 8 文字です。

タイム ステップ

クライアントによって生成された OTP が、サーバによって生成された OTP と同じである期間（秒単位）。 このタイム ステップが長いほど、2 つの OTP が長い期間一致するようになります。つまり、このタイム ステップが長いほど、クライアントからの OTP の受信の遅延に対応できます。

1 から 300 までの任意の値を入力できます。 デフォルト値は 30 です。

注: このオプションは OTP ベースの CA Auth ID OTP にのみ適用可能です。

ロゴ URL

ロゴが含まれる URL を入力します。ロゴは、CA Strong Authentication により保護されたアプリケーションの認証を受けるために CA Auth ID OTP を使用するユーザのクライアント デバイス上に表示されます。

表示名

クライアント デバイス上に CA Auth ID OTP を表示するために使用される名前を入力します。 固定文字列を入力することもできますし、または以下のユーザ変数を「$$(<変数>)$$」として渡すこともできます。

- ユーザ名（userName）
- 組織名（orgName）

- 認証情報のカスタム属性
- ユーザのカスタム属性

有効期間の開始日

発行された CA Auth ID OTP 認証情報が有効になる日付を設定します。

有効期間は、この認証情報が作成された日付から開始することも、カスタムの日付を指定することもできます。

有効期間の終了日

CA Auth ID OTP が期限切れになる日付を設定します。

期限切れになる日付を設定するには、以下のオプションのいずれかを選択できます。

- 期間の指定
- カスタム日付の指定
- CA Auth ID OTP が期限切れにならないようにするには、［無期限にする］オプションを選択します。

5. ［**+**］記号をクリックして［**詳細設定**］セクションを展開します。
6. ［**カスタム属性**］セクションで、**名前**と**値**のペアの形式で追加情報を指定します。 たとえば、プラグインで使用できる組織情報などです。
7. ［**カスタム カード属性**］セクションで、CA Auth ID OTP-OATH カードに追加するその他の情報を指定します。 これらのカスタム属性はカード文字列の一部として利用できます。
8. ［**ユーザ検証**］セクションで以下を設定します。
   - 現在の認証情報に関する以下の操作に対するユーザ ステータスを確認するには、［**アクティブなユーザ**］チェック ボックスをオンにします。
     - 認証情報の作成
     - 認証情報の再発行
     - 認証情報のリセット
     - 認証情報の有効期間のリセット
   - ユーザ属性が特定の値と一致するかどうか確認する場合は、［**ユーザ属性**］オプションを選択します。 以下のユーザ属性に対する値を設定できます。

- ユーザが作成された日付
- ユーザ詳細が変更された日付
- 電子メール アドレス
- First name
- ミドル ネーム
- Last name
- ユーザ ステータス
- 電話番号
- 一意のユーザ識別子

注: ユーザ属性確認機能は、組織レベルで設定を実行している場合にのみ利用可能です。

9. ［**複数認証情報オプション**］セクションで、［**使用タイプ**］フィールドに CA Auth ID OTP を使用する目的を識別するための説明を入力します。たとえば、ユーザは、ネットワークへのリモート ログインを実行するために一時認証情報を持つことができます。この認証情報用の使用タイプは「*temporary*」とすることができます。
10. ［**保存**］をクリックし、ArcotID OTP プロファイルを作成または更新します。
11. 展開された CA Strong Authentication インスタンスをすべてリフレッシュします。この方法の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

CA Auth ID OTP（OATH 準拠）認証ポリシーの設定

CA Auth ID OTP-OATH ポリシーは、OATH に準拠している CA Auth ID OTP の以下の認証関連の属性を指定するために使用できます。

- **ユーザ ステータス**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。

  注: ユーザ ステータスの確認を有効にすると、非アクティブ状態のユーザの認証は失敗します。

- **ロックアウトの条件：** 許可される試行の失敗数です。この数を超えると、ユーザの認証情報がロックされます。
- **ロック解除の条件：** ロックされた認証情報が再使用できるようになるまでの時間数です。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［ArcotOTP-OATH］セクションの［認証］リンクをクリックすると、［ArcotOTP-OATH 認証ポリシー名］ページが表示されます。

4. 必要に応じて、［ポリシー設定］セクションのフィールドに入力します。

作成

新規ポリシーを作成する場合は、以下の手順に従います。

- ［作成］オプションを選択します。
- 表示されるフィールドに、新規ポリシーの設定名を指定します。

更新

既存のポリシーを更新する場合は、表示される［設定の選択］リストから更新するポリシーを選択します。

設定のコピー

既存のポリシーから設定をコピーしてポリシーを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするポリシーを選択します。

認証ルック アヘッド数

ユーザが入力した CA Auth ID OTP を確認するために、CA Strong Authentication サーバの CA Auth ID OTP カウンタが増加される回数を入力します。 ユーザが入力した CA Auth ID OTP は、現在のカウント - 認証ルック バック数 ～ 現在のカウント + 認証ルック アヘッド数の範囲でサーバ上で生成されるすべての CA Auth ID OTP と比較され、ユーザが入力した CA Auth ID OTP が一致した場合、そのユーザは認証されます。

注: クライアントとサーバの CA Auth ID OTP が一致する場合、そのカウントはサーバ上の現在のカウントとして設定されます。

認証ルック バック数

ユーザが入力した CA Auth ID OTP を確認するために、CA Strong Authentication サーバの CA Auth ID OTP カウンタが減少される回数を入力します。

ユーザが入力した CA Auth ID OTP は、現在のカウント - 認証ルック バック数 ～ 現在のカウント + 認証ルック アヘッド数の範囲でサーバ上で生成されるすべての CA Auth ID OTP と比較され、ユーザが入力した CA Auth ID OTP が一致した場合、そのユーザは認証されます。

注: クライアントとサーバの CA Auth ID OTP が一致する場合、そのカウントはサーバ上の現在のカウントとして設定されます。

同期ルック アヘッド数

クライアント デバイス上の CA Auth ID OTP カウンタと同期するために、CA Strong Authentication サーバ上の CA Auth ID OTP カウンタが増加される回数を入力します。

クライアントとサーバの CA Auth ID OTP が同期を取るために、ユーザが 2 つの連続した CA Auth ID OTP を提供する必要があります。これらの CA Auth ID OTP が、検索範囲（カウント - 同期ルック バック数 ～ 現在のカウント + 同期ルック アヘッド数）にあるサーバの連続した CA Auth ID OTP と一致する場合、サーバのカウンタは、ユーザが入力した 2 番目の CA Auth ID OTP に対応するカウントに同期されます。

同期ルック バック数

クライアント デバイス上の CA Auth ID OTP カウンタと同期するために、CA Strong Authentication サーバ上の CA Auth ID OTP カウンタが減少される回数を入力します。

クライアントとサーバの CA Auth ID OTP が同期を取るために、ユーザが 2 つの連続した CA Auth ID OTP を提供する必要があります。これらの CA Auth ID OTP が、検索範囲（カウント - 同期ルック バック数 ～ 現在のカウント + 同期ルック アヘッド数）にあるサーバの連続した CA Auth ID OTP と一致する場合、サーバのカウンタは、ユーザが入力した 2 番目の CA Auth ID OTP に対応するカウントに同期されます。

認証情報ロックアウト

失敗した試行の数を指定します。この数を超えると、CA Auth ID OTP がロックされます。

認証前にユーザ ステータスを確認

認証の前にユーザのステータスがアクティブかどうかを確認する場合は、このオプションを選択します。

5. ［+］記号をクリックして［**詳細設定**］セクションを展開します。
6. 必要に応じて、このセクションのフィールドに入力します。

警告を発行

ユーザの認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

期限切れ認証によるログイン猶予日数

正常にログインするためにユーザが期限切れの認証情報を使用できる日数を指定します。

認証情報の自動ロック解除を有効化

認証情報が、次のフィールドに指定した時間の後に自動的にロック解除されるようにする場合は、このオプションを選択にします。

このフィールドは、［認証情報ロックアウト］フィールドで対応する値を指定する場合のみ有効です。

注: 認証情報は、ロック解除期間の後に自動的にロック解除されません。 認証情報をロック解除するには、ロック解除期間の後に認証に使用して成功させる必要があります。

ロック解除までの時間

ロックされた認証情報が認証に再使用できるようになるまでの時間数を指定します。

代替処理オプション

CA Advanced Authentication サーバはプロキシとして機能し、以下の条件に基づいて、認証リクエストをほかの認証サーバへ渡します。

- 見つからないユーザ： 認証しようとするユーザが CA Advanced Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。
- 見つからない認証情報: ユーザが認証に使用しようとしている認証情報が CA Advanced Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。

この機能を有効にする方法の詳細については、「RADIUS プロキシサーバとしての CA Strong Authentication の設定」を参照してください。

複数認証情報オプション

検証用の使用タイプ

ユーザが特定の CA Auth ID OTP 認証情報を使用して認証する場合は、このフィールドにその使用タイプの名前を入力します。

使用タイプを指定しないと、デフォルトの CA Auth ID OTP 認証ポリシーで指定された使用タイプが使用されます。

7. ［保存］をクリックします。
8. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

ArcotID OTP（EMV 準拠）の設定

ArcotID OTP（EMV 準拠）発行プロファイルの設定

CA Auth ID OTP-EMV プロファイルは、EMV （Europay、MasterCard、VISA）プロトコルに準拠している CA Auth ID OTP に関連する以下の属性を指定するために使用できます。

- **有効期間**： CA Auth ID OTP-EMV が有効な期間です。

CA Auth ID OTP-EMV プロファイルを設定し、それを 1 つ以上の組織に割り当てることによって、それらの組織のユーザに発行される CA Auth ID OTP-EMV 認証情報の特性を制御できます。 CA Auth ID OTP-EMV 認証情報プロファイルを作成するには、［ArcotOTP-EMV プロファイル名］ページを使用します。

注: ArcotID OTP-EMV プロファイルを設定するには、まずアカウント タイプを作成する必要があります。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［ArcotOTP-EMV］セクションの［発行］リンクをクリックすると、［ArcotOTP-EMV プロファイル名］ページが表示されます。
4. 必要に応じて、［プロファイル設定］セクションのフィールドに入力します。

   作成

   新規プロファイルを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規プロファイルの設定名を指定します。

   更新

   既存のプロファイルを更新する場合は、表示される［設定の選択］リストから更新するプロファイルを選択します。

   設定のコピー

既存のプロファイルから設定をコピーしてプロファイルを作成する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするプロファイルを選択します。

アカウント タイプ

ArcotID OTP-EMV 認証情報の作成に使用する必要があるアカウントタイプを指定します。

PAN シーケンス用の属性

同じ PAN を持つ 2 つのカードを区別するのに役立つ PAN （Primary Account Number）のシーケンスを指定します。 たとえば、有効期限が切れた後に再発行されるカードには、同じ PAN が使用されますが、シーケンス番号は異なります。

PAN のシーケンスを追加するには、アカウント タイプを設定する際にカスタム属性を追加する必要があります。 「アカウント タイプの設定」を参照してください。

組織のユーザに PAN のシーケンスを割り当てるには、ユーザ アカウントを編集して、カスタム属性に値を追加する必要があります。「アカウント ID の作成」を参照してください。 この値はカード文字列に含められます。カスタム属性の値は必須ではありませんが、指定しない場合は 00 がデフォルトで使用されます。

ロゴ URL

ロゴが含まれる URL を入力します。ロゴは、CA Strong Authentication により保護されたアプリケーションの認証を受けるために EMV OTP を使用するクライアント デバイス上に表示されます。

表示名

クライアント デバイス上に EMV OTP を表示するために使用される名前を入力します。 固定文字列を入力することもできますし、または以下のユーザ変数を「$$(<変数>)$$」として渡すこともできます。

- ユーザ名（userName）
- 組織名（orgName）
- 認証情報のカスタム属性

- ユーザのカスタム属性

有効期間の開始日

発行された ArcotID OTP 認証情報が有効になる日付を設定します。

有効期間は、この認証情報が作成された日付から開始することも、カスタムの日付を指定することもできます。

有効期間の終了日

ArcotID OTP が期限切れになる日付を設定します。

期限切れになる日付を設定するには、以下のオプションのいずれかを選択できます。

- 期間の指定
- カスタム日付の指定
- ArcotID OTP が期限切れにならないようにするには、［無期限にする］オプションを選択します。

5. ［**+**］記号をクリックして［**詳細設定**］セクションを展開します。
6. ［**カスタム属性**］セクションで、**名前**と**値**のペアの形式で追加情報を指定します。 たとえば、プラグインで使用できる組織情報などです。
7. ［**カスタム カード属性**］セクションで、ArcotID OTP-EMV カードに追加するその他の情報を指定します。
8. ［**ユーザ検証**］セクションで以下を設定します。
   - 現在の認証情報に関する以下の操作に対するユーザ ステータスを確認するには、［**アクティブなユーザ**］チェック ボックスをオンにします。
     - 認証情報の作成
     - 認証情報の再発行
     - 認証情報のリセット
     - 認証情報の有効期間のリセット
   - ユーザ属性が特定の値と一致するかどうか確認する場合は、［**ユーザ属性**］オプションを選択します。 以下のユーザ属性に対する値を設定できます。
     - ユーザが作成された日付
     - ユーザ詳細が変更された日付
     - 電子メール アドレス

- First name
- ミドル ネーム
- Last name
- ユーザ ステータス
- 電話番号
- 一意のユーザ識別子

注: ユーザ属性確認機能は、組織レベルで設定を実行している場合にのみ利用可能です。

9. ［**複数認証情報オプション**］セクションで、［**使用タイプ**］フィールドに EMV OTP を使用する目的を識別するための説明を入力します。たとえば、ユーザは、ネットワークへのリモート ログインを実行するために一時認証情報を持つことができます。この認証情報用の使用タイプは「*temporary*」とすることができます。
10. ［**保存**］をクリックし、EMV OTP プロファイルを作成または更新します。
11. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

ArcotID OTP（EMV 準拠）認証ポリシーの設定

ArcotID OTP-EMV ポリシーを使用して、EMV に準拠している ArcotID OTP の以下の認証関連属性を定義できます。

- **ユーザ ステータス**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。

  注: ユーザ ステータスの確認を有効にすると、非アクティブ状態のユーザの認証は失敗します。

- **ロックアウトの条件：** 許可される試行の失敗数です。この数を超えると、ユーザの認証情報がロックされます。
- **ロック解除の条件：** ロックされた認証情報が再使用できるようになるまでの時間数です。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［ArcotOTP-EMV］セクションの［認証］リンクをクリックすると、［ArcotOTP-EMV 認証ポリシー名］ページが表示されます。
4. 必要に応じて、［ポリシー設定］セクションのフィールドに入力します。

   作成

   新規ポリシーを作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新規ポリシーの設定名を指定します。

   更新

   既存のポリシーを更新する場合は、表示される［設定の選択］リストから更新するポリシーを選択します。

   設定のコピー

   既存のポリシーから設定をコピーしてポリシーを作成する場合は、このオプションを有効にします。

   注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーするポリシーを選択します。

認証ルック アヘッド数

ユーザが入力した ArcotID OTP-EMV を確認するために、CA Strong Authentication サーバの ArcotID OTP-EMV カウンタが増加される回数を入力します。ユーザが入力した ArcotID OTP-EMV は、現在のカウント - 認証ルック バック数 ～ 現在のカウント + 認証ルック アヘッド数の範囲でサーバ上で生成されるすべての ArcotID OTP-EMV と比較され、ユーザが入力した ArcotID OTP-EMV が一致した場合、そのユーザは認証されます。

注: クライアントとサーバの ArcotID OTP-EMV が一致する場合、そのカウントはサーバ上の現在のカウントとして設定されます。

認証ルック バック数

ユーザが入力した ArcotID OTP-EMV を確認するために、CA Strong Authentication サーバの ArcotID OTP-EMV カウンタが減少される回数を入力します。

ユーザが入力した ArcotID OTP-EMV は、現在のカウント - 認証ルック バック数 ～ 現在のカウント + 認証ルック アヘッド数の範囲でサーバ上で生成されるすべての ArcotID OTP-EMV と比較され、ユーザが入力した ArcotID OTP-EMV が一致した場合、そのユーザは認証されます。

注: クライアントとサーバの ArcotID OTP-EMV が一致する場合、そのカウントはサーバ上の現在のカウントとして設定されます。

同期ルック アヘッド数

クライアント デバイス上の ArcotID OTP-EMV カウンタと同期するために、CA Strong Authentication サーバ上の ArcotID OTP-EMV カウンタが増加される回数を入力します。

クライアントとサーバの ArcotID OTP が同期を取るために、ユーザが 2 つの連続した ArcotID OTP を提供する必要があります。これらの ArcotID OTP が、検索範囲（カウント - 同期ルック バック数 ～ 現在のカウント + 同期ルック アヘッド数）にあるサーバの連続した ArcotID OTP と一致する場合、サーバのカウンタは、ユーザが入力した 2 番目の ArcotID OTP-EMV に対応するカウントに同期されます。

同期ルック バック数

クライアント デバイス上の ArcotID OTP-EMV カウンタと同期するために、CA Strong Authentication サーバ上の ArcotID OTP-EMV カウンタが減少される回数を入力します。

クライアントとサーバの ArcotID OTP が同期を取るために、ユーザが 2 つの連続した ArcotID OTP を提供する必要があります。これらの ArcotID OTP が、検索範囲（カウント - 同期ルック バック数 ～ 現在のカウント + 同期ルック アヘッド数）にあるサーバの連続した ArcotID OTP と一致する場合、サーバのカウンタは、ユーザが入力した 2 番目の ArcotID OTP-EMV に対応するカウントに同期されます。

認証情報ロックアウト

失敗した試行の数を指定します。この数を超えると、ArcotID OTP-EMV がロックされます。

認証前にユーザ ステータスを確認

認証の前にユーザのステータスがアクティブかどうかを確認する場合は、このオプションを選択します。

5. ［**+**］記号をクリックして［**詳細設定**］セクションを展開します。
6. 必要に応じて、このセクションのフィールドに入力します。

警告を発行

ユーザの認証情報の有効期間の残り日数がこの日数より少なくなると、呼び出し元のアプリケーションに終了が近づいていることを通知する警告が送信されます。

期限切れ認証によるログイン猶予日数

正常にログインするためにユーザが期限切れの認証情報を使用できる日数を指定します。

認証情報の自動ロック解除を有効化

認証情報が、次のフィールドに指定した時間の後に自動的にロック解除されるようにする場合は、このオプションを選択にします。

このフィールドは、［認証情報ロックアウト］フィールドで対応する値を指定する場合のみ有効です。

注: 認証情報は、ロック解除期間の後に自動的にロック解除されません。 認証情報をロック解除するには、ロック解除期間の後に認証に使用して成功させる必要があります。

ロック解除までの時間

ロックされた認証情報が認証に再使用できるようになるまでの時間数を指定します。

代替処理オプション

CA Strong Authentication サーバはプロキシとして機能し、以下の条件に基づいて、認証リクエストをほかの認証サーバへ渡します。

- 見つからないユーザ： 認証しようとするユーザが CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。
- 見つからない認証情報: ユーザが認証に使用しようとしている認証情報が CA Strong Authentication データベースに存在しない場合、リクエストはほかのサーバに渡されます。

この機能を有効にする方法の詳細については、「RADIUS プロキシサーバとしての CA Strong Authentication の設定」を参照してください。

検証用の使用タイプ

ユーザが特定の ArcotID OTP-EMV 認証情報を使用して認証する場合は、このフィールドにその使用タイプの名前を入力します。

使用タイプを指定しないと、デフォルトの ArcotID OTP-EMV 認証ポリシーで指定された使用タイプが使用されます。

7. ［保存］をクリックします

展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

認証情報管理キーの設定

キーは、認証情報を生成および認証するために使用される共有秘密キーを保護するために使用できます。認証情報には、CA Auth ID PKI、OATH OTP、CA Auth ID OTP-OATH、および CA Auth ID OTP-EMV が含まれます。 ArcotID PKI の作成および管理に使用されるキーは、 *ドメイン キー*と呼ばれます。他の認証情報を作成および管理するために使用されるキーは*マスタ キー*と呼ばれます。

ユーザが自身の認証情報を使用して認証しようとすると、CA Strong Authentication は認証情報を保護するために正しいキーが使用されているかどうかを最初に確認します。 キーが有効であれば、ユーザは正しい認証情報を提示して認証されます。 そうでない場合、ユーザ認証は失敗します。

デフォルトでは、CA Strong Authentication サーバ が初めて起動されるときにキー設定が作成されます。このデフォルト設定を使用することも、［認証情報キー管理］ページを使用して独自の設定を作成することもできます。ユーザは複数のキー設定を作成できます。ただし、認証情報の作成およびそれらの設定の認証に使用するのは、認証情報 タイプに割り当てられた設定のみです。 その他のアクティブな設定は認証にのみ使用されます。

このセクションでは、以下の手順について説明します。

- キーの作成（P. 165）
- キーの有効期間の更新（P. 166）
- キーの廃棄（P. 168）

キーの作成

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［キー管理］セクションの［認証情報キー管理］リンクをクリックすると、［認証キー管理設定］ページが表示されます。
4. ［作成］ボタンをクリックして、［キーのセットアップ］ページを表示します。
5. ［設定名］フィールドにキー設定の名前を指定します。
6. キーを格納するために使用するラベルを［キー ラベル］フィールドに指定します。
7. ハードウェア セキュリティ モジュール（HSM）にキーを格納する場合は、［HSM 内のキー］オプションを選択します。

   注:［確認］ボタンを使用すると、キー ラベルが HSM に存在することを確認できます。 このボタンは、［HSM 内のキー］チェック ボックスを選択したときにのみ有効になります。
8. ［有効期間の終了日］フィールドにキーの有効期間を設定します。キーの有効期間を指定することもできますし、特定の日付を指定することもできます。
9. ［作成］をクリックしてキーを作成します。

   注: キー設定を作成した後、［デフォルト設定の割り当て］ページを使用して、この設定を認証情報に割り当てます。 詳細については、「RADIUS のための CA Strong Authentication の設定 (P. 172)」を参照してください。

キーの有効期間の更新

キーの有効期間を更新できます。 キーが期限切れになると、そのキーで発行された認証情報は有効でなくなります。 新しい認証情報を作成し、ユーザに発行する必要があります。 キーの有効期間を延長すると、新しいキーで認証情報を再度作成してユーザに配布する必要がなくなります。

キーがすでに期限切れになった場合も、期限切れになったキーの有効期間を延長し、既存の認証情報を継続して使用できます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［キー管理］セクションの［認証情報キー管理］リンクをクリックすると、［認証キー管理設定］ページが表示されます。
4. アクティブなキーまたは期限切れになったキーを更新できます。
   - アクティブなキーを更新する方法

     ［アクティブな設定］セクションで、有効期間を延長させたいキーの［<設定名>］リンクをクリックします。
   - 期限切れになったキーを更新する方法

     ［廃棄および期限切れ設定］セクションで、有効期間を延長させたい期限切れになったキーの［<設定名>］リンクをクリックします。

     ［認証キー管理設定］ページが表示されます。
5. ［更新］オプションを選択します。
6. ［有効期間の終了日］フィールドにキーの新しい有効期間を設定します。 キーの有効期間を指定することもできますし、特定の日付を指定することもできます。
7. ［更新］をクリックします。

キーの廃棄

キーの*廃棄*または取り消しとは、この操作の後にキーが無効になり、そのキーと関連付けられている認証情報が期限切れになることを意味します。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［キー管理］セクションの［認証情報キー管理］リンクをクリックすると、［認証キー管理設定］ページが表示されます。
4. アクティブなキーまたは期限切れになったキーを廃棄できます。
   - アクティブなキーを廃棄する方法

     ［アクティブな設定］セクションで、有効期間を延長させたいキーの［<設定名>］リンクをクリックします。
   - 期限切れになったキーを廃棄する方法

     ［廃棄および期限切れ設定］セクションで、有効期間を延長させたい期限切れになったキーの［<設定名>］リンクをクリックします。

   ［認証キー管理設定］ページが表示されます。
5. ［廃棄］オプションを選択します。
6. ［廃棄］をクリックします。

SAML トークンの設定

認証に成功すると、CA Strong Authentication から認証トークンが返されます。 CA Strong Authentication はいくつかのタイプの認証トークンをサポートしています。これには、（ネイティブ、OTT、およびカスタム トークン タイプに加えて）*SAML*（Secure Assertion Markup Language）トークンも含まれます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［SAML］で、［SAML トークン設定］リンクをクリックして［SAML トークン設定］ページを表示します。
4. 以下のいずれかのオプションを選択します。
   - 設定を作成する場合は、［設定名］フィールドに設定名を入力します。
   - 既存の設定を更新する場合は、更新する設定を［設定の選択］リストから選択します。
5. ハードウェア セキュリティ モジュール（HSM）で SAML アサーションの署名に使用するキーを格納する場合は、［HSM 内の SAML 署名キー］オプションを選択します。 それ以外の場合、キーはデータベースに格納されます。
6. （HSM のみ）［SAML 署名証明書チェーン（PEM 形式）］フィールドに対応する［参照］ボタンをクリックして、CA Strong Authentication サーバが SAML トークンの発行に使用する証明書をアップロードします。
7. ［SAML 署名キー ペアを含む P12 ファイル］フィールドに対応する［参照］ボタンをクリックして、CA Strong Authentication サーバが SAML トークンの発行に使用する証明書が含まれる PKCS#12 ファイルをアップロードします。
8. ［P12 ファイル パスワード］フィールドに、PKCS#12 ファイルのパスワードを入力します。
9. ［ダイジェスト メソッド］フィールドに、SAML トークンのハッシュ操作に使用するアルゴリズム（SHA1、SHA256、SHA384、SHA512、RIPEMD 160 など）を指定します。

10. CA Strong Authentication で生成された SAML トークンを提供する発行者の名前を入力します。

    たとえば、XYZ 社が CA Strong Authentication を使って SAML トークンを生成する場合は、このフィールドに「XYZ」と入力します。

11. ［サブジェクト形式指定子（SAML 1.1）］フィールドに、SAML 1.1 の SAML サブジェクトのフォーマットを指定します。

12. ［サブジェクト形式指定子（SAML 2.0）］フィールドに、SAML 2.0 の SAML サブジェクトのフォーマットを指定します。

13. 認証時の SAML トークンの使用回数を 1 回のみにする場合は、［使い捨てトークン］オプションを有効にします。

14. ［認証トークン有効期間（秒）］フィールドに、SAML トークンを使用できる期間を入力します。

15. 必要に応じて、［追加トークン属性］セクションで SAML トークンの生成に関係するその他の属性を設定します。

    必要な場合は、［さらに追加］ボタンをクリックして属性を追加します。

16. ［オーディエンス］セクション（テーブル）に、SAML トークンを使用できるオーディエンスの詳細を入力します。

    さらにオーディエンスを追加する場合は、［さらに追加］をクリックします。

17. ［保存］ボタンをクリックして SAML トークンの設定を保存します。

18. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ（P. 72）」を参照してください。

ASSP の設定

ASSP（*Adobe 署名サービス プロトコル*）は、CA SignFort を使用して PDF ドキュメントに署名するために使用します。 署名の前に、CA Strong Authentication の認証方式を使用してユーザが認証されます。 認証に成功すると、SAML トークンがユーザに返されます。 その後、このトークンは SignFort サーバによって確認されます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［ASSP］で、［ASSP 設定］リンクをクリックして［ASSP 設定］ページを表示します。
4. 以下のいずれかのオプションを選択します。
   - 設定を作成する場合は、［設定名］フィールドに設定名を入力します。
   - 既存の設定を更新する場合は、更新する設定を［設定の選択］リストから選択します。
5. CA Auth ID PKI のローミング ダウンロードで CA Auth ID PKI をダウンロードするために使用する CA Auth ID ローミング URL を指定します。

   CA Auth ID PKI 認証では、現在のシステムにユーザの CA Auth ID PKI が存在しない場合に、CA Auth ID ローミング URL を使用して CA Strong Authentication サーバに対する認証が行われ、ユーザの CA Auth ID PKI がダウンロードされます。

6. ［有効化する認証メカニズム］で、署名の前にユーザを認証するために使用される認証方式を選択します。

   CA Auth ID 認証方式を有効にした場合は、CA Auth ID PKI のローミングダウンロードに Q&A 認証方式が使用されるので、QnA も選択する必要があります。

7. 前の手順で Kerberos 認証方式を有効にした場合は、［Kerberos 設定］セクションで Kerberos 認証に必要な以下のいずれかのパラメータを設定する必要があります。 以下の手順のいずれかを実行します。

   - CA Strong Authentication サーバ プロセスの Kerberos トークンを使用する場合は、［Windows ログオン認証情報を使用］オプションを選択します。
   - ［ユーザ名］、［パスワード］、［ドメイン名］フィールドに、Kerberos 認証用の新しい認証情報を指定します。

8. ［SAML］セクションで、以下の作業を実行します。

   a. ハードウェア セキュリティ モジュール（HSM）で SAML アサーションの署名に使用するキーを格納する場合は、［HSM 内の SAML 署名キー］オプションを選択します。これを行わない場合、キーはデータベースに格納されます。

   b. （HSM のみ）［参照］をクリックして、CA Strong Authentication サーバが SAML トークンの発行に使用する証明書をアップロードします。

   c. ［参照］をクリックして、CA Strong Authentication サーバが SAML トークンの発行に使用するキーおよび証明書が含まれる PKCS#12 ファイルをアップロードします。

   d. ［P12 ファイル パスワード］フィールドに、PKCS#12 ファイルのパスワードを入力します。

   e. ［発行者］フィールドに CA Strong Authentication サーバの URL を入力します。

   f. 認証時の SAML トークンの使用回数を 1 回のみにする場合は、［使い捨てトークン］オプションを有効にします。

   g. ［認証トークン有効期間（秒）］フィールドに、SAML トークンを使用できる期間を入力します。

   h. ［オーディエンス］テーブルに、SAML トークンを使用できるオーディエンスの詳細を入力します。

      オーディエンスを追加するには、［さらに追加］ボタンをクリックします。

9. ［保存］ボタンをクリックして ASSP 設定を保存します。
10. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。

    手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

RADIUS のための AuthMinder の設定

このセクションでは、以下の手順について説明します。

- RADIUS クライアントの設定（P. 172）
- RADIUS プロキシ サーバとしての CA Strong Authentication の設定（P. 177）

RADIUS クライアントの設定

設定された場合、CA Strong Authentication は、設定された NAS （Network Access Server）または RADIUS クライアントに対する RADIUS サーバの役割を果たすことができます。

RADIUS クライアントの追加

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［RADIUS］セクションの［RADIUS クライアント］をクリックすると、対応するページが表示されます。
4. ［追加］をクリックして、RADIUS クライアントのセット アップを行います。
5. それぞれのフィールドに以下の情報を入力または選択します。
   - **RADIUS クライアント IP アドレス**： ユーザが CA Strong Authentication サーバに認証される RADIUS クライアントの IP アドレスを指定します。
   - **共有秘密キー**： RADIUS クライアントと CA Strong Authentication サーバの間で共有される秘密キーを指定します。

     注: キーの最小長は *1* 文字で、最大長は *512* 文字です。
   - **説明**： RADIUS クライアントを説明する文字列を入力します。 複数のクライアントが設定される場合、この説明は RADIUS クライアントを識別するうえで役立ちます。
   - **認証タイプ**： VPN 認証のための認証メカニズムを選択します。
     - **RADIUS OTP**： RADIUS リクエストの認証に使用するデフォルト認証メカニズムです。

- **インバンド パスワード**： このオプションは以下のシナリオで使用します。
  認証情報 タイプを解決する
  認証情報タイプの解決を使用して設定された認証情報タイプでユーザを認証する場合（「認証情報タイプの解決 (P. 180)」を参照）。デフォルトでは、パスワード認証メカニズムが使用されます。
  （グローバル設定のみに適用されるオプション）組織名を指定する
  RADIUS リクエストでは、<orgname>¥n<password> 形式で組織情報とパスワードを送信できます。 CA Strong Authentication は、この形式で指定されたパスワードから組織名を抽出できます。この機能の使用を有効にするには、組織と RADIUS クライアントを以下のように関連付けます。

  a. ［>］ボタンを使用して、必要な組織を［利用可能な組織］リストから［サポートされている組織］リストに移動させます。

  b. RADIUS クライアントのデフォルト組織を指定します。 組織情報が RADIUS リクエストに示されていない場合、このデフォルト組織が認証でユーザ詳細を解決するために検証されます。

- **EAP**： このオプションは現在サポートされていません。 したがって、このオプションは選択しないでください。

6. ［**RADIUS 再試行処理**］セクションで、以下を指定します。
   - RADIUS クライアントでレスポンスが受信されない場合に CA Strong Authentication サーバにリクエストを送信するようにしたいときは、［再試行の有効化］オプションを選択します。
   - ［再試行ウィンドウ］フィールドで、クライアントがレスポンスが受信されない場合に CA Strong Authentication サーバへの接続を再試行できる期間を秒で入力します。 この期間が過ぎた後は、再試行は無効と見なされます。 再試行が可能な期間がクライアントのタイムアウト期間より長くなるようにします。
7. ［RADIUS レスポンス追加属性］セクションで、CA Strong Authentication サーバが RADIUS クライアントに送信するレスポンスに含めたい属性を指定します。
   - **属性 ID**： この列に一意の属性識別子を入力します。 たとえば、「26」などです。

- **属性値**： 属性 ID に対応する値を入力します。静的な値または変数を指定できます。たとえば、ユーザ属性またはカスタム属性、または静的な値と変数の組み合わせなどです。 たとえば、JSmith というユーザを考えます。カスタム ユーザ属性のキーと値のペアが「Employee ID=150」である場合、RADIUS レスポンスに従業員 ID が含まれるようにするには、以下のように指定します。

JSmith = $$Employee ID$$

これによって JSmith = 150 が返ります。

8. 属性を追加するには、［さらに追加］ボタンをクリックします。
9. ［RADIUS パケット ドロップ オプション］セクションで、CA Strong Authentication サーバ が RADIUS パケットを処理するべきでない場合のオプションを選択します。

   RADIUS パケットをドロップするためにサポートされているオプションを以下に示します。

   - 見つからないユーザ
   - 見つからない認証情報
   - 無効なリクエスト
   - 内部エラー
10. ［追加］をクリックして、新しい RADIUS クライアントを追加します。
11. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。手順の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

RADIUS クライアントの更新

次の手順に従ってください:

1. ［設定済み RADIUS クライアント］セクションで、更新するクライアントの IP アドレスを選択します。
2. 選択したクライアントの任意の列を更新し（詳細については、「RADIUS クライアントの設定」を参照）、［更新］をクリックします。
3. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

RADIUS クライアントの削除

次の手順に従ってください:

1. ［設定済み RADIUS クライアント］セクションで、削除するクライアントの IP アドレスを選択します。
2. ［Delete］をクリックします。
3. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

RADIUS プロキシ サーバとしての CA Strong Authentication の設定

CA Strong Authentication は、パスワード ベースの認証リクエストを RADIUS プロトコルが機能するほかのサーバに転送するプロキシ サーバとして設定できます。

注: ［代替処理オプション］セクションで、認証に使用されているポリシーに対して［ユーザが見つかりません］または［認証情報が見つかりません］が選択されていることを確認してください。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［RADIUS］セクションの［RADIUS プロキシ］をクリックすると、対応するページが表示されます。
4. ［プロキシの有効化］オプションを選択します。
5. グローバル レベルで利用可能な設定を使用する場合は、［グローバル設定の使用］オプションを選択します。

   注: このオプションは組織固有の設定を行っている場合のみ使用できます。
6. ［プライマリ プロキシ サーバ詳細］セクションで、リクエストを処理する RADIUS サーバの詳細を以下のように入力します。
   - **IP アドレス**： RADIUS サーバの IP アドレスを指定します。
   - **RADIUS ポート**： RADIUS サーバがリスンするポート番号を指定します。
   - **共有秘密キー**： RADIUS クライアントと RADIUS サーバの間で共有される秘密キーを定義します。

     注: キーの最小長は *1* 文字で、最大長は *512* 文字です。
   - **説明**： RADIUS サーバを説明する文字列を入力します。複数のサーバが設定されている場合、この説明は RADIUS サーバの識別に役立ちます。
   - **読み取りタイムアウト**： RADIUS サーバからのレスポンスを待機する最長時間をミリ秒で指定します。

- **再試行回数**：CA Strong Authentication サーバがレスポンスを受信しなかった場合に、RADIUS サーバへのリクエストの送信を試行する回数を指定します。

7. ［RADIUS レスポンス追加属性］セクションで、CA Strong Authentication サーバが RADIUS サーバに送信するリクエストに含めたい属性を指定します。

   属性 ID： この列に一意の属性識別子を入力します。 たとえば、「26」などです。

   属性値： 属性 ID に対応する値を入力します。 たとえば、属性 ID 26 に対応する値などです。

8. 属性を追加するには、［さらに追加］ボタンをクリックします。
9. 追加の RADIUS サーバを設定する場合は、［バックアップ プロキシ サーバ詳細］セクションにそのサーバの詳細を指定します。
10. ［更新］をクリックします。

プラグインの設定

マスタ管理者によって登録されたプラグイン（「プラグインの登録と更新 (P. 92)」を参照）は、（GA のみが） CA Strong Authentication サーバで動作するように設定する必要があります。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［拡張設定］で、［プラグイン設定］リンクをクリックして［プラグインの設定］ページを表示します。
4. ［名前］ドロップダウン リストから、設定するプラグインを選択します。

   この画面に表示される設定情報は、MA がプラグインの登録時にアップロードしたハンドラ ファイルから提供されます。
5. プラグイン設定の詳細を入力します。
6. プラグインによるサポートを望むイベントを選択します。
7. ［サブミット］ボタンをクリックすると、プラグインが設定され、変更が保存されます。
8. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。

   この方法の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

認証情報タイプの解決

CA Strong Authentication サーバに対する認証リクエストでは、リクエストの処理に使用する認証情報のタイプを指定する必要があります。 RADIUS および ASSP 認証リクエストの場合、入力リクエストでは認証情報のタイプを指定できません。そのため、デフォルトでは、RADIUS ユーザのワンタイム パスワードおよび ASSP ユーザのパスワード認証情報を認証に使用します。

RADIUS および ASSP でパスワード ベースの認証メカニズムをサポートする場合、または verifyPlain 認証機能を使用する場合は、*認証情報タイプの解決*の設定を作成する必要があります。 入力リクエストは、CA Strong Authentication がサポートする以下のパスワード タイプのいずれかにマップできます。

- Password
- ワンタイム パスワード
- OATH OTP
- CA Auth ID OTP-OATH
- CA Auth ID OTP-EMV
- RADIUS OTP
- LDAP パスワード
- ネイティブ トークン

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［その他の設定］セクションの［認証情報タイプ解決］リンクをクリックすると、対応するページが表示されます。
4. 必要に応じて、このセクションのフィールドに入力します。

   作成

   新しい設定を作成する場合は、以下の手順に従います。

   - ［作成］オプションを選択します。
   - 表示されるフィールドに、新しい設定の設定名を指定します。

更新

既存の設定を更新する場合は、［設定の選択］リストから更新する設定を選択します。

設定のコピー

既存の設定をコピーして設定を作成または更新する場合は、このオプションを有効にします。

注: スコープがあるほかの組織に属する設定からコピーすることもできます。

利用可能な設定

設定をコピーする設定を選択します。

プレーン解決先

受信するパスワード タイプの認証情報をマップする認証メカニズムを選択します。

認証情報タイプ用のユーザ カスタム属性

ユーザを認証するために使用する認証情報タイプを定義するユーザのカスタム属性。

注: ここで設定するユーザ属性は、ユーザ作成時にユーザに対して指定した属性と一致する必要があります。 FirstName、LastName、および TelNumber は使用できるユーザ属性の例です。

5. ［保存］をクリックします。

デフォルト設定の割り当て

必要な設定（認証情報プロファイル、認証ポリシー、ASSP、および SAML など）を作成した後、それらをグローバルに（GA として）または特定の組織（組織管理者）に割り当てる必要があります。 ユーザは、両方のレベルに設定を割り当てるために同じページを使用します。ただし、タスクページへのアクセスは異なります。

このセクションでは、グローバル レベルで設定を適用する方法について説明します。 組織への設定の割り当てについては、「組織固有の設定の管理 (P. 217)」を参照してください。

注: OA（組織管理者）が組織レベルのプロファイルおよびポリシーを指定しない場合、これらのプロファイルとポリシーがデフォルトで使用されます。 一方、GA または OA は組織レベルで個別のプロファイルおよびポリシーを適用し、グローバル設定よりも優先させることができます。

次の手順に従ってください:

1. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
2. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
3. ［設定の割り当て］セクションの［デフォルト設定の割り当て］リンクをクリックすると、対応するページが表示されます。
4. 対応するドロップダウン リストから使用する設定を選択します。

   このページを使用して、以下を割り当てることができます。

   - サポートされているすべての認証情報に対するプロファイルおよびポリシー
   - ArcotID に対するドメイン キー設定
   - OATH-OTP トークン、CA Auth ID OTP-OATH、および CA Auth ID OTP-EMV に対するマスタ キー設定
   - SAML トークンの設定
   - ASSP の設定
   - 認証情報タイプが不明な場合に認証リクエストを解決するための設定

- ASSP 認証リクエストの処理に使用する認証情報タイプを識別するための設定
- RADIUS 認証リクエストの処理に使用する認証情報タイプを識別するための設定

5. ［保存］をクリックします。

   注: これらの設定は組織レベルで上書きできます。

6. 展開された CA Strong Authentication サーバインスタンスをすべてリフレッシュします。この方法の詳細については、「サーバインスタンスのリフレッシュ（P. 72）」を参照してください。

第 6 章: 組織の管理

1 つの*組織*を企業（または会社）全体、または企業内の特定の部門、部署、その他のエンティティにマップできます。 管理コンソールで用意されている組織構造がフラットな階層（親組織と子組織の形式）であることはサポートされて*おらず*、すべての組織はデフォルトの組織と同じレベルで作成されます

注: この章のほとんどのタスクは、GA（グローバル管理者）または OA（組織管理者）によって実行できます（その管理者が組織に対して必要なスコープを持っている場合）。

CA Strong Authentication でサポートされている組織管理操作には、以下のものが含まれます。

- 組織の作成とアクティブ化 (P. 186)
- 組織情報の更新 (P. 202)
- ユーザとユーザ アカウントの一括でのアップロード (P. 206)
- バルク データ アップロード リクエストのステータスの表示 (P. 211)
- 組織キャッシュのリフレッシュ (P. 212)
- 組織の非アクティブ化 (P. 213)
- 組織のアクティブ化 (P. 214)
- 組織の削除 (P. 215)

組織の作成とアクティブ化

組織を作成し、CA Strong Authentication リポジトリまたは既存の LDAP ベースのディレクトリ サーバ実装にそのデータを保存します。

注: 小規模な展開の場合には、新しい組織を作る代わりに、デフォルトの組織の名前を変更できます。

このセクションでは、以下の手順について説明します。

- CA Strong Authentication リポジトリでの組織の作成（P. 187）
- LDAP リポジトリでの組織の作成（P. 192）

必要な権限

組織を作成してアクティブ化するには、そのための適切な権限とスコープを持っていることを確認します。 MA と GA はすべての組織を作成し、アクティブにすることができます。

AuthMinder リポジトリでの組織の作成

次の手順に従ってください:

1. ［組織］タブをクリックします。
2. ［組織の管理］セクションで［組織の作成］リンクをクリックして［組織の作成］ページを表示します。
3. 組織の詳細の入力

組織情報

［Organization Name］

作成する組織に対する一意の ID を入力します。

注: この組織にログインするには、組織の表示名ではなく、この値を指定する必要があります。

表示名

組織のわかりやすい一意の名前を入力します。

注: この名前はほかのすべての管理コンソール ページやレポートに表示されます。

Description

この組織を管理する管理者に関する説明を入力します。

注: このフィールドを使用して、後で参照できるように組織の追加の詳細を入力できます。

管理者認証メカニズム

この組織に属する管理者を認証するために使用されるメカニズムを選択します。

管理コンソールでは、以下の 3 種類の認証メカニズムがサポートされています。

基本ユーザ パスワード

これは、管理コンソール によって提供される組み込みの認証メカニズムです。 このオプションを選択した場合、管理者は自分の ID とパスワードを指定して管理コンソールにログインします。

WebFort パスワード

これは、WebFort のパスワード認証方式です。 このオプションを選択した場合、管理者の認証情報は CA Strong Authentication サーバによって発行され、認証されます。

このメカニズムを使用するには、管理コンソールを CA Strong Authentication サーバに接続する必要があります。 接続の詳細は［AuthMinder 接続］ページで設定できます、詳細については、「CA Strong Authentication の接続の設定」を参照してください。

キー ラベル設定

CA Strong Authentication では、ハードウェアまたはソフトウェア ベースの機密データの暗号化を使用できます。 暗号化モードは arcotcommon.ini 設定ファイルを使用して選択できます。 詳細については、「CA Strong Authentication インストールガイド」の付録「設定ファイルおよびオプション」を参照してください。

ハードウェアの暗号化かソフトウェアの暗号化かに関係なく、すべての Arcot 製品は、ユーザや組織のデータの暗号化にグローバル キー ラベルまたは組織固有のキー ラベルを使用します。

ハードウェアの暗号化を使用している場合、このラベルは、HSM デバイスに格納されている実際の 3DES キーへの参照（ポインタ）としてのみ機能します。そのため、HSM キー ラベルと一致する必要があります。 ただし、ソフトウェア ベースの暗号化の場合、このラベルはキーとして機能します。

グローバル キーの使用

デフォルトでは、このオプションが選択されています。 ブートストラップ プロセスで指定したグローバル キー ラベルを無効にして、新たにソフトウェア ベースの暗号化またはハードウェア ベースの暗号化用のラベルを指定する場合は、このオプションを選択解除します。

キー ラベル

［グローバル キーの使用］オプションを選択解除した場合は、組織に対して使用する新しいキー ラベルを指定します。

暗号化ストレージ タイプ

暗号化キーがデータベース（ソフトウェア）に格納されるか HSM（ハードウェア）に格納されるかを示します。

ローカライズ設定

グローバル設定の使用

グローバル レベルで設定されたローカライゼーション パラメータを使用するには、このオプションを選択します。

日付/時刻形式

［グローバル設定の使用］オプションを選択解除した場合は、使用する日付/時刻形式を指定します。

優先ロケール

［グローバル設定の使用］オプションを選択解除した場合は、優先ロケールを選択します。

ユーザ データの場所

リポジトリ タイプ

Arcot データベースを選択します。 このオプションを指定すると、新しい組織のユーザや管理者の詳細が CA Strong Authentication でサポートされている RDBMS リポジトリに保存されます。

カスタム属性

このセクションを使用して、作成している組織に固有の情報を追加します。

Name

カスタム属性の名前です。

値

カスタム属性の値です。

4. ［次へ］をクリックします。

［暗号化する属性の選択］ページが表示されます。

5. ［暗号化する属性］セクションで、以下のいずれかを実行します。
   - グローバル設定を属性の暗号化セットの設定に使用する場合は、［グローバル設定の使用］を選択します。
   - 暗号化する属性を［暗号化用に利用可能な属性］リストから選択し、それを［暗号化用に選択した属性］に追加します。

     ［>］ボタンをクリックして、選択した属性を目的のリストに移動します。 ［>>］ボタンをクリックして、すべての属性を目的のリストに移動することもできます。

     注: 一度に複数の属性を選択するには、Ctrl キーを押しながら選択します。
6. ［次へ］をクリックします。

［管理者の追加］ページが表示されます。

注: システムに現在存在するすべての管理者がすべての組織を管理するためのスコープを持っている場合、このページは表示 *されません*。

［利用可能な管理者］リストから組織を管理する管理者を選択し、［>］ボタンをクリックして管理者を［管理している管理者］リストに追加します。

［利用可能な管理者］リストには、新しい組織を管理できるすべての管理者が表示されます。

注: 一部の管理者がシステム内のすべての組織を管理するためのスコープを持っている場合、それらの管理者に対応するエントリはこのリストに表示されません。

［管理している管理者］リストには、この組織を管理するために選択した管理者が表示されます。

7. ［次へ］ボタンをクリックして続行します。

   ［アカウント タイプの設定］ページは、ログインした管理者が管理するアカウント タイプを持っている場合にのみ表示されます。ログインした管理者が管理するアカウント タイプを持っていない場合は、［電子メール/電話のタイプの設定］ページが表示されます。

   a. ［アカウント タイプの割り当て］セクションで、［利用可能］リストからアカウント タイプを選択し、［>］ボタンをクリックしてそれらを［選択済み］リストに移動させます。

      ［アカウント カスタム属性の設定］ページが表示されます。

   b. アカウントの属性を 1 つ以上指定します。

8. ［次へ］ボタンをクリックして続行します。

   ［電子メール/電話のタイプの設定］ページが表示されます。

9. ユーザが用意する必要がある必須およびオプションの電子メール アドレスと電話番号のタイプを指定します。

10. ［スキップ］をクリックしてシステム レベルで設定された電子メールおよび電話タイプを使用し、次のページに移動するか、または［保存］をクリックして変更内容を保存します。

11. 組織のアクティブ化ページで、［有効］をクリックして新しい組織をアクティブにします。

    メッセージが表示されます。

12. ［OK］をクリックして処理を完了します。

注: 組織をアクティブにすることを選択しなくても、組織は初期状態で作成されます。 この組織を後からアクティブにすることができます。この手順については、「初期状態の組織のアクティブ化 (P. 214)」を参照してください。

13. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。この方法の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

    注: 組織を作成する際に、属性の暗号化セット、アカウント タイプ、および電子メールと電話のタイプを設定している場合は、システム設定と組織のキャッシュの*両方*をリフレッシュします。 組織レベルのキャッシュをリフレッシュしないと、システムは回復不可能な状態になります。

LDAP リポジトリでの組織の作成

LDAP ユーザ ディレクトリをサポートするには、CA Strong Authentication リポジトリに組織を作成してから、CA Strong Authentication の属性を LDAP の属性にマップします。

次の手順に従ってください:

1. ［組織］タブをクリックします。
2. ［組織の管理］セクションで［組織の作成］リンクをクリックして［組織の作成］ページを表示します。
3. 組織の詳細の入力

   組織情報

   ［Organization Name］

   作成する組織に対する一意の ID を入力します。

   注: 管理コンソールを使用してこの組織にログインするには、組織の表示名ではなく、この値を指定します。

   表示名

   組織のわかりやすい一意の名前を入力します。

   注: この名前はほかのすべての管理コンソール ページやレポートに表示されます。

   Description

   この組織を管理する管理者に関する説明を入力します。

   注: このフィールドを使用して、後で参照できるように組織の追加の詳細を入力できます。

管理者認証メカニズム

この組織に属する管理者を認証するために使用されるメカニズムを選択します。

管理コンソールでは、以下の 3 種類の認証メカニズムがサポートされています。

基本ユーザ パスワード

これは、管理コンソール によって提供される組み込みの認証メカニズムです。 このオプションを選択した場合、管理者は自分の ID とプレーン テキスト パスワードを指定してコンソールにログインします。

LDAP ユーザ パスワード

認証ポリシーは LDAP ディレクトリ サービスで定義されています。このオプションを選択した場合、管理者は LDAP に格納されている認証情報を使用して管理コンソールにログインする必要があります。

WebFort パスワード

これは、WebFort のパスワード認証方式です。 このオプションを選択した場合、管理者の認証情報は CA Strong Authentication サーバによって発行され、認証されます。

キー ラベル設定

グローバル キーの使用

デフォルトでは、このオプションが選択されています。 ブートストラップ プロセスで指定したグローバル キー ラベルを無効にして、新たにソフトウェア ベースの暗号化用のラベルを指定する場合は、このオプションを選択解除します。

キー ラベル

［グローバル キーの使用］オプションを選択解除した場合は、組織に対して使用する新しいキー ラベルを指定します。

暗号化ストレージ タイプ

暗号化キーがデータベース（ソフトウェア）に格納されるか HSM（ハードウェア）に格納されるかを示します。

ローカライズ設定

グローバル設定の使用

グローバル レベルで設定されたローカライゼーション パラメータを使用するには、このオプションを選択します。

日付/時刻形式

［グローバル設定の使用］オプションを選択解除した場合は、使用する日付/時刻形式を指定します。

優先ロケール

［グローバル設定の使用］オプションを選択解除した場合は、優先ロケールを選択します。

ユーザ データの場所

リポジトリ タイプ

［エンタープライズ LDAP］を選択します。 このオプションを指定すると、新しい組織のユーザや管理者の詳細が CA Strong Authentication リポジトリに保存されます。

カスタム属性

Name

カスタム属性の名前です。

値

カスタム属性の値です。

4. ［次へ］をクリックします。

LDAP リポジトリの詳細を収集するための［組織の作成］ページが表示されます。

5. 詳細を指定します。

ホスト名

LDAP リポジトリを使用できるシステムのホスト名を入力します。

Port Number

LDAP リポジトリ サービスがリスニングしているポート番号を入力します。

スキーマ名

LDAP リポジトリで使用される LDAP スキーマを指定します。 このスキーマには、LDAP リポジトリに含めることができるオブジェクトのタイプと、各オブジェクト タイプの必須属性および任意属性が指定されます。

通常、Active Directory のスキーマ名は user であり、SunOne Directory のスキーマ名は user および inetorgperson です。

ベース識別名

LDAP リポジトリのベース識別名を入力します。この値は、LDAP リポジトリ内を検索する際の LDAP 階層の開始ノードを示します。

たとえば、cn=rob laurie, ou=sunnyvale, o=arcot, c=us という DN を持つユーザを検索するには、ベース DN を以下のように指定する必要があります。

ou=sunnyvale, o=arcot, c=us

注: 通常、このフィールドでは大文字と小文字が区別され、このフィールドに指定されたベース DN のサブノードがすべて検索されます。

リダイレクト スキーマ名

「member」属性を定義するスキーマの名前を指定します。

これはオプション フィールドです。

組織に対して定義されたベース DN を使用して、LDAP リポジトリでユーザを検索できます。 ただし、この検索では、特定の OU（組織単位）に属するユーザしか返されません。LDAP 管理者は、グループ全体へのアクセスを制御するために、さまざまな組織単位に属するユーザのグループを作成し、さまざまなグループからユーザを検索したいと思われます。管理者がグループを作成すると、ユーザ ノード DN はグループ ノードの「member」属性に格納されます。デフォルトでは、UDS では属性値に基づいた検索や DN の解決が許可されていません。 リダイレクトを使用すると、特定のノードに対する特定の属性値に基づいて、LDAP 内のさまざまなグループに属するユーザを検索できます。

通常、Active Directory のリダイレクト スキーマ名は group であり、SunOne Directory のリダイレクト スキーマ名は groupofuniquenames です。

接続タイプ

管理コンソール と LDAP リポジトリの間で使用する接続のタイプを選択します。 サポートされているタイプは以下のとおりです。

- TCP
- 一方向 SSL
- 双方向 SSL

ログイン名

LDAP リポジトリ ユーザの完全識別名を入力します。このユーザは、リポジトリ サーバにログインし、ベース識別名を管理する権限を持つユーザです。

例： uid=gt,dc=arcot,dc=com

ログイン パスワード

［ログイン名］で指定したユーザのパスワードを入力します。

サーバ トラステッド ルート証明書

参照ボタンを使用して LDAP サーバに SSL 証明書を発行した信頼済みルート証明書のパスを入力します。

このフィールドは、［接続タイプ］フィールドで［一方向 SSL］または［双方向 SSL］を選択した場合に使用可能です。

クライアント キー ストア

参照ボタンを使用してクライアント証明書と対応するキーが含まれるキーストアのパスを入力します。

このフィールドは、［接続タイプ］フィールドで［双方向 SSL］を選択した場合にのみ使用可能です。

注: PKCS#12 または JKS のいずれかのキーストア タイプをアップロードします。

クライアント キー ストア パスワード

必要な SSL オプションが選択されている場合は、クライアント キーストアのパスワードを入力します。

このフィールドは、［接続タイプ］フィールドで［双方向 SSL］を選択した場合にのみ使用可能です。

6. ［次へ］ボタンをクリックして続行します。

   リポジトリの属性をマップするページが表示されます。

7. このページで、以下を実行します。

   a. ［Arcot データベース属性］リストから属性を選択し、Arcot の属性とマップする必要がある適切な属性を［エンタープライズ LDAP 属性］リストから選択して［マップ］ボタンをクリックします。

      重要: UserName 属性は必ずマップする必要があります。 Active Directory を使用している場合は、UserName を sAMAccountName にマップします。SunOne Directory を使用している場合は、UserName を uid にマップします。
      Active DIrectory の場合は、STATUS を userAccountControl にマップする必要があります。

   b. 必要なすべての属性のマップが完了するまで、属性をマップする作業を繰り返します。

      注: ［**Arcot データベース属性**］リスト内の属性をすべてマップする必要はありません。 使用する属性のみをマップします。

      マップされた属性は［マップされた属性］リストに移動されます。

      必要な場合は、属性のマッピングを解消できます。 一度に 1 つの属性のマッピングを解消する場合は、属性を選択してマップ解除ボタンをクリックします。 ただし、［マップされた属性］リストをクリアする場合は、リセット ボタンをクリックすると、マップされたすべての属性のマッピングが解消されます。

   c. 前のページで［リダイレクト スキーマ名］を指定した場合は、［リダイレクト検索属性］リストから検索属性を選択する必要があります。

      通常、Active Directory の属性は member であり、SunOne Directory の属性は uniquemember です。

8. ［次へ］ボタンをクリックして続行します。

   ［暗号化する属性の選択］ページが表示されます。

9. ［暗号化する属性］セクションで、以下のいずれかを実行します。

   - グローバル設定を属性の暗号化セットの設定に使用する場合は、［グローバル設定の使用］を選択します。
   - 暗号化する属性を［暗号化用に利用可能な属性］リストから選択し、それを［暗号化用に選択した属性］に追加します。

     ［>］ボタンをクリックして、選択した属性を目的のリストに移動します。 ［>>］ボタンをクリックして、すべての属性を目的のリストに移動することもできます。

     注: 一度に複数の属性を選択するには、Ctrl キーを押しながら選択します。

10. ［次へ］をクリックします。

    ［管理者の追加］ページが表示されます。

    注: システムに現在存在するすべての管理者がすべての組織を管理するためのスコープを持っている場合、このページは表示 *されません*。

    ［利用可能な管理者］リストから組織を管理する管理者を選択し、［>］ボタンをクリックして管理者を［管理している管理者］リストに追加します。

    ［利用可能な管理者］リストには、新しい組織を管理できるすべての管理者が表示されます。

    注: 一部の管理者がシステム内のすべての組織を管理するためのスコープを持っている場合、それらの管理者に対応するエントリはこのリストに表示されません。

    ［管理している管理者］リストには、この組織を管理するために選択した管理者が表示されます。

11. ［次へ］ボタンをクリックして続行します。

    ［アカウント タイプの設定］ページは、ログインした管理者が管理するアカウント タイプを持っている場合にのみ表示されます。ログインした管理者が管理するアカウント タイプを持っていない場合は、［電子メール/電話のタイプの設定］ページが表示されます。

    a. ［アカウント タイプの割り当て］セクションで、［利用可能］リストからアカウント タイプを選択し、［>］ボタンをクリックしてそれらを［選択済み］リストに移動させます。

       ［アカウント カスタム属性の設定］ページが表示されます。

    b. アカウントの属性を 1 つ以上指定します。

12. ［次へ］ボタンをクリックして続行します。

    ［組織のアクティブ化］ページが表示されます。

13. ［有効］ボタンをクリックして新しい組織をアクティブにします。

    警告メッセージが表示されます。

14. ［OK］をクリックします。

15. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。この方法の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

情報： 組織を作成する際に、属性の暗号化セット、アカウント タイプ、および電子メールと電話のタイプを設定している場合は、システム設定と組織のキャッシュの*両方*をリフレッシュします。 組織レベルのキャッシュをリフレッシュしないと、システムは回復不可能な状態になります。

組織の検索

必要な権限

組織を更新、アクティブ化、または非アクティブ化する必要がない限り、検索権限は必要ありません。 ただし、検索する組織がスコープに含まれている*必要があります*。 たとえば、対象となる組織が OA の権限の範囲内に*あれば*、OA はその組織を検索できます。

組織の検索

組織の検索には、名前とステータスを使用できます。

次の手順に従ってください:

1. ［**組織**］タブをクリックします。
2. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
3. 必要な組織の情報の一部または全部を入力します。 以下のオプションを選択して、検索の範囲を広げることができます。

   注: ［**組織**］フィールドには、実際の組織名 *では*なく、組織の表示名の一部または全部を入力する必要があります。

   - **初期**（作成されたが、まだアクティブ化されていない組織を表示する場合）
   - **アクティブ**（作成され、アクティブ化された組織を表示する場合）
   - **非アクティブ**（非アクティブ化された組織を表示する場合）
   - **削除済み**（削除された組織を表示する場合）
4. ［**検索**］ボタンをクリックすると、指定した条件に一致するすべての組織がページに表示されます。

組織情報の更新

組織の以下の情報を更新できます。

- 組織の表示名、説明、ステータス、電子メールのタイプ、電話のタイプ、暗号化タイプ、アカウント タイプとそのカスタム属性、および組織を管理する管理者を含む**組織情報**（「基本組織情報の更新（P. 202）」）。
- 認証情報プロファイル、認証ポリシー、拡張可能な設定、および割り当てられたデフォルト設定を含む組織の **CA Strong Authentication 固有の設定**（CA Strong Authentication 固有の設定の更新（P. 205））。

必要な権限

そのための適切な権限とスコープを持っていることを確認します。MA はすべての組織を更新できます。 GA と OA は、自分のスコープに含まれるすべての組織の情報を更新できます。

基本組織情報の更新

次の手順に従ってください:

1. ［組織］タブをクリックします。
2. ［組織の管理］セクションで［組織の検索］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［検索］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. ［組織］列で、必要な組織の <ORGANIZATION_NAME> リンクをクリックします。

   ［組織情報］ページが表示されます。

5. ［組織詳細］セクションで、必要なフィールド（［表示名］と［説明］）を編集します。

   組織に管理者がいない場合は、管理者認証メカニズムを変更できます。

6. ［ローカライズ設定］セクションで、以下のいずれかの手順を実行します。

   - ［グローバル設定の使用］を選択します。
   - ［日付/時刻形式］および［優先ロケール］を編集する。

7. ［カスタム属性］セクションで、必要に応じて［名前］フィールドと［値］フィールドを編集します。

8. ［次へ］をクリックして追加の設定に進みます。

   - 組織が CA Strong Authentication リポジトリ内に作成され、かつ組織内の管理者がシステム内の組織を管理するスコープを持っている場合は、以下を行います。

     a. ［暗号化する属性の選択］ページで、属性の暗号化セット設定にグローバル設定を使用する場合は［グローバル設定の使用］を選択し、そうでない場合は［暗号化用に利用可能な属性］リストから暗号化する属性を選択して［暗号化用に選択した属性］リストに追加します。
     組織でユーザがすでに作成されている場合は、属性を更新できません。

     b. ［管理者の更新］ページで、組織を管理する管理者を更新し、［次へ］をクリックします。

     c. ［アカウント タイプの設定］ページで、アカウント タイプを［利用可能］リストから選択して［選択済み］リストに移動させて［次へ］をクリックします。このページは更新する組織に適用可能なアカウント タイプがある場合にのみ表示されます。

     d. グローバル アカウント タイプはクリアできません。

     e. ［アカウント カスタム属性の設定］ページで、組織内のアカウント用の 1 つ以上のカスタム属性を設定し、［次へ］をクリックします。このページは更新する組織に適用可能なアカウント タイプがある場合にのみ表示されます。

     f. ［電子メール/電話のタイプの設定］ページで、ユーザ用の必須およびオプションの電子メール アドレスおよび電話のタイプを設定し、［保存］をクリックして処理を完了します。

- 組織が LDAP リポジトリに作成された場合は、組織編集のページが表示されます。

  a. 必要に応じて、「LDAP リポジトリでの組織の作成 (P. 192)」の情報を参照してフィールドを更新し、［次へ］をクリックしてポジトリ属性マッピングを編集するページを表示します。

  b. ユーザ名のマッピングは更新できません。このフローで、マップされていない属性があればマップできます。[次へ]をクリックして、［暗号化する属性の選択］ページを表示します。

  c. ［暗号化する属性の選択］ページで、属性の暗号化セット設定にグローバル設定を使用する場合は［グローバル設定の使用］を選択し、そうでない場合は［暗号化用に利用可能な属性］リストから暗号化する属性を選択してリストに追加し、［次へ］を選択します。

  注: 組織でユーザがすでに作成されている場合は、属性を更新できません。 LDAP の場合には、LDAP リポジトリ内のユーザに対する単純な検索操作でも、データベースにユーザを登録します。したがって、LDAP リポジトリのユーザを検索した場合は、属性を更新できません。

  d. ［管理者の更新］ページで、組織を管理する管理者を更新し、［次へ］をクリックします。

  e. ［アカウント タイプの設定］ページで、アカウント タイプを［利用可能］リストから選択して［選択済み］リストに移動させて［次へ］をクリックします。

  f. グローバル アカウント タイプはクリアできません。

  g. ［アカウント カスタム属性の設定］ページで、組織内のアカウント用の 1 つ以上のカスタム属性を設定し、［更新］をクリックして変更を保存して処理を完了します。

9. 展開された CA Strong Authentication サーバ インスタンスをすべてリフレッシュします。この方法の詳細については、「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

AuthMinder 固有の設定の更新

次の手順に従ってください:

1. ［組織］タブをクリックします。
2. ［組織の管理］セクションで［組織の検索］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報を一部または全部入力し、［検索］ボタンをクリックして、検索条件に一致する組織のリストを表示します。
4. ［組織］列で、組織情報を表示する組織の <ORGANIZATION_NAME> リンクをクリックします。
5. ［CA Strong Authentication 設定］タブをアクティブにして、タスク ペインにある［CA Strong Authentication 設定］のリンクを表示します。

   これらの設定の詳細については、「組織固有の設定の管理 (P. 217)」を参照してください。

ユーザとユーザ アカウントの一括でのアップロード

CA Strong Authentication では、管理コンソールを使用してユーザとユーザ アカウントを一括してアップロードできます。 複数のユーザおよびユーザ アカウントの情報をアップロードするには、CSV（カンマ区切り値）形式の入力ファイルが必要です。

ユーザの一括でのアップロード

ユーザをアップロードする CSV 形式の入力ファイル内の最初の行は、以下のようにする必要があります。

```
#UserID,fName,lName,status,EmailAddr,telephoneNumber,INFOLIST,mName#
```

注意： この最初の（テンプレート）行は*常に*必要です。 この行が指定されていないと、ユーザの一括アップロード操作は失敗します。

ユーザをアップロードするための CSV 入力ファイルを作成するときは、以下の点に注意してください。

- CSV ファイルには、ヘッダ行が必要です。この行の先頭と末尾に # 記号を指定し、この # 記号の間に他のすべてのフィールドを指定します。
- 必須のエントリは UserID だけです。その他のエントリはオプションです。 特定のユーザがすでに存在している場合は、そのレコードが更新されます。ユーザが存在しない場合は、新しいユーザが作成されます。
- 最大で 5 つの電子メール アドレスと 5 つの電話番号を指定できます。この場合は、以下のようにヘッダを指定します。

```
#UserID,fName,lName,status,EmailAddr,EMAIL.2,EMAIL.3,EMAIL.4,EMAIL.5,telephoneNumber,PHONE.2,PHONE.3,PHONE.4,PHONE.5,INFOLIST,mName#
```

ファイルのエントリについて、以下の表で説明します。

エントリ	Description
UserID	ユーザの一意の ID。
fName	ユーザの名。
mName	ユーザのミドル ネーム。
lName	ユーザの姓。
status	ユーザのステータス。 以下の値が使用可能です。 ■ INITIAL ■ ACTIVE

エントリ	Description
pam	個人の認証メッセージ。
pamURL	ユーザの個人の認証メッセージのイメージがある場所の URL。
EmailAddr	ユーザの連絡用電子メールの ID。
telephoneNumber	国際コードを伴うユーザの完全な電話番号。 たとえば、米国の電話番号は 1 で始まります。
PHONE.2	ユーザのオプションの電話番号。

たとえばファイルの例として、以下のエントリを含めることができます。

```
#UserID,fName,lName,status,EmailAddr,telephoneNumber,PHONE.2,INFOLIST#
mparker,martin,parker,ACTIVE,mparker@ca.com,12345,9999,age=29;favsport=cricket
jhume,john,hume,ACTIVE,jhume@ca.com,3939292,203939393,age=32;favbook=fiction
fantony,francis,antony,ACTIVE,fantony@ca.com,130203,29888,age=25;favfood=pizza
```

ユーザ アカウントの一括でのアップロード

ユーザ アカウントをアップロードする CSV 形式の入力ファイル内の最初の行は、以下のようにする必要があります。

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,accountIDAttribute3,customAttr1,customAttr2,customAttr3,customAttr4,customAttr5,customAttr6,customAttr7,customAttr8,customAttr9,customAttr10#
```

重要: この最初の（テンプレート）行は*常に*必要です。 この行が指定されていないと、ユーザ アカウントのバルク アップロード操作は失敗します。

ユーザ アカウントをアップロードするための CSV 形式の入力ファイルを作成するときは、以下に注意してください。

- 必須のエントリは、UserID、accountType、および accountID だけです。その他のエントリはオプションです。
- システムでユーザが作成済みである必要があります。
- アカウント タイプを作成して、組織にそれを割り当て済みである必要があります。
- アカウント タイプのカスタム属性を作成している必要があります。これはオプションで、特定のユーザ用のアカウント タイプにカスタム属性を追加する場合にのみ実行する必要があります。
- 1 つのアカウント タイプに最大 3 つまでのアカウント ID 属性を指定できます。
- 1 つのアカウント タイプに対して最大 10 までのカスタム属性を指定できます。

ファイルのエントリについて、以下の表で説明します。

エントリ	Description
UserID	ユーザの一意の ID。
accountType	アカウント タイプ。
accountID	ユーザの代替 ID。

エントリ	Description
status	アカウント ID のステータス。 以下の値が使用可能です。 ■ ［0-9］ : INITIAL ■ ［10-19］ : ACTIVE ■ ［20-29］ : INACTIVE
accountIDAttribute1	accountID の属性。 サポートされているアカウント ID 属性は 3 つだけです。
customAttr1	ユーザのカスタム属性。

たとえばファイルの例として、以下のエントリを含めることができます。

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,accountIDAttribute3,customAttr1,customAttr2#
prush,ONLINE_BANKING,OB_ID1,10,login,password,image,chicago,music
jhume,SAVINGS,SA_ID1,10,interest,deposit,check,florida,soccer
```

次の手順に従ってください:

1. ［**組織**］タブをクリックします。
2. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. ユーザとユーザ アカウントを一括してアップロードする組織を選択します。
5. ［**基本組織情報**］セクションで、［**バルク アップロード**］リンクをクリックし、［バルク データ アップロード］ページを表示します。
6. ［**バルク アップロード**］セクションで、以下の操作を実行します。
   a. ［**バルク アップロード操作**］ドロップダウン リストから、［**ユーザ アカウントのアップロード**］または［**ユーザのアップロード**］を選択します。
   b. **参照**ボタンをクリックして、ユーザ アカウントまたはユーザのエントリが含まれる CSV ファイルを指定します。
   c. 操作の［**説明**］を入力します。
7. ［**アップロード**］をクリックして、ユーザ アカウントまたはユーザを一括してアップロードします。

   操作が完了すると、メッセージにリクエスト ID が表示されます。

   重要: このリクエスト ID をメモしておいてください。 バルク データ アップロード操作のステータスを表示するために必要になります。 通常、バルク アップロード操作はすぐにトリガされず、開始されるまでに最大で 10 分程度かかることがあります。 各操作のリクエスト ID はリンクとして表示されます。 このリンクをクリックすると、ステータス結果ページを表示できます。

バルク データ アップロード リクエストのステータスの表示

次の手順に従ってください:

1. ［**組織**］タブをクリックします。
2. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. バルク アップロード リクエストのステータスを表示する組織を選択します。
5. ［**基本組織情報**］セクションで、［**バルク リクエストの表示**］リンクをクリックし、［バルク リクエストの検索］ページを表示します。
6. ［バルク リクエストの検索］ページで、以下の操作を実行します。
   a. 先にメモしておいたリクエスト ID を入力します（「ユーザとユーザ アカウントの一括でのアップロード (P. 206)」の手順 11）。

      または

   b. 表示したいバルク リクエストの［**ステータス**］を選択します。

      または

   c. ［**ユーザのアップロード**］リクエストを表示するか、または［**ユーザ アカウントのアップロード**］リクエストを表示するかに応じて、［**操作**］を選択します。
7. ［**検索**］をクリックすると、検索結果が表示されます。
8. ［**リクエスト ID**］リンクをクリックすると、バルク リクエストの詳細情報が表示されます。
9. ［**失敗した操作の数**］リンクをクリックすると、操作が失敗した理由が表示されます。

   注: リクエストの操作が失敗した場合は、［**エクスポート失敗**］ボタンが有効になります。［**エクスポート失敗**］ボタンをクリックすると、失敗したすべての操作を CSV ファイルにエクスポートできます。その後、エクスポートされたファイルでエラーを修正し、バルク アップロードのためにファイルを再サブミットできます。

組織キャッシュのリフレッシュ

属性暗号化セット、ローカライゼーション設定、および電子メールと電話のタイプなどのグローバル設定を参照しない組織設定は、組織レベルでキャッシュされます。 組織レベルでこれらの設定に変更を加えた場合、変更を有効にするには組織のキャッシュをリフレッシュします。

必要な権限

MA は、すべての組織のキャッシュをリフレッシュできます。GA と OA は、そのスコープ内のすべての組織のキャッシュをリフレッシュできます。

組織キャッシュのリフレッシュ

次の手順に従ってください:

1. ［**組織**］タブをクリックします。
2. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. キャッシュをリフレッシュする組織を選択します。
5. ［**キャッシュのリフレッシュ**］をクリックします。
6. キャッシュ リフレッシュ リクエストを確認するダイアログ ボックスで［**OK**］をクリックします。

   ［**キャッシュ リフレッシュ ステータスの確認**］リンクをクリックし、この**リクエスト ID** を選択すると、キャッシュ リフレッシュ リクエストのステータスを確認できます。

   注: ある組織のキャッシュをリフレッシュしても、その他の組織に対してその時間に実行されているトランザクションの応答時間には影響しません。

組織の非アクティブ化

組織のすべての管理者に対して CA Strong Authentication のメカニズムを使った管理コンソールへのログインを禁止し、組織のエンド ユーザに対して CA Strong Authentication のメカニズムを使ったアプリケーションへの認証を禁止する場合は、組織を非アクティブ化します。

必要な権限

そのための適切な権限とスコープを持っていることを確認します。MA はすべての組織を無効化できます。 GA と OA は、自分のスコープに含まれるすべての組織を無効化できます。

組織の非アクティブ化

次の手順に従ってください:

1. ［組織］タブをクリックします。
2. ［組織の管理］セクションで［組織の検索］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［検索］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. 非アクティブにする組織を 1 つ以上選択します。
5. ［非アクティブ化］ボタンをクリックすると、選択した組織が無効になります。

   組織を非アクティブにすることを確認するメッセージ ボックスが表示されます。
6. ［OK］をクリックします。

組織のアクティブ化

非アクティブになっている組織を再度アクティブにする必要がある場合があります。その場合は、組織の検索ページで検索条件を指定する際に、［**非アクティブ**］オプションを選択します。

必要な権限

組織を有効化できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。MA はすべての組織を有効化できます。 GA と OA は、自分のスコープに含まれるすべての組織を有効化できます。

組織のアクティブ化

次の手順に従ってください:

1. ［**組織**］タブをクリックします。
2. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. 再度有効にする組織を 1 つ以上選択します。
5. ［**アクティブ化**］ボタンをクリックすると、選択した組織がアクティブになります。

   組織をアクティブにすることを確認するメッセージ ボックスが表示されます。
6. ［OK］をクリックします。

組織の削除

組織を削除すると、その組織に関連付けられた管理者は管理コンソールを使用してログインできなくなり、その組織に属するエンド ユーザは自身を認証できなくなります。 ただし、組織に関連する情報は引き続きシステム内に保持されます。 削除された組織がスコープに含まれている管理者は、その組織の詳細を読み取ることができます。

必要な権限

そのための適切な権限とスコープを持っていることを確認します。 MA はすべての組織を削除できます。 GA と OA は、自分のスコープに含まれるすべての組織を削除できます。

組織の削除

次の手順に従ってください:

1. ［**組織**］タブをクリックします。
2. ［**組織の管理**］セクションで［**組織の検索**］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. 削除する組織を 1 つ以上選択します。
5. ［**削除**］ボタンをクリックすると、選択した組織が削除されます。

   組織を削除することを確認するメッセージ ボックスが表示されます。
6. ［OK］をクリックします。

第 7 章: 組織固有の AuthMinder の設定の管理

GA （グローバル管理者）によって設定された「テンプレート化された」プロファイル、ポリシー、その他の設定を使用することはできますが、自分の権限の範囲内で組織の特定のビジネス要件を満たすために、これらを変更するか新しいものを作成したい場合があります。

組織レベルで設定を行うと、変更は設定した特定の組織に限定されます。また、設定に対して行われた変更内容は自動的には適用されません。 これらの設定変更を適用するには、サーバ インスタンスをすべてリフレッシュします。

注: 組織の設定を管理できるようにするには、ユーザ（組織管理者）がそのための適切な権限およびスコープを持っていることを確認する必要があります。マスタ管理者は組織に固有の設定を管理できません。GA と OA は、自分のスコープに含まれるすべての組織の設定を管理できます。

指定された組織にスコープがある場合は、OA または GA として以下のタスクを実行できます。

- 組織固有の CA Strong Authentication の設定の割り当て（P. 218）
- 組織に対するその他の CA Strong Authentication 設定の設定（P. 219）

組織固有の AuthMinder の設定の割り当て

組織固有の設定はグローバル設定に似ていますが、それぞれのタスク ページへのナビゲーション パスは異なります。

次の手順に従ってください:

1. ［組織］タブをクリックします。
2. ［組織の管理］セクションで［組織の検索］リンクをクリックして［組織の検索］ページを表示します。
3. 検索する組織の情報の一部または全部を入力し、［検索］ボタンをクリックします。

   検索条件に一致する組織のリストが表示されます。
4. ［組織］列で、必要な組織のリンクをクリックします。

   ［組織情報］ページが表示されます。
5. ［CA Strong Authentication 設定］タブをアクティブにします。

   タスク ペインに組織固有の設定のリンクが表示されます。
6. 認証情報プロファイルと認証ポリシーを設定し、割り当てます。

   必要なプロファイルとポリシーの設定方法と割り当て方法の詳細については、必要に応じて「グローバルな CA Strong Authentication 設定の管理 (P. 99)」を参照してください。 「*グローバルな CA Strong Authentication 設定の管理*」で説明されている操作はグローバル レベルの操作です。 しかし、この章で説明される設定は組織レベルのものです。タスク ページにアクセスする方法は異なりますが、両方のレベルの設定は同じです。

組織に対するその他の AuthMinder 設定の設定

GA（グローバル管理者）、または OA（組織の管理者）として、組織に対して以下の設定を行うことができます。

- スコープ内の組織のプロファイルとポリシーの設定。

  詳細な手順については、「プロファイルとポリシーの設定 (P. 105)」を参照してください。

- OATH トークンの設定

  詳細な手順については、「OATH OTP トークンの管理 (P. 143)」を参照してください。

  注: この設定は OA では設定 *できません*。

- 認証情報の発行と認証に使用するキーの作成と管理。

  詳細な手順については、「認証情報管理キーの設定 (P. 164)」を参照してください。

  注: この設定は OA では設定 *できません*。

- 認証が成功した後にユーザに返される SAML トークンの設定。

  詳細な手順については、「SAML トークンの設定 (P. 168)」を参照してください。

- PDF ドキュメントの署名に使用する ASSP（Adobe 署名サービス プロトコル）の設定。

  詳細な手順については、「ASSP の設定 (P. 170)」を参照してください。

- CA Strong Authentication サーバに対する RADIUS クライアントの設定と、CA Strong Authentication サーバの RADIUS リクエストのプロキシとしての設定。

  詳細な手順については、「RADIUS のための CA Strong Authentication の設定 (P. 172)」を参照してください。

- 設定の割り当て。すぐに動作するデフォルト設定またはカスタム設定を割り当てることができます。

  詳細な手順については、「デフォルト設定の割り当て (P. 182)」を参照してください。

- CA Strong Authentication サーバの機能を拡張するためのプラグインの設定。

詳細な手順については、「プラグインの設定 (P. 179)」を参照してください。

- 不明なパスワード タイプの認証情報の解決。

  詳細な手順については、「認証情報タイプの解決 (P. 180)」を参照してください。

第 8 章: 管理者の管理

管理者のタイプ、および管理者のロールと責任は、展開の規模に依存します。小規模な単独組織の展開の場合、MA（マスタ管理者）と GA（グローバル管理者）を 1 人ずつ使用してエンドユーザの組織を管理します。一方、大規模な複数組織の展開の場合、複数の GA を持つ必要がある場合があります。GA は、展開の複雑さとエンド ユーザの数に基づいて、組織とユーザの管理作業をさらに複数の OA （組織管理者）および UA （ユーザ管理者）に委任できます。

- サポートされている管理ロールの詳細については、「サポートされるロール (P. 17)」を参照してください。 「管理権限の要約 (P. 19)」セクションに、これらの管理者がそれぞれ実行できるタスクの簡単なサマリを示します。

注: マスタ管理者は、この章で説明するすべての操作に加えて、カスタム ロールを作成する権限を持っています。これは CA Strong Authentication でサポートされている既存のデフォルト ロールから派生するロールです。詳細については、「カスタム ロール (P. 25)」を参照してください。

管理者の作成

管理者の作成に必要な権限

管理者は、管理階層の同じまたは低いレベルに属し、かつ同じまたは小さいスコープを持っている他の管理者を作成できます。 例：

- マスタ管理者は、他のすべてのタイプの管理者を作成できます。
- グローバル管理者 (GA) は、自分のスコープ内に以下を作成できます。
  - 他の GA
  - 組織の管理者（OA）
  - ユーザ管理者（UA）
- OA は自分のスコープ内に以下を作成できます。
  - 他の OA
  - UA

CA Strong Authentication パスワード認証情報を使用した管理者の作成

次の手順に従ってください:

1. ［ユーザと管理者］タブをクリックします。
2. ［ユーザと管理者の管理］セクションで、［管理者の作成］リンクをクリックし、［管理者の作成］ページを表示します。
3. ［管理者詳細］セクションで、管理者の詳細を入力します。

   User Name

   管理者の一意のユーザ名。

   組織

   管理者が属する組織の表示名。

   ユーザ パスワード認証メカニズムに対して設定する組織を選択する必要があります。 詳細については、「組織の作成とアクティブ化」を参照してください。

   注: これはこの管理者が管理する組織ではありません。

   ［First Name］

   管理者の名。

   ［Middle Name］

   管理者のミドル ネーム（ある場合）。

   （オプション）姓

   管理者の姓。
4. ［電子メール アドレス］セクションで、組織に設定された電子メール タイプに対する管理者の電子メール アドレスを入力します。
5. ［電話番号］セクションで、管理者に問い合わせるための電話番号を入力します。

   複数の電話タイプが設定されている場合は、必須のすべての電話タイプに値を入力する必要があります。
6. ［カスタム属性］セクションで、個人の電子メール アドレスや自宅の電話番号のように、追加したい任意の属性の名前と値を入力します。
7. ［次へ］ボタンをクリックして続行します。

   ［管理者の作成］の次のページが表示されます。
8. このページで、以下を実行します。

- ［ロール］ドロップダウン リストから新しい管理者のロールを指定します。
- ［管理対象］セクションで、以下のいずれかの手順を実行し、管理者のスコープ内の組織を選択します。
  - この管理者にシステム内の現在および将来の組織をすべて管理させる場合は、［全組織］オプションを選択します。
  - ［利用可能な組織］リストから必要な組織を選択し、［>］ボタンをクリックしてそれらの組織を［選択された組織］リストに追加します。

    ［利用可能な組織］リストには、この管理者を作成する管理者のスコープ内で選択可能なすべての組織が表示されます。［選択された組織］には、管理者の管理対象として選択した組織のリストが表示されます。

9. ［作成］をクリックして変更を保存し、管理者を作成します。

   管理者が正常に作成されたことを示すメッセージが表示されます。このメッセージには、新しい管理者が初めてログインするときに使用できるアクティベーション コードが含まれます。以下はメッセージの例です。

   「管理者を正常に作成しました。 この管理者の初回ログイン用のアクティベーション コードは 03768672 です。」

10. 成功メッセージの中に表示されたアクティベーション コードの数値を書き留めて、管理者にそれを伝えます。

基本ユーザ パスワード認証情報を使用した管理者の作成

基本ユーザ パスワード認証情報のために設定される組織で管理者を作成できます。

次の手順に従ってください:

1. 「CA Strong Authentication パスワード認証情報を使用した管理者の作成 (P. 222)」の説明に従って手順 1 から手順 8 までを実行して、［管理者の作成］ページを表示します。
2. このページで、以下を実行します。
   - ［ロール］ドロップダウン リストから新しい管理者のロールを指定します。
   - ［パスワードの設定］セクションで、管理者にパスワードを設定して確認します。
   - ［管理対象］セクションで、管理者のスコープ内にある組織を選択します。 以下の手順のいずれかを実行します。
     - この管理者にシステム内の現在および将来の組織をすべて管理させる場合は、［全組織］オプションを選択します。
     - ［利用可能な組織］リストから必要な組織を選択し、［>］ボタンをクリックしてそれらの組織を［選択された組織］リストに追加します。

     ［利用可能な組織］リストには、この管理者を作成する管理者のスコープ内で選択可能なすべての組織が表示されます。 ［選択された組織］には、管理者の管理対象として選択した組織のリストが表示されます。
3. ［作成］をクリックして変更を保存し、管理者を作成します。
4. 管理者に新しいパスワードを伝えます。

管理者のプロファイル情報の変更

管理者のプロファイル情報には以下の項目が含まれます。

- 個人情報（姓、名、ミドル ネーム、および連絡先情報）
- 管理者のパスワード
- 優先される組織（今後実行する可能性があるすべての管理者関連タスクの［**組織**］フィールドで、デフォルトで選択される組織）、日付/時刻形式、ロケール、およびタイム ゾーン情報などの管理者基本設定

注: 管理者はいつでも各自のプロファイル情報を変更できます。その他の管理者の情報を変更する場合は、「管理者情報の更新 (P. 229)」を参照してください。

CA Strong Authentication パスワード認証情報を使用する管理者の場合

次の手順に従ってください:

1. 管理コンソールにログインします。
2. ヘッダ フレームの <ADMINISTRATORNAME> リンクをクリックして、［マイ プロファイル］ページを表示します。
3. このページで、以下のように各セクション内の必要な設定を編集します。
   a. 必要に応じて、［個人情報］セクション内のフィールドを編集します。
   b. 現在のパスワードを変更する場合は、［パスワードの変更］セクションで[現在のパスワード]に入力し、[新規パスワード]フィールドと［パスワードの確認］フィールドに新しいパスワードを指定します。
   c. ［質問と回答の設定］セクションでは、パスワードをリセットするときに回答する質問を設定できます（「パスワードを忘れた場合」を参照）。 個別の質問と対応する回答を指定します。

      重要: このセクションのすべての質問を設定する*必要があります*。質問や回答のいずれかを繰り返して使用することは*できません*。また、セクション内の質問がこのセクションで設定した回答のいずれとも一致しないようにする必要があります。
   d. ［管理者基本設定］セクションで、以下を行います。
      - ［優先組織の有効化］オプションをオンにし、優先組織リストから組織を選択します。この組織は、今後実行するすべての管理者関連タスクで選択されます。
      - 優先される日付/時刻形式を指定します。
      - 使用する管理コンソールのインスタンスで優先されるロケールを選択します。
      - ［タイム ゾーン］リストから必要なオプションを選択します。このタイム スタンプは、管理コンソールのヘッダにある最終ログイン情報に表示されます。
4. [保存]ボタンをクリックすると、プロファイル情報が変更されます。

基本ユーザ パスワード認証情報を使用する管理者の場合

次の手順に従ってください:

1. 管理コンソールにログインします。
2. **ヘッダ** フレームの *<ADMINISTRATORNAME>* リンクをクリックして、［マイ プロファイル］ページを表示します。
3. このページで、以下のように各セクション内の必要な設定を編集します。
   a. 必要に応じて、［個人情報］セクション内のフィールドを編集します。
   b. 現在のパスワードを変更する場合は、［**パスワードの変更**］セクションで［**現在のパスワード**］に入力し、［**新規パスワード**］フィールドと［**パスワードの確認**］フィールドに新しいパスワードを指定します。
   c. ［管理者基本設定］セクションで、以下を行います。
      - ［**優先組織の有効化**］オプションをオンにし、**優先組織**リストから組織を選択します。この組織は、今後実行するすべての管理者関連タスクで選択されます。
      - 優先される**日付/時刻形式**を指定します。
      - 使用する管理コンソールのインスタンスで優先される**ロケール**を選択します。
   d. ［**タイム ゾーン**］リストから必要なオプションを選択します。 このタイム スタンプは時間関連のフィールドで表示されます。 たとえば、管理コンソールのヘッダやあらゆるレポートの**最終ログイン**情報です。
4. ［保存］をクリックします。

管理者の検索

管理者を更新、アクティブ化、または非アクティブ化する必要がない限り、検索権限は必要ありません。 ただし、管理者が属する組織がスコープに含まれている*必要があります*。 たとえば、対象となる組織が UA の権限の範囲内に*あれば*、UA はその組織の管理者を検索できます。 管理者情報を暗号化された形式で格納する場合、部分的な検索機能はサポートされません。

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 管理者のリストを表示するための検索条件を指定します。以下の操作を行うことができます。
   - このページの各フィールドに管理者の情報の一部または全部を指定して管理者を検索する。
   - 組織の表示名を指定して管理者を検索する。
   - 何も条件を指定せずに［**検索**］ボタンをクリックするだけで管理者を検索する。
   - ［**詳細検索**］リンクをクリックして［詳細検索］ページを表示し、管理者の［ステータス］または［ロール］を指定して必要な管理者を検索する。

   注:［**ユーザ ステータス**］セクションで、ユーザ ステータス（［アクティブ］、［非アクティブ］、または［初期］）に基づいて［**現在のユーザ**］を検索できます。また、**削除されたユーザ**も検索できます。
4. アカウント ID に基づいて管理者を検索する場合は、［**アカウント別検索の有効化**］を選択します。
5. 管理者の必要な詳細を指定し、［**検索**］ボタンをクリックします。

   検索条件に一致する管理者のリストが表示されます。

管理者情報の更新

必要な権限

そのための適切な権限とスコープを持っていることを確認します。MA はすべての管理者を更新できます。 GA は、MA を*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）を更新できます。 OA は自分の権限の範囲内に含まれるほかのすべての OA と UA を更新できます。一方、UA は自分のスコープに含まれる自分のピアのみを更新できます。

管理者情報の更新

次の手順に従ってください:

1. ［ユーザと管理者］タブをクリックします。
2. ［ユーザと管理者の管理］セクションで［ユーザと管理者の検索］リンクをクリックし、対応するページを表示します。
3. 前のセクションの説明に従って情報を更新する管理者の情報の一部または全部を入力し、［検索］ボタンをクリックします。

   検索条件に一致する管理者のリストが表示されます。
4. 情報を編集する管理者の *<user name>* リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。

   注: 何らかのアカウント タイプが設定されている場合、このページには［ユーザ アカウント情報］（［アカウント タイプ］、［アカウント ID］、［ステータス］）も表示されます。
5. ［編集］ボタンをクリックし、以下の図に示すように、このページで管理者の情報を変更します。
6. ［ユーザ詳細］セクションで、必要なフィールド（［名］、［ミドル ネーム］、［姓］）を編集します。
7. ［**電子メール アドレス**］セクションで、組織に設定された電子メール タイプに対する電子メール アドレスを編集します。
8. ［**電話番号**］セクションで、組織に設定された電話タイプに対する電話番号を編集します。
9. ［**カスタム属性**］セクションで、カスタム属性の［**名**］および［**値**］を編集します。
10. ［**保存**］をクリックして変更した内容を保存し、［ユーザ情報］ページに戻ります。［**次へ**］ボタンをクリックして追加の設定に進みます。

注: ［**次へ**］ボタンが表示されない場合、アカウント タイプが組織に設定されていないことを意味します。 この場合は、［**管理者詳細の更新**］をクリックし、手順 14 に移動します。

［**次へ**］をクリックすると、［ユーザ アカウント］ページが表示されます。

11. ［**ユーザ アカウント**］セクションで、以下の操作を実行します。
    - ［**アカウント タイプ**］フィールドと［**ステータス**］フィールドを編集します。
    - ［**詳細属性**］を展開し、アカウント ID の **AccountID 属性**を追加します。
12. ［**管理者詳細の更新**］をクリックします。

    ［管理者の更新］ページが表示されます。
13. このページの［**ロール**］セクションで、［**ロール**］ドロップダウン リストを使用して管理者のロールを変更します。
14. ［**パスワードの設定**］セクションで、以下の操作を実行します。
    - 管理者の［**パスワード**］と［**パスワードの確認**］を設定します。
    - ［**ロック**］を選択して、管理者の認証情報を特定の期間ロックします。この期間は、［**認証情報ロック期間**］セクションの［**開始**］フィールドと［**終了**］フィールドで指定できます。
15. ［**管理する**］セクションで、以下の操作を実行します。
    - 管理者が管理する組織を選択します。 また、［**選択された組織**］から［**利用可能な組織**］に組織を移動させることにより、管理者のスコープから組織を削除できます。
16. ［**保存**］をクリックします。

アクティベーション コードの再生成

組織の認証メカニズムとして CA Strong Authentication のパスワードが使用されており、管理者がログインするために必要なアクティベーション コードを忘れた場合、その管理者から新しいアクティベーション コードの問い合わせを受けます。 そのような場合に新しいアクティベーション コードを生成します。

注: この情報は、CA Strong Authentication のパスワード メカニズムにのみ適用可能です。

必要な権限

アクティベーション コードを再生成できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。 MA はすべての管理者のアクティベーション コードを再生成できます。 GA は、MA を除き、自分のスコープに含まれるすべての管理者（ほかの GA を含む）を更新できます。 OA は自分の権限の範囲内に含まれるほかのすべての OA と UA を更新できます。一方、UA は自分のスコープに含まれる自分のピアのみを更新できます。

アクティベーション コードの再生成

次の手順に従ってください:

1. 「管理者情報の更新」の手順 2 ～手順 13 を実行して、［管理者の更新 (P. 229)］ページを表示します。
2. ［アクティベーション コード］セクションで、［アクティベーション コードの再生成］オプションを選択します。
3. ［保存］ボタンをクリックしてアクティベーション コードを生成します。

   新しいアクティベーション コードを含むメッセージが表示されます。

   新しいアクティベーション コードを管理者に送信します。

管理者の認証情報の更新

管理者は、システムに認証されるために認証情報を使用する必要があります。CA Strong Authentication は、管理者がすぐに使用できる Q&A、パスワード、および OTP の各認証情報をサポートしています。 管理者の認証情報を更新するには、［認証情報の詳細］ページを使用します。 このページでは、認証情報を有効または無効にしたり、認証情報の有効期限を延長したりできます。

必要な権限

そのための適切な権限とスコープを持っていることを確認します。 MA は認証情報を管理できません。 GA は、MA を*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）の認証情報を管理できます。 OA は、自分の権限の範囲内にあるほかのすべての OA と UA の認証情報を管理できます。 UA は、自身のスコープ内のピアの認証情報のみを管理できます。

管理者の認証情報の更新

次の手順に従ってください:

1. ［**認証情報の管理**］タブをアクティブにして、［認証情報の詳細］ページを表示します。
2. 目的の認証情報セクションの前にある矢印記号をクリックして、そのセクションを展開します。
3. 目的の認証情報の設定を変更します。 このページを使用して、以下の認証情報の設定を変更できます。
   - 認証情報のステータス
   - 認証情報の有効期限の延長
4. 変更した認証情報に対応する［**保存**］ボタンをクリックします。

管理者のロールをユーザへ変更

管理者のロールをユーザに変更することができます。 そのユーザの詳細は保持できますが、ユーザの管理者権限は削除する必要があります。

次の手順に従ってください:

1. 適切な権限で管理コンソールにログインします。
2. 「管理者情報の更新」の手順 2 ～手順 13 を実行して、［管理者の更新 (P. 232)］ページを表示します。
3. ［管理者の更新］ページで、［**ロールをユーザに変更**］をクリックします。
4. 表示される確認ダイアログ ボックスで［**OK**］をクリックします。

   以下のメッセージが表示されます。

   管理者を正常に降格しました。

管理者用のアカウント ID の設定

アカウント ID は、ユーザを識別するためのユーザ名とは別の ID です。 組織で使用するアカウント タイプを設定した後、これらのアカウント タイプに対して、ユーザごとにアカウント ID を 1 つ関連付けることができます。

必要な権限

ユーザ アカウントを更新するために必要な権限とスコープを持っていることを確認します。 MA は、すべてのユーザ アカウントを更新できます。 GA は、スコープ内のすべてのユーザ アカウントを更新できます。 OA と UA は、権限の範囲内でユーザ アカウントを更新できます。

アカウント ID の作成

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. アカウントを更新する管理者の情報の一部または全部を入力し、［**検索**］をクリックします。

   検索条件に一致する管理者のリストが表示されます。
4. アカウントを編集する管理者の <*ユーザ名*> リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。
5. ［**編集**］をクリックして、［管理者の更新］ページを表示します。
6. ［**次へ**］をクリックして、［ユーザ アカウント］ページを表示します。
7. アカウント ID を追加する［**アカウント タイプ**］を選択します。
8. テキスト ボックスに一意の**アカウント ID** を指定します。

   このアカウント タイプとアカウント ID の組み合わせは、ユーザを識別するためにユーザ名に加えて使用されます。
9. ドロップダウン リストからユーザ アカウントの**ステータス**を選択します。
10. （オプション）［**詳細属性**］セクションを展開し、作成しているアカウント ID のアカウント ID 属性とカスタム属性を指定します。

    注: アカウント ID には最大 3 つの属性を指定できます。
11. ［**追加**］をクリックして、アカウント ID を追加します。

アカウント ID の更新

注: アカウント ID を作成した後、それを変更することはできません。ユーザ アカウントのステータスを変更することと、アカウント ID 属性を追加することのみ可能です。

次の手順に従ってください:

1. アカウント ID 情報を更新する**アカウント タイプ**を選択します。
2. （オプション）ドロップダウン リストからユーザ アカウントの**ステータス**を変更します。
3. （オプション）［**詳細属性**］セクションを展開し、作成するアカウント ID の属性を指定します。
4. ［**更新**］をクリックします。

アカウント ID の削除

次の手順に従ってください:

1. アカウント ID を削除する**アカウント タイプ**を選択します。
2. ［**削除**］をクリックして、アカウント ID を削除します。

管理者の非アクティブ化

セキュリティ上の理由で管理者がシステムにログインすることを禁止する場合は、アカウントを削除する代わりに、非アクティブ化することができます。 管理者を永久的に非アクティブにすると、管理者はロックアウトされ、再度アクティブ化しない限りはログインできません。

必要な権限

そのための適切な権限とスコープを持っていることを確認します。 MA はすべての管理者を非アクティブ化できます。一方、GA は、MA を*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）を非アクティブ化できます。 OA は自分の権限の範囲内に含まれるほかのすべての OA と UA を非アクティブ化できます。一方、UA は自分のスコープに含まれる自分のピアのみを非アクティブ化できます。

管理者の永久的な非アクティブ化

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをアクティブにします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 非アクティブ化する管理者の情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、UA）に基づいてユーザを検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
4. 非アクティブにする管理者を 1 人以上選択します。
5. ［**非アクティブ化**］ボタンをクリックして、選択した管理者を非アクティブにします。

管理者の一時的な非アクティブ化

管理者を*一時的に非アクティブ化*することは、管理者の*非アクティブ化*と異なります。管理者の非アクティブ化の場合、管理者がアクセスできるようにする場合は常に手動で再度アクティブ化する必要があります（「管理者の非アクティブ化 (P. 236)」を参照）。

一時的な非アクティブ化では、ロック期間が終了すると管理者は自動的にアクティブ化されます。

管理者を一時的に非アクティブにするには、管理者によるアクセスをロックする**ロック開始日**と**ロック終了日**を指定する必要があります。 **ロック終了日**に到達すると、管理者のアクセスは自動的にアクティブ化されます。

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 非アクティブ化する管理者の情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、または UA）に基づいて［**現在のユーザ**］を検索することもできます。
4. ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 一時的に非アクティブにする管理者を 1 人以上選択します。
6. ［**一時的に非アクティブ化**］をクリックします。［ユーザを一時的に非アクティブ化］ダイアログ ボックスが表示されます。
7. ［**開始日**］セクションで、ロックを開始する**日付**と**時間**を選択します。
8. ［**終了**］セクションで、ロックを終了する**日付**と**時間**を選択します。
9. ［**保存**］をクリックして変更内容を保存します。

   注: **ロック開始日**の値を指定しないと、管理者のアクセスは現在の時刻からロックされます。 **ロック終了日**を指定しないと、管理者のアクセスは永久的にロックされます。

管理者のアクティブ化

非アクティブになっている管理者をアクティブにする必要がある場合があります。 たとえば、管理者が長期休暇を取っているときには、管理者を非アクティブにした方が良い場合があります。 これにより、その管理者のログインに対する不正アクセスを防止できます。

非アクティブ化されている管理者は、［ユーザと管理者の検索］ページで検索条件を指定して［**検索**］ボタンをクリックするだけでは直接検索できません。 このようなユーザの場合には、［**詳細検索**］を実行し、［**現在のユーザ**］セクションで［**非アクティブ**］オプションを使用して検索する必要があります。

必要な権限

管理者をアクティブ化できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。 MA はすべての管理者をアクティブ化できます。一方、GA は、MA を*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）をアクティブ化できます。OA は自分の権限の範囲内に含まれるほかのすべての OA と UA をアクティブ化できます。一方、UA は自分のスコープに含まれる自分のピアのみをアクティブ化できます。

管理者のアクティブ化

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. ユーザのステータス（アクティブまたは非アクティブ）に基づいてユーザを検索するため、［**詳細検索**］リンクをクリックします。

   ［詳細検索］ページが表示されます。
4. ［**ユーザ詳細**］セクションに管理者の情報の一部または全部を入力します。
5. ［**ユーザ ステータス**］セクションで、［**現在のユーザ**］に対して［**非アクティブ**］オプションと［**初期**］オプションを選択し、すべての非アクティブまたは初期状態の管理者を検索します。
6. ［**検索**］ボタンをクリックすると、検索条件と一致するすべての管理者のリストが表示されます。

7. アクティブにする管理者を選択します。
8. ［**アクティブ化**］をクリックして、管理者をアクティブにします。

管理者の削除

CA Strong Authentication の管理者情報には、個人情報、認証情報、およびアカウントが含まれます。 管理者を削除しても、それらの認証情報とアカウント情報は引き続きデータベースに保持されます。 データベースからこの情報を削除するには、AuthMinder ソフトウェア開発キットを使用します。

以前に削除した管理者と同じ名前の管理者を新しく作成しても、新しい管理者が、以前に削除した管理者の権限を自動的に引き継ぐことはありません。 削除した管理者を複製するには、すべての権限を手動で再作成します。

必要な権限

適切な権限があるかどうかの確認。 MA はすべての管理者を削除できます。 一方、GA は、MA を*除き*、自分のスコープに含まれるすべての管理者（ほかの GA を含む）を削除できます。 OA は、自分の権限の範囲内にあるほかのすべての OA と UA を削除できます。 ただし、UA はほかの UA を削除*できません*。

管理者の削除

次の手順に従ってください:

1. ［ユーザと管理者］タブをクリックします。
2. ［ユーザと管理者の管理］セクションで［ユーザと管理者の検索］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 削除する管理者の情報の一部または全部を入力し、［検索］をクリックします。

   ［詳細検索］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、UA）に基づいてユーザを検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
4. 削除する管理者を 1 人以上選択します。
5. ［Delete］をクリックします。

   注: 管理者を削除しても、その情報はデータベースに引き続き保持されます。

第 9 章: RADIUS 用に CA AuthMinder を設定する方法

管理者は、CA Strong Authentication を以下のいずれかのロールに対して設定できます。

- RADIUS クライアントからの認証リクエストを処理する RADIUS サーバとして

  以下に、CA Strong Authentication を RADIUS サーバとして設定した場合に発生するプロセスの概要を示します。

  1. RADIUS クライアントは CA Strong Authentication に認証リクエストを送信します。
  2. CA Strong Authentication は、ユーザを認証し、認証レスポンスを送信します。

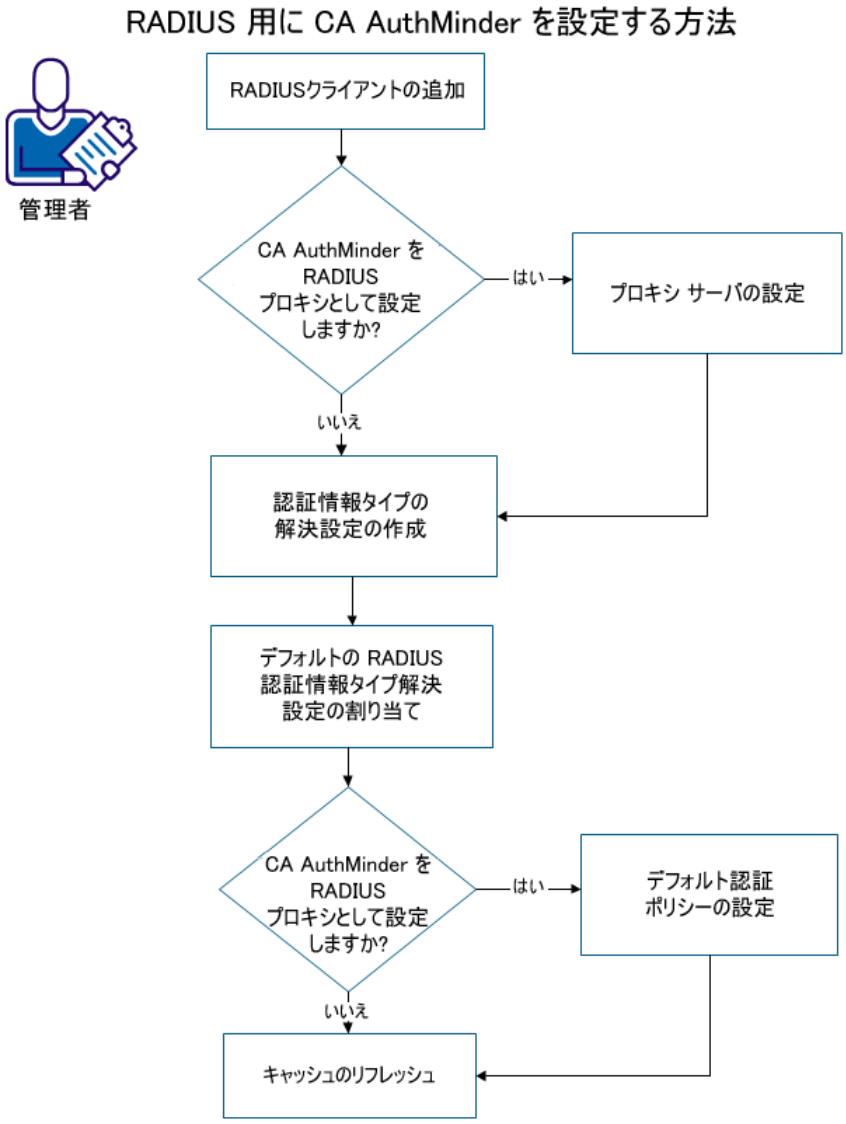
- 認証リクエストを既存の RADIUS サーバに渡すプロキシ サーバとして

  以下に、CA Strong Authentication を RADIUS サーバのプロキシ サーバとして設定した場合に発生するプロセスの概要を示します。

  1. RADIUS クライアントは CA Strong Authentication に認証リクエストを送信します。
  2. CA Strong Authentication に設定された認証ポリシーに基づいて、リクエストは RADIUS サーバに転送されます。 たとえば、ユーザまたはユーザの認証情報が CA Strong Authentication データベース内に見つからない場合に、認証リクエストを RADIUS サーバに転送するよう CA Strong Authentication を設定できます。

場合によっては、CA Strong Authentication を RADIUS サーバおよび RADIUS サーバへのプロキシとして設定します。たとえば、CA Strong Authentication を新たにインストールしたとします。 一部のユーザは CA Strong Authentication に移行され、残りのユーザは既存の RADIUS システムに存在しています。 この場合、CA Strong Authentication を RADIUS サーバおよび RADIUS サーバへのプロキシの両方として設定します。 CA Strong Authentication に移行されたユーザからの RADIUS 認証リクエストは CA Strong Authentication によって処理されます。 その他のすべてのユーザについては、認証情報が CA Strong Authentication データベース内に見つからないため、CA Strong Authentication は RADIUS 認証リクエストを既存の RADIUS サーバに転送します。

このシナリオでは、RADIUS に対して CA Strong Authentication を設定する手順について説明します。 以下の図は、この手順の概要を示しています。



次の手順に従ってください:

1. RADIUS クライアントを追加 (P. 245) します。
2. CA Strong Authentication を RADIUS サーバのプロキシとして設定する場合は、CA Strong Authentication をプロキシ サーバとして設定 (P. 249) します。
3. （オプション）認証情報タイプの解決設定を作成 (P. 251) します。
4. デフォルトの RADIUS 認証情報タイプ解決設定を割り当て (P. 254) ます。
5. RADIUS サーバのプロキシとして CA Strong Authentication を設定する場合は、デフォルト認証ポリシーを設定 (P. 255) します。
6. キャッシュをリフレッシュします。

RADIUS クライアントの追加

CA Strong Authentication には単一の RADIUS クライアントを設定できます。CA Strong Authentication 内の複数の組織で同じ RADIUS クライアントを使用するよう設定するには、グローバル レベルで RADIUS クライアントを追加します。 それ以外の売亜は、単一の組織に対して RADIUS クライアントを追加します。

次の手順に従ってください:

1. 管理コンソールにログインします。
2. グローバル レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
   b. ［CA Strong Authentication］タブが選択されていることを確認します。
3. 組織レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. ［組織］タブをクリックします。
   b. 組織を検索します。
   c. 検索結果から組織を選択します。
   d. ［CA Strong Authentication］タブをクリックします。

4. 左側のペインで、［RADIUS クライアント］をクリックします。
5. ［追加］をクリックします。
6. 以下の情報を入力します。

RADIUS クライアント IP アドレス

CA Strong Authentication サーバに対するユーザ認証に使用する RADIUS クライアントの IP アドレスを指定します。

共有秘密キー

RADIUS クライアントと CA Strong Authentication サーバの間の共有秘密キーを指定します。

注: キーの最小長は 1 文字で、最大長は 512 文字です。

Description

RADIUS クライアントの簡潔な説明を指定します。 複数のクライアントを設定する場合、各クライアントの説明はクライアントを区別するのに役立ちます。

認証タイプ

RADIUS ベースのアクセスに使用される認証メカニズムを示します。以下のいずれかの認証メカニズムを選択します。

- **RADIUS OTP**

  RADIUS リクエストの認証に使用するデフォルトの認証メカニズムです。 ワンタイム トークン（OTT）は認証のパスワードとして使用されます。

- **インバンド パスワード**

  どのパスワードまたは OTP も認証に使用できることを指定します。 通常、［インバンド パスワード］オプションは以下のシナリオで使用されます。

  認証情報タイプを解決するため

  認証情報タイプ解決を使用して設定された認証情報を持つユーザを認証する場合は、インバンド パスワード オプションを使用します。

  注: 認証情報タイプ解決を設定し、不明な認証情報タイプがある入力リクエストを特定のパスワード ベース認証メカニズムにマップするか、または RADIUS に対してあらゆるパスワード ベース認証メカニズムをサポートします。

  （グローバル設定のみに適用されるオプション）組織名を指定するため

  RADIUS リクエストでは、<orgname>¥n<password> 形式で組織情報とパスワードを送信できます。 AuthMinder は、この形式で指定されたパスワードから組織名を抽出できます。この機能の使用を有効にするには、組織と RADIUS クライアントを以下のように関連付けます。

  a. ［>］ボタンを使用して、必要な組織を［利用可能な組織］リストから［サポートされている組織］リストに移動させます。

  b. RADIUS クライアントのデフォルト組織を指定します。 組織情報がパスワードと共に送信されない場合、このデフォルト組織がユーザ詳細を解決するための認証で考慮されます。

- **EAP**： このオプションは現在サポートされていません。 したがって、このオプションは選択しないでください。

7. ［RADIUS 再試行処理］セクションで、以下を指定します。
   - RADIUS クライアントでレスポンスが受信されない場合に AuthMinder サーバにリクエストを再送信するようにしたいときは、［再試行の有効化］オプションを選択します。
   - ［再試行ウィンドウ］フィールドで、クライアントがレスポンスが受信されない場合に AuthMinder サーバへの接続を再試行できる期間を秒で入力します。 この期間が過ぎた後は、再試行は無効と見なされます。 再試行が可能な期間がクライアントのタイムアウト期間より長くなるようにします。
8. ［RADIUS レスポンス追加属性］セクションで、AuthMinder サーバが RADIUS クライアントに送信するレスポンスに含めたい属性を指定します。

   属性 ID

   一意の属性識別子を指定します。

   例： 26

   属性値

   属性 ID に対応する値を指定します。 静的な値または変数（たとえばユーザ属性やカスタム属性）、静的な値と変数の組み合わせを指定できます。 たとえば、JSmith というユーザが存在し。カスタム ユーザ属性のキーと値のペアが「Employee ID=150」である場合、以下のように RADIUS レスポンスに従業員 ID が含まれるように指定できます。

   ```
   JSmith = $$Employee ID$$
   ```

   この設定により、JSmith = 150 が返ります。
9. ［RADIUS パケット ドロップ オプション］セクションで、AuthMinder サーバが RADIUS パケットをドロップする必要があるイベントを選択します。 以下のイベントの任意の組み合わせを選択できます。
   - 見つからないユーザ
   - 見つからない認証情報
   - 無効なリクエスト
   - 内部エラー
10. ［追加］をクリックします。

RADIUS クライアントが追加されました。この設定は、キャッシュをリフレッシュした後に有効になります。

プロキシ サーバとしての AuthMinder の設定

RADIUS サーバのプロキシ サーバとして CA Strong Authentication を設定します。

注: このセクションに記載されている手順は、RADIUS プロキシとして CA Strong Authentication を設定する場合にのみ実行します。

次の手順に従ってください:

1. グローバル レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
   b. ［CA Strong Authentication］タブが選択されていることを確認します。
2. 組織レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. ［組織］タブをクリックします。
   b. 組織を検索します。
   c. 検索結果から組織を選択します。
   d. ［CA Strong Authentication］タブをクリックします。
3. 左側のペインで、［RADIUS プロキシ］をクリックします。
4. ［プロキシの有効化］を選択します。
5. 複数の組織が RADIUS 用プロキシ サーバとして CA Strong Authentication を使用する場合は、［グローバル設定の使用］チェックボックスをオンにします。

6. ［プライマリ プロキシ サーバ詳細］セクションで、RADIUS サーバの以下の詳細を入力します。

   IP アドレス

   RADIUS サーバの IP アドレスを指定します。

   RADIUS ポート

   RADIUS サーバがリスンするポート番号を指定します。

   共有秘密キー

   CA Strong Authentication サーバと RADIUS サーバの間の共有秘密キーを指定します。

   注: キーの最小長は 1 文字で、最大長は 512 文字です。

   Description

   RADIUS サーバを説明する文字列を入力します。 複数のサーバが設定されている場合、この説明は RADIUS サーバの識別に役立ちます。

   読み取りタイムアウト

   CA Strong Authentication が RADIUS サーバからのレスポンスを待つ必要がある最大時間をミリ秒単位で指定します。

   再試行回数

   CA Strong Authentication サーバがレスポンスを受信しなかった場合に、RADIUS サーバへのリクエストの送信を試行する回数を入力します。

7. ［RADIUS レスポンス追加属性］セクションで、認証の成功後に CA Strong Authentication サーバが RADIUS サーバに送信するリクエストに含めたい属性を指定します。

   属性 ID

   一意の属性識別子をこの列に指定します。 たとえば、「26」などです。

   属性値

   属性 ID に対応する値を指定します。 たとえば、属性 ID 26 に対応する値などです。

8. （オプション）さらに属性を追加する場合は、［さらに追加］をクリックします。

9. （オプション）追加の RADIUS サーバを設定する場合は、［バックアップ プロキシ サーバ詳細］セクションにそのサーバの詳細を指定します。

CA Strong Authentication は、事前に設定された再試行回数に到達した後、RADIUS 認証リクエストをこのバックアップ RADIUS サーバに転送します。

10. ［更新］をクリックして変更を保存します。

    CA Strong Authentication は RADIUS サーバ用プロキシ サーバとして設定されました。

認証情報タイプ解決設定を作成または更新します

このセクションに記載されている手順は、RADIUS クライアントの追加時に認証タイプとして［インバンド パスワード］オプションを設定した場合にのみ実行します。

認証情報タイプ解決を設定し、インバンド パスワードを以下のいずれかの認証タイプにマップできます。

- Password
- CA Mobile OTP （ArcotOTP-OATH） CA Mobile OTP （ArcotOTP-OATH）
- OATH OTP トークン
- OTP/アクティベーション コード
- CA Mobile OTP （ArcotOTP-EMV）
- RADIUS OTP
- LDAP パスワード
- ネイティブ トークン

CA Strong Authentication では、以下の事前定義済み認証情報タイプ解決が使用可能です。

- VerifyArcotOTP-EMV
- VerifyArcotOTP-OATH
- VerifyLDAPPassword
- VerifyNativeToken
- VerifyOATH
- VerifyOTP
- VerifyOTT
- VerifyPassword

これらの事前定義済み認証情報タイプ解決設定のいずれかがインバンドパスワードの処理に対する要件を満たす場合、このセクションに記載されている手順を実行する必要はありません。 これらの事前定義済み設定のどれも要件を満たさない場合にのみ、この手順を実行します。

認証情報タイプ解決は組織のデフォルトとして割り当てます。 認証情報タイプ解決をユーザごとに設定することもできます。そのためには、各ユーザに使用されるメカニズムを指定するカスタム ユーザ属性を設定します。このカスタム ユーザ属性は認証情報タイプ解決設定に含まれます。

次の手順に従ってください:

1. グローバル レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
   b. ［CA Strong Authentication］タブが選択されていることを確認します。
2. 組織レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. ［組織］タブをクリックします。
   b. 組織を検索します。
   c. 検索結果から組織を選択します。
   d. ［CA Strong Authentication］タブをクリックします。

3. 左ペインで［認証情報タイプ解決］をクリックします。

   ［認証情報タイプ解決設定］画面が表示されます。

4. ［作成］をクリックします。
5. 設定の名前を入力します。
6. 既存の設定をコピーする場合は、以下の手順に従います。
   a. ［設定のコピー］チェック ボックスをオンにします。
   b. ［利用可能な設定］ドロップダウン リストから、コピーする設定を選択します。
7. ［プレーン解決先］ドロップダウン リストから、受信パスワード タイプ認証情報をマップする認証情報タイプを選択します。
8. （オプション）認証情報タイプの指定でカスタム ユーザ属性を作成した場合は、そのカスタム属性の名前を［認証情報タイプ用のユーザ カスタム属性］フィールドに指定します。

   RADIUS 認証リクエストを受信すると、このカスタム ユーザ属性で指定された認証情報タイプが、前の手順で設定された認証情報タイプより優先されます。認証情報タイプがカスタム ユーザ属性に指定されていない場合、前の手順で設定された認証情報タイプがデフォルトの認証情報タイプとして使用されます。

   ユーザが作成されている場合、カスタム ユーザ属性の値が以下のいずれかの整数値に設定されていることを確認します。

   - パスワード： 1
   - CA Mobile OTP（ArcotOTP-OATH）CA Mobile OTP（ArcotOTP-OATH）： 8
   - OATH OTP トークン： 7
   - OTP/アクティベーション コード： 4
   - CA Mobile OTP （ArcotOTP-EMV） ： 8
   - RADIUS OTP： 5
   - LDAP パスワード： 10
   - ネイティブ トークン： 11

   たとえば、カスタム ユーザ属性によって認証情報タイプとして OATH OTP トークン を指定する場合、カスタム ユーザ属性の値として 7 が設定されていることを確認します。

9. ［保存］をクリックします。

   認証情報タイプ解決設定が保存されます。

デフォルトの RADIUS 認証情報タイプ解決設定の割り当て

このセクションに記載されている手順は、RADIUS クライアントの追加時に認証タイプとして［インバンド パスワード］オプションを設定した場合にのみ実行します。

認証情報タイプ解決設定を、RADIUS クライアントによって送信された認証リクエストのデフォルト設定として指定します。

次の手順に従ってください:

1. グローバル レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
   b. ［CA Strong Authentication］タブが選択されていることを確認します。
2. 組織レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. ［組織］タブをクリックします。
   b. 組織を検索します。
   c. 検索結果から組織を選択します。
   d. ［CA Strong Authentication 設定］タブをクリックします。
3. 左ペインで［デフォルト設定の割り当て］をクリックします。
4. ［RADIUS 認証情報タイプ解決設定］ドロップダウン リストから、インバンド パスワードの処理に対して使用する認証情報タイプ解決設定を選択します。
5. ［保存］をクリックします。

   デフォルトの RADIUS 認証情報タイプ解決設定が割り当てられます。

デフォルト認証ポリシーの設定

RADIUS プロキシとして CA Strong Authentication を設定している場合は、RADIUS プロキシとして CA Strong Authentication を設定している認証情報タイプ用の認証ポリシーを作成または更新します。 その認証情報タイプに対するデフォルト認証ポリシーとしてこのポリシーを設定します。 認証ポリシーは、認証リクエストが CA Strong Authentication によって RADIUS サーバに転送される必要がある条件を指定します。

注: このセクションに記載されている手順は、RADIUS プロキシとして CA Strong Authentication を設定する場合にのみ実行します。 RADIUS サーバとして CA Strong Authentication を設定する場合はこの手順を実行しないでください。

次の手順に従ってください:

1. グローバル レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
   b. ［CA Strong Authentication］タブが選択されていることを確認します。
2. 組織レベルで RADIUS クライアントを追加するには、以下の手順に従います。
   a. ［組織］タブをクリックします。
   b. 組織を検索します。
   c. 検索結果から組織を選択します。
   d. ［CA Strong Authentication］タブをクリックします。

3. 左ペインで、RADIUS プロキシ サーバとして CA Strong Authentication を設定している認証情報タイプに対する［*認証*］リンクをクリックします。

   ［パスワード認証ポリシー］画面が表示されます。

4. ポリシー設定を作成するには［作成］をクリックします。 あるいは、既存のポリシー設定を更新する場合は［更新］をクリックします。

5. ［ポリシー設定］セクションの残りのフィールドに必要なデータを入力します。

   注: ［ポリシー設定］セクションのフィールドに関する詳細情報については、「CA Strong Authentication 管理ガイド」を参照してください。

6. ［詳細設定］を展開します。

7. 以下のいずれかまたは両方のオプションを選択します。

   見つからないユーザ

   ユーザが CA Strong Authentication データベースに存在しない場合、認証リクエストを RADIUS サーバに転送する必要があることを指定します。

   見つからない認証情報

   ユーザが認証しようとしている認証情報が CA Strong Authentication データベースに存在しない場合、認証リクエストを RADIUS サーバに転送する必要があることを指定します。

8. ［詳細設定］セクションの残りのフィールドに必要なデータを入力します。

9. ［保存］をクリックします。

   認証ポリシーが設定されます。

キャッシュのリフレッシュ

すべての設定を有効にするには、キャッシュをリフレッシュします。

次の手順に従ってください:

1. ［システム設定］セクションで、［サービスおよびサーバの設定］、［管理コンソール］、［キャッシュのリフレッシュ］を選択します。

   ［キャッシュのリフレッシュ］画面が表示されます。

2. 単一の組織または複数の組織のどちらに CA Strong Authentication を RADIUS サーバとして設定しているかに応じて、以下のオプションのいずれかまたは両方を選択します。

   - システム設定をリフレッシュ
   - 組織設定をリフレッシュ

3. ［OK］をクリックします。

   リクエストが正常にサブミットされたことを示すメッセージが表示されます。

4. ［サービスおよびサーバの設定］、［管理コンソール］、［キャッシュ リフレッシュ ステータスの確認］を選択します。

   ［キャッシュ リフレッシュ リクエストの検索］画面が表示されます。

5. リフレッシュ リクエストのリクエスト ID を選択し、次に［検索］をクリックします。

   リフレッシュ リクエストのステータスが表示されます。［ステータス］列に SUCCESS メッセージがあれば、設定が有効になったことを示します。

第 10 章: ユーザと認証情報の管理

CA Strong Authentication はユーザのアプリケーションと連携して動作し、管理者とエンドユーザのための強い認証を管理します。 CA Strong Authentication では、管理コンソールを使用してエンドユーザを直接作成できます。 CA Strong Authentication ユーザを作成するこのプロセスは*移行*と呼ばれます。

注: ユーザ登録のワークフローを理解するには、「*CA Strong Authentication Web サービス開発者ガイド*」の「登録ワークフロー」を参照してください。

ユーザ情報を管理することは、安全なシステムを維持するために非常に重要です。

ユーザの作成

GA （グローバル管理者）、OA （組織管理者）、および UA （ユーザ管理者）は、自分のスコープ内に組織のユーザを作成できます。

ユーザを作成するために、ユーザの名および姓を指定することは必須ではありません。

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで、［**ユーザの作成**］リンクをクリックし、［ユーザの作成］ページを表示します。
3. ［**ユーザ詳細**］セクションで、ユーザの詳細を入力します。

   User Name

   一意のユーザ名。

   組織

   ユーザが属する組織の表示名。

   ［First Name］

   ユーザの名。

   ［Middle Name］

   ユーザのミドル ネーム（ある場合）。

   ［Last Name］

   ユーザの姓。
4. ［**電子メール アドレス**］セクションで、ユーザの**電子メール** アドレスを入力します。
5. ［**電話番号**］セクションで、ユーザに問い合わせるための**電話番号**を入力します。
6. ユーザを**初期**状態にするか、**アクティブ**状態にするかを選択します。
7. ［**カスタム属性**］セクションで、個人の電子メール アドレスや自宅の電話番号のように、追加したい任意の属性の**名前**と**値**を入力します。
8. ［**ユーザの作成**］をクリックして、ユーザを作成します。

ユーザの検索

必要な権限

ユーザの作成、更新、アクティブ化、または非アクティブ化を行う必要がない場合は、検索権限は必要ありません。 ただし、ターゲット ユーザが属する組織に対するスコープを持つ*必要があります*。たとえば、組織の GA は、他の組織が権限の範囲内である場合には、その組織のユーザを検索できます。

ユーザの検索

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 検索するユーザの条件を指定します。以下の操作を行うことができます。
   - このページのフィールドでユーザの部分的または完全な情報を指定してユーザを検索します。

   注: フィールドに暗号化のためのマークがされていない場合のみ、フィールドに部分的な情報を指定できます。 このページのいずれかのフィールドに暗号化のマークがされている場合、正しく機能するためには、検索する完全な値を指定する必要があります。

   - 組織の表示名を指定してユーザを検索します。
   - 基準は何も指定せず、［**検索**］をクリックするだけでユーザを検索します。
   - ［**詳細検索**］リンクをクリックすると、［詳細検索］ページが表示されます。ステータスまたはロールを指定してユーザを検索します。
4. ユーザに関する必要な詳細情報を指定し、［**検索**］をクリックします。

   検索条件に一致したユーザのリストが表示されます。

ユーザ情報の更新

ユーザ情報を更新できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。 MA は、すべてのユーザを更新できます。 GA は、自分のスコープに含まれるすべてのユーザを更新できます。 OA と UA は、権限の範囲内でユーザを更新できます。

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 前のセクションの説明に従って情報を更新するユーザの情報の一部または全部を入力し、［**検索**］ボタンをクリックします。

   検索条件に一致する管理者とユーザのリストが表示されます。
4. 情報を編集するユーザの *<user name>* リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。

   注: 何らかのアカウント タイプが設定されている場合、このページには［**ユーザ アカウント情報**］（［**アカウント タイプ**］、［**アカウント ID**］、［**ステータス**］）も表示されます。
5. ［**編集**］をクリックし、このページのユーザ情報を変更します。
6. ［**ユーザ詳細**］セクションで、必要なフィールド（［**名**］、［**ミドル ネーム**］、［**姓**］）を編集します。
7. ［**電子メール アドレス**］セクションで、組織に設定された電子メール タイプに対する電子メール アドレスを編集します。
8. ［**電話番号**］セクションで、組織に設定された電話タイプに対する電話番号を編集します。
9. （オプション）［**ユーザ ステータス**］を更新します。
10. （オプション）［**カスタム属性**］の**名前**および**値**を編集します。
11. ［**保存**］をクリックして変更保存し、［ユーザ情報］ページに戻ります。 ［**次へ**］ボタンをクリックして追加の設定に進みます。

    ［**次へ**］をクリックすると、［ユーザ アカウント］ページが表示されます。
12. ［**ユーザ アカウント**］セクションで、以下の操作を実行します。

- （オプション）［**アカウント タイプ**］を選択し、［**ステータス**］を編集します。
- ［**詳細属性**］を展開し、アカウント ID の［**AccountID 属性**］と［**カスタム属性**］を追加します。

注: これが作成する最初のアカウント ID である場合は、［**追加**］をクリックしてアカウント ID を追加してから更新します。

管理者へのユーザの昇格

必要な権限

そのための適切な権限とスコープを持っていることを確認します。 MA は、すべてのユーザのレベルを上げることができます。 GA は、管理権限の範囲内で、ユーザを組織の OA、UA、GA のレベルに上げることができます。 OA は、管理権限の範囲内で、ユーザを組織の OA または UA のレベルに上げることができます。 UA は、ユーザを管理者レベルに上げることが できません。

管理者へのユーザの昇格

次の手順に従ってください:

1. ［ユーザと管理者］タブをクリックします。
2. ［ユーザと管理者の管理］セクションで［ユーザと管理者の検索］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 前のセクションの説明に従ってレベルを上げるユーザの情報の一部または全部を入力し、［検索］ボタンをクリックします。

   検索条件に一致する管理者とユーザのリストが表示されます。
4. レベルを上げるユーザの <user name> リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。
5. ［編集］をクリックし、［ユーザ情報］ページを表示します。
6. ユーザの［名］、［姓］、［電子メール アドレス］、［電話番号］が指定されていない場合は、これらを入力します。 これらの属性は管理者にとって必須です。
7. ユーザの［電子メール］が指定されていない場合、電子メール アドレスを入力します。 この属性は管理者にとって必須です。
8. ［次へ］をクリックして、［ユーザ アカウント］ページを表示します。

   注: ユーザの組織に対してアカウント タイプが設定されていない場合は、［ロールを管理者に変更］ボタンが［ユーザの更新］ページに表示されます。
9. ［ユーザ アカウント］ページで、［ロールを管理者に変更］をクリックして、［管理者の作成］ページを表示します。
10. このページで、以下を実行します。

- ［ロール］ドロップダウン リストから新しい管理者のロールを指定します。
- ［パスワード］フィールドと［パスワードの確認］フィールドに管理者のパスワードを入力します。

注: 組織が CA Strong Authentication ユーザ パスワード認証に対して設定されている場合、これらのフィールドは表示されません。

- ［管理対象］セクションで、管理者のスコープ内にある組織を選択します。 以下の手順のいずれかを実行します。
  - この管理者にシステム内の現在および将来の組織をすべて管理させる場合は、［全組織］オプションを選択します。
  - ［利用可能な組織］リストから必要な組織を選択し、［>］ボタンをクリックしてそれらの組織を［選択された組織］リストに追加します。

  ［利用可能な組織］には、ログインしている管理者のスコープで利用可能なすべての組織が表示されます。 ［選択された組織］には、管理者の管理対象として選択した組織のリストが表示されます。

11. ［作成］をクリックして、変更の保存、管理者の作成およびアクティブ化を行います。

    注: レベルを上げるユーザが CA Strong Authentication ユーザ パスワード認証を使用する組織に属している場合は、［**作成**］をクリックした後にアクティベーション コードが生成されます。 これは、管理者に昇格したユーザが、管理コンソール にログインするときに使用します。

ユーザのアカウント ID の設定

アカウント ID （*アカウント*とも呼ばれます）は、ユーザを識別するためのユーザ名とは別の ID です。 組織で使用するアカウント タイプを設定した後、これらのアカウント タイプに対して、ユーザごとにアカウント ID を 1 つ関連付けることができます。

必要な権限

ユーザ情報を更新するための適切な権限およびスコープを持っていることを確認します。 MA は、すべてのユーザを更新できます。 GA は、自分のスコープに含まれるすべてのユーザを更新できます。 OA と UA は、権限の範囲内でユーザを更新できます。

アカウントの作成

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. アカウント ID を作成するユーザの情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、または UA）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
4. 編集するアカウントのユーザの <*ユーザ名*> リンクをクリックします。

   ［基本ユーザ情報］ページが表示されます。

   注: このページには、設定されているアカウント タイプの［**ユーザ アカウント情報**］（［**アカウント タイプ**］、［**アカウント ID**］、［**ステータス**］）も表示されます。
5. ［**編集**］をクリックして、［ユーザの更新］ページを表示します。
6. ［**次へ**］をクリックして、［ユーザ アカウント］ページを表示します。
7. アカウント ID を追加する［**アカウント タイプ**］を選択します。
8. テキスト ボックスに一意の**アカウント ID** を指定します。

   このアカウント タイプとアカウント ID の組み合わせは、ユーザを識別するためにユーザ名に加えて使用されます。アカウント タイプとアカウント ID の組み合わせが特定の組織にとって一意であることを確認します。
9. ドロップダウン リストからユーザ アカウントの**ステータス**を選択します。
10. （オプション）［詳細属性］セクションを展開し、以下の手順を実行します。
    a. 作成しているアカウント ID に属性値を入力します。

       注: アカウント ID には最大 3 つの属性を指定できます。
    b. アカウント タイプに対して設定する**カスタム属性**の値を指定します。

11. ［**追加**］をクリックして、アカウント ID を追加します。

アカウントの更新

アカウントが作成された後にアカウント ID を変更することはできません。ユーザ アカウントのステータスの変更、アカウント ID 属性およびカスタム属性を追加または削除のみが可能です。

次の手順に従ってください:

1. 「アカウントの作成 (P. 266)」の手順 1 ～手順 7 を実行して、［ユーザ アカウント］ページを表示します。
2. アカウント ID を更新する［**アカウント タイプ**］を選択します。
3. （オプション）ドロップダウン リストからユーザ アカウントの**ステータス**を変更します。
4. （オプション）［**詳細属性**］セクションを展開し、更新しているアカウント ID の**アカウント ID 属性**と**カスタム属性**を指定します。
5. ［**更新**］をクリックして、変更内容を保存します。

アカウントを削除する

次の手順に従ってください:

1. 「アカウントの作成 (P. 266)」の手順 1 ～手順 7 を実行して、［ユーザ アカウント］ページを表示します。
2. アカウント ID を削除する**アカウント タイプ**を選択します。
3. ［**削除**］をクリックして、アカウント ID を削除します。

ユーザ認証情報の更新

ユーザは、システムに認証されるために認証情報を使用します。

注: ユーザの認証情報を更新するには、更新するための適切な権限とスコープを持っていることを確認します。 MA は認証情報を管理できません。 GA は、スコープ内のほかの GA を含むすべてのユーザの認証情報を管理できます。 OA と UA は、権限の範囲内のすべてのユーザの認証情報を管理できます。

次の手順に従ってください:

1. 「ユーザ情報の更新 (P. 262)」の手順 2 ～手順 5 を実行します。
2. ［認証情報の管理］タブをクリックして、［認証情報の詳細］ページを表示します。
3. 選択したユーザのすべての認証情報を同じステータスに設定するには、［すべての認証情報］セクションを使用してこれを行うことができます。 以下の手順に従います。
   a. ［すべての認証情報］セクションを展開します。これをするには、左横の矢印記号をクリックします。
   b. 以下のいずれかのオプションを選択します。

      注: 認証情報が検証済み状態である場合、これらのステータスは OTP に適用されません。

      - **有効化**： ユーザのすべての認証情報を有効にします。 たとえば、ユーザの認証情報がロックされている場合は、このオプションでそれらを有効にできます。
      - **無効期間の有効化とリセット**: 無効になっている認証情報を有効にし、無効期間をリセットします。 たとえば、ユーザが休暇中でアカウントが無効のとき、このユーザの無効期間の終了日より前にこのユーザの認証情報を有効にしたい場合は、このオプションを使用して認証情報を有効にし、無効期間をリセットすることができます。
      - **無効化**： ユーザのすべての認証情報を無効にします。
      - **一定期間無効化**: ユーザのすべての認証情報を、指定した期間において無効にします。

   c. このセクションに対応する［保存］ボタンをクリックします。
4. 認証情報ごとに異なる設定を適用するには、以下の手順に従います。

a. 目的の認証情報セクションの前にある矢印記号をクリックして、そのセクションを展開します。

   注: ユーザが同じタイプの複数の認証情報を所有している場合、それらの認証情報ごとに別々のセクション（<*認証情報タイプ*> <（使用タイプ）>）が表示されます。

b. 目的の認証情報の設定を変更します。 このページを使用して、以下の認証情報の設定を変更できます。

   - 認証情報のステータス
   - 認証情報の有効期限の延長
   - 既存の認証情報のカスタム属性の追加または変更

   注: OATH OTP トークン 認証情報の場合は、廃棄されたトークンの再利用、新しいトークンの割り当て、トークンの割り当て解除、CA Strong Authentication サーバが生成する OATH OTP トークン とベンダー トークン ID の関連付け、OATH OTP トークン の同期を実行できます。

c. 変更した認証情報に対応する［保存］ボタンをクリックします。

ユーザの非アクティブ化

セキュリティ上の理由でユーザがシステムにログインすることを禁止する場合は、アクセスを削除するのではなく、非アクティブ化することができます。 ユーザを非アクティブにすると、ユーザはシステムからロックされ、再度アクティブ化するまでログインできなくなります。

必要な権限

そのための適切な権限とスコープを持っていることを確認します。 MA はすべてのユーザを非アクティブ化できます。GA はスコープ内のほかの GA を含むすべてのユーザを非アクティブ化できます。 OA と UA は、権限の範囲内ですべてのユーザを非アクティブ化できます。

ユーザの非アクティブ化

次の手順に従ってください:

1. ［ユーザと管理者］タブをクリックします。
2. ［ユーザと管理者の管理］セクションで［ユーザと管理者の検索］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 非アクティブ化するユーザの情報の一部または全部を入力し、［検索］をクリックします。

   ［詳細検索］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、UA）に基づいてユーザを検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
4. 非アクティブにするユーザを 1 人以上選択します。
5. ［非アクティブ化］ボタンをクリックして、選択したユーザを非アクティブにします。

ユーザの一時的な非アクティブ化

ユーザを*一時的に非アクティブ化*することは、ユーザの*非アクティブ化*と異なります。ユーザの非アクティブ化の場合、システムにアクセスできるようにする場合は常に手動で再度アクティブ化する必要があります（「ユーザの非アクティブ化 (P. 270)」を参照）。

一時的な非アクティブ化では、ロック期間が終了するとユーザは自動的にアクティブ化されます。

次の手順に従ってください:

1. ユーザを一時的に非アクティブ化するために必要な権限とスコープでログインしていることを確認します。
2. ［**ユーザと管理者**］タブをアクティブにします。
3. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
4. 一時的に非アクティブ化するユーザの情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックして、ユーザのステータス（アクティブまたは非アクティブ）またはユーザのロール（GA、OA、または UA）に基づいて［**現在のユーザ**］を検索することもできます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
5. 一時的に非アクティブにするユーザを 1 人以上選択します。
6. ［**一時的に非アクティブ化**］をクリックします。［ユーザを一時的に非アクティブ化］ダイアログ ボックスが表示されます。
7. ［**開始日**］セクションで、ロックを開始する**日付**と**時間**を選択します。
8. ［**終了**］セクションで、ロックを終了する**日付**と**時間**を選択します。
9. ［**保存**］をクリックして変更内容を保存します。

   注: **ロック開始日**の値を指定しないと、ユーザのアクセスは現在の時刻からロックされます。**ロック終了日**を指定しないと、ユーザのアクセスは永久的にロックされます。

ユーザのアクティブ化

非アクティブになっているユーザをアクティブにできます。

非アクティブ化されているユーザは、［ユーザと管理者の検索］ページで検索条件を指定して［**検索**］ボタンをクリックするだけでは直接検索できません。 このようなユーザの場合には、［**詳細検索**］を実行し、［**現在のユーザ**］セクションで［**非アクティブ**］オプションを使用して検索する必要があります。

必要な権限

そのための適切な権限とスコープを持っていることを確認します。MA はすべてのユーザをアクティブ化できます。GA はスコープ内のすべてのユーザをアクティブ化できます。 OA と UA は、権限の範囲内ですべてのユーザをアクティブ化できます。

ユーザのアクティブ化

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. ［**詳細検索**］リンクをクリックして、ステータス（アクティブまたは非アクティブ）に基づいて［**現在のユーザ**］を検索します。

   ［詳細検索］ページが表示されます。
4. ［**ユーザ アカウント**］セクション内にユーザの部分的または完全な情報を入力します。
5. ［**ユーザ ステータス**］セクションで、［**現在のユーザ**］に対して［**非アクティブ**］オプションと［**初期**］オプションを選択し、すべての非アクティブまたは初期状態のユーザを検索します。
6. ［**検索**］をクリックすると、検索条件に一致するすべてのユーザのリストが表示されます。
7. アクティブにするユーザを選択します。
8. ［**アクティブ化**］をクリックして、ユーザをアクティブ化します。

ユーザの削除

ユーザを削除すると、すべての権限が永久的に削除されます。ユーザは、アプリケーションにログインできなくなります。 そのユーザの情報と認証情報はシステムから削除されます。

以前に削除したユーザと同じ名前のユーザを新しく作成しても、新しいユーザが、以前に削除したユーザの権限を自動的に引き継ぐことは*ありません*。 削除したユーザを複製するには、すべての権限を手動で再作成します。

必要な権限

適切な権限およびスコープを持っていることを確認します。MA はすべてのユーザを削除できます。一方、GA は、MA を*除き*、自分のスコープに含まれるすべてのユーザ (ほかの GA を含む) を削除できます。OA と UA は、権限の範囲内ですべてのユーザを削除できます。

ユーザの削除

次の手順に従ってください:

1. ［**ユーザと管理者**］タブをクリックします。
2. ［**ユーザと管理者の管理**］セクションで［**ユーザと管理者の検索**］リンクをクリックし、［ユーザと管理者の検索］ページを表示します。
3. 削除するユーザの情報の一部または全部を入力し、［**検索**］をクリックします。

   ［**詳細検索**］リンクをクリックすると、ステータス（アクティブまたは非アクティブ）、またはロール（ユーザ）に基づいてユーザを検索できます。

   ［検索結果］ページに、指定した条件に一致するすべてのユーザが表示されます。
4. 削除するユーザを 1 人以上選択します。
5. ［**削除**］をクリックします。

   注: ユーザを削除すると、その情報はデータベースから削除されます。ユーザの履歴は課金の目的でアーカイブされます。

第 11 章: システム管理者ユーティリティ

このセクションでは、システム管理タスクを実行するための、CA Strong Authentication の CA Advanced Authentication に含まれるコマンド ライン ツールについて説明します。 CA Strong Authentication で利用可能で、管理者に役立つツールの機能および有用なオプションの概要を説明します。

DBUtil: AuthMinder データベース ユーティリティ

CA Strong Authentication のインストール時に、インストーラは、CA Strong Authentication データベースに接続するための情報を収集します。 インストールが完了すると、この情報は securestore.enc ファイルに暗号化された形式で格納されます。

このファイルは、CA Strong Authentication データベースに接続するために必要な以下の暗号化された情報を格納します。

- データベース ユーザの名前とパスワード（CA Strong Authentication サーバがデータベースに接続するために使用）
- マスタ キー（securestore.enc に格納されるデータベース ユーザの名前とパスワードを暗号化するために使用）

CA Strong Authentication では、データを保護するためにソフトウェア モードとハードウェア モードの両方をサポートしています。 DBUtil ツールは、この両方のモードのデータベース操作を実行するために使用できます。

何らかの理由により、インストール*後*に新しいデータベース ユーザの名前、パスワード、または DSN を追加したり、マスタ キー値を変更したりする必要がある場合は、DBUtil を使用します。

注: マスタ キーは機密情報の暗号化に使用するため、セキュリティ上の理由から、DBUtil ツールにはこのキーの値を表示するオプションが*ありません*。

DBUtil オプションの使用法

DBUtil のオプションを以下の表に示します。 この表で *キーと値*のペアは、DSN とパスワード、またはデータベースのユーザ名とパスワードのペアとなります。CA Strong Authentication サーバは DSN/パスワードを使用しますが、管理コンソールおよびユーザ データ サービスはユーザ名/パスワードを使用します。

オプション	Description
-h	ツールのヘルプを表示します。 構文 dbutil -h
-init	指定した新しいマスタ キーで新しい securestore.enc を作成します。 「マスタ キーの更新 (P. 279)」を参照してください。 **構文** `dbutil -init key` **例：** dbutil -init MasterKeyNew dbutil -init WebFortDatabaseMKNew **注**: このコマンドは conf ディレクトリに securestore.enc がない場合にのみ、成功します。

オプション	Description

-pi	追加のキーと値のペアを securestore.enc に挿入します。「マスタ キーの更新 (P. 279)」を参照してください。
	構文
	`dbutil -pi <key> <value> [-h HSMPin [-d HSMModule]]`
	securestore.enc が HSM 暗号化法によって保護される場合は、-h HSMPin が必要です。
	-d HSMModule は -h を指定する場合のオプションです。 デフォルトは「nfast」（NCipher です）。
	例：
	`dbutil -pi WebFortBackupDSN dbapassword`
	`dbutil -pi Jack userpassword`
	`dbutil -pi Jack userpassword -h hsmpassword -d chrysalis`
	注: 各キーは 1 つの値のみを持つことができます。すでにキーと値のペアを挿入している場合、同じキーに別の値を挿入することはできません。

-pu	securestore.enc にすでに存在するキーと値のペアの値を更新します。この機能はデータベース パスワードを更新する必要がある場合に使用できます。
	構文
	`dbutil -pu <key> <value> [-h HSMPin [-d HSMModule]]`
	例：
	`dbutil -pu WebFortDatabaseDSN newPassword`
	`dbutil -pu Jack userPassword`
	`dbutil -pu Jack userpassword -h hsmpassword -d chrysalis`

-pd	指定したキーと値のペアを securestore.enc から削除します。
	構文
	`dbutil -pd <key> [-h HSMPin [-d HSMModule]]`
	例：
	`dbutil -pd WebFortDatabaseDSNOld`
	`dbutil -pd Jack`

オプション	Description
-i	securestore.enc ファイル内のデータを保護するためにハードウェア ベースの暗号化を使用している場合に、指定するプライマリの名前と値のペアをこのファイルに挿入します。 これは HSM 初期化情報を提供するためにサーバ スタートアップ時に使用されます。 **構文** dbutil -i <primeKey> <HSMPin> primeKey には、HSM モジュールの名前を指定します。 **例 :** dbutil -i chrysalis pin
-u	securestore.enc ファイル内のデータを保護するためにハードウェア ベースの暗号化を使用している場合に、このファイルに指定されたプライマリの名前と値のペアを更新します。 **構文** dbutil -u <primeKey> <HSMPin> primeKey には、HSM モジュールの名前を指定します。 **例 :** dbutil -u chrysalis newHSMpin
-d	このファイル内のデータを保護するためにハードウェア ベースの暗号化を使用している場合に、指定されたプライマリの名前と値のペアを削除します。 **構文** dbutil -d <primeKey> primeKey には、HSM モジュールの名前を指定します。 例 : dbutil -d chrysalis

マスタ キーの更新

マスタ キーは securestore.enc ファイル内の値を暗号化するために使用されます。 また、この製品によって使用され、CA Strong Authentication データベースに格納される暗号化キーもすべて暗号化します。

次の手順に従ってください:

1. 現在の securestore.enc ファイルをバックアップします。

   現在の securestore.enc は以下の場所にあります。

   - **Windows の場合**
     `<install_location>¥Arcot Systems¥conf¥`
   - **UNIX の場合**
     `<install_location>/arcot/conf/`
2. 前の手順で説明したディレクトリにある securestore.enc ファイルを削除します。
3. コマンド プロンプト ウィンドウを開きます。
4. 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。

   - **Windows の場合**
     `<install_location>¥Arcot Systems¥tools¥win`
   - **UNIX の場合:**
     `<install_location>/arcot/tools/<platform_name>`
5. 以下のコマンドを実行します。

   （ソフトウェア モードの場合） dbutil -init *<master_key>*

   （ハードウェア モードの場合） dbutil -init *<master_Key_Label>*

   ツールは指定されたマスタ キー名を持った securestore.enc を再作成します。

   重要: マスタ キーの設定が失敗した場合は、CA サポートにお問い合わせください。
6. securestore.enc ファイル内のデータベース情報を更新します。

   CA Advanced Authentication インストーラは、securestore.enc にデータベース ユーザ名/パスワードおよびデータベース DSN/パスワード情報を自動的に設定します。 ただし、securestore.enc ファイルを作成した後に、dbutil -pi オプションを使用して、新しいファイルにこの情報を手動で挿入します。

提供されたデータベースの値を securestore.enc に挿入するには、以下のコマンドを入力します。

- （ソフトウェア モードの場合） dbutil -pi <*dbUser*> <*dbPassword*>
- （ハードウェア モードの場合）dbutil -pi <*dbUser*> <*dbPassword*> [-h *HSMPin [*-d *HSMModule]]*

  前述のコマンドでは、dbUser はデータベース ユーザ名で、dbPassword は指定されたユーザ名に関連付けられたパスワードです。 例：

  ```
  dbutil -pi arcotuser welcome123
  ```

  注: このコマンドで指定するユーザ名では大文字と小文字が区別されます。

- （ソフトウェア モードの場合） dbutil -pi <*dsn*> <*dbPassword*>

  注: <*dbPassword*> はデータベース ユーザのパスワードです。

- （ハードウェア モードの場合） dbutil -pi <*dsn*> <*dbPassword*> [-h *HSMPin [*-d *HSMModule]]*

  上記のコマンドで、dsn はデータ ソース名です。また dbPassword はデータベースのパスワードです。 例：

  ```
  dbutil -pi arcotdsn welcome123
  ```

  注: このコマンドで指定する DSN 名では大文字と小文字が区別されます。

7. CA Strong Authentication の分散展開を実行した場合は、新しい securestore.enc ファイルを CA Strong Authentication のコンポーネントがインストールされているすべてのシステムにコピーします。

arwfserver: サーバ管理ツール

arwfserver ユーティリティは、CA Strong Authentication サーバの設定を管理し、接続エラーをトラブルシュートするために使用できる対話型のユーティリティです。 たとえば、管理コンソールは CA Strong Authentication サーバ インスタンスの管理に Server Management プロトコルを使用します。このプロトコルのデフォルト ポート番号は 9743 です。 このポートがほかのアプリケーションによってすでに使用されている場合は、arwfserver ツールを使用して別のポートにプロトコルを設定できます。

サーバ設定管理のほかに、arwfserver ツールでは、めったに使用されない（Web サービス API の認証および許可）か、ある展開シナリオでのみ必要（プラグインを有効または無効にする）な CA Strong Authentication 設定を設定できます。

arwfserver ユーティリティの対話モードでの実行

このユーティリティは対話モードで実行できます。 このモードでは、リスナが開始されない点を除き、サービス モードと同様の方法ですべてのサーバ設定が実行されます。

このモードで実行した場合、arwfserver ツールは、独自のコンソール プロンプトを開始し（wf>）、スタートアップ ログを <install_location>/logs/arcotwebfortstartupcmd.log に、トランザクション ログを <install_location>/logs/arcotwebfortcmd.log に生成します。

次の手順に従ってください:

1. ツールが利用可能な場所に移動します。
   - **Windows の場合**
     `<install_location>¥Arcot Systems¥bin¥`
   - **UNIX ベースのプラットフォームの場合**
     `<install_location>/arcot/bin/`
2. 以下のコマンドを実行します。
   - **Windows の場合**
     `arwfserver -i`
   - **UNIX ベースのプラットフォームの場合**
     `./webfortserver -i`

   ツールが対話モードで起動されます。
3. 以下の表に示すオプションを指定して、必要なタスクを実行します。

オプション	Description
メッセージ表示操作	
ddn	表示名をファイルにダウンロードします。表示名をダウンロードするアプリケーションのコンテキスト名と、ファイルをダウンロードするパスを入力する必要があります。 **構文** ddn *<application_context> <file_location>* **例：** ddn Admin ARCOT_HOME>/logs
dmsg	表示メッセージをファイルにダウンロードします。 ファイルのダウンロード先のアプリケーション コンテキストおよびパスを入力する必要があります。 **構文** dmsg *<application_context> <file_location>* **例：** dmsg Admin ARCOT_HOME>/logs
udn	カスタマイズされた表示名が含まれるファイルをデータベースにアップロードします。 **構文** udn *<file_path>*
umsg	カスタマイズされた表示メッセージが含まれるファイルをデータベースにアップロードします。 **構文** umsg *<file_path>*
プラグイン設定	
getmodconf	現在のモジュールの設定を取得します。たとえば、認証情報モジュールおよびプラグインの設定を取得します。 **構文** getmodconf

オプション	Description
upluginstatus	プラグインのステータスを更新します。サポートされているステータスは以下のとおりです。 ■ 0： プラグインが無効であることを示します。 ■ 1： プラグインがアクティブであることを示します。 ■ 2： プラグインがロードされていないことを示します。 **構文** upluginstatus
プロトコル操作	
getprotoconf	すべてのプロトコルの設定を取得します。 **構文** getprotoconf
setsvrmgmtport	サーバ管理プロトコルのポート番号を変更します。 CA Strong Authentication サーバで SSL を有効にしている場合、このツールを使用して、トランスポート モードを SSL から TCP に変更できます。 **構文** setsvrmgmtconf <*サーバ管理ポート*> TCP **例：** setsvrmgmtconf 9743 TCP
サーバ管理操作	
バージョン	arcotwebfort-ver-<*dd*>-<*mmm*>-<*yy*>.txt というファイルを生成します。このファイルには、すべての CA Strong Authentication ライブラリ ファイルのバージョンがリストされます。 このファイルは、以下のディレクトリにあります。 **Windows**： <*install_location*>¥Arcot Systems¥logs **UNIX ベースのプラットフォーム**： <*install_location*>/arcot/logs **構文** バージョン
ユーティリティ操作	

オプション	Description
??	指定したパターンに基づいてコマンドを検索します。 構文 ?? <*検索テキスト*> 例： ?? conf 設定を設定または取得するためのすべてのオプションが表示されます。 例： ■ getmodconf ■ getprotoconf
?	arwfserver でサポートされているコマンドをリスト表示します。 このオプションと一緒にコマンド名を指定すると、ツールからコマンドの使用方法についてのヘルプが表示されます。 **構文** ■ ? サポートされているコマンドをすべてリスト表示します。 ■ ? *<command_option>* コマンドの使用方法についてのヘルプを表示します。 **例：** ? setsvrmgmtport サーバ管理ポートを設定するコマンドの使用方法が表示されます。
help	コマンドの使用方法についてのヘルプを表示します。 **構文** help *<command_option>* コマンドの使用方法についてのヘルプを表示します。 **例：** help setsvrmgmtport サーバ管理ポートを設定するコマンドの使用方法が表示されます。

オプション	Description
log2c	管理コンソールにログを出力できます。 ログを管理コンソールに出力するには「Y」を、ログをファイルに出力するには「N」を入力します。 **構文** log2c <*オプション*> **例：** log2c n
q	対話モードを終了します。

arwfutil : ユーティリティ ツール

arwfutil ツールを使用して、サーバ キャッシュの管理、サーバのリフレッシュ、サーバのシャットダウンを行うことができます。また、プロトコル設定、サーバ統計などのサーバ設定情報を読み取ることもできます。

このツールは対話型モードで実行するか、または直接コマンドを実行します。

次の手順に従ってください:

1. ツールが利用可能な場所に移動します。
   - **Windows の場合**
     `<install_location>¥Arcot Systems¥bin¥`
   - **UNIX の場合**
     `<install_location>/arcot/sbin/`
2. ツールは以下のいずれかのモードで実行可能です。
   - 対話型モードの場合は、以下のように入力します。
     - **Windows の場合**
       `arwfutil -i`
     - **UNIX の場合**
       `./arwfutil -i`

     ツールが対話モードで起動されます。 以下の表に示されるコマンドを実行します。
   - コマンドを直接入力する場合は、以下のように入力します。
     - **Windows の場合**
       `arwfutil <command_option>`
     - **UNIX の場合**
       `./arwfutil <command_option>`

     以下の表に、arwfutil ユーティリティに用意されているコマンド オプションを示します。

オプション	Description
サーバ管理操作	

オプション	Description
cr	CA Strong Authentication サーバ インスタンスのキャッシュをリフレッシュします。インスタンス IP およびサーバ管理ポート番号を入力する*必要*があります。 操作が正常に完了すると、「操作が正常に完了しました」というメッセージが表示され、トランザクション ID が返されます。 **構文** arwfutil cr <*AuthMinder サーバ IP*> < *サーバ管理ポート*> **例：** arwfutil cr localhost 9743
dc	arcotwebfortcache-< *トランザクション ID*>.log というファイルにサーバ設定キャッシュをダウンロードします このファイルは、以下のディレクトリにあります。 **Windows の場合**： <*install_location*>¥Arcot Systems¥logs **UNIX ベースのプラットフォームの場合**： <*install_location*>/arcot/logs サーバ設定キャッシュをダウンロードするごとに、新しいファイルが一意のトランザクション識別子で作成されます。 **構文** ■ arwfutil dc 完全なキャッシュまたは部分的なキャッシュのどちらをダウンロードするかを確認するプロンプトが表示されます。 完全なキャッシュの場合は「1」を、部分的なキャッシュの場合は「0」を入力します。 ■ arwfutil dc <AuthMinder *サーバ IP*> < *サーバ管理ポート*> 完全なキャッシュをダウンロードします。 **例：** arwfutil dc localhost 9743

オプション	Description
gss	wf-server-stats-<*dd*>-<*mmm*>-<*yy*>.xml というファイルを生成します。このファイルは、サーバ統計をリスト表示します。 このファイルは、以下のディレクトリにあります。 **Windows の場合**： <*install_location*>¥Arcot Systems¥logs **UNIX ベースのプラットフォームの場合**： <*install_location*>/arcot/logs 統計ファイルには、各プロトコルの以下の情報が含まれます。 ■ 受信したリクエストの数 ■ 成功したトランザクションの数 ■ 失敗したトランザクションの数 ■ リクエストを処理するために費やされた最小時間 ■ リクエストを処理するために費やされた最大時間 ■ リクエストを処理するために費やされた合計時間 ■ リクエストを処理するために費やされた平均時間 操作が正常に完了すると、「操作が正常に完了しました」というメッセージが表示され、トランザクションの詳細が返されます。 **構文** arwfutil gss
sd	CA Strong Authentication サーバ インスタンスをシャットダウンします。インスタンス IP およびサーバ管理ポート番号を入力する*必要*があります。 操作が正常に完了すると、「操作が正常に完了しました」というメッセージが表示され、トランザクションの詳細が返されます。 **構文** ■ arwfutil sd ■ arwfutil sd <*AuthMinder サーバ IP*> <*サーバ管理ポート*> **例：** arwfutil sd localhost 9743

オプション	Description
ssc	CA Strong Authentication サーバの設定を行います。 CA Strong Authentication サーバの IP アドレスと、Server Management プロトコルのポート番号を指定する必要があります。 **構文** arwfutil -i ssc *<AuthMinder サーバ IP> <サーバ管理ポート>* **例：** arwfutil -i ssc localhost 9743 **注**: このコマンドは、対話モードで実行することをお勧めします。 そうしないと、このコマンドを使用して設定されるサーバ設定が他のコマンドによって使用できません。
設定の検証操作	
vah	CA Strong Authentication サーバ ファイルの 16 進数にエンコードされた MD5 を計算して、ARCOT_HOME を検証します。 このコマンドによって、arcotwebfort-vah-*<dd>-<mmm>-<yy>*.txt というファイルが生成されます。このファイルには、CA Strong Authentication ファイルの MD5 がリスト表示されます。 このファイルは、以下のディレクトリにあります。 **Windows の場合**： *<install_location>*¥Arcot Systems¥logs **UNIX ベースのプラットフォームの場合**： *<install_location>*/arcot/logs **構文** arwfutil vah
vdb	CA Strong Authentication データベース テーブルを検証します。 このコマンドによって、arcotwebfort-vdb-*<dd>-<mmm>-<yy>*.txt というファイルが生成されます。このファイルには、CA Strong Authentication データベース テーブルがリスト表示されます。 このファイルは、以下のディレクトリにあります。 **Windows の場合**： *<install_location>*¥Arcot Systems¥logs **UNIX ベースのプラットフォームの場合**： *<install_location>*/arcot/logs **構文** arwfutil vdb

オプション	Description
vsetup	CA Strong Authentication サーバ ファイルと CA Strong Authentication データベース テーブルの 16 進数にエンコードされた MD5 を計算して、ARCOT_HOME を検証します。 このコマンドによって、arcotwebfort-setup-<*dd*>-<*mmm*>-<*yy*>.txt というファイルが生成されます。このファイルには、CA Strong Authentication ファイルとデータベース テーブルの MD5 がリスト表示されます。 このファイルは、以下のディレクトリにあります。 **Windows の場合**： <*install_location*>¥Arcot Systems¥logs **UNIX ベースのプラットフォームの場合**： <*install_location*>/arcot/logs **構文** arwfutil vdb
ユーティリティ操作	
??	指定したパターンに基づいてコマンドを検索します。 たとえば、「?? ss」と入力すると、名前に ss が含まれるコマンドがすべて表示されます。 **構文** arwfutil ?? <*検索テキスト*> **例：** arwfutil ?? SS 上記のコマンドでは、以下のオプションが取得されます。 ■ gss ■ ssc
?	arwfserver でサポートされているコマンドをリスト表示します。 このオプションと一緒にコマンド名を指定すると、ツールからコマンドの使用方法についてのヘルプが表示されます。 **構文** ■ arwfutil ? サポートされているコマンドをすべてリスト表示します。 ■ arwfutil ? <*command_option*> コマンドの使用方法についてのヘルプを表示します。 **例：** arwfutil ? ssc SSC （Set Server Configuration） コマンドの使用方法が表示されます。

オプション	Description
help	コマンドの使用方法についてのヘルプを表示します。 **構文** help <*command_option*> コマンドの使用方法についてのヘルプを表示します。 **例：** arwfutil help ssc SSC （Set Server Configuration） コマンドの使用方法が表示されます。
q	対話モードを終了します。
rai	ほかのコマンドを呼び出すときに含める追加の入力を読み取ります。 このコマンドを実行する前に、追加する入力の名前と値のペアを以下のように追加する必要があります。 ■ 1. 以下の場所に移動します。 **Windows の場合**： <*install_location*>¥Arcot Systems¥conf **UNIX プラットフォームの場合**： <*install_location*>/conf ■ 2. テキスト エディタで arcotcommon.ini ファイルを開きます。 ■ 3. [arcot/webfort/tool/additionalInputs] というセクションを追加します。 ■ 4. 前の手順で追加したセクションに名前と値のペアを含めます。 ■ 5. arcotcommon.ini ファイルを保存して閉じます。 **構文** rai

第 12 章: レポートの管理

レポートを使用すると、CA Strong Authentication データベースの情報を要約および分析できます。 上位レベルの管理者は、システムにアクセスした管理者名、アクセスした日時、実行されたアクティビティなどの情報をレポートから入手できます。 「すべての管理者が使用可能なレポートのサマリ (P. 293)」では、さまざまな管理者が使用可能なレポートのサマリが表形式で提供されています。

管理コンソールを通じて提供されるレポートは、指定したパラメータ（フィルタ）に基づいて生成されます。 つまり、レポートの実行時に指定する値によって、レポートの出力を制御できます。 データをフィルタするために、以下のフィルタが使用できます。

- 日付範囲
- ［Administrator Name］
- 組織
- User Name

すべての管理者が使用可能なレポートのサマリ

以下の表に、すべての管理者がシステムで使用可能なすべてのカテゴリのレポート（管理者レポートおよび CA Strong Authentication レポート）の概要を示します。 これらのレポートについては、以降のセクションで詳しく説明します。

[レポート]	MA（マスタ管理者）	GA（グローバル管理者）	OA（組織の管理者）	UA（ユーザ管理者）	
管理者レポート					
マイ アクティビティ レポート		✓	✓	✓	✓
管理者アクティビティ レポート		✓	✓	✓	✓
ユーザ アクティビティ レポート			✓	✓	✓

[レポート]	MA（マスタ管理者）	GA（グローバル管理者）	OA（組織の管理者）	UA（ユーザ管理者）	
ユーザ作成レポート			✓	✓	✓
組織レポート		✓	✓	✓	
AuthMinder レポート					
サーバ管理アクティビティ レポート		✓			
認証アクティビティ レポート			✓	✓	✓
認証情報管理アクティビティ レポート			✓	✓	✓
設定管理アクティビティ レポート			✓	✓	

管理者レポート

システムで使用可能なすべての管理者レポートには、以下のものが含まれます。

- マイ アクティビティ レポート（P. 295）
- 管理者アクティビティ レポート（P. 296）
- ユーザ アクティビティ レポート（P. 296）
- ユーザ作成レポート（P. 297）
- 組織レポート（P. 298）

マイ アクティビティ レポート

このレポートは、レポートを作成している管理者が実行したすべての操作、およびこれらの操作に関連する詳細をリスト表示します。

ログインしている管理者は、管理者アクティビティ レポート (P. 296)を使用して自身のアクティビティを確認できますが、このレポートは、以下の理由により別途提供されています。

- 管理者が所属している組織をスコープ内に持たないことがあります。たとえば、管理者 *Alan* は組織「MyOrg」に属していますが、「ScopeOrg」をスコープに持つとします。 この場合、Alan は必要なスコープを持たないので、管理者アクティビティ レポート を使用して自身のアクティビティを表示することはできません。
- 管理者アクティビティ レポートは、指定したユーザ名に完全にまたは部分的にユーザ名が一致するすべての管理者のアクティビティをリスト表示します。 そのため、管理者は、自身のアクティビティ報告を取得するためにレポートのすべてのページを検索する必要があります。マイ アクティビティ レポートはログインしている管理者のみのアクティビティを表示するので、この問題が解決されます。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
Date	アクティビティを実行した日時です。
管理者 ID	レポートを生成している管理者の名前です。
管理者の組織	管理者が属する組織の名前です。
トランザクション ID	管理者によって実行されたアクティビティごとに生成された一意の ID です。
［Event Type］	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）です。
ステータス	実行されたアクションのステータスです。 ■ **成功** - アクションは正常に完了しました。 ■ **失敗** - アクションは正常に終了しませんでした。
理由	操作が失敗した理由を示します。
ユーザ ID	属性が管理者によって管理されたユーザの名前です。
ターゲット組織	アクティビティが実行された組織です。

レポート フィールド	Description
［Component］	タスクを実行するために使用されたリソースです。 列の値は以下のいずれかです。 ■ 管理コンソール ■ AuthMinder
［Session ID］	管理者がログインした管理コンソールのセッション識別子です。
インスタンス ID	複数の管理コンソール アプリケーション インスタンスが実行している場合、インスタンスの一意の識別子です。

管理者アクティビティ レポート

このレポートは、このレポートを生成する管理者のスコープ内にある組織に属する管理者が実行したすべてのアクティビティをリスト表示します。このレポートを使用することによって、特定の管理者のアクティビティをフィルタしたり、または単独の組織または複数の組織のすべての管理者のアクティビティを表示できます。 このレポートは、管理者のログインおよびログアウトのタイム スタンプ、組織検索、管理者アカウントの更新、関連する詳細などの情報を表示します。

ユーザ アクティビティ レポート

このレポートは、ユーザ属性に対して実行されたすべてのアクティビティをリスト表示します。たとえば、ユーザの作成、ユーザの更新、PAM 設定、ユーザの削除、ユーザ ステータスの更新、ユーザの認証などが対象です。レポートは、ユーザ名、ユーザのステータス、実行された操作のタイプ、ユーザ システムの IP アドレスなどの詳細を表示します。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
Date	アクティビティを実行した日時です。
ユーザ ID	実行したアクティビティの対象となったユーザの名前です。
アカウント タイプ	ユーザが所属する組織と関連付けられたアカウント タイプ。
アカウント ID	ユーザのアカウント ID。

レポート フィールド	Description
［Event Type］	管理者によって実行されたアクティビティのタイプ（ユーザの作成、更新、削除など）です。
組織	ユーザが属する組織の名前です。
ステータス	操作のステータスです。 ■ **成功** - 操作は正常に完了しました。 ■ **失敗** - 操作は正常に終了しませんでした。
トランザクション ID	ユーザによって実行されたアクティビティごとに生成された一意の識別子です。
理由	操作が失敗した理由を示します。
クライアント IP アドレス	エンドユーザのシステムの IP アドレスです。
コール元 ID	呼び出し元のアプリケーションによって設定された一意の識別子です。 **注**: 呼び出し元のアプリケーションが値を設定しなかった場合、［コール元 ID］はブランクになることがあります。

ユーザ作成レポート

ユーザ作成レポートには、CA Strong Authentication システムで作成されたユーザの詳細が表示されます。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
作成日	ユーザが作成された日時を示します。
ユーザ ID	作成されたユーザの名前です。
組織	ユーザが属する組織の名前です。
ユーザ ステータス	ユーザのステータスです。以下の値になります。 ■ **アクティブ** - ユーザがアクティブなユーザである場合。 ■ **非アクティブ** - ユーザが非アクティブにされている場合。 ■ **初期** - ユーザが作成されているが、まだアクティブにされていない場合。
［First Name］	ユーザの名です。

レポート フィールド	Description
［Middle Name］	ユーザのミドル ネームです。
［Last Name］	ユーザの姓です。
［Email Address］	ユーザの電子メール アドレスです。
電話番号	ユーザの電話番号です。

組織レポート

このレポートは、指定した組織上で実行されたすべての操作の詳細をリスト表示します。 このレポートは、ポリシーに関係なく、管理者の権限の範囲内の組織のすべてのアクティビティを表示します。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
Date	アクティビティを実行した日時です。
［Administrator Name］	処理を実行した管理者の名前です。
管理者の組織	管理者が属する組織の名前です。
トランザクション ID	管理者によって実行されたアクティビティごとに生成された一意の識別子です。
［Event Type］	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）です。
ステータス	実行されたアクションのステータスです。 ■ **成功** - アクションは正常に完了しました。 ■ **失敗** - アクションは正常に終了しませんでした。
理由	操作が失敗した理由を示します。
ターゲット ユーザ	属性が管理者によって管理されたユーザの名前です。
ターゲット組織	ユーザが属する組織です。
［Component］	タスクを実行するために使用されたリソースです。 列の値は以下のいずれかです。 ■ 管理コンソール ■ AuthMinder

レポート フィールド	Description
［Session ID］	管理者がログインした管理コンソールのセッション識別子です。
インスタンス ID	複数の管理コンソール アプリケーション インスタンスが実行している場合、インスタンスの一意の識別子です。

AuthMinder レポート

このセクションでは、以下のレポートに関する情報を確認できます。

- サーバ管理アクティビティ レポート（P. 299）
- 認証アクティビティ レポート（P. 300）
- 認証情報管理アクティビティ レポート（P. 302）
- 設定管理アクティビティ レポート（P. 304）

サーバ管理アクティビティ レポート

このレポートは、MA によって実行された AuthMinder サーバ設定をリスト表示します。ログ設定、データベース設定、プロトコル設定、プラグイン設定、信頼された認証局の設定、およびサーバの起動、シャットダウン、リフレッシュに関連するアクティビティの情報が表示されます。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
アクティビティ時間	アクティビティを実行した日時です。
レスポンス タイム（ms）	リクエストを処理するために CA Strong Authentication サーバによって費やされた時間（ミリ秒）です。
インスタンス設定	すべての CA Strong Authentication サーバ インスタンス設定の詳細を示します。 **注**: インスタンス設定の完全な詳細を表示するには、列エントリ上にマウスを移動します。
［Instance Name］	CA Strong Authentication サーバ インスタンスの名前です。

レポート フィールド	Description
インスタンス ステータス	CA Strong Authentication サーバ インスタンスのステータスです。
操作	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）です。
レスポンス コード	実行されたアクションのステータスです。 ■ **成功** - アクションは正常に完了しました。 ■ **失敗** - アクションは正常に終了しませんでした。
トランザクション ID	CA Strong Authentication サーバによって生成されたトランザクションの一意の識別子です。
アプリケーション IP	呼び出し元のアプリケーションがホストされているシステムの IP アドレスです。
コール元 ID	呼び出し元のアプリケーションによって設定された一意の識別子です。 **注**: 呼び出し元のアプリケーションが値を設定しなかった場合、［コール元 ID］はブランクになることがあります。

認証アクティビティ レポート

このレポートは、すべてのユーザの認証アクティビティの詳細をリスト表示します。 使用された認証情報のタイプ、認証情報の有効性、OTP の使用可能な回数、認証失敗の回数など、認証の詳細を表示します。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
アクティビティ時間	アクティビティを実行した日時です。
レスポンス タイム（ms）	リクエストを処理するために CA Strong Authentication サーバによって費やされた時間（ミリ秒）です。
組織	ユーザが属する組織の名前です。
ユーザ ID の入力	ユーザによって実行された操作を追跡するためにユーザに割り当てられる一意の識別子です。
User Name	認証アクティビティを実行したユーザの ID です。
アカウント ID	ユーザのアカウント ID。

レポート フィールド	Description
アカウント タイプ	ユーザが所属する組織と関連付けられたアカウント タイプ。
認証情報タイプ	認証に使用された認証情報のタイプです。
認証情報ステータス	認証情報のステータスです。
有効期間の開始日	認証情報の有効期間の開始日時のタイム スタンプです。
有効期間の終了日	認証情報の有効期間の終了日時のタイム スタンプです
試行失敗	ユーザが認証情報を使用して認証に失敗した回数です。
残り使用回数	OTP を認証のために使用できる残りの回数です。 **注**: このフィールドは、その他の認証情報には適用 *されません*。
操作	ユーザを認証するために CA Strong Authentication サーバによって実行されたタスクです。
レスポンス コード	実行されたアクションのステータスです。 ■ **成功** - アクションは正常に完了しました。 ■ **失敗** - アクションは正常に終了しませんでした。
理由コード	操作が失敗した理由を示します。
トークン タイプ	認証が成功した後に返されたトークンのタイプです。
［Session ID］	現在の管理者がログインしている管理コンソールのセッション識別子です。
トランザクション ID	トランザクションを追跡するために CA Strong Authentication サーバによって生成された一意の識別子です。
プロトコル ID	アクティビティを実行するために使用されたプロトコルの名前です。
［Instance Name］	リクエストを処理した CA Strong Authentication サーバ インスタンスの名前です。
アプリケーション IP	呼び出し元のアプリケーションがホストされているシステムの IP アドレスです。
コール元 ID	呼び出し元のアプリケーションによって AR_WF_CALLER_ID 追加入力に設定された一意の識別子。
ユーザ エージェント	呼び出し元のアプリケーションによって AR_WF_USER_AGENT 追加入力で渡されたユーザ エージェントの値。
参照元	呼び出し元のアプリケーションによって AR_WF_REFERRER 追加入力で渡された参照元の値。

レポート フィールド	Description
クライアント セッション ID	AR_WF_CLIENT_SESSION_ID 追加入力で渡されたクライアント セッションの識別子。
コール元 IP	呼び出し元のアプリケーションによって AR_WF_IP_ADDRESS 追加入力で渡された一意の IP。

認証情報管理アクティビティ レポート

このレポートは、ユーザに発行されるクレデンシャルの概要を表示します。発行されたクレデンシャルのタイプ、クレデンシャルに対する操作、発効日、クレデンシャルの現在のステータスなどを表示します。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
アクティビティ時間	アクティビティを実行した日時です。
レスポンス タイム（ms）	認証リクエストを処理するために CA Strong Authentication サーバによって費やされた時間（ミリ秒）です。
組織	ユーザが属する組織の名前です。
ユーザ ID の入力	ユーザによって実行された操作を追跡するためにユーザに割り当てられる一意の識別子です。
User Name	クレデンシャルが更新されたユーザの名前です。
アカウント ID	ユーザのアカウント ID。
アカウント タイプ	ユーザが所属する組織と関連付けられたアカウント タイプ。
認証情報タイプ	影響を受けた（変更された）クレデンシャルのタイプです。以下のいずれかの値を示します。 ■ ArcotID PKI ■ Q&A ■ OTP ■ Password ■ OATH ■ ArcotID OTP-OATH ■ ArcotID OTP-EMV

レポート フィールド	Description
認証情報ステータス	クレデンシャルの現在の状態です。 以下の値が使用可能です。 ■ アクティブ ■ Disabled （無効） ■ 検証済み ■ ロック
有効期間の開始日	認証情報の有効期間の開始日時のタイム スタンプです。
有効期間の終了日	認証情報の有効期間の終了日時のタイム スタンプです
試行失敗	クレデンシャルを使用して、ユーザが認証に失敗した回数です。
残り使用回数	OTP を認証のために使用できる残りの回数です。
操作	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）です。
レスポンス コード	実行されたアクションのステータスです。 ■ **成功** - アクションは正常に完了しました。 ■ **失敗** - アクションは正常に終了しませんでした。
理由コード	操作が失敗した理由を示します。
トランザクション ID	トランザクションを追跡するために CA Strong Authentication サーバによって生成された一意の識別子です。
プロトコル ID	アクティビティを実行するために使用されたプロトコルの名前です。
［Instance Name］	リクエストを処理した CA Strong Authentication サーバ インスタンスの名前です。
アプリケーション IP	呼び出し元のアプリケーションがホストされているシステムの IP アドレスです。
コール元 ID	呼び出し元のアプリケーションによって AR_WF_CALLER_ID 追加入力に設定された一意の識別子。
ユーザ エージェント	呼び出し元のアプリケーションによって AR_WF_USER_AGENT 追加入力で渡されたユーザ エージェントの値。
参照元	呼び出し元のアプリケーションによって AR_WF_REFERRER 追加入力で渡された参照元の値。
クライアント セッション ID	AR_WF_CLIENT_SESSION_ID 追加入力で渡されたクライアント セッションの識別子。

レポート フィールド	Description
コール元 IP	リクエストの呼び出し元のシステムの IP アドレスです。
Profile Name	アクティビティの実行時に使用されたクレデンシャルに関連付けられたプロファイルの名前です。

設定管理アクティビティ レポート

このレポートは、GA（または OA）によって作成されるすべての CA Strong Authentication 設定をリスト表示します。認証ポリシー、認証情報プロファイル、プラグイン、SAML トークン、RADIUS クライアント、および ArcotID PKI と Q&A 用の認証チャレンジの各設定情報を表示します。

以下の表に、このレポートのフィールドの説明を示します。

レポート フィールド	Description
アクティビティ時間	アクティビティを実行した日時です。
［Administrator Name］	設定を実行した管理者の名前です。
管理者の組織	管理者が属する組織の名前です。
［Session ID］	管理者がログインした管理コンソールのセッション識別子です。
ターゲット組織	設定作成の対象となる組織です。
設定名	設定の名前です。
設定タイプ	影響を受けた（変更された）設定のタイプです。
操作	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）です。
現在の関連付けバージョン	設定の現バージョンです。
［Previous Association Version］	前の関連付けバージョン
レスポンス コード	実行されたアクションのステータスです。 ■ **成功** - アクションは正常に完了しました。 ■ **失敗** - アクションは正常に終了しませんでした。
理由コード	操作が失敗した理由を示します。

レポート フィールド	Description
トランザクション ID	CA Strong Authentication サーバによって生成されたトランザクションの一意の識別子です。
［Instance Name］	CA Strong Authentication サーバ インスタンスの名前です。
アプリケーション IP	呼び出し元のアプリケーションがホストされているシステムの IP アドレスです。
コール元 ID	呼び出し元のアプリケーションによって AR_WF_CALLER_ID 追加入力に設定された一意の識別子。
ユーザ エージェント	呼び出し元のアプリケーションによって AR_WF_USER_AGENT 追加入力で渡されたユーザ エージェントの値。
参照元	呼び出し元のアプリケーションによって AR_WF_REFERRER 追加入力で渡された参照元の値。
クライアント セッション ID	AR_WF_CLIENT_SESSION_ID 追加入力で渡されたクライアント セッションの識別子。
コール元 IP	呼び出し元のアプリケーションによって AR_WF_IP_ADDRESS 追加入力で渡された一意の IP。

レポートの生成

このセクションでは、次の項目について説明します。

- レポートを生成する際の注意事項（P. 305）
- レポートを生成する方法（P. 306）

レポートを生成する際の注意事項

レポートの生成時には、以下の点に注意する必要があります。

- 管理者は、スコープを持つ組織のレポートのみを生成できます。
- 管理者は、下位または同レベルの管理者のレポートを生成できます。たとえば、組織の管理者（OA）は、OA とユーザ管理者（UA）のレポートを生成できます。
- Oracle データベースを使用している場合は、UNLIMITED TABLESPACE 権限を有効にしていることを確認します。

レポートを生成する方法

これまでに説明されたレポートを生成する方法

1. 適切な認証情報（MA、GA、OA、または UA）でログインしていることを確認します。
2. メイン メニューの［レポート］タブをアクティブにします。
3. 生成するレポートに応じて、以下の手順に従います。
   - 管理者アクティビティ レポートを生成する場合は、［管理者レポート］サブメニューを選択します。
   - CA Strong Authentication 固有のレポートを生成する場合は、［AuthMinder レポート］サブメニューを選択します。

   レポート タイプに対応するリンクが、左側のタスク ペインに表示されます。
4. 生成するレポートに基づいて、必要なレポート リンクをクリックします。
5. レポートを表示するために条件を指定します。
   a. 暗号化されたデータをクリア テキストで表示する場合は、［機密情報の復号化］オプションを有効にします。
   b. 以下のいずれかを指定します。
      - ドロップダウン リストから［日付範囲］
      - ［開始］と［終了］フィールドで事前定義済み日付範囲
   c. ［組織名］リストから、レポートに含めるデータを所有する組織を選択します。
   d. ［ユーザ名］フィールドで、生成するレポートに基づいて、以下のいずれかの手順を実行します。
      - 認証アクティビティ レポート および認証管理レポートの場合、ユーザ名を入力します。
      - 設定レポートの場合、管理者名を入力します。
6. ［**レポートの表示**］をクリックすると、指定した基準に基づいたレポートが生成されます。

レポートのエクスポート

管理コンソールには、レポートをファイルにエクスポートする機能が用意されています。 レポートをエクスポートすることによって、レポートのローカル コピーを保存し、傾向を追跡できます。また、保存したレポート データを別のアプリケーションで使用することもできます。

エクスポートされるレポートは、カンマ区切り値（CSV）形式で生成されるため、テキスト エディタや Microsoft Excel などのスプレッドシート アプリケーションで表示できます。 エクスポート オプションは、各レポートの右上に表示される［**エクスポート**］ボタンを介して利用できます。

レポートをローカル ファイルにエクスポートする方法

1. 必要なレポートを生成します。

   レポートが表示されます。

2. ［**エクスポート**］をクリックします。

   レポートを保存するか、開くかを問い合わせるプロンプトが表示されます。

3. ［**開く**］または［**保存**］をクリックします。 ［保存］をクリックした場合は、ダウンロード場所を指定します。

   このファイルは、後で適切なアプリケーションを使用して表示できます。

arreporttool：レポートのダウンロード ツール

arreporttool では、CA Strong Authentication レポートまたは Risk Authentication レポートのデータを CSV ファイルにエクスポートできます。

重要：report-id および report-url パラメータは、エクスポートしようとしているレポートに対して正しい必要があります。

その後、テキスト エディタや、Microsoft Excel などのスプレッドシート アプリケーションを使用して、これらのレポートを表示できます。

ツールの使用

arreporttool.jar ファイルは、以下の場所にあります。

Windows の場合

<*install_location*>¥Arcot Systems¥tools¥common¥arreporttool

UNIX の場合

<*install_location*>/arcot/tools/common/arreporttool

構文

ツールを使用するには、以下のコマンドを実行します。

```
java -jar arreporttool.jar –-protocol <protocol> --host <host>
--port <app_server_port> --admin-orgid <admin-organization>
--admin-id <admin-user-id> --admin-password <password>
[--report-type hour | day | month [duration] | range]
--report-id <Report ID> --reporturl <Url of the report>
--is-filter-req <true | false> --data-type <Data Type>
--reportdata [Report Data] --start-date-time <date-and-time> [--end-date-time
<date-andtime>] [--logfile <logfile>]
[--log-level <loglevel>][log-file-max-size] <logfilesize>] [--organizations <target
orgNames>] [--userName <User/Admin Name>] [--output-file <output-file>.CSV]
[--is-url-encoded [true|false]]
```

以下の表に、ツールでサポートされているオプションを示します。

オプション	Description
protocol	通信に使用するプロトコル。指定可能な値は http と https です。デフォルトのプロトコルは http です。
ホスト	管理コンソールを展開したシステムのホスト名または IP アドレス。
app_server_port	管理コンソールがリスンするポート。
admin-orgid	管理者が属する組織。
admin-id	一意の管理者 ID。
admin-password	管理者パスワード。

オプション	Description
report-type	時間、日、月または範囲を指定します。 ■ 時間、日、月の後に数値を指定できます。たとえば、--report-type day 2 は、指定した start-date-time からの 2 日間の記録を示します。 ■ 範囲： range を指定した場合は、end-date-time を指定します。
report-id	取得するレポートの識別子。使用できるレポート識別子のリストについては、「レポートの識別子のリスト (P. 310)」を参照してください。
reporturl	レポートの管理者の URL。使用できるレポートの URL のリストについては、「レポート URL のリスト (P. 311)」を参照してください。
is-filter-req	デフォルトでは true に設定されます。 たとえば、AuthMinder レポートなど、フィルタ ページがないレポートに対してはこの値を false に設定します。
data-type	これは AuthMinder レポートを ACTIVE または STAGING に指定する場合にのみ使用できます。
reportdata	開始日と終了日のほかに、レポートによってはさらにフィルタが必要になることがあります。 これらの追加フィルタはレポート データとして指定します。 レポート データは「キー=値」の形式で指定する必要があります。複数のキーと値のペアを区切るには、セミコロンを使用します。 レポートのデータに ; または = が含まれている場合は、URL エンコードする必要があります。 URL エンコードされた値を渡す場合には、is-url-encoded パラメータを true に設定します。
start-date-time	レポートの内容をこの後から取得する必要がある日付または時刻を指定します。 **形式** MM/dd/yyyy HH:mm:ss 時間（HH）および分（mm）はオプションで、時間単位でのレポートにのみ使用します。 日単位および月単位のレポート対しては、日付部分だけを使用します。 デフォルトでは、タイムゾーンは GMT です。 **例：** 03/21/2010 09:10:20
end-date-time	（オプション）レポートの内容をこの前まで選択する必要がある日付または時刻を指定します。

オプション	Description
logfile	（オプション）ログ ファイルの場所を指定します。 ログ ファイルが指定されていないと、**arreporttool.log** ファイルが現在のディレクトリに自動的に作成されます。
log-level	（オプション）ログのレベルを指定します。 デフォルトのログ レベルは［情報］です。
log-file-max-size	（オプション）ログ ファイルの最大サイズを指定します。 デフォルト値は 10MB です。
organizations	（オプション）レポートの対象となる組織の名前をセミコロンで区切って指定します。組織が必須パラメータであるレポートにはこの値を指定する*必要があります*。 組織名にセミコロン（;）が含まれる場合は、値を URL エンコードする必要があります。 URL エンコードされた値を渡す場合には、is-url-encoded パラメータを true に設定します。
userName	（オプション）ユーザまたは管理者の名前を指定します。
output-file	（オプション）レポートの内容を書き込む必要がある出力ファイルを指定します。 ファイル名を指定しないと、**<reporttype>-timestamp.CSV** が使用されます。
is-url-encoded	（オプション）この値は、レポート データや組織に URL エンコードされた情報が含まれているかどうかによって true または false に設定します。 デフォルト値は false です。

レポートの識別子のリスト

以下の表に、report-id 引数に使用できるさまざまなレポート識別子を示します。

Report	レポート ID
マイ アクティビティ レポート	AAC.ViewMyActivityReport
管理者アクティビティ レポート	AAC.ViewActivityReport
ユーザ アクティビティ レポート	AAC.ViewUserActivityReport
組織レポート	AAC.ViewOrgActivityReport

レポート URL のリスト

以下の表に、reporturl 引数に使用できるさまざまなレポート URL を示します。

Report	レポート URL
マイ アクティビティ レポート	/Ac_AdminMyActivity/view.htm
管理者アクティビティ レポート	/Ac_Adminreport/view.htm
ユーザ アクティビティ レポート	/Ac_AdminUserActivity/view.htm
組織レポート	/Ac_AdminOrgActivity/view.htm

ツールの使用例

ユーザ アクティビティ レポートをダウンロードするためのコード スニペットを以下に示します。

```
java –jar arreporttool.jar --protocol http --host localhost --port
8080
-- admin-org-id arcot --admin-id ga --admin-password ga123
--report-id AAC.ViewUserActivityReport --report-url
/Ac_AdminUserActivity/view.htm --startdate-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log -- organizations
ARCOT –-userName ua
```

組織レポートをダウンロードするためのコード スニペットを以下に示します。

```
java -jar arreporttool.jar --protocol http --host localhost --port
8080 -- admin-org-id arcot --admin-id ga --admin-password ga123
--report-id AAC.ViewOrgActivityReport –report-url
/Ac_AdminOrgActivity/view.htm --start-date-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log --organizations
ARCOT;TEST
```

第 13 章: CA Strong Authentication のログ

CA Strong Authentication サーバとアプリケーションの間の通信を効果的に管理するには、サーバのアクティビティとパフォーマンス、および発生の可能性がある問題に関する情報が必要とされます。

ログ ファイルについて

これらのファイル内のログ記録を制御するパラメータは、管理コンソール ログ ファイル、UDS ログ ファイル、および CA Strong Authentication サーバ スタートアップ ログ ファイルの場合は関連する INI ファイルを使用することにより、CA Strong Authentication ログ ファイルの場合は管理コンソール自体を使用することにより設定できます。これらのファイル中で変更できる主なログ記録設定オプションには以下のものが含まれます。

- **Specifying log file name and path：** CA Strong Authentication ではログ ファイルの書き込み先およびバックアップ ログ ファイルの保存先のディレクトリを指定できます。診断ログ記録ディレクトリを指定することにより、管理者はシステムとネットワークのリソースを管理できます。
- **Log file size：** ログ ファイルに保存できる最大バイト数。 ログ ファイルがこのサイズに達すると、新しいファイルが作成され、古いファイルがバックアップ ディレクトリに移動されます。
- **Using log file archiving**： CA Strong Authentication コンポーネントが診断メッセージを実行し生成すると共に、ログ ファイルのサイズは増加します。ログ ファイルのサイズが増加し続けるように許可する場合、管理者はログ ファイルを手動で監視しクリーンアップする必要があります。 CA Strong Authentication では、収集されて保存されるログ ファイル データの量を制限する設定オプションを指定できます。CA Strong Authentication では、診断ログ ファイルのサイズを制御する設定オプションを指定することができます。この設定により、ログ ファイルの最大サイズを指定できます。 最大サイズに達すると、古いログ情報がバックアップ ファイルに移動され、その後新しいログ情報が保存されます。
- **Setting logging levels：** CA Strong Authentication ではログ レベルも設定できます。 ログ レベルを設定して、診断ログ ファイルに保存されるメッセージ数を減らしたり、増やしたりすることができます。 たとえば、クリティカルなメッセージのみをレポートおよび保存するように、ログ レベルを設定できます。 サポートされているログ レベルの詳細については、「サポートされる重大度レベル (P. 321)」を参照してください。
- **Specifying time zone information：** CA Strong Authentication ではログ記録された情報のタイム スタンプに、ローカル タイムゾーンまたは GMT を使用できます。

インストール ログ ファイル

CA Strong Authentication をインストールする際に、インストーラは、インストール中にユーザが指定した情報、およびインストーラが実行したアクション（CA Strong Authentication ディレクトリ構造の作成、レジストリ エントリの作成など）を Arcot_WebFort_Install_*[assign the value for mm in your book]*_<dd>_<yyyy>_<hh>_*[assign the value for mm in your book]*_*SpectroSERVER*.log ファイルにすべて記録します。 このファイルの情報は、CA Strong Authentication インストールが正常に完了しなかった場合、問題の原因を特定するために非常に役立ちます。

このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合：

<install_location>¥

UNIX

<install_location>/

AuthMinder サーバ スタートアップ ログ ファイル

CA Strong Authentication サーバを起動すると、スタートアップ（またはブート）操作がすべて arcotwebfortstartup.log ファイルに記録されます。 CA Strong Authentication サービスが起動しない場合、問題の原因を特定するためにこのファイルの情報が役立ちます。

このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合：

<install_location>¥Arcot Systems¥logs¥

UNIX の場合：

<install_location>/arcot/logs/

AuthMinder サーバ ログ ファイル

プロトコル設定、プロファイル設定などの CA Strong Authentication サーバ設定を行うと、これらの設定が arcotwebfort.log ファイルに書き込まれます。 このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX の場合:

```
<install_location>/arcot/logs/
```

このファイルのログを制御するパラメータは、管理コンソールで設定できます。 パラメータを設定するには、対象のインスタンスを［**インスタンス管理**］画面でクリックし、インスタンス固有のサブ画面を使用します。

ログ ファイル パス、ログ ファイルの最大サイズ（バイト単位）、バックアップ ディレクトリ、ロギング レベル、およびタイム スタンプ情報に加えて、トレース ロギングを有効にするかどうかも制御できます。このファイルで使用されるデフォルトの形式については、「AuthMinder ログ ファイルの形式 (P. 319)」を参照してください。

UDS ログ ファイル

UDS (ユーザ データ サービス) 情報およびアクションはすべて arcotuds.log ファイルに記録されます。 この情報には、以下のものが含まれます。

- UDS データベースの接続情報
- UDS データベースの設定情報
- UDS インスタンス情報、およびこのインスタンスによって実行されたアクション

このファイル内の情報は、管理コンソールが UDS インスタンスに接続できなかった場合に問題の原因を特定するうえで役立ちます。 このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX の場合:

```
<install_location>/arcot/logs/
```

このファイルでのログ記録を制御するパラメータは、udsserver.ini ファイルを使用することによって設定できます。このファイルは、ARCOT_HOME の conf フォルダにあります。

ロギング レベル、ログ ファイル名およびパス、ファイルの最大サイズ (バイト単位) 、ならびにアーカイブ情報に加えて、log4j.appender.debuglog.layout.ConversionPattern に対する適切な値を指定することにより、UDS のログ記録パターンのレイアウトも制御できます。このファイルで使用されるデフォルトの形式については、「UDS および管理コンソールのログ ファイル形式 (P. 320)」を参照してください。

管理コンソール ログ ファイル

管理コンソールを展開して起動すると、そのすべてのアクションおよび処理されたリクエストの詳細が arcotadmin.log ファイルに記録されます。 この情報には、以下のものが含まれます。

- データベースの接続情報
- データベースの設定情報
- インスタンス情報、およびこのインスタンスによって実行されたアクション
- UDS 設定情報
- キャッシュ リフレッシュなど、マスタ管理者が指定したその他の管理コンソール情報

このファイル内の情報は、管理コンソールが開始しない場合に問題の原因を識別するうえで非常に役立ちます。 このファイルのデフォルトの場所は、以下のとおりです。

Windows の場合:

```
<install_location>¥Arcot Systems¥logs¥
```

UNIX の場合:

```
<install_location>/arcot/logs/
```

このファイルでのログ記録を制御するパラメータは、adminserver.ini ファイルを使用することによって設定できます。このファイルは、ARCOT_HOME の conf フォルダにあります。

ログ レベル、ログ ファイル名およびパス、ログ ファイルの最大サイズ（バイト単位）、ならびにログ ファイルのアーカイブ情報に加えて、log4j.appender.debuglog.layout.ConversionPattern に対する適切な値を指定することにより、コンソールのログ記録パターンのレイアウトも制御できます。このファイルで使用されるデフォルトの形式については、「UDS および管理コンソールのログ ファイル形式 (P. 320)」を参照してください。

AuthMinder ログ ファイルの形式

以下の表に、以下の CA Strong Authentication ロガーのエントリの形式を示します。

- arcotwebfort.log （AuthMinder サーバ ログ ファイル (P. 316)）
- arcotwebfortstartup.log （AuthMinder サーバ スタートアップ ログ ファイル (P. 315)）

列	Description
タイム スタンプ	エントリがログに記録された時刻は、設定したタイムゾーンに変換されます。 この情報のログの形式は次のとおりです。 mm/dd/yy HH: MM: SS.mis mis はミリ秒を表します。
ログ レベル（LEVEL）（または重大度）	ログに記録されたエントリの重大度レベル。 詳細については、「サポートされる重大度レベル (P. 321)」を参照してください。 **注**: CA Strong Authentication ではトレース ログも作成されます。このログには、フローの詳細が含まれます。トレース ログは、arcotwebfort.log ファイルに記録されます。 トレース メッセージのエントリは「TRACE」で始まります。
プロトコル名（PROTOCOLNAME）	トランザクションに使用されたプロトコル。 以下の値が使用可能です。 ■ TXN_NATIVE ■ ADMIN_WS ■ ASSP_WS ■ RADIUS ■ SVRMGMT_WS ■ TXN_WS サーバが起動中、シャットダウン中、またはモニタリング モードのときはプロトコルは使用されないため、それぞれ次の値が表示されます。 ■ STARTUP ■ SHUTDOWN ■ MONITOR
スレッド ID（THREADID）	このエントリをログに記録したスレッドの ID。

列	Description
トランザクション ID（000TXNID）	このエントリをログに記録したトランザクションの ID。
メッセージ	自由形式でログ ファイルに記録されるメッセージ。 **注**: メッセージの情報量は、ログ ファイルに設定した**ログ レベル**によって異なります。

UDS および管理コンソールのログ ファイル形式

以下の表に、以下のロガーのエントリの形式を示します。

- arcotuds.log （UDS ログ ファイル (P. 317)）
- arcotadmin.log （管理コンソール ログ ファイル (P. 318)）

列	関連付けられたパターン（ログ ファイル内）	Description
タイム スタンプ	%d{yyyy-MM-dd hh:mm:ss,SSS z} :	エントリがログ記録された時刻です。 このエントリはアプリケーション サーバのタイム ゾーンを使用します。 この情報のログの形式は次のとおりです。 yyyy-MM-dd hh:mm:ss,SSS z ここで、SSS はミリ秒を表します。
スレッド ID	[%t] :	このエントリをログに記録したスレッドの ID。
ログ レベル（または重大度）	%-5p :	ログに記録されたエントリの重大度レベル。 詳細については、「サポートされる重大度レベル (P. 321)」を参照してください。
ロガー クラス	%-5c{3}(%L) :	ログ リクエストを作成したロガーの名前です。
メッセージ	%m%n :	自由形式でログ ファイルに記録されるメッセージ。 **注**: メッセージの情報量は、ログ ファイルに設定した**ログ レベル**によって異なります。

UDS ログ ファイルおよび管理コンソール ログ ファイルの **PatternLayout** パラメータをカスタマイズするには、以下の URL を参照してください。

http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html

サポートされる重大度レベル

ログ レベル（*重大度レベル*）を使用して、CA Strong Authentication ログに保存される情報の詳細のレベルを指定できます。また、この設定により、ログ ファイルが増大する速度を制御できます。

サーバ ログ ファイルのセキュリティ レベル

以下の表に、すべてのログ ファイルに出現するログ レベルを重大度の*降順*で示します。

［Log Level］		Description
0	FATAL	CA Strong Authentication サービスの突然の終了を引き起こす可能性がある、重大で回復不可能なエラーにはこのログ レベルを使用します。
1	注意	望まないランタイム例外、潜在的に有害な状況、および回復可能で FATAL（致命的）ではない問題にはこのログ レベルを使用します。
2	INFO	ランタイム イベントに関する情報を取得する場合にこのログ レベルを使用します。 言い換えれば、この情報は、アプリケーションの進捗状況を強調します。進捗状況には、次の変化が含まれます。 ■ 起動、停止、再起動などのサーバ状態。 ■ サーバのプロパティ。 ■ サービスの状態。 ■ サーバ上のプロセスの状態。
3	DEBUG	デバッグ目的で詳細情報をログに記録する場合に、このログ レベルを使用します。 これには、プロセス追跡およびサーバ状態の変化が含まれる場合があります。

注: CA Strong Authentication サーバ（arcotwebfort.log）では、これらの任意のレベルのログを設定でき、トレース ログを有効にしてフローの詳細を取得することもできます。

注: ログ レベルを指定すると、それよりも重要度が*高い*レベルのメッセージもレポートされます。 たとえば、LogLevel が 3 と指定されている場合、FATAL、WARNING、および INFO の各レベルのログ レベルを持つメッセージも収集されます。

管理コンソール ログ ファイルおよび UDS ログ ファイルの重大度レベル

以下の表に、管理コンソール ログ ファイルおよび UDS ログ ファイルに出現するログ レベルを重大度の*降順*で示します。

［Log Level］		Description
0	OFF	ログ記録をすべて無効にするには、このレベルを使用します。
1	FATAL	管理コンソールまたは UDS の突然の終了を引き起こす可能性がある、重大で回復不可能なエラーにはこのログ レベルを使用します。
2	注意	望まないランタイム例外、潜在的に有害な状況、および回復可能で FATAL（致命的）ではない問題にはこのログ レベルを使用します。
3	ERROR	アプリケーションの実行を続行できるエラー イベントを記録するには、このログ レベルを使用します。
4	INFO	ランタイム イベントに関する情報を取得する場合にこのログ レベルを使用します。 言い換えれば、この情報は、アプリケーションの進捗状況を強調します。進捗状況には、次の変化が含まれます。 ■ 起動、停止、再起動などのサーバ状態。 ■ サーバのプロパティ。 ■ サービスの状態。 ■ サーバ上のプロセスの状態。
5	TRACE	DEBUG より詳しい情報イベントを取得する場合にこのログ レベルを使用します。
6	DEBUG	デバッグ目的で詳細情報をログに記録する場合に、このログ レベルを使用します。 これには、プロセス追跡およびサーバ状態の変化が含まれる場合があります。
7	すべて	ログ記録をすべて有効にするには、このログ レベルを使用します。

注: ログ レベルを指定すると、それよりも重要度が*高い*レベルのメッセージもレポートされます。 たとえば、LogLevel が 4 と指定されている場合、FATAL、WARNING、ERROR、および INFO の各ログ レベルを持つメッセージも収集されます。

各ログ レベルのサンプル エントリ

以下のサブセクションでは、AuthMinder ログ ファイル内のサンプル エントリを（ログ レベルごとに）示します。

FATAL

```
09/07/17 11:49:20.404  FATAL  STARTUP  00002872  00WFMAIN - Unable to
initialize the database

09/07/17 11:49:20.405  FATAL  STARTUP  00002872  00WFMAIN - Failed to
load the ini parameters

09/07/17 11:49:20.406  FATAL  STARTUP  00002872  00WFMAIN - Cannot
continue due to setConfigData failure, SHUTTING DOWN
```

注意

```
09/07/17 12:50:05.848  INFO  AUTH_NATIVE  00002780  00022508 - Fail
to connect to Database prdsn for 1 time(s). DbUsername system

09/07/17 12:50:05.848  INFO  AUTH_NATIVE  00002780  00022508 -
ReportError: SQL Error State:08001, Native Error Code: FFFFFFFF, ODBC
Error: [Arcot Systems][ODBC Oracle Wire Protocol
driver][Oracle]TNS-12505: TNS:listener could not resolve SID given in
connect descriptor
```

INFO

```
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mMinConnections [4]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mMaxConnections [128]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mCurrPoolSize   [4]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mNumDBFailure     [0]
09/07/17 11:51:20.166 INFO MONITOR 00000424 STATSMON - mCurrNumUsed
[0]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mCurrNumAvailable [4]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [0]
mNumTimesConnIdxLocked   [24]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [0]
mNumTimesConnIdxReleased [24]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [1]
mNumTimesConnIdxLocked   [24]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [1]
mNumTimesConnIdxReleased [24]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [2]
mNumTimesConnIdxLocked   [24]
```

```
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [2]
mNumTimesConnIdxReleased [24]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [3]
mNumTimesConnIdxLocked   [23]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [3]
mNumTimesConnIdxReleased [23]
09/07/17 11:51:20.166  INFO  MONITOR  00000424  STATSMON - ----------
logging stats for databse [wf-test-p] : [primary] [ACTIVE] end
----------
```

DEBUG

```
10/03/25 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBPoolManagerImpl::getLockedDBConnection: [primary] DSN [webfort]
is active. Will get the connection from this
10/03/25 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBPoolManagerImpl::getLockedDBConnection: Returning DBPool
[0112FD80]
10/03/25 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBM::Number of queries being executed [1]
10/03/25 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBM::Found query string for query-id : [SSL_TRUST_STORE_FETCH_ALL].
10/03/25 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBM::Executing Query[ArWFSSLTrustStoreQuery_FetchAll]
10/03/25 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 - Number
of rows fetched : 0
```

(AuthMinder サーバのみ)トレース ログ

```
10/03/25 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
Released Cache read lock on [01129D98]
10/03/25 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
CallTrace::Leaving : [ArDBPoolManagerImpl::selectAnActivePool].
time : 0
10/03/25 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
CallTrace::Entering : [ArDBPool::getLockedDBConnectionConst]
10/03/25 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
ArDBPool::getLockedDBConnection [(primary)] : GotContext [1], [3]
more connections available
10/03/25 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
CallTrace::Leaving : [ArDBPool::getLockedDBConnectionConst]. time :
0
```

付録 A: マルチバイト文字および暗号化されるパラメータ

CA Strong Authentication は UTF-8 をサポートしています。これは、ユニバーサル Unicode エンコーディング スキームの可変長 8 ビットのエンコード形式です。

注: UTF-8 の設定の詳細については、「*CA Strong Authentication インストール ガイド*」の「クライアント システムの UTF-8 サポートの設定」を参照してください。

CA Strong Authentication では、ハードウェアまたはソフトウェア ベースの機密データの暗号化も使用できます。 機密パラメータを暗号化することを選択でき、レポートにクリア テキスト データを表示するか、暗号化されたデータを表示するかを決定することもできます。

以下の表に、暗号化およびマルチバイト文字のエンコーディングに選択できるユーザと認証情報のパラメータを示します。 また、パラメータに使用するキーや、キーを使用できるレベルについても示します。

注: この表の「キー タイプ」列に示すキーは、HSM に格納できます。

パラメータ	マルチバイト	暗号化	Salt の追加	キー レベル	キー タイプ	大文字と小文字の区別
User Name	はい	オプション	いいえ	組織レベル	組織キー	はい
ユーザ属性	はい	オプション	いいえ	組織レベル	組織キー	はい
Password	はい	はい	はい	組織レベル	組織キー	いいえ
ワンタイム パスワード	いいえ	はい	はい	組織レベル	組織キー	いいえ
OATH シード	いいえ	はい	はい	組織レベル	OATH マスタ キー	いいえ
OATH OTP	いいえ	いいえ	いいえ	NA	NA	いいえ

パラメータ	マルチバイト	暗号化	Salt の追加	キー レベル	キー タイプ	大文字と小文字の区別
ArcotOTP OATH シード	いいえ	はい	はい	組織レベル	ArcotOTP OATH マスタ キー	いいえ
ArcotOTP OATH OTP	いいえ	いいえ	いいえ	NA	NA	いいえ
ArcotOTP EMV シード	いいえ	はい	はい	組織レベル	ArcotOTP EMV マスタ キー	いいえ
ArcotOTP EMV OTP	いいえ	いいえ	いいえ	NA	NA	いいえ
Q&A 質問	はい	はい	はい	組織レベル	組織キー	はい
Q&A 回答	はい	はい	はい	組織レベル	組織キー	はい
ArcotID 秘密キー	いいえ	はい	はい	組織レベル	組織キー	いいえ
ArcotID プライマリ キー	いいえ	はい	はい	組織レベル	ArcotID マスタ キー	いいえ
ワンタイム トークン	いいえ	はい	はい	組織レベル	グローバル キー	いいえ
EMV 用のアカウント ID	はい	はい	はい	組織レベル	組織キー	はい
一時的なデータ暗号化キー	いいえ	はい	いいえ	グローバル レベル	グローバル キー	いいえ
ネイティブ トークン	いいえ	はい	いいえ	グローバル レベル	一時的なデータ暗号化キー	いいえ
パスワード チャレンジ	いいえ	はい	はい	グローバル レベル	一時的なデータ暗号化キー	いいえ
ArcotID チャレンジ	いいえ	はい	いいえ	グローバル レベル	一時的なデータ暗号化キー	いいえ

パラメータ	マルチバイト	暗号化	Salt の追加	キー レベル	キー タイプ	大文字と小文字の区別
Q&A 質問 ID	いいえ	はい	いいえ	グローバル レベル	一時的なデータ暗号化キー	いいえ
認証情報のカスタム属性	はい	はい	いいえ	組織レベル	組織キー	はい

以下の表に、暗号化およびマルチバイト文字のエンコーディングに選択できる設定パラメータを示します。 また、パラメータに使用するキーや、キーを使用できるレベルについても示します。

注: この表の「キー タイプ」列に示すキーは、HSM に格納できます。

パラメータ	マルチバイト	暗号化	Salt の追加	キー レベル	キー タイプ	大文字と小文字の区別
アップロードされたトークン内の OATH シード	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
RADIUS 共有秘密キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
SAML 署名キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
ASSP SAML 署名キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
ASSP Kerberos 認	はい	はい	はい	グローバル レベル	グローバル キー	いいえ

パラメータ	マルチバイト	暗号化	Salt の追加	キー レベル	キー タイプ	大文字と小文字の区別
証情報	はい	はい	はい	組織レベル	組織キー	いいえ
ArcotID CA キー	いいえ	はい	いいえ	グローバル レベル	グローバル キー	いいえ
ArcotID マスタ キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
OATH OTP マスタ キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
ArcotOTP OATH OTP マスタ キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
ArcotOTP EMV OTP マスタ キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
	いいえ	はい	はい	組織レベル	組織キー	いいえ
SSL 署名キー	いいえ	はい	はい	グローバル レベル	グローバル キー	いいえ
メッセージ	はい	いいえ	いいえ	NA	NA	はい
表示名	はい	いいえ	いいえ	NA	NA	はい
監査 - 理由	はい	いいえ	いいえ	NA	NA	いいえ
監査 - イベント メッセージ	はい	いいえ	いいえ	NA	NA	いいえ
監査 - 内部追加情報	はい	いいえ	いいえ	NA	NA	いいえ

パラメータ	マルチバイト	暗号化	Salt の追加	キー レベル	キー タイプ	大文字と小文字の区別
監査 - 外部追加情報	はい	いいえ	いいえ	NA	NA	いいえ
ユーザ属性チェック	はい	いいえ	いいえ	NA	NA	いいえ

付録 B: サーバ リフレッシュおよび再起動タスクのサマリ

設定変更を行うと、サーバを再起動しなければならない場合があります。たとえば、.ini ファイルを変更する場合はすべて、サーバを再起動する必要があります。また、管理コンソールを使用して変更を行った場合にも、サーバを再起動またはリフレッシュが必要になることがあります。 そのような場合、管理コンソールが必要に応じてリフレッシュまたは再起動するようにユーザに通知します。

注: リフレッシュを選択した場合、サーバのダウン タイムは一切発生しません。

以下の表に、設定変更を行った後にリフレッシュまたは再起動が必要になるサーバ タスクを示します。

タスク	リフレッシュ	再起動
UDS 接続の設定	✓	
UDS の設定	✓	
属性の暗号化の設定	✓	
カスタム ロケールの設定	✓	
デフォルト組織の設定	✓	
アカウント タイプの追加	✓	
アカウント タイプの更新	✓	
アカウント タイプの削除	✓	
アカウント タイプへのカスタム属性の追加	✓	
電子メール/電話のタイプの設定	✓	
基本認証ポリシーの設定	✓	
Web サービスの認証および許可の有効化	✓	
AuthMinder 接続		✓

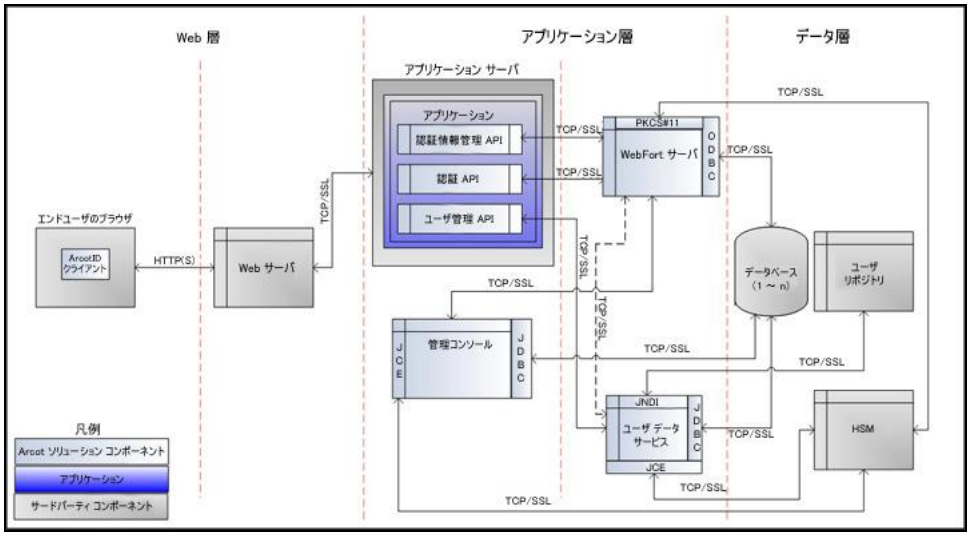
タスク	リフレッシュ	再起動
［インスタンス管理］ページを使用する以下の操作の更新 ■ ［Log Level］ ■ トレース ログの有効化 ■ クエリ詳細のログ	✓	
［インスタンス管理］ページを使用する以下の操作の更新 ■ インスタンス属性 ■ トランザクション ログ ディレクトリ ■ ロールオーバー開始サイズ ■ トランザクション ログ バックアップ ディレクトリ ■ GMT でのタイム スタンプのログ記録 ■ データベース構成		✓
トラステッド認証機関	✓	
プロトコルの管理	✓	✓
［その他の設定］ページを使用する［**一般**］設定の更新	✓	
［その他の設定］ページを使用する［**認証メカニズム ステータスの変更**］の更新		✓
プロファイル設定	✓	
ポリシー設定	✓	
認証情報キー管理	✓	
SAML トークン設定	✓	
ASSP 設定	✓	
認証情報タイプ解決	✓	
プラグイン登録	✓	✓
プラグイン設定	✓	
デフォルト設定の割り当て	✓	
RADIUS クライアント	✓	
RADIUS プロキシ	✓	

付録 C: SSL の設定

CA Strong Authentication コンポーネントは、コンポーネント間の通信に TCP を使用します。SSL（Secure Socket Layer）をサポートするように Server Management プロトコルおよび Transaction Native プロトコルを設定することで、安全性の低いメディア上でアプリケーションどうしが安全に通信できるようにします。

CA Strong Authentication コンポーネントおよび通信モード

以下の図は、CA Strong Authentication とそのコンポーネントの間でサポートされている通信モードを示しています。



コンポーネント間の通信のデフォルト モードは TCP です。 CA Strong Authentication サーバは、トランザクション中に交換されるデータの整合性と機密性を確保するために、以下のコンポーネントとの SSL 通信（双方向および一方向）をサポートしています。

- 管理コンソール
- ユーザ データ サービス
- AuthMinder データベース（一方向のみ）
- AuthMinder Java SDK （認証および発行）
- AuthMinder Web サービス（認証および発行）

SSL 通信の準備

CA Strong Authentication コンポーネント間の SSL 通信を有効にするには、まずサーバとクライアントの証明書を取得します。 これらの証明書は、以下のいずれかの方法を使用して取得できます。

- 認証機関（CA）から直接取得（P. 335）
- ユーティリティを使用した証明書リクエストの生成（P. 339）

CA がユーザ用の証明書を生成すると（「認証機関（CA）から直接取得 (P. 335)」を参照）、その証明書と関連付けられた秘密キーも生成されます。その結果、秘密キーはユーザ側で生成されるときほど安全ではない場合があります。キーが「オフサイト」で生成されないようにするには、「ユーティリティを使用した証明書リクエストの生成 (P. 339)」の手順に従います。

認証機関（CA）から直接取得

Microsoft CA 2008 で有効

次の手順に従ってください:

1. 任意の CA へのリンクにアクセスします。 Microsoft CA の場合は、以下のとおりです。

   http://<IP_Address_of_the_CA>/certsrv/

2. 証明書リクエストを作成し、サブミットするためのリンクに移動します。

   たとえば、**MSCA** を使用する場合、［**タスクの選択**］セクションで、［**証明書の要求**］オプション、［**証明書の要求の詳細設定**］オプション、［**この CA への要求を作成し送信する**］オプションの順にクリックします。

3. 表示される証明書リクエスト フォームで詳細を指定します。

   - 証明書の識別情報について、以下の表で説明します。

証明書属性	必要な情報
共通名 （名前）	サーバの完全修飾ドメイン名（FQDN）。 共通名の入力を促すメッセージが表示されたら、SSL によって保護されるサーバの完全修飾ドメイン名（FQDN）を指定する*必要があります*。 たとえば、login.my-bank.com に対して発行された SSL 証明書は、online.my-partner.com に対して有効に*なりません*。 SSL に対して使用される URL が login.my-bank.com である場合は、CSR でサブミットされた共通名が login.my-bank.com であることを確認します。
［Email Address］	組織内の担当者の電子メール ID。 通常、これは、証明書管理者または IT 部門の管理者の電子メール アドレスです。
組織 （会社）	組織の名前。 このエントリが短縮されて*いない*ことを確認します。また、Inc.、Corp.、LLC などのサフィックスを指定していないことも確認する必要があります。

証明書属性	必要な情報
組織単位 （部門）	証明書を処理する組織の部門（たとえば IT）。
市区町村 （市区町村）	組織単位がある市区町村（たとえば、ブリズベーン）。
都道府県	組織単位がある都道府県（たとえば、クィーンズランド）。 このエントリが短縮されていないことを確認します。
国 （地域）	組織の本部がある国の ISO コード（たとえば、AU）。

- 証明書の詳細。 これらの証明書の詳細を指定する際には、以下の表で指定されている詳細を考慮してください。

証明書属性	必要な情報
証明書のタイプ	**サーバ認証証明書**： サーバ証明書を生成する場合。 **クライアント認証証明書**： クライアント証明書を生成する場合。
CSP	任意の CSP。
キーの使用方法	キー使用法のタイプとして［**交換**］を選択します。
キー サイズ	バイト単位のキー サイズ。
キーのエクスポート可能性	［**エクスポート可能なキーとしてマークする**］を選択します。
リクエストの形式	証明書をダウンロードする形式を指定します。

4. ［**送信**］をクリックして証明書をリクエストします。
5. ［**この証明書のインストール**］リンクをクリックして、ブラウザ ストアに証明書をインストールします。

証明書のダウンロード

MS CA 2008 を介してリクエストした証明書はブラウザ ストアにインストールされます。そのブラウザ ストアから証明書をダウンロードする必要があります。証明書をダウンロードする必要がある形式は、暗号化モードによって異なります。 ソフトウェア暗号化が使用される場合、証明書は PKCS#12 形式である必要があります。 ハードウェア暗号化が使用される場合、証明書は PEM 形式である必要があります。

PKCS#12 形式の場合

Microsoft CA 2008 を使用して PKCS#12 ファイルに証明書と秘密キーをダウンロードするには、以下の手順に従います。

1. Internet Explorer ウィンドウを開きます。
2. ［**ツール**］-［**インターネット オプション**］に移動します。

   ［インターネット オプション］ダイアログ ボックスが表示されます。
3. ［**コンテンツ**］タブをアクティブにし、［証明書］セクションで［**証明書**］をクリックします。

   ［証明書］ダイアログ ボックスが表示されます。
4. ダウンロードする証明書を選択し、［**エクスポート**］をクリックします。

   ［証明書のエクスポート］ウィザードが表示されます。
5. ウィザードの開始画面で［**次へ**］をクリックします。
6. ［**はい、秘密キーをエクスポートします**］オプションを選択し、［**次へ**］を選択します。
7. ［**Personal Information Exchange - PKCS # 12 (.PFX)**］オプションが選択されていることを確認します。
8. ［**強力な保護を有効にする**］オプションを選択し、［**次へ**］をクリックします。
9. ［**パスワード**］フィールドと［**パスワードの確認入力**］フィールドに PKCS#12 （.PFX）ファイルのパスワードを入力し、［**次へ**］をクリックします。
10. ［**ファイル名**］に PKCS#12 （.PFX）ファイルのダウンロードに使用するファイル名を入力し、［**次へ**］をクリックします。
11. ［**完了**］をクリックして、ウィザードを終了します。

    これで証明書と秘密キーは指定された場所のシステムで利用できます。

PEM 形式の場合

ブラウザ証明書ストアから直接 PEM 形式の証明書をエクスポートすることはできません。したがって、まず DER 形式でダウンロードし、以下のように PEM に変換する必要があります。

Microsoft CA 2008 を使用して、DER 形式で証明書をダウンロードし、これを PEM に変換するには、以下の手順に従います。

1. Internet Explorer ウィンドウを開きます。
2. ［**ツール**］-［**インターネット オプション**］に移動します。

   ［インターネット オプション］ダイアログ ボックスが表示されます。
3. ［**コンテンツ**］タブをアクティブにし、［証明書］セクションで［**証明書**］をクリックします。

   ［証明書］ダイアログ ボックスが表示されます。
4. ダウンロードする証明書を選択し、［**エクスポート**］をクリックします。

   ［証明書のエクスポート］ウィザードが表示されます。
5. ウィザードの開始画面で［**次へ**］をクリックします。
6. ［**いいえ、秘密キーをエクスポートしません**］オプションを選択し、［**次へ**］をクリックします。
7. ［**DER encoded binary X.509 (.CER)**］オプションが選択されていることを確認します。
8. ［**次へ**］をクリックします。
9. ［**ファイル名**］に証明書のダウンロードに使用するファイル名を入力し、［**次へ**］をクリックします。
10. ［**完了**］をクリックして、ウィザードを終了します。

    これで証明書は指定された場所のシステムで利用できます。
11. 証明書を DER 形式から PEM 形式に変換します。OpenSSL などのオープン ソース ツールを使用することもできます。OpenSSL ツールを使用して変換するには、以下のコマンドを使用します。

    openssl x509 -inform der -in <*certificate*>.cer -out <*certificate*>.pem

ユーティリティを使用した証明書リクエストの生成

証明書リクエストは、任意のユーティリティまたはツールを使用して生成できます。その後、証明書リクエストを CA にサブミットして証明書を取得します。

次の手順に従ってください:

1. キーストアを生成します。

   keytool は、*キーストア*と呼ばれるファイルにキーと証明書を格納します。キーストアは、クライアントまたはサーバの識別に使用される証明書のリポジトリです。 通常、キーストアは 1 つのクライアントまたは 1 つのサーバに固有です。デフォルト キーストア実装は、ファイルとしてキーストアを実装します。 これはパスワードを使用して秘密キーを保護します。キーストアは、keytool を実行するディレクトリで作成されます。

   以下のコマンドを使用して、キーストアを生成します。

   ```
   %JAVA_HOME%/bin/keytool -genkey -keyalg RSA -alias
   <server/or/client> -keystore <keystore_name>.jks -storetype JKS
   -storepass <password> -keysize 1024 -validity
   <validity_period_in_days>
   ```

2. 証明書署名リクエスト（CSR）を生成します。

   CSR は暗号化された識別テキストで、証明書が使用されるシステム上で生成する必要があります。 秘密キーは通常 CSR を作成するのと同時に作成されます。

   以下のコマンドを使用して、CSR を生成します。

   ```
   %JAVA_HOME%/bin/keytool -certreq -v -alias <server/or/client>
   -keystore <keystore_name>.jks -storepass <password> -file
   <server/or/client>certreq.csr
   ```

3. 前の手順で生成された CSR を CA にサブミットして証明書を生成します。

   a. 任意の CA へのリンクにアクセスします。

      たとえば、**MSCA** を使用する場合、リンクは以下のようになります。

      http://<IP_Address_of_the_CA>/certsrv/

   b. 証明書リクエストを作成し、サブミットするためのリンクに移動します。

たとえば、**MSCA** を使用する場合、［**タスクの選択**］セクションで、［**証明書の要求**］オプション、［**証明書の要求の詳細設定**］オプション、［**Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信する**］オプションの順にクリックします（または、証明書を更新する場合、base-64-encoded PKCS #7 ファイルを使用して更新リクエストをサブミットします）。 最後に、*<server/or/client>*certreq.csr の内容をコピーして **Base-64-encoded certificate request** フィールドに貼り付け、［**提出**］をクリックします。

c. DER エンコード形式で以下のファイルをダウンロードします。

- *<server/or/client>*cert.cer としての署名された証明書
- *<server/or/client>*cert.p7b としての完全な証明書チェーン
- *<server/or/client>*cacert.cer としての CA 証明書

4. キーストアに証明書チェーンをインポートします。

以下のコマンドを使用します。

```
%JAVA_HOME%/bin/keytool -import -keystore
<server/or/client>keystore.jks -storepass <password> -file
<server/or/client>certchain.p7b -alias <server/or/client>
```

5. OpenSSL などのオープン ソース ツールを使用して、証明書またはキーストアを必要とする形式に変換します。

- DER 形式からの場合
  - DER 形式を PEM 形式に変換するには、以下のコマンドを使用します。

```
openssl x509 -inform der -in <server/or/client>cert.cer -out
<server/or/client>cert.pem
```

  - DER 形式を PKCS#12 に変換するには、まず上記のコマンドを使用して DER を PEM に変換し、次に以下のコマンドを使用して PEM を PKCS#12 に変換します。

```
openssl pkcs12 -export -out <server/or/client>cert.pfx -inkey
privateKey.key -in <server/or/client>cert.cer -certfile
<server/or/client>cacert.cer
```

- P7B 形式からの場合
  - P7B 形式を PEM 形式に変換するには、以下のコマンドを使用します。

```
openssl pkcs7 -print_certs -in <server/or/client>cert.p7b -out
<server/or/client>cert.cer
```

- P7B 形式を PKCS#12 に変換するには、まず上記のコマンドを使用して P7B を PEM に変換し、次に以下のコマンドを使用して PEM を PKCS#12 に変換します。

```
openssl pkcs12 -export -in <server/or/client>cert.cer -inkey
privateKey.key -out <server/or/client>cert.pfx -certfile
<server/or/client>cacert.cer
```

CA Strong Authentication サーバとユーザ データ サービスの間の保護された通信の有効化

CA Strong Authentication サーバとユーザ データ サービス（UDS）の間で一方向 SSL を設定する場合は、管理コンソールの［ユーザ データ サービス接続設定］ページを使用して SSL 通信に必要な UDS サーバ証明書をアップロードする必要があります。 双方向 SSL の場合は、［ユーザ データ サービス接続設定］ページを使用して CA Strong Authentication サーバのクライアント証明書もアップロードする必要があります。

注: この通信では、CA Strong Authentication サーバ がクライアントで、UDS がサーバです。

一方向 SSL の有効化

次の手順に従ってください:

1. UDS が SSL 通信用に展開されているアプリケーション サーバをクリックします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. MA （マスタ管理者）として管理コンソールにログインします。
3. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
4. サブ メニューの［管理コンソール］タブがアクティブであることを確認します。
5. ［システム設定］で、［UDS 接続設定］リンクをクリックして、該当するページを表示します。
6. ［プロトコル］フィールドで、［一方向 SSL］を選択します。
7. ［ポート］の値をデフォルトの SSL ポートに設定します。
8. ［サーバ ルート証明書］フィールドの隣の参照ボタンをクリックし、UDS ルート証明書を選択します。
9. ［保存］をクリックします。
10. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。

双方向 SSL の有効化

次の手順に従ってください:

1. SSL 通信用にユーザ データ サービス（UDS）が展開されているアプリケーション サーバをクリックします。

   詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。

2. MA として管理コンソールにログインします。
3. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
4. サブ メニューの［管理コンソール］タブがアクティブであることを確認します。
5. ［管理コンソール］で、［UDS 接続設定］リンクをクリックし、該当するページを表示します。
6. ［プロトコル］フィールドで、［双方向 SSL］を選択します。
7. ［ポート］の値をデフォルトの SSL ポートに設定します。
8. ［サーバ ルート証明書］フィールドの横の［参照］ボタンをクリックし、UDS ルート証明書を選択します。
9. ［クライアント証明書］フィールドの横の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
10. ［クライアント秘密キー］フィールドの横の［参照］ボタンをクリックし、CA Strong Authentication 秘密キーを選択します。
11. ［保存］をクリックします。
12. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。

管理コンソールと CA Strong Authentication サーバの間の保護された通信の有効化

管理コンソールと CA Strong Authentication サーバとの間で一方向 SSL を設定する場合は、CA Strong Authentication サーバ ルート証明書をアップロードします。この作業は、管理コンソールの［プロトコル管理］（サーバ管理 Web サービス）ページおよび［AuthMinder 接続］（サーバ管理 Web サービス）ページを使用して行います。

双方向 SSL の場合は、管理コンソールの［トラステッド認証局］ページを使用してクライアント ストアを作成し、［プロトコル管理］（サーバ管理 Web サービス）ページを使用してクライアント ストアを設定し、［AuthMinder 接続］（サーバ管理 Web サービス）ページを使用してクライアント証明書を設定する必要があります。

注: この通信では、管理コンソールがクライアントで、CA Strong Authentication サーバがサーバです。

一方向 SSL の有効化

次の手順に従ってください:

1. Web ブラウザから管理コンソールにアクセスします。
2. MA として管理コンソールにログインします。
3. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
4. サブメニューの［CA Strong Authentication］タブをクリックします。
5. ［インスタンス設定］で、［プロトコル管理］リンクをクリックし、該当するページを表示します。

   ［プロトコル設定］ページが表示されます。
6. プロトコルを設定するサーバ インスタンスを選択します。
7. ［プロトコルのリスト］セクションで、［サーバ管理 Web サービス］リンクをクリックします。

   プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - プロトコルが有効であることを確認します。
   - ［トランスポート］フィールドで、［SSL （1 方向）］を選択します。
   - HSM に SSL キーを格納する場合は、［HSM 内のキー］を選択します。
   - （前の手順で［HSM 内のキー］を選択した場合のみ）［証明書チェーン（PEM 形式）］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - ［キー ペアを含む P12 ファイル］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - PKCS#12 ストアのパスワードを［P12 ファイル パスワード］に入力します。
9. ［保存］ボタンをクリックします。
10. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。

11. メイン メニューの［サービスおよびサーバの設定］タブをアクティブにします。
12. サブメニューの［CA Strong Authentication］タブをクリックします。
13. ［システム設定］で、［AuthMinder 接続］リンクをクリックして、該当ページを表示します。

    ［AuthMinder 接続］ページが表示されます。
14. Server Management Web Services プロトコルに対して以下を設定します。
    - CA Strong Authentication サーバの IP アドレスとポート番号が適切に設定されていることを確認します。
    - ［トランスポート］フィールドで、［SSL （1 方向）］を選択します。
    - ［サーバ CA 証明書（PEM）］フィールドの横の［参照］ボタンをクリックして、CA Strong Authentication ルート証明書を選択します。
15. **［保存］**をクリックします。
16. CA Strong Authentication サーバを再起動します。
17. 以下の手順に従って、CA Strong Authentication サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
    b. テキスト エディタで arcotwebfortstartup.log ファイルを開きます。
    c. Server Management Web Services プロトコル（[ServerManagement-WS]）の [ArWFProtocolConfiguration] セクションの以下の行を確認します。
       `PORTTYPE : [SSL]`
    d. ファイルを閉じます。

双方向 SSL の有効化

次の手順に従ってください:

1. SSL 通信用に管理コンソールが展開されているアプリケーション サーバをクリックします。 詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。
2. マスタ管理者アカウントを使用して、管理コンソールにログインします。
3. メイン メニューの［サービスおよびサーバの設定］タブをアクティブにします。
4. サブメニューの［CA Strong Authentication］タブをクリックします。
5. ［インスタンス設定］で、［トラステッド認証機関］リンクをクリックし、該当するページを表示します。

   ［トラステッド認証機関］ページが表示されます。
6. 以下の情報を設定します。
   - ［名前］フィールドに、SSL トラスト ストアの名前を入力します。
   - 参照ボタンをクリックして、管理コンソールが展開されているアプリケーション サーバのルート証明書を選択します。
7. ［保存］ボタンをクリックします。
8. ［インスタンス設定］で、［プロトコル管理］リンクをクリックし、該当するページを表示します。

   ［プロトコル設定］ページが表示されます。
9. プロトコルを設定するサーバ インスタンスを選択します。
10. ［プロトコルのリスト］セクションで、［サーバ管理 Web サービス］リンクをクリックします。

    プロトコルを設定するページが表示されます。
11. 以下のフィールドを設定します。
    - プロトコルが有効であることを確認します。
    - ［トランスポート］フィールドで、［SSL （双方向）］を選択します。
    - HSM に SSL キーを格納する場合は、［HSM 内のキー］を選択します。

- （前の手順で［HSM 内のキー］を選択した場合のみ）［証明書チェーン（PEM 形式）］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
- ［キー ペアを含む P12 ファイル］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
- PKCS#12 ストアのパスワードを［P12 ファイル パスワード］に入力します。
- 手順 6 で作成したクライアント ストアを選択します。

12. ［保存］をクリックします。
13. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。
14. メイン メニューの［サービスおよびサーバの設定］タブをアクティブにします。
15. サブメニューの［WebFort］タブを有効化します。
16. ［システム設定］で、［AuthMinder 接続］リンクをクリックして、該当ページを表示します。

    ［AuthMinder 接続］ページが表示されます。
17. Server Management Web Services プロトコルに対して以下を設定します。
    - CA Strong Authentication サーバの IP アドレスとポート番号が適切に設定されていることを確認します。
    - ［トランスポート］フィールドで、［SSL （双方向）］を選択します。
    - ［サーバ CA 証明書（PEM）］フィールドの横の［参照］ボタンをクリックして、CA Strong Authentication ルート証明書を選択します。
    - ［PKCS#12 内のクライアント証明書キー ペア］フィールドの横の［参照］ボタンをクリックし、管理コンソールが展開されているアプリケーション サーバのルート証明書を含む PKCS#12 ファイルを選択します。
    - ［クライアント PKCS#12 パスワード］フィールドに PKCS#12 ファイルのパスワードを入力します。
18. ［保存］ボタンをクリックします。

19. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」 を参照してください。

20. 以下の手順に従って、CA Strong Authentication サーバで SSL 通信が有効になっていることを確認します。

    a. 以下の場所に移動します。

       - **Windows の場合**

         `<install_location>¥Arcot Systems¥logs`

       - **UNIX の場合**

         `<install_location>/arcot/logs`

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

    c. 以下のセクションを探します。

       Listing : [Successful listeners(Type-Port-FD)]

    d. このセクションで、以下の行を探します。

       ```
       ServerManagement-WS.............................. :
       [SSL-9743-<Internal_listener_identifier>-[subject
       [<cert_subject>] issuer [<cert_issuer>] sn
       [<cert_serial_number>] device [<device_name>]]]
       ```

    e. ファイルを閉じます。

Java SDK と CA Strong Authentication サーバの間の保護された通信の有効化

Java SDK （認証および発行）と CA Strong Authentication サーバ間の一方向 SSL を設定する場合は、まず管理コンソールの［プロトコル管理］ページを使用して Transaction Native プロトコルを設定し、webfort.authentication.properties ファイルおよび webfort.issuance.properties ファイルを設定する必要があります。

双方向 SSL の場合は、管理コンソールの［トラステッド認証局］ページを使用してクライアント ストアを作成し、［プロトコル管理］（ネイティブ トランザクション）ページを使用してクライアント ストアを設定し、［AuthMinder 接続］（ネイティブ トランザクション）ページを使用してクライアント証明書を設定し、webfort.authentication.properties ファイルおよび webfort.issuance.properties のファイルを設定する必要があります。

注: 管理 Web サービスと CA Strong Authentication サーバ間の SSL を有効にする場合は、このセクションの手順に従う必要があります。

注: この通信では、Java SDK に統合されたアプリケーションがクライアントで、CA Strong Authentication サーバがサーバです。

一方向 SSL の有効化

次の手順に従ってください:

1. Web ブラウザから管理コンソールにアクセスします。
2. MA としてログインしていることを確認します。
3. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
4. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
5. ［インスタンス設定］セクションの［プロトコル管理］リンクをクリックすると、［プロトコル設定］ページが表示されます。
6. プロトコルを設定するサーバ インスタンスを選択します。
7. ［プロトコルのリスト］セクションで、Transaction Native プロトコルのリンクをクリックします。

   プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - ［プロトコル ステータス］が［有効］であることを確認します。
   - ［トランスポート］フィールドで、［SSL （1 方向）］を選択します。
   - HSM に SSL キーを格納する場合は、［HSM 内のキー］を選択します。
   - （前の手順で［HSM 内のキー］を選択した場合のみ）［証明書チェーン（PEM 形式）］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - ［キー ペアを含む P12 ファイル］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - PKCS#12 ストアのパスワードを［P12 ファイル パスワード］に入力します。
9. ［保存］ボタンをクリックします。
10. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。
11. 以下の場所に移動します。

- **Windows の場合**
  <*install_location*>¥Arcot Systems¥sdk¥client¥java¥properties
- **UNIX の場合**
  <*install_location*>/arcot/sdk/client/java/properties

12. エディタ ウィンドウで webfort.authentication.properties ファイルを開きます。
    a. 以下のパラメータを設定します。
       - authentication.transport = 1SSL（デフォルトでは、このパラメータは TCP に設定されます）
       - authentication.serverCACertPEMPath = <*PEM 形式のルート証明書の絶対パス*>

       たとえば、次のように指定できます：
       authentication.serverCACertPEMPath =
       <install_location>/certs/<ca_cert>.pem。

       注：webfort.authentication.properties ファイルの詳細については、「CA Strong Authentication インストール ガイド」の「設定ファイルおよびオプション」を参照してください。
    b. 変更を保存して、ファイルを閉じます。
13. エディタ ウィンドウで webfort.issuance.properties ファイルを開きます。
    a. 以下のパラメータを設定します。
       - issuance.transport = SSL （デフォルトで、このパラメータは TCP に設定されます。）
       - issaunce.serverCACertPEMPath = <*PEM 形式のルート証明書の絶対パス*>

       たとえば、次のように指定できます：issuance.serverCACertPEMPath = <install_location>/certs/<ca_cert>.pem。

       注：webfort.issuance.properties ファイルの詳細については、「CA Strong Authentication インストール ガイド」の「設定ファイルおよびオプション」を参照してください。
    b. 変更を保存して、ファイルを閉じます。
14. Java SDK が展開されているアプリケーション サーバを再起動します。

双方向 SSL の有効化

次の手順に従ってください:

1. SSL 通信用に Java SDK が展開されているアプリケーション サーバを有効にします。 詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。
2. Web ブラウザから管理コンソールにアクセスします。
3. MA として管理コンソールにログインします。
4. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
5. サブメニューの［CA Strong Authentication］タブをクリックします。
6. ［インスタンス設定］で、［トラステッド認証機関］リンクをクリックし、該当するページを表示します。

   ［トラステッド認証機関］ページが表示されます。
7. 以下の情報を設定します。
   - ［名前］フィールドに、SSL トラスト ストアの名前を入力します。
   - ［参照］ボタンをクリックし、Java SDK が展開されているアプリケーション サーバのルート証明書を選択します。
8. ［保存］をクリックします。
9. ［インスタンス設定］で、［プロトコル管理］リンクをクリックし、該当するページを表示します。

   ［プロトコル設定］ページが表示されます。
10. プロトコルを設定するサーバ インスタンスを選択します。
11. ［プロトコルのリスト］セクションで、［ネイティブ トランザクション］リンクをクリックします。

    プロトコルを設定するページが表示されます。
12. 以下のフィールドを設定します。
    - プロトコルが有効であることを確認します。
    - ［トランスポート］フィールドで、［SSL （双方向）］を選択します。
    - HSM に SSL キーを格納する場合は、［HSM 内のキー］を選択します。

- （前の手順で［HSM 内のキー］を選択した場合のみ）［証明書チェーン（PEM 形式）］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
- ［キー ペアを含む P12 ファイル］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
- PKCS#12 ストアのパスワードを［P12 ファイル パスワード］に入力します。
- 手順 7 で作成したクライアント ストアを選択します。

13. ［保存］ボタンをクリックします。
14. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。
15. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
16. サブメニューの［CA Strong Authentication］タブをクリックします。
17. ［システム設定］で、［AuthMinder 接続］リンクをクリックして、該当ページを表示します。

    ［AuthMinder 接続］ページが表示されます。
18. Transaction Native プロトコルに対して以下を設定します。
    - CA Strong Authentication サーバの IP アドレスとポート番号が適切に設定されていることを確認します。
    - ［トランスポート］フィールドで、［SSL （双方向）］を選択します。
    - ［サーバ CA 証明書（PEM）］フィールドの横の［参照］ボタンをクリックして、CA Strong Authentication ルート証明書を選択します。
    - ［PKCS#12 内のクライアント証明書キー ペア］フィールドの横の［参照］ボタンをクリックし、Java SDK が展開されているアプリケーション サーバのルート証明書を含む PKCS#12 ファイルを選択します。
    - ［クライアント PKCS#12 パスワード］フィールドに PKCS#12 ファイルのパスワードを入力します。
19. ［保存］ボタンをクリックします。

20. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」 を参照してください。

21. 以下の場所に移動します。

    - **Windows の場合**
      `<install_location>¥Arcot Systems¥sdk¥client¥java¥properties`
    - **UNIX の場合**
      `<install_location>/arcot/sdk/client/java/properties`

22. エディタ ウィンドウで webfort.authentication.properties ファイルを開きます。

    a. 以下のパラメータを設定します。

       - authentication.transport = 2SSL （デフォルトでは、このパラメータは TCP に設定されます）
       - authentication.serverCACertPEMPath = <*PEM 形式のルート証明書の絶対パス*>

       たとえば、次のように指定できます : authentication.serverCACertPEMPath = <install_location>/certs/<ca_cert>.pem。

       - authentication.clientCertKeyP12Path = <*absolute_path_of_Client_Certificate_in_P12_FORMAT*>
       - authentication.clientCertKeyPassword = クライアントの PKCS#12 ファイルのパスワード

       注: webfort.authentication.properties ファイルの詳細については、「CA Strong Authentication インストール ガイド」の「設定ファイルおよびオプション」を参照してください。

    b. 変更を保存して、ファイルを閉じます。

23. エディタ ウィンドウで webfort.issuance.properties ファイルを開きます。

    a. 以下のパラメータを設定します。

       - issuance.transport = SSL （デフォルトで、このパラメータは TCP に設定されます。）
       - issaunce.serverCACertPEMPath = <*PEM 形式のルート証明書の絶対パス*>

       たとえば、次のように指定できます : issuance.serverCACertPEMPath = <install_location>/certs/<ca_cert>.pem。

- issuance.clientCertKeyP12Path = <*absolute_path_of_Client_Certificate_in_P12_FORMAT*>
- issuance.clientCertKeyPassword = クライアントの PKCS#12 ファイルのパスワード

注: webfort.issuance.properties ファイルの詳細については、「CA Strong Authentication インストール ガイド」の「設定ファイルおよびオプション」を参照してください。

b. 変更を保存して、ファイルを閉じます。

24. Java SDK が展開されているアプリケーション サーバを再起動します。
25. 以下の手順に従って、CA Strong Authentication サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
    - **Windows の場合**

    <*install_location*>¥Arcot Systems¥logs

    - **UNIX ベースのプラットフォームの場合**

    <*install_location*>/arcot/logs

    b. テキスト エディタで arcotwebfortstartup.log ファイルを開きます。
    c. 以下のセクションを探します。

    Listing : [Successful listeners(Type-Port-FD)]

    d. このセクションで、以下の行を探します。

```
Transaction-Native.............................. :
[SSL-9742-<Internal_listener_identifier>-[subject
[<cert_subject>] issuer [<cert_issuer>] sn
[<cert_serial_number>] device [<device_name>]]]
```

    e. ファイルを閉じます。

トランザクション Web サービスと CA Strong Authentication サーバの間の保護された通信の有効化

トランザクション Web サービス（認証情報の発行と認証に使用）と CA Strong Authentication サーバの間で一方向 SSL を設定する場合は、まず 管理コンソールの［プロトコル管理］ページを使用して、Transaction Web Services プロトコルを設定する必要があります。

双方向 SSL の場合は、管理コンソールの［トラステッド認証局］ページを使用してクライアント ストアを作成し、［プロトコル管理］（トランザクション Web サービス）ページを使用してクライアント ストアを設定し、［AuthMinder 接続］（トランザクション Web サービス）ページを使用してクライアント証明書を設定する必要があります。

注: この通信では、Web サービスと統合されているアプリケーションがクライアントで、CA Strong Authentication サーバがサーバです。

一方向 SSL の有効化

次の手順に従ってください:

1. Web ブラウザから管理コンソールにアクセスします。
2. MA （マスタ管理者）として管理コンソールにログインします。
3. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
4. サブメニューの［CA Strong Authentication］タブがアクティブであることを確認します。
5. ［インスタンス設定］セクションの［プロトコル管理］リンクをクリックすると、［プロトコル設定］ページが表示されます。
6. プロトコルを設定するサーバ インスタンスを選択します。
7. ［プロトコルのリスト］セクションで、Transaction Web Services プロトコルのリンクをクリックします。

   プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - ［プロトコル ステータス］が［有効］であることを確認します。
   - ［トランスポート］フィールドで、［SSL （1 方向）］を選択します。
   - HSM に SSL キーを格納する場合は、［HSM 内のキー］を選択します。
   - （前の手順で［HSM 内のキー］を選択した場合のみ）［証明書チェーン（PEM 形式）］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - ［キー ペアを含む P12 ファイル］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - PKCS#12 ストアのパスワードを［P12 ファイル パスワード］に入力します。
9. ［保存］をクリックします。
10. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。

双方向 SSL の有効化

次の手順に従ってください:

1. SSL 通信用に Web サービスと統合されているクライアントが展開されているアプリケーション サーバを有効にします。詳細については、アプリケーション サーバ ベンダーのドキュメントを参照してください。
2. MA として管理コンソールにログインします。
3. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
4. サブメニューの［CA Strong Authentication］タブをクリックします。
5. ［インスタンス設定］で、［トラステッド認証機関］リンクをクリックし、該当するページを表示します。

   ［トラステッド認証機関］ページが表示されます。
6. 以下の情報を設定します。
   - ［名前］フィールドに、SSL トラスト ストアの名前を入力します。
   - 参照ボタンをクリックして、Web サービス クライアントが展開されているアプリケーション サーバのルート証明書を選択します。
7. ［保存］をクリックします。
8. ［インスタンス設定］で、［プロトコル管理］リンクをクリックし、該当するページを表示します。

   ［プロトコル設定］ページが表示されます。
9. プロトコルを設定するサーバ インスタンスを選択します。
10. ［プロトコルのリスト］セクションで、［トランザクション Web サービス］リンクをクリックします。

    プロトコルを設定するページが表示されます。
11. 以下のフィールドを設定します。
    - プロトコルが有効であることを確認します。
    - ［トランスポート］フィールドで、［SSL （双方向）］を選択します。
    - HSM に SSL キーを格納する場合は、［HSM 内のキー］を選択します。

- （前の手順で［HSM 内のキー］を選択した場合のみ）［証明書チェーン（PEM 形式）］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
- ［キー ペアを含む P12 ファイル］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
- PKCS#12 ストアのパスワードを［P12 ファイル パスワード］に入力します。
- 手順 6 で作成したクライアント ストアを選択します。

12. ［保存］をクリックします。
13. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。
14. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
15. サブメニューの［CA Strong Authentication］タブをクリックします。
16. ［システム設定］で、［AuthMinder 接続］リンクをクリックして、該当ページを表示します。

    ［AuthMinder 接続］ページが表示されます。
17. Transaction Web Services プロトコルに対して以下を設定します。
    - CA Strong Authentication サーバの IP アドレスとポート番号が適切に設定されていることを確認します。
    - ［トランスポート］フィールドで、［SSL （双方向）］を選択します。
    - ［サーバ CA 証明書（PEM）］フィールドの横の［参照］ボタンをクリックして、CA Strong Authentication ルート証明書を選択します。
    - ［PKCS#12 内のクライアント証明書キー ペア］フィールドの横の［参照］ボタンをクリックし、Java SDK が展開されているアプリケーション サーバのルート証明書を含む PKCS#12 ファイルを選択します。
    - ［クライアント PKCS#12 パスワード］フィールドに PKCS#12 ファイルのパスワードを入力します。
18. ［保存］をクリックします。

19. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動」を参照してください。
20. 以下の手順に従って、CA Strong Authentication サーバで SSL 通信が有効になっていることを確認します。
    a. 以下の場所に移動します。
       - **Windows の場合**
         `<install_location>¥Arcot Systems¥logs`
       - **UNIX の場合**
         `<install_location>/arcot/logs`
    b. テキスト エディタで arcotwebfortstartup.log ファイルを開きます。
    c. 以下のセクションを探します。
       Listing : [Successful listeners(Type-Port-FD)]
    d. このセクションで、以下の行を探します。
       ```
       Transaction-WS.............................. :
       [SSL-9744-<Internal_listener_identifier>-[subject
       [<cert_subject>] issuer [<cert_issuer>] sn
       [<cert_serial_number>] device [<device_name>]]]
       ```
    e. ファイルを閉じます。

arwfutil と CA Strong Authentication サーバの間の保護された通信の有効化

ユーティリティ ツールの arwfutil (P. 286) と CA Strong Authentication サーバとの間で一方向 SSL を設定する場合は、まず CA Strong Authentication サーバ ルート証明書をアップロードする必要があります。この作業は、管理コンソールの［プロトコル管理］（サーバ管理 Web サービス）ページを使用して行います。その後、arcotcommon.ini ファイルを編集して、トランスポート モードとサーバ証明書を設定します。

双方向 SSL の場合は、管理コンソールの［トラステッド認証局］ページを使用してクライアント ストアを作成し、［プロトコル管理］（サーバ管理 Web サービス）ページを使用してクライアント ストアを設定し、arcotcommon.ini ファイルを編集してトランスポート モードとサーバとクライアントの証明書を設定します。

一方向 SSL の有効化

次の手順に従ってください:

1. Web ブラウザから管理コンソールにアクセスします。
2. MA として管理コンソールにログインします。
3. メイン メニューの［**サービスおよびサーバの設定**］タブをクリックします。
4. サブメニューの［CA Strong Authentication］タブをクリックします。
5. ［**インスタンス設定**］で、［**プロトコル管理**］リンクをクリックし、該当するページを表示します。

   ［プロトコル設定］ページが表示されます。
6. プロトコルを設定する**サーバ インスタンス**を選択します。
7. ［**プロトコルのリスト**］セクションで、［**サーバ管理 Web サービス**］リンクをクリックします。

   プロトコルを設定するページが表示されます。
8. 以下のフィールドを設定します。
   - プロトコルが有効であることを確認します。
   - ［**トランスポート**］フィールドで、［**SSL （1 方向）**］を選択します。
   - HSM に SSL キーを格納する場合は、［**HSM 内のキー**］を選択します。
   - （前の手順で［**HSM 内のキー**］を選択した場合のみ）［**証明書チェーン（PEM 形式）**］フィールドの隣の［**参照**］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - ［**キー ペアを含む P12 ファイル**］フィールドの隣の［**参照**］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
   - PKCS#12 ストアのパスワードを［**P12 ファイル パスワード**］に入力します。
9. ［**保存**］をクリックします。
10. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。

11. 以下の場所に移動します。
    - **Windows の場合**
      `<install_location>¥Arcot Systems¥conf`
    - **UNIX の場合**
      `<install_location>/arcot/conf`
12. エディタ ウィンドウで arcotcommon.ini ファイルを開き、SSL 設定パラメータを追加します。
    a. 以下のセクションをファイルの最後に追加します。

```
[arcot/webfort/wfutil]
Transport=
ReadTimeOut=
ServerRootPEM=
ClientP12=
ClientP12PwdKey=
ClientPEM=
```

以下のセクションに、これらのパラメータの説明を示します。

Transport

arwfutil ユーティリティと CA Strong Authentication サーバの間の通信モード。 サポートされている値は以下のとおりです。

- TCP
- 1SSL
- 2SSL

デフォルト： TCP

ReadTimeout

CA Strong Authentication サーバからのレスポンスに許容される最大時間（ミリ秒）。

デフォルト： デフォルトなし。

ServerRootPEM

サーバの CA 証明書ファイルの完全なパスを指定します。 このファイルは PEM 形式である必要があります。

例：

server.CACertPEMPath=<%SystemDrive%>/certs/webfort_ca.pem

デフォルト： デフォルトなし。

（ソフトウェア暗号化の場合） ClientP12

p12 形式のクライアント証明書のパスを提供します。

デフォルト： デフォルトなし

（ソフトウェア暗号化の場合） ClientP12PwdKey

securestore.enc ファイルに格納されているクライアント P12 のパスワードにアクセスするために使用するキー ラベルを入力します。

デフォルト： デフォルトなし。

（ハードウェア暗号化の場合） ClientPEM

クライアントの CA 証明書ファイルの完全なパスを指定します。このファイルは PEM 形式である必要があります。

デフォルト： デフォルトなし。

b. 変更を保存して、ファイルを閉じます。

13. 以下の手順に従って、CA Strong Authentication サーバで SSL 通信が有効になっていることを確認します。

a. 以下の場所に移動します。

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

c. Server Management Web Services プロトコル（[ServerManagement-WS]）の [ArWFProtocolConfiguration] セクションの以下の行を確認します。
`PORTTYPE : [SSL]`

d. ファイルを閉じます。

双方向 SSL の有効化

次の手順に従ってください:

1. マスタ管理者アカウントを使用して、管理コンソールにログインします。
2. メイン メニューの［サービスおよびサーバの設定］タブをクリックします。
3. サブメニューの［CA Strong Authentication］タブをクリックします。
4. ［インスタンス設定］で、［トラステッド認証機関］リンクをクリックし、該当するページを表示します。

   ［トラステッド認証機関］ページが表示されます。
5. 以下の情報を設定します。
   - ［名前］フィールドに、SSL トラスト ストアの名前を入力します。
   - 参照ボタンをクリックして、arwfutil で使用するルート証明書を選択します。
6. ［保存］をクリックします。
7. ［インスタンス設定］で、［プロトコル管理］リンクをクリックし、該当するページを表示します。

   ［プロトコル設定］ページが表示されます。
8. プロトコルを設定するサーバ インスタンスを選択します。
9. ［プロトコルのリスト］セクションで、［サーバ管理 Web サービス］リンクをクリックします。

   プロトコルを設定するページが表示されます。
10. 以下のフィールドを設定します。
    - プロトコルが有効であることを確認します。
    - ［トランスポート］フィールドで、［SSL （双方向）］を選択します。
    - HSM に SSL キーを格納する場合は、［HSM 内のキー］を選択します。
    - （前の手順で［HSM 内のキー］を選択した場合のみ）［証明書チェーン（PEM 形式）］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。

- ［キー ペアを含む P12 ファイル］フィールドの隣の［参照］ボタンをクリックし、CA Strong Authentication ルート証明書を選択します。
- PKCS#12 ストアのパスワードを［P12 ファイル パスワード］に入力します。
- 手順 6 で作成したクライアント ストアを選択します。

11. ［保存］をクリックします。
12. CA Strong Authentication サーバ インスタンスを再起動します。 CA Strong Authentication サーバを再起動する方法については、「サーバ インスタンスの再起動 (P. 81)」を参照してください。
13. 以下の場所に移動します。
    - **Windows の場合**
      `<install_location>¥Arcot Systems¥conf`
    - **UNIX の場合**
      `<install_location>/arcot/conf`
14. エディタ ウィンドウで arcotcommon.ini ファイルを開き、SSL 設定パラメータを追加します。
    a. 以下のセクションをファイルの最後に追加します。

```
[arcot/webfort/wfutil]
Transport=
ReadTimeOut=
ServerRootPEM=
ClientP12=
ClientP12PwdKey=
ClientPEM=
```

以下のセクションに、これらのパラメータの説明を示します。

Transport

arwfutil ユーティリティと CA Strong Authentication サーバの間の通信モード。 サポートされている値は以下のとおりです。

- TCP
- 1SSL
- 2SSL

デフォルト： TCP

ReadTimeout

CA Strong Authentication サーバからのレスポンスに許容される最大時間（ミリ秒）。

デフォルト： デフォルトなし

ServerRootPEM

サーバの CA 証明書ファイルの完全なパスを指定します。 このファイルは PEM 形式である必要があります。

例：

server.CACertPEMPath=<%SystemDrive%>/certs/webfort_ca.pem

デフォルト： デフォルトなし

（ソフトウェア暗号化の場合） ClientP12

p12 形式のクライアント証明書のパスを提供します。

デフォルト： デフォルトなし

（ソフトウェア暗号化の場合） ClientP12PwdKey

securestore.enc ファイルに格納されているクライアント P12 のパスワードにアクセスするために使用するキー ラベルを入力します。

デフォルト： デフォルトなし

（ハードウェア暗号化の場合） ClientPEM

クライアントの CA 証明書ファイルの完全なパスを指定します。このファイルは PEM 形式である必要があります。

デフォルト： デフォルトなし

b. 変更を保存して、ファイルを閉じます。

15. 以下の手順に従って、CA Strong Authentication サーバで SSL 通信が有効になっていることを確認します。

a. 以下の場所に移動します。

- **Windows の場合**

<*install_location*>¥Arcot Systems¥logs

- **UNIX の場合**

<*install_location*>/arcot/logs

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

c. 以下のセクションを探します。

Listing : [Successful listeners(Type-Port-FD)]

d. このセクションで、以下の行を探します。

```
ServerManagement-WS.............................. :
[SSL-9743-<Internal_listener_identifier>-[subject
[<cert_subject>] issuer [<cert_issuer>] sn
[<cert_serial_number>] device [<device_name>]]]
```

e. ファイルを閉じます。

AuthMinder コンポーネントとデータベースの間の保護された一方向通信の有効化

このセクションでは、CA Strong Authentication コンポーネントと CA Strong Authentication データベースの間の一方向 SSL 通信を設定する手順について説明します。

注: このセクションで説明する設定に進む前に、SSL 通信用のデータベース サーバが有効になっていることを確認してください。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。

CA Strong Authentication サーバとデータベース

CA Strong Authentication は、DataDirect ドライバを使用してデータベースに接続します。 このセクションでは、CA Strong Authentication サーバをインストールしたシステムで実行する必要がある設定について説明します。

Windows の場合

次の手順に従ってください:

1. CA Strong Authentication サーバをインストールしているシステムにログインします。
2. ODBC データ ソース マネージャを開きます。
3. ［システム DSN］タブをクリックします。
4. SSL を設定するために CA Strong Authentication によって使用されるデータ ソースを選択します。
5. ［構成］をクリックします。

   ODBC Oracle Wire Protocol ドライバのセットアップ ダイアログ ボックスが表示されます。
6. ［Encryption］セクションで、［Encryption Method］ドロップダウン リストから［1-SSL Auto］を選択します。
7. ［Truststore］を、CA Strong Authentication によって信頼される有効な認証局（CA）のリストが含まれるトラスト ストア ファイルの場所に設定します。
8. ［Truststore Password］フィールドでトラスト ストアのパスワードを指定します。
9. ［Host Name in Certificate］フィールドをデータベース サーバがインストールされているシステムのホスト名に設定します。 このパラメータについては、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。
10. ［OK］をクリックして設定を保存します。

UNIX の場合

UNIX プラットフォームで CA Strong Authentication とデータベースの間の SSL を有効にするには、odbc.ini ファイルを編集し、DataDirect ドライバを設定する必要があります。

次の手順に従ってください:

1. 以下の場所に移動します。
   `<install_location>/arcot/odbc32v70wf`
2. ファイル エディタで odbc.ini ファイルを開きます。
3. 使用しているデータベースに対応する［*<Database_name>* Wire Protocol］セクションで、SSL 接続に必要なパラメータを編集する必要があります。

   EncryptionMethod

   ドライバが、ドライバとデータベース サーバ間で送信されるデータを暗号化するために使用する方法を指定します。

   このパラメータを 1 に設定すると、SSL を使用してデータが暗号化されます。

   Truststore

   トラスト ストア ファイルの場所を指定します。この場所には、SSL サーバ認証用にクライアント マシンによって信頼されている有効な認証機関（CA）のリストが含まれています。

   TrustStorePassword

   トラスト ストア ストアへのアクセスに必要なパスワードを指定します。

   ValidateServerCertificate

   SSL 認証ハンドシェイクの一環として、サーバのセキュリティ証明書を検証します。

   データベース サーバから送られた証明書を検証するには、このパラメータを 1 に設定します。
4. odbc.ini ファイルを保存して閉じます。

UNIX ベースのプラットフォームの場合

UNIX プラットフォームで CA Strong Authentication とデータベースの間の SSL を有効にするには、odbc.ini ファイルを編集し、DataDirect ドライバを設定する必要があります。

次の手順に従ってください:

1. 以下の場所に移動します。
   `<install_location>/arcot/odbc32v70wf`
2. ファイル エディタで odbc.ini ファイルを開きます。
3. 使用しているデータベースに対応する［*<Database_name>* Wire Protocol］セクションで、SSL 接続に必要なパラメータを編集する必要があります。

   EncryptionMethod

   ドライバが、ドライバとデータベース サーバ間で送信されるデータを暗号化するために使用する方法を指定します。

   このパラメータを 1 に設定すると、SSL を使用してデータが暗号化されます。

   Truststore

   トラスト ストア ファイルの場所を指定します。この場所には、SSL サーバ認証用にクライアント マシンによって信頼されている有効な認証機関（CA）のリストが含まれています。

   TrustStorePassword

   トラスト ストア ストアへのアクセスに必要なパスワードを指定します。

   ValidateServerCertificate

   SSL 認証ハンドシェイクの一環として、サーバのセキュリティ証明書を検証します。

   データベース サーバから送られた証明書を検証するには、このパラメータを 1 に設定します。
4. odbc.ini ファイルを保存して閉じます。

管理コンソールとデータベース

管理コンソールは、Java Database Connectivity （JDBC）を使用して、データベースに接続します。

次の手順に従ってください:

1. SSL 用に管理コンソールが展開されているアプリケーション サーバを設定します。
2. arcotcommon.ini ファイル内の TrustStorePath.*<N>* および HostNameInCertificate.*<N>* パラメータを設定します。

   注: arcotcommon.ini パラメータの詳細については、「CA Strong Authentication インストール ガイド」の「設定ファイルおよびオプション」を参照してください。

ユーザ データ サービスとデータベース

UDS は JDBC を使用して、データベースに接続します。

次の手順に従ってください:

1. UDS が SSL 用に展開されているアプリケーション サーバを設定します。
2. arcotcommon.ini ファイル内の TrustStorePath.*<N>* および HostNameInCertificate.*<N>* パラメータを設定します。

注: arcotcommon.ini パラメータの詳細については、「CA Strong Authentication インストール ガイド」の「設定ファイルおよびオプション」を参照してください。

付録 D: 管理コンソールのエラーのトラブルシューティング

この付録では、管理コンソールの使用時に発生する可能性があるエラーを解決するのに役立つトラブルシューティング手順について説明します。

トラブルシューティング タスクを実行する前に、管理コンソールのログ ファイル（arcotadmin.log）でエラーがあるかどうかを確認してください。デフォルトでは、arcotadmin.log ファイルは以下の場所に保存されます。

Windows の場合

`<install_location>¥Arcot Systems¥logs¥`

UNIX ベースのプラットフォームの場合

`<install_location>/arcot/logs/`

注: CA Strong Authentication のログ ファイルの詳細については、「CA Strong Authentication のログ (P. 311)」を参照してください。

問題:

MA（マスタ管理者）のアカウントを使用して 管理コンソールにログインすることができません。「この管理者アカウントはロックされています。」というメッセージが表示されます。

原因

誤ったパスワードを使用して、許可されている認証試行数を超えて認証しようとした可能性があります。

解決方法:

以下のスクリプトを使用して、認証の試行回数（または*失敗回数*）を 0 にリセットします。

MS SQL の場合

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN';
GO
```

Oracle の場合：

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN'; commit;
```

DB2 の場合

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN'; commit;
```

MySQL の場合

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN';
```

問題:

管理コンソールにマスタ管理者としてログインしようとすると、以下のエラー メッセージが表示されます。

データベース クエリの処理中に内部サーバ エラーが発生しました。 データベース管理者に連絡してください。

原因

この問題の考えられる原因として、データベース プール内のアクティブなデータソースがすべて使い尽くされたことが考えられます。

解決方法:

この問題を解決するには、以下の手順に従います。

1. データベース サーバがアクセス可能であることを確認します。
2. データベースまたはデータベース リスナを再起動します
3. 管理コンソールと CA Strong Authentication サーバが同じデータベースを使用している場合
   a. CA Strong Authentication サービスを再起動します。
   b. ブラウザを再起動します。

問題:

MA のパスワードを忘れてしまいました。パスワードをリセットするには、どうしたらいいですか。

解決方法:

MA のパスワードをリセットする方法

1. データベース タイプに対応するスクリプトが格納されたフォルダを見つけます。 デフォルトの場所は以下のとおりです。

   （Windows-MS SQL の場合） <*install_location*>¥Arcot Systems¥dbscripts¥mssql

   （Windows-Oracle の場合） <*install_location*>¥Arcot Systems¥dbscripts¥oracle

   （Windows- IBM DB2 UDB の場合） <*install_location*>¥Arcot Systems¥dbscripts¥db2

   （Windows-MySQL の場合） <*install_location*>¥Arcot Systems¥dbscripts¥mysql

   （UNIX-MS SQL の場合） <*install_location*>/arcot/dbscripts/mssql

   （UNIX-Oracle の場合） <*install_location*>/arcot/dbscripts/oracle

   （UNIX-IBM DB2 UDB の場合） <*install_location*>/arcot/dbscripts/db2

   （UNIX-MySQL の場合） <*install_location*>/arcot/dbscripts/mysql

2. データベース ベンダーのツールを使用して、arcot-masteradmin-password-reset-2.0.sqll スクリプトを実行します。

   以上の操作で MA のパスワードがデフォルト パスワード（master1234）にリセットされます。

問題:

［サービスおよびサーバの設定］タブから CA Strong Authentication のページにアクセスできません。 以下のエラー メッセージが表示されます。
現在サーバに接続できません。 後で再試行してください。

解決方法:

以下の点を確認します。

- WebFort サーバが実行されている。
- WebFort サーバの接続の詳細が正しい。

  管理コンソールに MA としてログインします。 ［サービスおよびサーバの設定］-［WebFort］-［接続情報］ページの順に移動し、［サーバ管理 Web サービス］の CA Strong Authentication のホストとポートの情報が正しく設定されているかどうかを確認します。

問題

管理コンソールにログインしようとすると、以下のメッセージが表示されます。
エラー コード 500： 内部サーバ エラー。

原因

- ブラウザのキャッシュがいっぱいになっている可能性があります。
- アプリケーション サーバのタイムアウト設定をリセットする必要がある場合があります。

解決方法:

以下の手順を実行します。

- 管理コンソールを開こうとしているブラウザのキャッシュを空にして、再度試してみてください。
- 依然としてメッセージが表示される場合は、別のブラウザを使用して管理コンソールを開いてみてください。
- アプリケーション サーバ コンテナのタイムアウト設定を確認します。
- 問題がまだ解決されない場合は、arcotadmin.log ファイルを開き、「Administration Console configured successfully」という文字列を検索してください。
- 「Administration Console configured successfully」という文字列が見つからない場合は、エラーの説明を確認して、これに従って操作してください。

問題:

管理コンソールが正しく展開されませんでした。
java.lang.ClassNotFoundException 例外が arcotadmin.log ファイルに記録されています。

原因

この問題は、WAR または EAR が正しく展開されなかったか、破損した場合にのみ発生します。

解決方法:

この問題を解決するには、以下の手順に従います。

1. アプリケーション サーバの作業ディレクトリをクリーンアップします。

   たとえば、Apache Tomcat では、このディレクトリは work です。
2. 再度 WAR または EAR ファイルを展開します。

問題:

組織を作成してアクティブにしましたが、CA Strong Authentication の設定を行おうとすると、以下のエラーが表示されます。
組織が見つかりません

原因

考えられる原因は、作成した新しい組織に対して操作を実行しようとしていますが、CA Strong Authentication サーバのキャッシュがリフレッシュされていないことです。

解決方法:

CA Strong Authentication サーバのキャッシュをリフレッシュします。

管理コンソールを使用して新しい組織を作成したときには、必ず CA Strong Authentication サーバのキャッシュを再起動してください。

注: 詳細については、「*CA Strong Authentication 管理者ガイド*」の「サーバ インスタンスのリフレッシュ (P. 72)」を参照してください。

問題

ユーザと管理者を検索しているときに、以下のエラー メッセージが表示されます。
ユーザ データ サービスとの通信中に内部サーバ エラーが発生しました。 管理者に連絡してください。

原因

検索対象のユーザの数が多すぎて、指定した組織で検索できない可能性があります。 その結果として、操作がタイムアウトになったと考えられます。

解決方法:

以下の手順を実行します。

1. 管理コンソールに MA としてログインします。
2. ［**サービスおよびサーバの設定**］-［**管理コンソール**］-［UDS 接続設定］ページに移動します。
   - ［**接続タイムアウト**］フィールドの値を大きくします。
   - ［**読み取りタイムアウト**］フィールドの値を大きくします。
3. 検索条件を変更して、予想される検索結果を少なくします。

付録 E: 管理権限の要約

以下の表に、カスタム ロールの作成に使用するサポートされている 3 つのレベルの管理者が使用できる権限を要約して示します。

この表で使用される列名の頭字語を以下に示します。

- グローバル管理者 -> **GA**
- 組織の管理者 -> **OA**
- ユーザ管理者 -> **UA**

注: ✓ 記号は、指定されたレベルの管理者が利用できるアクション（または権限）を示します。

アクセス権	GA	OA	UA
組織管理の権限 これらの権限に関係するタスクの詳細については、「組織の管理 (P. 185)」を参照してください。			
組織の作成		✓	
組織の更新		✓	✓
組織ステータスの更新		✓	✓
組織の一覧表示		✓	✓
デフォルト組織の取得		✓	✓
組織の削除		✓	✓
アカウント タイプの管理権限 これらの権限に関係するタスクの詳細については、「アカウント タイプの設定 (P. 45)」を参照してください。			
アカウント タイプの作成		✓	
アカウント タイプの更新		✓	✓
アカウント タイプの削除		✓	

✓
✓

アクセス権	GA	OA	UA
管理者の管理権限 これらの権限に関係するタスクの詳細については、「管理者の管理 (P. 221)」を参照してください。			
管理者の作成		✓	✓
管理者の更新		✓	✓
管理者の削除		✓	✓
ユーザの管理権限 これらの権限に関係するタスクの詳細については、「ユーザと認証情報の管理 (P. 259)」を参照してください。			
Create User		✓	✓
ユーザの更新		✓	✓
ユーザ ステータスの更新		✓	✓
ユーザの一覧表示		✓	✓
アカウントのユーザの一覧表示		✓	✓
ユーザ ステータスの取得		✓	✓
ユーザ カスタム属性の設定		✓	✓
ユーザの検索		✓	✓
PAM の取得		✓	✓
PAM の設定	✓	✓	✓
ユーザの削除	✓	✓	✓
ユーザ アカウントの管理権限 これらの権限に関係するタスクの詳細については、「ユーザと認証情報の管理 (P. 259)」を参照してください。			
ユーザ アカウントの作成	✓	✓	✓
ユーザ アカウントの更新	✓	✓	✓
ユーザ アカウントの一覧表示	✓	✓	✓

アクセス権	GA	OA	UA
ユーザ アカウントの取得	✓	✓	✓
ユーザ アカウントの削除	✓	✓	✓
キャッシュの管理権限 これらの権限に関係するタスクの詳細については、「キャッシュのリフレッシュ (P. 36)」を参照してください。			
システム キャッシュのリフレッシュ	✓		
組織キャッシュのリフレッシュ	✓	✓	
グローバル キャッシュ リフレッシュ リクエストの表示	✓		
組織キャッシュ リフレッシュ リクエストの表示	✓	✓	
電子メールと電話のタイプの権限 これらの権限に関係するタスクの詳細については、「電子メールと電話のタイプの設定 (P. 47)」を参照してください。			
電子メール/電話のタイプの追加	✓	✓	
電子メール/電話のタイプの更新	✓	✓	
電子メール タイプの一覧表示	✓	✓	
電話タイプの一覧表示	✓	✓	
基本認証権限 これらの権限に関係するタスクの詳細については、「基本認証設定の指定 (P. 49)」を参照してください。			
グローバル基本認証ポリシーの更新	✓		
組織の基本認証ポリシーの更新	✓	✓	
暗号化権限 これらの権限に関係するタスクの詳細については、「属性の暗号化の設定 (P. 41)」を参照してください。			
組織レベルで選択された暗号化セットの設定	✓	✓	
暗号化用に設定された属性の一覧表示	✓	✓	

アクセス権	GA	OA	UA
認証情報の管理権限 これらの権限に関係するタスクの詳細については、「ユーザ認証情報の更新 (P. 268)」を参照してください。			
ArcotID キーバッグへのエレメントの追加	✓	✓	✓
認証情報の作成	✓	✓	✓
ArcotID 属性の削除	✓	✓	✓
認証情報の削除	✓	✓	✓
ArcotID キーからのエレメントの削除	✓	✓	✓
認証情報の無効化	✓	✓	✓
認証情報のダウンロード	✓	✓	✓
認証情報の有効化	✓	✓	✓
認証情報の取得	✓	✓	✓
ArcotID の取得	✓	✓	✓
ArcotID キーバッグからのエレメントの取得	✓	✓	✓
質問と回答の取得	✓	✓	✓
認証情報の再発行	✓	✓	✓
認証情報のリセット	✓	✓	✓
認証情報のリセット カスタム属性	✓	✓	✓
認証情報の有効性のリセット	✓	✓	✓
ArcotID 属性の設定	✓	✓	✓
認証情報詳細の表示	✓	✓	✓
設定権限 これらの権限に関係するタスクの詳細については、「グローバルな CA Strong Authentication 設定の管理 (P. 99)」を参照してください。			
デフォルトとしての設定の割り当て	✓	✓	
設定の割り当て	✓	✓	

アクセス権	GA	OA	UA
HSM 内のキー ラベルの確認	✓	✓	
プラグインの設定	✓	✓	
ArcotID ポリシーの作成	✓	✓	
ArcotOTP-EMV OTP ポリシーの作成	✓	✓	
ArcotOTP-OATH ポリシーの作成	✓	✓	
OATH OTP トークン ポリシーの作成	✓	✓	
OTP ポリシーの作成	✓	✓	
Q&A ポリシーの作成	✓	✓	
パスワード ポリシーの作成	✓	✓	
認証情報キー管理	✓	✓	
認証情報タイプの解決設定	✓	✓	
認証情報設定の取得	✓	✓	✓
ASSP 設定の管理	✓	✓	
ArcotID プロファイルの管理	✓	✓	
ArcotOTP プロファイルの管理	✓	✓	
ArcotOTP-EMV プロファイルの管理	✓	✓	
OATH OTP プロファイルの管理	✓	✓	
OTP プロファイルの管理	✓	✓	
Q&A プロファイルの管理	✓	✓	
RADIUS 設定の管理	✓	✓	
RADIUS プロキシの管理	✓	✓	
SAML トークンの設定の管理	✓	✓	
パスワード プロファイルの管理	✓	✓	
モジュールの関連付け	✓	✓	
OATH トークンの管理	✓		
他の権限			
Q&A 属性の取得	✓	✓	

アクセス権	GA	OA	UA
Q&A 値の取得	✓	✓	✓
Arcot 属性の一覧表示	✓	✓	
リポジトリ属性の一覧表示	✓	✓	
Q&A 検証の実行	✓	✓	✓
バルク アップロード	✓	✓	
バルク アップロード リクエストの表示	✓	✓	
レポート権限 これらの権限に関係するタスクの詳細については、「レポートの管理 (P. 293)」を参照してください。			
マイ アクティビティ レポートの表示	✓	✓	✓
ユーザ アクティビティ レポートの表示	✓	✓	✓
ユーザ作成レポートの表示	✓	✓	✓
組織レポートの表示	✓	✓	
管理者アクティビティ レポートの表示	✓	✓	✓
認証レポートの表示	✓	✓	✓
認証情報レポートの表示	✓	✓	✓
設定管理レポートの表示	✓	✓	

付録 F: IBM DB2 Universal Database の代替スキーマの設定

IBM DB2 Universal Database（UDB）では、デフォルト スキーマ以外のスキーマを使用することができます。 このスキーマは代替スキーマと呼ばれます。 この付録では、代替スキーマをセットアップし使用するために実行する必要がある手順について説明します。 この章では、以下の内容について説明します。

スキーマの作成

代替スキーマをセットアップするには、以下の手順に従います。

1. IBM DB2 UDB データベースにログインします。

   ログイン名が arcotuser の場合、このユーザのデフォルト スキーマは arcotuser になります。

2. 代替スキーマを作成します。

   たとえば、arcotalternateuser という代替スキーマにします。

   注: 代替スキーマの作成方法の詳細については、IBM DB2 UDB データベースのドキュメントを参照してください。

3. 以下のクエリを実行して、代替スキーマ（arcotalternateuser）をセットアップします。

   ```
   set current schema ARCOTALTERNATEUSER
   set current path ARCOTALTERNATEUSER
   ```

   注: 代替スキーマは大文字で指定する*必要があります*。

4. 以下の場所に移動します。

   <*install_location*>/arcot/dbscripts/db2

5. *以下の順序でスクリプトを*実行します。

   a. arcot-db-config-for-common-2.0.sql

   b. arcot-db-config-for-webfort-7.1.01.sql

   注: スクリプトの実行中にエラーが発生した場合は、必要な権限が付与されているかどうかをデータベース管理者に確認します。

6. データベース ユーザ名（arcotuser）および対応するパスワードが securestore.enc ファイルに設定されていることを確認します。 DBUtil ツールを使用して、データベース ユーザ名とパスワードを挿入できます。

   詳細については、「CA AuthMinder 管理ガイド」の「システム管理者用のツール」を参照してください。

設定ファイルの編集

IBM DB2 UDB の代替スキーマを使用する場合、arcotcommon.ini ファイルを編集して、それらを設定します。

以下の手順に従います。

1. 以下の場所に移動します。
   <*install_location*>/arcot/**conf**
2. テキスト エディタで arcotcommon.ini ファイルを開きます。
3. [arcot/db/primarydb] および [arcot/db/backupdb] セクションで、以下のパラメータを設定します。
   - **URL.1**： このパラメータを JDBC データ ソースに以下のように設定します。
     jdbc:db2://<*server*>:<*database_port*>/<*database*>:currentSchema=<*alternateID*>;currentFunctionPath="SYSIBM","SYSFUN","SYSPROC","SYSIBMADM","<*alternateID*>";

     以下に例を示します。
     jdbc:db2://db2server:50000/arcotdb:currentSchema=ARCOTALTERNATEUSER;currentFunctionPath="SYSIBM","SYSFUN","SYSPROC","SYSIBMADM","ARCOTALTERNATEUSER";
   - **Username.1**： このパラメータをデータベースへのアクセスに使用するユーザ名に設定します。 たとえば、arcotuser などです。
4. arcotcommon.ini ファイルを保存して閉じます。

ODBC DSN の設定

AuthMinder サーバは、ODBC（Open Database Connectivity）を使用してデータベースに接続します。 代替スキーマを使用してデータベースに接続するには、AuthMinder サーバの ODBC 設定を編集します。

ODBC 設定を編集するには、以下の手順に従います。

1. 以下の場所に移動します。

   <install_location>/arcot/odbc32v70wf

2. ファイル エディタで odbc.ini ファイルを開きます。
3. 使用しているデータベースに対応する [*<Database_name>*] セクションで、以下の表にリストされているパラメータを編集します。

パラメータ	説明
AlternateID	手順 2 で作成した代替スキーマ。
CurrentFuncPath	このフィールドを SYSIBM, SYSFUN, SYSPROC, SYSIBMADM, *<Alternate_ID>* に設定します。 たとえば、SYSIBM, SYSFUN, SYSPROC, SYSIBMADM, ARCOTALTERNATEUSER などです。

4. odbc.ini ファイルを保存して閉じます。

第 14 章: サンプル アプリケーションの使用

サンプル アプリケーションを使用すると、AuthMinder でサポートされている認証情報の発行および認証を行うことができます。 サンプル アプリケーションを使用してこれらの操作を実行し、AuthMinder が正常にインストールされているかどうかをテストできます。

このセクションでは、以下のタスクについて説明します。

- ユーザの作成（P. 391）
- ArcotID PKI クライアントのセットアップ（P. 392）
- ArcotID PKI 認証情報の作成（P. 393）
- ArcotID PKI のダウンロード（P. 394）
- ArcotID PKI を使用した認証（P. 395）

ユーザの作成

注: ユーザは、管理コンソールまたは Web サービスを使用して作成する必要があります。

管理コンソールを使用してユーザを作成する方法

1. GA（グローバル管理者）または OA（組織管理者）として管理コンソールにログインします。 URL は以下のとおりです。

   http://<host>:<app_server_port>/arcotadmin/adminlogin.htm

2. アクティブでない場合は、［**ユーザと管理者**］タブの［**ユーザと管理者の管理**］サブタブをアクティブにします。
3. 左側のペインで、［**ユーザと管理者の管理**］の［**ユーザの作成**］をクリックして［ユーザの作成］ページを開きます。
4. ［ユーザの作成］ページで以下の操作を実行します。
   a. ［**ユーザ詳細**］セクションに一意のユーザ名、それらの組織名、および必要に応じてその他のユーザ情報を入力します。
   b. （オプション）ページ上の対応するフィールドでその他のユーザ情報を指定します。
   c. 必要な**ユーザ ステータス**を選択します。
   d. ［**ユーザの作成**］をクリックします。

   指定したユーザがデータベースに正常に追加されると、「ユーザを正常に作成しました」というメッセージが表示されます。
5. サンプル アプリケーション ページに戻ります。

ArcotID PKI クライアントのセットアップ

AuthMinder サーバと通信するために ArcotID PKI クライアントをセットアップし、ArcotID PKI でユーザを認証するようにします。

以下の手順に従います。

1. 以下の URL を使用してサンプル アプリケーションにアクセスします。

   http://<host>:<app_server_port>/webfort-7.1.01-sample-application/

2. 左側のペインで、［**Setup**］-［**ArcotID Client**］をクリックして［ArcotID Client Settings］ページを開きます。
3. ［**Choose ArcotID Client**］セクションで、ArcotID PKI を認証するために使用するクライアントのタイプを選択します。
4. ［**Choose ArcotID Download Type**］セクションで、ArcotID PKI を格納する場所を選択します。
5. ［**Choose Where & When to Obtain the ArcotID Challenge**］セクションで、ArcotID PKI のチャレンジを取得するモードを選択します。
6. ［**Select**］をクリックして設定を保存します。

   ArcotID PKI クライアントの設定が正常に実行されると、「The operation was successful」というメッセージが表示されます。

ArcotID PKI 認証情報の作成

ユーザの ArcotID PKI 認証情報を作成する方法

1. 以下の URL を使用してサンプル アプリケーションにアクセスします。

   http://<host>:<app_server_port>/webfort-7.1.01-sample-application/

2. 左側のペインで、［**ArcotID**］-［**Issuance**］-［**Create**］をクリックして［Create ArcotID］ページを開きます。
3. ［**User Name**］フィールドで、作成済みのユーザの名前を指定します。
4. （オプション）［**Organization**］フィールドでユーザの組織を指定します。
5. ［**ArcotID Password**］フィールドで、認証に使用するパスワードを指定します。
6. （オプション）ArcotID の発行に対して使用されるプロファイルを［Profile Name］フィールドに指定します。
7. （オプション）**無署名属性**の名前と値のペアを指定します。 この属性は、ArcotID PKI の無署名の部分に設定されます。
8. （オプション）ArcotID PKI の作成に使用する**カスタム属性**を指定します。
9. （オプション）AuthMinder サーバへ渡す**追加入力**を指定します。
10. （オプション）以下の**トランザクション ログ パラメータ**を渡します。
    - ［**Log Level**］フィールドで、ログ レベルを選択します。

      注: ログ レベルの詳細については、「CA AuthMinder 管理ガイド」の「AuthMinder のログ」のトピックを参照してください。
    - フローの詳細を取得する場合は、［**Enable Trace Logging**］を選択します。
    - データベース アクティビティをログ記録する場合は、［**Enable DB Logging**］を選択します。
    - 機密データをログ記録する場合は、［**Enable Sensitive Data Logging**］を選択します。
11. ［**Create**］をクリックして認証情報を作成します。

    ArcotID PKI がユーザに対して正常に作成されると、「The operation was successful」というメッセージが表示されます。

ArcotID PKI のダウンロード

ArcotID PKI をダウンロードする方法

1. 以下の URL を使用してサンプル アプリケーションにアクセスします。

   http://<host>:<app_server_port>/webfort-7.1.01-sample-application/

2. 左側のペインで、［**ArcotID**］-［**Issuance**］-［**Download**］をクリックして［Download ArcotID］ページを開きます。
3. ［**User Name**］フィールドで、作成済みのユーザの名前を指定します。
4. （オプション）［**Organization**］フィールドでユーザの組織を指定します。
5. （オプション）［**Profile Name**］フィールドで ArcotID PKI を発行するために使用されたプロファイルを指定します。
6. （オプション）AuthMinder サーバへ渡す**追加入力**を指定します。
7. （オプション）以下の**トランザクション ログ パラメータ**を渡します。
   - ［**Log Level**］フィールドで、ログ レベルを選択します。

     注: ログ レベルの詳細については、「CA AuthMinder 管理ガイド」の「AuthMinder のログ」のトピックを参照してください。
   - フローの詳細を取得する場合は、［**Enable Trace Logging**］を選択します。
   - データベース アクティビティをログ記録する場合は、［**Enable DB Logging**］を選択します。
   - 機密データをログ記録する場合は、［**Enable Sensitive Data Logging**］を選択します。
8. ［**Download**］をクリックしてユーザの ArcotID PKI をダウンロードします。

ArcotID PKI を使用した認証

ArcotID PKI を使用して認証を行う方法

1. 以下の URL を使用してサンプル アプリケーションにアクセスします。

   http://<host>:<app_server_port>/webfort-7.1.01-sample-application/

2. 左側のペインで、［**ArcotID**］-［**Authentication**］-［**Authenticate**］をクリックして［ArcotID Authentication］ページを開きます。
3. ［**User Name**］フィールドで、作成済みのユーザの名前を指定します。
4. ［**Organization**］フィールドでユーザの組織を指定します。
5. ［**ArcotID Password**］フィールドで、ユーザの ArcotID PKI パスワードを指定します。
6. ユーザを識別するためにエイリアスを使用している場合は、認証するユーザのエイリアスに応じて**アプリケーション コンテキスト**を指定します。
7. （オプション）認証成功後にユーザに返す**トークン タイプ**を選択します。

   注: トークン タイプの詳細については、「CA AuthMinder Java 開発者ガイド」の「ユーザの認証」の章を参照してください。

8. （オプション）ユーザの認証に使用される**認証ポリシー名**を指定します。
9. トークン タイプとして SAML を選択した場合は、使用する **SAML ポリシー名**を指定します。
10. （オプション）AuthMinder サーバへ渡す**追加入力**を指定します。
11. （オプション）以下の**トランザクション ログ パラメータ**を渡します。
    - ［**Log Level**］フィールドで、ログ レベルを選択します。

      注: ログ レベルの詳細については、「CA AuthMinder 管理ガイド」の「AuthMinder のログ」のトピックを参照してください。

    - フローの詳細を取得する場合は、［**Enable Trace Logging**］を選択します。
    - データベース アクティビティをログ記録する場合は、［**Enable DB Logging**］を選択します。
    - 機密データをログ記録する場合は、［**Enable Sensitive Data Logging**］を選択します。

12. ［**Authenticate**］をクリックしてユーザの ArcotID PKI を検証します。

付録 G: デフォルトのポート番号および URL

この付録では、AuthMinder で使用するデフォルトのポート番号を表にまとめています。 本章は以下の節によって構成されています。

デフォルトのポート番号

AuthMinder は、異なるポートで設定される 4 つのプロトコルをサポートします。 以下の表に、AuthMinder で使用されるデフォルトのポート番号を示します。

プロトコル	デフォルトポート番号	デフォルトのステータス	説明
Server Management Web Services	9743	有効	このプロトコルは AuthMinder サーバの管理に使用されます。 管理コンソールおよび arwfutil クライアントは、このポートを使用して通信し、サーバ管理アクティビティを行います。
Transaction Web Services	9744	有効	このプロトコルは、認証 Web サービスおよび発行 Web サービスのクライアントが AuthMinder サーバへの接続に使用します。
Transaction Native	9742	有効	これは、AuthMinder が認証および認証情報発行の目的で使用する専用のバイナリプロトコルです。 このポートは認証 SDK および認証情報管理 SDK が使用します。
Administration Web Services	9745	有効	このプロトコルを使用して、プロファイル、ポリシー、SAML、ASSP などの設定が作成および管理されます。

プロトコル	デフォルト ポート番号	デフォルトのステータス	説明
RADIUS	1812	無効	RADIUS（Remote Authentication Dial In User Service）プロトコルをサポートするために使用されます。RADIUS プロトコルをサポートする設定になっている場合は、AuthMinder サーバは RADIUS サーバとして動作します。
ASSP	9741	無効	このプロトコルは、PDF 文書のサーバ サイドのデジタル署名を用いてユーザを認証する際に、Adobe® Reader および Adobe® Acrobat® と一緒に使用されます。
Transaction HTTP	9746	無効	このプロトコルは、HTTP クライアントから AuthMinder サーバに HTTP リクエスト パケットを転送するために使用されます。

ほかのサービスがすでにデフォルト ポート上で実行されている場合、以下のように、該当プロトコル用に新しいポートを設定します。

- **Server Management Web Services プロトコル用の新しいポート番号を設定するには**、webfortserver ツールを使用します。

  注: ツールの詳細については、「CA AuthMinder 管理ガイド」の「システム管理者用のツール」を参照してください。

- **その他のプロトコル用の新しいポート番号を設定するには**、管理コンソールの［プロトコル設定］画面を使用します。

  注: ポート番号の変更の詳細については、「CA AuthMinder 管理ガイド」の「AuthMinder サーバ インスタンスの管理」を参照してください。

AuthMinder コンポーネントの URL

インストール後に AuthMinder コンポーネントにアクセスする際は、以下の表に記載されている URL を使用します。

コンポーネントまたはサービス	URL
マスタ管理者用の管理コンソールの URL	*http://<Apphost>:<app_server_port>/arcotadmin/masteradminlogin.htm* **注**: **Apphost** は、管理コンソールが展開されているシステムを指します。 **App_Server_Port** は、管理コンソールが展開されているアプリケーション サーバのポート番号を指します。
他の管理者用の管理コンソール の URL	*http://<Apphost>:<app_server_port>/arcotadmin/adminlogin.htm* **注**: **Apphost** は、管理コンソールが展開されているシステムを指します。 **App_Server_Port** は、管理コンソールが展開されているアプリケーション サーバのポート番号を指します。
組織管理 Web サービス	http://*<Apphost>:<app_server_port>/arcotuds/services/ArcotUserRegistryMgmtSvc* **注**: **Apphost** は、ユーザ データ サービス（UDS）コンソールが展開されているシステムを指します。 **App_Server_Port** は、UDS が展開されているアプリケーション サーバのポート番号を指します。
ユーザ管理 Web サービス	http://*<Apphost>:<app_server_port>/arcotuds/services/ArcotUserRegistrySvc* **注**: **Apphost** は、ユーザ データ サービス（UDS）コンソールが展開されているシステムを指します。 **App_Server_Port** は、UDS が展開されているアプリケーション サーバのポート番号を指します。
構成レジストリ Web サービス	http://*<Apphost>:<app_server_port>/arcotuds/services/ArcotConfigRegistrySvc* **注**: **Apphost** は、ユーザ データ サービス（UDS）コンソールが展開されているシステムを指します。 **App_Server_Port** は、UDS が展開されているアプリケーション サーバのポート番号を指します。

コンポーネントまたはサービス	URL
認証情報管理 Web サービス	http://*<Apphost>:<Protocol_port>/WebFortIssuanceSvc* **注**: **Apphost** は、AuthMinder サーバがインストールされているシステムです。 **Protocol_port** は、Transaction Web Services プロトコルのポート番号です。デフォルトでは、この値は 9744 です。
管理 Web サービス	http://*<Apphost>:<Protocol_port>/ArcotWebFortAdminSvc* **注**: **Apphost** は、AuthMinder サーバがインストールされているシステムです。 **Protocol_port** は、Administration Web Services プロトコルのポート番号です。デフォルトでは、この値は 9745 です。
認証 Web サービス	http://*<Apphost>:<Protocol_port>/WebFortAuthSvc* **注**: **Apphost** は、AuthMinder サーバがインストールされているシステムです。 **Protocol_port** は、Transaction Web Services プロトコルのポート番号です。デフォルトでは、この値は 9744 です。
バルク操作 Web サービス	http://*<Apphost>:<Protocol_port>/WebFortBulkOperationsSvc* **注**: **Apphost** は、AuthMinder サーバがインストールされているシステムです。 **Protocol_port** は、Administration Web Services プロトコルのポート番号です。デフォルトでは、この値は 9745 です。
サンプル アプリケーション	*http://<Apphost>:<app_server_port>/webfort-7.1.01-sample-application/* **注**: **App_Server_Port** は、サンプル アプリケーションが展開されているアプリケーション サーバのポート番号を指します。

付録 H: アプリケーション サーバの設定

この付録では、以下のトピックについて説明します。

- データベース接続プールの有効化 (P. 401)
- LDAP 接続プールの有効化 (P. 410)
- Apache Tomcat のセキュリティ マネージャの有効化 (P. 418)

データベース接続プールの有効化

通常は、データベースへのアクセスはボトルネックとはなりませんが、リクエストごとに新しい接続をセットアップするとオーバーヘッドとなり、システムのパフォーマンスを低下させることがあります。 データベース接続プールを作成することで、潜在的なボトルネックを回避できます。これは、アプリケーション サーバに展開されている AuthMinder コンポーネントがデータベースへのアクセスを要求するたびに、新しいデータベース接続を作成するオーバーヘッドを回避するのに接続プールが役立つためです。

このセクションでは、以下のアプリケーション サーバの設定手順について説明します。

- Apache Tomcat (P. 402)
- IBM WebSphere アプリケーション サーバ (P. 404)
- Oracle WebLogic アプリケーション サーバ (P. 407)
- JBoss アプリケーション サーバ (P. 409)

Apache Tomcat

ここでは、JNDI ベースのデータベース操作用に Apache Tomcat を有効にする手順について説明します。

Apache Tomcat 内に JNDI 接続を作成するには、以下の手順に従います。

1. Apache Tomcat をインストールし、以下の URL を使用してインストールをテストします。

   http://localhost:8080/

   上記の URL で Apache Tomcat ホーム ページを開く必要があります。

2. *<TOMCAT-HOME>*/conf ディレクトリにある server.xml ファイルを開きます。

3. データ ソースを定義することに対して以下の情報を収集します。

   - JNDI 名

     製品コンポーネントによって使用される JNDI 名。 この名前は、arcotcommon.ini （java:comp/env/ プレフィックスなし）の AppServerConnectionPoolName.*N* と一致する必要があります。

   - ユーザ ID

     データベース ユーザ ID。

   - パスワード

     データベース パスワード。

   - JDBC ドライバ クラス

     JDBC ドライバ クラス名。たとえば、oracle.jdbc.driver.OracleDriver。

   - JDBC URL

     データベース サーバ用の JDBC URL。 たとえば、Oracle ドライバを使用している場合、この URL は jdbc:oracle:thin:@*<server>*:*<database_port>*:*<sid>* となります。

4. *<GlobalNamingResources>* タグ内に以下のエントリを追加してデータ ソースを定義します。

```
<Resource name="SampleDS"
auth="Container"
type="javax.sql.DataSource"
factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory"
username="<userid>"
password="<password>"
driverClassName="<JDBC driver class>"
```

```
url="<jdbc-url>"
maxWait="30000"
maxActive="32"
maxIdle="8"
initialSize="4"
timeBetweenEvictionRunsMillis="300000"
minEvictableIdleTimeMillis="30000"/>
```

5. *<TOMCAT-HOME>*/conf ディレクトリにある context.xml ファイルを開きます。
6. <Context> タグ内に以下のエントリを追加してデータ ソースを定義します。
   ```
   <ResourceLink global="SampleDS" name="SampleDS"
   type="javax.sql.DataSource"/>
   ```
7. 以下のデータベース接続プール（DBCP）関係ファイルを *<TOMCAT-HOME>*/common/**lib** ディレクトリにコピーします。
   - commons-dbcp-1.2.2.jar
   - ojdbc14-10.2.0.1.0.jar （Oracle データベースの場合）
   - sqljdbc.jar（Microsoft SQL Server 2005 用 Microsoft JDBC ドライバ バージョン 1.2.2828）
   - db2jcc-9.5.jar （IBM DB2 UDB の場合）
   - mysql-connector-java-5.1.22-bin.jar （MySQL の場合）

IBM WebSphere アプリケーション サーバ

ここでは、JNDI ベースのデータベース操作に対して IBM WebSphere を有効にする手順について説明します。

AuthMinder の Java 依存コンポーネントを展開するために IBM WebSphere を設定するには、以下の手順に従います。

1. WebSphere Administration Console にログインします。
2. ［**Resources**］を選択し、［**JDBC**］ノードを展開します。
3. ［**JDBC Providers**］をクリックします。

   ［JDBC Providers］ページが表示されます。
4. ［**Preferences**］セクションで、［**New**］をクリックします。

   ［Create a new JDBC Provider］ページが表示されます。
5. 以下の手順に従って、JDBC プロバイダを作成します。

   注: JDBC プロバイダの詳細については、http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.iseries.doc/info/iseries/ae/tdat_ccrtprov.html を参照してください。

   a. ［**Database Type**］および［**Provider Type**］を指定します。

   b. ［**Implementation Type**］ドロップダウン リストから［**Connection pool data source**］を選択します。

   c. JDBC プロバイダの**名前**を入力します。JDBC プロバイダの**説明**を入力することもできます。

   d. ［**Next**］をクリックします。

      ［Enter database class path information］画面が表示されます。

   e. JAR ファイルの絶対パスを入力します。

   f. ［**Next**］をクリックします。

      ［Summary］画面が表示されます。

   g. 入力した情報のサマリを確認したら、［**Finish**］をクリックします。
6. 手順 5 で作成した JDBC プロバイダの CLASSPATH を設定します。

   a. ［**Resources**］を選択し、［**JDBC**］ノードを展開します。

   b. ［**JDBC Providers**］をクリックします。

      ［JDBC Providers］ページが表示されます。

c. 手順 5 で作成した JDBC プロバイダをクリックします。

d. JDBC JAR の**クラス パス**を設定します。

e. ［**Apply**］をクリックして、変更を保存します。

7. 以下の手順に従って、データ ソースを作成します。

a. ［**Resources**］に移動し、［**JDBC**］をクリックします。

b. ［**JDBC**］の［**Data Sources**］を開き、［**New**］をクリックします。データ ソースを作成するには、以下の手順に従います。

c. **データ ソース名**を指定します。

d. **JNDI 名**を指定します。 この名前は arcotcommon.ini の AppServerConnectionPoolName.*N* と一致する必要があります。

e. ［**Next**］をクリックします。

f. 手順 3 で作成した JDBC プロバイダを選択します。

g. ［**Next**］をクリックします。

［Enter database specific properties for the data source］画面が表示されます。

h. データベースの種類に応じて、以下の情報を入力します。

- **Oracle の場合**

  JDBC URL の**値**を指定します。 この URL は以下の形式になります。

  `jdbc:oracle:thin:@<server>:<oracle_port>:<sid>`

  ［**Data store helper class name**］を選択します。

- **Microsoft SQL Server の場合**

  `jdbc:sqlserver://<server>:<sql_port>;databaseName=<database name>;selectMethod=cursor`

- **IBM DB2 の場合**

  `jdbc:db2://<server>:<db2_port>/<database>`

- **MySQL の場合**

  `jdbc:mysql://<server>:<mysql_port>/<database>`

i. ［**Next**］をクリックします。

［Setup Security aliases］画面が表示されます。

j. ［**Next**］をクリックして［Summary］画面を確認し、［**Finish**］をクリックします。

8. 手順 7 で作成したデータ ソースをクリックします。

9. ［**Related Items**］セクションで、［**JAAS - J2C authentication data**］をクリックします。
10. ［New］をクリックして認証情報を作成します。
11. データベースへの接続に使用されるログイン クレデンシャルを入力し、クレデンシャルを保存します。
12. ［Apply］をクリックし、［OK］をクリックして変更を保存します。
13. ［**Data Sources**］をクリックし、手順 7 で作成したデータ ソースを選択します。
14. ［**Security Settings**］-［**Component-managed authentication alias**］で、手順 11 で作成した JAAS 認証情報を選択し、［**Apply**］-［**OK**］の順にクリックします。
15. ［**Data Sources**］をクリックし、手順 7 で作成したデータ ソースのチェック ボックスをオンにします。
16. ［**Test connection**］をクリックし、接続が正しく指定されているかどうかを検証します。

注: このテストでは、データベース サーバへの接続のみが確認され、データ ソースの定義が正しいかどうかは必ずしも確認されません。

Oracle WebLogic Server

このセクションでは、JNDI ベースのデータベース操作用に Oracle WebLogic を有効にする手順について説明します。

Oracle WebLogic にデータ ソースを作成するには、以下の手順に従います。

1. WebLogic Administration Console にログインします。
2. ロックと編集が終わっていない場合は、［**Lock & Edit**］ボタンをクリックします。
3. ［**Resources**］に移動し、［**JDBC**］をクリックします。
4. ［**JDBC**］の［**Data Sources**］を開き、［**New**］をクリックしてデータ ソースを作成します。データ ソースを作成するには、以下の手順に従います。
5. 以下の JNDI 情報とデータベース情報を設定します。
   a. ［**Name**］を「ArcotDB」に設定します。
   b. ［**JNDI Name**］を「ArcotDB」に設定します。
   c. ［**Database Type**］で適切な値（Oracle など）を選択します。
   d. ［**Database Driver**］で適切な値（Oracle Thin Driver など）を選択します。
6. ［**Next**］をクリックし、デフォルト値をそのまま使用して［**Next**］をクリックします。
7. ［Connection Properties］ページで、データベースの詳細情報を設定します。 以下に示す値は Oracle データベース用の値です。
   - **Database**： DB サーバの SID またはサービス名
   - **Hostname**： DB サーバの IP アドレスまたはホスト名
   - **Port**： 1521 または DB サーバが動作している他の任意のポート
   - **Database User Name**
   - **Database Password / Confirm Password**
8. ［**Test Configuration**］をクリックし、データベース パラメータが正しく指定されたかどうかを確認します。
9. ［**Next**］をクリックし、データ ソースの展開先として優先の WebLogic サーバ インスタンスを設定します。
10. ［**Finish**］をクリックして、データ ソースの一覧ページに戻ります。

11. ［**Activate**］をクリックして、データ ソース設定を有効にします。

JBoss アプリケーション サーバ

このセクションでは、JNDI ベースのデータベース操作用に JBoss アプリケーション サーバを有効にする手順について説明します。

1. WAR ファイルを展開した場所に移動します。 以下に例を示します。
   `<JBOSS_HOME>/server/default/deploy`
2. arcotdatabase-ds.xml というデータ ソース記述子ファイルを作成します。
3. arcotdatabase-ds.xml ファイルにデータ ソースを定義するための以下の情報を収集します。
   - JNDI Name

     Arcot コンポーネントによって使用される JNDI 名。 この名前は、arcotcommon.ini （java:comp/env/ プレフィックスなし）の AppServerConnectionPoolName.*N* と一致する必要があります。
   - ユーザ ID

     データベース ユーザ ID。
   - パスワード

     データベース パスワード。
   - JDBC ドライバ クラス

     JDBC ドライバ クラス名。たとえば、oracle.jdbc.driver.OracleDriver。
   - JDBC URL

     データベース サーバ用の JDBC URL。 たとえば、Oracle ドライバを使用している場合、この URL は jdbc:oracle:thin:*<server>*:*<database_port>*:*<sid>* となります。
   - Exception Sorter クラス

     例外が接続エラーを示すかどうかを判断する org.jboss.resource.adapter.jdbc.ExceptionSorter インターフェースを実装するクラス。

     このパラメータは、Oracle データベースにのみ使用します。 org.jboss.resource.adapter.jdbc.vendor.OracleExceptionSorter に設定します。
4. テキスト エディタで arcotdatabase-ds.xml を開きます。
5. 以下の内容を追加します。
   ```
   <?xml version="1.0" encoding="UTF-8"?>
   ```

```
<datasources>
<local-tx-datasource>
<jndi-name>SampleDS</jndi-name>
<connection-url><jdbcurl></connection-url>
<driver-class><JDBC Driver class></driver-class>
<user-name><database_userid></user-name>
<password><database_password></password>
<exception-sorter-class-name><Exception Sorter
Class></exception-sorter-class-name>
</local-tx-datasource>
</datasources>
```

6. ファイルを保存して閉じます。

LDAP 接続プールの有効化

このセクションでは、以下のアプリケーション サーバの LDAP 接続プールを有効化するための設定手順について説明します。

- Apache Tomcat（P. 411）
- IBM WebSphere アプリケーション サーバ（P. 412）
- Oracle WebLogic Server（P. 413）
- JBoss アプリケーション サーバ（P. 416）

Apache Tomcat

LDAP 接続プールを作成するには、以下の手順に従います。

1. Apache Tomcat アプリケーション サーバをインストールし、以下の URL を使用してインストールをテストします。

   http://localhost:8080/

   上記の URL で Apache Tomcat ホーム ページを開く必要があります。

2. 以下の場所に移動します。
   <TOMCAT-HOME>/conf
3. テキスト エディタで catalina.properties ファイルを開きます。
4. ファイルに、以下のエントリを追加します。
   - com.sun.jndi.ldap.connect.pool.protocol=plain ssl
   - com.sun.jndi.ldap.connect.pool.authentication=simple
   - com.sun.jndi.ldap.connect.pool.maxsize=64
   - com.sun.jndi.ldap.connect.pool.prefsize=32
   - com.sun.jndi.ldap.connect.pool.timeout=240000
   - com.sun.jndi.ldap.connect.pool.initsize=8
5. ファイルを保存して閉じます。
6. アプリケーション サーバを再起動します。

IBM WebSphere アプリケーション サーバ

LDAP 接続プールを作成するには、以下の手順に従います。

1. WebSphere Administration Console にログインします。
2. ［Servers］-［Server Types］-［WebSphere application servers］に移動します。
3. ［Application servers］ページが表示されます。
4. 設定するサーバをクリックします。
5. ［**Server Infrastructure**］セクションで、［**Java and Process Management**］をクリックします。
6. ［**Process Definition**］リンクをクリックします。
7. ［**Additional Properties**］セクションで、［**Java Virtual Machine**］をクリックします。
8. ［**Additional Properties**］セクションで、［**Custom Properties**］をクリックします。
9. ［**New**］をクリックして、カスタム プロパティを追加します。

   ［**General Properties**］セクションが表示されます。
10. 以下の表にリストされている設定を、名前と値をペアにして［General Properties］セクションに追加します。名前と値のペアごとに処理を繰り返します。

名前	値
com.sun.jndi.ldap.connect.pool.maxsize	64
com.sun.jndi.ldap.connect.pool.prefsize	32
com.sun.jndi.ldap.connect.pool.initsize	8
com.sun.jndi.ldap.connect.pool.timeout	240000
com.sun.jndi.ldap.connect.pool.protocol	plain ssl
com.sun.jndi.ldap.connect.pool.authentication	simple

11. ［**Apply**］をクリックします。
12. WebSphere を再起動します。

Oracle WebLogic Server

このセクションでは、Oracle WebLogic Server の LDAP 接続プールの有効化に関する以下のトピックについて説明します。

- 起動スクリプトへの LDAP オプションの追加 (P. 414)
- 管理対象サーバを使用した LDAP プール オプションの指定 (P. 415)

起動スクリプトへの LDAP オプションの追加

このセクションでは、WebLogic サーバの起動スクリプトに LDAP 接続プール パラメータを含める手順について説明します。

1. システムにログインします。
2. WebLogic サーバの起動スクリプトのバックアップ コピーを作成します。 このスクリプトは以下の場所にあります。
   `domain-name/bin/startWebLogic.sh`
3. テキスト エディタでスクリプトを開きます。
4. WebLogic サーバの起動に使用されるセクションに以下のエントリを追加します。
   - -Dcom.sun.jndi.ldap.connect.pool.maxsize=64
   - -Dcom.sun.jndi.ldap.connect.pool.prefsize=32
   - -Dcom.sun.jndi.ldap.connect.pool.initsize=8
   - -Dcom.sun.jndi.ldap.connect.pool.timeout=240000
   - -Dcom.sun.jndi.ldap.connect.pool.protocol="plain ssl"
   - -Dcom.sun.jndi.ldap.connect.pool.authentication=simple

   以下のコード スニペットは、LDAP 接続プール パラメータが設定されているサンプル スクリプトを示しています。

```
# START WEBLOGIC
echo "starting weblogic with Java version:"
${JAVA_HOME}/bin/java ${JAVA_VM} -version
if [ "${WLS_REDIRECT_LOG}" = "" ] ; then
echo "Starting WLS with line:"
echo "${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
-Dweblogic.Name=${SERVER_NAME} -Djava.security.poli
cy=${WL_HOME}/server/lib/weblogic.policy ${PROXY_SETTINGS} ${SERVER_CLASS}"
${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
-Dcom.sun.jndi.ldap.connect.pool.maxsize=64
-Dcom.sun.jndi.ldap.connect.pool.prefsize=32
-Dcom.sun.jndi.ldap.connect.pool.initsize=8
-Dcom.sun.jndi.ldap.connect.pool.timeout=240000
-Dcom.sun.jndi.ldap.connect.pool.authentication=simple
-Dcom.sun.jndi.ldap.connect.pool.protocol="plain ssl"
-Dweblogic.Name=${SERVER_NAME}
-Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy
${PROXY_SETTINGS} ${SERVER_CLASS}
else
echo "Redirecting output from WLS window to ${WLS_REDIRECT_LOG}"
```

```
${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
-Dweblogic.Name=${SERVER_NAME}
-Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy
${PROXY_SETTINGS} ${SERVER_CLASS} >"${WLS_REDIRECT_LOG}" 2>&1
fi
```

5. ファイルを保存して閉じます。
6. Oracle WebLogic Server を再起動します。

管理対象サーバを使用した LDAP プール オプションの指定

1. WebLogic Administration Console にログインします。
2. ［**Lock & Edit**］ボタンをクリックします。
3. ［**Domain Structure**］ペインで、［**Environment**］-［**Servers**］に移動します。
4. 設定するサーバをクリックします。
5. 右側のペインで、［**Server Start**］をクリックします。
6. ［**Arguments**］フィールドに、以下の JVM オプションを含めます。
   - -Dcom.sun.jndi.ldap.connect.pool.maxsize=64
   - -Dcom.sun.jndi.ldap.connect.pool.prefsize=32
   - -Dcom.sun.jndi.ldap.connect.pool.initsize=8
   - -Dcom.sun.jndi.ldap.connect.pool.timeout=240000
   - -Dcom.sun.jndi.ldap.connect.pool.protocol="plain ssl"
   - -Dcom.sun.jndi.ldap.connect.pool.authentication=simple
7. ［**Save**］をクリックして、［**Activate Changes**］をクリックします。
8. Oracle WebLogic Server を再起動します。

JBoss アプリケーション サーバ

LDAP 接続プールを作成するには、以下の手順に従います。

1. 以下の場所に移動します。
   `<JBOSS_HOME>/server/<Profile>/deploy/`
2. テキスト エディタで properties-service.xml ファイルを開きます。
3. 以下のプロパティを <attribute name="Properties"> セクションに追加します。
   - com.sun.jndi.ldap.connect.pool.protocol=plain ssl
   - com.sun.jndi.ldap.connect.pool.authentication=simple
   - com.sun.jndi.ldap.connect.pool.maxsize=64
   - com.sun.jndi.ldap.connect.pool.prefsize=32
   - com.sun.jndi.ldap.connect.pool.timeout=240000
   - com.sun.jndi.ldap.connect.pool.initsize=8
4. ファイルを保存して閉じます。
5. JBoss アプリケーション サーバを再起動します。

JBoss

LDAP 接続プールを作成するには、以下の手順に従います。

1. 以下の場所に移動します。
   <*JBOSS_HOME*>¥standalone¥configuration
2. テキスト エディタで standalone.xml ファイルを開きます。
3. 以下のプロパティを追加します。

```
<system-properties>
<property name="com.sun.jndi.ldap.connect.pool.protocol"
value="plain ssl"/>
<property name="com.sun.jndi.ldap.connect.pool.authentication"
value="simple"/>
<property name="com.sun.jndi.ldap.connect.pool.maxsize"
value="64"/>
<property name="com.sun.jndi.ldap.connect.pool.prefsize"
value="32"/>
<property name="com.sun.jndi.ldap.connect.pool.timeout"
value="240000"/>
<property name="com.sun.jndi.ldap.connect.pool.initsize"
value="8"/>
<system-properties>
```

4. ファイルを保存して閉じます。
5. JBoss AS を再起動します。

Apache Tomcat のセキュリティ マネージャの有効化

Tomcat のセキュリティ マネージャを有効にするには、以下の手順に従います。

1. **JAVA_OPTS** 環境変数にセキュリティ マネージャ エントリを以下のように追加します。
   ```
   export CATALINA_OPTS="-Djava.security.manager
   -Djava.security.policy=<Tomcat_Home>/conf/catalina.policy"
   ```
2. 以下の Apache Tomcat のインストール場所に移動します。
   <Tomcat_Home>/conf/
3. テキスト エディタで catalina.policy ファイルを開きます。
4. 以下のコードを **WEB APPLICATION PERMISSIONS** セクションに追加します。
   ```
   grant {
   permission java.io.FilePermission
   "${catalina.base}${file.separator}webapps${file.separator}arcotuds${file.separator}-", "read";
   permission java.util.PropertyPermission "adb.converterutil", "read";
   permission java.lang.RuntimePermission "accessDeclaredMembers";
   permission java.security.SecurityPermission "putProviderProperty.BC";
   permission java.security.SecurityPermission "insertProvider.BC";
   permission java.security.SecurityPermission "putProviderProperty.SHAProvider";
   permission java.io.FilePermission "${arcot.home}${file.separator}-",
   "read,write";
   permission java.net.SocketPermission "*:1024-65535", "connect,accept,resolve";
   permission java.net.SocketPermission "*:1-1023", "connect,resolve";
   };
   ```
5. 管理コンソール (arcotadmin) およびユーザ データ サービス (arcotuds) に対する権限を付与するために、以下のセクションを追加します。
   ```
   grant codeBase "file:${catalina.home}/webapps/arcotuds/-" {
   permission java.lang.RuntimePermission "getenv.ARCOT_HOME", "";
   permission java.lang.RuntimePermission
   "accessClassInPackage.org.bouncycastle.asn1.*";
   permission java.security.AllPermission;
   };
   grant codeBase "file:${catalina.home}/webapps/arcotadmin/-" {
   permission java.lang.RuntimePermission "getenv.ARCOT_HOME", "";
   permission java.security.AllPermission;
   };
   ```
6. ファイルを保存して閉じます。
7. Apache Tomcat を再起動します。

第 15 章: AuthMinder Java SDK および Web サービスの設定

この章では、AuthMinder で提供される Java SDK（Software Development Kit）および Web サービスの設定手順について説明します。

この章は以下のトピックで構成されます。

AuthMinder API

AuthMinder には、JAR ファイルとして利用可能な Java API のセットが付属しており、以下の場所に保存されています。
`<install_location>/arcot/sdk/client/java/lib/arcot/`

このディレクトリには、以下の .JAR ファイルがあります。

- **arcot-webfort-authentication.jar**

  AuthMinder 認証 SDK を実装するために必要な JAR ファイル。このファイルは、ユーザ認証用のロジックを含む Java パッケージで構成されています。 このパッケージによって、以下の操作を実行できます。

  - AuthMinder がサポートする認証情報を使用したユーザの認証
  - カスタム認証情報の認証

- **arcot-webfort-common.jar**

  このファイルは、認証および認証情報管理（発行）操作に共通のクラスを含む Java パッケージで構成されています。このパッケージは以下の操作に使用されます。

  - AuthMinder サーバへの追加の情報の送信
  - ワンタイム パスワード タイプの指定
  - ユーザおよび認証情報ステータスの指定

- **arcot-webfort-issuance.jar**

  WebFort 認証情報管理 SDK を実装するために必要な JAR ファイル。 このファイルは、認証情報を管理するためのロジックを含む Java パッケージで構成されています。 このパッケージによって、以下の操作を実行できます。

  - 認証情報の作成と管理
  - ArcotID PKI キー バッグの管理

Java SDK の設定

このセクションでは、認証 Java SDK と認証情報管理 Java SDK を既存のアプリケーションと統合できるように設定する手順について説明します。

注: このセクションの設定手順を実行する前に、Java API を実装するために必要な JAR ファイルが、*<install_location>*/arcot/**sdk/client/java/lib/** にインストールされていることを確認してください。

認証 Java SDK の設定

J2EE アプリケーションで使用するために認証 SDK を設定する方法

1. 以下の場所から、以下のリストの JAR ファイルをコピーします。
   <install_location>/arcot

   コピー先には、*<APP_SERVER_HOME>* ディレクトリ内の適切な場所を選択します。 たとえば、Apache Tomcat の場合、この場所は *<Application_Home>/WEB-INF/lib* です。

   - sdk/client/java/lib/arcot/arcot-webfort-authentication.jar
   - sdk/client/java/lib/arcot/arcot-webfort-common.jar
   - sdk/client/java/lib/external/bcprov-jdk15-146.jar
   - sdk/client/java/lib/external/commons-pool-1.5.5.jar
2. 以下の場所から、サーバ接続パラメータを含む webfort.authentication.properties 設定ファイルをコピーします。
   <install_location>/arcot/sdk/client/java/properties

   コピー先には、<APP_SERVER_HOME> ディレクトリ内の適切な場所を選択します。 たとえば、Apache Tomcat の場合、コピー先は <Application_Home>/WEB-INF/classes/properties です。

注: API とその初期化の詳細については、「CA AuthMinder Java 開発者ガイド」および AuthMinder Javadoc（*<install_location>*/arcot/docs/webfort/Arcot-WebFort-7.1.01-authentication-sdk-javadocs.zip）を参照してください。

認証情報管理 Java SDK の設定

J2EE アプリケーションで使用する認証情報管理 SDK を設定する方法

1. 以下の場所から、以下のリストの JAR ファイルをコピーします。
   `<install_location>/arcot`

   コピー先には、*<APP_SERVER_HOME>* ディレクトリ内の適切な場所を選択します。 たとえば、Apache Tomcat の場合、この場所は *<Application_Home>/WEB-INF/lib* です。

   - sdk/client/java/lib/arcot/arcot-webfort-common.jar
   - sdk/client/java/lib/arcot/arcot-webfort-issuance.jar
   - sdk/client/java/lib/external/bcprov-jdk15-146.jar
   - sdk/client/java/lib/external/commons-pool-1.5.5.jar
2. 以下の場所から、サーバ接続パラメータを含む webfort.issuance.properties 設定ファイルをコピーします。
   `<install_location>/arcot/sdk/client/java/properties`

   コピー先には、<APP_SERVER_HOME> ディレクトリ内の適切な場所を選択します。 たとえば、Apache Tomcat の場合、コピー先は <Application_Home>/WEB-INF/classes/properties です。

注: Java API とその初期化の詳細については、「CA AuthMinder Java 開発者ガイド」、および AuthMinder Javadoc （*<install_location>*¥Arcot Systems¥docs¥webfort¥Arcot-WebFort-7.1.01-issuance-sdk-javadocs.zip）を参照してください。

AuthMinder Web サービスの使用方法

このセクションでは、以下のトピックについて説明します。

AuthMinder Web サービスの概要

AuthMinder は、ユーザ、組織、およびユーザ認証情報の管理、ユーザの認証、およびバルク操作を実行するための Web サービスを提供します。

以下の表に、AuthMinder サーバと通信するための Web サービス クライアント コードを生成するために使用できる WSDL ドキュメントを示します。これらの WSDL は、以下の場所にあります。
`<install_location>/arcot/wsdls/`

WSDL ファイル	説明
uds/**ArcotOrganizationManagementSvc.wsdl**	セットアップ内の組織の作成と管理のために使用します。
uds/**ArcotConfigManagementSvc.wsdl**	ユーザ アカウント タイプの作成と管理のために使用します。
uds/**ArcotUserManagementSvc.wsdl**	ユーザとユーザ アカウントの作成と管理のために使用します。
webfort/**ArcotWebFortAdminSvc.wsdl**	AuthMinder 設定を定義するために使用します。
webfort/**ArcotWebFortIssuanceSvc.wsdl**	ユーザ認証情報を管理するために使用します。
webfort/**ArcotWebFortAuthSvc.wsdl**	ユーザを認証するために使用します。
webfort/**ArcotWebFortBulkOperationsSvc.wsdl**	認証情報の作成、組織が利用可能な OATH トークンの割り当てと取得などのバルク操作を実行するために使用します。

クライアント コードの生成

クライアント コードを生成するには、以下の手順に従います。

1. アプリケーション サーバを停止します。
2. 以下の場所に移動します。
   <install_location>/arcot/wsdls/*<required_folder>*
3. WSDL ファイルを使用して、クライアント コードを生成します。
4. アプリケーション サーバを再起動します。
5. ブラウザ ウィンドウで、エンド ポイント URL にアクセスして、クライアントが Web サービスにアクセスできるかどうかを確認します。

注: エンドポイント URL へのアクセス方法の詳細については、「CA AuthMinder Web サービス開発者ガイド」を参照してください。

SSL 通信の有効化

AuthMinder は、AuthMinder サーバおよび Java SDK 間の SSL（Secure Socket Layer）をサポートしています。 AuthMinder サーバとそのクライアントの間のトランスポート モードを SSL に設定する方法については、「*CA AuthMinder 管理ガイド*」の「SSL の設定」のトピックを参照してください。

付録 I: AuthMinder ファイル システム構造

この付録では、AuthMinder インストーラによってインストールされるすべてのファイルの場所について説明します。

重要: AuthMinder によってインストールされるファイルを削除しないでください。

発行および認証 AuthMinder サーバ ファイル

以下の表に、AuthMinder サーバで使用されるファイルのフォルダの場所を示します。

フォルダ	ファイル説明
<install_location>/	arcotkey および wfkey ファイルが含まれています。 これらのファイルは、インストーラによって使用され、過去にインストールした Arcot 製品を検出します。 これらのファイルを削除した場合、インストーラは過去にインストールした Arcot 製品を検出できず、任意の場所で新規インストールが実行されます。 その結果、インストーラは、複数の Arcot 製品およびコンポーネントの、同一の宛先フォルダを確保できません。この場合、製品（またはコンポーネント）は、正常に機能しない場合があります。このファイルは、パッチおよびアップグレードに影響を及ぼしません。 wfdbkey ファイルおよび wftpkey ファイルは、データベースおよびサードパーティの JAR ファイルの参照キー ファイルです。これらのキー ファイルはアップグレード時に使用されます。

フォルダ	ファイル説明
<*install_location*>/arcot/bin	sbin フォルダ内のサーバのバイナリを呼び出す webfortserver スクリプトが含まれています。
<*install_location*>/arcot/conf	以下の設定ファイルが含まれています。 ■ arcotcommon.ini（P. 437） ■ securestore.enc： 機密データの暗号化に使用されるキーが含まれているファイル。
<*install_location*>/arcot/dbscripts	AuthMinder スキーマを作成する SQL スクリプトが含まれています。 データベース スクリプトの詳細については、「データベース スクリプトの実行」を参照してください。
<*install_location*>/arcot/logs	AuthMinder サーバのログ ファイルが含まれています。
<*install_location*>/arcot/odbc32v70wf	AuthMinder によってサポートされるすべてのデータベース用の、ブランド製品の DataDirect ODBC ライブラリが含まれています。
<*install_location*>/arcot/sbin	管理者に必要なライブラリ ファイルおよび以下の実行可能ファイルが含まれています。 ■ arwfutil - AuthMinder サーバをシャットダウンし、リフレッシュするために使用されます。 ■ arwfserver.real - 構成を設定し、arwfutil バイナリを実行するスクリプトへのシンボリック リンクが含まれています。 ■ arwfwatchdog - このツールはサーバ健全性を監視し、また、停止したサーバを起動します。 ■ arwfenv - 環境変数を設定するために使用されるスクリプト。
<*install_location*>/samples/xml/webfort	ArcotWebFortBulkOperationsSvc.wsdl ファイルで使用される以下のファイルが含まれています。 ■ oath-token-assign.xml ■ oath-token-upload.xml
<*install_location*>/arcot/sdk/server/plugin/c/docs	以下のプラグイン インターフェース ファイルが含まれています。 ■ webfort-plugin-cpp-interface.html

フォルダ	ファイル説明
<*install_location*>/arcot/sdk/server/plugin/c/include/webfort/vas	以下の SDK プラグイン ヘッダ ファイルが含まれています。 ■ wf-common-interface.h ■ wf-common-interface.hpp ■ wf-plugin-interface.h
<*install_location*>/arcot/sdk/server/plugin/c/lib	プラグイン ライブラリを含む arwfpluginsdk.so が含まれています。
<*install_location*>/arcot/tools/<*platform_name*>	以下のファイルが含まれています。 ■ **DBUtil**： AuthMinder データベースに接続するために必要なデータベース情報を暗号化された形式で格納する securestore.enc を編集するためのツール。
<*install_location*>/arcot/Uninstall_Arcot WebFort	AuthMinder のアンインストールに必要な実行可能ファイルが含まれています。

管理コンソールのファイル

以下の表に、管理コンソールで使用されるファイルのフォルダの場所を示します。

フォルダ	ファイル説明
<*install_location*>/	arcotkey および wfkey ファイルが含まれています。これらのファイルは、インストーラによって使用され、過去にインストールした Arcot 製品を検出します。これらのファイルを削除した場合、インストーラは過去にインストールした Arcot 製品を検出できず、任意の場所で新規インストールが実行されます。 その結果、インストーラは、複数の Arcot 製品およびコンポーネントの、同一の宛先フォルダを確保できません。この場合、製品（またはコンポーネント）は、正常に機能しない場合があります。 このファイルは、パッチおよびアップグレードに影響を及ぼしません。 wfdbkey ファイルおよび wftpkey ファイルは、データベースおよびサードパーティの JAR ファイルの参照キー ファイルです。 これらのキー ファイルはアップグレード時にインストーラによって使用されます。

フォルダ	ファイル説明
<*install_location*>/arcot/conf	以下の設定ファイルが含まれています。 ■ arcotcommon.ini（P. 437） ■ adminserver.ini（P. 447） ■ securestore.enc： 機密データの暗号化に使用されるキーが含まれているファイル。
<*install_location*>/arcot/conf/resourcebundles	以下のメッセージ プロパティ ファイルが含まれています。 ■ arcot-common-message_en_US.properties ■ arcot-uds-message_en_US.properties
<*install_location*>/arcot/dbscripts	管理コンソールのスキーマを作成する SQL スクリプトが含まれています。 データベース スクリプトの詳細については、「データベース スクリプトの実行」を参照してください。
<*install_location*>/arcot/java/lib	管理コンソール フレームワークに必要な以下の WAR ファイルおよび JAR ファイルが含まれています。 ■ adminframework.jar ■ adminframework.war ■ arcot-common.jar ■ arcot-crypto-util.jar ■ bcprov-jdk15-146.jar
<*install_location*>/arcot/java/lib/sdk	これは空のディレクトリです。arcotadmin.war ファイルおよび arcotuds.war ファイルを作成するために bundlemanager ツールで使用される必要がある JAR ファイルを含める必要があります。
<*install_location*>/arcot/java/webapps	管理コンソールの展開に必要な arcotadmin.war ファイルが含まれています。
<*install_location*>/arcot/logs	管理コンソールのログ ファイルが含まれています。
<*install_location*>/arcot/java/native/<*platform_name*>/<*32 or 64 bit*>	securestore.enc ファイルの内容を読み取るために使用される libArcotAccessKeyProvider.so ファイルが含まれています。
<*install_location*>/arcot/odbc32v70wf	AuthMinder によってサポートされるすべてのデータベース用の、ブランド製品の DataDirect ODBC ライブラリが含まれています。

フォルダ	ファイル説明
<*install_location*>/arcot/resourcepacks	以下の AuthMinder および管理コンソール パッケージが含まれています。 ■ bundle_webfort.zip ■ bundler_adminconsole.zip
<*install_location*>/arcot/resourcepacks/i18n//	アカウント ステータス値を更新するための以下のプロパティ ファイルが含まれています。 ■ framework-useraccount-status.properties
<*install_location*>/arcot/tools/common/	以下のサブディレクトリがあります。 ■ **arreporttool** サブディレクトリには、レポートをエクスポートできるレポート ツールが含まれています。 ■ **bundlemanager** サブディレクトリには管理コンソール リソース パックに必要なファイルが含まれています。
<*install_location*>/arcot/tools/<*platform_name*>	以下のファイルが含まれています。 ■ **DBUtil**： AuthMinder データベースに接続するために必要なデータベース情報を暗号化された形式で格納する securestore.enc を編集するためのツール。
<*install_location*>/arcot/Uninstall_Arcot WebFort	アンインストール関連のファイルが含まれています。

ユーザ データ サービスのファイル

以下の表に、ユーザ データ サービスで使用されるファイルのフォルダの場所を示します。

フォルダ	ファイル説明
<*install_location*>/	arcotkey ファイルが含まれています。 このファイルは、以前にインストールされた Arcot 製品を検出するためにインストーラによって使用されます。 これらのファイルを削除した場合、インストーラは過去にインストールした Arcot 製品を検出できず、任意の場所で新規インストールが実行されます。 その結果、インストーラは、複数の Arcot 製品およびコンポーネントの、同一の宛先フォルダを確保できません。この場合、製品（またはコンポーネント）は、正常に機能しない場合があります。 このファイルは、パッチおよびアップグレードに影響を及ぼしません。 wfdbkey ファイルおよび wftpkey ファイルは、データベースおよびサードパーティの JAR ファイルの参照キー ファイルです。 これらのキー ファイルはアップグレード時に使用されます。
<*install_location*>/arcot/conf	以下の設定ファイルが含まれています。 ■ arcotcommon.ini（P. 437） ■ udsserver.ini（P. 449） ■ securestore.enc： 機密データの暗号化に使用されるキーが含まれているファイル。
<*install_location*>/arcot/conf/resource bundles	以下のメッセージ プロパティ ファイルが含まれています。 ■ arcot-common-message_en_US.properties ■ arcot-uds-message_en_US.properties
<*install_location*>/arcot/dbscripts	管理コンソールのスキーマを作成する SQL スクリプトが含まれています。 データベース スクリプトの詳細については、「データベース スクリプトの実行」を参照してください。
<*install_location*>/arcot/docs/uds	UDS の WSDL ドキュメントを含む arcot-uds-2_0-wsdl-docs.zip ファイルが含まれています。

フォルダ	ファイル説明
<*install_location*>/arcot/java/lib	ユーザ データ サービスに必要な WAR ファイルおよび JAR ファイルが含まれています。 ■ arcot-common.jar ■ arcot-crypto-util.jar ■ arcot-euds.jar ■ bcprov-jdk15-146.jar ■ udsframework.war
<*install_location*>/arcot/java/lib/sdk	これは空のディレクトリです。arcotadmin.war ファイルおよび arcotuds.war ファイルを作成するために bundlemanager ツールで使用される必要がある JAR ファイルを含める必要があります。
<*install_location*>/arcot/java/webapps	展開に必要な arcotuds.war ファイルおよびユーザ データ サービスが含まれています。
<*install_location*>/arcot/logs	UDS ログ ファイルが含まれています。
<*install_location*>/arcot/java/native/<*platform_name*>/<*32 or 64 bit*>	securestore.enc ファイルの内容を読み取るために使用される libArcotAccessKeyProvider.so ファイルが含まれています。
<*install_location*>/arcot/odbc32v70wf	AuthMinder によってサポートされるすべてのデータベース用の、ブランド製品の DataDirect ODBC ライブラリが含まれています。
<*install_location*>/arcot/tools/common/	以下のサブディレクトリが含まれています。 ■ **uds-monitor** サブディレクトリには、UDS を監視できるツールが含まれています。
<*install_location*>/arcot/tools/<*platform_name*>	以下のファイルが含まれています。 ■ **DBUtil** : AuthMinder データベースに接続するために必要なデータベース情報を暗号化された形式で格納する securestore.enc を編集するためのツール。
<*install_location*>/arcot/Uninstall_Arcot WebFort	アンインストール関連のファイルが含まれています。

フォルダ	ファイル説明
<*install_location*>/arcot/wsdls/uds	以下のドキュメントが含まれています。 ■ Web サービス クライアントがコードを生成するために使用する WSDL ファイル ArcotConfigManagementSvc.wsdl ArcotOrganizationManagementSvc.wsdl ArcotUserManagementSvc.wsdl ■ バルク操作を実行するために Web サービスで使用される XSD ファイル ArcotUserSchema.xsd

認証 Java SDK ファイル

以下の表に、認証 Java SDK で使用されるファイルのフォルダの場所を示します。

フォルダ	ファイル説明
<*install_location*>/arcot/docs/webfort	認証 SDK 用の Javadoc を含む Arcot-WebFort-7.1.01-authentication-sdk-javadocs.zip ファイルが含まれています。
<*install_location*>/arcot/samples/java	サンプル アプリケーションを展開するための webfort-7.1.01-sample-application.war ファイルが含まれています。
<*install_location*>/arcot/sdk/client/java/lib/arcot	AuthMinder 認証 Java SDK 用の以下の JAR ファイルが含まれています。 ■ arcot-webfort-common.jar ■ arcot-webfort-authentication.jar
<*install_location*>/arcot/sdk/client/java/lib/external	AuthMinder 認証 Java SDK に必要なサードパーティ JAR ファイルが含まれています。 ■ bcprov-jdk15-146.jar ■ commons-pool-1.5.5.jar
<*install_location*>/arcot/sdk/client/java/properties	サンプル プロパティ（webfort.authentication.properties）ファイルが含まれています。 Java SDK の初期化にこのファイルのパラメータを使用することも、init() 関数を使用することもできます。

発行 Java SDK ファイル

以下の表に、発行 Java SDK で使用されるファイルのフォルダの場所を示します。

フォルダ	ファイル説明
<*install_location*>/arcot/docs/webfort	発行 SDK 用の Javadoc を含む Arcot-WebFort-7.1.01-issuance-sdk-javadocs.zip ファイルが含まれています。
<*install_location*>/arcot/samples/java	サンプル アプリケーションを展開するための webfort-7.1.01-sample-application.war ファイルが含まれています。
<*install_location*>/arcot/sdk/client/java/lib/arcot	発行 Java SDK 用の以下の JAR ファイルが含まれています。 ■ arcot-webfort-common.jar ■ arcot-webfort-issuance.jar
<*install_location*>/arcot/sdk/client/java/lib/external	AuthMinder 発行 Java SDK に必要なサードパーティ JAR ファイルが含まれています。 ■ bcprov-jdk15-146.jar ■ commons-pool-1.5.5.jar
<*install_location*>/arcot/sdk/client/java/properties	サンプル プロパティ（webfort.issuance.properties）ファイルが含まれています。 Java SDK の初期化にこのファイルのパラメータを使用することも、init() 関数を使用することもできます。

Web サービス ファイル

以下の表に、UDS Web サービスに関連するファイルのフォルダの場所を示します。

フォルダ	ファイル説明
<*install_location*>/arcot/docs/uds	UDS の WSDL ドキュメントを含む arcot-uds-2_0-wsdl-docs.zip ファイルが含まれています。

フォルダ	ファイル説明
<*install_location*>/arcot/docs/webfort	以下の WSDL ドキュメントが含まれています。 ■ Arcot-WebFort-7.1.01-admin-wsdldocs.zip ■ Arcot-WebFort-7.1.01-authentication-wsdldocs.zip ■ Arcot-WebFort-7.1.01-issuance-wsdldocs.zip
<*install_location*>/arcot/wsdls/uds	以下のドキュメントが含まれています。 ■ Web サービス クライアントがコードを生成するために使用する WSDL ファイル ArcotConfigManagementSvc.wsdl ArcotOrganizationManagementSvc.wsdl ArcotUserManagementSvc.wsdl ■ バルク操作を実行するために Web サービスで使用される XSD ファイル ArcotUserSchema.xsd
<*install_location*>/arcot/wsdls/webfort	以下のドキュメントが含まれています。 ■ Web サービス クライアントがコードを生成するために使用する WSDL ファイル ArcotWebFortAdminSvc.wsdl ArcotWebFortAuthSvc.wsdl ArcotWebFortBulkOperationsSvc.wsdl ArcotWebFortIssuanceSvc.wsdl ■ 管理および認証情報のバルク操作を実行するために Web サービスで使用される XSD ファイル ArcotWebFortAdminMsgs.xsd ArcotWebFortAdminSchema.xsd ArcotWebFortAuthMsgs.xsd ArcotWebFortAuthSchema.xsd ArcotWebFortCommonSchema.xsd ArcotWebFortCredMgmt.xsd ArcotWebFortIssuanceMsgs.xsd ArcotWebFortIssuanceSchema.xsd ArcotWebFortTokenXchange.xsd

プラグイン SDK

以下の表に、プラグイン SDK で使用されるファイルのフォルダの場所を示します。

フォルダ	ファイル説明
<*install_location*>/arcot/sdk/server/plugin/c/lib	プラグイン ライブラリを含む arwfpluginsdk.so が含まれています。
<*install_location*>/arcot/sdk/server/plugin/c/include/webfort/vas	以下の SDK プラグイン ヘッダ ファイルが含まれています。 ■ wf-common-interface.h ■ wf-common-interface.hpp ■ wf-plugin-interface.h
<*install_location*>/arcot/sdk/server/plugin/c/lib	プラグイン ライブラリを含む arwfpluginsdk.so が含まれています。

付録 J: 設定ファイルおよびオプション

このトピックでは、AuthMinder が使用する設定ファイル、およびこれらのファイル内で設定する必要があるパラメータについて説明します。

以下の AuthMinder 設定ファイルは、*<install_location>*/arcot/**conf** にあります。

- arcotcommon.ini（P. 437）
- adminserver.ini（P. 447）
- udsserver.ini（P. 449）

以下のプロパティ ファイルは、*<install_location>*/arcot/sdk/client/java/**properties/** にあります。

- webfort.authentication.properties（P. 451）
- webfort.issuance.properties（P. 453）

INI ファイル

arcotcommon.ini

arcotcommon.ini ファイルには、データベース用のパラメータ、AuthMinder サーバ、および AuthMinder のその他のコンポーネント（管理コンソールおよびユーザ データ サービス）用のインスタンス設定が含まれています。このセクションでは、arcotcommon.ini ファイルの以下のパラメータについて説明します。

- AuthMinder サーバによって使用されるパラメータ（P. 438）
- 管理コンソールおよびユーザ データ サービスによって使用されるパラメータ（P. 441）

AuthMinder サーバによって使用されるパラメータ

以下の表に、AuthMinder サーバで使用されるデータベースと暗号化の設定を示します。 AuthMinder サーバ用のデータベースの追加設定は、管理コンソールのインスタンス管理画面を使用して実行する必要があります。

パラメータ	デフォルト	説明
[arcot/db/dbconfig] セクションの共通のデータベース パラメータ		
DbType	デフォルト値なし	すべてのデータベース接続に適用可能なデータベースのタイプ。 サポートされている値は以下のとおりです。 ■ mssqlserver ■ oracle ■ db2 ■ mysql
EnableBrandLicensing	0	ブランド設定された ODBC ドライバが使用されているかどうか。 これは、DataDirect のブランド設定された ODBC ドライバを使用しているときに使用できます。
BrandLicenseFile	デフォルト値なし	ブランド設定された ODBC ドライバを使用するときのライセンス ファイル名。
StartWithAnyPool	1 （有効）	プライマリ データベースが使用不可能な場合、AuthMinder でバックアップ データベースを使用できるようにします。
[arcot/db/primarydb] および [arcot/db/backupdb] セクションのプライマリおよびバックアップ データベース接続パラメータ		
Datasource.*N*	デフォルト値なし	サーバ データをホストするプライマリ データベースを示す ODBC システム データ ソース名（DSN）の名前。
Username.*N*	デフォルト値なし	データベースへのアクセス用に、サーバによって使用されるユーザ名。
[arcot/crypto/device] セクションの暗号化モード設定パラメータ		

パラメータ	デフォルト	説明
HSMDevice	s/w	データベースに格納されているキーを使用して、またはハードウェア セキュリティ モジュール（HSM）の 1 つを使用して、AuthMinder 情報を暗号化する必要があるかどうかを設定するモード。 サポートされている値は以下のとおりです。 ■ **s/w**： データベースに格納されているキー ラベルを使用してデータが暗号化されることを示します。 ■ **chrysalis**： データを暗号化するために Chrysalis（Luna） HSM が使用されることを示します。 ■ **nfast**： データを暗号化するために nFast（nCipher netHSM）が使用されることを示します。
[crypto/pkcs11modules/chrysalis] セクションの Chrysalis （Luna） HSM 設定パラメータ		
sharedLibrary	デフォルト値なし	HSM に対応する PKCS#11 共有ライブラリへの絶対パス。 Chrysalis（Luna）のデフォルト値は、以下のとおりです。 /usr/lunasa/lib/libCryptoki2.so
storageSlot	0	データの暗号化に使用された 3DES キーが存在する HSM スロット。
accelSlot	0	Arcot で内部的に使用されるスロット。
sessionCount	20	HSM デバイスで確立できるセッションの最大数。
[crypto/pkcs11modules/nfast] セクションの nFast （nCipher netHSM） HSM 設定パラメータ		
sharedLibrary	デフォルト値なし	HSM に対応する PKCS#11 共有ライブラリへの絶対パス。 nFast （nCipher netHSM）のデフォルト値は、以下のとおりです。 /opt/nfast/toolkits/pkcs11/libcknfast.so
storageSlot	1	データの暗号化に使用された 3DES キーが存在する HSM スロット。
accelSlot	0	Arcot で内部的に使用されるスロット。

パラメータ	デフォルト	説明
sessionCount	200	HSM デバイスで確立できるセッションの最大数。
[arcot/watchdog] セクション内の Watchdog 設定		
ServerStartsTimeout	25	サーバ起動からの期間。 watchdog が ServerStartsTimeout（25 分）の指定された期間内に 5 回サーバを起動すると、サーバは再び再起動されなくなります。 時間は分単位です。
ServerStartsCount	5	サーバを再起動する最大回数。 この後には、サーバは再び再起動されません。
RestartSleepTime	5000	watchdog がサーバを再起動する前のスリープ時間。 スリープ時間はミリ秒単位です。

サーバ起動ログ パラメータの変更

AuthMinder サーバの起動時に表示されるログ パラメータを変更する場合は、以下の手順に従います。

1. ARCOT_HOME 内の conf ディレクトリに移動します。
2. 任意のテキスト エディタで arcotcommon.ini を開きます。
3. 以下のセクションをファイルの最後に追加します。

```
[arcot/WebFort/startup]
LogFile=
LogFileSize=10485760
BackupLogFileDir=
LogLevel=
LogTimeGMT=0
```

以下の表に、これらのパラメータの説明を示します。

パラメータ	デフォルト	説明
LogFile		ログ ファイルのデフォルト ディレクトリのファイル パスとログ ファイルの名前。 **注**: このパスは ARCOT_HOME（<*install_location*>/arcot/）からの相対パスです。

パラメータ	デフォルト	説明
LogFileSize	10485760	ログ ファイルが記録できる最大**バイト**数。 ログ ファイルがこのサイズに達すると、新しいファイルが生成され、古いファイルは BackupLogFileDir で指定した場所に移動されます。
BackupLogFileDir		現在のファイルが LogFileSize のバイト数を超えた後で、バックアップ ログ ファイルが保持されるディレクトリの場所。 **注**: このパスは ARCOT_HOME（<*install_location*>/arcot/）からの相対パスです。
LogLevel		サーバのデフォルトのログ記録レベル（上書きが指定されていない場合）。 以下の値を指定できます。 ■ 0 FATAL ■ 1 WARNING ■ 2 INFO ■ 3 DETAIL
LogTimeGMT	0	ログ ファイル内のタイム スタンプのタイム ゾーンを示すパラメータ。 以下の値を指定できます。 ■ 0 ローカル時間 ■ 1 GMT

1. 変更するパラメータに必要な値を設定します。
2. ファイルを保存して閉じます。
3. AuthMinder サーバを再起動します。

管理コンソールおよびユーザ データ サービスによって使用されるパラメータ

以下の表に、arcotcommon.ini ファイルのデータベース設定パラメータの説明を示します。

パラメータ	デフォルト	説明
[arcot/db/dbconfig] セクションの共通のデータベース パラメータ		

パラメータ	デフォルト	説明
DbType	デフォルト値なし	すべてのデータベース接続に利用可能なデータベースのタイプ。サポートされている値は以下のとおりです。 ■ oracle ■ mssqlserver ■ db2 ■ mysql
Driver	デフォルト値なし	JDBC ドライバ ベンダーによって提供される JDBC ドライバ クラスの完全修飾名。正しいドライバ名を知るには、JDBC ベンダーのマニュアルを参照してください。 ■ **Oracle データベースの場合** - oracle.jdbc.driver.OracleDriver ■ **Microsoft SQL Server の場合** - com.microsoft.sqlserver.jdbc.SQLServerDriver ■ **IBM DB2 UDB の場合** - jcom.ibm.db2.jcc.DB2Driver ■ **MySQL の場合** - com.mysql.jdbc.Driver
MinConnections	4	AuthMinder コンポーネントとデータベース間に最初に作成する接続の最小数。
MaxConnections	32	AuthMinder コンポーネントとデータベース間に作成できる接続の最大数。
IncConnections	2	AuthMinder コンポーネントとデータベース間に新しい接続が必要なときに作成される接続の数。
MaxIdleConnections	4	サーバが管理できるアイドル データベース接続の最大数。
MaxWaitTimeForConnection	30000	接続が、タイムアウトする前に、使用可能になるまで、サーバが待機する必要がある（使用可能な接続がない場合）最大時間（ミリ秒単位）。

パラメータ	デフォルト	説明
AutoRevert	1	フェイルオーバーの発生後に、システムがプライマリ データベースへの接続を試みるかどうかを指定します。 バックアップ データベースを設定している場合、およびフェイルオーバ発生後にサーバがプライマリ データベースに接続するようにする場合は、AutoRevert=1 を設定します。
MaxTries	3	サーバがデータベースへの接続を中止する前の接続試行回数。
ConnRetrySleepTime	100	データベースへの接続試行間の遅延時間（ミリ秒単位）。
MonitorSleepTime	50	すべてのデータベースに対するハートビート チェック間に監視スレッドがスリープする時間（秒単位）。
Profiling	0	データベース メッセージをログに記録するかどうかを指定します。 データベース メッセージのログ記録を有効にする場合は、値を 1 に設定します。
EnableBrandLicensing	0	ブランド設定された ODBC ドライバが使用されているかどうかを指定します。
BrandLicenseFile	IVWF.LIC	ブランド設定された ODBC ドライバを使用するときのライセンス ファイル名。EnableBrandLicensing の値が 1 の場合に、このパラメータが必要です。それ以外の場合は無視されます。 この値が存在する場合は編集 *しないでください*。
MaxTransactionRetries	3	事前定義されたエラー状態についてデータベース インスタンスでトランザクションを再試行する最大回数。
TransactionRetrySleepTime	10	2 つの連続するトランザクション再試行間の間隔（ミリ秒単位）。
[arcot/db/primarydb] および [arcot/db/backupdb] セクションのプライマリおよびバックアップ データベース接続パラメータ		

パラメータ	デフォルト	説明
Datasource.*N*		サーバ データをホストするプライマリ データベースを示す ODBC システム データ ソース名（DSN）の名前。
AppServerConnectionPoolName.*N*	デフォルト値なし	アプリケーション サーバのデータベース接続プーリング機能を使用している場合、接続プール オブジェクトの検索に使用する JNDI 名。 この JNDI 名によるプールは、含まれるアプリケーション サーバ内に作成する必要があります。また、AuthMinder Web アプリケーションに対して、接続プールを使用するための十分なアクセス権限を与える必要があります。 ■ JNDI 名を **Apache Tomcat** 内で設定する場合は、完全修飾 JNDI 名を使用します。 以下に例を示します。 AppServerConnectionPoolName.1=java:comp/env/SampleDS ■ **Apache 以外のアプリケーション サーバ**については、JNDI 名だけ指定します。 以下に例を示します。 AppServerConnectionPoolName.1=SampleDS 詳細については、付録「アプリケーション サーバの設定」を参照してください。 アプリケーション サーバ接続プールが*必要でない*場合は、この設定を空のままにします。

パラメータ	デフォルト	説明
URL.*N*	デフォルト値なし	JDBC データ ソースの名前。 ■ Oracle データベースの場合 - jdbc:oracle:thin:@<*server*>:<*oracle_port*>:<*sid*> ■ Microsoft SQL Server の場合 - jdbc:sqlserver://<*server*>:<*sql_port*>;databaseName=<*databasename*>;selectMethod=cursor ■ IBM DB2 UDB の場合 - jdbc:db2://<*server*>:<*db2_port*>/<*database*> ■ MySQL の場合 - jdbc:mysql://<*server*>:<*mysql_port*>/<*database*>
Username.*N*	デフォルト値なし	データベースへのアクセス用に、サーバによって使用されるユーザ名。
TrustStorePath.*N*	デフォルト値なし	Datasource.*N* に対応する SSL 証明書トラスト ストア パス。 このパス（ファイル名を含む）は証明書 truststore ファイルを参照します。このファイルには、クライアントが信頼する証明書のリストが含まれています。 **注**: TrustStore Path.*N* に対応するパスワードは、DBUtil ツールを使用して、キーとして TrustStorePath.*N* の値と共に securestore.enc に安全に格納する必要があります。 このツールの詳細については、「CA AuthMinder 管理ガイド」を参照してください。
KeyStorePath.*N*	デフォルト値なし	**注**: この属性は MySQL でのみ使用されます。 RiskMinder および MySQL データベースの間で一方向の SSL を設定する場合、これは値を指定する必要があるパラメータの 1 つです。 このパラメータは、Datasource.N に対応する SSL 証明書キーストア パスを保持します。 パス（ファイル名を含む）は、証明書キーストア ファイルを参照します。KeyStorePath.*N* に対応するパスワードは、キーとして KeyStorePath.*N* の値と共に securestore.enc 内に安全に格納する必要があります。

パラメータ	デフォルト	説明
HostNameInCertificate.*N*	デフォルト値なし	トラスト ストア内の Datasource.*N* SSL 証明書に含まれるサブジェクト識別名（DN）の共通名（CN）の値。 **注**: このパラメータは、Microsoft SQL Server を使用している場合のみ必要です。
[arcot/crypto/device] セクションの暗号化モード設定パラメータ		
HSMDevice	s/w	データベースに格納されているキーを使用して、またはハードウェア セキュリティ モジュール（HSM）の 1 つを使用して、情報を暗号化する必要があるかどうかを設定するモード。 サポートされている値は以下のとおりです。 ■ **s/w**： データベースに格納されているキー ラベルを使用してデータが暗号化されることを示します。 ■ **chrysalis**： データを暗号化するために Chrysalis（Luna） HSM が使用されることを示します。 ■ **nfast**： データを暗号化するために nFast（nCipher netHSM）が使用されることを示します。
[crypto/pkcs11modules/chrysalis] セクションの Chrysalis （Luna） HSM 設定パラメータ		
sharedLibrary	デフォルト値なし	HSM に対応する PKCS#11 共有ライブラリへの絶対パス。 Chrysalis （Luna）のデフォルト値は、以下のとおりです。 /usr/lunasa/lib/libCryptoki2.so
storageSlot	0	データの暗号化に使用された 3DES キーが存在する HSM スロット。
accelSlot	0	Arcot で内部的に使用されるスロット。
sessionCount	20	HSM デバイスで確立できるセッションの最大数。
[crypto/pkcs11modules/nfast] セクションの nFast （nCipher netHSM） HSM 設定パラメータ		

パラメータ	デフォルト	説明
sharedLibrary	デフォルト値なし	HSM に対応する PKCS#11 共有ライブラリへの絶対パス。 nFast （nCipher netHSM）のデフォルト値は、以下のとおりです。 /opt/nfast/toolkits/pkcs11/libcknfast.so
storageSlot	1	データの暗号化に使用された 3DES キーが存在する HSM スロット。
accelSlot	0	Arcot で内部的に使用されるスロット。
sessionCount	200	HSM デバイスで確立できるセッションの最大数。
[arcot/system] セクションのインスタンス ID 設定パラメータ		
InstanceId	1	管理コンソールまたはユーザ データ サービス インスタンスを識別するために使用できるパラメータ。 サーバのすべてのインスタンスに対して一意の値を指定する必要があります。 インスタンス ID はトランザクション レポートにも表示されます。 このパラメータには整数値を指定する必要があります。

adminserver.ini

adminserver.ini ファイルには、管理コンソールのログ情報を設定するパラメータが含まれています。 以下の表に、管理コンソールのログ ファイル情報を示します。

パラメータ	デフォルト値	説明
[arcot/admin/logging] セクションのログ設定パラメータ		

パラメータ	デフォルト値	説明
log4j.rootCategory	ERROR、roothandle **重要**: roothandle は管理コンソール ログ ハンドルの名前で、*必ず*指定する必要があります。	ロガー階層の一番上に存在するルート ロガー。値が指定されていない場合、子ロガーはすべてこの値を継承します。
■ log4j.logger.com.arcot.euds ■ log4j.logger.com.arcot.admin ■ log4j.logger.com.arcot.admin.framework ■ log4j.logger.com.arcot.adminconsole ■ log4j.logger.com.arcot.common.cache ■ log4j.logger.com.arcot.common.crypto ■ log4j.logger.com.arcot.crypto.impl.SecureStoreUtil ■ log4j.logger.com.arcot.common.database ■ log4j.logger.com.arcot.common.ldap	INFO	管理コンソールのログを書き込むために使用する必要のあるログ レベルを指定します。サポートされるログ レベルは以下のとおりです。 ■ FATAL ■ WARNING ■ INFO ■ DEBUG **注**: ログ レベルの詳細については、「CA AuthMinder 管理ガイド」を参照してください。
log4j.appender.roothandle.Encoding	UTF-8	ログ ファイルにエントリを書き込むときに使用するエンコーディング。

パラメータ	デフォルト値	説明
log4j.appender.roothandle.File	${arcot.home}/logs/arcotadmin.log	管理コンソール ログのファイル名と、ログが作成される場所。 管理コンソールのデフォルトのログ ファイル名は arcotadmin.log で、以下の場所に作成されます。 <*install_location*>/arcot/**logs/**
log4j.appender.roothandle.MaxFileSize	10 MB	ログ ファイルについて許可される最大サイズ。
log4j.appender.roothandle.MaxBackupIndex	100	作成できるバックアップ ファイルの最大数。 バックアップ ファイルの数がこの値に達すると、アプリケーションは先頭のログ ファイルから上書きを開始します。
log4j.appender.roothandle.layout	org.apache.log4j.PatternLayout	ConversionPattern で指定されている出力形式。
log4j.appender.roothandle.layout.ConversionPattern	%d{yyyy-MM-dd hh:mm:ss,SSSz} : [%t] : %-5p : %-5c{3} : %m%n	管理コンソール ログ ファイル エントリが書き込まれる形式 ■ タイム スタンプ（%d{yyyy-MM-dd hh:mm:ss,SSSz} :） ■ スレッド ID （[%t] :） ■ ログ レベル（または重大度）（%-5p :） ■ ロガー クラス（%-5c{3} :） ■ メッセージ（%m%n） このパターンは C 言語の printf 関数に似ています。

udsserver.ini

udsserver.ini ファイルには、ユーザ データ サービス（UDS）のログ情報を設定するためのパラメータが含まれています。 以下の表に、UDS のログ ファイル情報を示します。

パラメータ	デフォルト値	説明
[arcot/uds/logger] セクションのログ設定パラメータ		

パラメータ	デフォルト値	説明
log4j.rootCategory	ERROR、debuglog	ロガー階層の一番上に存在するルート ロガー。値が指定されていない場合、子ロガーはすべてこの値を継承します。
■ log4j.logger.com.arcot.euds ■ log4j.logger.com.arcot.crypto.impl.SecureStoreUtil ■ log4j.logger.com.arcot.common.database ■ log4j.logger.com.arcot.common.cache	INFO	UDS ログを書き込むために使用する必要のあるログ レベルを指定します。 サポートされるログ レベルは以下のとおりです。 ■ FATAL ■ WARNING ■ INFO ■ DEBUG **注**: ログ レベルの詳細については、「CA AuthMinder 管理ガイド」を参照してください。
log4j.appender.debuglog.File	${arcot.home}/logs/arcotuds.log	ログ ファイル名、および UDS ログを書き込む必要のある場所を指定します。 デフォルトでは、UDS ログ ファイル名は arcotuds.log で、<*install_location*>/arcot/ にあるログ フォルダ内に作成されます。
log4j.appender.debuglog.MaxFileSize	10 MB	ログ ファイルのサイズを指定します。デフォルトでは、2 MB です。
log4j.appender.debuglog.MaxBackupIndex	100	作成できるバックアップ ファイルの数を指定します。バックアップ ファイルの数がこの数と等しいとき、アプリケーションは最初のログ ファイルから上書きを開始します。
log4j.appender.debuglog.layout	org.apache.log4j.PatternLayout	ConversionPattern で指定されている出力形式。
log4j.appender.debuglog.Encoding	UTF-8	ログ ファイルにエントリを書き込むときに使用するエンコーディング。

パラメータ	デフォルト値	説明
log4j.appender.debuglog.layout.ConversionPattern	%d{yyyy-MM-dd hh:mm:ss,SSS z} : [%t] : %-5p : %-5c{3} : %m%n	UDS ログ ファイル エントリが書き込まれる形式 ■ タイム スタンプ（%d{yyyy-MM-dd hh:mm:ss,SSS z} :） ■ スレッド ID （[%t] :） ■ ログ レベル（または重大度） （%-5p :） ■ ロガー クラス（%-5c{3} :） ■ メッセージ（%m%n） このパターンは C 言語の printf 関数に似ています。

プロパティ ファイル

webfort.authentication.properties

webfort.authentication.properties ファイルは、認証 Java SDK が AuthMinder サーバ情報を読み取るためのパラメータを提供します。 以下の表に、設定パラメータを示します。

デフォルトでは、設定パラメータには、**.1** が追加されます。これは、それらの設定がプライマリ AuthMinder サーバ用であることを示します。AuthMinder サーバのインスタンスが複数あり、フェイルオーバを有効にする場合、サポートするサーバの数に基づいてセクションを複製し、それに応じてパラメータを設定します。

パラメータ	デフォルト	説明
pool.maxActive	64	SDK から AuthMinder サーバへの、プール内に許容される接続の最大数。
pool.maxIdle	16	SDK から AuthMinder サーバへの、プール内に許容されるアイドル接続の最大数。
pool.maxWaitTimeMillis	-1	リクエストが接続まで待機する最大時間（ミリ秒単位）。デフォルトの -1 は、スレッドが無限に待機することを示します。

パラメータ	デフォルト	説明
pool.minEvictableIdleTimeMillis	-1	接続がアイドル接続エビクター(ある場合)によって削除されるまでの、プール内で接続がアイドルになる可能性のある最小時間。
pool.timeBetweenEvictionRunsMillis	-1	プールをチェックしてアイドル接続を削除するまでの待機時間（ミリ秒）。
authentication.host.*n*	localhost	AuthMinder サーバのホスト名または IP アドレス。
authentication.port.*n*	9742	Authentication Native プロトコル用に設定されたポート番号。
authentication.transport.*n*	tcp	AuthMinder 認証 SDK と AuthMinder サーバ間の SSL 通信を有効にするには、このパラメータを 1SSL または 2SSL に設定します。 **注**: トランスポート モードを SSL に変更する場合は、AuthMinder サーバを再起動してください。
authentication.connectionTimeout.*n*	10000	AuthMinder サーバが到達できないと考えられるまでの最大時間（ミリ秒）。
authentication.readTimeout.*n*	30000	AuthMinder サーバからのレスポンスに許容される最大時間（ミリ秒）。
authentication.serverCACertPEMPath.*n*	デフォルト値なし	サーバの CA 証明書ファイルのパスを提供します。このファイルは PEM 形式である*必要があります*。 ファイルの完全パスを入力します。 以下に例を示します。 server.CACertPEMPath=<*%SystemDrive%*>/certs/webfort_ca.pem
authentication.clientCertKeyP12Path.*n*	デフォルト値なし	p12 形式のクライアント証明書のパスを提供します。
authentication.clientCertKeyPassword.*n*	デフォルト値なし	p12 ファイルを開くためのクライアント鍵ペア パスワードを入力します。

webfort.issuance.properties

webfort.issuance.properties ファイルは、発行 Java SDK が AuthMinder サーバ情報を読み取るためのパラメータを提供します。 以下の表に、設定パラメータを示します。

デフォルトでは、設定パラメータには、**.1** が追加されます。これは、設定がプライマリ AuthMinder サーバ用であることを示します。 AuthMinder サーバのインスタンスが複数あり、フェイルオーバを有効にする場合、サポートするサーバの数に基づいてセクションを複製し、それに応じてパラメータを設定します。

パラメータ	デフォルト	説明
pool.maxActive	64	SDK から AuthMinder サーバへの、プール内に許容される接続の最大数。
pool.maxIdle	16	SDK から AuthMinder サーバへの、プール内に許容されるアイドル接続の最大数。
pool.maxWaitTimeMillis	-1	リクエストが接続まで待機する最大時間（ミリ秒単位）。 デフォルトの -1 は、スレッドが無限に待機することを示します。
pool.minEvictableIdleTimeMillis	-1	接続がアイドル接続エビクター（ある場合）によって削除されるまでの、プール内で接続がアイドルになる可能性のある最小時間。
pool.timeBetweenEvictionRunsMillis	-1	プールをチェックしてアイドル接続を削除するまでの待機時間（ミリ秒）。
issuance.host.*n*	localhost	AuthMinder サーバのホスト名または IP アドレス。
issuance.port.*n*	9744	Transaction Web Service プロトコル用に設定されたポート番号。
issuance.transport.*n*	tcp	AuthMinder 発行 SDK と AuthMinder サーバ間の SSL 通信を有効にするには、このパラメータを 1SSL または 2SSL に設定します。 **注**: トランスポート モードを SSL に変更する場合は、AuthMinder サーバを再起動してください。
issuance.connectionTimeout.*n*	10000	AuthMinder サーバが到達できないと考えられるまでの最大時間（ミリ秒）。

パラメータ	デフォルト	説明
issuance.readTimeout.*n*	30000	AuthMinder サーバからのレスポンスに許容される最大時間（ミリ秒）。
issuance.serverCACertPEMPath.*n*	デフォルト値なし	サーバの CA 証明書ファイルのパスを提供します。 このファイルは PEM 形式である*必要があります*。 ファイルの完全パスを入力します。 以下に例を示します。 server.CACertPEMPath=<*%SystemDrive%*>/certs/webfort_ca.pem
issuance.clientCertKeyP12Path.*n*	デフォルト値なし	p12 形式のクライアント証明書のパスを提供します。
issuance.clientCertKeyPassword.*n*	デフォルト値なし	p12 ファイルを開くためのクライアント鍵ペアパスワードを入力します。

付録 K: HSM 設定の変更

この付録では、インストール時に指定したハードウェア セキュリティ モジュール（HSM）の設定を変更する場合に実行する必要がある手順を示します。

注: このセクションで説明されている設定を行う前に、HSM サーバおよびクライアントをセットアップしていて、HSM 内に 3DES キーを生成していることを確認します。 詳細については、「（オプション、HSM を使用している場合のみ） HSM の要件」を参照してください。

「ハードウェア セキュリティ モジュール（HSM）の要件」で説明されているように、AuthMinder はデータを保護するためにハードウェア セキュリティ モジュール（HSM）をサポートするようになりました。 HSM を使用してデータを暗号化する場合、データベースに保存されているデータは HSM にあるキーを使用して暗号化されます。

AuthMinder はハードウェアを使用したデータの暗号化のために、Luna および nCipher netHSM をサポートしています。 HSM の設定は arcotcommon.ini ファイルで行うことができます。 このファイルには、必要な HSM を設定するための個別のセクションがあります。現在のリリースでは以下のとおりです。

- Luna HSM （[crypto/pkcs11modules/chrysalis]）
- nCipher netHSM （[crypto/pkcs11modules/nfast]）

設定している HSM に基づいて、対応するセクションで sharedLibrary パラメータを指定します。 HSM 情報を指定したら、HSM キー ラベルを使用して securestore.enc ファイルを再作成し、HSM を初期化して、HSM キーを使用するように AuthMinder を初期化します。

AuthMinder が必要とする HSM 情報を変更する方法

1. 以下の場所に移動します。
   `<install_location>/arcot/conf`
2. securestore.enc ファイルのバックアップをとります。
3. <*install_location*>/arcot/conf から既存の securestore.enc ファイルを削除します。

4. AuthMinder が必要とする HSM 情報を変更する方法
   a. 以下の場所に移動します。
   <*install_location*>/arcot/conf
   b. テキスト エディタで arcotcommon.ini を開きます。
   c. [arcot/crypto/device] セクションの HSMDevice パラメータが使用する HSM に設定されていることを確認します。
      - Luna HSM の場合は chrysalis。

      または

      - nCipher netHSM の場合は nfast。
   d. 設定する HSM に応じて、sharedLibrary パラメータを HSM ライブラリ ファイルがある場所に設定します。

      Luna （libCryptoki2.so）および nCipher netHSM （libcknfast.so）の場合は、ファイルの絶対パスとフル ネームを入力します。

      注: このセクションで使用可能なその他の HSM 設定パラメータの詳細については、「arcotcommon.ini (P. 437)」を参照してください。
   e. arcotcommon.ini ファイルを保存して閉じます。
5. DBUtil ツールがある以下の場所に移動します。
   <*install_location*>/arcot/tools/<*platform_name*>
6. 以下のコマンドを使用して DBUtil ツールを実行します。
   a. dbutil -init *<HSM_key_label>*

      注: *<HSM_key_label>* は、HSM に存在する 3DES キーに対応します。

      上記のコマンドは指定したキー ラベルで securestore.enc ファイルを作成します。生成されたファイルは、*<install_location>*/arcot/conf に保存されます。
   b. dbutil -i *<HSM_module_name>* *<HSM_password>*

      注: *<HSM_module_name>* は、 Luna HSM の場合は chrysalis、nCipher netHSM の場合は nfast です。

      上記のコマンドは HSM を初期化します。

c. dbutil -pi *<DSN_Name>* *<Database_password>* -h *<HSM_password>* -d *<HSM_module_name>*

   注: *<DSN_NAME>* は、AuthMinder データベースに接続するために AuthMinder サーバが使用する ODBC DSN を指します。 *<Database_password>* は、データベースに接続するために使用されるパスワードを指します。

   上記のコマンドは、HSM を使用して暗号化されるように AuthMinder サーバ データを初期化します。

d. dbutil -pi *<Database_Username>* *<Database_password>* -h *<HSM_password>* -d *<HSM_module_name>*

   注: *<Database_Username>* は、AuthMinder データベースに接続するために使用されるユーザ名を指します。 データベース ユーザ名は大文字と小文字が区別されるため、正しい値を入力する必要があります。 *<Database_password>* は、データベースに接続するために使用されるパスワードを指します。

   上記のコマンドは、HSM を使用して暗号化されるように、管理コンソールおよびユーザ データ サービス データを初期化します。

付録 L: データベース リファレンス

AuthMinder データベースには多くのテーブルが含まれます。テーブルの中には、多く使うほど拡大するものがあります。 ユーザ数に直接比例して肥大化するテーブルもあれば、製品の使用に直接比例して肥大化するテーブルもあります。 また、ユーザがシステムに複数回アクセスすることによってもテーブルは拡大します。 ディスク容量には制限があるので、AuthMinder の展開を管理しているデータベース管理者にとって、テーブルが無制限に拡大するのは望ましいことではありません。 この付録では、一部のテーブルを削除することで、ディスク容量を管理し、データベース パフォーマンスを向上させる方法について説明します。

削除するテーブルは、監査ログ情報など、トランザクションの詳細が含まれるテーブルに限定します。 ユーザの認証に必要なユーザ情報が含まれるテーブルは削除 *しないでください*。

注: 設定およびデータのレポートの必要性に応じて、SQL データベースに適切な調整を行うことをお勧めします。 たとえば、大量のデータを削除すると、削除処理中のパフォーマンスに悪影響が生じます。 ロールバック セグメントのサイズによっては、システムが停止してしまう可能性すらあります。 また、古いレコードはアーカイブし、完全には削除しないことをお勧めします。

この付録では、以下のトピックについて説明します。

AuthMinder データベースのテーブル

このセクションでは、すべてのデータベース テーブルについて簡単に説明します。

AuthMinder によって使用されるデータベース テーブル

以下の表に、AuthMinder サーバによって使用されるデータベース テーブルを示します。

テーブル名	説明
ARWFADMINAUDITLOG	AuthMinder 管理アクティビティの監査ログ情報が含まれています。
ARWFARCOTEMV	ユーザの ArcotID OTP-EMV 認証情報が含まれています。これには、各ユーザの個人エントリが含まれています。
ARWFARCOTEMVHISTORY	*再発行*状態のすべての ArcotID OTP-EMV 認証情報が含まれています。
ARWFARCOTID	ユーザの ArcotID PKI 認証情報が含まれています。 これには、各ユーザの個人エントリが含まれています。
ARWFARCOTIDHISTORY	*再発行*状態のすべての ArcotID PKI が含まれています。
ARWFARCOTOTP	ユーザの ArcotID OTP-OATH 認証情報が含まれています。これには、各ユーザの個人エントリが含まれています。
ARWFARCOTOTPHISTORY	*再発行*状態のすべての ArcotID OTP-OATH 認証情報が含まれています。
ARWFAUTHAUDITLOG	認証アクティビティの監査ログ情報が含まれています。
ARWFAUTHTOKENS	正常な認証の後に生成される認証トークンが含まれています。 リクエストされたトークン タイプとは無関係に、それぞれの正常な認証に対し 1 つのエントリがこのテーブル内に作成されます。

テーブル名	説明
ARWFCONFIG	AuthMinder 設定情報が含まれています。 このテーブルの情報にはバージョン情報が含まれているため、設定ごとに複数のエントリがあります。
ARWFDBERRORCODES	通信失敗を示すデータベース エラー コードが含まれています。
ARWFDBQUERIES	AuthMinder サーバによって使用されるデータベース クエリのリストが含まれています。
ARWFDISPLAYNAMES	AuthMinder で使用されるさまざまなキーの名前および値が含まれています。
ARWFGENERICCRED	ユーザのその他のクレデンシャルに関する情報が含まれています。 たとえば、カスタム API によってサポートされるクレデンシャルなどです。
ARWFGENERICCREDHISTORY	*再発行*状態のその他のすべての（サポートされている API など）クレデンシャルが含まれています。
ARWFINSTANCES	特定のデータベースと通信する AuthMinder サーバのすべてのインスタンスに関する情報が含まれています。
ARWFISSUANCEAUDITLOG	クレデンシャル発行アクティビティの監査ログ情報が含まれています。
ARWFMESSAGES	AuthMinder サーバによって送信されるメッセージが含まれています。
ARWFMODULEREGISTRY	AuthMinder サーバの内部モジュールおよびプラグインに関する情報が含まれています。
ARWFOATH	ユーザの OATH ワンタイム パスワード（OTP）認証情報が含まれています。 これには、各ユーザの個人エントリが含まれています。
ARWFOATHHISTORY	*再発行*状態のすべての OATH OTP クレデンシャルが含まれています。
ARWFOATHTOKENREGISTRY	シード値、トークン ID、およびトークン タイプなどの OATH トークン詳細が含まれています。
ARWFORGACTIVECONFIG	現在アクティブな組織の設定マッピングが含まれています。 このテーブルの情報にはバージョン情報が含まれているため、設定ごとに複数のエントリがあります。

テーブル名	説明
ARWFORGCONFIG	組織ごとの設定マッピングが含まれています。 このテーブルの情報にはバージョン情報が含まれているため、設定ごとに複数のエントリがあります。
ARWFOTP	ユーザのワンタイム パスワード（OTP）クレデンシャルが含まれています。 これには、各ユーザの個人エントリが含まれています。
ARWFPASSWORD	ユーザのユーザ名/パスワード クレデンシャルが含まれています。 これには、各ユーザの個人エントリが含まれています。
ARWFPASSWORDHISTORY	*再発行*状態のすべての user-name パスワード クレデンシャルが含まれています。
ARWFPROTOCOLCONFIGURATION	AuthMinder サーバの各リスナ ポートの設定が含まれています。
ARWFQNA	ユーザの質問と回答（Q&A）クレデンシャルが含まれています。 これには、各ユーザの個人エントリが含まれています。
ARWFQNAHISTORY	*再発行*状態のすべての質問と回答クレデンシャルが含まれています。
ARWFSEQUENCE	バージョン設定に使用されるシーケンスに関する情報が含まれています。
ARWFSSLTRUSTSTORE	AuthMinder サーバによって信頼される SSL ルート証明書が含まれています。
ARWFSVRMGMTAUDITLOG	サーバ管理アクティビティの監査ログ情報が含まれています。
ARWFUNIQUEFIELDS	設定内の特定のフィールドの一意性を適用します。 たとえば、RADIUS クライアントの IP アドレスは 2 つの組織で使用することはできません。
ARWFVERIFIEDCHALLENGES	ArcotID PKI 署名が正常に検証されるチャレンジに関する情報が含まれています。 チャレンジ用の No Replay がオンになった場合、正常な ArcotID PKI 認証用にエントリが作成されます。 デフォルトでは、このオプションはオフになっています。

管理コンソールによって使用されるデータベース テーブル

以下の表に、管理コンソールによって使用されるすべてのデータベース テーブルを示します。

テーブル名	説明
ARADMINAUDITTRAIL	管理者アクティビティ監査が格納されます。
ARADMINAUTHTOKEN	管理コンソールがプラグ可能な認証に使用するトークンが格納されます。 ユーザがパスワードを使用してコンソールにログインするたびに、パスワードが一致し、このテーブルに格納された後、トークンが内部的に生成されます。
ARADMINBASICAUTHPWDHISTORY	管理者用の基本認証を使用して管理コンソールにログインする、すべての組織のすべての管理者の最後の *n* 個のパスワードが格納されます。 この情報はパスワードの再利用を防ぐために格納されます。
ARADMINBASICAUTHUSER	管理者用の基本認証を使用して管理コンソールにログインする、すべての組織のすべての管理者の基本認証の認証情報が格納されます。
ARADMINCONFIG	管理コンソールの設定が格納されます。
ARADMINCUSTOMROLE	すべてのカスタム定義ロールの設定が格納されます。
ARADMINMANAGEROLE	指定したロールが管理できるロールのリストが格納されます。
ARADMINMAP	キーと値のペアとして入力される、AuthMinder サーバ インスタンスの情報が格納されます。
ARADMINPAFCONFIG	システム内のすべての組織のすべての管理者の認証設定が格納されます。
ARADMINPREDEFINEDROLE	すべてのサポートされている管理者のロール情報が格納されます。
ARADMINPWDPOLICY	すべての組織のすべての管理者のパスワード ポリシーの詳細が格納されます。
ARADMINROLEPRIVILEGE	Administration Console によってサポートされるすべての管理アクション（またはタスク）、各タスクのスコープ、およびタスクを実行できるロールの間のマッピングが格納されます。

テーブル名	説明
ARADMINSCOPE	各管理者が管理権（スコープ）を持つ組織のリストが格納されます。
ARADMINSCOPEALL	システム内にある既存のすべての組織に対して管理権（スコープ）を持つすべての管理者のリストが格納されます。
ARADMINSUPPORTEDAUTHMECH	管理コンソールにログインするためにサポートされているすべての認証メカニズムに関する情報が格納されます。
ARADMINSUPPORTEDTIMEZONE	すべての使用可能なタイム ゾーンのリストが格納されます。 **注**: これは内部テーブルです。
ARADMINTURNEDOFFPRIVILEGE	特定のカスタム ロールで使用できない権限のリストが格納されます。
ARADMINTXID	各トランザクションの一意の ID を生成するために必要な情報が格納されます。
ARADMINUITAB	使用可能なタブに関する情報と、それらのタブを管理コンソールで使用できる順序に関する情報が格納されます。
ARADMINUITASK	使用可能なすべてのタスクに関する情報と、それらのタスクを管理コンソールで使用できる順序に関する情報が格納されます。
ARADMINUITASKATTRIBUTES	管理コンソールの第 1 階層および第 2 階層のタブがクリックされると表示されるタスクの詳細が格納されます。 これらのタスクはランディング ページと呼ばれます。
ARADMINUITASKCONTAINER	使用可能なタスク コンテナに関連する情報が格納されます。タスク コンテナは、Administration Console 内の第 2 レベル タブ ID またはタスク グループのいずれかです。
ARADMINUSER	既存のすべての管理者に関する詳細情報（所属先の組織、現在のステータス、タイム ゾーン、ロケール、最終ログイン時間など）が格納されます。
ARADMINUSER_ARCHIVE	削除されたすべてのユーザに関する情報が格納されます。

テーブル名	説明
ARADMINWIZARDTASK	ブートストラップ ウィザードを使用して実行可能なすべてのタスクに関する情報が格納されます。
ARCMNBULKOPERATION	ユーザのアップロードやユーザ アカウントのアップロードを含む、サポートされているすべてのバルク操作に関する情報が格納されます。
ARCMNBULKOPERATIONATTRIBUTE	ARCMNBULKOPERATION テーブル内のすべてのバルク操作の属性が格納されます。
ARCMNBULKREQUEST	各バルク アップロード リクエストの詳細（組織名、リクエスト ID、リクエストのステータス、アップロードされたデータ、および操作など）が格納されます。
ARCMNBULKTASKPARAM	システムでサポートされている各タスクの各属性の名前と値が格納されます。
ARCMNBULKUPLOADTASK	すべてのバルク アップロード リクエストの各タスクのステータスが格納されます。
ARCMNCACHEREFRESH	管理コンソールをリフレッシュする必要があるかどうかを示すキャッシュ関連のハウスキーピング情報が格納されます。
ARCMNCONFIG	管理コンソールの共通の設定情報が格納されます。 ブートストラップが完了しているかどうか、キャッシュ リフレッシュは自動か手動か、属性の暗号化が有効になっているかどうか、バルク アップロード機能が有効になっているかどうかなどの設定情報が含まれます。
ARCMNDBERRORCODES	データベースがダウンしているか、応答していないことを示す、ベンダー固有のデータベース エラー コードおよび SQL 状態値が格納されます。 バックアップ データベースが設定されている場合、データベースをフェイルオーバーするべきかどうかを判断するために、この情報がシステムによって使用されます。
ARCMNMAPDATATYPE	コンソールのページを表示するために管理コンソールが使用する CA 製品固有の情報が格納されます。
ARCMNKEY	組織の作成または更新時に使用される重要な設定が格納されます。
ARPFCMNCACHEREFRESHEVENT	システム内のすべてのインスタンスのすべてのキャッシュ リフレッシュ イベントの詳細が格納されます。

テーブル名	説明
ARPFCMNCACHEREFRESHSCOPE	サーバ キャッシュ リフレッシュ イベントが発生した場合に影響を受けるすべての組織に関する情報が格納されます。
ARPFCMNCACHEREFRESHSTATUS	トリガされたすべてのインスタンスに対する各キャッシュ リフレッシュ イベントのステータスが格納されます。
ARPFCMNINSTANCE	システムに設定されているすべての AuthMinder サーバ インスタンスの詳細情報が格納されます。 インスタンスが最後にリフレッシュされた時刻も含まれます。
ARPFCMNORGCONFIGDATA	各組織の設定の詳細が格納されます。 通常、組織レベルで優先可能なグローバル設定も含まれます。
ARPFCMNORGCONFIGSTATE	ARPFCMNORGCONFIGDATA テーブルの割り当て済みの各設定のステータスが格納されます。
ARPFCMNPRIVILEGEMAPPING	管理コンソールから使用可能な各権限の詳細が格納されます。
ARREPORTTABLES	管理コンソールを使用して生成されるレポートに関する情報が格納されます。
ARSEQUENCETABLE	ストアド プロシージャを使用して、シーケンスをシミュレートします。 **注**: このテーブルは MS SQL Server でのみ使用されます。

ユーザ データ サービスによって使用されるデータベース テーブル

以下の表に、UDS によって使用されるデータベース テーブルを示します。

テーブル名	説明
ARUDSACCOUNTTYPE	システムに設定されているすべてのアカウント タイプの詳細が格納されます。
ARUDSATTRMAP	各組織に固有のアカウントのカスタム属性のフィールド名を表す設定の詳細が格納されます。
ARUDSAUTHSESSION	現在アクティブなセッションの認証セッションの詳細が格納されます。このテーブルが複製されないと、アクティブな認証セッションは失われる可能性があります。

テーブル名	説明
ARUDSCALLOUT	ユーザ固有のコールアウト設定が格納されます。 これらのコールアウトは、ユーザの作成や更新などの特定のイベントに対して呼び出されます（設定されている場合）。
ARUDSCALLOUTINTERNAL	カスケード効果のある削除イベントがトリガまたは有効にされた場合のコールアウトに関する設定情報（呼び出される SDK メソッド）が格納されます。
ARUDSCALLOUTINTERNALPARAMS	内部コールアウトに固有のパラメータやタイプなどの詳細が格納されます。
ARUDSCALLOUTPARAM	外部コールアウトに固有のパラメータやタイプなどの詳細が格納されます。
ARUDSCONFIG	UDS 設定パラメータおよびその値が格納されます。
ARUDSCONFIGAUDITLOG	ユーザ データ ソース（UDS）の操作およびそのリターン ステータスの監査ログ情報が格納されます。
ARUDSCONTACTTYPE	組織またはグローバル レベルで設定可能な追加の連絡先情報（予備の電子メールや電話番号など）が格納されます。
ARUDSCUSTOMATTREXT	追加のユーザ アカウント カスタム属性が格納されます。 デフォルトでは、最大 10 個のユーザ アカウント カスタム属性が ARUDSUSERACCOUNT テーブルに格納されます。最初の 10 個以降の追加の属性はこのテーブルに格納されます。
ARUDSCUSTOMATTREXT_ARCHIVE	ユーザ アカウントが削除されたときに、ユーザ アカウント カスタム属性に関するアーカイブ情報が格納されます。
ARUDSLDAPREPOSITORYCONFIG	LDAP ホストやポートの詳細など、LDAP リポジトリの設定が格納されます。
ARUDSORGANIZATION	組織の定義、その属性、およびリポジトリの接続性の詳細が格納されます。
ARUDSORGANIZATIONAUDITLOG	組織固有の UDS 監査ログ情報の詳細が格納されます。

テーブル名	説明
ARUDSORGREPOATTRIBUTES	組織固有のリポジトリ マッピング情報が格納されます。 たとえば、ユーザ リポジトリとして LDAP を使用している場合、CA 属性（たとえば、FNAME）が対応する LDAP 属性（たとえば、GIVENNAME）にマップされている場合があります。
ARUDSORGSECUREATTRIBUTES	暗号化する必要がある組織固有の属性（PII フィールドなど）が格納されます。 **注**: これらの属性は管理コンソールを使用して設定されます。
ARUDSREPOCLONESTATUS	外部リポジトリ（LDAP など）から ARUDSREPOSITORYUSER テーブルにユーザ情報の一時クローニングのステータスが格納されます。
ARUDSREPOSITORYTYPES	UDS によってサポートされるすべてのリポジトリの定義が格納されます。
ARUDSREPOSITORYUSER	パフォーマンスを向上させるために、外部リポジトリ（LDAP など）からのユーザ情報が一時的に格納されます。 これは通常、外部リポジトリから多数のユーザのユーザ データを取得する必要がある場合に行われます。
ARUDSRESOURCESCOPE	リソースと組織間のマッピングが格納されます。 つまり、このテーブルは、どのリソースがどの組織に適用可能かを指定します。 たとえば、特定のアカウント タイプは特定の組織にのみ適用可能な場合があります。
ARUDSRESOURCESCOPEALL	リソースと組織間のマッピングが格納されます。ただし、すべての組織に適用可能なリソースを指定するので、ARUDSRESOURCESCOPE テーブルとは異なります。
ARUDSSECUREATTRIBUTES	暗号化する必要がある属性（PII フィールドなど）に関する情報が格納されます。 **注**: これらの属性は管理コンソールを使用して設定されます。
ARUDSUSER	組織に所属するすべてのユーザの詳細と属性が格納されます。
ARUDSUSER_ARCHIVE	システムから削除されたすべてのユーザ アカウントのユーザの詳細が格納されます。
ARUDSUSERACCOUNT	特定のユーザのユーザ アカウント情報が格納されます。

テーブル名	説明
ARUDSUSERACCOUNT_ARCHIVE	システムから削除されたすべてのユーザ アカウントのユーザ アカウント情報が格納されます。
ARUDSUSERATTRIBUTE	すべてのユーザ属性の定義が格納されます。 個々の製品によって、新規ユーザ属性が追加される場合のみ、このテーブルを変更することをお勧めします。
ARUDSUSERAUDITLOG	ユーザ操作固有の詳細な監査ログ情報が格納されます。
ARUDSUSERCONTACT	ユーザの予備の連絡先情報（電子メールや電話番号など）が格納されます。
ARUDSUSERCONTACT_ARCHIVE	システムから削除されたユーザ アカウントの予備の連絡先情報（電子メールや電話番号など）が格納されます。

データベース サイズの計算

このセクションを使用して、データベース管理者は AuthMinder 用に設定する必要があるデータベースのおおよそのサイズを計算できます。

サンプル計算で使用される記号

以下の記号が計算で使用されます。

- ユーザ数 = *N*
- 1 日あたりのトランザクションの平均数 = *T*
- 処理時間枠（日単位） = *D*

前提値

計算用に以下の前提が定義されています。

- ユーザ数（**N**） = 1,000,000 （100 万）
- 1 日あたりのトランザクションの平均数（**T**） =24,000
- 処理時間枠（**D**） = 90 日

前提に基づいたサンプル計算

「前提値 (P. 469)」で前提となる数字を考慮すると、最終的な要件は以下のようになります。

- **ユーザの総数**を基にした要件： データベース サイズ = （21 * *N*） KB
- **日常のアクティビティ**を基にした要件： データベース サイズ = （*T* * *D* * 5） KB

データベース テーブルの複製に関するアドバイス

このセクションでは、プライマリ データベースとバックアップ データベースの間でテーブルをどれくらいの頻度で複製する必要があるのかについて説明します。 この章では、以下の内容について説明します。

- リアルタイム同期が必要なテーブル（P. 470）
- 定期的な同期が必要なテーブル（P. 472）
- 同期が必要ないテーブル（P. 474）

リアルタイム同期が必要なテーブル

以下の表に、プライマリ データベースとバックアップ データベース間のリアルタイム同期が必要なデータベース テーブルを示します。 このカテゴリには、主にユーザ関連情報が含まれるテーブルが含まれており、このデータは認証に必要です。そのため、これらのテーブルのリアルタイム同期を実行する必要があります。

AuthMinder コンポーネント	テーブル
管理コンソール	ARADMINAUDITTRAIL
	ARADMINBASICAUTHUSER
	ARADMINSCOPE
	ARADMINSCOPEALL
	ARADMINUSER
	ARADMINTXID
	ARPFCMNINSTANCE
	ARSEQUENCETABLE

AuthMinder コンポーネント	テーブル
ユーザ データ サービス	ARUDSORGANIZATION
	ARUDSORGREPOATTRIBUTES
	ARUDSORGSECUREATTRIBUTES
	ARUDSLDAPREPOSITORYCONFIG
	ARUDSACCOUNTTYPE
	ARUDSRESOURCESCOPE
	ARUDSRESOURCESCOPEALL
	ARUDSATTRMAP
	ARUDSCONTACTTYPE
	ARUDSUSER
	ARUDSUSERACCOUNT
	ARUDSCUSTOMATTREXT
	ARUDSAUTHSESSION
	ARUDSUSERCONTACT
	ARUDSREPOSITORYUSER
WebFort サーバ	ARWFARCOTEMV
	ARWFARCOTID
	ARWFARCOTOTP
	ARWFAUTHTOKENS
	ARWFINSTANCES
	ARWFGENERICCRED
	ARWFOATH
	ARWFOTP
	ARWFQNA
	ARWFPASSWORD
	ARWFVERIFIEDCHALLENGES

定期的な同期が必要なテーブル

以下の表に、プライマリ データベースとバックアップ データベース間の定期的な同期が必要なデータベース テーブルを示します。 設定に変更があった場合、これらのデータベース テーブルは同期化されます。

コンポーネント	テーブル
管理コンソール	ARADMINCONFIG
	ARADMINCUSTOMROLE
	ARADMINMAP
	ARADMINPAFCONFIG
	ARADMINPWDPOLICY
	ARADMINBASICAUTHPWDHISTORY
	ARADMINTURNEDOFFPRIVILEGE
	ARADMINCACHEREFRESH
	ARADMINAUDITTRAIL
	ARADMINUSER_ARCHIVE
	ARADMINMANAGEROLE
	ARADMINROLEPRIVILEGE
	ARPFCMNORGCONFIGDATA
	ARPFCMNORGCONFIGSTATE
	ARPFCMNCACHEREFRESHSTATUS
	ARPFCMNCACHEREFRESHEVENT
	ARPFCMNCACHEREFRESHSCOPE
	ARCMNBULKTASKPARAM
	ARCMNBULKUPLOADTASK
	ARCMNBULKREQUEST
	ARCMNBULKOPERATIONATTRIBUTE
	ARCMNBULKOPERATION

コンポーネント	テーブル
UDS	ARUDSUSERAUDITLOG
	ARUDSORGANIZATIONAUDITLOG
	ARUDSCONFIGAUDITLOG
	ARUDSCONFIG
	ARUDSREPOSITORYTYPES
	ARUDSUSERATTRIBUTE
	ARUDSUSERACCOUNT_ARCHIVE
	ARUDSCUSTOMATTREXT_ARCHIVE
	ARUDSUSER_ARCHIVE
	ARUDSUSERCONTACT_ARCHIVE
	ARCMNCONFIG
	ARUDSREPOCLONESTATUS
	ARUDSCALLOUTINTERNAL
	ARUDSCALLOUTINTERNALPARAMS
	ARUDSCALLOUT
	ARUDSCALLOUTPARAM
WebFort	ARWFADMINAUDITLOG
	ARWFARCOTEMVHISTORY
	ARWFARCOTIDHISTORY
	ARWFARCOTOTPHISTORY
	ARWFAUTHAUDITLOG
	ARWFCONFIG
	ARWFGENERICCREDHISTORY
	ARWFISSUANCEAUDITLOG
	ARWFMODULEREGISTRY
	ARWFOATHHISTORY

コンポーネント	テーブル
	ARWFOATHTOKENREGISTRY
	ARWFORGACTIVECONFIG
	ARWFORGCONFIG
	ARWFPASSWORDHISTORY
	ARWFPROTOCOLCONFIGURATION
	ARWFQNAHISTORY
	ARWFSEQUENCE
	ARWFSSLTRUSTSTORE
	ARWFSVRMGMTAUDITLOG
	ARWFUNIQUEFIELDS

同期が必要ないテーブル

以下の表に、プライマリ データベースとバックアップ データベース間の同期が必要ないデータベース テーブルを示します。

コンポーネント	テーブル
管理コンソール	ARCMNDBERRORCODES
	ARADMINAUTHTOKEN
	ARADMINMANAGEROLE
	ARADMINPREDEFINEDROLE
	ARADMINSUPPORTEDAUTHMECH
	ARADMINSUPPORTEDTIMEZONE
	ARADMINUITAB
	ARADMINUITASK
	ARADMINUITASKATTRIBUTES
	ARADMINUITASKCONTAINER
	ARADMINWIZARDTASK
	ARCMNMAPDATATYPE
	ARCMNCACHEREFRESH

コンポーネント	テーブル
	ARPFCMNPRIVILEGEMAPPING
	ARREPORTTABLES
ユーザ データ サービス	ARUDSSECUREATTRIBUTES
WebFort	ARWFDBERRORCODES
	ARWFDBQUERIES
	ARWFDISPLAYNAMES
	ARWFMESSAGES

データベース調整パラメータ

以下の表に、AuthMinder サーバとデータベース間の接続を調整するために使用できる共通パラメータを示します。 これらの設定は Administration Console の［インスタンス管理］画面を使用して定義されます。

フィールド	説明
最小接続数	サーバの起動時に、AuthMinder サーバとデータベースとの間で作成される接続の最小数を入力します。
最大接続数	AuthMinder サーバとデータベースとの間で作成可能な接続の最大数を入力します。 **注**: この値は、MaxConnections パラメータより優先されるため、データベースがサポートする最大接続数に応じてこの値を設定する必要があります。 詳細については、データベース ベンダーのマニュアルを参照してください。
接続数の増分	接続の追加が必要になった場合に、既存の接続に対して一度に追加する接続の数を入力します。 **重要**: 接続の総数は、接続の最大数を超えることはできません。
スレッド モニタ スリープ時間 (秒)	モニタリング スレッドがすべてのデータベースに対して継続してハートビート チェックを行う間隔を入力します。

フィールド	説明
障害状態でのスレッド モニタ スリープ時間 (秒)	データベース接続に障害が発生した場合に、データベース モニタ スレッドが接続プールの健全性をチェックする間隔を入力します。
クエリ詳細のログ	すべてのデータベース クエリの詳細をログ記録する場合は、このチェック ボックスをオンにします。
データベース接続のモニタ	データベース モニタ スレッドで、プールを事前にチェックするには、このチェック ボックスをオンにします。
自動的にプライマリに戻る	フェールオーバ条件後にプライマリ データベースが再度利用可能になった場合に、サーバがバックアップ データベースからプライマリ データベースに切り替わるようにするには、このチェック ボックスをオンにします。