Arcot WebFort®
管理ガイド
バージョン 6.2

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot WebFort 管理ガイド
バージョン 6.2
2010 年 5 月
部品番号：WF-0062-00AG-10

商標

特許

Arcot Systems, Inc., 455 West Maude Avenue, Sunnyvale, CA 94085

サードパーティ ソフトウェア

Arcot WebFort および関連コンポーネントで使用されているサードパーティ製ソフトウェアの一覧については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の付録「サードパーティ製ソフトウェアのライセンス」を参照してください。

目次

序文 ix
対象読者 ix
このガイドの内容 ix
関連するドキュメント x
表記規則および形式 x
サポートへのお問い合わせ xii
第 1 章
Administration Console の概要 1
Administration Console について 1
Administration Console の要素 2
サポートされるロール 5
ユーザ 6
デフォルトの管理ロール 6
管理ロールのスコープ 7
Master Administrator 8
Global Administrator 9
Organization Administrator 10
User Administrator 10
管理権限の要約 11
カスタム ロール 15
次の手順 16
単純な展開 16
カスタム展開 18
第 2 章
はじめに 21
Administration Console へのアクセス 21
Administration Console 設定の構成 23
UDS 設定の指定 23
組織のグローバル設定の指定 28

キャッシュ リフレッシュ設定の指定 31
基本認証設定の指定 32
基本認証パスワードの指定 32
プロファイル情報の変更 34
第 3 章
WebFort サーバ インスタンスの管理 37
WebFort Connectivity の設定 38
サーバ インスタンスのセットアップ 41
インスタンスのリフレッシュまたはシャットダウン 43
サーバ インスタンスの再起動 44
インスタンス名の変更 44
WebFort サーバ ログ記録設定の管理 45
データベース パラメータの設定 47
接続統計ログ記録の有効化 48
インスタンス タイム スタンプの詳細の読み取り 49
信頼されるストアの作成 50
通信プロトコルの設定 51
インスタンス統計のモニタリング 56
データベース接続性 58
サーバ プロトコル 59
ユーザ データ サービス接続性 60
プラグインの登録と更新 61
プラグインの登録 62
プラグイン設定の更新 64
その他の設定 64
カスタム ロールの操作 67
カスタム ロールの作成 67
カスタム ロール情報の更新 69
カスタム ロールの削除 71
第 4 章
グローバルな WebFort 設定の管理 73
WebFort プロファイルおよびポリシーの理解 74
クレデンシャル プロファイル 74
認証ポリシー 75
Global Administrator としてのログイン 75

WebFort ユーザ名 - パスワードの使用 75
パスワードを忘れた場合 78
基本ユーザ名 - パスワードの使用 81
Administration Console のログアウト 83
Administration Console 使用時のセキュリティに関する推奨事項 83
ArcotID の設定 84
ArcotID クレデンシャル プロファイルの設定 84
ArcotID 認証ポリシーの設定 88
Q&A の設定 91
Q&A 発行プロファイルの設定 91
Q&A 認証ポリシーの設定 95
ユーザ名 - パスワードの設定 99
ユーザ名 - パスワード発行プロファイルの設定 99
ユーザ名 - パスワード認証ポリシーの設定 104
OTP の設定 107
OTP 発行プロファイルの設定 107
OTP 認証ポリシーの設定 111
OATH OTP 設定の設定 114
OATH OTP 発行プロファイルの設定 114
OATH OTP 認証ポリシーの設定 117
ArcotOTP の設定 121
ArcotOTP 発行プロファイルの設定 121
ArcotOTP 認証ポリシーの設定 124
デフォルト設定の割り当て 128
RADIUS クライアントの設定 130
RADIUS クライアントの設定 131
RADIUS クライアントの更新および削除 133
RADIUS クライアントの更新 133
RADIUS クライアントの削除 134

第 5 章
組織の管理 135

組織の作成とアクティブ化 135
Arcot リポジトリでの組織の作成 136
LDAP リポジトリでの組織の作成 141
組織の検索 147

組織固有の設定の管理 149
SAML トークンの設定 152
ASSP の設定 155
コールアウトの設定 158
プラグインの設定 161
イベントの関連付け 163
組織情報の更新 165
組織情報の更新 165
WebFort 固有の設定の更新 167
組織の無効化 168
組織の有効化 169
初期状態の組織のアクティブ化 170
組織の削除 171
第 6 章
管理者の管理 175
管理者の作成 176
管理者の作成に必要な権限 176
WebFort のユーザ名 - パスワード クレデンシャルを使ったアカウントの作成 176
基本ユーザ名 - パスワード クレデンシャルを使ったアカウントの作成 180
管理者アカウントのプロファイル情報の変更 182
WebFort のユーザ名 - パスワード クレデンシャルを使ったアカウントの場合 182
基本ユーザ名 - パスワード クレデンシャルを使ったアカウントの場合 184
管理者の検索 186
管理者アカウント情報の更新 189
アクティベーション コードの再生成 193
管理者のクレデンシャルの更新 196
管理者アカウントの無効化 198
管理者アカウントの有効化 199
管理者アカウントの削除 201
第 7 章
ユーザの管理 203
ユーザの検索 204
ユーザ情報の更新 206
ユーザを管理者レベルに上げる 209
ユーザ クレデンシャル情報の更新 211

ユーザ アカウントの無効化 215
ユーザ アカウントの有効化 216
ユーザ アカウントの削除 217
第 8 章
レポートの管理 219
Master Administrator レポート 219
管理者レポート 220
My Activity Report 220
Administrator Activity Report 221
Organization Report 222
WebFort レポート 222
Server Management Activity Report 222
Global Administrator レポート 224
管理者レポート 224
My Activity Report 224
Administrator Activity Report 224
Organization Report 225
ユーザ アクティビティ レポート 225
WebFort レポート 225
Authentication Activity Report 225
Credential Management Activity Report 227
Configuration Management Report 228
Organization Administrator レポート 230
管理者レポート 230
My Activity Report 230
Administrator Activity Report 230
Organization Report 231
ユーザ アクティビティ レポート 232
WebFort レポート 232
Authentication Activity Report 232
Credential Management Activity Report 232
Configuration Management Report 232
User Administrator レポート 233
管理者レポート 233
My Activity Report 233

Administrator Activity Report 233
ユーザ アクティビティ レポート 233
WebFort レポート 235
Authentication Activity Report 235
Credential Management Report 235
レポートの生成 235
レポートを生成する際の注意事項 235
レポートを生成する方法 236
レポートをエクスポートする方法 237
第 9 章
システム管理者用のツール 239
DBUtil 239
arwfserver 240
arwfclient 243
付録 A
WebFort のログ 247
ログ ファイルについて 247
スタートアップ ログ ファイル 248
トランザクション ログ ファイル 248
WebFort サーバのログ 249
WebFort 統計ログ ファイル 249
UDS ログ ファイル 249
Administration Console ログ ファイル 250
WebFort ログ ファイルのフォーマット 251
UDS ログ ファイルおよび Administration Console ログ ファイルのフォーマット 252
サポートされる重大度レベル 253
付録 B
用語集 259
索引 263

序文

「Arcot WebFort 6.2 管理ガイド」は、Arcot Administration Console を使用して、Arcot WebFort 6.2 をセットアップし、管理するための情報を説明します。このガイドは、Windows および UNIX ベースのプラットフォーム（Solaris SPARC® および Red Hat Enterprise Linux）の両方の情報について説明します。

対象読者

このガイドは Arcot WebFort の管理者を対象にしています。Administration Console を使用して、メンテナンス、プロビジョニング、更新、パフォーマンスの監視、および WebFort 設定の変更に関連する典型的な管理タスクを実行する方法を説明します。

このガイドは、以下の分野に経験が豊富なユーザを対象にしています。

- オペレーティング システムベースの管理
- 適用可能な Oracle および（または）MS SQL データベース
- アプリケーション サーバおよび Web サーバの管理

このガイドの内容

このガイドは、以下の項目で構成されます。

- 第 1 章の「Administration Console の概要」: WebFort Administration Console のインターフェースおよび管理階層を説明します。
- 第 2 章の「はじめに」: 管理者の作成、Administration Console のログインおよびログアウト、管理者パスワードの変更など、基本的な管理タスクを説明します。また、管理者アカウントの作成、更新、および削除を行うための手順も説明します。
- 第 3 章の「WebFort サーバ インスタンスの管理」: WebFort サーバ インスタンスをセットアップし、管理する方法を説明します。
- 第 4 章の「グローバルな WebFort 設定の管理」: グローバル レベルで設定でき、システムで設定された個別の組織によって継承できる設定を説明します。

- 第 5 章の「組織の管理」: WebFort の組織を対象に作成、検索、アクティブ化、有効化、無効化、または削除を行う方法を説明します。この章では、グローバル レベルで設定できない、組織に固有の設定を管理するためのタスクについても説明します。
- 第 6 章の「管理者の管理」: システムのさまざまな管理者を対象に作成、検索、アクティブ化、有効化、無効化、および削除を行う方法を説明します。
- 第 7 章の「ユーザの管理」: Administration Console を使用して、エンド ユーザを対象に検索、アクティブ化、有効化、無効化、または削除を行う方法を説明します。
- 第 8 章の「レポートの管理」: 各管理レベルで利用可能なレポート、およびこれらのレポートの使用方法について説明します。
- 第 9 章の「システム管理者用のツール」: システムを監視し、管理するためにシステム管理者が使用できる、WebFort によって提供されるツールを説明します。
- 付録 A の 「WebFort のログ」: すべての WebFort ログ ファイル、ログ ファイルに記録される重大度レベル、およびログ ファイルのエントリの形式を説明します。
- 付録 B の 「用語集」: このガイドで使用される重要な用語をリストします。

関連するドキュメント

その他の関連するドキュメントは以下のとおりです。

ドキュメント	説明
Arcot WebFort 6.2 インストールおよび展開ガイド	このガイドは、WebFort とそのコンポーネントをインストールおよび設定する方法について説明します。
Arcot WebFort 6.2 クイック インストール ガイド	このガイドは、WebFort をインストールするために実行する必要があるタスクを簡略に説明します。
Arcot WebFort 6.2 Java 開発者ガイド	このガイドは、WebFort で提供される Java API と、それらの使用方法について説明します。
ArcotID Client 6.0.2 リファレンス ガイド	このガイドは、ArcotID Client のタイプ、およびクライアントによって提供される API について説明します。

表記規則および形式

このマニュアルの表記規則、形式、およびスコープについては、以下のパラグラフで説明します。

表記規則

このマニュアルは、以下の表記規則を使用します。

斜体	強調、ガイド名
太字	ユーザ入力、GUI 画面テキスト
等幅	ファイル名およびディレクトリ名、拡張子、コマンド プロンプト、CLI のテキスト、コード
等幅太字	パス内のターゲット ファイルまたはディレクトリ名
等幅斜体	ユーザによって異なる可能性があるファイル名またはディレクトリ名
リンク	ガイド、URL リンク内のリンク

形式

このマニュアルは、以下の強調形式を使用して、特別なメッセージを示します。

注 : 重要または特別な注意が必要な情報を強調します。

ヒント : 時間またはリソースを節約する手順を強調します。

警告 : このタイプのメッセージを考慮しないと、機器の誤動作または損傷が発生することがあります。

重要 : 操作を実行する前に知っておく必要がある情報。

注意 : ユーザに危険性の存在を喚起します。

関連文書： 他のガイドへの参照情報を提供します。

サポートへのお問い合わせ

ヘルプを必要とする場合は、以下の手段のいずれかを使用して Arcot のテクニカル サポートにお問い合わせください。

E-MAIL（電子メール）	*support@arcot.com*
Web サイト	*http://www.arcot.com/support/index.html*

第 1 章
Administration Console の概要

Arcot Administration Console （以下、「Administration Console」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、すべての Arcot 製品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。

このコンソールは、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、Administration Console 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のみを構築する機能を提供します。

この章では、Administration Console 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。この章には、以下のトピックがあります。

- Administration Console について
- Administration Console の要素
- サポートされるロール
- 次の手順

注： Administration Console 用に推奨されるデスクトップの画面解像度は、1024 × 768 です。

Administration Console について

Administration Console は、Web 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、管理サーバにネットワーク アクセス可能な、サポートされる任意の Web ブラウザからアクセスできます。Administration Console を使用すると、展開しているすべての WebFort インスタンスを管理できます。インスタンスは、指定したポートで利用できる WebFort サーバを表します。

Administration Console では、WebFort の設定、ユーザおよび管理ロールのセットアップを行うことができます。また、以下の管理操作および設定タスクを実行することもできます。

- サーバ インスタンスの設定およびリフレッシュ
- サーバと他の WebFort コンポーネントとの間の通信パラメータの設定
- 組織、管理者、ユーザ、およびそれらのクレデンシャルの管理
- 認証ポリシーの設定
- クレデンシャル 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

実行することが許可されているタスクが、Administration Console 上のさまざまなタブを介して表示されます。各管理者は、個別のロールまたはユーザ グループに属することができます。各管理者が利用可能なタスクは、ロールに割り当てられた権限によって異なります。

Administration Console の要素

Administration Console の典型的な画面は、以下の要素で構成されます。

- ヘッダ
- メイン メニュー
- サブ メニュー
- タスク
- 本体

図 1-1 は、Administration Console でのこれらの要素の配置を示します。

図 1-1 Administration Console の一般的なレイアウト

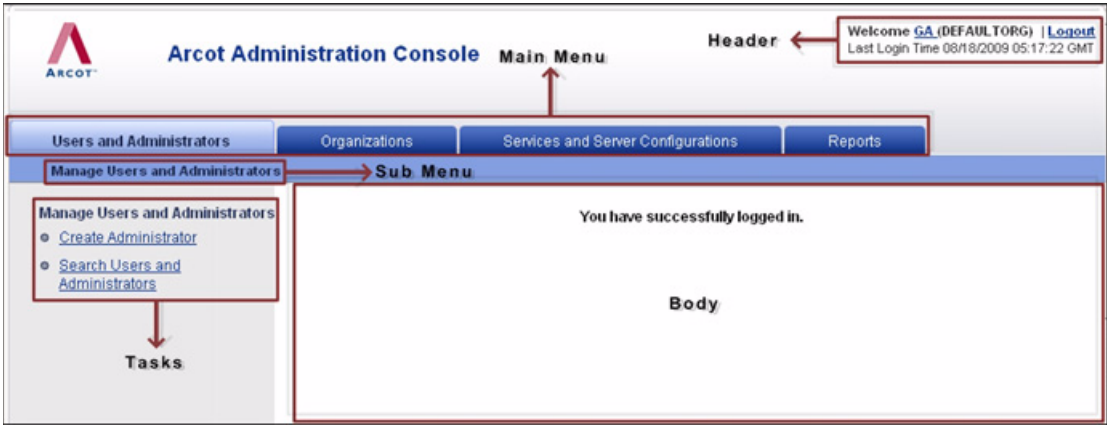


表 1-1 はこれらの要素を説明します。

表 1-1. Administration Console の要素

要素	説明
ヘッダ	ログイン情報（管理者名、管理者が属する組織、最後のログイン日付および時間）が表示されます。 ヘッダのリンクを使用して、以下を行うことができます。 • プロファイル情報（名前、電話番号、電子メール ID）およびパスワードの変更。また、今後実行する可能性があるすべてのタスクで優先して使用する組織を指定できます。 • Administration Console からのログアウト。
メイン メニュー	現在の管理者に利用可能な高レベルのオプションを表示します。
サブメニュー	選択したメイン メニューで利用できるオプションが表示されます。
タスク	選択したサブメニューで利用できるタスクが表示されます。
本体	選択したタスクに対応するページが表示されます。

コンソール メッセージ

図 1-2 に示されるように、Administration Console の使用時に生成される情報、警告、およびエラーの各メッセージは、本体ページの上部に表示されます。

図 1-2 に示されるように、エラー メッセージは赤字で表示されます。成功を示すメッセージは青字で表示されます。図 1-3 に示されるように、これらのメッセージの一部として追加の指示が表示されることもあります。

図 1-2 コンソール メッセージ：エラー

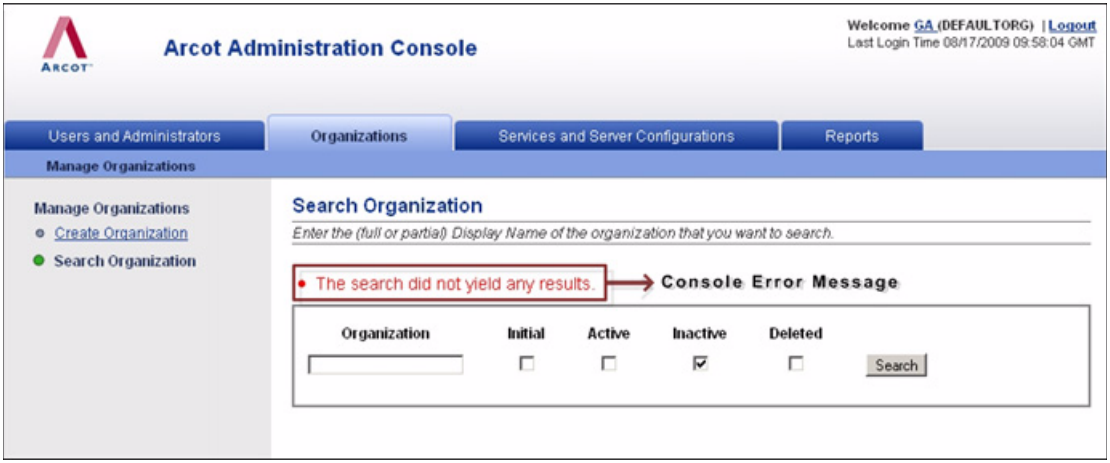
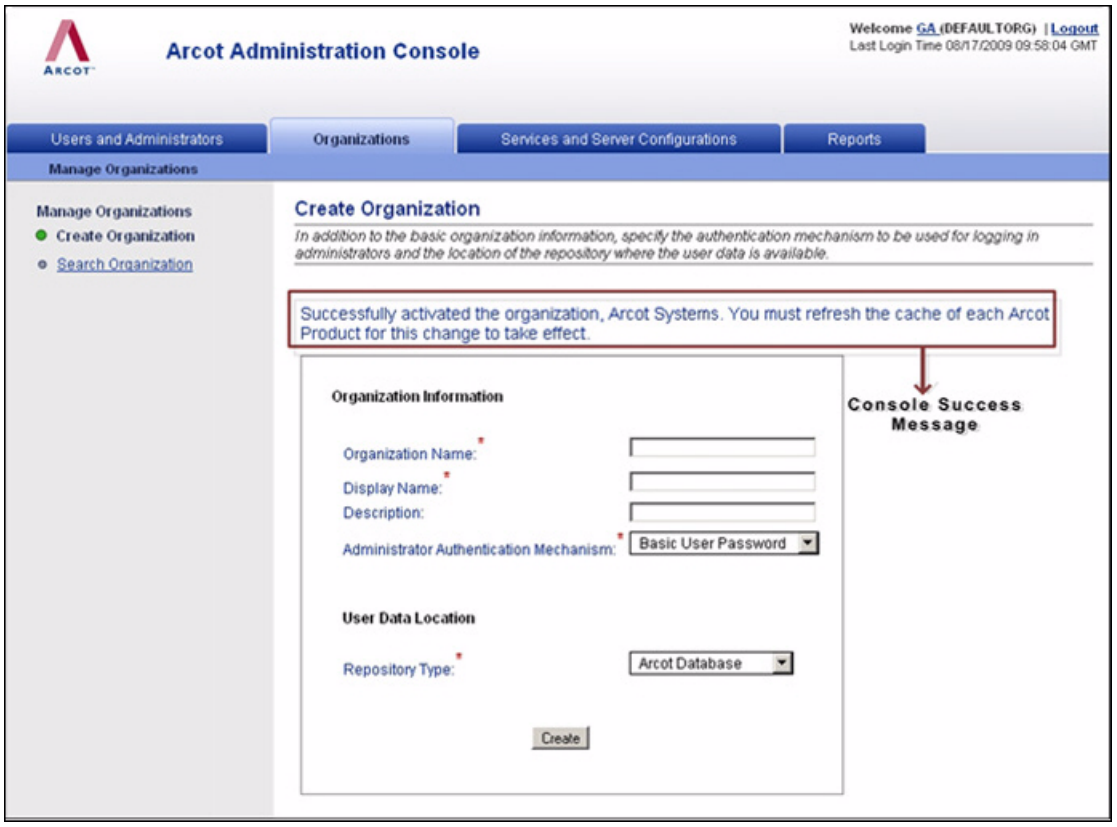


図 1-3 コンソール メッセージ：成功



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。ユーザが特定の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管理できます。

Arcot Administration Console 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。

Administration Console は、以下のタイプのロールをサポートします。

- ユーザ
- デフォルトの管理ロール
- カスタム ロール

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、Arcot Administration Console 内でユーザと呼ばれます。これらのユーザは、LDAP（Lightweight Directory Access Protocol）リポジトリまたは Arcot データベースのいずれかに存在できます。

ユーザが LDAP システムにすでに存在する場合、組織の LDAP 属性を、Arcot でサポートされる属性にマッピングする必要があります。これをする方法の詳細については、「LDAP リポジトリでの組織の作成」を参照してください。

デフォルトの管理ロール

Administration Console には、高いレベルの設定を実行できる Master Administrator と呼ばれる組み込みの管理者が含まれており、この管理者はすぐに使用できます。これ以外に、WebFort 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、ユーザを管理ロールに割り当てる必要があります。管理者権限を持つユーザは、管理者ユーザと呼ばれます。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。

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」を参照してください。

Administration Console 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。

- Master Administrator
- Global Administrator
- Organization Administrator
- User Administrator

さらに、カスタム ロールも作成できます。

注： 管理者もシステムのユーザと見なされます。

管理ロールのスコープ

Arcot Administration Console 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。

スコープに関する重要な注意事項

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。

- Master Administrator のスコープは、デフォルトで**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。
- ロール（Global Administrator、Organization Administrator、および User Administrator）は、管理階層の下方向のみ管理できます（上方向の階層は管理できません）。言い換えれば、子ロールを管理するロールは、子の親を管理できません。

  たとえば、Global Administrator は Organization Administrator と User Administrator を管理できます。ただし、Master Administrator は管理できません。
- Global Administrator のロールを割り当てられた管理者は、すべての組織のスコープを割り当てることができます。その場合には、この管理者は既存および今後作成される組織をすべて管理できます。
- Organization Administrator または User Administrator は特定の組織のみを管理できます。
- 管理者がカスタム ロールを使用して派生している場合、派生した管理者は親と同じレベルに属します。

たとえば、管理者 MyGlobalAdmin を Global Administrator から派生させて作成した場合、MyGlobalAdmin は、Global Administrator とみなされます。これは、MyGlobalAdmin に、Organization Administrator または User Administrator より少ない権限を割り当てた場合も同じです。

注： **Organization Administrator** および **User Administrator** のロールは、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*。

Master Administrator

Master Administrator （MA）はスーパーユーザで、システム全体に対する、無制限のアクセス権が割り当てられています。MA のデフォルト 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ブートストラップする（または、初期化する）。
- ユーザ データ サービス（UDS）接続パラメータを設定する。
- Administration Console およびユーザ データ サービス用に、グローバル組織設定およびキャッシュリフレッシュ設定を設定する。
- WebFort サーバの通信パラメータを設定する。
- WebFort サーバ インスタンス設定、信頼されるストア設定、およびプロトコル設定を設定する。
- Administration Console 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 WebFort 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」を、コールアウトを設定する方法の詳細については 5-158 ページの「コールアウトの設定」を、プラグインを設定する方法については 5-161 ページの「プラグインの設定」を、参照してください。

- 必要に応じて、組織を作成し、管理する。

- 必要に応じて、任意のロール（Global Administrator、Organization Administrator、または User Administrator）の管理者を作成し、管理する。
- カスタム ロールを作成し、管理する。
- インスタンス統計を生成する。

Administration Console が正常にインストールされたら、最初に MA としてログインする必要があります。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。MA のアクションはシステム全体のセキュリティに影響を及ぼす可能性があるため、Arcot は、初めてコンソールにログインした後、このパスワードを変更することを強く推奨します。さらに、Arcot は、このパスワードを保護し、定期的に変更することを推奨します。

注： MA アカウントがロックされた場合は、弊社テクニカル サポート（*support@arcot.com*）に問い合わせてください。

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るだけでなく、システム内の他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。

Global Administrator

Global Administrator （GA）は、管理階層の 2 番目のレベルに位置します。Global Administrator は、システムのブートストラップ、Administration Console の初期設定、サーバ設定の指定、およびカスタム ロールの管理を除く、MA のほとんどのタスクを実行できます。

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、ロール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 Global Administrator、Organization Administrator、User Administrator を作成し、管理する。
- Administration Console 用の認証を設定する。
- 必要に応じて、組織を作成し、管理する。
- ユーザ クレデンシャルを管理する。

- サポートされる認証メカニズム用の WebFort 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。
- コールアウトおよび登録済みプラグインを設定する。

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、およびクレデンシャル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 Organization Administrator と User Administrator のレポートを表示できます。

Organization Administrator

Organization Administrator （OA）は、管理階層の 3 番目のレベルに位置します。Organization Administrator は、MA または GA のいずれか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。以下のタスクが実行できます。

- 必要に応じて、他の Organization Administrator または User Administrator を作成し、管理する。
- 権限の範囲内の組織を管理する。
- 組織固有の設定を管理する（更新する）。
- 権限の範囲内の組織に属するユーザを管理する。

OA を作成する際には、管理のスコープを指定する必要があります。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 User Administrator のレポートを表示できます。

User Administrator

User Administrator （UA）ロールは、管理階層の最下位のレベルに位置します。User Administrator 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。以下のタスクが実行できます。

- 必要に応じて、他の UA を管理する。
- 必要に応じて、権限の範囲内の組織のユーザを管理する。

注： これには、ユーザ詳細を編集することも含まれます。

- ユーザ クレデンシャルの管理。

UA を作成する際には、管理のスコープを指定する必要があります。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。

管理権限の要約

表 1-2 は、サポートされる 4 レベルの各管理者で利用可能な権限を要約します。

表で使用されている列名の頭字語は次のとおりです。

- Master Administrator -> **MA**
- Global Administrator -> **GA**
- Organization Administrator -> **OA**
- User Administrator -> **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。

表 1-2. 管理者権限の要約

機能	タスク	MA	GA	OA	UA
認証管理	ベーシック認証の更新	✓	✓	✓	
	WebFort 認証設定の更新	✓			
キャッシュ管理	キャッシュ リフレッシュ設定の更新	✓			

表 1-2. 管理者権限の要約（続き）

機能	タスク	MA	GA	OA	UA
Global Administrator アカウント管理	Global Administrator アカウントの作成	✓	✓		
	Global Administrator 詳細の検索または表示	✓	✓	✓	✓
	Global Administrator アカウント情報の更新	✓	✓	✓	✓
	Global Administrator アカウントの有効化	✓	✓		
	Global Administrator アカウントの無効化	✓	✓		
	Global Administrator アカウントの削除	✓	✓		
Organization Administrator アカウント管理	Organization Administrator アカウントの作成	✓	✓	✓	
	Organization Administrator 詳細の検索または表示	✓	✓	✓	✓
	Organization Administrator アカウント情報の更新	✓	✓	✓	✓
	Organization Administrator アカウントの有効化	✓	✓	✓	
	Organization Administrator アカウントの無効化	✓	✓	✓	
	Organization Administrator アカウントの削除	✓	✓	✓	
User Administrator アカウント管理	User Administrator アカウントの作成	✓	✓	✓	
	User Administrator 詳細の検索または表示	✓	✓	✓	✓
	User Administrator アカウント情報の更新	✓	✓	✓	✓
	User Administrator アカウントの有効化	✓	✓	✓	✓
	User Administrator アカウントの無効化	✓	✓	✓	✓
	User Administrator アカウントの削除	✓	✓	✓	✓
ユーザ データ サービス（UDS）の管理	グローバル ユーザ データ サービス（UDS）設定の更新	✓			

表 1-2. 管理者権限の要約（続き）

機能	タスク	MA	GA	OA	UA
カスタム ロールの管理	カスタム ロールの作成	✓			
	カスタム ロールの更新	✓			
	カスタム ロールの削除	✓			
デフォルトの組織の管理	デフォルトの組織の設定	✓			
組織管理	組織の作成	✓	✓		
	組織詳細の検索および表示	✓	✓	✓	✓
	組織情報の更新	✓	✓	✓	
	組織のアクティブ化	✓	✓	✓	✓
	組織の非アクティブ化	✓	✓	✓	✓
	組織の削除	✓	✓		
ユーザの管理	ユーザ詳細の検索および表示	✓	✓	✓	✓
	ユーザ情報の更新	✓	✓	✓	✓
	ユーザのアクティブ化	✓	✓	✓	✓
	ユーザの非アクティブ化	✓	✓	✓	✓
	ユーザの削除	✓	✓	✓	✓
WebFort 設定	ArcotID の作成		✓	✓	
	設定の割り当て		✓	✓	
	ArcotID の取得		✓	✓	✓
	コールアウトの登録		✓	✓	
	プラグインの設定		✓	✓	
	ArcotID 属性の削除		✓	✓	✓
	ArcotID 属性の設定		✓	✓	✓
	クレデンシャル設定の取得		✓	✓	✓
	クレデンシャルの作成		✓	✓	✓
	クレデンシャルの削除		✓	✓	✓
	クレデンシャルの無効化		✓	✓	✓
	クレデンシャルの有効化		✓	✓	✓
	クレデンシャルの取得		✓	✓	✓
	クレデンシャルの再発行		✓	✓	✓
	クレデンシャルのリセット		✓	✓	✓
	クレデンシャルの注釈のリセット		✓	✓	✓

表 1-2. 管理者権限の要約（続き）

機能	タスク	MA	GA	OA	UA
WebFort 設定	クレデンシャルの有効性のリセット		✓	✓	✓
	ArcotID プロファイルの管理		✓	✓	
	ASSP 設定の管理		✓	✓	
	OTP プロファイルの管理		✓	✓	
	ユーザ名 - パスワード 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		✓	✓	
	SAML トークンの管理		✓	✓	
	OTP ポリシーの作成		✓	✓	
	パスワード ポリシーの作成		✓	✓	
	モジュールの関連付け		✓	✓	
	Q&A ポリシーの作成		✓	✓	
	クレデンシャル詳細の表示		✓	✓	✓
インスタンスの管理	WebFort 接続性	✓			
	インスタンスの管理	✓			
	プロトコルの管理	✓			
	プラグインの登録	✓			
	その他の設定	✓			
	インスタンス統計の生成	✓			
	信頼された CA の設定	✓			
レポートの管理	管理者アクティビティ レポートの表示	✓	✓	✓	✓
	My Activity Report の表示	✓	✓	✓	✓
	組織レポート	✓	✓	✓	
	ユーザ アクティビティ レポートの表示		✓	✓	✓
	認証レポートの表示		✓	✓	
	クレデンシャルレポートの表示		✓	✓	
	サーバ管理レポート	✓			
	設定レポート		✓	✓	

カスタム ロール

MA は、以下の事前定義済み親ロールの 1 つ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。

- Global Administrator
- Organization Administrator
- User Administrator

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 に対して「組織作成権限」を無効にする必要があれば、この権限を無効にしてカスタム ロールを作成できます。

作成したカスタム ロールは、管理アカウントの作成または更新時にロール オプションとして利用可能になります。

カスタム ロールに関する注意事項

- 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。言い換えれば、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、事前定義済み OA ロールに組織を作成する権限が割り当てられていない場合、この OA ロールに基づくカスタム ロールにこの権限を割り当てることはできません。
- カスタム ロールを作成するときには、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、［Search Organizations］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、Administration Console サーバのキャッシュをリフレッシュした後にのみ、Administration Console の他のインスタンスで利用できます。

次の手順

ここまでは、WebFort Administration Console の概念について説明してきました。このセクションでは、展開を行うための手順について簡単に説明します。この目的のために、以下の展開について簡単な説明を示します。

- 単純な展開
- カスタム展開

単純な展開

WebFort の最も単純な実装は、通常、小規模なユーザ ベースに対して強い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 WebFort 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、WebFort がインストールされているのと同じシステム、または別のシステムに配置できます。

関連文書： この展開タイプの詳細については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の第 2 章「展開の計画」を参照してください。

表 1-3 は、この展開タイプの典型的な特徴を要約します。

表 1-3. 単純な展開の特徴

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。これは単一組織システムであるため、システムの初期化時に自動的に作成されるデフォルトの組織を使用でき、新しい組織をセットアップする必要はありません。結果として、OA アカウントの作成も必要としない場合があります。必要なのは、必須の GA アカウントおよび UA アカウントを作成することのみです。

WebFort のエンド ユーザは、システムに付属する SDK を使用して作成できます （SDK を使用してユーザを作成する方法の詳細については、「Arcot WebFort 6.2 Java 開発者ガイド」を参照してください)。

ヒント：また、WebFort のサンプル アプリケーションを使用してユーザを作成することもできます。サンプル アプリケーションは *http://< ホスト >:< ポート >/webfort-6.2-sample-application* URL で入手できます。

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. WebFort が正しくインストールおよび設定されており、Administration Console およびユーザ 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。

   関連文書： WebFort のインストール、WAR ファイルの展開、および行う必要のある他のインストール後タスクの詳細については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の第 4 章「単一システム上の WebFort の展開」を参照してください。

2. MA として Administration Console にログインし（2-21 ページの「Administration Console へのアクセス」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。

   関連文書： 詳細については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の第 4 章の「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 アカウントおよび UA アカウントを作成します。

   詳細については、6-176 ページの「管理者の作成」を参照してください。

4. WebFort にユーザを登録します。

   この目的のために WebFort に付属している Java SDK を使用します。

   関連文書： これらの SDK を統合する方法の詳細については、「Arcot WebFort 6.2 Java 開発者ガイド」を参照してください。

これで、システムを管理できるようになりました。システム（第 3 章の「WebFort サーバ インスタンスの管理」）、管理者（第 6 章の「管理者の管理」）、およびユーザ（第 7 章の「ユーザの管理」）を管理できます。

カスタム展開

展開が複雑で、高可用性が不可欠な大企業では、WebFort を実装することにより、大きなユーザ ベースに対して強い認証を提供し、システムを管理する管理者を作成できます。この展開タイプでは、WebFort 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。これは、高いセキュリティ、パフォーマンス、および可用性を実現することを目的とします。また、複数のアプリケーションが強い認証の機能を使用できるようにすることも目的の 1 つです。

関連文書： この展開タイプの詳細については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の第 2 章「展開の計画」を参照してください。

表 1-4 は、この展開タイプの典型的な特徴を要約します。

表 1-4. 分散展開の特徴

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. WebFort が正しくインストールおよび設定されており、Administration Console およびユーザ 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。

   関連文書： WebFort のインストール、WAR ファイルの展開、および行う必要のある他のインストール後タスクの詳細については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の第 4 章「単一システム上の WebFort の展開」を参照してください。

2. MA として Administration Console にログインし（2-21 ページの「Administration Console へのアクセス」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。

   関連文書： 詳細については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の第 4 章の「システムのブートストラップ」を参照してください。

3. Administration Console を設定します。これには、UDS 設定、グローバル組織設定、Administration Console キャッシュ設定、および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、2-23 ページの「Administration Console 設定の構成」を参照してください。

4. 別のシステムで WebFort 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、3-41 ページの「サーバ インスタンスのセットアップ」を参照してください。

5. Administration Console、SDK、および Web サービスと WebFort 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、3-51 ページの「通信プロトコルの設定」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、5-135 ページの「組織の作成とアクティブ化」を参照してください。

7. 必要に応じて、管理者（6-176 ページの「管理者の作成」を参照する）とカスタム ロール（3-67 ページの「カスタム ロールの操作」を参照する）を計画し、作成します。

8. 適切なクレデンシャル プロファイル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、第 4 章の「グローバルな WebFort 設定の管理」を参照してください。

9. WebFort にユーザを登録します。

   この目的のために WebFort に付属している Java SDK を使用します。

関連文書： これらの SDK を統合する方法の詳細については、「Arcot WebFort 6.2 Java 開発者ガイド」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、5-149 ページの「組織固有の設定の管理」を参照してください。

11. 必要に応じて、WebFort 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、3-50 ページの「信頼されるストアの作成」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、3-64 ページの「その他の設定」を参照してください。

13. WebFort の機能を拡張するためにコールアウトと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」を、コールアウトを設定する方法の詳細については 5-158 ページの「コールアウトの設定」を、プラグインを設定する方法については 5-161 ページの「プラグインの設定」を、参照してください。

これで、システムを管理できるようになりました。システム（第 3 章の「WebFort サーバ インスタンスの管理」）、管理者（第 6 章の「管理者の管理」）、およびユーザ（第 7 章の「ユーザの管理」）を管理できます。

第 2 章
はじめに

この章では、WebFort を正常にインストールし、コンソールを展開した後で、Master Administrator として Administration Console 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。ここでは、以下のタスクについて説明します。

- Administration Console へのアクセス
- Administration Console 設定の構成
- プロファイル情報の変更

Administration Console へのアクセス

デフォルトの Master Administrator （MA）アカウントは、初めて Administration Console にログインするために使用されます。以下の既定のクレデンシャルを使用して、コンソールにログインします。

- ユーザ名：**masteradmin**
- パスワード：**master1234!**

Administration Console にログインする方法

1. Web ブラウザ ウィンドウを開きます。
2. Administration Console にアクセスするための URL を入力します。デフォルトの Administration Console のアドレスは以下のとおりです。

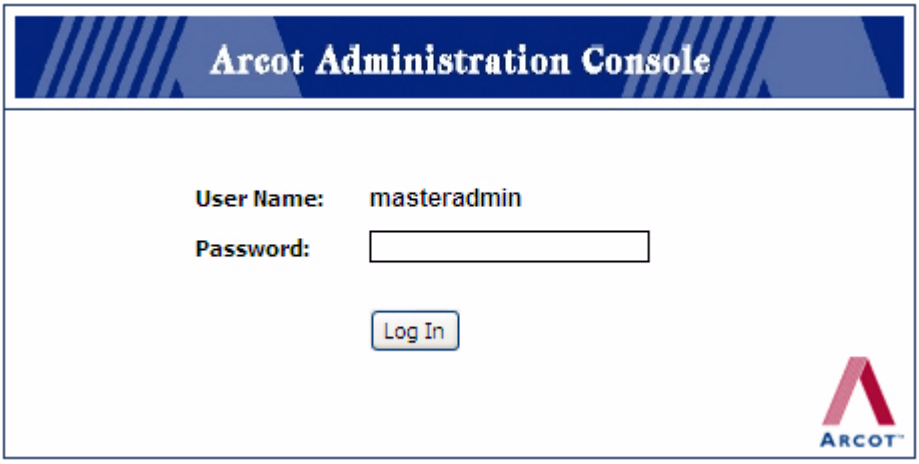
   http://<hostname>:<port>/arcotadmin/masteradminlogin.htm

   上記の URL で、以下を実行します。

   - *hostname* および *port* を、それぞれ、Administration Console を展開したシステムのホスト名または IP アドレス、コンソールがリスンしているポートに置き換えます。
   - デフォルトのアプリケーション コンテキスト（arcotadmin）を変更した場合、これを新しい値に置換する必要があります。

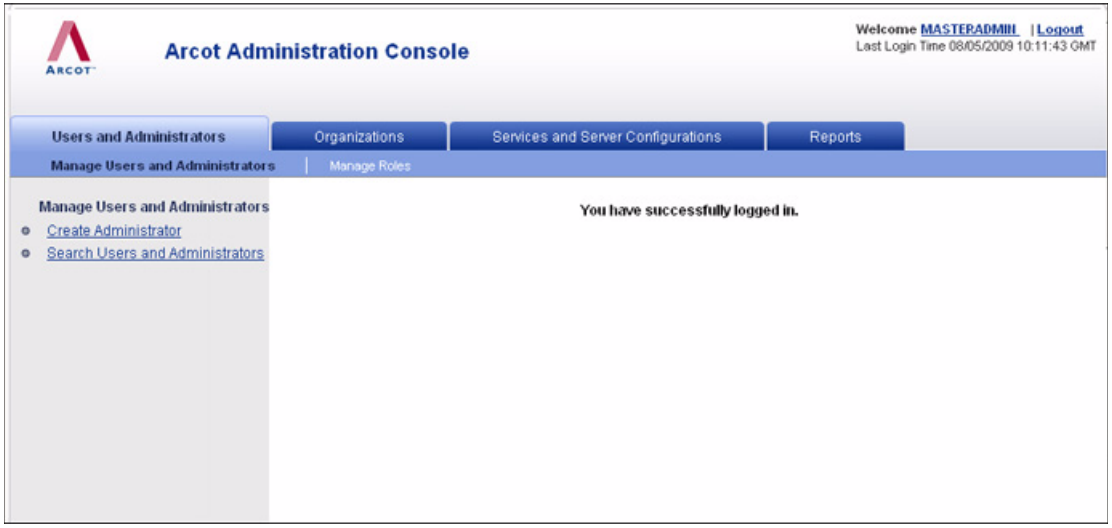
   図 2-1 に示されているように、［Master Administrator Login］ページが表示されます。

図 2-1 ［Master Administrator Login］ページ



3. ［**Password**］フィールドに「**master1234!**」と入力し、［**Log In**］をクリックします。Administration Console のランディング ページ（図 2-2）が表示されます。

図 2-2 Master Administrator: Successfully Logged In



Administration Console 使用時のセキュリティに関する推奨事項

Administration Console 使用時にブラウザ セッションを通した悪意のある攻撃から WebFort を保護するために、次のことを遵守してください。

- 他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。
- Console を操作しながら他のサイトを開かない。
- Administration Console のために厳しいパスワード制限を実施する。
- Administration Console 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。
- 実行する必要のあるタスクに応じて、管理者に適切なロールを割り当てる。

Administration Console のログアウト

Administration Console からログアウトするには、コンソールのヘッダ領域の右上隅にある、［**Logout**］リンクをクリックします。

Administration Console 設定の構成

WebFort 固有の設定を構成する前に、以下の Administration Console のグローバル設定を構成することをお勧めします。

- ユーザ データ サービス（UDS）設定
- 組織のグローバル設定
- キャッシュ リフレッシュ設定
- 基本認証設定

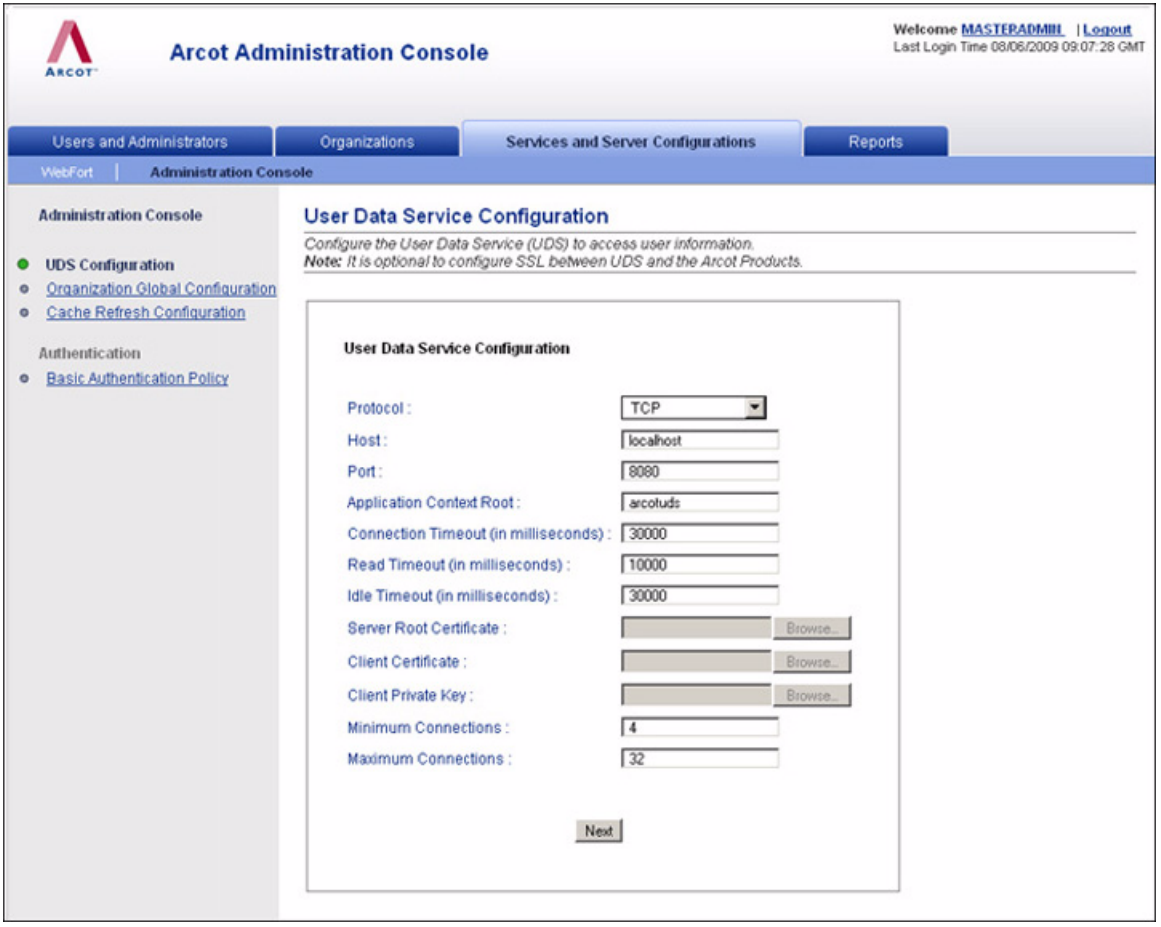
以下のサブセクションでは、これらのグローバル設定を構成するための手順について説明します。

UDS 設定の指定

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 データ リポジトリ（LDAP ディレクトリ サーバなど）へのアクセスを有効にするための Administration Console モジュールです。UDS は WebFort および Administration Console が既存データにシームレスにアクセスできるようにし、標準的な Arcot SQL データベース テーブル内でこれを複製する必要なしに、エンドユーザ情報を活用できるようにします。

通常、システムのブートストラップ中に UDS パラメータを指定します。（これに関連する詳細については、「Arcot WebFort 6.2 インストールおよび展開ガイド」の「システムのブートストラップ」を参照してください。）ただし、UDS パラメータ設定を更新する場合、［User Data Service Configuration］ページ（図 2-3）を使用して、これを行ってください。

図 2-3 User Data Service Configuration：1 ページ目



UDS 設定を更新する方法

1. 必ず MA としてログインしてください。
2. ［**Services and Server Configurations**］タブを有効化します。
3. タブのサブメニューの［**Administration Console**］オプションをクリックします。
4. ［User Data Service Configuration］ページがまだ表示されない場合、［**UDS Configuration**］リンクをクリックして、このページを表示します（図 2-3）。
5. ［**User Data Service Configuration**］セクションの表 2-1 にリストされた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。

表 2-1. UDS 設定パラメータ

パラメータ	デフォルト値	説明
Protocol	TCP	Administration Console 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** • **One-Way SSL** • **Two-Way SSL**
Host	localhost	UDS が使用可能な IP アドレス。
Port	8080	UDS が使用可能なポート。
Application Context Root	arcotuds	UDS がアプリケーション サーバ インスタンス（現在動作している複数の Administration Console アプリケーションのインスタンス）内でアクセス可能な一意のベース URL。たとえば、UDS を `arcotuds` のコンテキスト ルートで実行している場合、以下の URL を使用して、使用可能な UDS サービスを表示します。 *http://<host>:<port>/arcotuds/services/listServices*
Connection Timeout (in milliseconds)	30000	UDS サービスが到達できないと見なされるまでの最大時間（ミリ秒）。
Read Timeout (in milliseconds)	10000	UDS からのレスポンスを待機する最大時間（ミリ秒）。
Idle Timeout (in milliseconds)	30000	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）。
Server Root Certificate		UDS サーバの CA 証明書ファイルへのパス。このファイルは PEM 形式である必要があります。

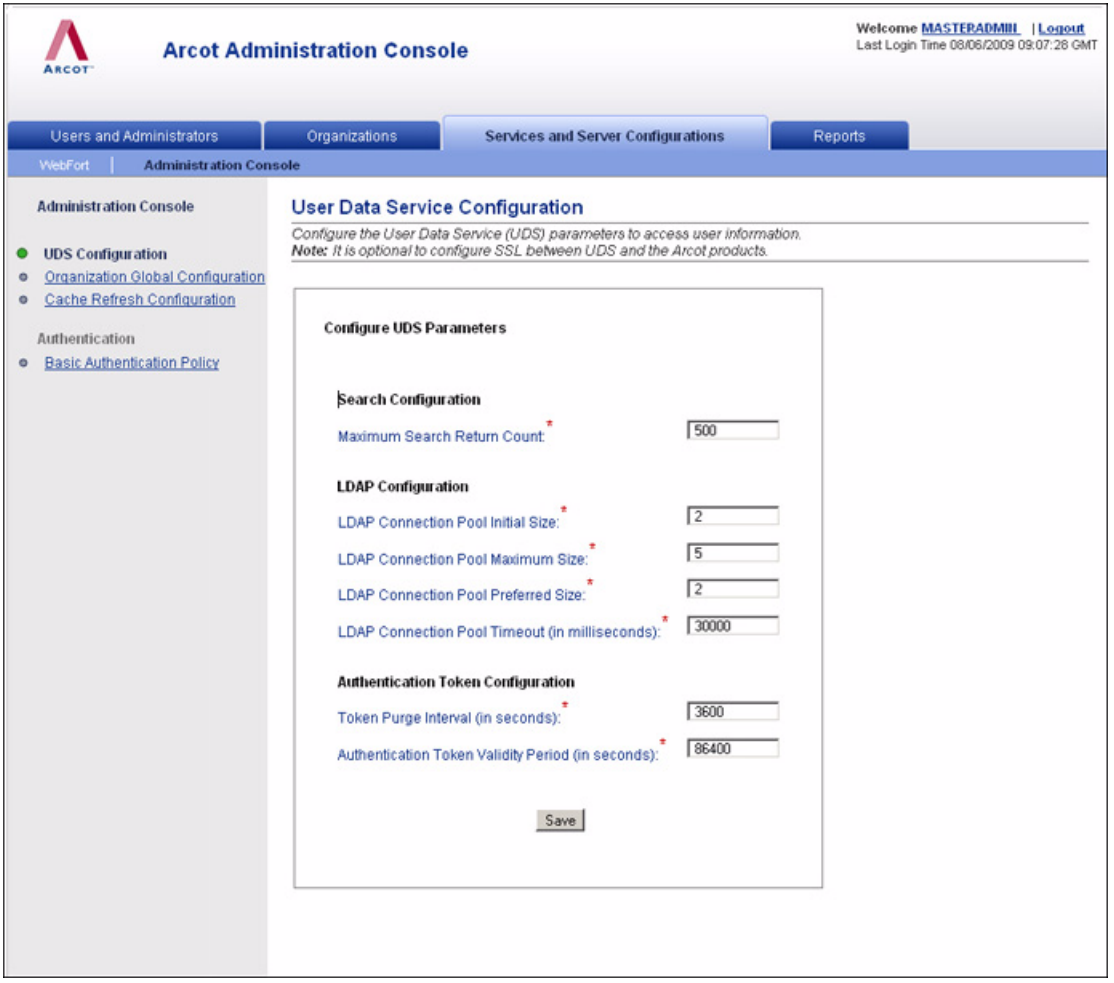
表 2-1. UDS 設定パラメータ

パラメータ	デフォルト値	説明
Client Root Certificate		Administration Console の CA 証明書ファイルへのパス。このファイルは PEM 形式である必要があります。
Client Private Key		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。
Minimum Connections	4	WebFort サーバと UDS サーバの間で作成される接続の最小数。
Maximum Connections	32	WebFort サーバと UDS サーバ間で作成できる接続の最大数。

6. ［**Next**］をクリックして、設定を続行します。

   図 2-4 に示されているように、次のページが表示されます。

図 2-4 User Data Service Configuration：2 ページ目



7. ［**User Data Service Configuration**］セクションの表 2-2 にリストされた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。

表 2-2. UDS 検索、LDAP、および認証設定パラメータ

パラメータ	デフォルト値	説明
Search Configuration		
Maximum Search Return Count	**500**	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。
LDAP Configuration		
LDAP Connection Pool Initial Size	**2**	プール内に作成される UDS と LDAP 間の接続の初期数。
LDAP Connection Pool Maximum Size	**5**	UDS と LDAP 間で許可される接続の最大数。
LDAP Connection Pool Preferred Size	**2**	UDS と LDAP 間の接続の優先順位。
LDAP Connection Pool Timeout (in milliseconds)	**30000**	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。
Authentication Token Configuration		
Token Purge Interval (in seconds)	**3600**	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。
Authentication Token Validity Period (in seconds)	**86400**	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）。

8. ［**Save**］をクリックして、加えた変更を保存します。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の手順については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

組織のグローバル設定の指定

Administration Console 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。

新しい組織を作成する必要がないため、単一の組織システムとして、「デフォルトの組織」は有用です。「デフォルトの組織」の設定を構成し、「表示名」を変更し、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、設定を構成し、これを既定として続けて使用できます。また、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、組織を指定せずに管理者を作成するか、ユーザを登録する場合、これらは「デフォルトの組織」内で作成されます。

［Organization Global Configuration］ページ（図 2-5）では、デフォルトの組織として使用される組織を選択し、システムの今後の組織がデフォルトの組織の設定を継承するかどうかを制御できます。また、このページを個別に編集して、これらの設定を上書きできます。

図 2-5 ［Organization Global Configuration］ページ

デフォルトの組織を指定し、設定を組織レベルで構成するかどうかを指定する方法

1. 必ず MA としてログインしてください。

2. ［**Services and Server Configurations**］タブを有効化します。
3. タブのサブメニューの［**Administration Console**］オプションをクリックします。
4. タスク ペインで、［**Organization Global Configuration**］リンクをクリックして、対応するページ（図 2-5）を表示します。
5. 組織固有の設定を構成しない場合は、［**Organization Configuration**］で、［**Allow Configuration at Organization Level**］オプションを選択解除します。

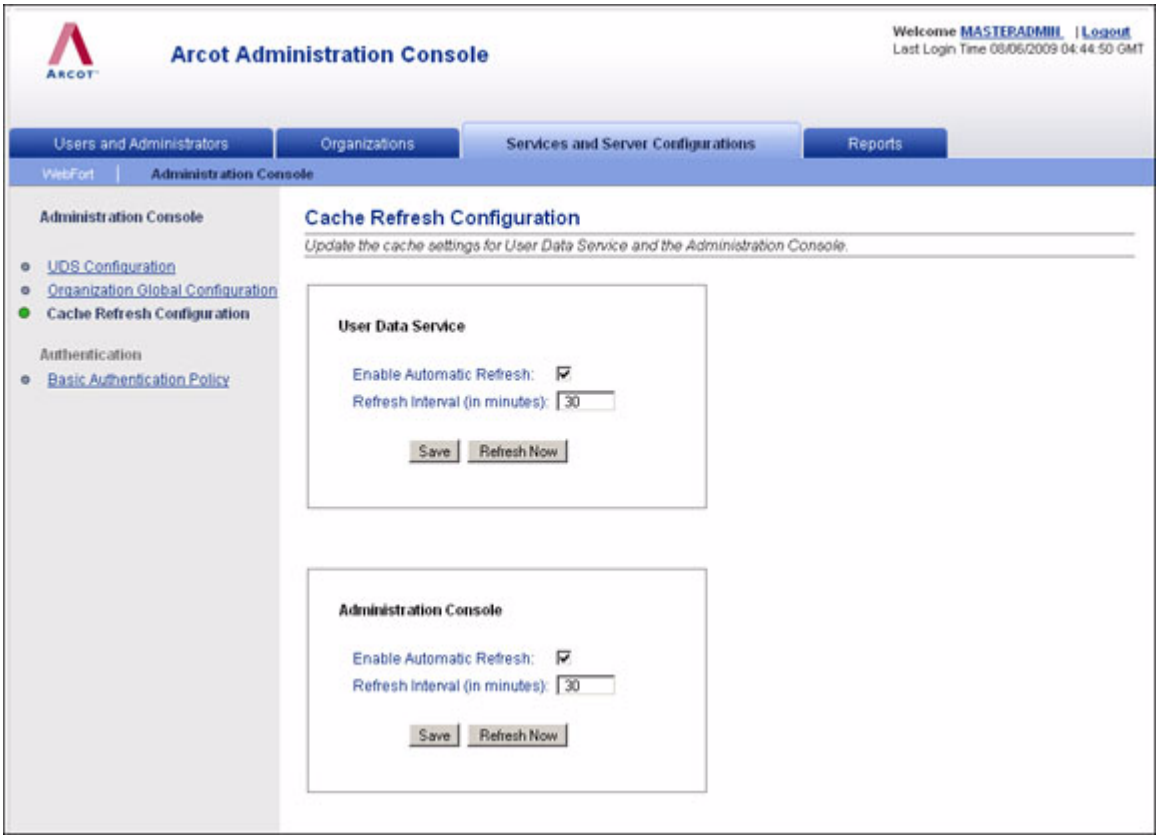
   このオプションはデフォルトで有効になっています。
6. ［**Default Organization**］で、［**Organization Name**］リストからデフォルトの組織として設定する組織を選択します。
7. ［**Save**］をクリックして、このページに対して行った変更を保存します。

   「Successfully updated the global organization configuration」というメッセージが表示されます。

キャッシュ リフレッシュ設定の指定

Administration Console 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。この設定は、［Cache Refresh Configuration］ページ（図 2-6）を使用して更新できます。

図 2-6 ［Cache Refresh Configuration］ページ



UDS または Administration Console の設定を更新する方法

1. 必ず MA としてログインしてください。
2. ［**Services and Server Configurations**］タブを有効化します。
3. タブのサブメニューの［**Administration Console**］オプションをクリックします。

4. タスク ペインで、［**Cache Refresh Configuration**］リンクをクリックして、対応するページ（図 2-6）を表示します。
5. ［**User Data Service**］または［**Administration Console**］セクションで、以下を実行します。
   a. ［**Enable Automatic Refresh**］オプションを選択または選択解除します。
   b. ［**Cache Refresh Interval**］の値を編集します。

      キャッシュは、指定する間隔でリフレッシュされます。たとえば、**60** を入力すると、1 時間ごとに自動的にリフレッシュされます。デフォルト値は 30 分です。
6. ［**Save**］をクリックし、加えた変更を保存します。

基本認証設定の指定

Administration Console にログインしている管理者は、基本認証または WebFort User-Password メカニズムを使用して認証できます。使用されるメカニズムは、以下のように、組織の作成時に選択したオプションによって決定されます。

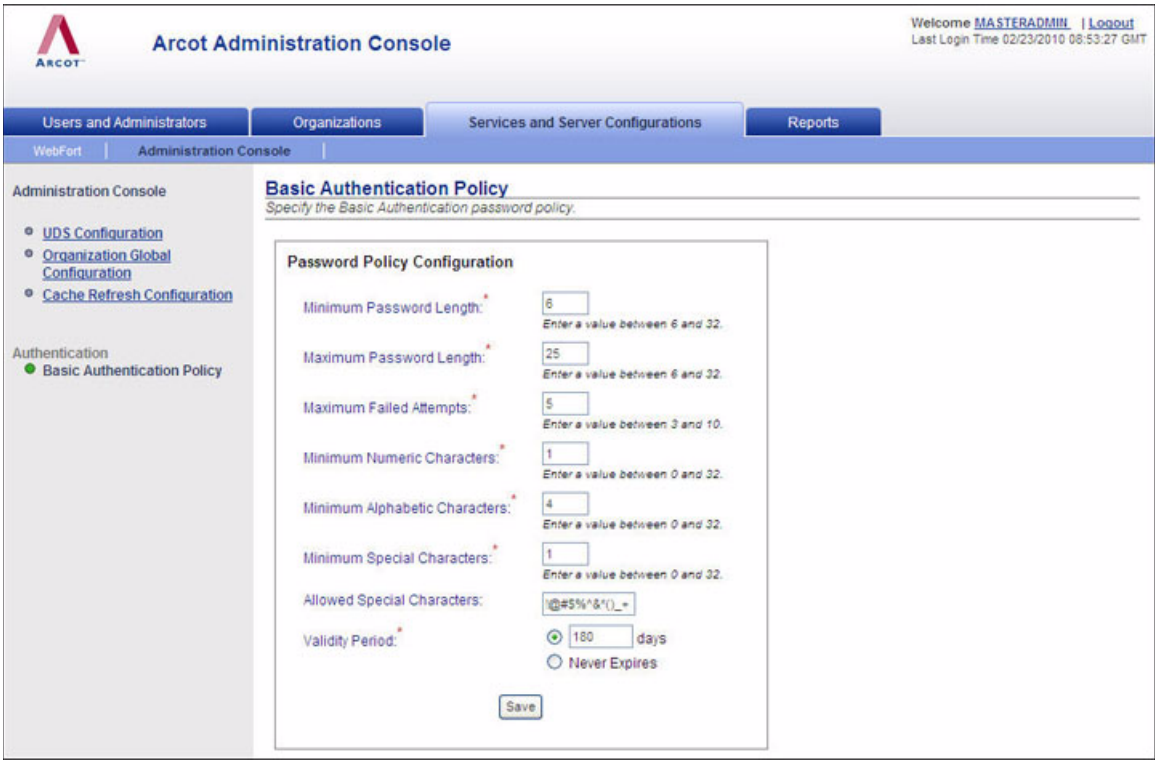
- 組織の作成時に BA を選択した場合、デフォルトの認証を使用するか、基本認証パスワードの指定（グローバル レベル用）またはユーザ名 - パスワード認証ポリシーの設定（組織レベル用）で説明されているように、新しく設定できます。
- WebFort User Password オプションを選択した場合、まず WebFort サーバ（3-38 ページの「WebFort Connectivity の設定」セクションで説明）への接続情報を指定する必要があります。

基本認証パスワードの指定

名前からわかるように、基本認証は、管理者に、ユーザ ID およびパスワードを使用してコンソールにログインさせる認証方式です。

［Basic Authentication］ページ（図 2-7）を使用して、パスワードの長さ、特殊文字の許容文字数、およびアカウントをロックする前に許容される失敗したログインの試行の数などの情報を更新します。

図 2-7 ［Basic Authentication］ページ



基本認証を指定する方法

1. 必ず MA としてログインしてください。
2. ［**Services and Server Configurations**］タブを有効化します。
3. タブのサブメニューの［**Administration Console**］オプションをクリックします。
4. タスク ペインで、［**Basic Authentication**］リンクをクリックして、対応するページ（図 2-7）を表示します。

5. ［**Password Configuration**］セクションの 2-34 ページの表 2-3 にリストされた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。

表 2-3. 基本認証パラメータ

パラメータ	デフォルト値	説明
Minimum Password Length	**6**	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。
Maximum Password Length	**25**	パスワードに含めることのできる最大文字数。6 ～ 32 文字の値を設定できます。
Maximum Failed Attempts	**5**	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。この後に、クレデンシャルがロックされます。3 ～ 10 の値を設定できます。
Minimum Numeric Characters	**1**	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。
Minimum Alphabetic Characters	**4**	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。
Minimum Special Characters	**1**	パスワードに含める必要のある Allowed Special Characters の最小数。値は 0 ～ 32 文字で設定できます。
Allowed Special Characters（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。
Validity Period	**180 日**	パスワードが有効な最大日数。

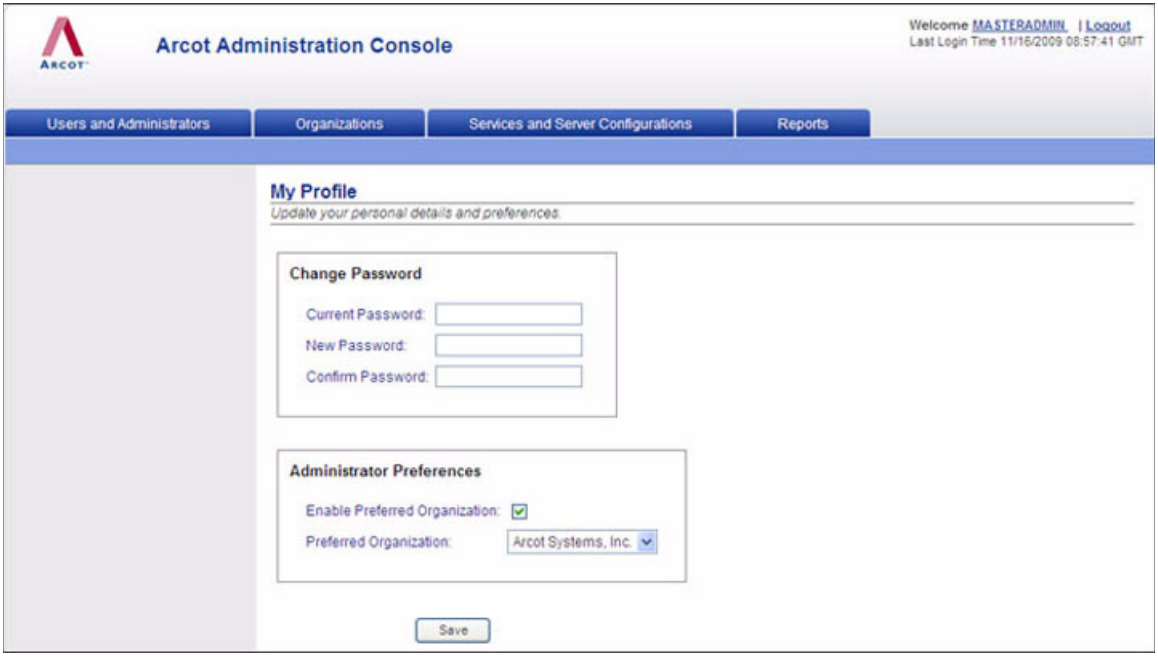
6. ［Save］をクリックして、このページに対して行った変更を保存します。

プロファイル情報の変更

Arcot は、Master Administrator パスワードを定期的に変更し、高いセキュリティを維持することを強く推奨します。これにより、権限のないユーザが MA クレデンシャルを使用して Administration Console にアクセスするのを防ぐことができます。

図 2-8 に示されている［My Profile］ページを使用して、今後実行する可能性のあるすべての管理者関連のタスク用の［Organization］フィールドで、デフォルトで選択される現在のパスワードおよび組織を変更します。

図 2-8 Master Administrator：［My Profile］ページ



現在のパスワードを変更する方法および組織の基本設定を構成する方法

1. コンソール ヘッダの［**MASTERADMIN**］リンクをクリックします。
   図 2-8 に示されているように、［My Profile］ページが表示されます。
2. ［**Change Password**］セクションで、以下を指定します。
   - ［**Current Password**］
   - ［**New Password**］
   - ［**Confirm Password**］フィールドに、再び新しいパスワードを入力します。
3. ［**Administrator Preferences**］セクションで、以下を指定します。
   - ［**Enable Preferred Organization**］オプション（必要に応じて）。
   - ［**Preferred Organization**］（今後実行する可能性のあるすべての管理者関連のタスク用の［Organization］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。
4. ［**Save**］をクリックします。

第 3 章
WebFort サーバ インスタンスの管理

重要 : この章で説明されるすべての設定およびタスクは、**Master Administrator** のみが実行できます。

WebFort サーバがインストールされており、指定されたポートで待ち受けている各システムは、インスタンスと呼びます。各サーバ インスタンスは、ホスト名と一意の数が組み合わされたインスタンス名により、一意に識別されます。

Master Administrator は、各 WebFort 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。ただし、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 （方法の詳細については、「WebFort Connectivity の設定」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にのみ、他の WebFort サーバ インスタンスを管理できます。インスタンスを管理するためのタスクには、以下があります。

- WebFort Connectivity の設定
- サーバ インスタンスのセットアップ
- 信頼されるストアの作成
- 通信プロトコルの設定
- インスタンス統計のモニタリング
- プラグインの登録と更新
- その他の設定
- カスタム ロールの操作

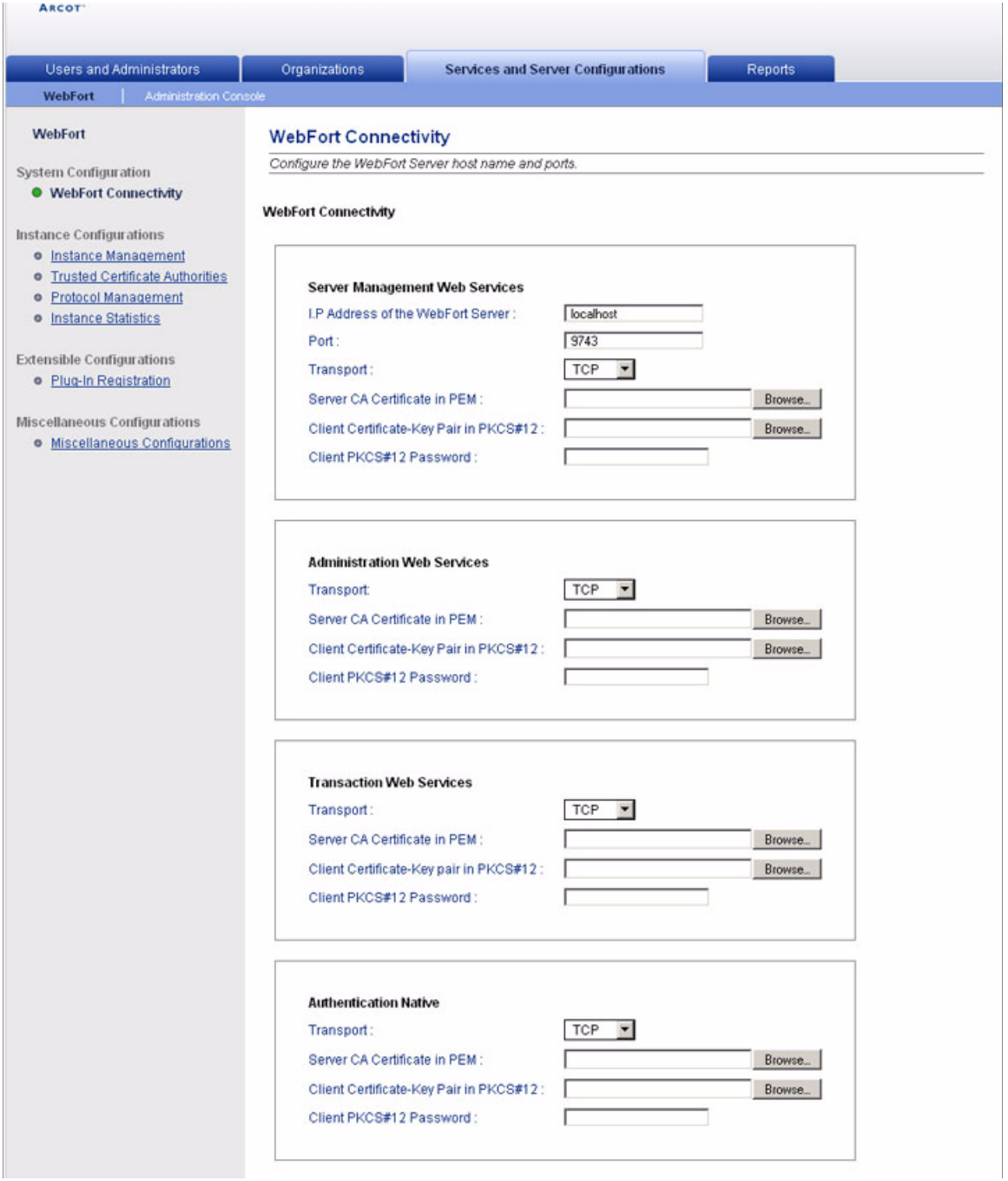
注 : 第 9 章の「システム管理者用のツール」で説明されているように、これらのタスクのうちのいくつかはシステム ツールを使用して実行できます。

WebFort Connectivity の設定

WebFort 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、Administration Console （図 3-1）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。その後、この設定されたインスタンスはシステム内の他のインスタンスをポーリングし、すべてのインスタンスを管理するために必要なすべての情報を収集します。

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。

図 3-1 ［WebFort Connectivity］ページ



WebFort 接続パラメータを指定する方法

1. MA としてログインします。
2. ［**Services and Server Configurations**］タブをアクティブにします。
3. タブのサブメニューで **WebFort** オプションが選択されていることを確認します。
4. 表示されていない場合は、タスク ペイン内の［**WebFort Connectivity**］をクリックすると、対応するページ（図 3-1）が表示されます。
5. 表 3-1 の情報を使用して、［WebFort Connectivity］ページのフィールドを編集します。

表 3-1. 汎用 WebFort 接続パラメータ

フィールド	説明
［IP Address of the WebFort Server］	必要な WebFort サーバ インスタンスをインストールしたシステムの IP アドレスを入力します。 **注：** WebFort 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。
［Port］	プロトコル用のサービスが提供されているポートを入力します。
［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 サービスおよびネイティブ認証）のトランスポート モード（**TCP** または **SSL**）を指定して、指定した WebFort サーバ インスタンスに接続します。
［Server CA Certificate in PEM］	サーバ証明書が含まれる PKCS#12 ストア パスを参照し、アップロードします。
［Client Certificate-Key Pair in PKCS#12］	クライアント証明書および秘密キーが含まれる PKCS#12 ストア パスを参照し、アップロードします。
［Password for Client PKCS#12］	PKCS#12 ストアのパスワードを入力します。

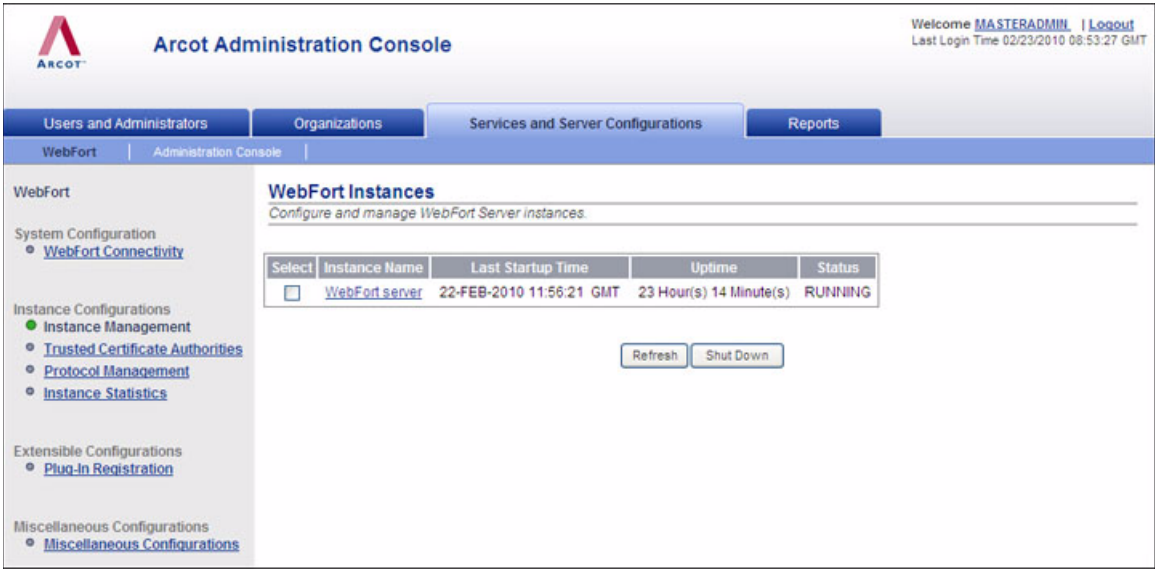
6. ［**Save**］をクリックすると、設定した設定が保存されます。

注： 新しい WebFort 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［**Save**］をクリックする必要があります。これにより、Administration Console にすべてのインスタンスの詳細が登録され、すべての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

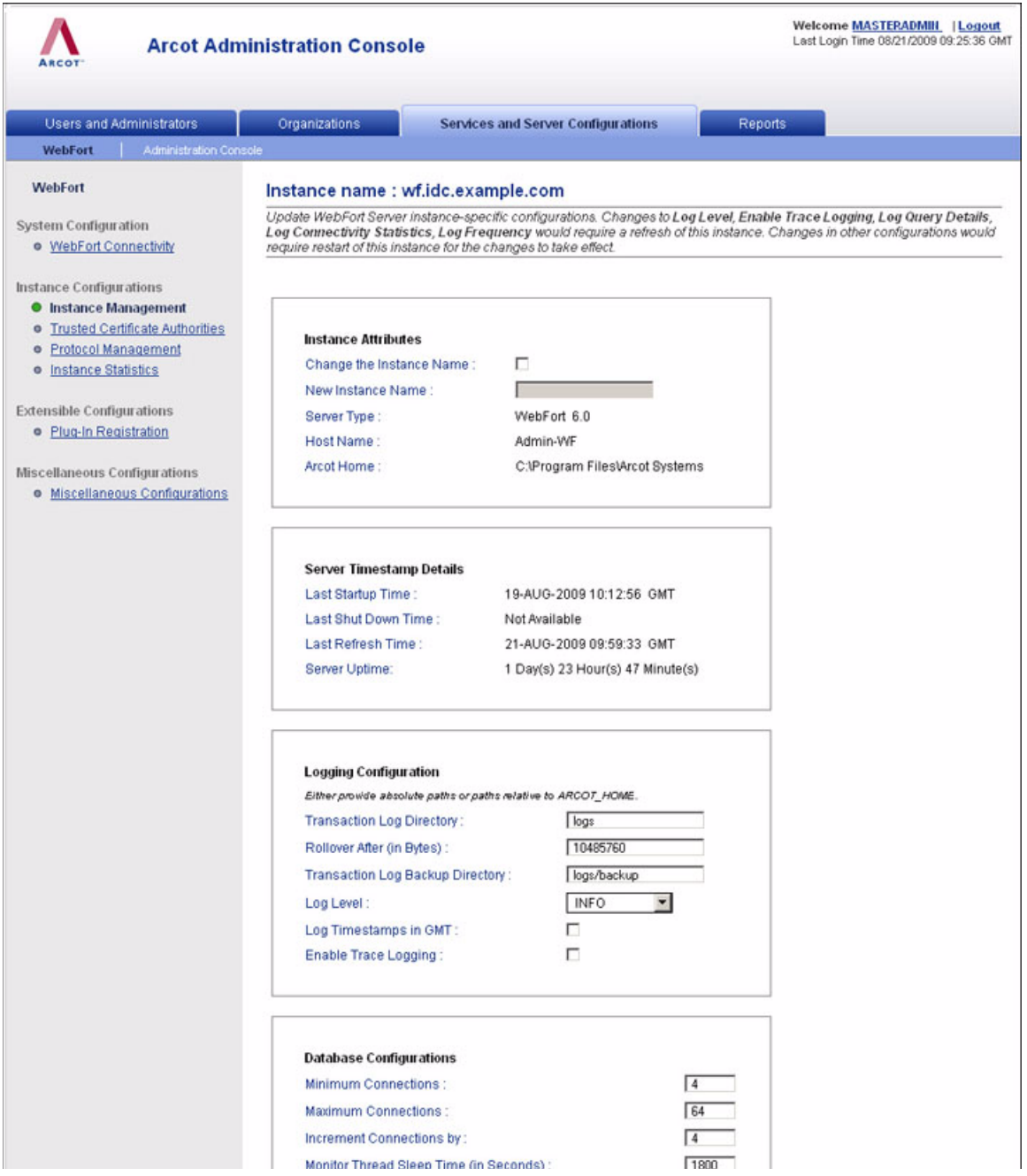
［WebFort Instances］ページ（図 3-2）には、同じ WebFort データベースを Administration Console として共有する、設定されたすべての WebFort サーバ インスタンスがリスト表示されます。［WebFort Connectivity］ページを使用して以前に設定したサーバ インスタンスにより、他のすべてのインスタンスに関する必要な情報がポーリングにより収集され、Administration Console に渡されます。その後、これらの情報が Administration Console によりこのページに表示されます。

図 3-2 ［WebFort Instances］ページ



WebFort 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。［WebFort Instances］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、次に、インスタンス ページ上で必要な変更を行う必要があります。図 3-3 はインスタンス固有のページの例を示します。

図 3-3 インスタンス固有のページ



典型的なインスタンス管理操作には、次があります。

- インスタンスのリフレッシュまたはシャットダウン
- インスタンス名の変更
- WebFort サーバ ログ記録設定の管理
- データベース パラメータの設定
- 接続統計ログ記録の有効化
- インスタンス タイム スタンプの詳細の読み取り

注： また、このセクションで説明されている操作のほとんどは、`arwfclient` コマンド ライン ツールを使用することにより実行できます。詳細については、9-243 ページの「arwfclient」を参照してください。

インスタンスのリフレッシュまたはシャットダウン

WebFort サーバ インスタンスをリフレッシュまたはシャットダウンする方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. ［**Instance Configurations**］セクションの［**Instance Management**］リンクをクリックすると、［WebFort Instances］ページ（図 3-2）が表示されます。
4. ［**Select**］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。
5. 必要なアクションを実行します。
   - ［**Refresh**］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。
   - ［**Shut Down**］をクリックすると、選択したインスタンスが停止されます。

注： Administration Console を使用して WebFort サーバ インスタンスをシャットダウンできない場合は、arwfclient ツールを使用してサーバ インスタンスをシャットダウンします。

サーバ インスタンスの再起動

Windows の場合

Windows 上のサーバ インスタンスを開始する方法

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**］をダブルクリックします。
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

UNIX ベースのプラットフォーム上のサーバ インスタンスを開始する方法

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. 以下のディレクトリに移動します。
   < *インストール ディレクトリ* >/arcot/bin/
3. 以下のコマンドを実行します。

```
./webfortserver start
```

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、WebFort 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。インスタンスを容易に識別するために、Arcot は、ユーザが各インスタンスに適切な名前を設定することを推奨します。

WebFort サーバ インスタンスのインスタンス名を変更する方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。

4. ［**Instance Configurations**］セクションの［**Instance Management**］リンクをクリックすると、［WebFort Instances］ページ（図 3-2）が表示されます。
5. ［**Instance Name**］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（図 3-3）が表示されます。
6. ［**Instance Attributes**］セクションで、［**Change the Instance Name**］チェック ボックスをオンにします。
7. ［**New Instance Name**］フィールドに新しい名前を入力します。
8. ［**Save**］をクリックすると、変更内容が保存されます。
9. 変更を行った WebFort サーバ インスタンスをリフレッシュします。これを行う方法の詳細については、「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

WebFort サーバ ログ記録設定の管理

WebFort 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。

- WebFort ログ ファイル（`arcotwebfort.log`）
- WebFort スタートアップ ログ ファイル（`arcotwebfortstartup.log`）
- WebFort 統計ログ ファイル（`arcotwebfortstats.log`）
- Administration Console 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、付録 A の 「WebFort のログ」を参照してください。

インスタンス固有のページ（図 3-3）を使用することによって、インスタンス用の WebFort ログ ファイルおよび WebFort 統計ログ ファイルのログ記録設定を個別に管理できます。WebFort サーバ ログ設定を変更するには、以下の手順に従います。

注： Administration Console を使用して WebFort 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、「接続統計ログ記録の有効化」を参照してください。

1. MA としてログインします。

2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブ メニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Instance Configurations**］セクションの［**Instance Management**］リンクをクリックすると、［WebFort Instances］ページ（図 3-2）が表示されます。
5. ［**Instance Name**］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（図 3-3 を参照）が表示されます。
6. 必要に応じて［**Logging Configurations**］セクション内のフィールドを編集します。表 3-2 は、このセクションのフィールドについて説明します。

表 3-2. ログ設定フィールド

フィールド	説明
［Transaction Log Directory］	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。
［Rollover After (in Bytes)］	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。
［Transaction Log Backup Directory］	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 • WARNING • INFO • DETAIL ログ レベルの詳細については、A-253 ページの「サポートされる重大度レベル」を参照してください。
GMT でのタイム スタンプのログ記録	WebFort 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。
［Enable Trace Logging］	WebFort 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。

7. ［**Save**］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 WebFort サーバ インスタンスをリフレッシュします。これを行う方法の詳細については、「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

データベース パラメータの設定

WebFort は、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避けるために、接続プーリングを使用します。インスタンス固有のページ（図 3-3）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。［**Instance Statistics**］ページ（「インスタンス統計のモニタリング」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。

データベース設定パラメータを変更する方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Instance Configurations**］セクションの［**Instance Management**］リンクをクリックすると、［WebFort Instances］ページ（図 3-2）が表示されます。
5. ［**Instance Name**］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（図 3-3 を参照）が表示されます。
6. 必要に応じて［**Database Configurations**］セクション内のフィールドを編集します。表 3-3 は、このセクションのフィールドについて説明します。

表 3-3. WebFort サーバとデータベースとの間の接続プーリング パラメータ

フィールド	説明
[Minimum Connections]	サーバの起動時に、WebFort 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。
[Maximum Connections]	WebFort 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**：データベースによって許可される接続数には制限があります。また、この制限はこのパラメータよりも優先されます。詳細については、データベース ベンダーのドキュメントを参照してください。

表 3-3. WebFort サーバとデータベースとの間の接続プーリング パラメータ（続き）

フィールド	説明
[Increment Connections By]	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**：接続の総数が、接続の最大数を超えることはできません。
[Monitor Thread Sleep Time (in Seconds)]	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。
[Monitor Thread Sleep Time in Fault Condition (in Seconds)]	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。
[Connection Retry Sleep Time (in Seconds)]	データベースへの接続再試行を継続して行う間隔を入力します。
[Log Query Details]	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。
[Monitor Database Connectivity]	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。
[Auto-Revert to Primary]	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。

7. ［**Save**］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 WebFort サーバ インスタンスをリフレッシュします。これを行う方法の詳細については、「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

接続統計ログ記録の有効化

［**Statistics Configurations**］セクションで提供されているオプションを使用することにより、`arcotwebfortstats.log` ファイルにログ記録される、指定したインスタンスの接続統計を制御できます。［**Instance Statistics**］ページ（「インスタンス統計のモニタリング」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。

WebFort サーバで統計データをログ記録する方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。

3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Instance Configurations**］セクションの［**Instance Management**］リンクをクリックすると、［WebFort Instances］ページ（図 3-2）が表示されます。
5. ［**Instance Name**］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（図 3-3 を参照）が表示されます。
6. ［**Statistics Configurations**］セクションで、以下を行います。
   - ［**Log Connectivity Statistics**］チェック ボックスをオンにして、WebFort サーバですべての接続統計がログ記録されるようにします。
   - ［**Log Frequency (in Minutes)**］フィールドに、統計がログ記録される間隔を入力します。たとえば、「30」と入力すると、統計が 30 分ごとにログ記録されます。
7. ［**Save**］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 WebFort サーバ インスタンスをリフレッシュします。これを行う方法の詳細については、「インスタンスのリフレッシュまたはシャットダウン」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、［**Server Timestamp Details**］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。表 3-4 は、これらの詳細について説明します。

表 3-4. サーバ タイム スタンプの詳細

フィールド	説明
［Last Startup Time］	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。
［Last Shutdown Time］	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。
［Last Refresh Time］	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。
［Server Up Time］	サーバ インスタンスが実行されている期間です。

信頼されるストアの作成

信頼されるストアを作成して、SSL ベースの通信中に WebFort サーバ インスタンスをそのクライアントに対して認証することができます。信頼されるストアは、Administration Console および Java SDK を含む WebFort クライアントによって信頼された CA ルート証明書が含まれるキー ファイルです。

各 WebFort サーバ インスタンスは、個別の信頼されるストアを使用することにより、異なる証明書を提示できるように設定できます。［Trusted Certificate Authorities］ページ（図 3-4）を使用することにより、信頼されるストアを作成し、新しいルート証明書を信頼されるストアに追加できます。

図 3-4 ［Trusted Certificate Authorities］ページ

現在のサーバ インスタンス用の信頼されるストアを作成する方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。

3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Instance Configurations**］セクションの［**Trusted Certificate Authorities**］リンクをクリックすると、［Trusted Certificate Authorities］ページ（図 3-4）が表示されます。
5. ［**Name**］フィールドに、作成する信頼されるストアの名前を入力します。
6. 対応する［**Browse**］ボタンをクリックすると、信頼された CA のルート証明書がアップロードされます。［**Add More**］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。
7. 必要な証明書がすべてアップロードされたら、［**Save**］をクリックします。

通信プロトコルの設定

［Protocol Configuration］ページ（図 3-5）を使用することにより、認証と管理の目的のための WebFort サーバ インスタンスと通信するために、Administration Console、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。サーバ インスタンスが各プロトコルを待ち受けるポートもこのページで設定できます。

図 3-5 ［Protocol Configuration］ページ

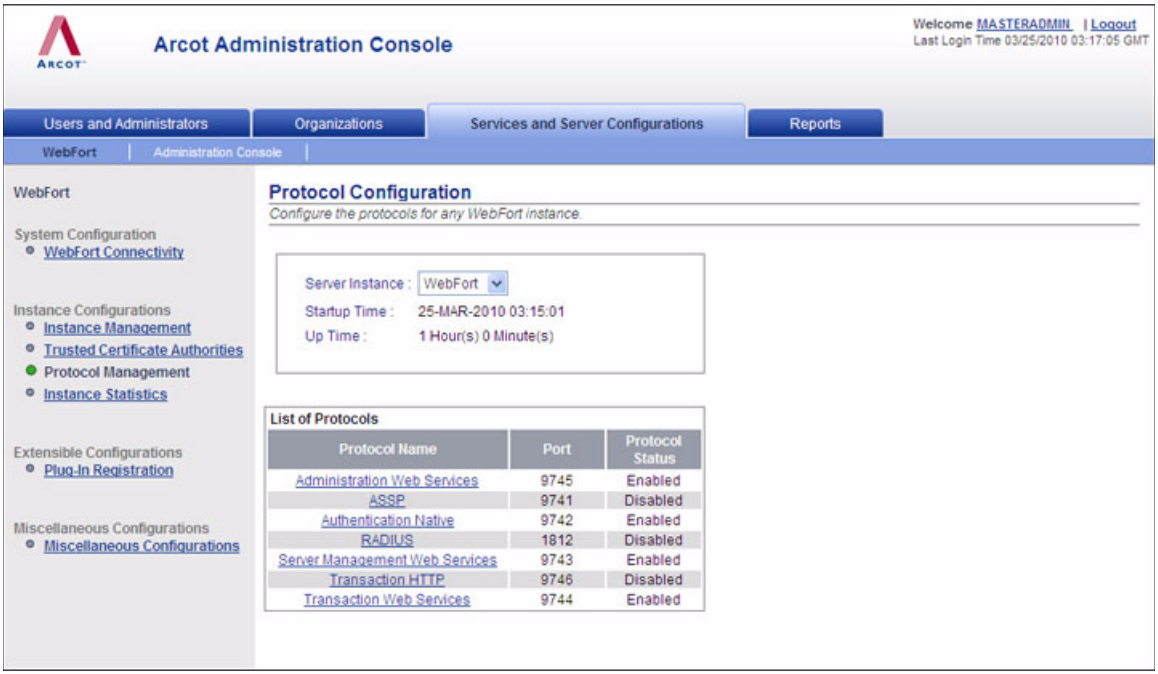


表 3-5 は、［Protocol Configuration］ページに表示されるプロトコルについて説明し、それらのデフォルト ポート番号を示します。

表 3-5. WebFort プロトコル

プロトコル	デフォルト ポート番号	説明
サーバ管理 Web サービス	9743	Administration Console および `arwfclient` 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 WebFort サーバ インスタンスと通信します。
管理 Web サービス	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。
トランザクション Web サービス	9744	このプロトコルは、WebFort サーバ インスタンスに接続するために、認証および発行 Web サービスによって使用されます。

表 3-5. WebFort プロトコル

プロトコル	デフォルト ポート番号	説明
ネイティブ認証	9742	これは、認証用の専用バイナリ WebFort プロトコルです。このプロトコルは、認証 Java SDK によって使用されます。
トランザクション HTTP	9746	このプロトコルは、基本 HTTP 形式でデータを受信します。このプロトコルは、ArcotOTP プロビジョニングおよび ArcotID キーバッグ管理操作に使用されます。 **注：** 他の汎用 WebFort 操作には公開されません。
RADIUS	1812	このプロトコルは、WebFort 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ます。 **注：** RADIUS をサポートするように設定すると、WebFort サーバは RADIUS サーバとして動作します。

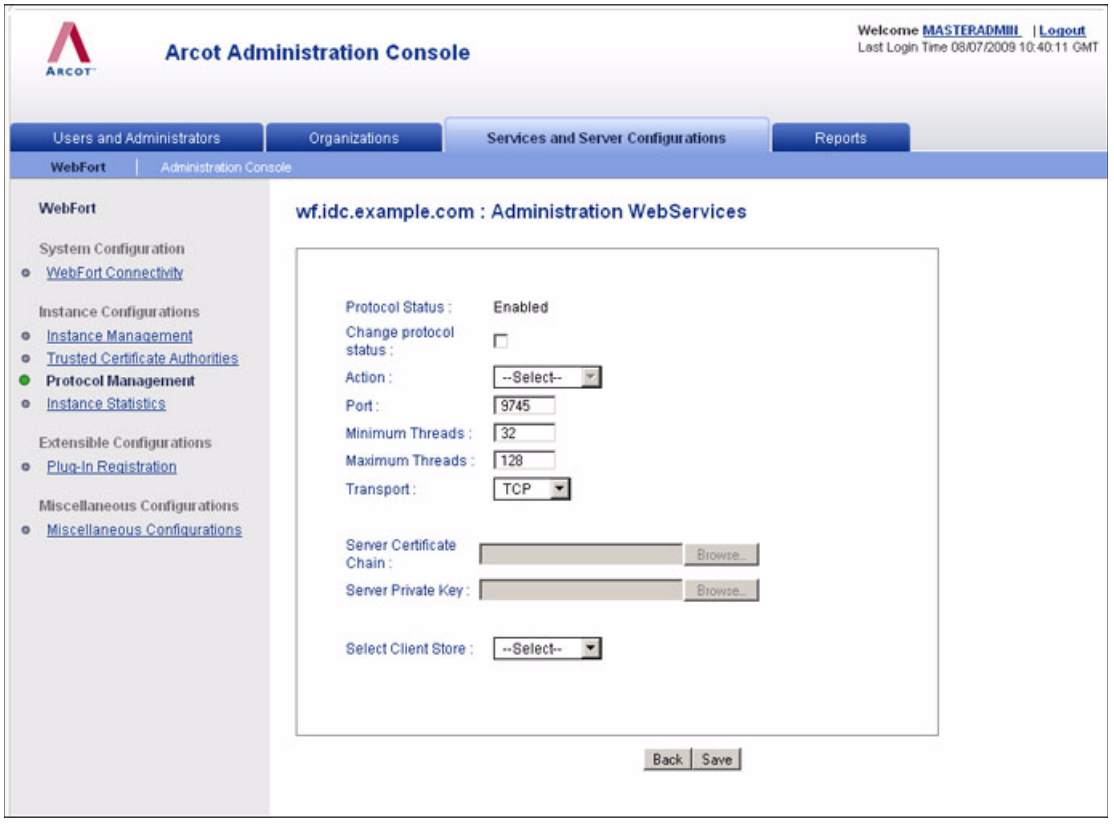
WebFort ネットワーク プロトコルを設定する方法

注： ［**Instance Statistics**］ページ（「インスタンス統計のモニタリング」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. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Instance Configurations**］セクションの［**Protocol Management**］リンクをクリックすると、［Protocol Configuration］ページ（図 3-5）が表示されます。
5. プロトコルを設定する対象の**サーバ インスタンス**を選択します。
6. ［**List of Protocols**］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 （たとえば、図 3-6 は、管理 Web サービス用のプロトコル設定ページを示します)。

図 3-6 ［Protocol Configuration］ページ：管理 Web サービス



7. 必要に応じて、ページ上でフィールドを編集します。表 3-6 は、これらのフィールドについて説明します。

表 3-6. WebFort プロトコルを設定するためのフィールド

フィールド	説明
[Protocol Status]	プロトコルが **Enabled** または **Disabled** のいずれであるかを示します。
[Change the Protocol Status] **[Action]**	[**Change the Protocol Status**] オプションを選択して [**Action**] リストを有効にし、新しいステータスを [**Action**] ドロップダウン リストから選択します。 **注：** サーバ管理プロトコルは無効にできません。このため、このプロトコルに対しては、これらのオプションは表示されません。
[Port]	プロトコル サービスが利用可能なポート番号を入力します。
[Minimum Threads]	クライアントと WebFort サーバとの間で維持されるスレッドの最小数を指定します。
[Maximum Threads]	クライアントと WebFort 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。
[Transport]	データ転送のモードを指定します。 **注：** RADIUS を設定している場合、このフィールドには UDP（User Datagram Protocol）を指定します。これは RADIUS によってサポートされる標準的な転送プロトコルです。 指定できる値は以下のとおりです。 • **SSL**：SSL（Secure Sockets Layer）は PKI を使用して、転送中のデータを暗号化および復号化します。 • **TCP**：TCP（Transmission Control Protocol）モードは WebFort RADIUS プロトコル以外のすべての WebFort プロトコルでサポートされています。
[Server Certificate Chain]	対応するフィールドの [**Browse**] ボタンをクリックすると、証明書チェーンがアップロードされます。 このサーバ証明書チェーンは SSL 転送セキュリティ モードによって使用されます。

表 3-6. WebFort プロトコルを設定するためのフィールド（続き）

フィールド	説明
[Server Private Key]	対応するフィールドの［Browse］ボタンをクリックすると、証明書チェーンがアップロードされます。 このサーバ秘密キーは SSL 転送セキュリティ モードによって使用されます。
[Select Client Store]	信頼された CA のルート証明書が含まれる信頼されるストアを選択します。 信頼されるストアを設定する方法の詳細については、「信頼されるストアの作成」を参照してください。

8. ページ上で設定を完了したら、［**Save**］をクリックします。

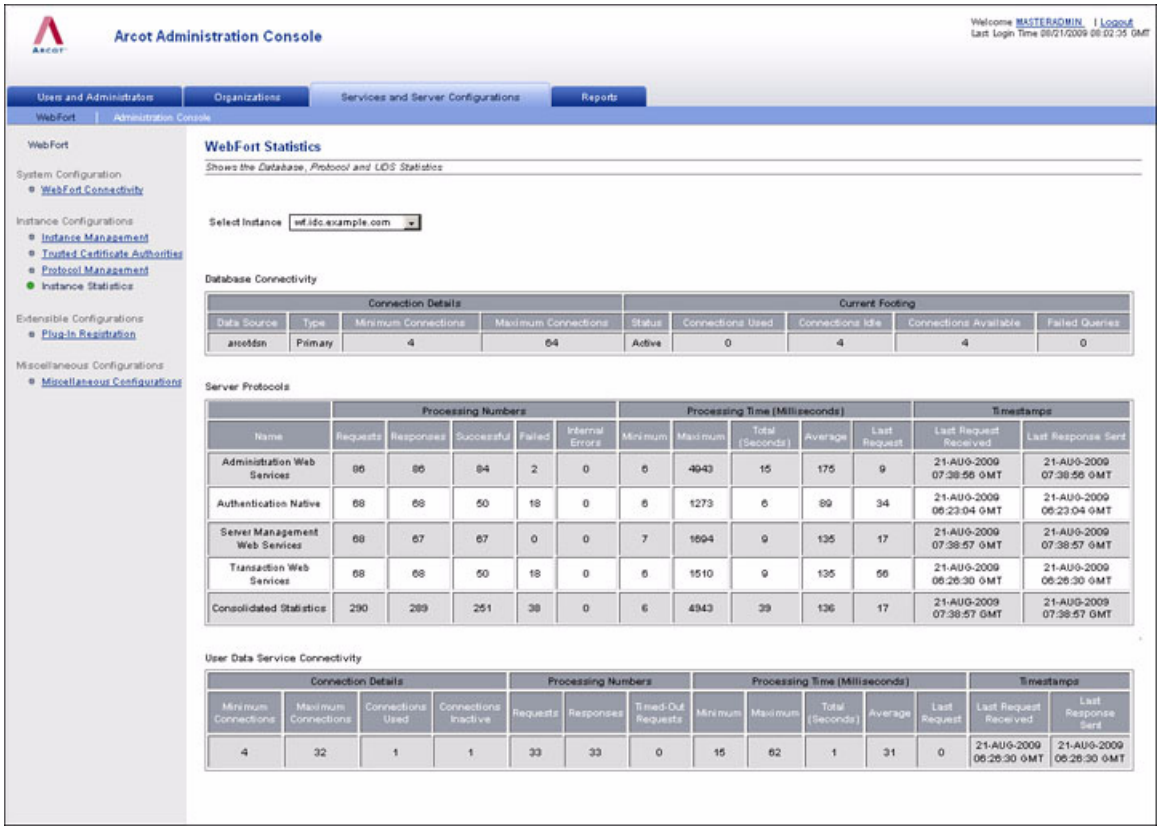
注： 各プロトコルを個別に設定する必要があります。

9. 変更を行った WebFort サーバ インスタンスをリフレッシュします。これを行う方法の詳細については、「サーバ インスタンスの再起動」を参照してください。

インスタンス統計のモニタリング

Administration Console の［WebFort Statistics］ページ（図 3-7）を使用すると、各サーバ インスタンスの WebFort 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 WebFort プロトコルを監視できます。これらの統計を使用することによって、以前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。

図 3-7 ［WebFort Statistics］ページ



インスタンスの統計詳細を表示する方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Instance Configurations**］セクションの［**Instance Statistics**］リンクをクリックすると、［WebFort Statistics］ページ（図 3-7）が表示されます。
5. 詳細を監視するインスタンスを［**Select Instance**］リストから選択します。

   インスタンスの詳細が、以下のように分類されて表示されます。

- データベース接続性
- サーバ プロトコル
- ユーザ データ サービス接続性

データベース接続性

表 3-7 はデータベース接続情報を示します。

表 3-7. インスタンスのデータベース接続性の詳細

フィールド	説明
[Connection Details]	
[Data Source]	選択した WebFort 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。
[Minimum Connections]	WebFort 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。
[Maximum Connections]	WebFort 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。
[Current Footing]	
[Status]	プールがアクティブか非アクティブかを示します。
[Connections Used]	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。
[Connections Available]	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。
[Failed Queries]	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

表 3-8 は、設定されている各 WebFort 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。

表 3-8. インスタンスのプロトコル情報

フィールド	説明
[Processing Numbers]	
[Name]	設定されているプロトコルの名前です。
[Requests]	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。
[Responses]	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。
[Successful]	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。
[Internal Errors]	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。
[Processing Time (Milliseconds)]	
[Minimum]	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。
[Maximum]	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。
[Total (Seconds)]	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。
[Average]	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。
[Last Request]	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。
[Timestamps]	
[Last Request Received]	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。
[Last Response Sent]	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。

ユーザ データ サービス接続性

表 3-9 は、WebFort 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。

表 3-9. インスタンスの UDS 接続性の詳細

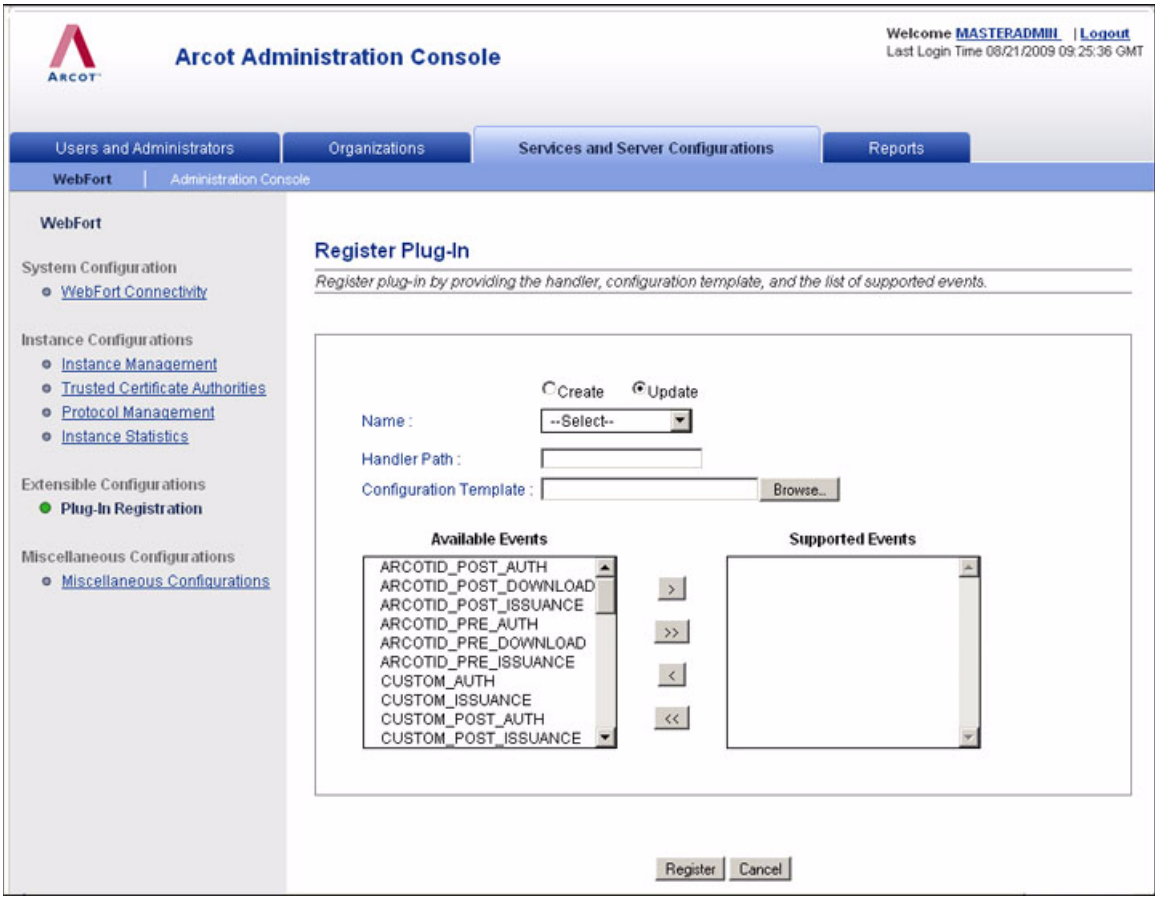
フィールド	説明
[Connection Details]	
[Minimum Connections]	サーバ インスタンスと UDS との間に存在する必要がある接続の最小数です。
[Maximum Connections]	サーバ インスタンスと UDS との間に存在できる接続の最大数です。
[Connections Used]	サーバ インスタンスと UDS との間に確立されている接続の数です。
[Connections Inactive]	サーバ インスタンスと UDS との間のアイドル接続の数です。
[Processing Numbers]	
[Requests]	サーバ インスタンスから UDS へのリクエストの総数です。
[Responses]	サーバ インスタンスによって UDS から受信されたレスポンスの総数です。
[Timed-Out Requests]	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。
[Processing Time (Milliseconds)]	
[Minimum]	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。
[Maximum]	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。
[Total (Seconds)]	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。
[Average]	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。
[Last *Request*]	UDS によって受信された最後のリクエストを処理するために費やされた時間です。
[Timestamps]	
[Last Request Received]	最後のリクエストが UDS によって受信されたときのタイム スタンプです。
[Last Response Sent]	最後のレスポンスが UDS によって送信されたときのタイム スタンプです。

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、C または C++ で開発されています。プラグインを使用すると、WebFort サーバの機能を拡張できます。プラグインは WebFort 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する必要があります。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。そうするには、［Register Plug-In］ページ（図 3-8）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。

図 3-8 ［Register Plug-In］ページ



プラグインの登録

システムに新しいプラグインを登録する方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Extensible Configurations**］セクションの［**Plug-In Registration**］リンクをクリックすると、［Register Plug-In］ページ（図 3-8）が表示されます。

5. ［**Create**］オプションを選択します。
6. ［**Name**］にプラグインの名前を指定します。
7. ［**Handler Path**］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、WebFort からアクセスできる必要があります。

   UNIX プラットフォームで、このファイルが `LD_LIBRARY_PATH` によって指定されたパス内で利用できる場合、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内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。
8. ［**Configuration Template**］の［**Browse**］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、Administration Console のプラグイン設定画面を表示するために使用されます。

注： Arcot はサンプルのプラグイン テンプレート ファイルを提供しています。

9. プラグインに関連付けるイベントを［**Available Events**］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［**Supported Events**］リストに追加されます。

注： ［**Available Events**］リストには、WebFort で利用可能なすべてのイベントが表示され、［**Supported Events**］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。

10. ［**Register**］をクリックすると、WebFort のすべてのインスタンスがプラグインに登録されます。
11. 展開されているすべての WebFort サーバ インスタンスを再起動します。これを行う方法の詳細については、「サーバ インスタンスの再起動」を参照してください。

プラグイン設定の更新

既存のプラグイン設定を更新する方法

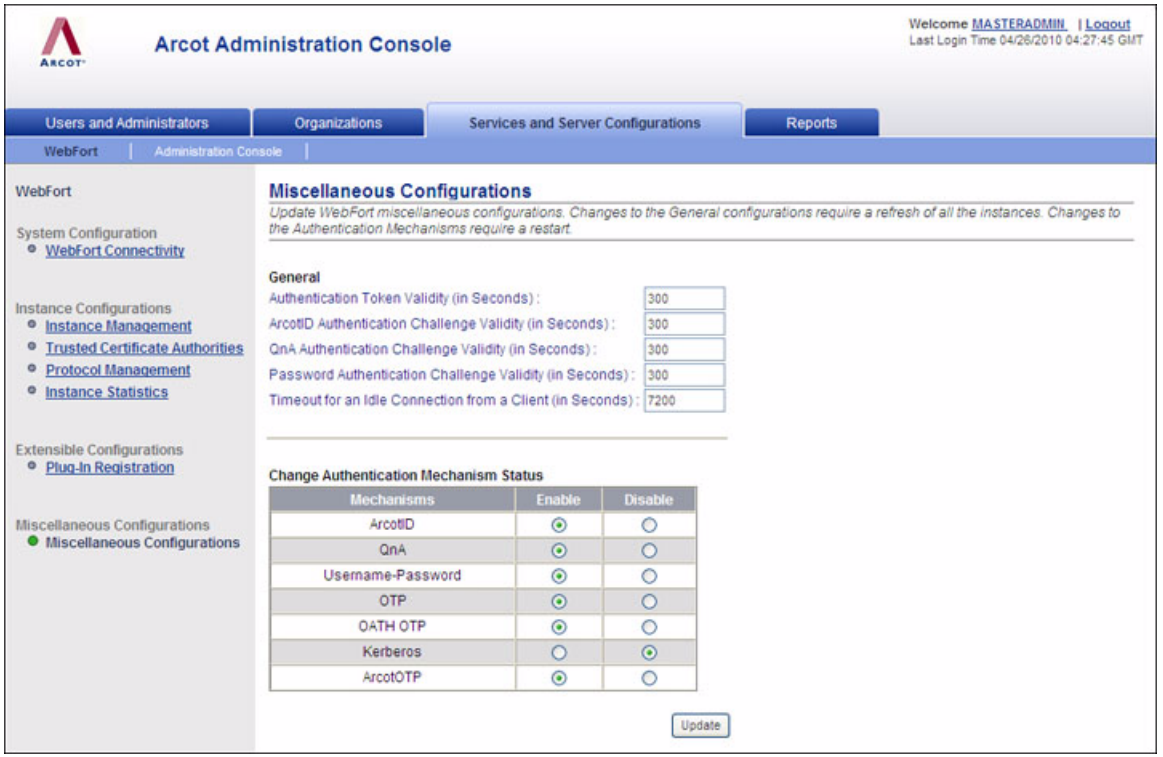
1. MA としてログインします。
2. ［Register Plug-In］ページ（図 3-8）に移動します。
3. ［**Update**］オプションを選択します。
4. ［**Name**］リストから必要なプラグインを選択します。
5. プラグインの［**Handler Path**］および（または）［**Configuration Template**］設定を更新します。
6. プラグインに関連付けられているイベントを更新します。
7. ［**Register**］をクリックすると、変更が更新されます。
8. 展開されているすべての WebFort サーバ インスタンスを再起動します。これを行う方法の詳細については、「サーバ インスタンスの再起動」を参照してください。

その他の設定

［Miscellaneous Configurations］ページ（図 3-9）を使用すると、状況に応じて更新する必要がある以下の設定（WebFort サーバのすべてのインスタンスに適用可能）を変更できます。

- 認証トークンの有効性
- ArcotID 認証チャレンジの有効性
- Q&A チャレンジの有効性
- 部分パスワード認証が使用される場合、Password 認証チャレンジの有効性
- アイドル クライアント接続のタイムアウト
- 認証メカニズム（ArcotID、Q&A（Questions and Answers）、ユーザ名 - パスワード、ワンタイム パスワード （OTP）、OATH OTP、Kerberos、ArcotOTP など）の有効化または無効化

図 3-9 ［Miscellaneous Configurations］ページ



その他の設定を変更する方法

1. MA としてログインします。
2. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Miscellaneous Configurations**］セクションの［**Miscellaneous Configurations**］リンクをクリックすると、対応するページ（図 3-9）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。表 3-10 は、このページのフィールドについて説明します。

表 3-10. その他の WebFort 設定

フィールド	デフォルト値	説明
[General]		
[Authentication Token Validity (in Seconds)]	300	WebFort 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。
[ArcotID Authentication Challenge Validity (in Seconds)]	300	WebFort によって発行される ArcotID 認証チャレンジの有効期間を指定します。
[QnA Authentication Challenge Validity (in Seconds)]	300	WebFort によって発行される Q&A 認証チャレンジの有効期間を指定します。
[Password Authentication Challenge Validity (in Seconds)]	300	WebFort によって発行されるユーザ名 - パスワード認証チャレンジの有効期間を指定します。
[Timeout for an Idle Connection from a Client (in Seconds)]	7200	アイドル クライアント接続が閉じられるまでの時間を指定します。
[Change Authentication Mechanism Status]		
[ArcotID]	有効	WebFort が ArcotID 認証機能を提供するかどうかを指定します。
[Q&A]	有効	WebFort が Q&A 認証機能を提供するかどうかを指定します。
[Username-Password]	有効	WebFort が基本的なユーザ名 - パスワード認証機能を提供するかどうかを指定します。
[OTP]	有効	WebFort 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。
[OATH OTP]	有効	WebFort が OATH OTP ベースの認証をサポートするかどうかを指定します。
[Kerberos]	無効	WebFort 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。
[ArcotOTP]	有効	WebFort が ArcotOTP ベースの認証をサポートするかどうかを指定します。

6. [**Update**] をクリックすると、変更が保存されます。

7. ［**General**］設定を変更したら、展開したすべての WebFort 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、WebFort サーバを再起動する必要があります。これを行う方法の詳細については、「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

カスタム ロールの操作

この概念の詳細については、1-15 ページの「カスタム ロール」を参照してください。このセクションでは、以下の手順について説明します。

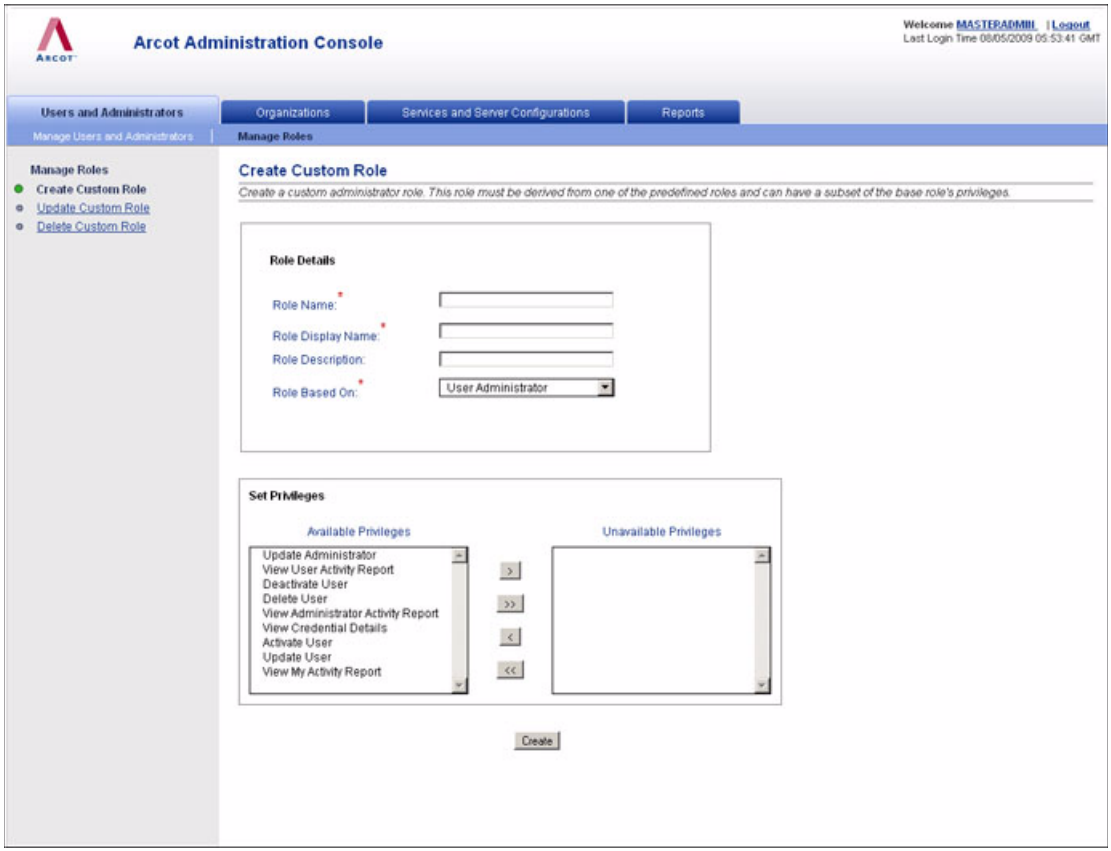
- カスタム ロールの作成
- カスタム ロール情報の更新
- カスタム ロールの削除

カスタム ロールの作成

カスタム ロールを作成する方法

1. ［**Users and Administrators**］タブをアクティブにします。
2. サブメニューから［**Manage Roles**］リンクをクリックすると、［Create Custom Role］ページ（図 3-10）が表示されます。

図 3-10 ［Create Custom Role］ページ



3. ［**Role Details**］セクションで、以下の情報を指定します。
   - ［**Role Name**］：新規ロールを識別する一意の名前です。この名前は、この新規ロールを認証し許可するために WebFort によって内部的に使用されます。
   - ［**Role Display Name**］：Administration Console の他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です。
   - ［Role Description］：以降での参照に役立つ、ロールに関連する情報です。
   - ［Role Based On］：このカスタム ロールの派生元の既存のロールです。
4. ［**Set Privileges**］セクションで、以下の手順に従います。
   a. ［**Available Privileges**］リストで、カスタム ロールに関して無効にすることが必要なすべての権限を選択します。

このリストには、［**Role Based On**］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。

ヒント：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［**Unavailable Privileges**］リストに移動されます。

5. ［**Create**］をクリックすると、カスタム ロールが作成されます。

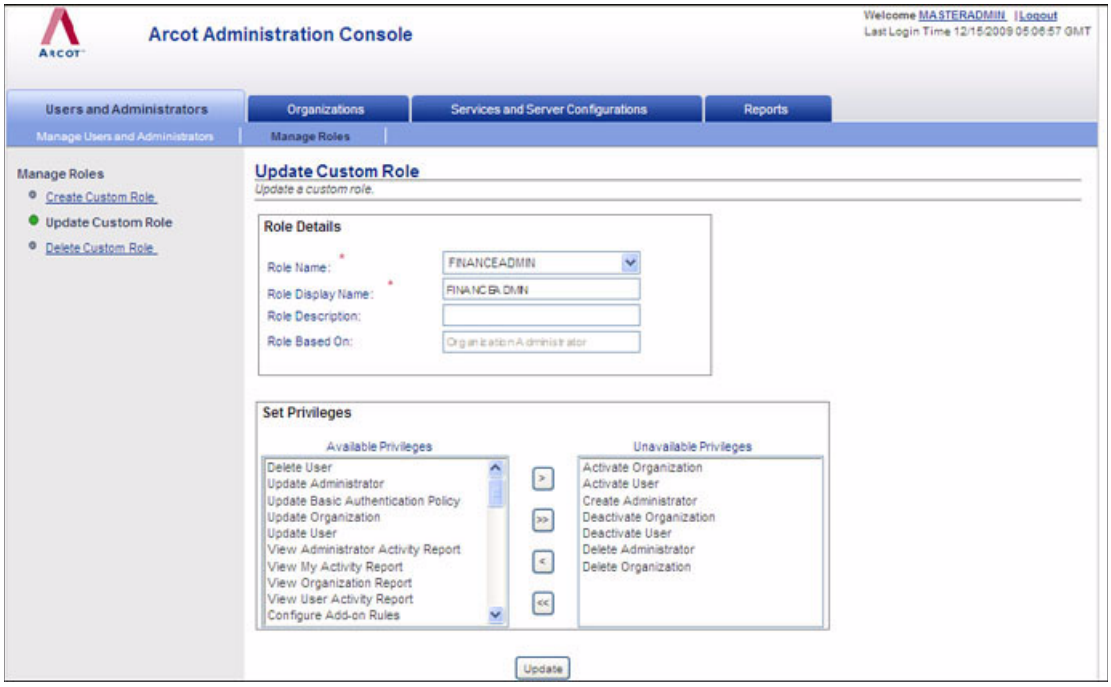
カスタム ロール情報の更新

既存のカスタム ロールの定義を更新する方法

1. ［**Users and Administrators**］タブをアクティブにします。
2. サブメニューから、［**Manage Roles**］リンクをクリックします。
3. ［Tasks］メニューから、［**Update Custom Role**］リンクをクリックします。

   図 3-11 に示されるような［Update Custom Role］ページが表示されます。

図 3-11 ［Update Custom Role］ページ



4. 更新する［**Role Name**］を選択します。
5. ［**Role Details**］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. ［**Set Privileges**］セクションで、以下の手順に従います。
   a. ［**Available Privileges**］リストで、このロールに関して無効にすることが必要なすべての権限を選択します。

      このリストには、［**Role Based On**］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。

      または

   b. ［**Unavailable Privileges**］リストで、このロールに関して有効にする権限を選択します。

このリストには、［**Role Based On**］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。

	ヒント :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。

c. ［**>**］ボタンをクリックすると、選択した権限が［**Unavailable Privileges**］リストに移動されます。

7. ［**Update**］をクリックすると、カスタム ロールの定義が更新されます。

カスタム ロールの削除

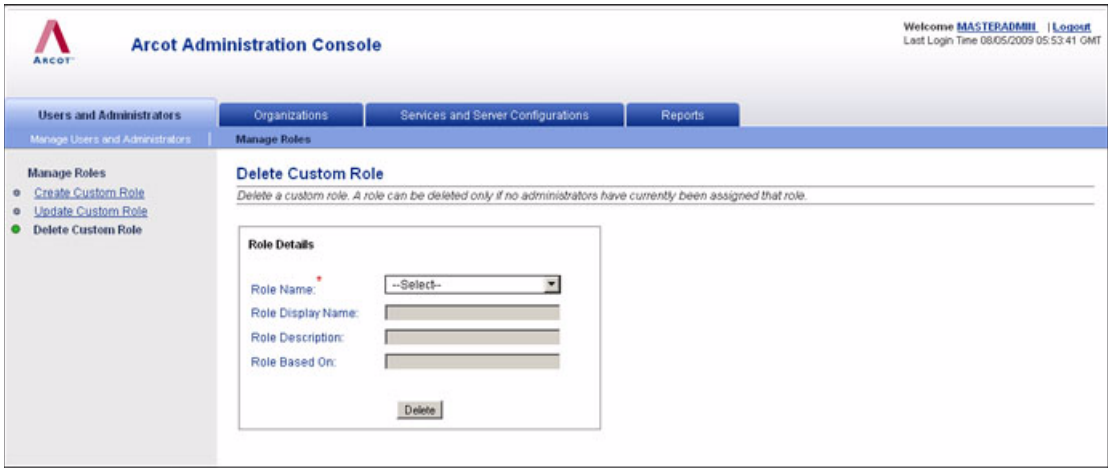
	重要 : 管理者に現在割り当てられるカスタム ロールを削除することは *できません*。そのようなロールを削除する必要がある場合、最初に、［Update Administrator］ページを使用して、このロールが割り当てられているすべての管理者のロールを変更する必要があります。

既存のカスタム ロールを削除する方法

1. ［**Users and Administrators**］タブをアクティブにします。
2. サブメニューから、［**Manage Roles**］リンクをクリックします。
3. ［Tasks］メニューから、［**Delete Custom Role**］リンクをクリックします。

   図 3-12 に示されるような［Delete Custom Role］ページが表示されます。

図 3-12 ［Delete Custom Role］ページ



4. ［**Role Details**］セクションで、削除する必要のあるカスタム ロールを［**Role Name**］リストから選択します。
5. ［**Delete**］をクリックすると、選択したカスタム ロールが削除されます。

	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、削除 できません。

第 4 章
グローバルな WebFort 設定の管理

重要 : この章で説明される設定およびタスクはすべて、**Global Administrator** のみが実行できます。

以下の 2 つのレベルで WebFort 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*。これらの設定変更を適用するためにサーバ インスタンスをすべてリフレッシュする必要があります。

グローバル設定の管理は、WebFort 管理および最適化の重要な部分であり、Global Administrator （GA）の重要な担当業務です。この章では、GA がシステムのすべての現在と将来の組織に設定できるグローバル設定について説明します。これらの設定には次のものが含まれます。

- WebFort プロファイルおよびポリシーの理解
- Global Administrator としてのログイン
- ArcotID の設定
- Q&A の設定
- ユーザ名 - パスワードの設定
- OTP の設定
- OATH OTP 設定の設定
- ArcotOTP の設定
- デフォルト設定の割り当て

- RADIUS クライアントの設定

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、Global Administrator （GA）、または対象組織の Organization Administrator （OA）としてログインする必要があります。詳細については、5-149 ページの「組織固有の設定の管理」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。この方法の詳細については、2-32 ページの「基本認証パスワードの指定」を参照してください。

WebFort プロファイルおよびポリシーの理解

WebFort の各エンド ユーザは、少なくとも 1 つのクレデンシャル（ArcotID、Q&A、ユーザ名 - パスワード、OTP など）と関連付けられ、システム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。

クレデンシャル プロファイル

多くのエンド ユーザを WebFort に登録する場合、同じクレデンシャル テンプレートが多くのユーザにそのまま適用できることがあります。そのような場合、WebFort では、すぐに使える共通の認証設定（クレデンシャル プロファイルと言います）を柔軟に作成できます。このクレデンシャル 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、クレデンシャル プロファイルを使用することにより、クレデンシャル発行の管理が簡単になります。

クレデンシャル 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クレデンシャル属性を指定します。

WebFort には、各クレデンシャルのデフォルト プロファイルが付属しています。また、クレデンシャル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、組織への 1 つ以上のプロファイルを割り当てることができます。また、そのうちの 1 つをデフォルトとして設定できます。WebFort では、ユーザへのクレデンシャルの発行時に、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

WebFort 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 WebFort に対する認証を試行するごとに、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、クレデンシャル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。

WebFort 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 Arcot 専用トークンです。
- **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。WebFort は、SAML（Secure Assertion Markup Language）のバージョン 1.1 および 2.0 をサポートします。

クレデンシャル プロファイルと同様に、WebFort には各トークン タイプのデフォルト ポリシーが付属します。また、すべての認証メカニズムに複数のポリシーを作成し、それぞれ一意の名前を付けることができます。その後、1 つの組織に 1 つ以上のポリシーを割り当てることができます。

Global Administrator としてのログイン

最初の GA アカウントは、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 からアカウント詳細を取得する必要があります。GA は WebFort ユーザ名 - パスワードの使用、または 基本ユーザ名 - パスワードの使用 によってログインできます。

WebFort ユーザ名 - パスワードの使用

MA が WebFort ユーザ名 - パスワード クレデンシャル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）を使用してログインできます。アクティベーション コードは、初めてアカウントにログインするときにパスワードとして使用されます。何らかの理由で、このアクティベーション コードを紛失した場合、管理者に連絡し、アクティベーション コードを再生成して、それを再度送信してもらう必要があります。

WebFort ユーザ名 - パスワード クレデンシャルを使用して GA として Administration Console にログインする方法

1. Web ブラウザ ウィンドウを開きます。
2. Administration Console にアクセスするための URL を入力します。Administration Console のデフォルト URL は次のとおりです。

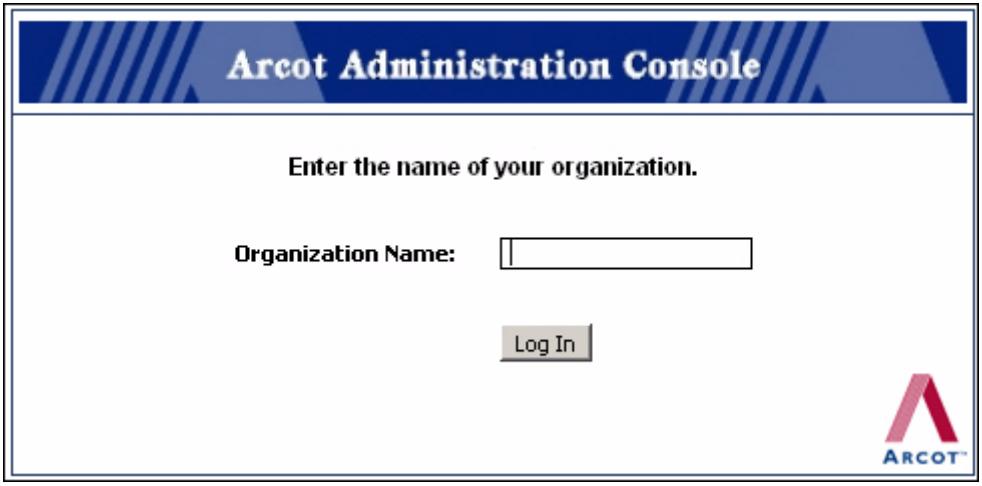
   `http://<hostname>:<port>/arcotadmin/adminlogin.htm`

   上記の URL の *`hostname`* と *`port`* をそれぞれ、Administration Console を展開したシステムのホスト名または Administration Console が待ち受けているポートの IP アドレスと置き換えます。

> **注：** Administration Console にアクセスするために、この URL をお気に入りに登録することをお勧めします。いずれの GA、OA、または UA も、WebFort ユーザ名 - パスワード クレデンシャルを使用して Administration Console にログインするためにこの URL を使用できます。

［Administrator Login］ページ（図 4-1）が表示されます。

図 4-1 Administrator Login：1 ページ

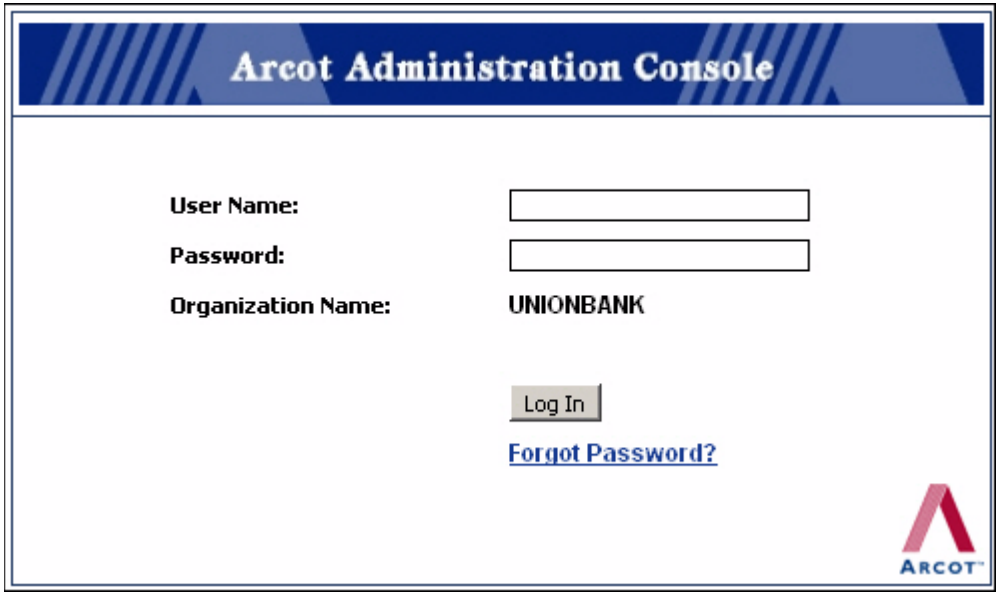


3. ログインする**組織名**を入力します。

> **重要：**組織の**表示名**を入力しないでください。（組織名によって定義される）組織の一意の ID を入力する必要があります。たとえば、デフォルトの組織（その表示名は Arcot Systems）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**」を入力する必要があります。ここで Arcot Systems を指定しないでください。

4. ［**Log In**］をクリックします。
   ［Login］ページ（図 4-2）が表示されます。

図 4-2 Administrator Login：2 ページ



5. ［**User Name**］フィールドでユーザ ID を指定し、提供された対応するアクティベーション コードを［**Password**］フィールドに入力して、［**Log In**］をクリックします。
   Administration Console のランディング ページ（図 4-3）が表示されます。

図 4-3 Administrator: Successfully Logged In

パスワードを忘れた場合

アクティベーション コードまたは WebFort パスワード クレデンシャルを忘れた場合、再生成するには以下の手順に従います。

1. ブラウザ ウィンドウで、Administration Console にアクセスするための URL を入力します。Administration Console のデフォルト URL は次のとおりです。

   `http://<hostname>:<port>/arcotadmin/adminlogin.htm`

   ［Administrator Login］ページ（図 4-1）が表示されます。

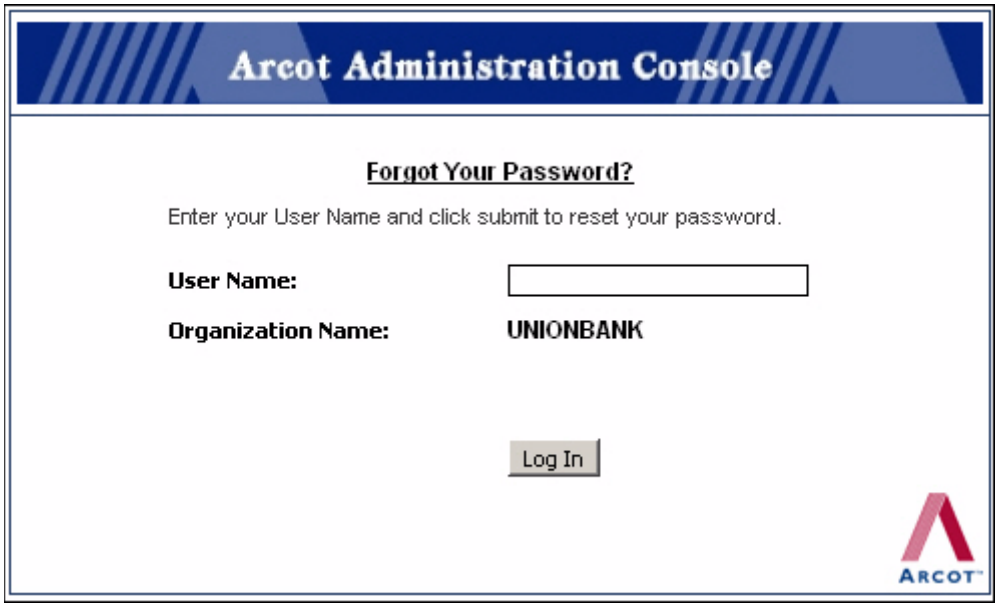
2. ［**Organization Name**］にログインする組織名を入力し、［**Log In**］をクリックします。

   ［Login］ページ（図 4-2）が表示されます。

3. ［**Forgot Password?** ］をクリックします。

   ［Forgot Your Password?］ページ（図 4-4）が表示されます。

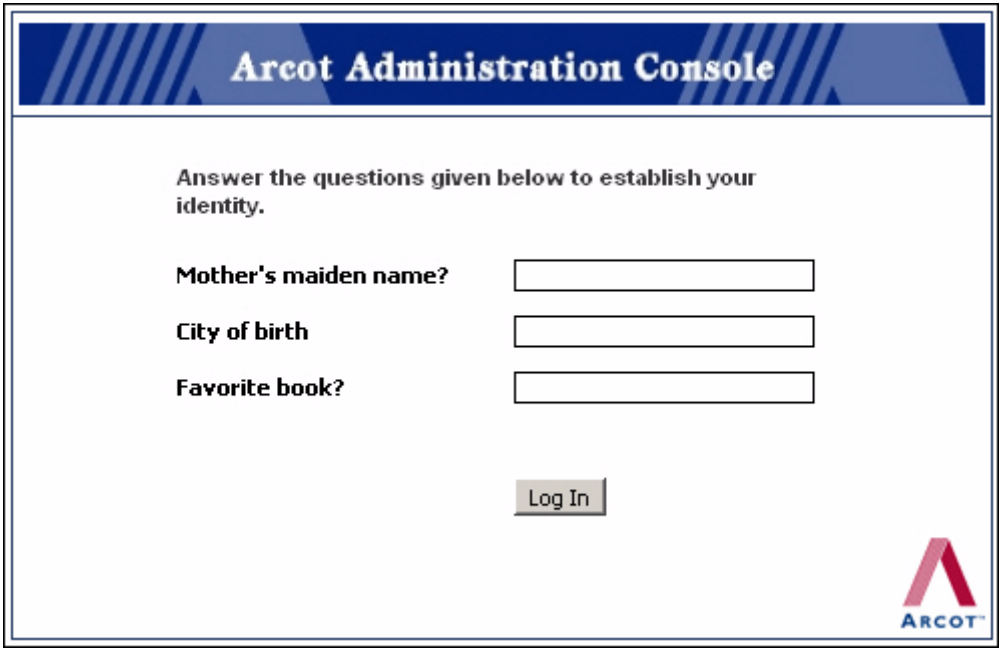
図 4-4 ［Forgot Your Password?］ページ



4. ［**User Name**］フィールドでユーザ ID を指定し、［**Log In**］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 6-182 ページの「管理者アカウントのプロファイル情報の変更」を参照してください）を表示するページ（図 4-5）が表示されます。

図 4-5 ［Questions and Answers］ページ



5. 表示された質問に対応する回答を指定し、［**Log In**］をクリックします。
［Reset Password］ページ（図 4-6）が表示されます。

図 4-6 ［Reset Password］ページ

6. ［**New Password**］および［**Confirm Password**］の各フィールドに新しいパスワードを入力します。
7. ［**Log In**］をクリックします。

   ［Login］ページ（図 4-7）が表示されます。
8. ［**Password**］にパスワードを指定し、［**Log In**］をクリックして、Administration Console にログインします。

基本ユーザ名 - パスワードの使用

基本ユーザ名 - パスワード クレデンシャルを使用して GA として Administration Console にログインする方法

1. Web ブラウザ ウィンドウを開きます。
2. Administration Console にアクセスするための URL を入力します。Administration Console のデフォルト URL は次のとおりです。

   `http://<hostname>:<port>/arcotadmin/adminlogin.htm`

上記の URL の *hostname* と *port* をそれぞれ、Administration Console を展開したシステムのホスト名または Administration Console が待ち受けているポートの IP アドレスと置き換えます。

	**注 :** Administration Console にアクセスするために、この URL をお気に入りに登録することをお勧めします。いずれの GA、OA、または UA も、クレデンシャルを使用して Administration Console にログインするためにこの URL を使用できます。

［Administrator Login］ページ（図 4-1）が表示されます。

3. ログインする**組織名**を入力します。

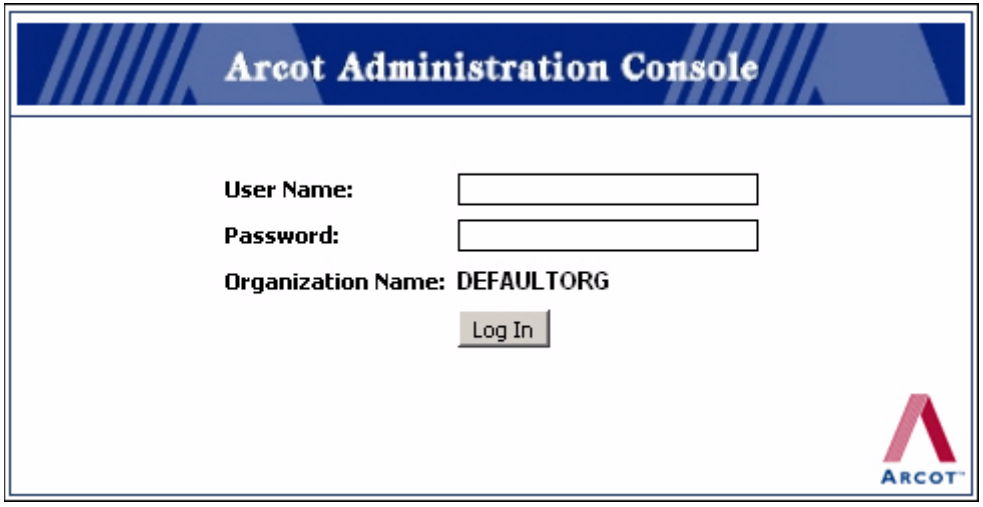
	**重要 :** 組織の**表示名**を入力しないでください。（組織名によって定義される）組織の一意の ID を入力する必要があります。たとえば、デフォルトの組織（その表示名は Arcot Systems）にログインする場合、この組織の（デフォルト）一意の ID である「**defaultorg**」を入力する必要があります。ここで Arcot Systems を指定しないでください。

4. ［**Log In**］をクリックします。

［Login］ページ（図 4-7）が表示されます。

	**注 :** このページには、［**Forgot Password?**］リンクは表示され*ません*。このリンクは、WebFort ユーザ名 - パスワード クレデンシャルを使用してログインするときに利用できます。

図 4-7 Administrator Login：2 ページ



5. ［**User Name**］フィールドでのユーザ ID を指定し、［**Password**］フィールリドに対応するパスワードを入力して、［**Log In**］をクリックします。

   図 4-3 のような Administration Console のログイン後ページが表示されます。

Administration Console のログアウト

Administration Console からログアウトするには、Administration Console のヘッダ領域の右上隅にある［**Logout**］リンクをクリックします。

Administration Console 使用時のセキュリティに関する推奨事項

Administration Console 使用時にブラウザ セッションを通した悪意のある攻撃から WebFort を保護するために、次のことを遵守してください。

- 他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。
- Console を操作しながら他のサイトを開かない。
- Administration Console のために厳しいパスワード制限を実施する。
- Administration Console 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。

ArcotID 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。

- ArcotID クレデンシャル プロファイルの設定
- ArcotID 認証ポリシーの設定

ArcotID クレデンシャル プロファイルの設定

ArcotID クレデンシャルに関連する以下の属性を定義するために ArcotID プロファイルを使用できます。

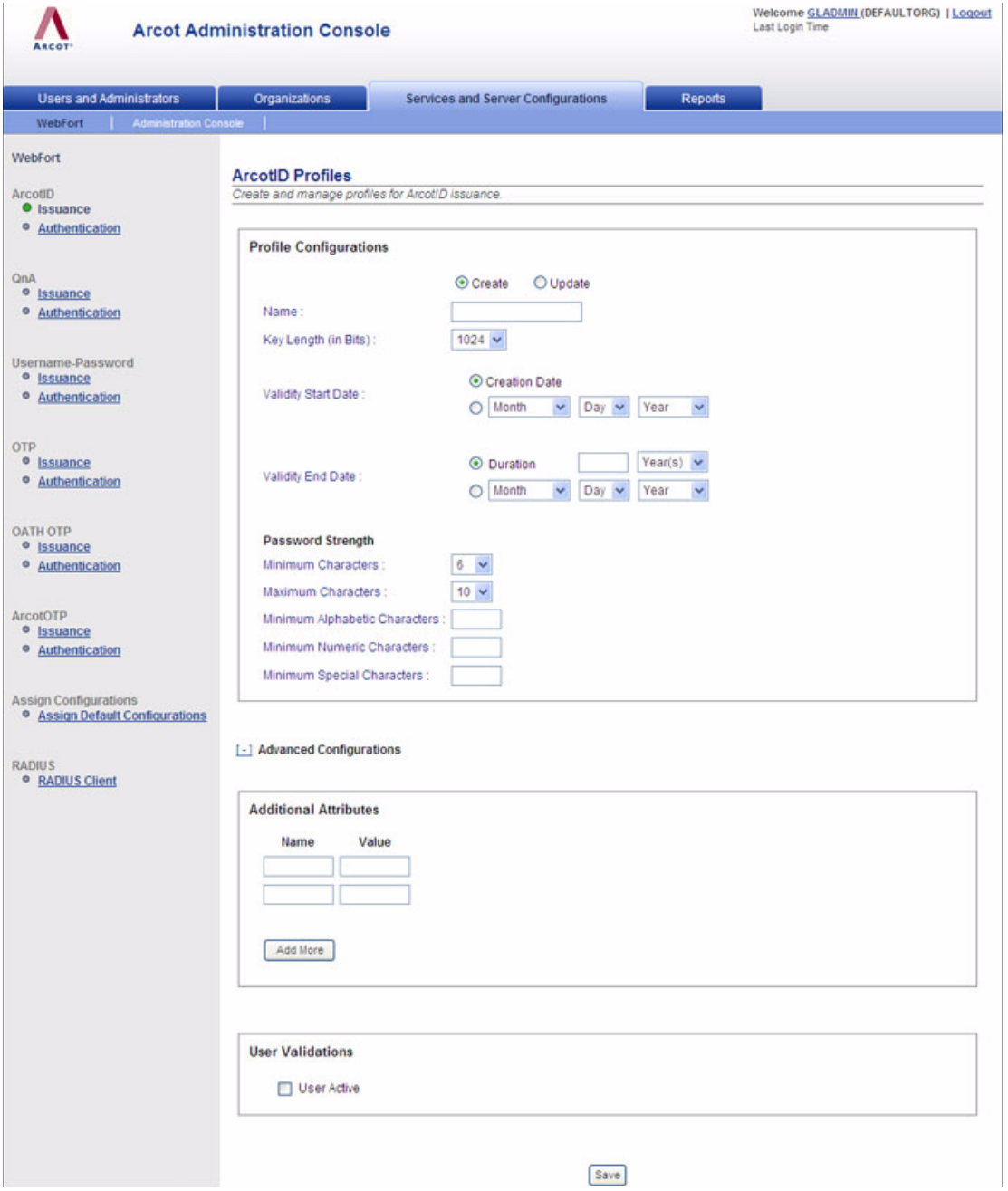
- **Key strength**：ArcotID の Cryptographic Camouflage アルゴリズムで使用されるキーのサイズ（ビット単位）です。
- **Validity period**：ArcotID クレデンシャルが有効な期間です。
- **Password strength**：パスワードの長さとそれに含まれるアルファベット、数字、および特殊文字の数の組み合わせによって決定される、パスワードの有効性です。

ArcotID 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 ArcotID の特性を制御できます。ArcotID クレデンシャル プロファイルを作成するために［ArcotID Profiles］ページ（図 4-8）を使用します。

ArcotID プロファイルを作成する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**ArcotID**］セクションの［**Issuance**］リンクをクリックすると、［ArcotID Profiles］ページ（図 4-8）が表示されます。

図 4-8 ［ArcotID Profiles］ページ



5. 必要に応じて、［**Profile Configurations**］セクションのフィールドに入力します。
表 4-1 に、このセクションのフィールドを示します。

表 4-1. ArcotID プロファイル設定のフィールド

フィールド	説明
[Profile Configurations]	
［Create］	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。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規プロファイルの**名前**を指定します。
［Update］	既存のプロファイルを更新する場合は、［**Select Profile**］リストから更新するプロファイルを選択します。
［Copy Profile］	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。
［Available Profiles］	設定をコピーするプロファイルを選択します。
［Key Length (in Bits)］	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。 **重要：**この値は ArcotID の強度の決定するうえで不可欠です。ArcotID の強度を高めるために、より高い値を選択することをお勧めします。
［Validity Start Date］	発行された ArcotID クレデンシャルが有効になる日付を設定します。有効期間は、ArcotID 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。
［Validity End Date］	ArcotID が期限切れになる日付を設定します。 クレデンシャル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。
[Password Strength]	
［Minimum Characters］	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。
［Maximum Characters］	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。
［Minimum Alphabetic Characters］	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、［**Minimum Characters**］フィールドで指定した値以下にする必要があります。

表 4-1. ArcotID プロファイル設定のフィールド

フィールド	説明
［Minimum Numeric Characters］	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。
［Minimum Special Characters］	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。

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. ［**Additional Attributes**］セクションで、ArcotID クレデンシャルを**名前**と**値**のペアのフォーマットで渡す必要がある追加情報（符号のない属性）を指定します。

   たとえば、エンド ユーザのハード ディスクなどの特定のデバイスに ArcotID を固定する場合は、このセクションを使用して、以下のこの追加情報を送信する必要があります。

表 4-2. ArcotID 用の追加属性の提供

名前	値
`devlock_required`	はい
`devlock_type`	`hd`

関連文書： このセクションで指定できる追加情報の詳細については、「ArcotID Client 6.0.2 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、［**Add More**］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。

8. ［**User Validations**］セクションで以下を設定します。
   - 現在のクレデンシャル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場合は、［**User Active**］チェック ボックスをオンにします。
     - クレデンシャルの作成
     - クレデンシャルの再発行
     - クレデンシャルのリセット
     - クレデンシャル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、[**User Attribute**] 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。
  - 電子メール アドレス
  - 名
  - ミドル ネーム
  - 姓
  - 電話番号

9. ArcotID プロファイルを作成または更新するには、[**Save**] をクリックします。
10. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

ArcotID 認証ポリシーの設定

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

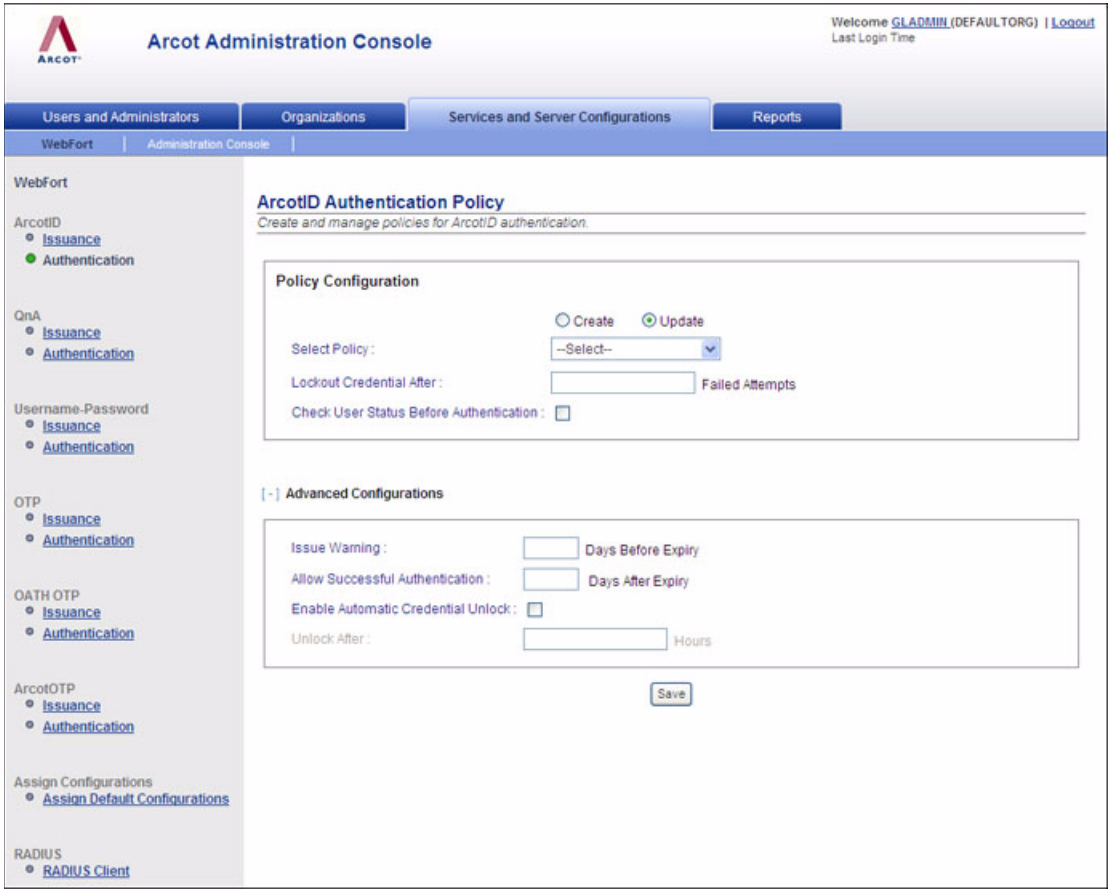
- **User status**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。
- **Lockout criteria**：失敗した試行の数です。この数を超えると、ユーザのクレデンシャルがロック アウトされます。
- **Unlocking criteria**：ロックされた ArcotID クレデンシャルを使用して再度ログイン可能になるまでの時間数です。この機能は、クレデンシャル リセットのリクエスト数を大きく減らすことができます。
- **Credential expiration settings**：呼び出し元のアプリケーションにユーザの ArcotID 有効期限に関する警告が通知されるまでの期間です。
- **期限切れの ArcotID の使用**：ユーザが期限切れの ArcotID クレデンシャルを使用して認証に成功できる日数です。
- **Expiry warning settings**：ユーザの ArcotID クレデンシャル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、非常に慎重に使用する必要があります。

グローバル ArcotID 認証ポリシーを設定する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**ArcotID**］セクションの［**Authentication**］リンクをクリックすると、［ArcotID Authentication Policy］ページ（図 4-9）が表示されます。

図 4-9 ［ArcotID Authentication Policy］ページ



5. 必要に応じて、［**Policy Configuration**］セクションのフィールドに入力します。表 4-3 に、このセクションのフィールドを示します。

表 4-3. ArcotID 認証ポリシー設定フィールド

フィールド	説明
［Policy Configurations］	
［Create］	新規ポリシーを作成する場合は、以下の手順に従います。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規ポリシーの**名前**を指定します。
［Update］	既存のポリシーを更新する場合は、表示される［**Select Policy**］リストから更新するポリシーを選択します。
［Copy Policy］	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。
［Available Policies］	設定をコピーするポリシーを選択します。
［Lockout Credential After］	失敗した試行の数を指定します。この数を超えると、ユーザのクレデンシャルがロックされます。
［Check User Status Before Authentication］	現在のクレデンシャル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、このチェック ボックスをオンにします。 • クレデンシャルの作成 • クレデンシャルの再発行 • クレデンシャルのリセット • クレデンシャルの有効期間のリセット

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。

7. 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。表 4-4 に、このセクションのフィールドを示します。

表 4-4. ArcotID 認証ポリシー詳細設定フィールド

フィールド	説明
［Advanced Configurations］	
［Issue Warning］	ユーザの ArcotID クレデンシャル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。
［Allow Successful Authentication］	正常にアカウントにログインするためにユーザが期限切れの ArcotID クレデンシャルを使用できる日数を指定します。

表 4-4. ArcotID 認証ポリシー詳細設定フィールド

フィールド	説明
[Enable Automatic Credential Unlock]	ロックされたクレデンシャルが、[**Unlock After**] 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、[Lockout Credential After] フィールドで対応する値を指定する場合のみ有効です。
[Unlock After]	ロックされたクレデンシャル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。

8. ArcotID ポリシーを作成または更新するには、[**Save**] をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

Q&A 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
- Q&A 認証ポリシーの設定

Q&A 発行プロファイルの設定

Q&A クレデンシャルに関連する以下の属性を指定するために Q&A プロファイルを使用できます。

- **Number of questions**：
  - 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。
- **Validity period**：Q&A クレデンシャルが有効な期間です。
- **Case-sensitive Answers**：ユーザが入力した応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。
- **Caller Verification**：回答はサードパーティによって確認され、その後で結果が WebFort サーバに送信されます。

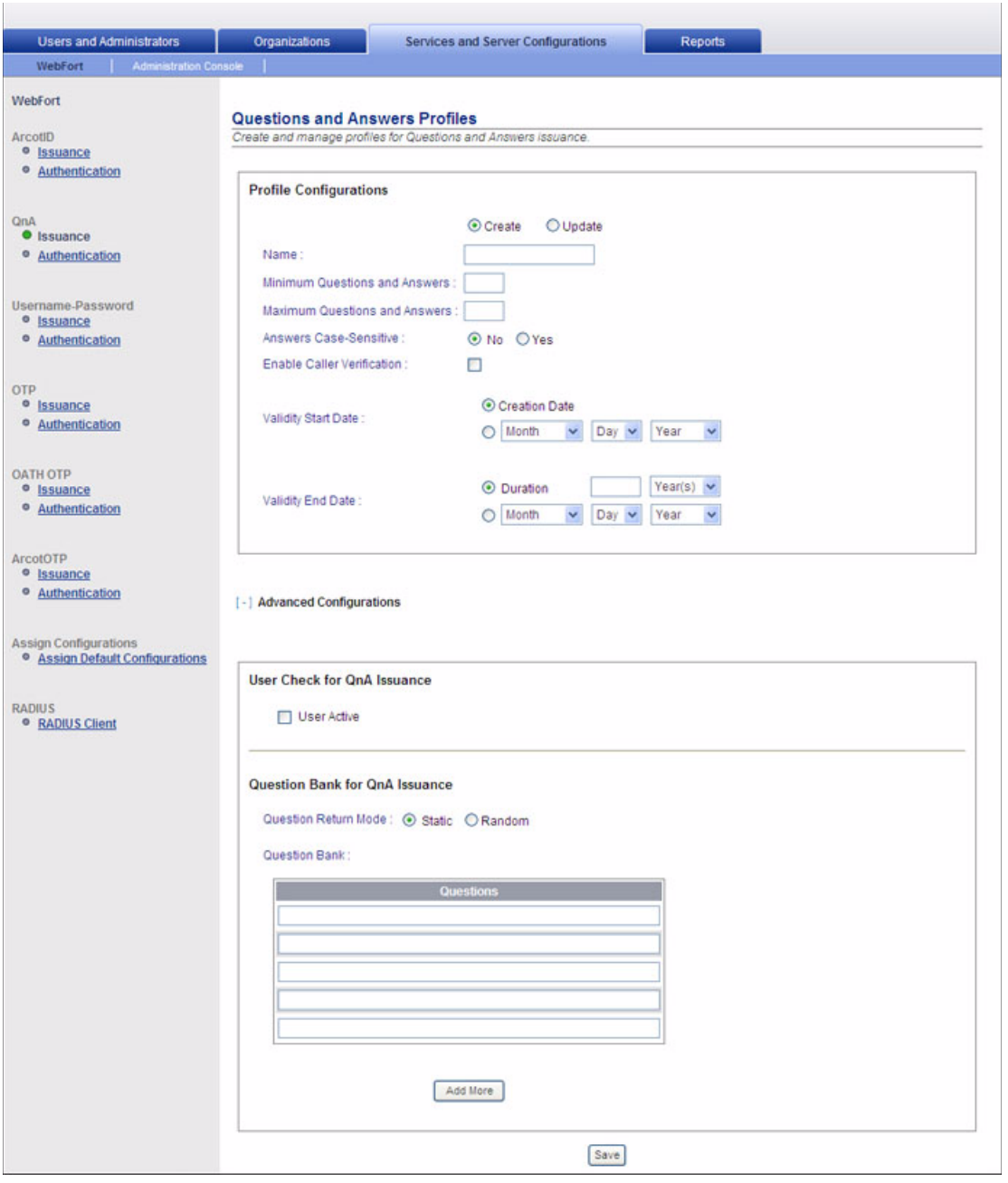
- **Question Bank**：ユーザは、Q&A クレデンシャルをセットアップするため、質問銀行のあらかじめ設定済みの質問を使用します。

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 クレデンシャルの特性を制御できます。Q&A クレデンシャル プロファイルを作成するには、［Questions and Answers Profiles］ページ（図 4-9）を使用します。

Q&A プロファイルを作成または更新する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**QnA**］セクションの［**Issuance**］リンクをクリックすると、［Questions and Answers Profiles］ページ（図 4-10）が表示されます。

図 4-10 ［Questions and Answers Profiles］ページ



5. 必要に応じて、［**Profile Configurations**］セクションのフィールドに入力します。表 4-5 に、このセクションのフィールドを示します。

表 4-5. Q&A プロファイル設定のフィールド

フィールド	説明
［Profile Configurations］	
［Create］	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。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規プロファイルの**名前**を指定します。
［Update］	既存のプロファイルを更新する場合は、表示される［**Select Profile**］リストから更新するプロファイルを選択します。
［Copy Profile］	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。
［Available Profiles］	設定をコピーするプロファイルを選択します。
［Minimum Questions and Answers］	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、［Maximum Questions and Answers］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 つの質問に対する回答が求められます。
［Maximum Questions and Answers］	ユーザが設定できる質問と回答の最大数を指定します。
［Answers Case-Sensitive］	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。
［Enable Caller Verification］	このオプションを有効にする場合、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 WebFort サーバに送信されます。
［Validity Start Date］	発行された Q&A クレデンシャルが有効になる日付を設定します。有効期間は、Q&A 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。
［Validity End Date］	Q&A クレデンシャルが期限切れになる日付を設定します。クレデンシャル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。

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. ［**User Check For QnA Issuance**］セクションで以下を設定します。

- 現在のクレデンシャル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場合は、[**User Active**] チェック ボックスをオンにします。
  - クレデンシャルの作成
  - クレデンシャルの再発行
  - クレデンシャルのリセット
  - クレデンシャル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、[**User Attribute**] 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。
  - 電子メール アドレス
  - 名
  - ミドル ネーム
  - 姓
  - 電話番号

8. [**Question Bank for QnA Issuance**] セクションで、質問を設定できます。これは、このプロファイルを使用する組織のために設定されます。
9. Q&A プロファイルを作成または更新するには、[**Save**] をクリックします。
10. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」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。

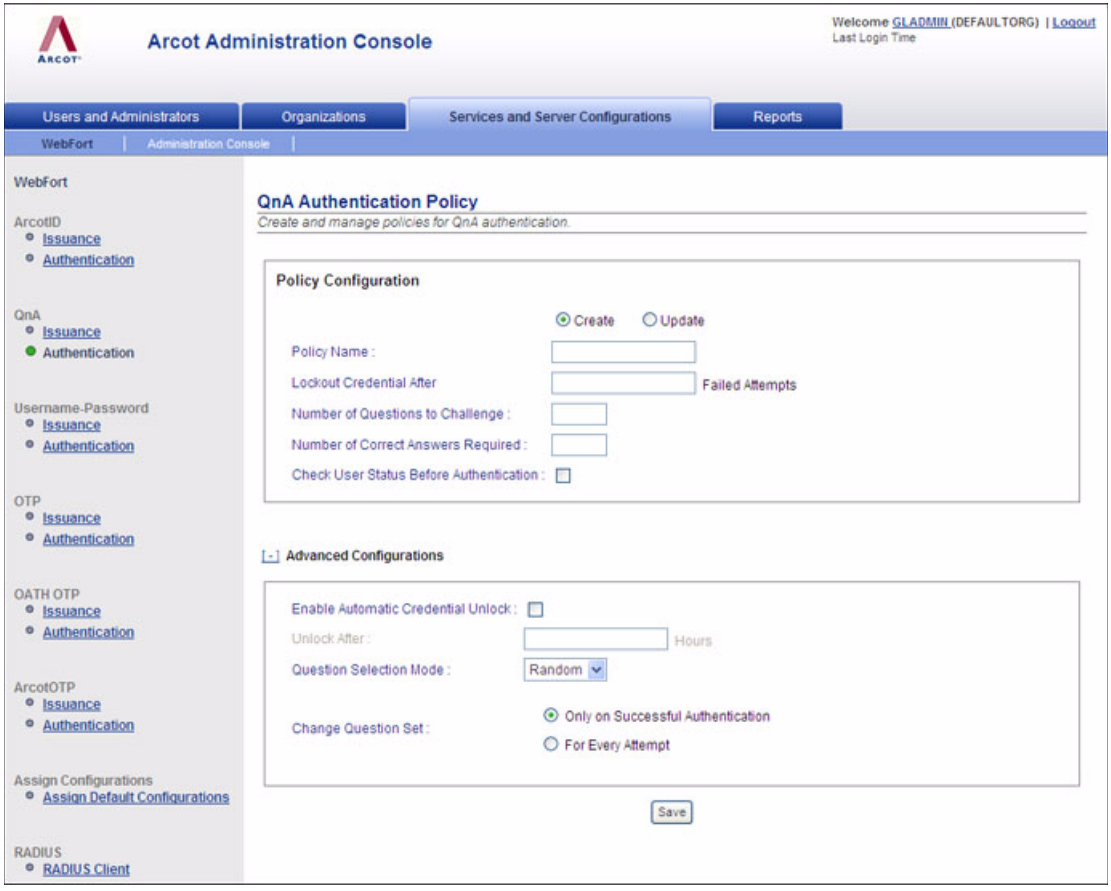
- **User status**：ユーザのステータスです。アクティブまたは非アクティブのいずれかです。
- **Number of questions**：
  - WebFort では、認証処理中にユーザに質問を行う必要があります。
  - そのため、正しい回答が認証時に必要です。
- **Lockout criteria**：失敗した試行の数です。この数を超えると、ユーザのクレデンシャルがロック アウトされます。

- **Unlocking criteria：**ロックされた Q&A クレデンシャルをログインに再使用できるようになるまでの時間数です。
- **Question Selection Mode**：質問は、ランダムまたは交互に選択されます。つまり、［**Change Question Set**］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。
- **Change Question Set**: 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。

組織の Q&A 認証ポリシーを設定する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**QnA**］セクションの［**Authentication**］リンクをクリックすると、［QnA Authentication Policy］ページ（図 4-11）が表示されます。

図 4-11 ［QnA Authentication Policy］ページ



5. 必要に応じて、［**Policy Configuration**］セクションのフィールドに入力します。表 4-6 に、このセクションのフィールドを示します。

表 4-6. Q&A 認証ポリシー設定フィールド

フィールド	説明
［Policy Configuration］	
［Create］	新規ポリシーを作成する場合は、以下の手順に従います。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規ポリシーの**名前**を指定します。

表 4-6. Q&A 認証ポリシー設定フィールド（続き）

フィールド	説明
［Update］	既存のポリシーを更新する場合は、表示される［**Select Policy**］リストから更新するポリシーを選択します。
［Copy Policy］	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。
［Available Policies］	設定をコピーするポリシーを選択します。
［Lockout Credential After］	失敗した試行の数を指定します。この数を超えると、ユーザのクレデンシャルがロックされます。
［Number of Questions to Ask］	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。
［Number of Correct Answers Required］	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、［Number of Questions to Ask］フィールドに「5」を設定する場合、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。
［Check User Status Before Authentication］	現在のクレデンシャル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、このチェック ボックスをオンにします。 • クレデンシャルの作成 • クレデンシャルの再発行 • クレデンシャルのリセット • クレデンシャルの有効期間のリセット

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. 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。表 4-7 に、このセクションのフィールドを示します。

表 4-7. Q&A 認証ポリシー詳細設定フィールド

フィールド	説明
［Advanced Configurations］	
［Enable Automatic Credential Unlock］	ロックされたクレデンシャルが、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、［Lockout Credential After］フィールドで対応する値を指定する場合のみ有効です。
［Unlock After］	ロックされたクレデンシャル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。

表 4-7. Q&A 認証ポリシー詳細設定フィールド（続き）

フィールド	説明
［Question Selection Mode］	提示される質問が選択される方法を指定します。サポートされる値は以下のとおりです。 • ［**Random**］- 質問は、設定されたセットからランダムに選択されます。 • ［**Alternate**］- 設定されたセットから新しい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。
［Change Question Set］	WebFort 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。 • ［**Only on Successful Authentication**］- ユーザ認証が成功した後でのみ、［Question Selection Mode］に基づいて新しい質問セットが選択されます。 • ［**For Every Attempt**］- 認証が試行されるたびごとに、認証結果に関係なく、［Question Selection Mode］に基づいて新しい質問セットが選択されます。

8. Q&A ポリシーを作成または更新するには、［**Save**］をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

ユーザ名 - 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。

- ユーザ名 - パスワード発行プロファイルの設定
- ユーザ名 - パスワード認証ポリシーの設定

ユーザ名 - パスワード発行プロファイルの設定

パスワード クレデンシャルに関連する以下の属性を指定するために、ユーザ名 - パスワード プロファイルを使用できます。

- **Password strength**：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。
- **Validity period**：ユーザ名 - パスワード クレデンシャルが有効な期間です。

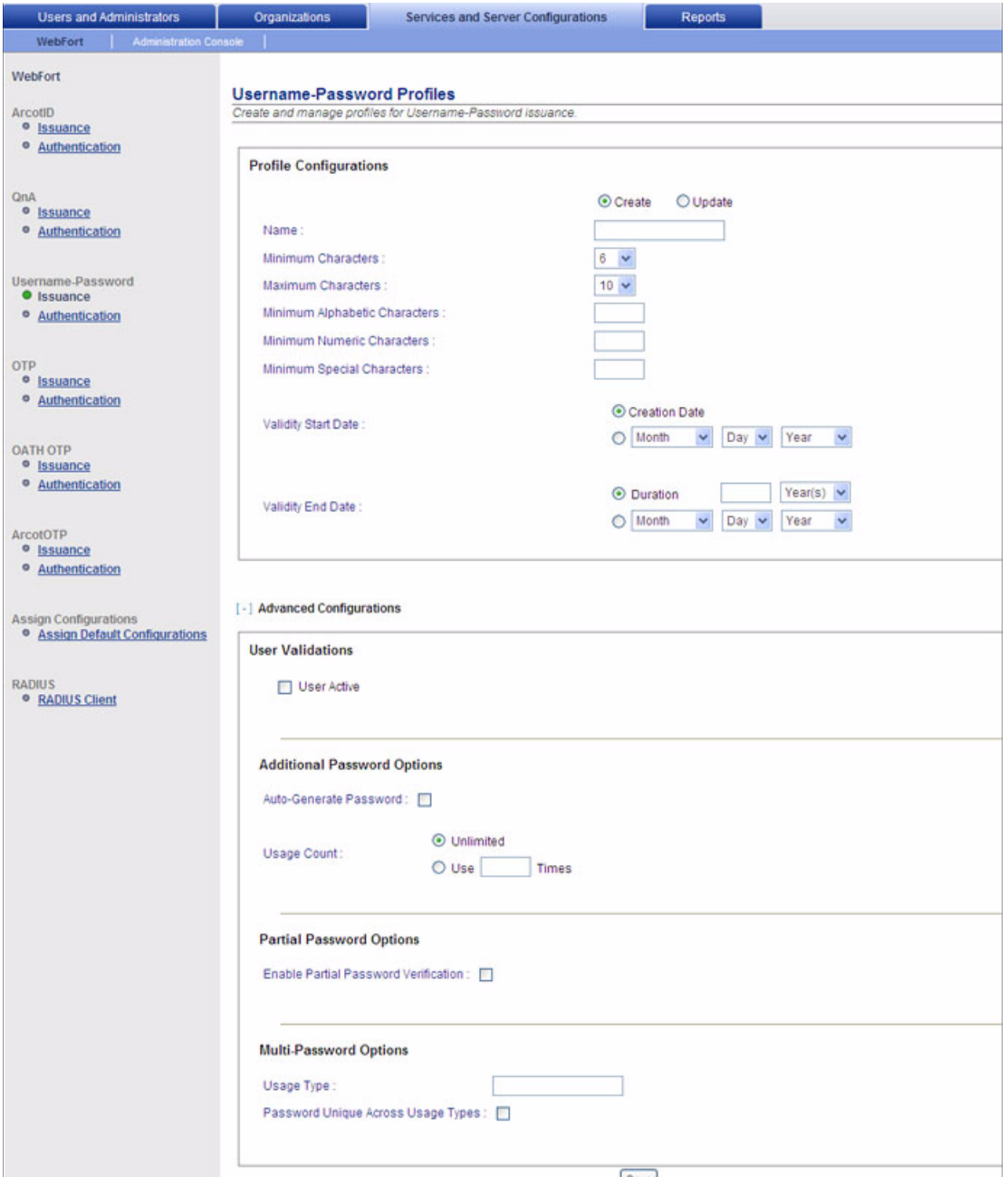
- **Auto-generate password**：WebFort サーバによってパスワードが作成されます。
- **Usage count**：パスワードを使用可能な回数です。
- **Usage type and password uniqueness**：1 人のユーザに複数のパスワードを設定できます。パスワードは同じとすることもできますし、一意とすることもできます。
- **Partial password settings**：ユーザは、さまざまな場所のパスワード文字の入力を求められます。

ユーザ名 - 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 クレデンシャルの特性を制御できます。パスワード クレデンシャル プロファイルを作成するには、［Username-Password Profiles］ページ（図 4-12）を使用します。

ユーザ名 - パスワード プロファイルを作成または更新する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Username-Password**］セクションの［**Issuance**］リンクをクリックすると、［Username-Password Profiles］ページ（図 4-12）が表示されます。

図 4-12 ［Username-Password Profiles］ページ



5. 必要に応じて、［**Profile Configurations**］セクションのフィールドに入力します。
表 4-8 に、このセクションのフィールドを示します。

表 4-8. ユーザ名 - パスワード プロファイル設定のフィールド

フィールド	説明
[Profile Configurations]	
［Create］	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。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規プロファイルの**名前**を指定します。
［Update］	既存のプロファイルを更新する場合は、［**Select Profile**］リストから更新するプロファイルを選択します。
［Copy Profile］	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。
［Available Profiles］	設定をコピーするプロファイルを選択します。
［Minimum Characters］	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。
［Maximum Characters］	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。
［Minimum Alphabetic Characters］	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、［**Minimum Characters**］フィールドで指定した値以下にする必要があります。
［Minimum Numeric Characters］	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。
［Minimum Special Characters］	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。
［Validity Start Date］	発行されたパスワード クレデンシャルが有効になる日付を設定します。 有効期間は、このクレデンシャルが作成された日付から開始することもできますし、カスタムの日付を指定することもできます。
［Validity End Date］	パスワードが期限切れになる日付を設定します。 クレデンシャルの有効期間を指定することもできますし、カスタムの日付を指定することもできます。

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. ［**User Validations**］セクションで以下を設定します。
   - 現在のクレデンシャル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場合は、［**User Active**］チェック ボックスをオンにします。
     - クレデンシャルの作成
     - クレデンシャルの再発行
     - クレデンシャルのリセット
     - クレデンシャル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、［**User Attribute**］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。
     - 電子メール アドレス
     - 名
     - ミドル ネーム
     - 姓
     - 電話番号
8. ［**Additional Password Options**］セクションで以下を設定します。
   - WebFort サーバでユーザ パスワードを生成する場合は、［**Auto-Generate Password**］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。
   - ［**Usage Count**］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に［**Unlimited**］をクリックします。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. ユーザを部分パスワードで認証する場合は、［**Partial Password Options**］セクションの［**Enable Partial Password Verification**］チェック ボックスをオンにします。この機能を有効にする場合、パスワードのさまざまな位置に文字を入力することが要求されます。たとえば、パスワードが「casablanca!」である場合、ユーザは、位置 1、3 および 8 の文字を入力するよう求められます。入力する文字は、「csn」になります。
10. ［**Multi-Password Options**］セクションで以下を設定します。

- ［**Usage Type**］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。
- ユーザのパスワードが一意である必要がある場合は、［**Password Unique Across Usage Types**］チェック ボックスを有効にします。

11. ユーザ名 - パスワード プロファイルを作成または更新するには、［**Save**］をクリックします。
12. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

ユーザ名 - パスワード認証ポリシーの設定

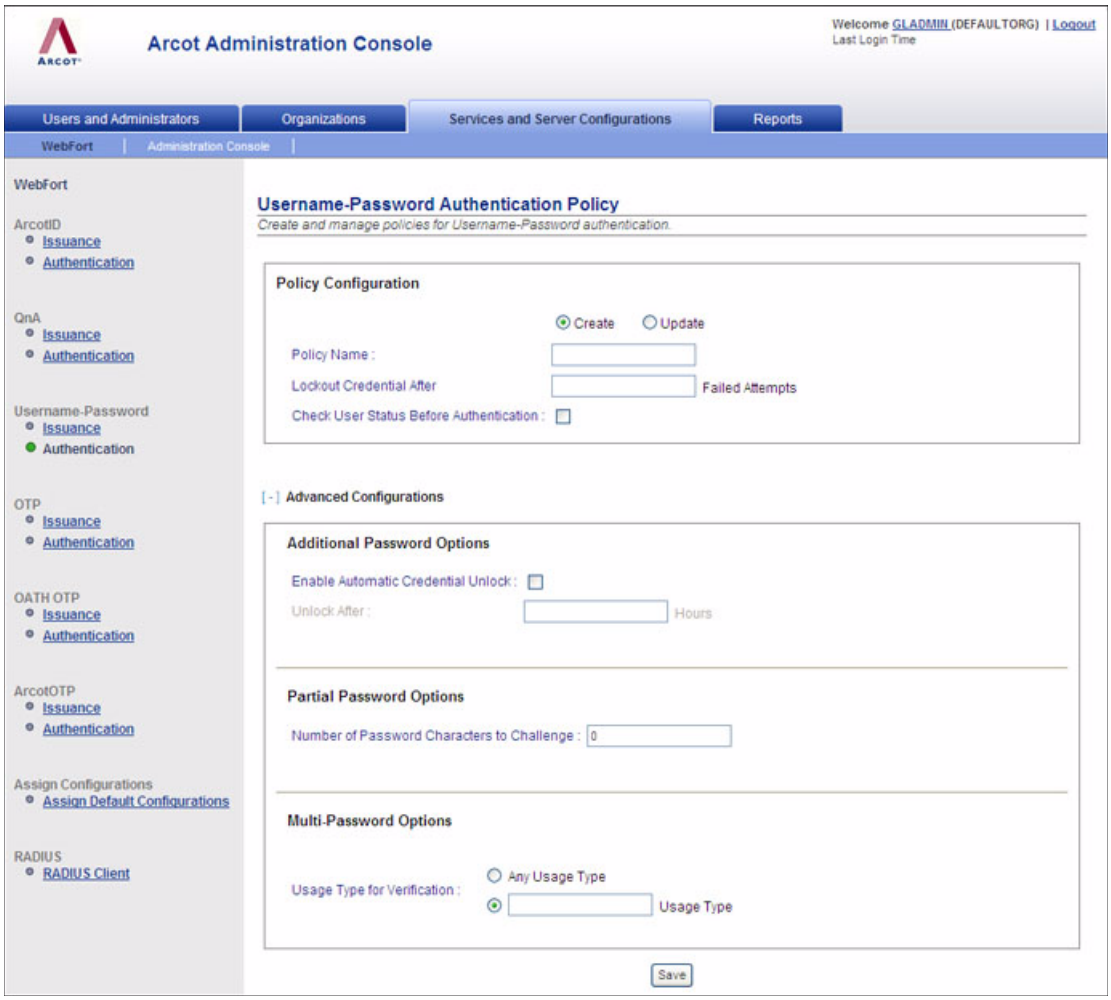
ユーザ名 - パスワード ベースの認証に関連する以下の属性を定義するためにパスワード ポリシーを使用できます。

- **User status**：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。
- **Lockout criteria**：失敗した試行の数です。この数を超えると、ユーザのクレデンシャルがロック アウトされます。
- **Unlocking criteria**：ロックされたユーザ パスワード クレデンシャルを使用して再度ログイン可能になるまでの時間数です。
- **Partial password settings**：認証でユーザに提示される必要がある文字の数です。
- **Multi-password settings**：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。

組織のユーザ名 - パスワード認証ポリシーを設定する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Username-Password**］セクションの［**Authentication**］リンクをクリックすると、［Username-Password Authentication Policy］ページ（図 4-13）が表示されます。

図 4-13 ［Username-Password Authentication Policy］ページ



5. 必要に応じて、［**Policy Configuration**］セクションのフィールドに入力します。表 4-9 に、このセクションのフィールドを示します。

表 4-9. ユーザ名 - パスワード認証ポリシー設定のフィールド

フィールド	説明
[Policy Configurations]	
［Create］	新規ポリシーを作成する場合は、以下の手順に従います。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規ポリシーの**名前**を指定します。
［Update］	既存のポリシーを更新する場合は、表示される［**Select Policy**］リストから更新するポリシーを選択します。
［Copy Policy］	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。
［Available Policies］	設定をコピーするポリシーを選択します。
［Lockout Credential After］	失敗した試行の数を指定します。この数を超えると、ユーザのクレデンシャルがロックされます。
［Check User Status Before Authentication］	現在のクレデンシャル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場合は、このチェック ボックスをオンにします。 • クレデンシャルの作成 • クレデンシャルの再発行 • クレデンシャルのリセット • クレデンシャルの有効期間のリセット

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。

7. 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。表 4-10 に、このセクションのフィールドを示します。

表 4-10. ユーザ名 - パスワード認証ポリシーの詳細設定

フィールド	説明
[Additional Password Options]	
［Enable Automatic Credential Unlock］	クレデンシャルが、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、［Lockout Credential After］フィールドで対応する値を指定する場合のみ有効です。
［Unlock After］	ロックされたクレデンシャル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。

表 4-10. ユーザ名 - パスワード認証ポリシーの詳細設定（続き）

フィールド	説明
[Partial Password Options]	
[Number of Password Characters to Challenge]	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。WebFort 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。
[Multi-Password Options]	
[Usage Type for Verification]	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、[**Any Usage Type**] 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、[**UsageType**] フィールドにその使用タイプの名前を入力します。

8. ユーザ名 - パスワード ポリシーを作成または更新するには、[**Save**] をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」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
- OTP 認証ポリシーの設定

OTP 発行プロファイルの設定

ワンタイム パスワード クレデンシャルに関連する以下の属性を定義するために OTP プロファイルを使用できます。

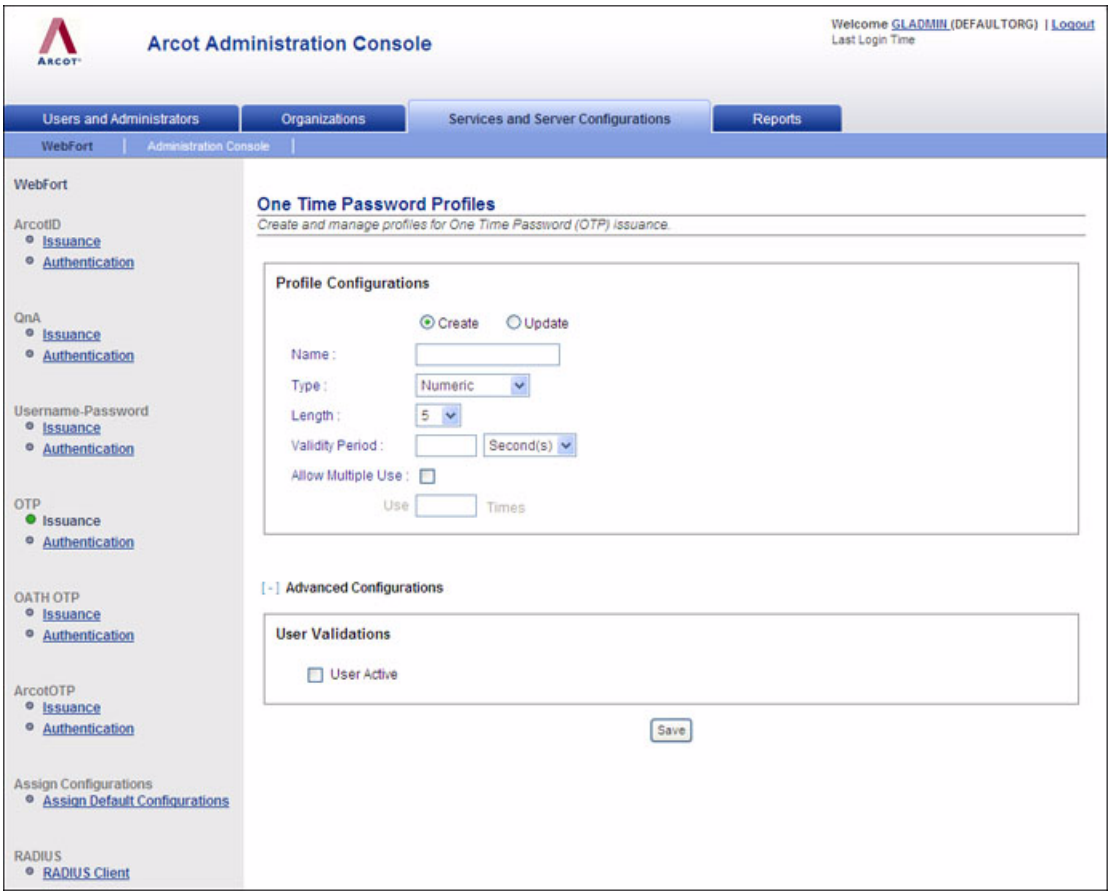
- **OTP strength**：OTP のタイプ（数字または英数字）および長さです。
- **Validity period**：OTP が有効な期間です。
- **Usage**：OTP を認証に再使用できる回数です。

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 OTP クレデンシャルの特性を制御できます。OTP クレデンシャル プロファイルを作成するには、［One-Time Password Profiles］ページ（図 4-14）を使用します。

OTP プロファイルを作成または更新する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**OTP**］セクションの［**Issuance**］リンクをクリックすると、［One Time Password Profiles］ページ（図 4-14）が表示されます。

図 4-14 ［One-Time Password Profiles］ページ



5. 必要に応じて、［**Profile Configurations**］セクションのフィールドに入力します。表 4-11 に、このセクションのフィールドを示します。

表 4-11. OTP プロファイル設定のフィールド

フィールド	説明
［Profile Configurations］	
［Create］	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。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規プロファイルの**名前**を指定します。

表 4-11. OTP プロファイル設定のフィールド

フィールド	説明
［Update］	既存のプロファイルを更新する場合は、表示される［**Select Profile**］リストから更新するプロファイルを選択します。
［Copy Profile］	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。
［Available Profiles］	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［Numeric］です。
［Length］	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。
［Validity Period］	発行された OTP クレデンシャルが有効である期間を設定します。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。
［Allow Multiple Use］	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。
［Use］	［**Allow Multiple Use**］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。

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. ［**User Validations**］セクションで以下を設定します。
   - 現在のクレデンシャル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場合は、［**User Active**］チェック ボックスをオンにします。
     - クレデンシャルの作成
     - クレデンシャルの再発行
     - クレデンシャルのリセット
     - クレデンシャル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、［**User Attribute**］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。
     - 電子メール アドレス
     - 名

- ミドル ネーム
- 姓
- 電話番号

8. OTP プロファイルを作成または更新するには、[**Save**] をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

OTP 認証ポリシーの設定

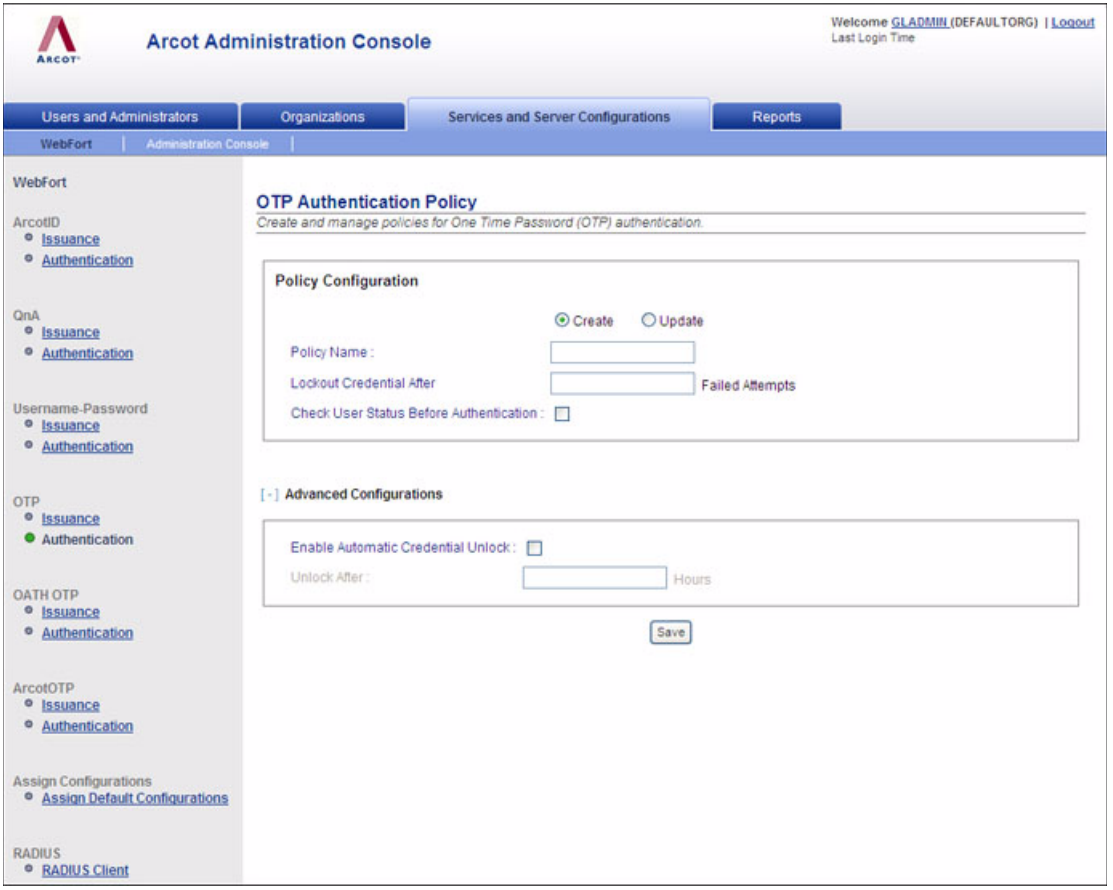
OTP ベースの認証に関連する以下の属性を定義するために OTP ポリシーを使用できます。

- **User status**：ユーザ アカウントのステータスです。アクティブまたは非アクティブのいずれかです。
- **Lockout criteria**：失敗した試行の数です。この数を超えると、ユーザのクレデンシャルがロックされます。
- **Unlocking criteria**：ロックされたクレデンシャルが再使用できるようになるまでの時間数です。

組織の OTP 認証ポリシーを設定する方法

1. Global Administrator （GA）として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 [**Services and Server Configurations**] タブをアクティブにします。
3. サブメニュー内の [**WebFort**] タブがアクティブであることを確認します。
4. [**OTP**] セクションの [**Authentication**] リンクをクリックすると、[OTP Authentication Policy] ページ（図 4-15）が表示されます。

図 4-15 ［OTP Authentication Policy］ページ



5. 必要に応じて、［**Policy Configuration**］セクションのフィールドに入力します。表 4-12 に、このセクションのフィールドを示します。

表 4-12. OTP 認証ポリシー設定のフィールド

フィールド	説明
［Policy Configurations］	
［Create］	新規ポリシーを作成する場合は、以下の手順に従います。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規ポリシーの**名前**を指定します。

表 4-12. OTP 認証ポリシー設定のフィールド（続き）

フィールド	説明
[Update]	既存のポリシーを更新する場合は、表示される［**Select Policy**］リストから更新するポリシーを選択します。
[Copy Policy]	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。
[Available Policies]	設定をコピーするポリシーを選択します。
[Lockout Credential After]	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。
[Check User Status Before Authentication]	現在のクレデンシャル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場合は、このチェック ボックスをオンにします。 • クレデンシャルの作成 • クレデンシャルの再発行 • クレデンシャルのリセット • クレデンシャルの有効期間のリセット

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. 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。表 4-13 に、このセクションのフィールドを示します。

表 4-13. OTP 認証ポリシーの詳細設定

フィールド	説明
[Advanced Configurations]	
[Enable Automatic Credential Unlock]	クレデンシャルが、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、［Lockout Credential After］フィールドで対応する値を指定する場合のみ有効です。
[Unlock After]	ロックされたクレデンシャル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。

8. OTP ポリシーを作成または更新するには、［**Save**］をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」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
- OATH OTP 認証ポリシーの設定

OATH OTP 発行プロファイルの設定

OATH ワンタイム パスワード クレデンシャルに関連する以下の属性を定義するために OATH OTP プロファイルを使用できます。

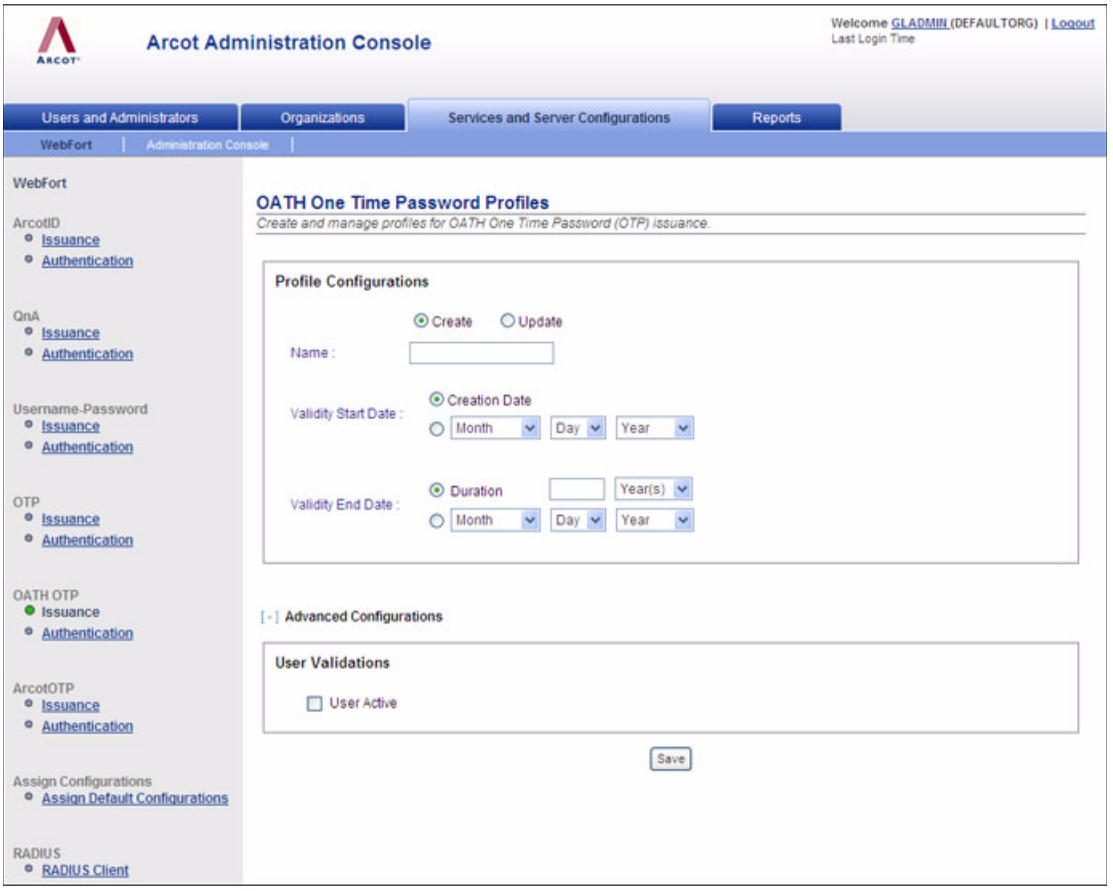
- **Validity period**：OATH OTP が有効な期間です。

OATH 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 OATH OTP クレデンシャルの特性を制御できます。OATH OTP クレデンシャル プロファイルを作成するには、［OATH OTP Profiles］ページ（図 4-16）を使用します。

OATH OTP プロファイルを作成または更新する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**OATH OTP**］セクションの［**Issuance**］リンクをクリックすると、［OATH One Time Password Profiles］ページ（図 4-16）が表示されます。

図 4-16 ［OATH OTP Profiles］ページ



5. 必要に応じて、［**Profile Configurations**］セクションのフィールドに入力します。表 4-14 に、このセクションのフィールドを示します。

表 4-14. OATH OTP プロファイル設定のフィールド

フィールド	説明
［Profile Configurations］	
［Create］	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。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規プロファイルの**名前**を指定します。

表 4-14. OATH OTP プロファイル設定のフィールド（続き）

フィールド	説明
［Update］	既存のプロファイルを更新する場合は、表示される［**Select Profile**］リストから更新するプロファイルを選択します。
［Copy Profile］	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。
［Available Profiles］	設定をコピーするプロファイルを選択します。
［Validity Start Date］	発行された OATH OTP クレデンシャルが有効になる日付を設定します。 有効期間は、OATH OTP 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。
［Validity End Date］	OATH OTP が期限切れになる日付を設定します。 クレデンシャル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。

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. ［**User Validations**］セクションで以下を設定します。
   - 現在のクレデンシャル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場合は、［**User Active**］チェック ボックスをオンにします。
     - クレデンシャルの作成
     - クレデンシャルの再発行
     - クレデンシャルのリセット
     - クレデンシャル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、［**User Attribute**］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。
     - 電子メール アドレス
     - 名
     - ミドル ネーム
     - 姓
     - 電話番号
8. OATH OTP プロファイルを作成または更新するには、［**Save**］をクリックします。

9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

OATH OTP 認証ポリシーの設定

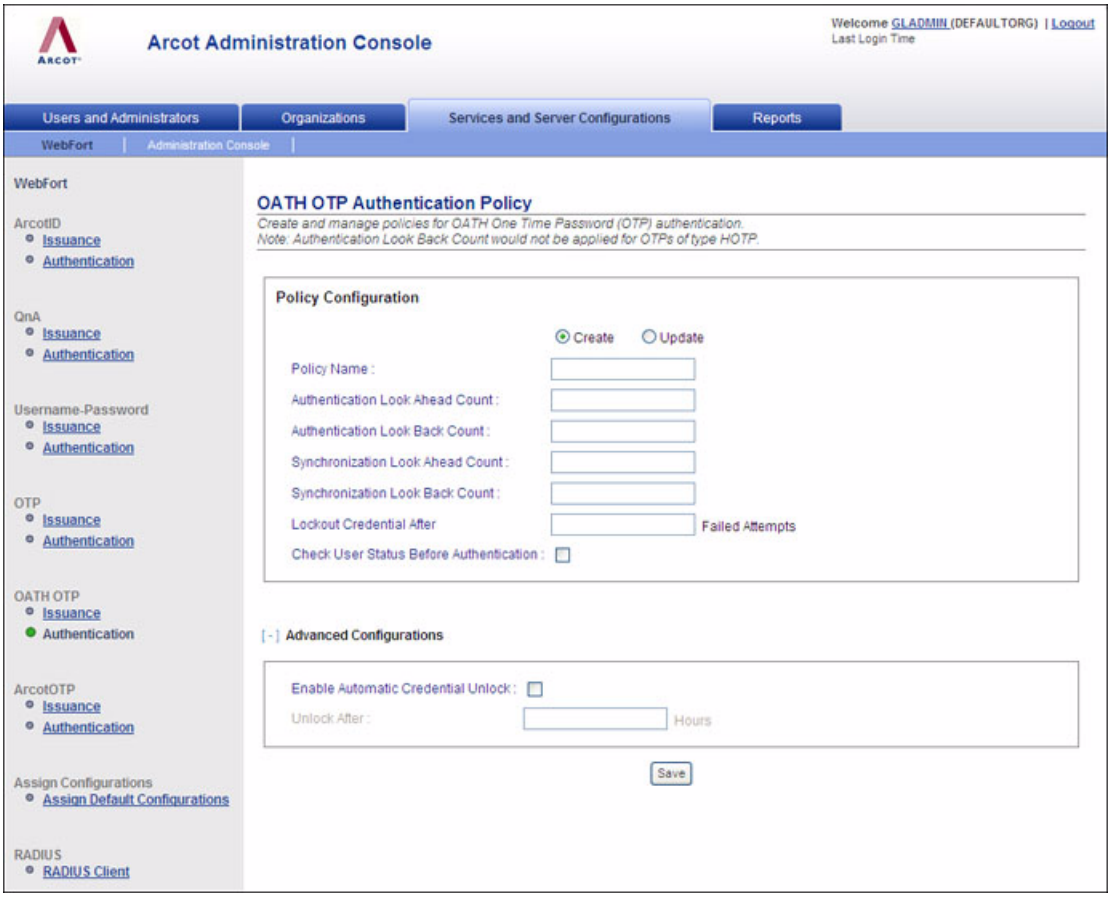
OATH OTP ベースの認証に関連する以下の属性を定義するために OATH OTP ポリシーを使用できます。

- **User status**：ユーザ アカウントのステータスです。アクティブまたは非アクティブのいずれかです。
- **Lockout criteria**：失敗した試行の数です。この数を超えると、ユーザのクレデンシャルがロックされます。
- **Unlocking criteria**：ロックされたクレデンシャルが再使用できるようになるまでの時間数です。

組織の OATH OTP 認証ポリシーを設定する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**OATH OTP**］セクションの［**Authentication**］リンクをクリックすると、［OATH OTP Authentication Policy］ページ（図 4-17）が表示されます。

図 4-17 ［OATH OTP Authentication Policy］ページ



5. 必要に応じて、［**Policy Configuration**］セクションのフィールドに入力します。表 4-15 に、このセクションのフィールドを示します。

表 4-15. OATH OTP 認証ポリシー設定のフィールド

フィールド	説明
[Policy Configurations]	
[Create]	新規ポリシーを作成する場合は、以下の手順に従います。 1. [**Create**] オプションを選択します。 2. 表示されるフィールドに、新規ポリシーの**名前**を指定します。
[Update]	既存のポリシーを更新する場合は、表示される [**Select Policy**] リストから更新するポリシーを選択します。
[Copy Policy]	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。
[Available Policies]	設定をコピーするポリシーを選択します。
[Authentication Look Ahead Count]	ユーザが入力した OATH OTP を確認するために、WebFort サーバの OATH 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 OATH OTP は、現在のカウント – [Authentication Look Back Count] ～現在のカウント + [Authentication Look Ahead Count] 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 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。
[Authentication Look Back Count]	ユーザが入力した OATH OTP を確認するために、WebFort サーバの OATH 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 OATH OTP は、現在のカウント – [Authentication Look Back Count] ～ 現在のカウント + [Authentication Look Ahead Count] 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 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。

表 4-15. OATH OTP 認証ポリシー設定のフィールド（続き）

フィールド	説明
[Synchronization Look Ahead Count]	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、WebFort サーバ上の OATH 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 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 － [Synchronization Look Back Count] ～ 現在のカウント ＋ [Synchronization Look Ahead Count]）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。
[Synchronization Look Back Count]	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、WebFort サーバ上の OATH 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 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 － [Synchronization Look Back Count] ～ 現在のカウント ＋ [Synchronization Look Ahead Count]）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。
[Lockout Credential After]	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。
[Check User Status Before Authentication]	現在のクレデンシャル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場合は、このチェック ボックスをオンにします。 • クレデンシャルの作成 • クレデンシャルの再発行 • クレデンシャルのリセット • クレデンシャルの有効期間のリセット

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。

7. 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。表 4-16 に、このセクションのフィールドを示します。

表 4-16. OATH OTP 認証ポリシーの詳細設定

フィールド	説明
[Advanced Configurations]	
[Enable Automatic Credential Unlock]	クレデンシャルが、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、[Lockout Credential After] フィールドで対応する値を指定する場合のみ有効です。
[Unlock After]	ロックされたクレデンシャル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。

8. OATH OTP ポリシーを作成または更新するには、[**Save**] をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

ArcotOTP 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。

- ArcotOTP 発行プロファイルの設定
- ArcotOTP 認証ポリシーの設定

ArcotOTP 発行プロファイルの設定

ArcotOTP クレデンシャルに関連する以下の属性を指定するために ArcotOTP プロファイルを使用できます。

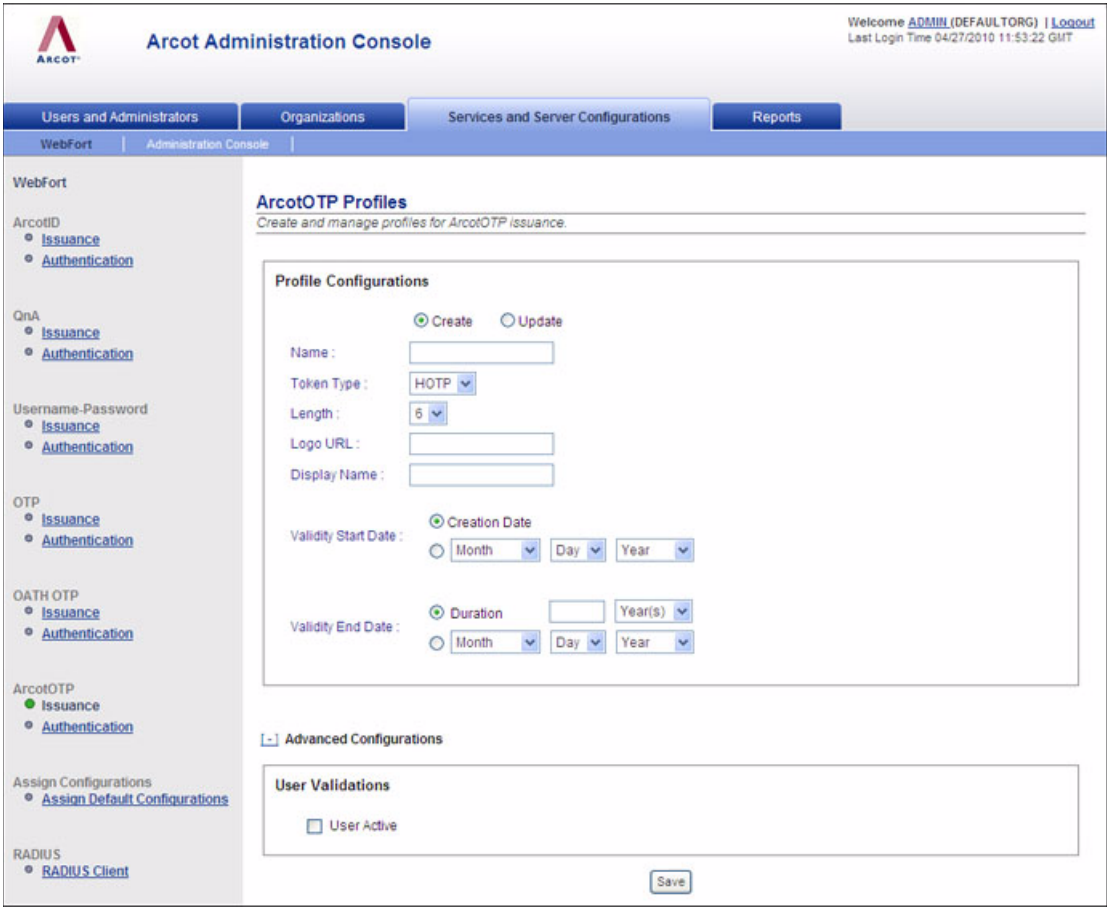
- **Length**：OTP の長さです。
- **Validity period**：ArcotOTP が有効な期間です。

ArcotOTP 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 ArcotOTP クレデンシャルの特性を制御できます。ArcotOTP クレデンシャル プロファイルを作成するには、[ArcotOTP Profiles] ページ（図 4-18）を使用します。

ArcotOTP プロファイルを作成または更新する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**ArcotOTP**］セクションの［**Issuance**］リンクをクリックすると、［ArcotOTP Profiles］ページ（図 4-18）が表示されます。

図 4-18 ［ArcotOTP Profiles］ページ



5. 必要に応じて、［**Profile Configurations**］セクションのフィールドに入力します。
表 4-17 に、このセクションのフィールドを示します。

表 4-17. ArcotOTP プロファイル設定のフィールド

フィールド	説明
［Profile Configurations］	
［Create］	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。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規プロファイルの**名前**を指定します。
［Update］	既存のプロファイルを更新する場合は、表示される［**Select Profile**］リストから更新するプロファイルを選択します。
［Copy Profile］	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。
［Available Profiles］	設定をコピーするプロファイルを選択します。
［Token Type］	ユーザのために作成される必要がある ArcotOTP 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** はタイマ ベースのトークンです。
［Length］	ArcotOTP の長さを設定します。 ArcotOTP 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。
［Logo URL］	ロゴが含まれる URL を入力します。ロゴは、WebFort 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 ArcotOTP 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。
［Display Name］	クライアント デバイス上に ArcotOTP 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） • クレデンシャルのカスタム属性 • ユーザのカスタム属性
［Validity Start Date］	発行された ArcotOTP クレデンシャルが有効になる日付を設定します。 有効期間は、ArcotOTP 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。
［Validity End Date］	ArcotOTP が期限切れになる日付を設定します。 クレデンシャル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。

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。
7. ［**User Validations**］セクションで以下を設定します。
   - 現在のクレデンシャル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場合は、［**User Active**］チェック ボックスをオンにします。
     - クレデンシャルの作成
     - クレデンシャルの再発行
     - クレデンシャルのリセット
     - クレデンシャル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、［**User Attribute**］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。
     - 電子メール アドレス
     - 名
     - ミドル ネーム
     - 姓
     - 電話番号
8. ArcotOTP プロファイルを作成または更新するには、［**Save**］をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

ArcotOTP 認証ポリシーの設定

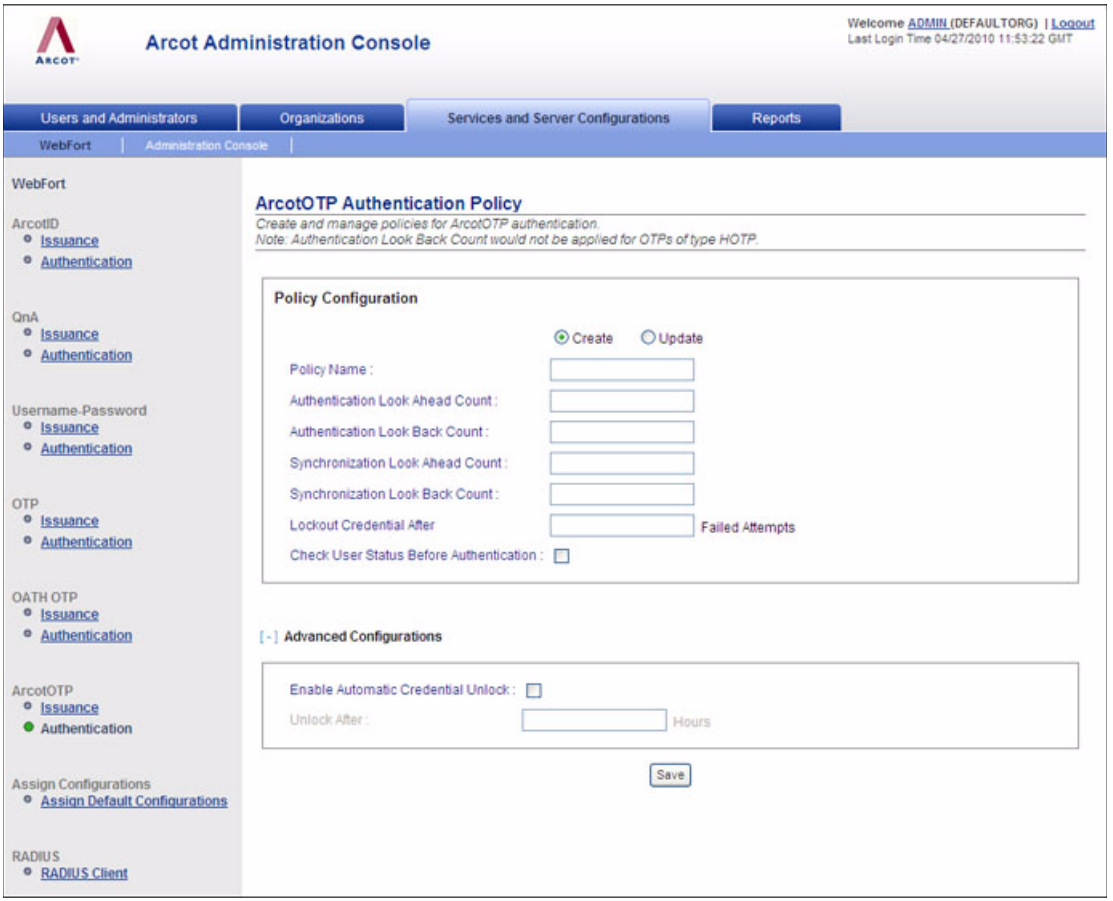
ArcotOTP ベースの認証に関連する以下の属性を定義するために ArcotOTP ポリシーを使用できます。

- **User status**：ユーザ アカウントのステータスです。アクティブまたは非アクティブのいずれかです。
- **Lockout criteria**：失敗した試行の数です。この数を超えると、ユーザのクレデンシャルがロックされます。
- **Unlocking criteria**：ロックされたクレデンシャルが再使用できるようになるまでの時間数です。

組織の ArcotOTP 認証ポリシーを設定する方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**ArcotOTP**］セクションの［**Authentication**］リンクをクリックすると、［ArcotOTP Authentication Policy］ページ（図 4-19）が表示されます。

図 4-19 ［ArcotOTP Authentication Policy］ページ



5. 必要に応じて、［**Policy Configuration**］セクションのフィールドに入力します。
表 4-15 に、このセクションのフィールドを示します。

表 4-18. ArcotOTP 認証ポリシー設定のフィールド

フィールド	説明
[Policy Configurations]	
［Create］	新規ポリシーを作成する場合は、以下の手順に従います。 1. ［**Create**］オプションを選択します。 2. 表示されるフィールドに、新規ポリシーの**名前**を指定します。
［Update］	既存のポリシーを更新する場合は、表示される［**Select Policy**］リストから更新するポリシーを選択します。
［Copy Policy］	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。
［Available Policies］	設定をコピーするポリシーを選択します。
［Authentication Look Ahead Count］	ユーザが入力した ArcotOTP を確認するために、WebFort サーバの ArcotOTP 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 ArcotOTP は、現在のカウント － ［Authentication Look Back Count］～現在のカウント ＋ ［Authentication Look Ahead Count］の範囲でサーバ上で生成されるすべての ArcotOTP と比較され、ユーザが入力した ArcotOTP 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 ArcotOTP 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。
［Authentication Look Back Count］	ユーザが入力した ArcotOTP を確認するために、WebFort サーバの ArcotOTP 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 ArcotOTP は、現在のカウント － ［Authentication Look Back Count］～現在のカウント ＋ ［Authentication Look Ahead Count］の範囲でサーバ上で生成されるすべての ArcotOTP と比較され、ユーザが入力した ArcotOTP 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 ArcotOTP 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。

表 4-18. ArcotOTP 認証ポリシー設定のフィールド（続き）

フィールド	説明
[Synchronization Look Ahead Count]	クライアント デバイス上の ArcotOTP カウンタと同期するために、WebFort サーバ上の ArcotOTP 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 ArcotOTP が同期を取るために、ユーザが 2 つの連続した ArcotOTP を提供する必要があります。これらの ArcotOTP が、検索範囲（カウント － [Synchronization Look Back Count] ～ 現在のカウント ＋ [Synchronization Look Ahead Count]）に含まれる、サーバの連続した ArcotOTP 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 ArcotOTP に対応するカウントに同期されます。
[Synchronization Look Back Count]	クライアント デバイス上の ArcotOTP カウンタと同期するために、WebFort サーバ上の ArcotOTP 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 ArcotOTP が同期を取るために、ユーザが 2 つの連続した ArcotOTP を提供する必要があります。これらの ArcotOTP が、検索範囲（カウント － [Synchronization Look Back Count] ～ 現在のカウント ＋ [Synchronization Look Ahead Count]）に含まれる、サーバの連続した ArcotOTP 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 ArcotOTP に対応するカウントに同期されます。
[Lockout Credential After]	失敗した試行の数を指定します。この数を超えると、ArcotOTP がロックされます。
[Check User Status Before Authentication]	現在のクレデンシャル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場合は、このチェック ボックスをオンにします。 • クレデンシャルの作成 • クレデンシャルの再発行 • クレデンシャルのリセット • クレデンシャルの有効期間のリセット

6. ［**Advanced Configurations**］セクションを展開するには、［**+**］記号をクリックします。

7. 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。表 4-16 に、このセクションのフィールドを示します。

表 4-19. ArcotOTP 認証ポリシーの詳細設定

フィールド	説明
[Advanced Configurations]	
[Enable Automatic Credential Unlock]	クレデンシャルが、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、[Lockout Credential After] フィールドで対応する値を指定する場合のみ有効です。
[Unlock After]	ロックされたクレデンシャル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。

8. ArcotOTP ポリシーを作成または更新するには、[**Save**] をクリックします。
9. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

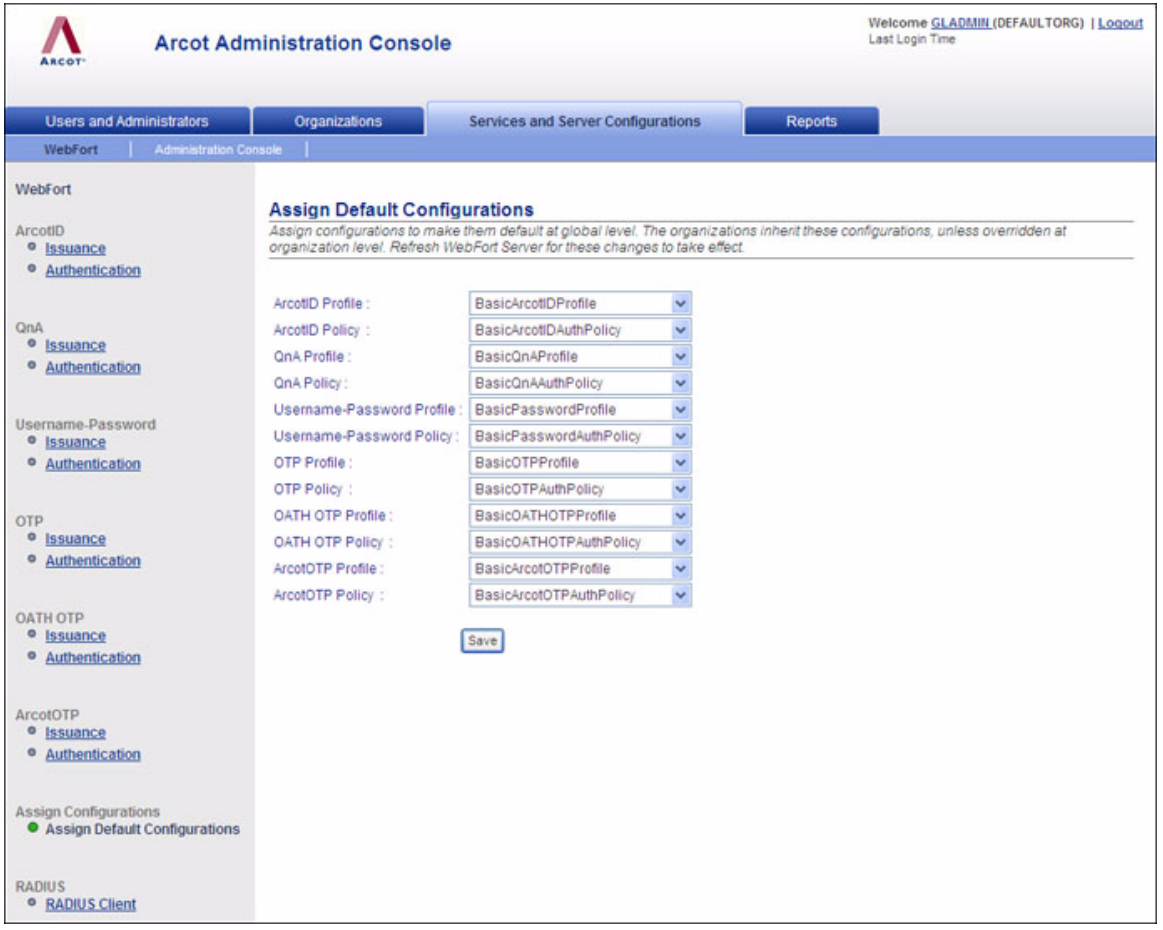
デフォルト設定の割り当て

目的のクレデンシャル プロファイルおよび認証ポリシーを作成した後、[Assign Default Configurations] ページを使用して、それらを全体的に（GA として）または特定の組織（Organization Administrator として）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する必要があります。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 レベルに設定を適用する方法について説明します。組織の設定の割り当て方法については、5-149 ページの「組織固有の設定の管理」を参照してください。

注： Organization Administrator （OA）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。

図 4-20 ［Assign Default Configurations］ページ



デフォルト設定をグローバルとして割り当てる方法

1. Global Administrator （GA）として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［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**Assign Configurations**］セクションの［**Assign Default Configuration**］リンクをクリックすると、対応するページ（図 4-20）が表示されます。

5. 対応するドロップダウン リストからクレデンシャル プロファイルまたは認証ポリシーを選択します。

   各クレデンシャル イプのデフォルト プロファイル（**Basic<Credential_*Name*>Profile**）またはポリシー（**Basic<Credential_*Name*>AuthPolicy**）もこれらのリストで使用可能です。

6. デフォルト プロファイルおよびポリシーを割り当てるには、［**Save**］をクリックします。

注： これらのプロファイルとポリシーは組織レベルの設定で優先できます。

7. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

RADIUS クライアントの設定

設定された場合、WebFort 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 クライアントは SSL VPN（Virtual Private Networks）および IPSec（Internet Protocol Security）VPN として分類できます。

SSL VPN ワークフロー

通常、クライアントレスまたは SSL VPN の認証ワークフローは以下のとおりです。

1. ユーザは、クレデンシャルを提供することによって、セキュリティ保護されている Web サイトにアクセスしようとします。
2. WebFort サーバに統合されたユーザのアプリケーションは、ユーザ認証を実行し、WebFort サーバによって生成されたワンタイム トークン（OTT）によるレスポンスを返します。
3. OTT は検証のために VPN ゲートウェイを介して WebFort サーバに送信されます。
4. WebFort サーバはトークンを検証します。
5. 認証トークンの検証に成功した後、ユーザはセキュリティ保護されている Web サイトへのアクセス権を付与されます。

IPSec VPN ワークフロー

IPSec VPN の認証ワークフローは通常以下のとおりです。

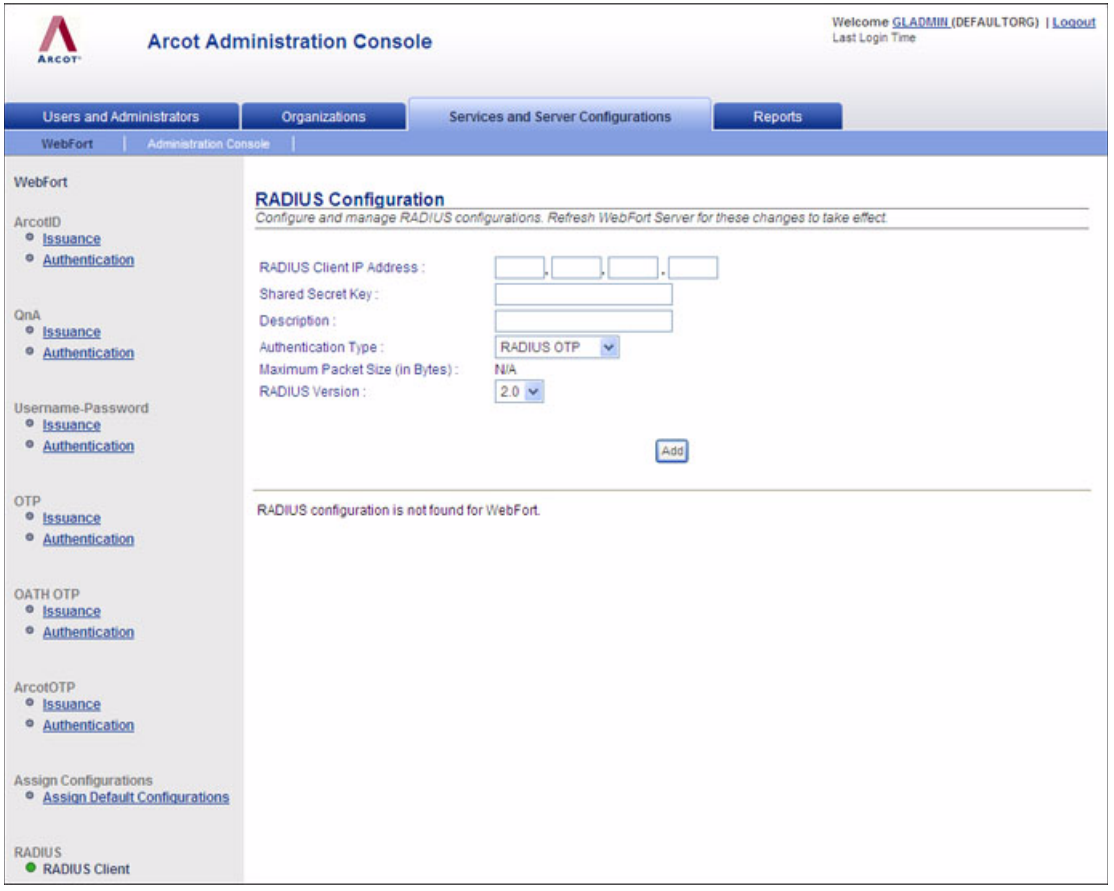
1. ユーザは、クレデンシャルを提供することによって、セキュリティ保護されている Web サイトにアクセスしようとします。
2. ユーザは Q&A と ArcotID を作成することによりサイン アップします。
3. ユーザは ArcotID をダウンロードします。
4. VPN クライアントのログイン ページで、ユーザは、VPN ゲートウェイを介して WebFort サーバに認証されるために、ユーザ名および ArcotID パスワードを指定します。
5. WebFort サーバはトークンを検証します。
6. 認証トークンの検証に成功した後、ユーザはセキュリティ保護されている Web サイトへのアクセス権を付与されます。

RADIUS クライアントの設定

組織の RADIUS クライアントを設定する方法

1. 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. メイン メニューの［**Services and Server Configurations**］タブをアクティブにします。
3. サブメニュー内の［**WebFort**］タブがアクティブであることを確認します。
4. ［**RADIUS**］セクションの［**RADIUS Client**］をクリックすると、対応するページ（図 4-21）が表示されます。

図 4-21 ［RADIUS Configuration］ページ



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 Client IP Address**］：ユーザが WebFort サーバに認証される RADIUS クライアントの IP アドレスです。

- ［**Shared Secret Key**］: RADIUS クライアントと WebFort サーバの間で共有される秘密キーです

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。
- ［**Authentication Type**］: 認証に使用される認証メカニズムを選択します。
  - ［**RADIUS OTP**］: SSL VPN クライアントに使用されます。
  - ［**In-Band ArcotID**］: IPSec VPN クライアントに使用されます。
- ［**Maximum Packet Size (in Bytes)**］: RADIUS メッセージの適切なパケット サイズを選択します。

関連文書 : パケットのフォーマットの詳細については、*RFC 2865* を参照してください。

- ［**RADIUS Version**］: 追加するクライアントでサポートされる RADIUS のバージョンを指定します。

6. 新しい RADIUS クライアントの IP アドレスを追加するには、［**Add**］をクリックします。
7. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

RADIUS クライアントの更新および削除

設定が検出される場合、［RADIUS Configuration］ページには［**Configured RADIUS Clients**］表が表示されます。この表を使用して、RADIUS クライアントの IP アドレスを更新または削除できます。

RADIUS クライアントの更新

RADIUS クライアントを更新する方法

1. ［**Configured RADIUS Clients**］セクションで、更新する IP アドレスを選択します。
2. 選択した IP アドレスの該当する列を更新し、［**Update**］をクリックします。
3. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。

   この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

RADIUS クライアントの削除

RADIUS クライアントを削除する方法

1. ［**Configured RADIUS Clients**］画面で、削除する IP アドレスを選択します。
2. ［**Delete**］をクリックします。
3. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。

   この方法の詳細については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

第 5 章
組織の管理

Arcot Administration Console では、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。Administration Console に用意されている組織構造はフラットです。つまり、組織階層（親組織と子組織の形式）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 （デフォルトの組織の詳細については、2-28 ページの「組織のグローバル設定の指定」を参照してください）。

企業の規模が大きくなるほど、その組織構成は複雑になります。その結果、組織の管理は管理の中でも特に重要な部分になっています。WebFort 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
- 組織の検索
- 組織固有の設定の管理
- 組織情報の更新
- 組織の無効化
- 組織の有効化
- 初期状態の組織のアクティブ化
- 組織の削除

組織の作成とアクティブ化

組織を作成し、WebFort 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（Microsoft Active Directory や Sun ONE Directory Server など）にそのデータを保存できます。

	**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、実際の実装に基づいて、以下の手順について説明します。

- Arcot リポジトリでの組織の作成
- LDAP リポジトリでの組織の作成

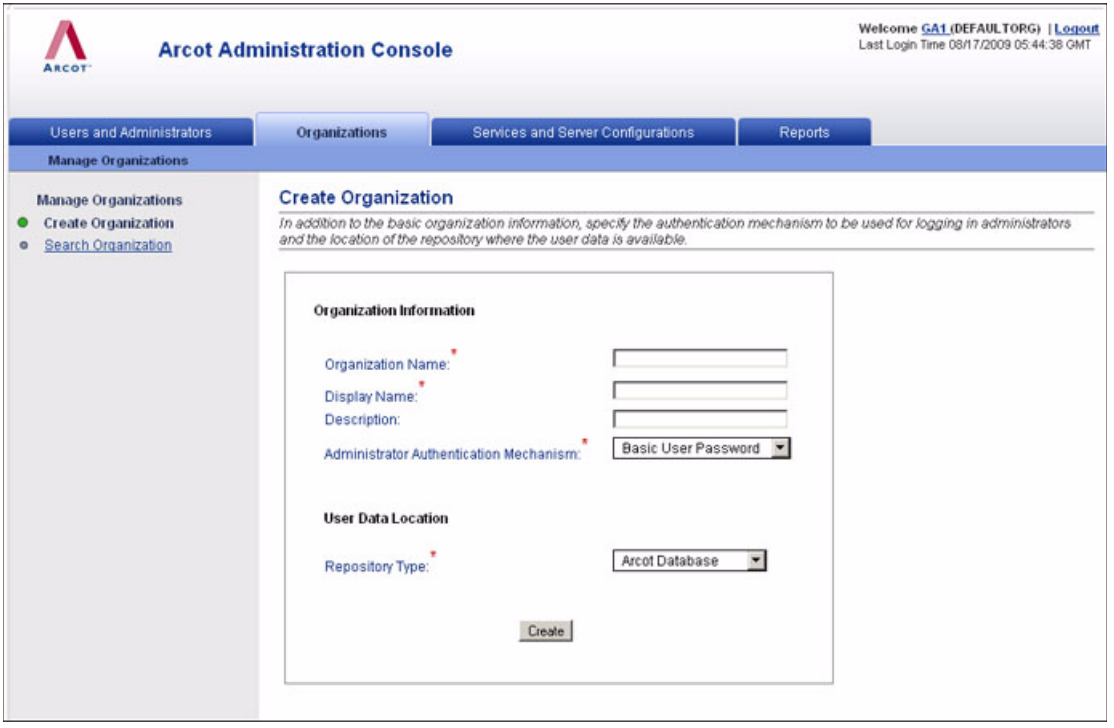
	注： 組織を作成してアクティブ化できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。MA はすべての組織を作成してアクティブ化できます。GA と OA は、自分のスコープに含まれるすべての組織を作成してアクティブ化できます。

Arcot リポジトリでの組織の作成

Arcot リポジトリに組織を作成する方法

1. 組織の作成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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Create Organization**］リンクをクリックして［Create Organization］ページ（図 5-1）を表示します。

図 5-1 ［Create Organization］ページ



4. 表 5-1 の説明に従って組織の詳細を入力します。

表 5-1. ［Create Organization］のフィールド

フィールド	説明
［Organization Information］	
［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［Display Name］ではなく、この値を指定する必要があります。
［Display Name］	組織のわかりやすい名前を入力します。 **注：** この名前は、Administration Console の他のすべてのページとレポートに表示されます。

表 5-1. ［Create Organization］のフィールド

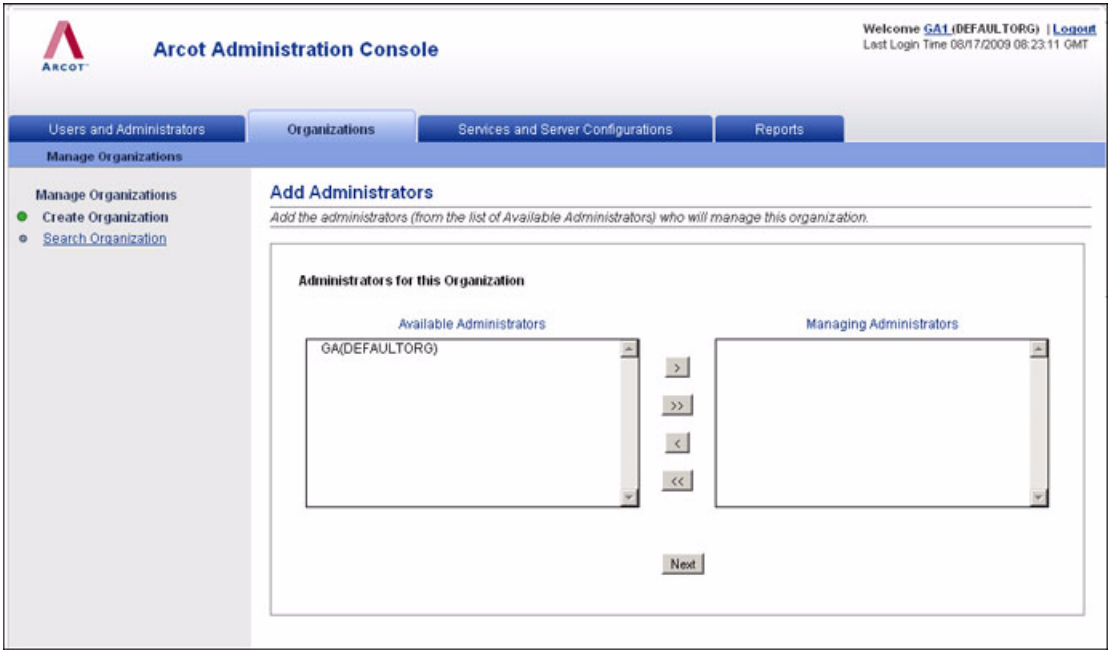
フィールド	説明
［Description］	この組織を管理する管理者に関する説明を入力します。 **注：** このフィールドを使用して、後で組織を参照するときに役立つ追加の詳細を入力できます。
［Administrator Authentication Mechanism］	この組織に属する管理者を認証するために使用されるメカニズムを選択します。 Administration Console では、以下の 2 種類の認証メカニズムがサポートされます。 • **Basic User Password** これは、Administration Console によって提供される組み込みの認証メカニズムです。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コンソールにログインします。 • **WebFort User Password** これは、WebFort のユーザ名 - 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、管理者のクレデンシャルは WebFort 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、［WebFort Connectivity］ページを使用して Administration Console を WebFort サーバに接続する必要があります。詳細については、3-38 ページの「WebFort Connectivity の設定」を参照してください。
［User Data Location］	
［Repository Type］	［**Arcot Database**］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 WebFort でサポートされている RDBMS リポジトリに保存されます。

5. ［**Create**］ボタンをクリックして新しい組織を作成します。

   ［Add Administrators］ページ（図 5-2）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*。

図 5-2 Add Administrators



6. ［**Available Administrators**］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［**Managing Administrators**］リストに追加します。

   ［**Available Administrators**］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。

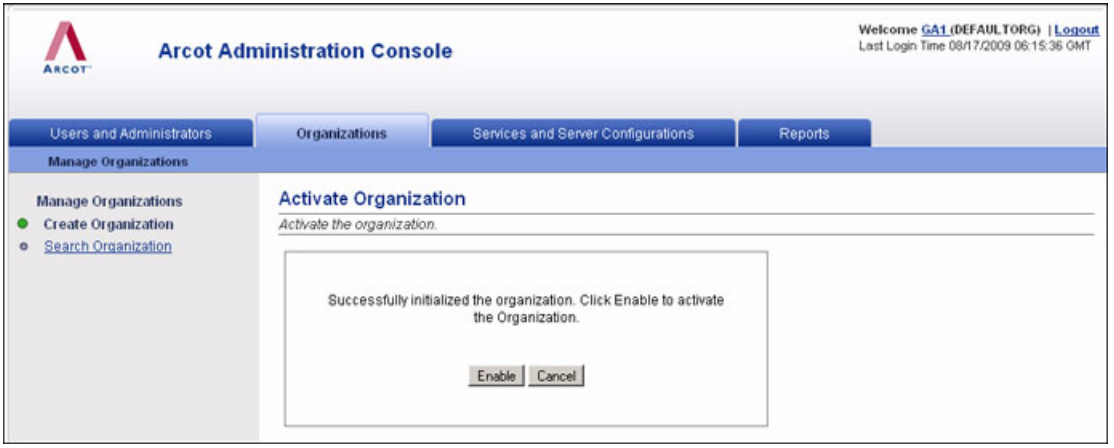
> **注：** 一部の管理者がシステム内のすべての組織を管理するためのスコープを持っている場合、このリストにはそれらの管理者に対応するエントリは表示されません。

   ［**Managing Administrators**］リストには、この組織を管理するために選択された管理者が表示されます。

7. ［**Next**］ボタンをクリックして続行します。

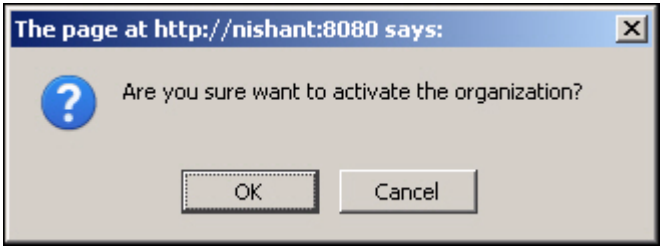
   ［Activate Organization］ページ（図 5-3）が表示されます。

図 5-3 Activate Organization



8. ［**Enable**］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。
   図 5-4 に示すメッセージ ボックスが表示されます。

図 5-4 組織のアクティブ化：メッセージ



9. ［**OK**］ボタンをクリックして処理を完了します。
10. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。この作業の方法については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

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、Arcot リポジトリに組織を作成してから、Arcot の属性を LDAP の属性にマップする必要があります。以下の手順に従ってください。

1. 組織の作成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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Create Organization**］リンクをクリックして［Create Organization］ページ（図 5-1）を表示します。
4. 表 5-2 の説明に従って組織の詳細を入力します。

表 5-2. LDAP リポジトリにおける［Create Organization］のフィールド

フィールド	説明
［Organization Information］	
［Organization Name］	作成する組織に対する一意の ID を入力します。 **注：** Administration Console を使ってこの組織にログインするには、組織の［Display Name］ではなく、この値を指定する必要があります。
［Display Name］	組織のわかりやすい名前を入力します。 **注：** この名前は、Administration Console の他のすべてのページと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、後で組織を参照するときに役立つ追加の詳細を入力できます。
［Administrator Authentication Mechanism］	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。 Administration Console では、以下の 2 種類の認証メカニズムがサポートされます。 • **Basic User Password** これは、Administration Console 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。 • **WebFort User Password** これは、WebFort のユーザ名 - 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、管理者のクレデンシャルは WebFort サーバによって発行され、認証されます。

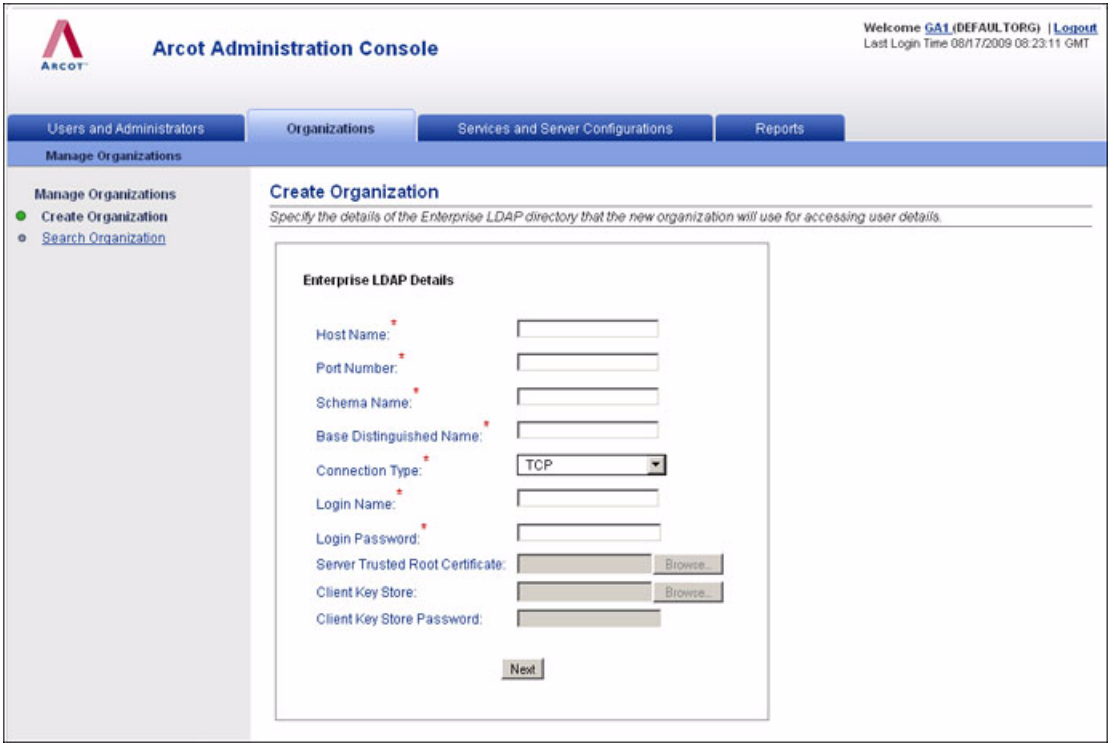
表 5-2. LDAP リポジトリにおける［Create Organization］のフィールド

フィールド	説明
［User Data Location］	
［Repository Type］	［**Enterprise 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と管理者の詳細が次のページで指定する LDAP リポジトリに保存されます。

5. ［**Create**］ボタンをクリックして新しい組織を作成します。

   LDAP リポジトリの詳細を収集するための［Create Organization］ページ（図 5-5）が表示されます。

図 5-5 Create Organization: Enterprise LDAP Details



6. LDAP リポジトリに接続するための詳細を入力します。入力項目を表 5-3 に示します。

表 5-3. LDAP リポジトリの詳細

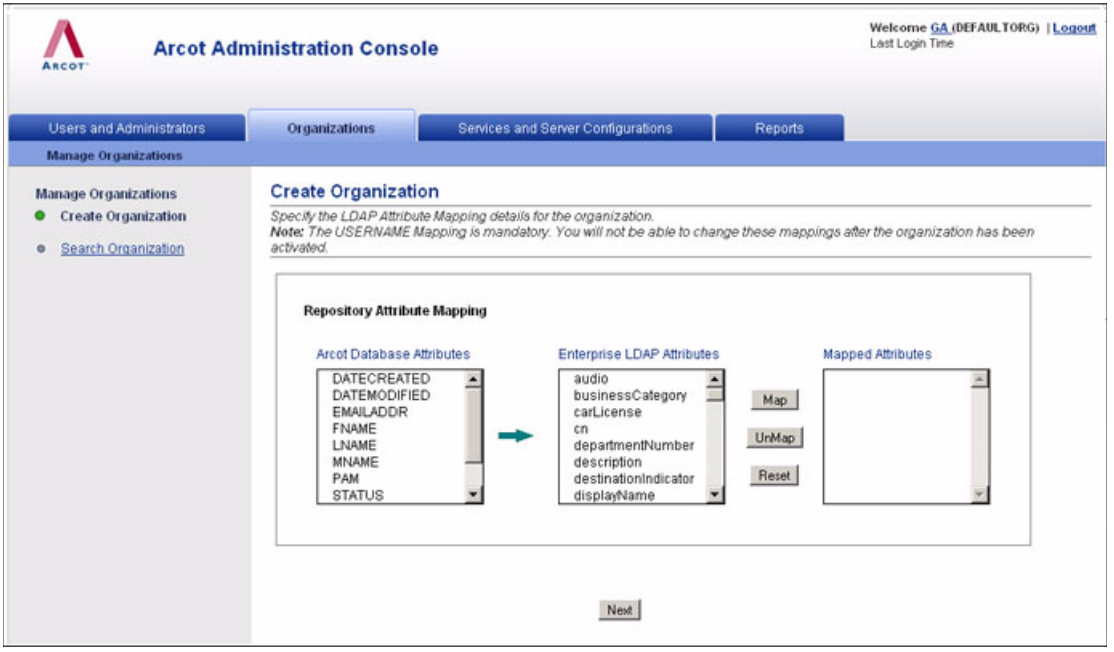
フィールド	説明
［Host Name］	LDAP リポジトリを使用できるシステムのホスト名を入力します。
［Port Number］	LDAP リポジトリ サービスがリスニングしているポート番号を入力します。
［Schema Name］	LDAP リポジトリで使用される LDAP スキーマを指定します。このスキーマには、LDAP リポジトリに含めることができるオブジェクトのタイプと、各オブジェクト タイプの必須属性および任意属性が指定されます。 通常、Active Directory のスキーマ名は `user` であり、SunOne Directory のスキーマ名は `inteorgperson` です。
［Base Distinguished Name］	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。
［Connection Type］	Administration Console 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
［Login Name］	リポジトリ サーバにログインし、［Base Distinguished Name］を管理する権限を持つ LDAP リポジトリ ユーザの完全識別名を入力します。 例を以下に示します。 `uid=gt,dc=arcot,dc=com`
［Login Password］	［Login Name］で指定したユーザのパスワードを入力します。
［Server Trusted Root Certificate］	必要な SSL オプションが選択されている場合は、［**Browse**］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。

表 5-3. LDAP リポジトリの詳細

フィールド	説明
[Client Key Store Path]	必要な SSL オプションが選択されている場合は、[**Browse**] ボタンを使用してクライアント証明書と対応するキーを含むキーストアのパスを入力します。 **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する必要があります。
[Client Key Store Password]	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。

7. [**Next**] 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（図 5-6）が表示されます。

図 5-6 組織の作成：リポジトリ属性のマッピング



8. このページで、以下の作業を実行します。

a. ［**Arcot Database Attributes**］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［**Enterprise LDAP Attributes**］リストから選択して［**Map**］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 `cn` 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。

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 Database Attributes**］リスト内の属性をすべてマップする必要はありません。マップする必要があるのは、使用する属性のみです。

マップされた属性は［**Mapped Attributes**］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［**Unmap**］ボタンをクリックします。ただし、［**Mapped Attribute**］リストをクリアする場合は、［**Reset**］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。

9. ［**Next**］ボタンをクリックして続行します。

［Add Administrators］ページ（図 5-2）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*。

10. ［**Available Administrators**］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［**Managing Administrators**］リストに追加します。

> **注 :** 管理者への組織の割り当ては、既存の管理者のスコープを更新するか、または組織を管理する新しい管理者を作成することによっていつでも実行できます。

［**Available Administrators**］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、このリストにはそれらの管理者に対応するエントリは表示されません。

［**Managing Administrators**］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. ［**Next**］ボタンをクリックして続行します。

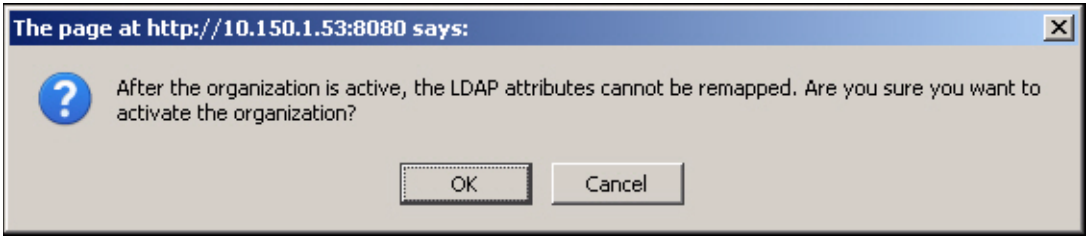
    ［Activate Organization］ページ（図 5-3）が表示されます。

> **注：** 組織がアクティブになると、マッピングの詳細を変更したり、更新したりできなくなります。

12. ［**Enable**］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。

    図 5-7 に示す警告メッセージが表示されます。

図 5-7 LDAP ベースの組織のアクティブ化



13. ［**OK**］ボタンをクリックして処理を完了します。

組織の検索

注： 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、検索する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。

組織の検索には、名前とステータスを使用できます。1 つ以上の組織を検索するには、以下の手順に従います。

1. 組織の作成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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。

図 5-8 ［Search Organization］ページ

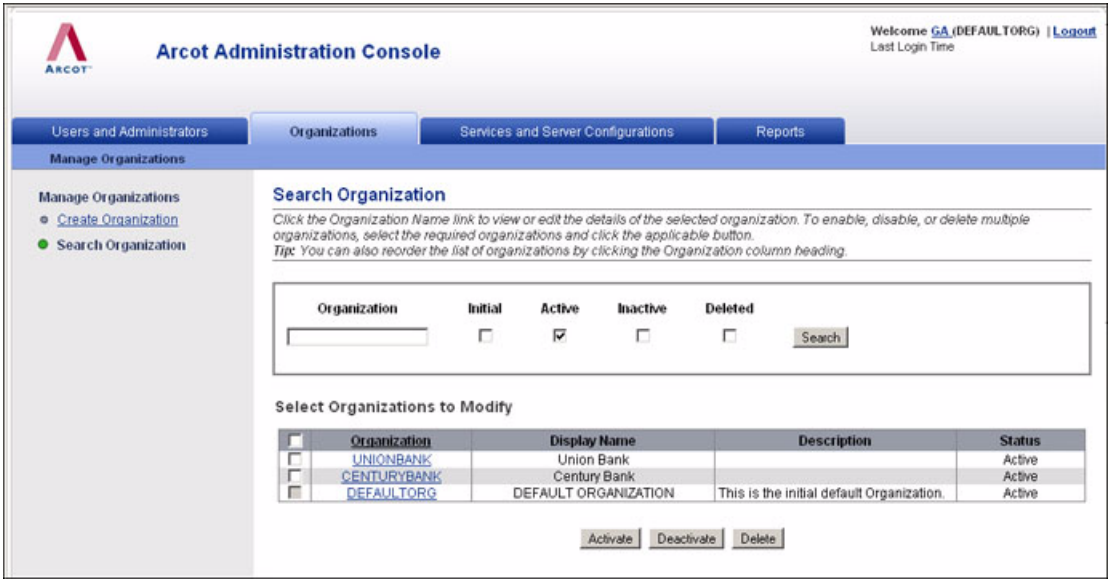
4. 必要な組織の情報の一部または全部を入力します。以下のオプションを選択して、検索の範囲を広げることができます。

注： ［**Organization**］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。

- ［**Initial**］（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）
- ［**Active**］（作成され、アクティブ化された組織を表示する場合）
- ［**Inactive**］（無効化された組織を表示する場合）
- ［**Deleted**］（削除された組織を表示する場合）

5. ［**Search**］ボタンをクリックすると、（図 5-9 のように）指定した条件に一致するすべての組織がページ上に表示されます。

図 5-9 ［Search Organization］ページ：結果



組織固有の設定の管理

組織を管理するスコープを持っている GA または OA は、個々の組織用の設定を行うことができます。組織固有の設定を行うと、第 4 章の「グローバルな WebFort 設定の管理」で説明したように、組織固有の設定によってグローバル設定が上書きされます。

注 : 組織の設定を管理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 は組織固有の設定を管理 *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。

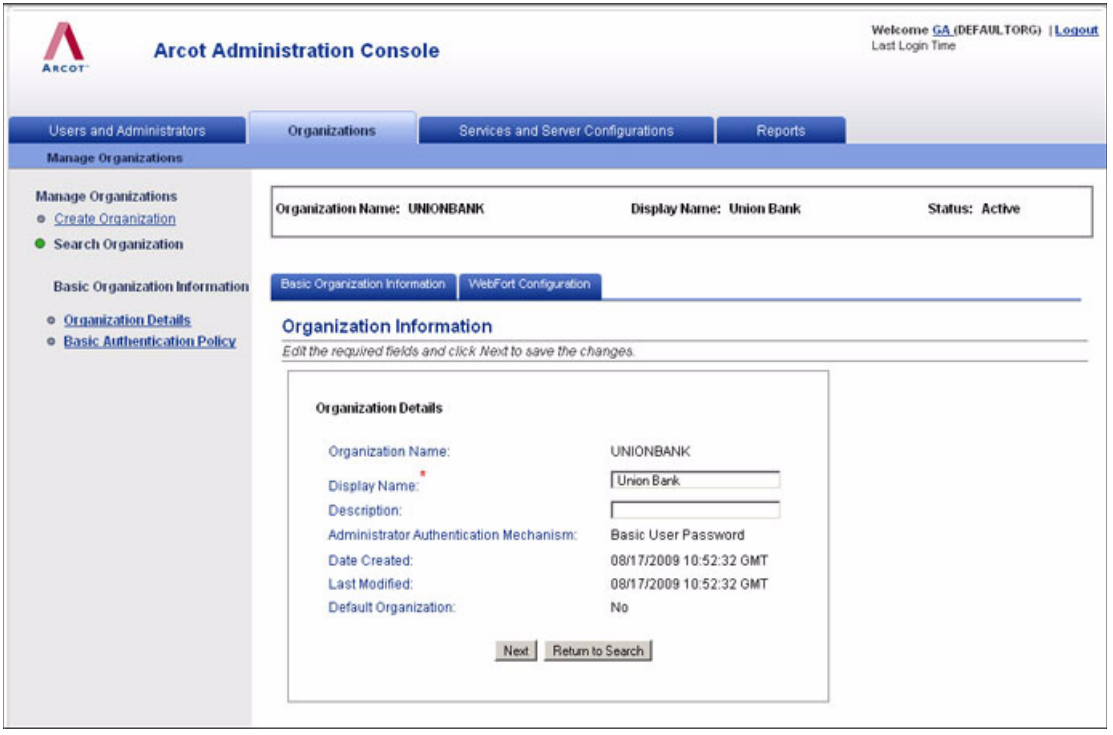
組織固有の設定はグローバル設定に似ていますが、それぞれのタスク ページへのナビゲーション パスは異なります。組織固有の設定を行うためのタスク ページにアクセスするには、以下の手順に従います。

1. 組織の作成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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］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（図 5-9 のように）表示されます。
5. ［**Organization**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

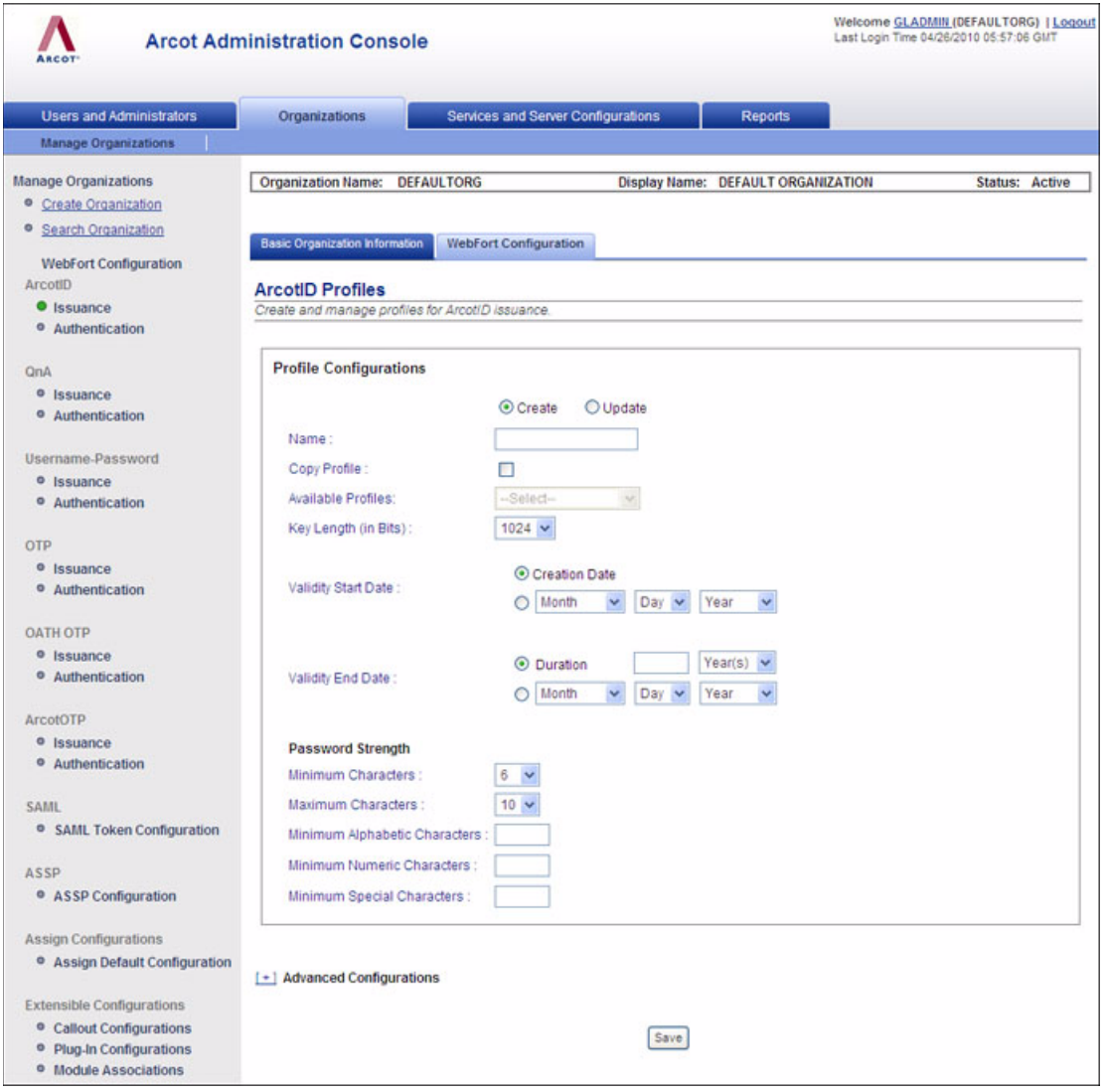
   （図 5-10 のような）［Organization Information］ページが表示されます。

図 5-10 ［Organization Information］ページ



6. ［**WebFort Configuration**］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（図 5-11）。

図 5-11 組織固有の WebFort 設定



7. クレデンシャル 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、必要に応じて第 4 章の「グローバルな WebFort 設定の管理」を参照してください。第 4 章の「グローバルな WebFort 設定の管理」で説明している操作はグローバル レベルですが、この章で説明している設定は組織レベルです。設定内容はどちらも同じですが、このセクションの冒頭で説明したように、タスク ページにアクセスする方法のみが異なります。

組織の ArcotID、Q&A、ユーザ名 - パスワード、OTP、OATH OTP、および ArcotOTP のプロファイルとポリシーに加えて、以下の組織固有の設定項目も設定できます。

- SAML トークンの設定
- ASSP の設定
- コールアウトの設定
- プラグインの設定
- イベントの関連付け

SAML トークンの設定

認証に成功すると、WebFort からトークンを返すことができます。WebFort はさまざまな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。

SAML を認証トークンとして発行する場合は、SAML トークンのプロパティを設定する必要があります。以下の手順に従ってください。

1. 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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

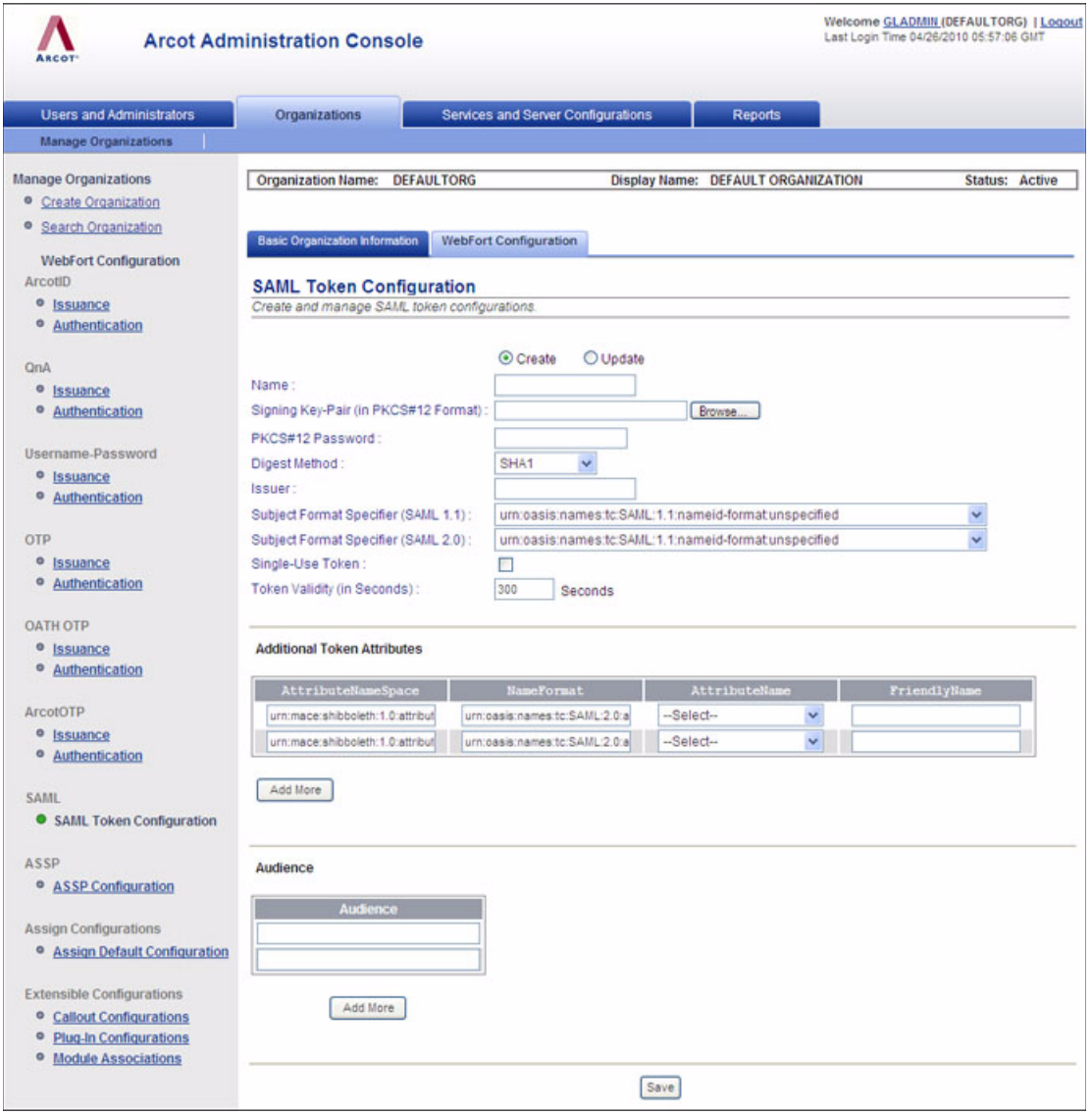
   検索条件に一致する組織のリストが（図 5-9 のように）表示されます。
5. ［**Organization**］列で、必要な組織の <*ORGANIZATION_NAME*> リンクをクリックします。

   （図 5-10 のような）［Organization Information］ページが表示されます。
6. ［**WebFort Configuration**］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（図 5-11）。

7. ［**SAML**］で、［**SAML Token Configuration**］リンクをクリックして［SAML Token Configuration］ページ（図 5-12）を表示します。

図 5-12 ［SAML Token Configuration］ページ



8. 新しい SAML 設定を作成するか、既存の SAML 設定を更新するかに応じて、それぞれのオプションを選択します。
   - 新しい設定を作成する場合は、［**Create**］を選択し、［**Name**］フィールドに設定名を入力します。

     または
   - 既存の設定を更新する場合は、［**Update**］を選択し、［**Name**］リストから更新する設定を選択します。
9. ［**Signing Key-Pair (in PKCS#12 Format)**］で、SAML 証明書と秘密キーが用意されている PKCS#12 ストアの場所に移動します。
10. 対応する［**PKCS#12 Password**］を入力します。
11. ［**Digest Method**］フィールドに、SAML トークンのハッシュ操作に使用されるアルゴリズム（SHA1、SHA256、SHA384、SHA512、RIPEMD 160 など）を指定します。
12. WebFort で生成された SAML トークンを提供する［**Issuer**］の名前を入力します。

    たとえば、XYZ 社が WebFort 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。
13. ［**Subject Format Specifier (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。
14. ［**Subject Format Specifier (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。
15. 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、［**Single-Use Token**］オプションを有効にします。
16. ［**Token Validity (in Seconds)**］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。
17. ［**Additional Token Attributes**］セクションで、追加の属性を設定します（SAML トークンの生成に必要な場合）。

    必要な場合は、［**Add More**］ボタンをクリックして属性を追加します。
18. ［**Audience**］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。

    必要な場合は、［**Add More**］ボタンをクリックしてオーディエンスを追加します。
19. ［**Save**］ボタンをクリックして SAML トークンの設定を保存します。

20. 展開したすべてのWebFort サーバ インスタンスをリフレッシュします。この作業の方法については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」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、Arcot SignFort を使用して PDF 文書に署名するために使用されます。署名の前に、WebFort の認証方式を使っ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。

ASSP を設定する方法

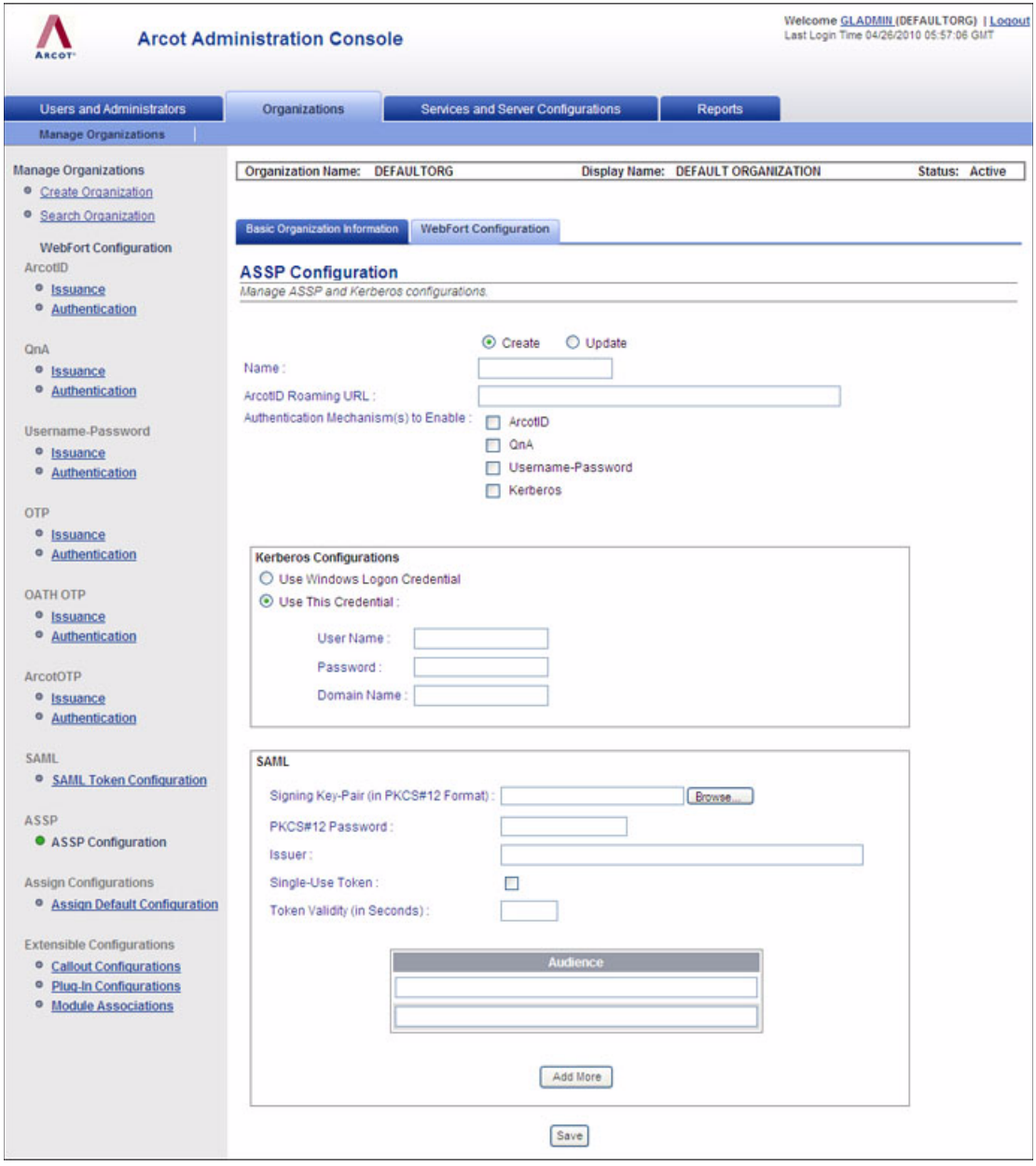
1. 必要な権限とスコープでログインしていることを確認します。
2. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

   検索条件に一致する組織のリストが（図 5-9 のように）表示されます。
5. ［**Organization**］列で、必要な組織の <*ORGANIZATION_NAME*> リンクをクリックします。

   （図 5-10 のような）［Organization Information］ページが表示されます。
6. ［**WebFort Configuration**］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（図 5-11）。
7. ［**ASSP**］で、［**ASSP Configuration**］リンクをクリックして［ASSP Configuration］ページ（図 5-13）を表示します。

図 5-13 ［ASSP Configuration］ページ



8. 新しい ASSP 設定を作成するか、既存の ASSP 設定を更新するかに応じて、それぞれのオプションを選択します。
   - 新しい設定を作成する場合は、［**Create**］を選択し、［**Name**］フィールドに設定名を入力します。

     または
   - 既存の設定を更新する場合は、［**Update**］を選択し、［**Name**］リストから更新する設定を選択します。
9. ArcotID のローミング ダウンロードで ArcotID をダウンロードするために使用される［**ArcotID Roaming URL**］を入力します。

   ArcotID のローミング ダウンロードでは、現在のシステムにユーザの ArcotID が存在しない場合に、［**ArcotID Roaming URL**］を使って WebFort サーバに対する認証が行われ、ユーザの ArcotID がダウンロードされます。
10. ［**Authentication Mechanism(s) to Enable**］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。

    ［**ArcotID**］認証方式を有効にした場合は、ArcotID 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。
11. 前の手順で［**Kerberos**］認証方式を有効にした場合は、［**Kerberos Configurations**］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。
    - WebFort サーバ プロセスの Kerberos トークンを使用する場合は、［**Use Windows Logon Credential**］オプションを選択します。

      または
    - ［**User Name**］、［**Password**］、および［**Domain Name**］フィールドに、Kerberos 認証用の新しいクレデンシャルを指定します。
12. ［**SAML**］セクションで、以下の作業を実行します。
    a. ［**Signing Key-Pair (in PKCS#12 Format)**］フィールドに PKCS#12 ストアの場所を指定します。このストアには、WebFort サーバが SAML トークンを発行するために使用する証明書と秘密キーが含まれています。
    b. 対応する［**PKCS#12 Password**］を入力します。
    c. ［**Issuer**］フィールドに WebFort サーバの URL を入力します。
    d. 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、［**Single-Use Token**］オプションを有効にします。

e. ［**Token Validity (in Seconds)**］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。

f. ［**Audience**］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、［**Add More**］ボタンをクリックします。

13. ［**Save**］ボタンをクリックして ASSP の設定を保存します。

14. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。

この作業の方法については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

コールアウトの設定

*コールアウト*は、WebFort サーバによって公開されたイベントを提供する HTTP ベースの外部プロセスです。WebFort サーバが送信するデータには、エンコードされた URL と共に、HTTP POST の名前 - 値ペアのデータが含まれます。

コールアウトを設定する方法

1. 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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］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（図 5-9 のように）表示されます。

5. ［**Organization**］列で、必要な組織の <*ORGANIZATION_NAME*> リンクをクリックします。

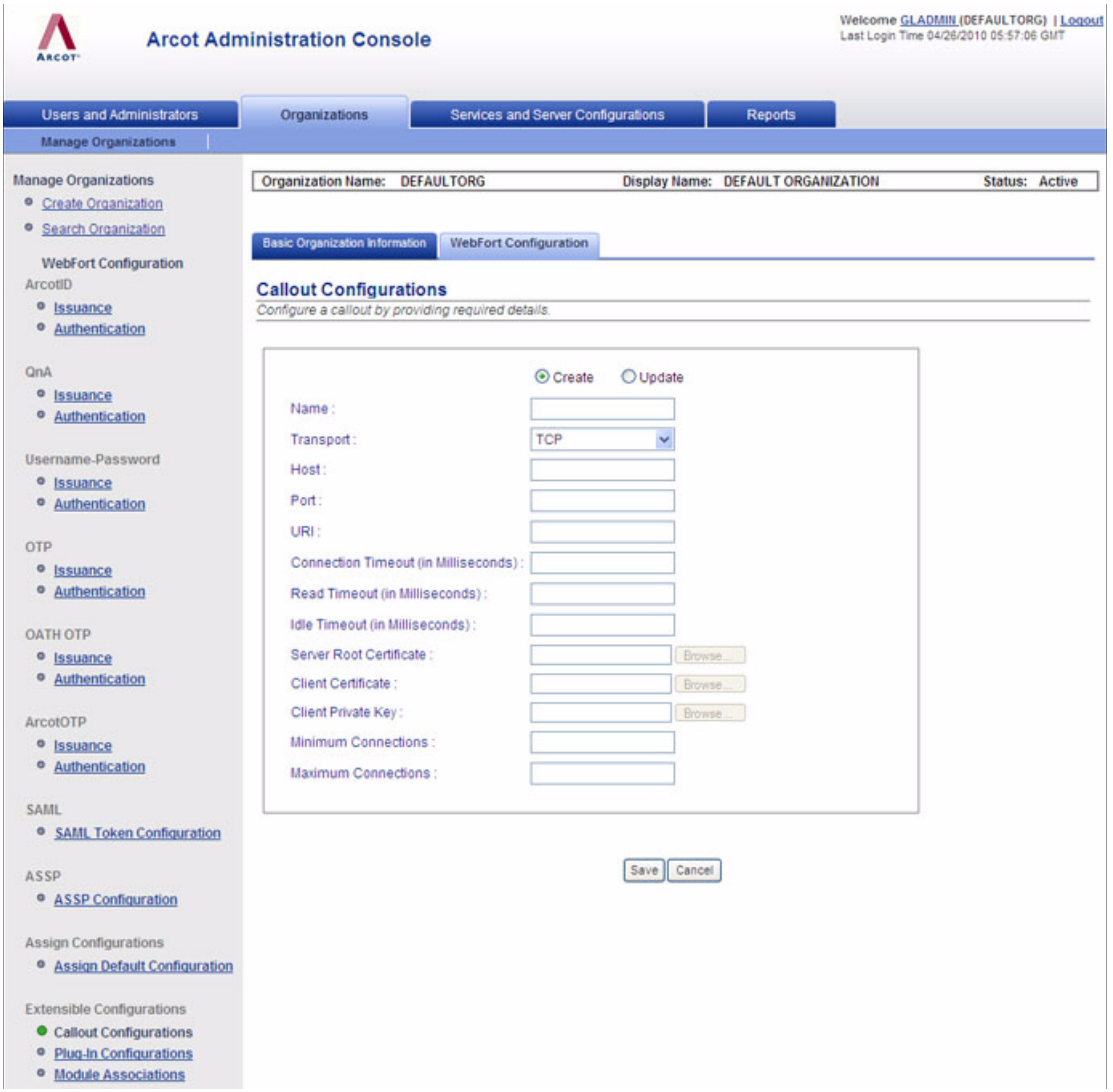
（図 5-10 のような）［Organization Information］ページが表示されます。

6. ［**WebFort Configuration**］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（図 5-11）。

7. ［**Extensible Configurations**］で、［**Callout Configurations**］リンクをクリックして［Callout Configurations］ページ（図 5-14）を表示します。

図 5-14 ［Callout Configuration］ページ



8. 必要に応じて、このページのフィールドを編集します。表 5-4 に、このセクションのフィールドを示します。

表 5-4. コールアウトの登録

ページ フィールド	説明
［Create］	新しいコールアウトを作成する場合は、以下の手順に従います。 1. ［**Create**］オプションを選択します。 2. ［**Name**］フィールドに新しいコールアウトの名前を指定します。
［Update］	既存のコールアウトを更新する場合は、［**Name**］リストから更新するコールアウトを選択します。
［Transport］	サポートされている以下のいずれかのデータ転送モードを指定します。 • ［**TCP**］：コールアウト サーバと WebFort サーバ間のデフォルト モードです。データをクリア テキストで送信します。 • ［**One-Way SSL**］：一方向 SSL（Secure Sockets Layer）では、データの暗号化と復号化に加えて、コールアウト サーバがセッションごとに WebFort サーバに対する認証を行うため、トランザクションに高度なセキュリティが提供されます。 • ［**Two-Way SSL**］：双方向 SSL では、データの暗号化と復号化に加えて、コールアウト サーバと WebFort サーバがセッションごとに相互に認証を行うため、トランザクションに高度なセキュリティが提供されます。 **注：** SSL を選択した場合は、XML ファイルに秘密キーと証明書チェーンのフィールドを追加してください。
［Host］	コールアウト サーバのホスト名を入力します。
［Port］	コールアウト サーバを接続できるポート番号を入力します。
［URI］	WebFort サーバからコールアウト サーバにアクセスするための URI（Uniform Resource Identifier）を入力します。
［Connection Timeout (in Milliseconds)］	接続プールに使用可能な接続がなく、新しい接続を作成できない場合に、接続リクエストが待機する間隔（ミリ秒単位）を入力します。
［Read Timeout (in Milliseconds)］	WebFort サーバがコールアウトからのリクエストに対するレスポンスを待機する時間を入力します。
［Idle Timeout (in Milliseconds)］	WebFort サーバが接続を閉じる前に待機する間隔（ミリ秒単位）を入力します。
［Server Root Certificate］	コールアウト サーバのルート証明書が含まれる PKCS#12 ストアのパスを参照し、アップロードします。
［Client Certificate］	WebFort サーバの証明書が含まれる PKCS#12 ストアのパスを参照し、アップロードします。
［Client Private Key］	WebFort サーバの証明書の秘密キーを参照し、アップロードします。

表 5-4. コールアウトの登録（続き）

ページ フィールド	説明
［Minimum Connections］	WebFort サーバとコールアウト サーバ間で保持できる接続の最大数を入力します。
［Maximum Connections］	WebFort サーバとコールアウト サーバ間で保持する必要がある接続の最小数を入力します。

9. ［**Save**］ボタンをクリックすると、新しいコールアウトが作成されるか、または既存のコールアウト定義が更新されます。
10. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。

    この作業の方法については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

プラグインの設定

Master Administrator によって登録されたプラグイン（3-61 ページの「プラグインの登録と更新」を参照）は、（GA のみが）WebFort サーバで動作するように設定する必要があります。

登録済みのプラグインを GA として設定する方法

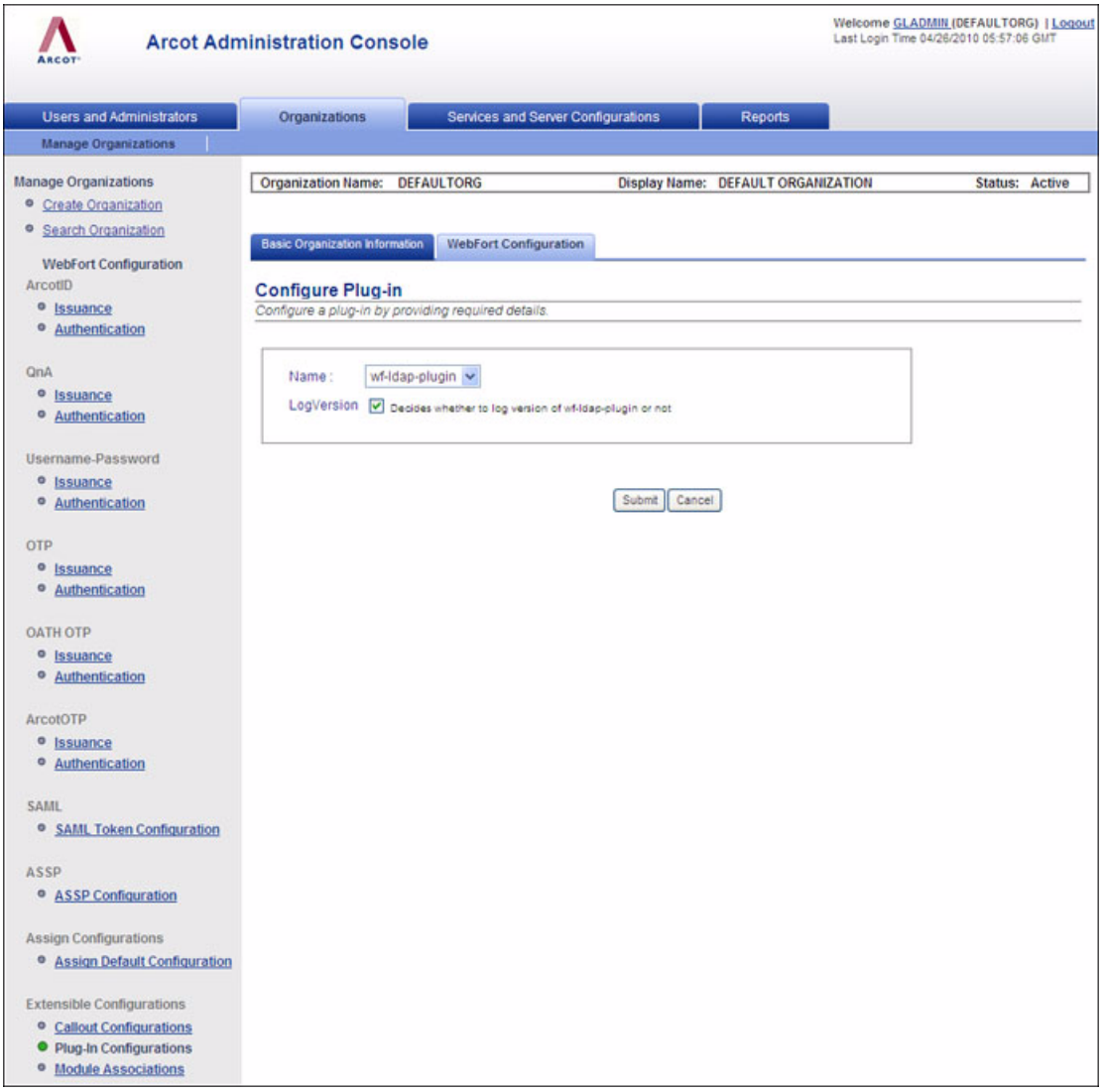
1. 必要な GA の権限とスコープでログインしていることを確認します。
2. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

   検索条件に一致する組織のリストが（図 5-9 のように）表示されます。
5. ［**Organization**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   （図 5-10 のような）［Organization Information］ページが表示されます。
6. ［**WebFort Configuration**］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（図 5-11）。
7. ［**Extensible Configurations**］で、［**Plug-In Configurations**］リンクをクリックして［Plug-In Configurations］ページ（図 5-15）を表示します。

図 5-15 ［Configure Plug-In］ページ



8. ［**Name**］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。

9. プラグイン設定の詳細を入力します。
10. ［**Submit**］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。
11. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。

    この作業の方法については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

イベントの関連付け

*イベント*とは、事前に定義された WebFort システムの操作のことです。設定済みのコールアウトまたはプラグインを呼び出すイベントを定義する必要があります。GA のみがこのタスクを実行できます。

（GA として）イベントを済みのコールアウトまたはプラグインに関連付ける方法

1. 必要な GA の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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

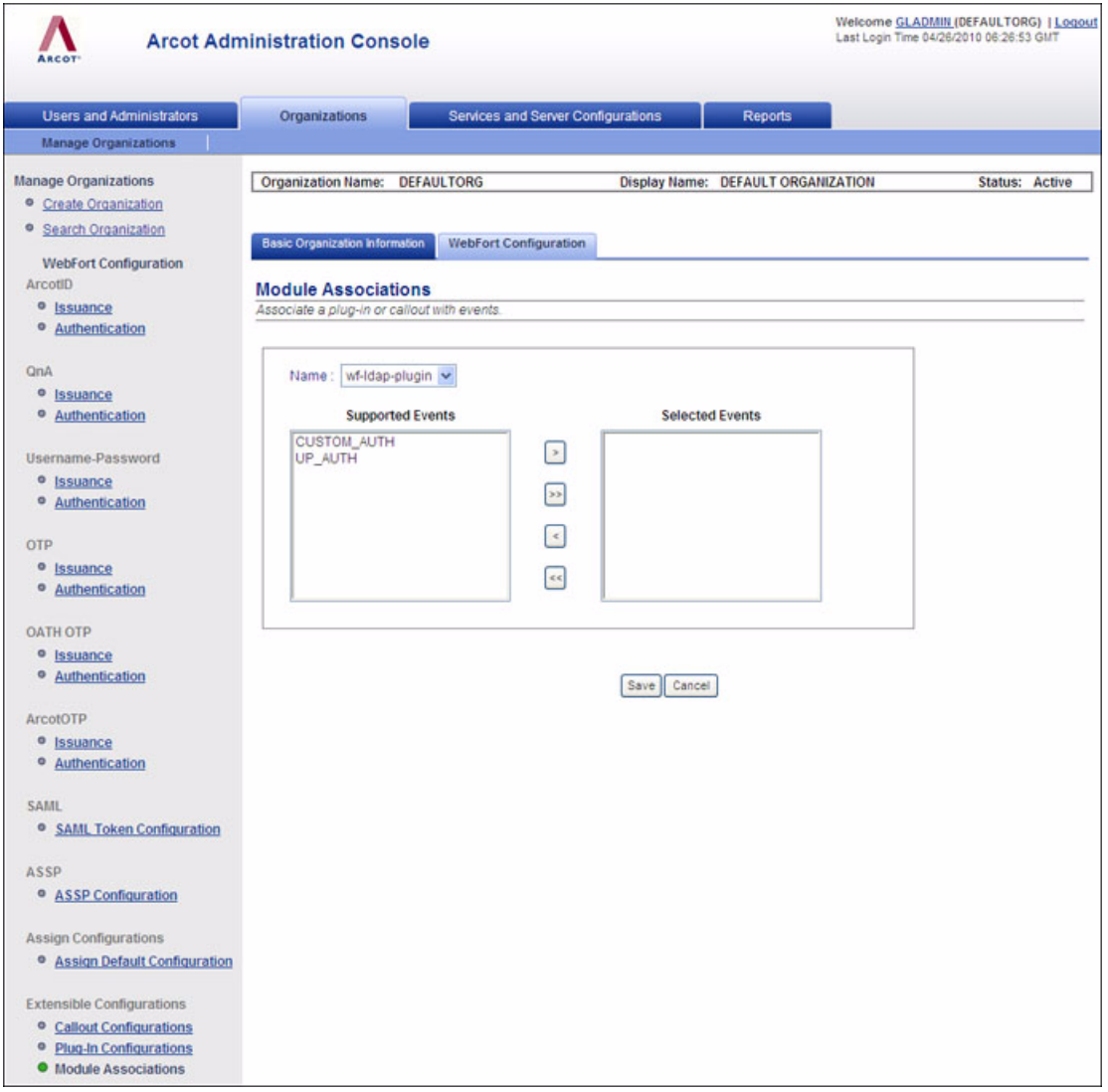
   検索条件に一致する組織のリストが（図 5-9 のように）表示されます。
5. ［**Organization**］列で、必要な組織の［< *組織名* >］リンクをクリックします。

   （図 5-10 のような）［Organization Information］ページが表示されます。
6. ［**WebFort Configuration**］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（図 5-11）。

7. ［**Extensible Configurations**］で、［**Module Associations**］リンクをクリックして［Module Associations］ページ（図 5-16）を表示します。

図 5-16 ［Module Associations］ページ



8. ［**Name**］ドロップダウン リストから、イベントに関連付けるモジュール（コールアウトまたはプラグイン）を選択します。

9. ［**Supported Events**］リストから関連付けるイベントを選択し、［>］ボタンをクリックして、選択したイベントのグループを［**Selected Events**］リストに追加します。

   ［**Supported Events**］リストには、そのモジュールに設定されているすべてのイベントが表示されます。一方、［**Selected Events**］リストには、そのモジュール用に選択したイベントが表示されます。

10. ［**Save**］ボタンをクリックすると、関連付けが完了し、変更が保存されます。
11. 展開したすべての WebFort サーバ インスタンスをリフレッシュします。

    この作業の方法については、3-43 ページの「インスタンスのリフレッシュまたはシャットダウン」を参照してください。

組織情報の更新

Administration Console を使用して、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、および組織を管理する管理者を含む**組織情報**（「組織情報の更新」）。
- クレデンシャル 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 **WebFort 固有の設定**（「WebFort 固有の設定の更新」）。

注： 組織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。

組織情報の更新

基本的な組織情報を更新する方法

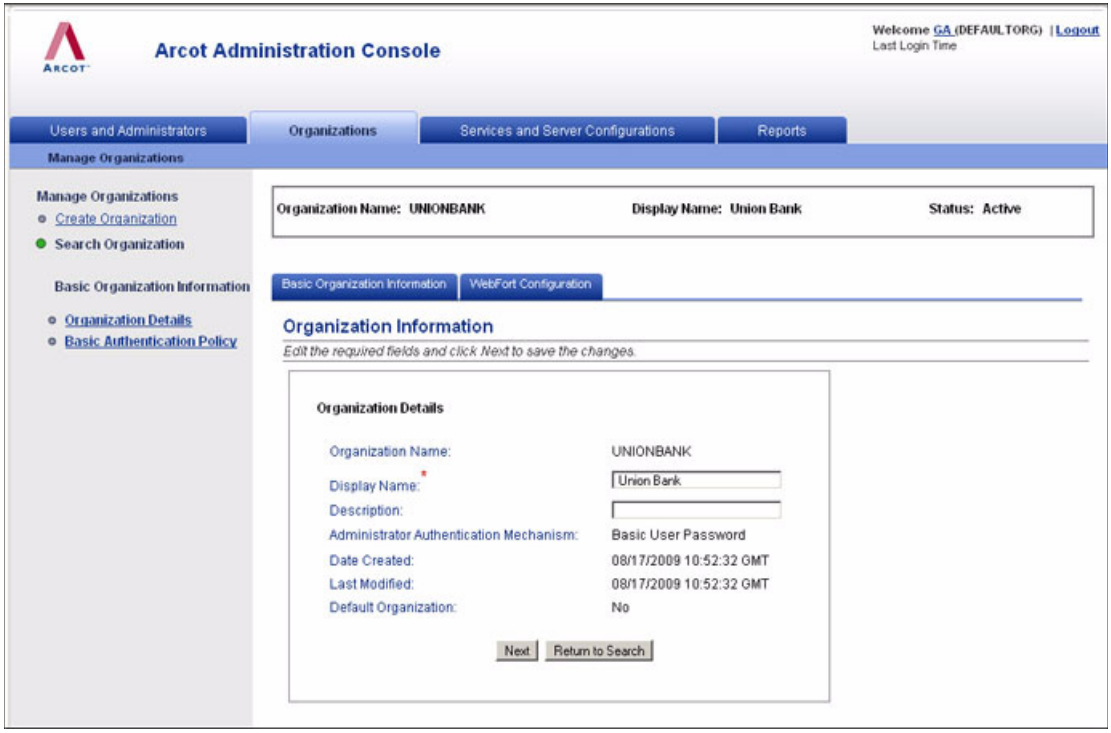
1. 組織の作成に必要な権限とスコープでログインしていることを確認します。
2. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

検索条件に一致する組織のリストが（図 5-9 のように）表示されます。

5. ［**Organization**］列で、必要な組織の *<ORGANIZATION_NAME>* リンクをクリックします。

   （図 5-17 のような）［Organization Information］ページが表示されます。

図 5-17 ［Organization Information］ページ



6. ［**Organization Details**］セクションで、必要なフィールド（［**Display Name**］と［**Description**］）を編集します。
7. ［**Next**］ボタンをクリックして追加の設定に進みます。
   - 組織が **Arcot 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すべての組織を管理するスコープを持っている場合は、（図 5-2 に示すような）［Update Administrators］ページが表示されます。

このページで、組織を管理する管理者を更新し、［**Update**］をクリックして変更を保存し、このプロセスを完了します。

- 組織が **LDAP リポジトリ**に作成された場合は、［Edit Organization］ページ（図 5-5）が表示されます。

  i. 必要に応じて表 5-3 の情報を使ってフィールドを更新し、［**Next**］ボタンをクリックして［Repository Attribute Mapping］を編集するページ（図 5-6）を表示します。

  ii. 組織を作成したときに作成されたマッピングは編集 *できません*。［**Update**］をクリックして［Update Administrators］ページ（図 5-6）を表示します。

  iii.［Update Administrators］ページで、組織を管理する管理者を更新し、［**Update**］をクリックして変更を保存し、このプロセスを完了します。

WebFort 固有の設定の更新

組織の WebFort 設定を更新する方法

1. 組織の作成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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］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（図 5-9 のように）表示されます。
5. ［**Organization**］列で、必要な組織の <*ORGANIZATION_NAME*> リンクをクリックします。

   （図 5-17 のような）［Organization Information］ページが表示されます。
6. ［**WebFort Configuration**］タブをアクティブにします。

   タスク パネルに WebFort 設定のリンクが表示されます。
7. これらの設定の詳細については、「組織固有の設定の管理」を参照してください。

組織の無効化

組織のすべての管理者に対して WebFort のメカニズムを使った Administration Console へのログインを禁止し、組織のエンド ユーザに対して WebFort 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、組織を無効にします。

注： 組織を無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。

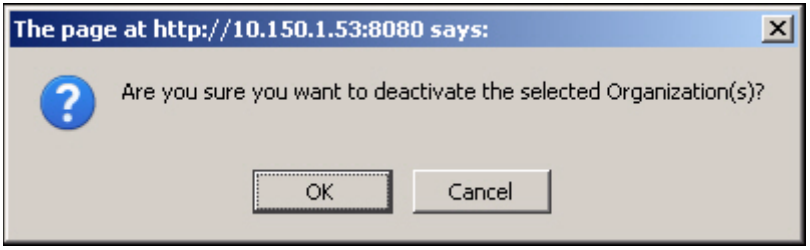
1 つ以上の組織を無効にする方法

1. 組織の無効化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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］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（図 5-9 のように）表示されます。
5. 無効にする組織を 1 つ以上選択します。
6. ［**Deactivate**］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。

   図 5-18 に示すメッセージ ボックスが表示されます。

図 5-18 組織の非アクティブ化：メッセージ



7. ［**OK**］ボタンをクリックして非アクティブ化を確定します。

組織の有効化

非アクティブになっている組織を再度有効にする必要がある場合があります。その場合は、［Search Organization］ページで検索条件を指定する際に、［**Inactive**］オプションを選択する必要があります。

注： 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。

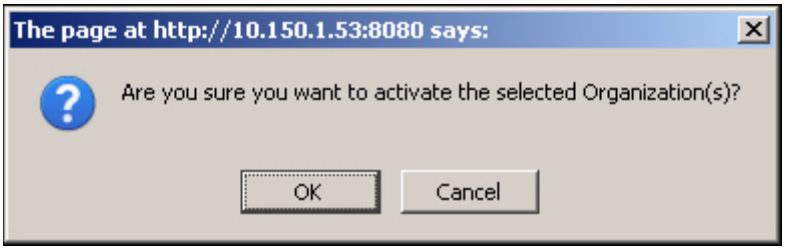
非アクティブになっている組織を有効にする方法

1. 組織の有効化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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］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（図 5-9 のように）表示されます。
5. 再度有効にする組織を 1 つ以上選択します。
6. ［**Activate**］ボタンをクリックすると、選択した組織が有効になります。

   図 5-19 に示すメッセージ ボックスが表示されます。

図 5-19 組織のアクティブ化：メッセージ



7. ［**OK**］ボタンをクリックしてアクティブ化を確定します。

初期状態の組織のアクティブ化

場合によっては、組織を作成し始めても、組織をアクティブにしないことがあります。たとえば、［Create Organization］ページで［**Organization Information**］や［**User Data Location**］を指定しても、LDAP リポジトリの詳細や組織を管理する管理者を指定しない場合があります。このような場合、組織は作成されますが、アクティブではなく、通常は（［**Initial**］オプションを選択して検索しない限り）検索時に表示されません。

このような組織は、アクティブにしない限り、システム内では初期状態のままです。後で初期状態の組織と同じ詳細情報を使って新しい組織を作成しようとしても、その組織が存在するため、作成できません。

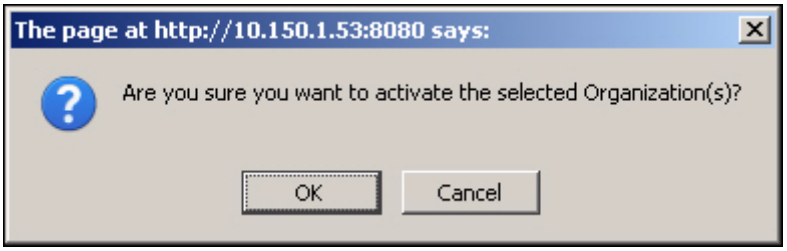
注： 初期状態の組織をアクティブ化できるようにするには、そのための適切な権限とスコープを持っていることを確認する必要があります。MA はすべての組織をアクティブ化できます。GA と OA は、自分のスコープに含まれるすべての組織をアクティブ化できます。

初期状態の組織をアクティブにする方法

1. 組織の作成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. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 必要な組織の情報の一部または全部を入力し、［**Initial**］オプションを選択します。
5. ［**Search**］ボタンをクリックすると、（図 5-9 のように）指定した条件に一致するすべての組織がページ上に表示されます。
6. アクティブにする組織を選択します。

7. ［**Activate**］ボタンをクリックすると、選択した組織が有効になります。図 5-20 に示すメッセージ ボックスが表示されます。

図 5-20 組織のアクティブ化：メッセージ



8. ［**OK**］ボタンをクリックしてアクティブ化を確定します。

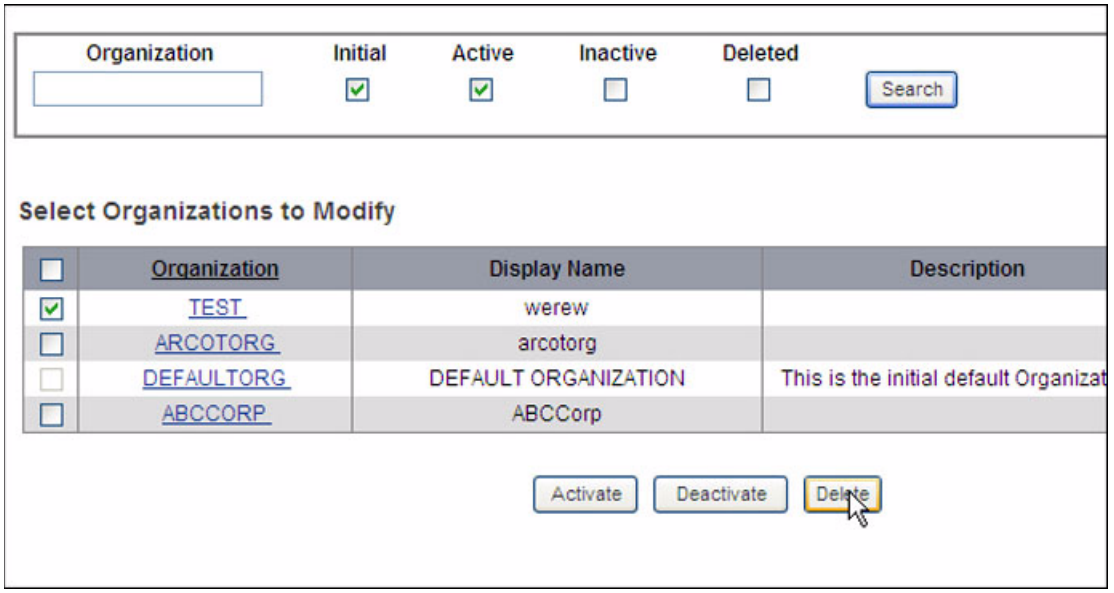
組織の削除

組織を削除すると、その組織に関連付けられた管理者は Administration Console 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 ユーザは認証できなくなります。ただし、組織に関連する情報はシステム内に保持され続けます。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。

	注： 組織を削除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。

組織を削除する方法

図 5-21 組織の削除

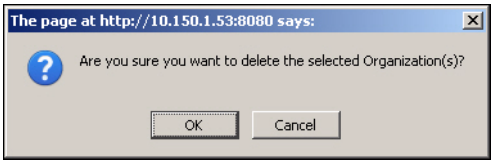


1. 組織の削除に必要な権限とスコープでログインしていることを確認します。
2. ［**Organizations**］タブをアクティブにします。
3. ［**Manage Organizations**］セクションで［**Search Organization**］リンクをクリックして［Search Organization］ページ（図 5-8）を表示します。
4. 検索する組織の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

   検索条件に一致する組織のリストが（図 5-9 のように）表示されます。
5. 削除する組織を 1 つ以上選択します。
6. ［**Delete**］ボタンをクリックすると、選択した組織が削除されます。

   図 5-22 に示すメッセージ ボックスが表示されます。

図 5-22 組織の削除：メッセージ



7. ［**OK**］ボタンをクリックして確定します。

第 6 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。小規模な単独組織への展開では、Master Administrator （MA）1 人のみと、エンド ユーザのために組織を管理する Global Administrator （GA）を配置する場合があります。一方、大規模な複数組織への展開では、展開の複雑さとエンド ユーザの数に基づいて複数の GA を配置する必要がある場合があります。GA は、組織とユーザの管理作業をさらに複数の Organization Administrator （OA）および User Administrator （UA）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、1-5 ページの「サポートされるロール」を参照してください。1-11 ページの表 1-2 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。この章では、以下の管理者管理操作について説明します。

- 管理者の作成
- 管理者アカウントのプロファイル情報の変更
- 管理者の検索
- 管理者アカウント情報の更新
- アクティベーション コードの再生成
- 管理者のクレデンシャルの更新
- 管理者アカウントの無効化
- 管理者アカウントの有効化
- 管理者アカウントの削除

注： Master Administrator は、この章で説明するすべての操作に加えて、1-15 ページの「カスタム ロール」を作成する権限を持っています。これは WebFort 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。

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。以下に例を示します。

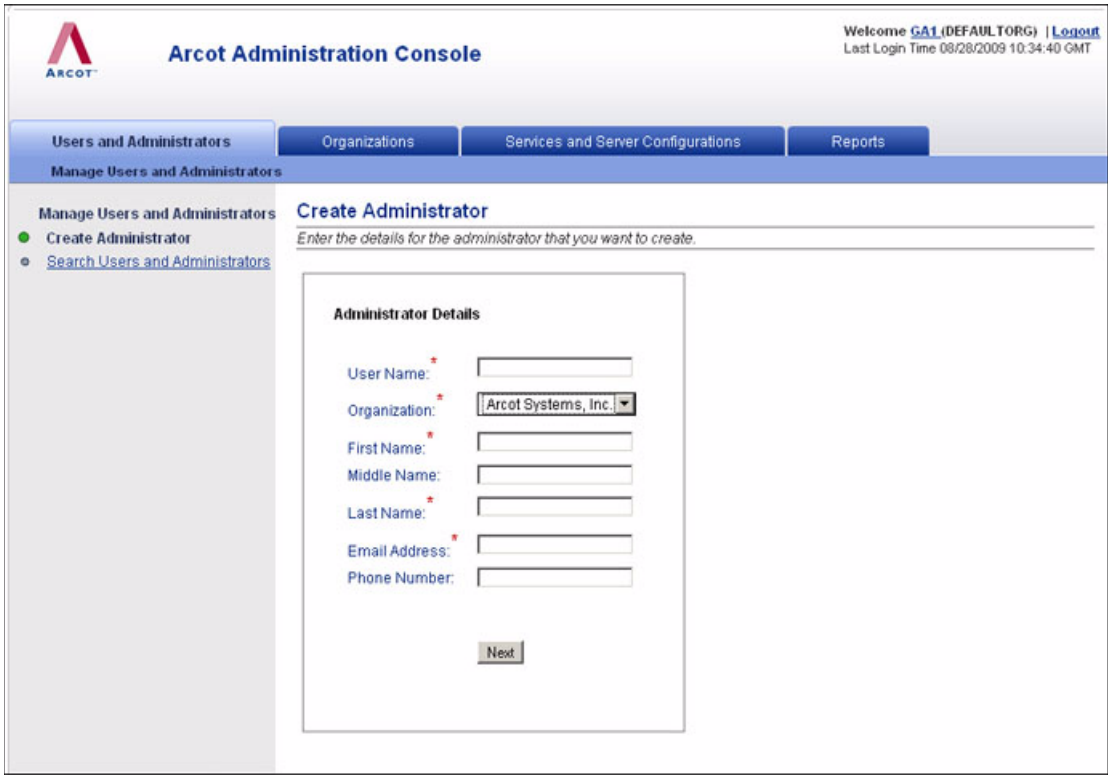
- Master Administrator は、他のすべてのタイプの管理者を作成できます。
- Global Administrator （GA）は、自分のスコープ内に以下を作成できます。
  - 他の GA
  - Organization Administrator （OA）
  - User Administrator （UA）
- OA は自分のスコープ内に以下を作成できます。
  - 他の OA
  - UA
- UA は自分のスコープ内に他の UA を作成できます。

WebFort のユーザ名 - パスワード クレデンシャルを使ったアカウントの作成

WebFort のユーザ名 - パスワード クレデンシャルを使って管理者アカウントを作成する方法

1. 管理ユーザの作成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. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションで［**Create Administrator**］リンクをクリックし、［Create Administrator］ページ（図 6-1）を表示します。

図 6-1 Create Administrator：1 ページ目



4. ［**Administrator Details**］セクションで、管理者の詳細を入力します。表 6-1 で、このページ上のフィールドについて説明します。

表 6-1. 管理者を作成するための入力

入力	説明
［User Name］	管理者の一意のユーザ名。
［Organization］	管理者が属する組織の表示名。 **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。

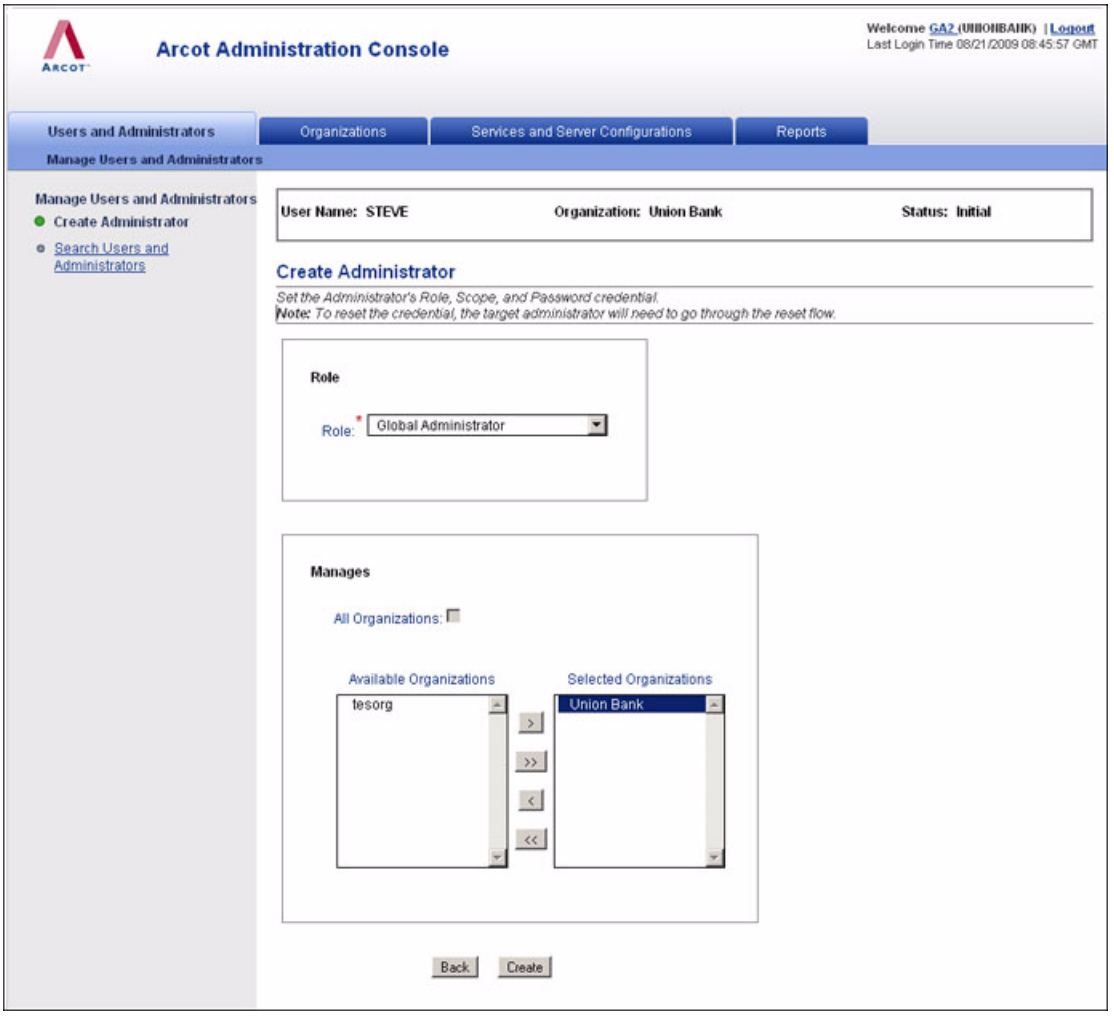
表 6-1. 管理者を作成するための入力

入力	説明
[Middle Name]（オプション）	管理者のミドル ネーム（ある場合）。
[Last Name]	管理者の姓。
[Email Address]	管理者の電子メール アドレス。
[Phone Number]（オプション）	管理者に連絡する際の電話番号。

5. [**Next**] ボタンをクリックして続行します。

   [Create Administrator] の次のページ（図 6-2）が表示されます。

図 6-2 Create Administrator：2 ページ目



6. このページで、以下の作業を実行します。
   - ［**Role**］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。
   - ［**Manages**］セクションで、管理者がスコープを持っている組織を選択します。

- 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、［**All Organizations**］オプションを選択します。

  または

- ［**Available Organizations**］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［**Selected Organizations**］リストに追加します。

  ［**Available Organizations**］リストには、この新規アカウント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。［**Selected Organizations**］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。

7. ［**Create**］ボタンをクリックすると、変更が保存され、アカウントが作成されてアクティブになります。

   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する必要があるアクティベーション コードも表示されます。たとえば、以下のような成功メッセージが表示されます。

```
「Successfully created the administrator.The activation code for
first login for this administrator is 03768672.」
```

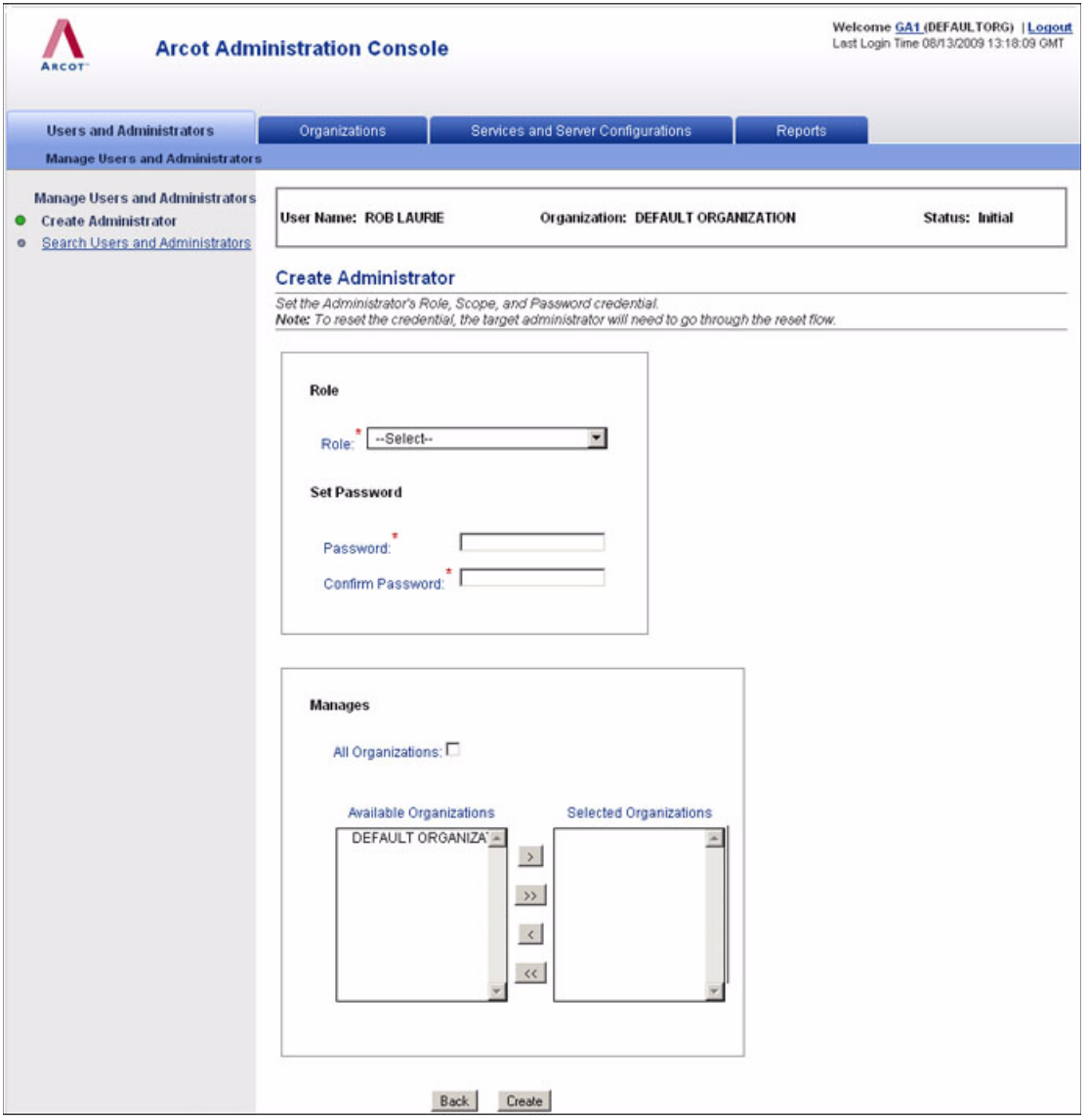
8. 成功メッセージの中に表示されたアクティベーション コードの数値を書き留めて、管理者にそれを伝えます。

基本ユーザ名 - パスワード クレデンシャルを使ったアカウントの作成

基本ユーザ名 - パスワード クレデンシャルを使って管理者アカウントを作成する場合は、以下の手順に従います。

1. 「WebFort のユーザ名 - パスワード クレデンシャルを使ったアカウントの作成」で説明した手順 1 ～手順 5 を実行して、［Create Administrator］ページ（図 6-3）を表示します。

図 6-3 Create Administrator：2 ページ目



2. このページで、以下の作業を実行します。
   - ［**Role**］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。

- ［**Password**］フィールドと［**Confirm Password**］フィールドに管理者アカウントのパスワードを入力します。
- ［**Manages**］セクションで、管理者がスコープを持っている組織を選択します。

3. ［**Create**］ボタンをクリックすると、変更が保存され、アカウントが作成されてアクティブになります。
4. 管理者に新しいパスワードを伝えます。

管理者アカウントのプロファイル情報の変更

アカウント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）
- アカウントのパスワード
- 優先される組織（今後実行するすべての管理者関連タスクの［**Organization**］フィールドで、デフォルトで選択される組織）

注： 管理者はいつでも各自のアカウントのプロファイル情報を変更できます。他の管理者アカウントの情報を変更する場合は、「管理者アカウント情報の更新」を参照してください。

WebFort のユーザ名 - パスワード クレデンシャルを使ったアカウントの場合

WebFort のユーザ名 - パスワード クレデンシャルを使って作成された自分のアカウントの管理者プロファイル情報を変更する方法

1. 自分のアカウントにログインしていることを確認します。
2. **ヘッダ** フレームの *<ADMINISTRATORNAME>* リンクをクリックして［My Profile］ページ（図 6-4）を表示します。
3. このページには以下の 3 つのセクションがあります。
   - **個人情報**

     このセクションでは、姓、名、ミドル ネーム、電子メール ID および電話番号を変更できます。
   - **パスワードの変更**

     このセクションでは、新しいパスワードを設定できます。

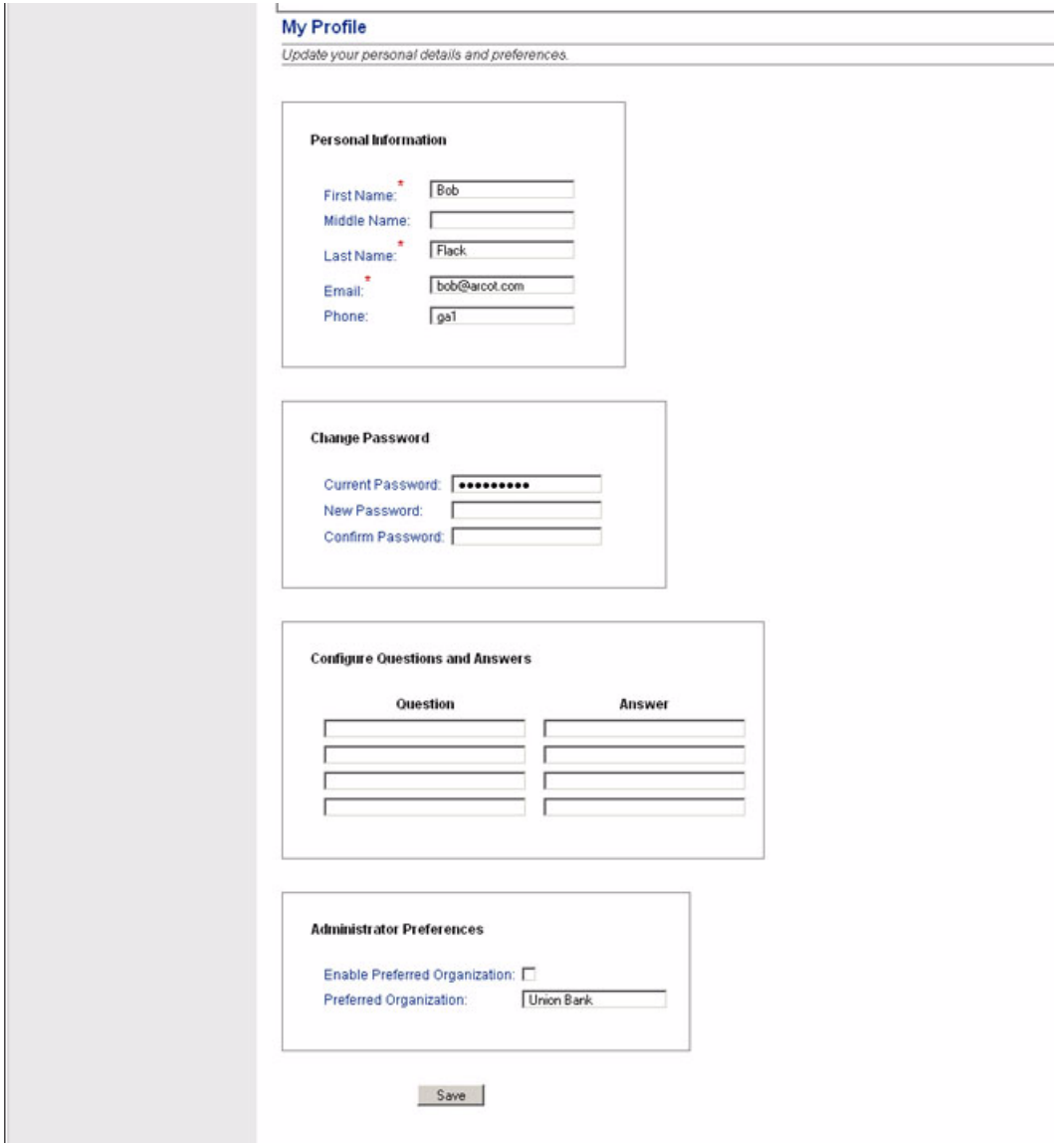
- 質問と回答

  このセクションでは、パスワードを忘れた場合のように、パスワードをリセットするときに回答する必要のある質問を設定できます。

- **Administrator Preferences**

  このセクションでは、管理者が対応するデフォルトの組織を設定できます。

図 6-4 ［My Profile］ページ



4. 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、［**Personal Information**］セクション内のフィールドを編集します。
   b. ［**Configure Questions and Answers**］セクションで、明確に識別できる［**Question**］とそれに対応にする［**Answer**］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。

   c. 現在のパスワードを変更する場合は、［**Change Password**］セクションで［**Current Password**］を入力し、［**New Password**］フィールドと［**Confirm Password**］フィールドで新しいパスワードを指定します。
   d. ［**Administrator Preferences**］セクションで、［**Enable Preferred Organization**］オプションを選択し、［**Preferred Organization**］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。
5. ［**Save**］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。

基本ユーザ名 - パスワード クレデンシャルを使ったアカウントの場合

基本ユーザ名 - パスワード クレデンシャルを使って作成された自分のアカウントの管理者プロファイル情報を変更する方法

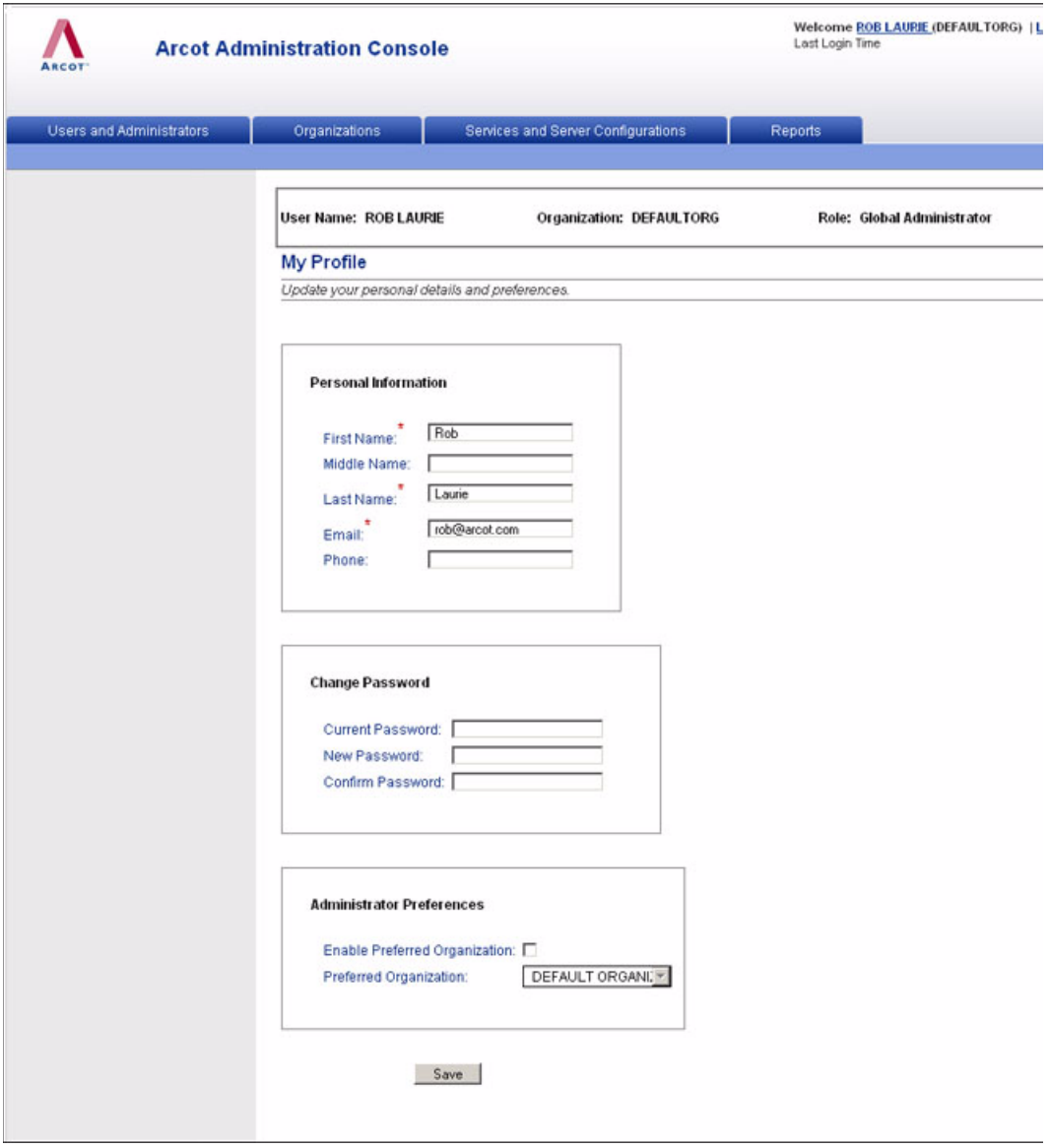
1. 自分のアカウントにログインしていることを確認します。
2. **ヘッダ** フレームの <*ADMINISTRATORNAME*> リンクをクリックして［My Profile］ページ（図 6-5）を表示します。
3. このページには以下の 3 つのセクションがあります。
   - 個人情報

     このセクションでは、姓、名、ミドル ネーム、電子メール ID および電話番号を変更できます。
   - パスワードの変更

     このセクションでは、新しいパスワードを設定できます。
   - Administrator Preferences

     このセクションでは、管理者が対応するデフォルトの組織を設定できます。

図 6-5 ［My Profile］ページ



4. 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、［**Personal Information**］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、［**Change Password**］セクションで［**Current Password**］を入力し、［**New Password**］フィールドと［**Confirm Password**］フィールドで新しいパスワードを指定します。
   c. ［**Administrator Preferences**］セクションで、［**Enable Preferred Organization**］オプションを選択し、［**Preferred Organization**］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。
5. ［**Save**］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。

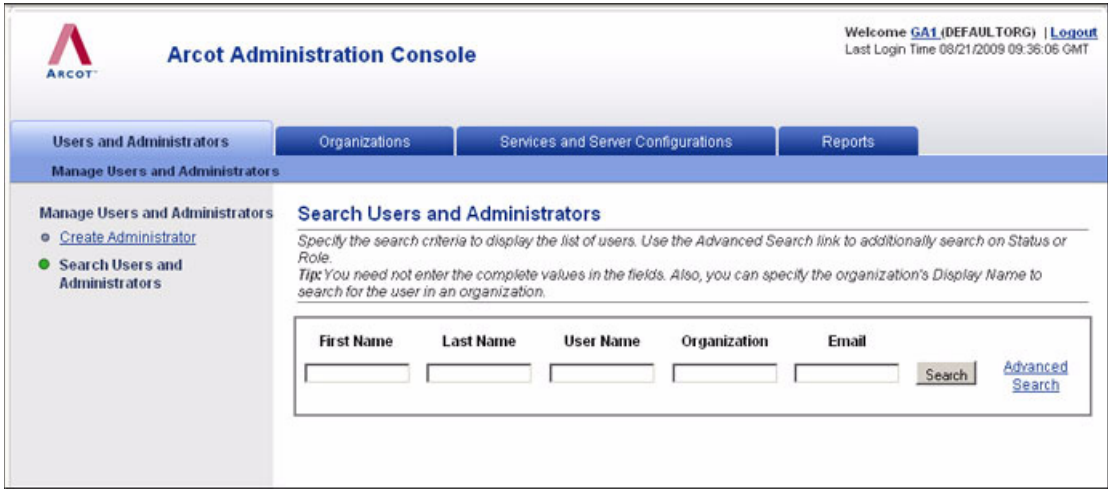
管理者の検索

	**注 :** 管理者アカウントを更新、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、検索する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。

条件を指定して管理者を検索する方法

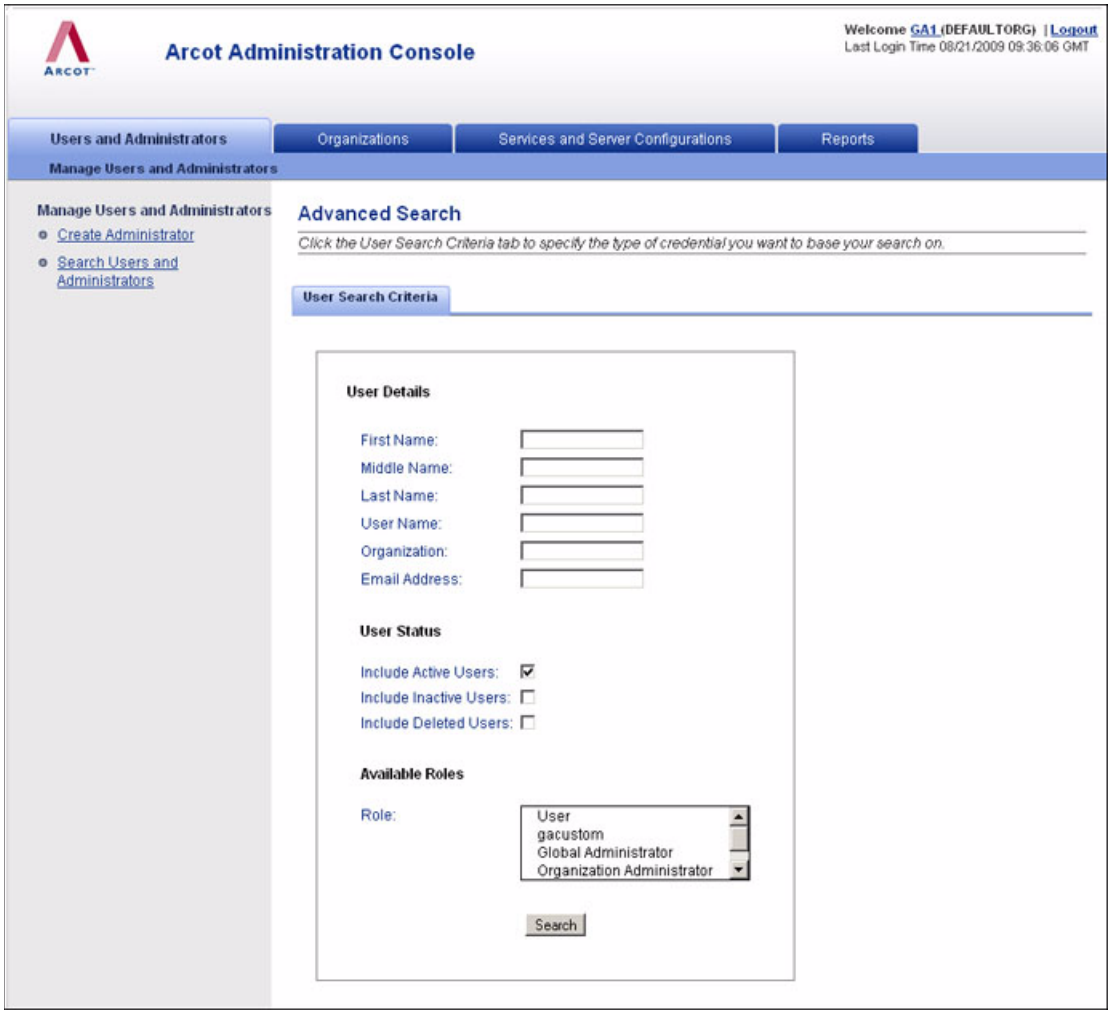
1. 必要な権限とスコープでログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションで［**Search Users and Administrators**］リンクをクリックし、［Search Users and Administrators］ページ（図 6-6）を表示します。

図 6-6 ［Search Users and Administrators］ページ



4. 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。以下の方法が可能です。
   - 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［Display Name］を指定して管理者を検索する。
   - 何も条件を指定せずに［**Search**］ボタンをクリックするのみで管理者を検索する。
   - ［**Advanced Search**］リンクをクリックして［Advanced Search］ページ（図 6-7）を表示し、管理者の［Status］または［Role］を指定して必要な管理者を検索する。

図 6-7 ［Advanced Search］ページ



5. 管理者の必要な詳細を指定し、［**Search**］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。

管理者アカウント情報の更新

注： 管理ユーザ アカウント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 は任意のアカウントを更新できます。GA は、MA アカウントを*除き*、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを更新できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを更新できます。一方、UA は自分のスコープに含まれる自分の同格者のアカウントのみを更新できます。

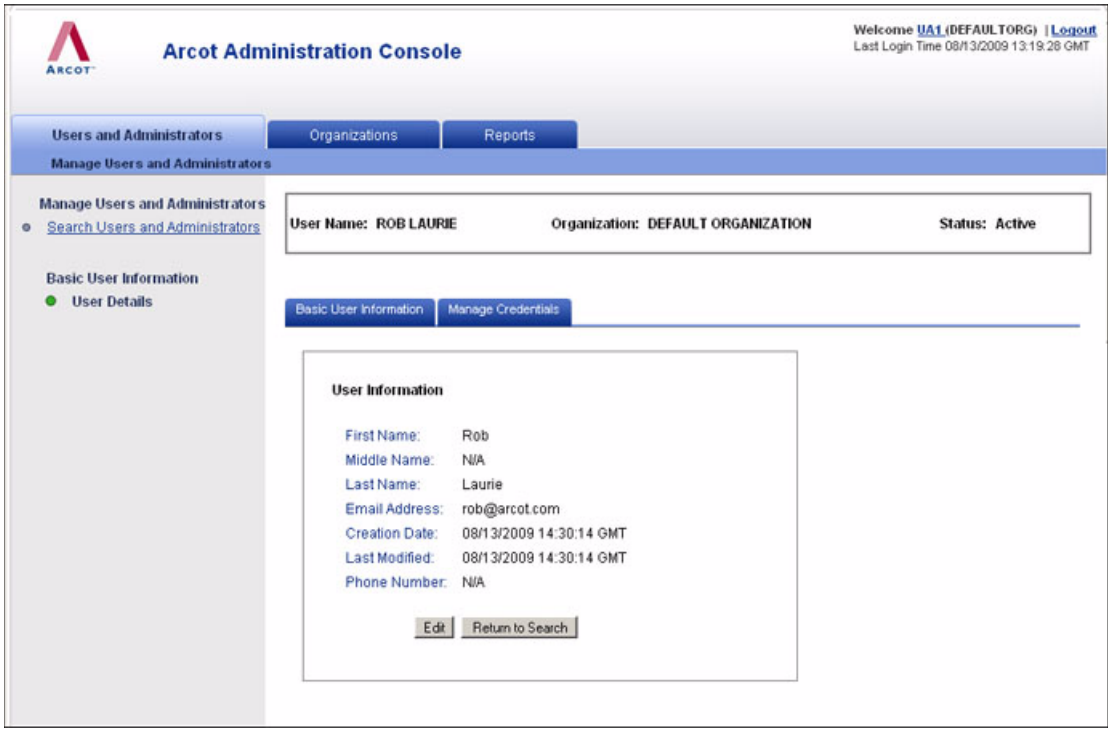
管理者の基本的な詳細（名、ミドル ネーム、姓、連絡先情報など）や管理者の管理ロール、パスワード、管理スコープを更新する方法

1. 管理ユーザの更新に必要な権限でログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションで［**Search Users and Administrators**］リンクをクリックし、対応するページ（図 6-6）を表示します。
4. 前のセクションの説明に従って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、［**Search**］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。
5. アカウントを編集する管理者の *<user name>* リンクをクリックします。

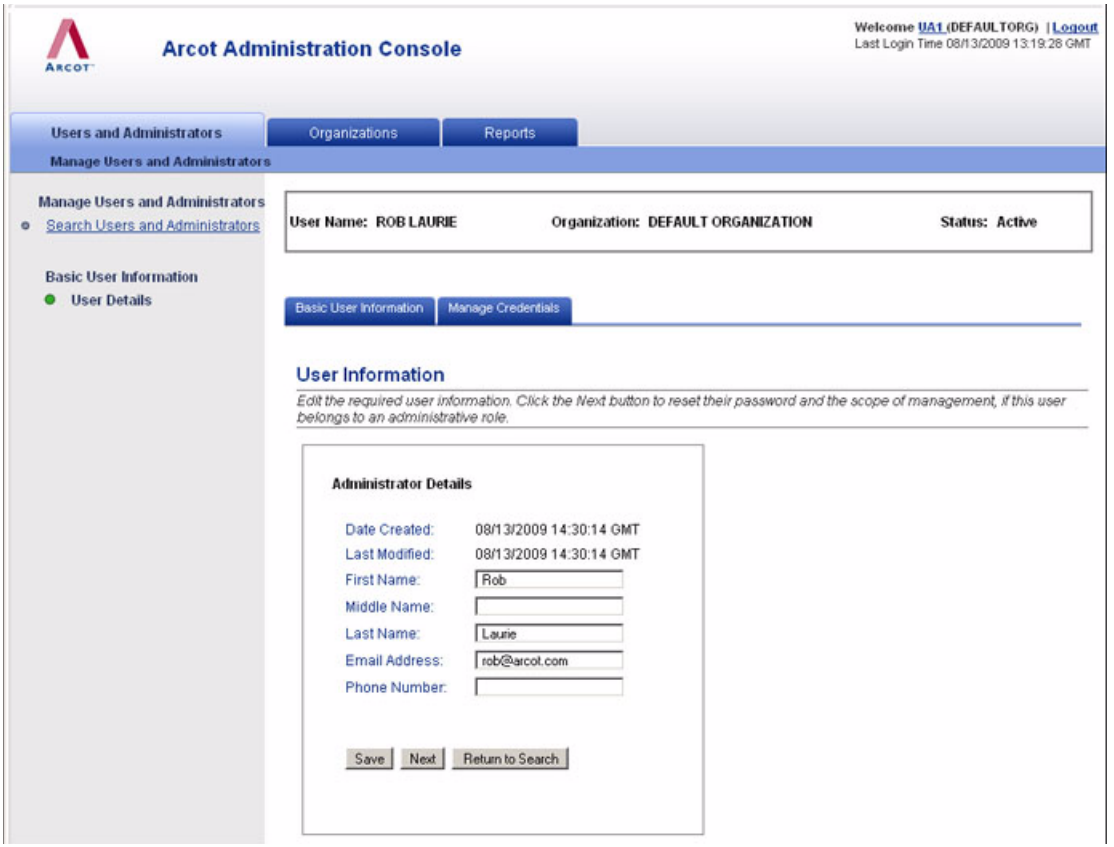
   図 6-8 に示すような［Basic User Information］ページが表示されます。

図 6-8 ［Basic Administrator Information］ページ



6. ［**Edit**］ボタンをクリックし、以下の図（図 6-9）に示すページで管理者の情報を変更します。

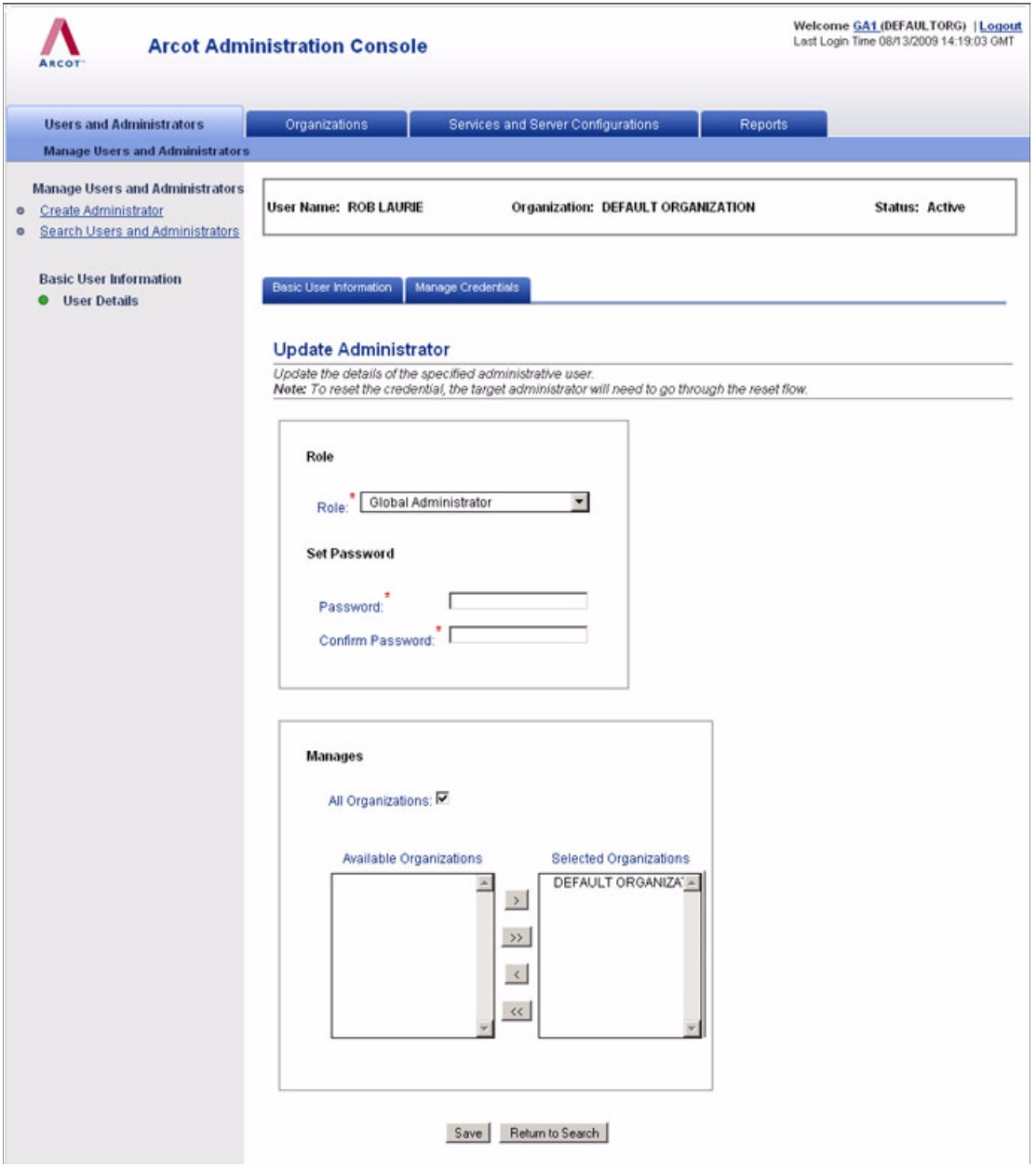
図 6-9 ［User Information］ページ



7. ［**Administrator Details**］セクションで、必要なフィールド（［**First Name**］、［**Middle Name**］、［**Last Name**］、［**Email Address**］、および［**Phone Number**］）を編集します。
8. ［**Save**］ボタンをクリックして変更を保存し、［User Information］ページに戻るか、または［**Next**］ボタンをクリックして追加の設定に進みます。

   ［**Next**］ボタンをクリックすると、［Update Administrator］ページ（図 6-10）が表示されます。

図 6-10 ［Update Administrator］ページ



9. このページで以下のように必要なフィールドを編集します。
   - ［**Role**］ドロップダウン リストを使って管理者のロールを変更します。
   - 管理者の［**Set Password**］を行います。
   - 管理者が管理する組織を選択します。また、［**Selected Organizations**］から［**Available Organizations**］に組織を移動させることにより、スコープから組織を削除できます。
10. ［**Save**］ボタンをクリックして更新を保存します。

アクティベーション コードの再生成

注： この情報は、WebFort のユーザ名 - パスワード メカニズムにのみ適用可能です。

組織の認証メカニズムとして WebFort のユーザ名 - パスワードが使用されており、管理者が自分のアカウントに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は、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。この場合、新しいアクティベーション コードを再生成し、それを管理者に伝える必要があります。

注： 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 は任意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 アカウントを*除き*、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを更新できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを更新できます。一方、UA は自分のスコープに含まれる自分の同格者のアカウントのみを更新できます。

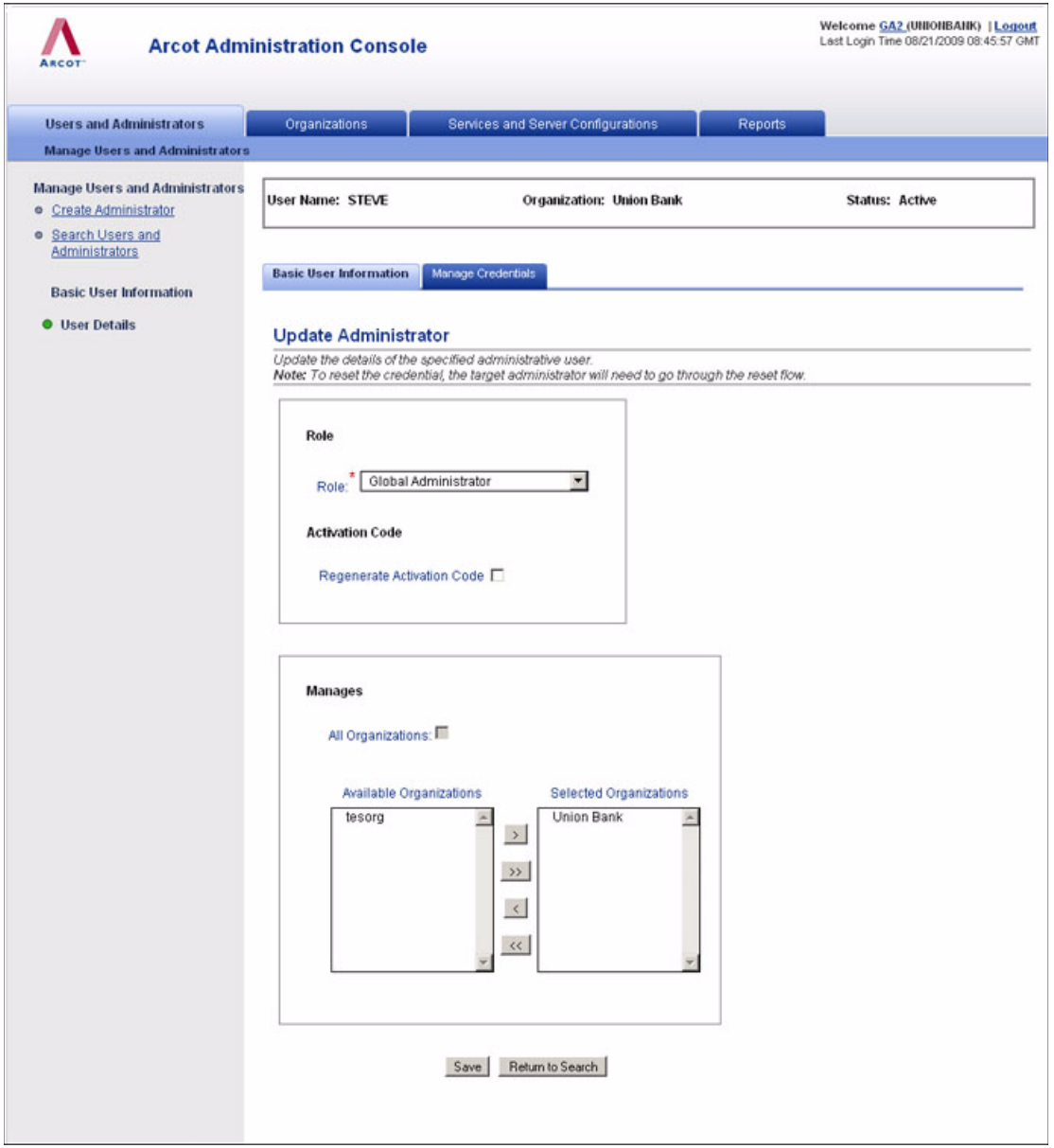
管理者のアクティベーション コードを再生成する方法

1. 管理ユーザの更新に必要な権限でログインしていることを確認します。
2. 「管理者アカウント情報の更新」で説明した手順 2 ～手順 8 を実行して、［Update Administrator］ページ（図 6-11）を表示します。

3. ［**Activation Code**］セクションで、［**Regenerate Activation Code**］オプションを選択します。
4. ［**Save**］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 コードを示す成功メッセージが表示されます。
5. 管理者に新しいアクティベーション コードを伝えます。

図 6-11 ［Update Administrator］ページ



管理者のクレデンシャルの更新

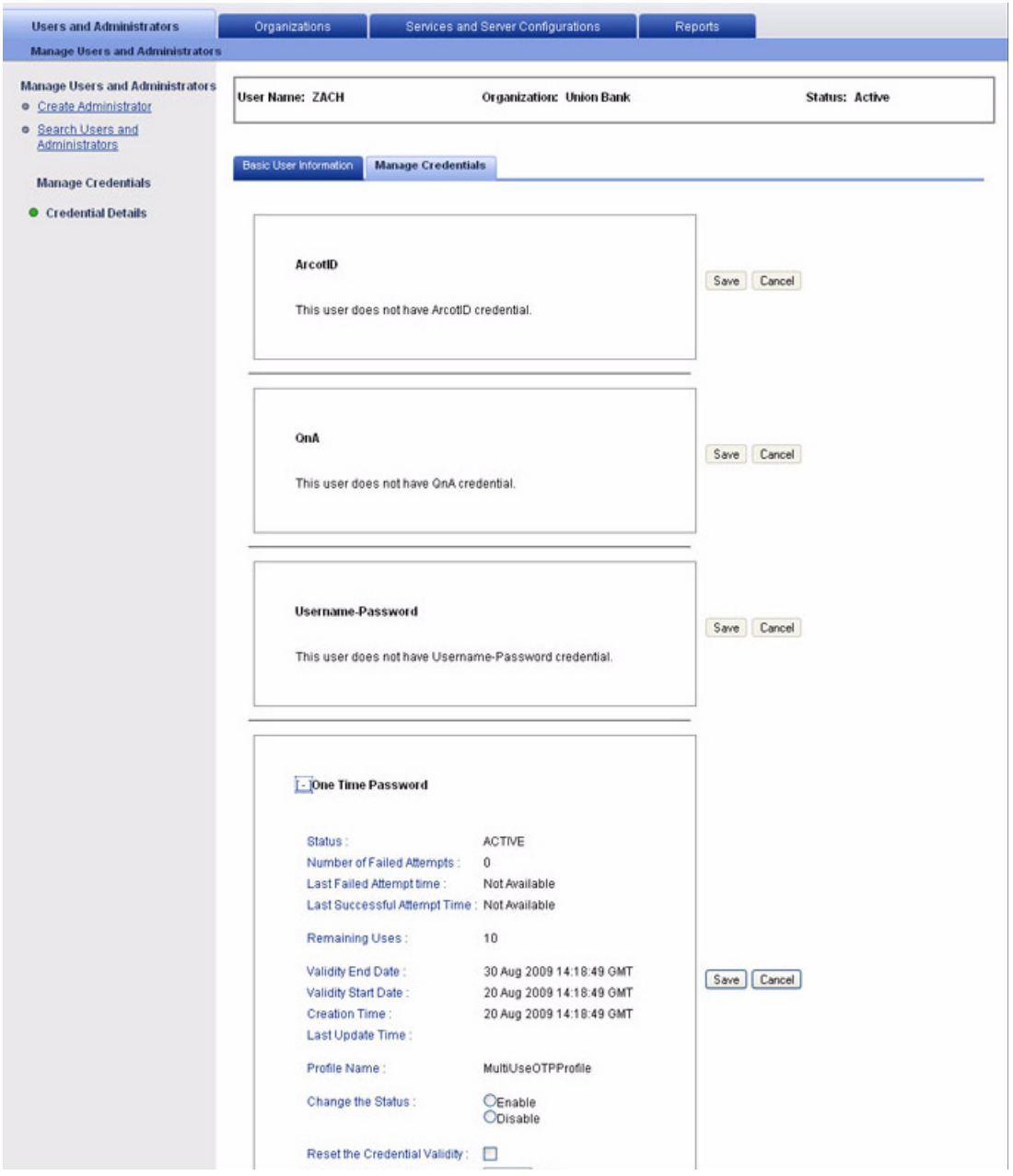
管理者は、エンド ユーザのようにクレデンシャルを使ってシステムに対する認証を行う必要があります。WebFort は、管理者がすぐに使用できる Q&A、ユーザ名 - パスワード、および OTP の各クレデンシャルをサポートします。管理者のクレデンシャルを更新するには、［Credential Details］ページ（図 6-12）を使用する必要があります。このページを使用して、クレデンシャルを有効または無効にしたり、クレデンシャルの有効期限を延長したりできます。

注： 管理ユーザ アカウント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 はクレデンシャルを管理 *できません*。GA は、MA アカウントを *除き*、自分のスコープに含まれる（他の GA を含む）すべてのアカウントのクレデンシャルを管理できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントのクレデンシャルと UA アカウントを管理できます。一方、UA は自分のスコープに含まれる自分の同格者のクレデンシャルのみを管理できます。

管理者のクレデンシャルを更新する方法

1. 管理ユーザのクレデンシャルの更新に必要な権限でログインしていることを確認します。
2. 「管理者アカウント情報の更新」の手順 2 ～手順 5 を実行します。
3. ［**Manage Credentials**］タブをアクティブにして、［Credential Details］ページ（図 6-12）を表示します。
4. 目的のクレデンシャル セクションの前にある **Åm+Ån** 記号をクリックして、そのセクションを展開します。
5. 目的のクレデンシャルの設定を変更します。このページを使用して、以下のクレデンシャルの設定を変更できます。
   - クレデンシャルのステータス
   - クレデンシャルの有効期限の延長
6. 変更したクレデンシャルに対応する［**Save**］ボタンをクリックします。

図 6-12 ［Credential Details］ページ



管理者アカウントの無効化

セキュリティ上の理由で管理者が自分のアカウントにログインすることを禁止する場合は、アカウントを削除せずに無効にすることができます。管理者アカウントを無効にすると、管理者は自分のアカウントからロックアウトされ、アカウントが再度有効にならない限りログインできません。

注： 管理ユーザ アカウントを無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 は任意のアカウントを無効化できます。一方、GA は、MA アカウントを*除き*、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを無効化できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを無効化できます。一方、UA は自分のスコープに含まれる自分の同格者のアカウントのみを無効化できます。

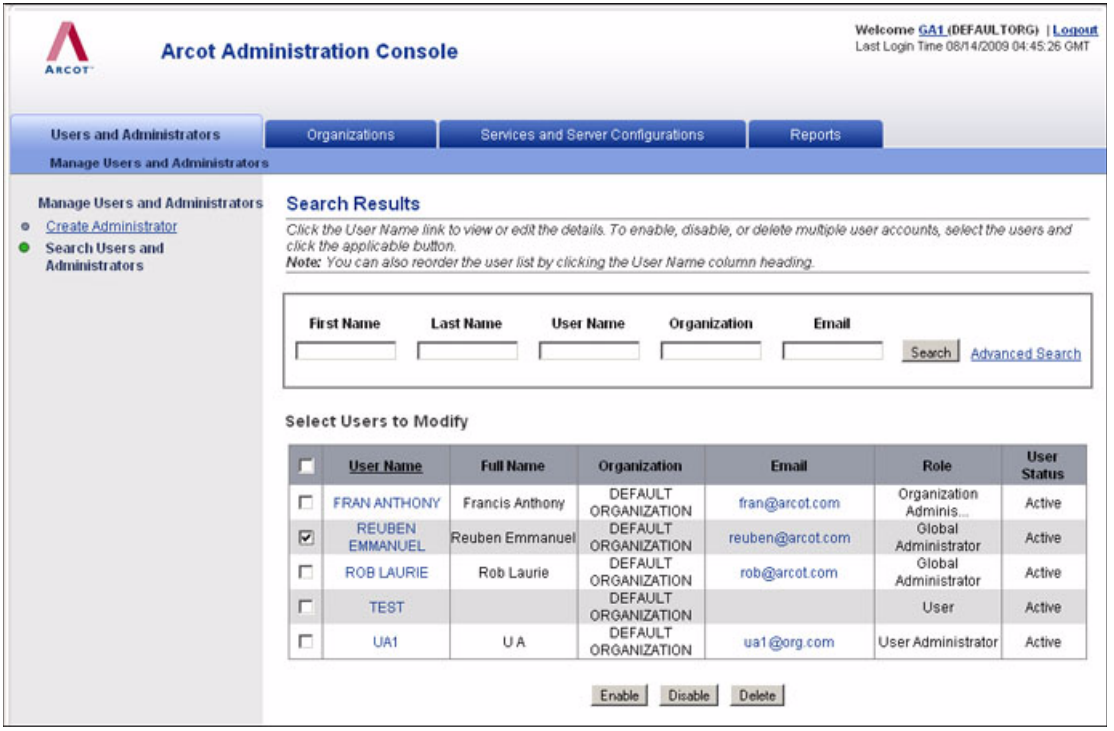
管理者アカウントを無効にする方法

1. 管理ユーザ アカウントの無効化に必要な権限でログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションで［**Search Users and Administrators**］リンクをクリックし、［Search Users and Administrators］ページ（図 6-6）を表示します。
4. アカウントを無効にする管理者の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

   ［**Advanced Search**］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）に基づいてユーザを検索することもできます。

   ［Search Results］ページ（図 6-13）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。

図 6-13 検索結果



5. アカウントを無効にする管理者を 1 人以上選択します。
6. ［**Disable**］ボタンをクリックして、選択した管理者アカウントを無効にします。

管理者アカウントの有効化

無効になっているアカウントを有効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場合は、管理者アカウントを無効にします。これによって、その管理者のアカウントに対する不正アクセスを防止できます。

無効になっているアカウントは、［Search Users and Administrators］ページで検索条件を指定し、［**Search**］ボタンをクリックするのみでは検索できません。このようなユーザを検索するには、［**Advanced Search**］で［**Include Inactive Users**］オプションを使用する必要があります。

	**注 :** 管理ユーザ アカウント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 は任意のアカウントを有効化できます。一方、GA は、MA アカウントを*除き*、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを有効化できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを有効化できます。一方、UA は自分のスコープに含まれる自分の同格者のアカウントのみを有効化できます。

無効になっている管理者アカウントを有効にする方法

1. 管理ユーザ アカウントの有効化に必要な権限でログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションで［**Search Users and Administrators**］リンクをクリックし、［Search Users and Administrators］ページ（図 6-6）を表示します。
4. 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、［**Advanced Search**］リンクをクリックします。

   ［Advanced Search］ページ（図 6-7）が表示されます。
5. ［**User Account**］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。
6. ［**User Status**］セクションで、すべての非アクティブな管理者アカウントを検索するために［**Include Inactive Users**］オプションを選択します。
7. ［**Search**］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。
8. アカウントを有効にする管理者を選択します。
9. ［**Enable**］ボタンをクリックして管理者アカウントを有効にします。

管理者アカウントの削除

管理者アカウントを削除すると、その管理者アカウントに関連付けられた権限はすべて完全に削除されます。その結果、その管理者は Administration Console にログインできなくなります。ただし、アカウント情報とクレデンシャルはシステムから削除されません。

同じ組織内では、以前に削除された管理者アカウントと同じ名前で新しい管理者アカウントを作成することはできませんが、別の組織では作成できます。

注： 管理ユーザ アカウントを削除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 は任意のアカウントを削除できます。一方、GA は、MA アカウントを*除き*、自分のスコープに含まれる（他の GA を含む）すべてのアカウントを削除できます。OA は自分の権限の範囲内に含まれる他のすべての OA アカウントと UA アカウントを削除できます。一方、UA は自分のスコープに含まれる自分の同格者のみを削除できます。

管理者アカウントを削除する方法

1. 管理ユーザ アカウントの削除に必要な権限でログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションで［**Search Users and Administrators**］リンクをクリックし、［Search Users and Administrators］ページ（図 6-6）を表示します。
4. アカウントを削除する管理者の情報の一部または全部を入力し、［**Search**］ボタンをクリックします。

   ［**Advanced Search**］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）に基づいてユーザを検索することもできます。

   ［Search Results］ページに、（図 6-13 のように）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. アカウントを削除する管理者を 1 人以上選択します。

6. ［**Delete**］をクリックします。

注： 管理者を削除しても、そのアカウント情報はデータベースに引き続き保持されます。

第 7 章
ユーザの管理

WebFort 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。ただし、WebFort では、Administration Console を使用してエンド ユーザを直接に作成することはできません。バルク操作で WebFort データベースに既存ユーザを移行したり、新規ユーザを作成できるようにするために、WebFort では広範な SDK および Web サービスが用意されています。WebFort ユーザを作成するこのプロセスは移行と呼ばれます。

関連文書 : ユーザ登録のワークフローの詳細については、「Arcot WebFort 6.2 Java 開発者ガイド」の第 2 章の「WebFort ワークフローについて」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。この目的のための WebFort によってサポートされるエンド ユーザ管理操作には、以下があります。

- ユーザの検索
- ユーザ情報の更新
- ユーザを管理者レベルに上げる
- ユーザ クレデンシャル情報の更新
- ユーザ アカウントの無効化
- ユーザ アカウントの有効化
- ユーザ アカウントの削除

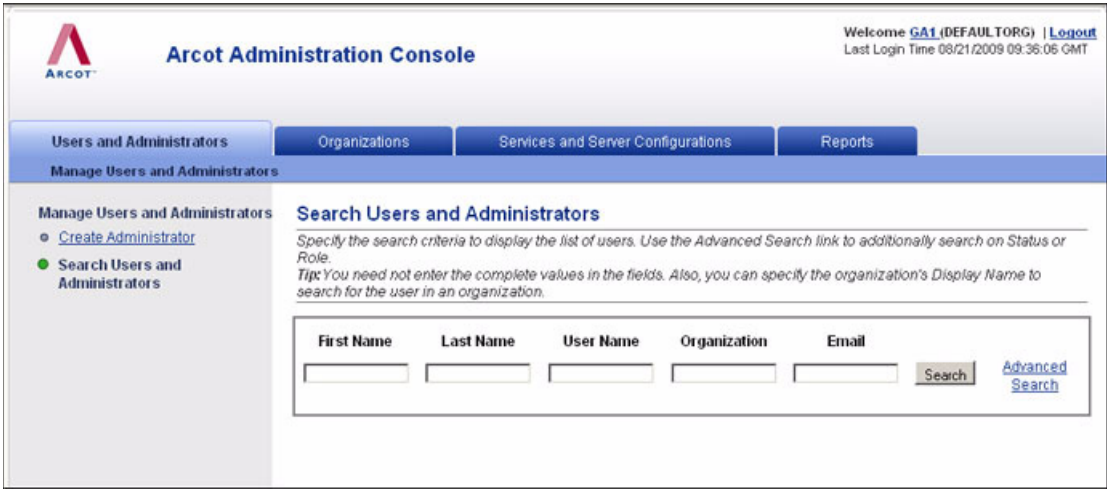
ユーザの検索

	注： ユーザ アカウントの更新、アクティブ化、および非アクティブ化を行う必要がない場合は、検索の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。

条件を指定してユーザを検索する方法

1. 適切なスコープでログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションの［**Search Users and Administrators**］リンクをクリックすると、［Search Users and Administrators］ページ（図 7-1）が表示されます。

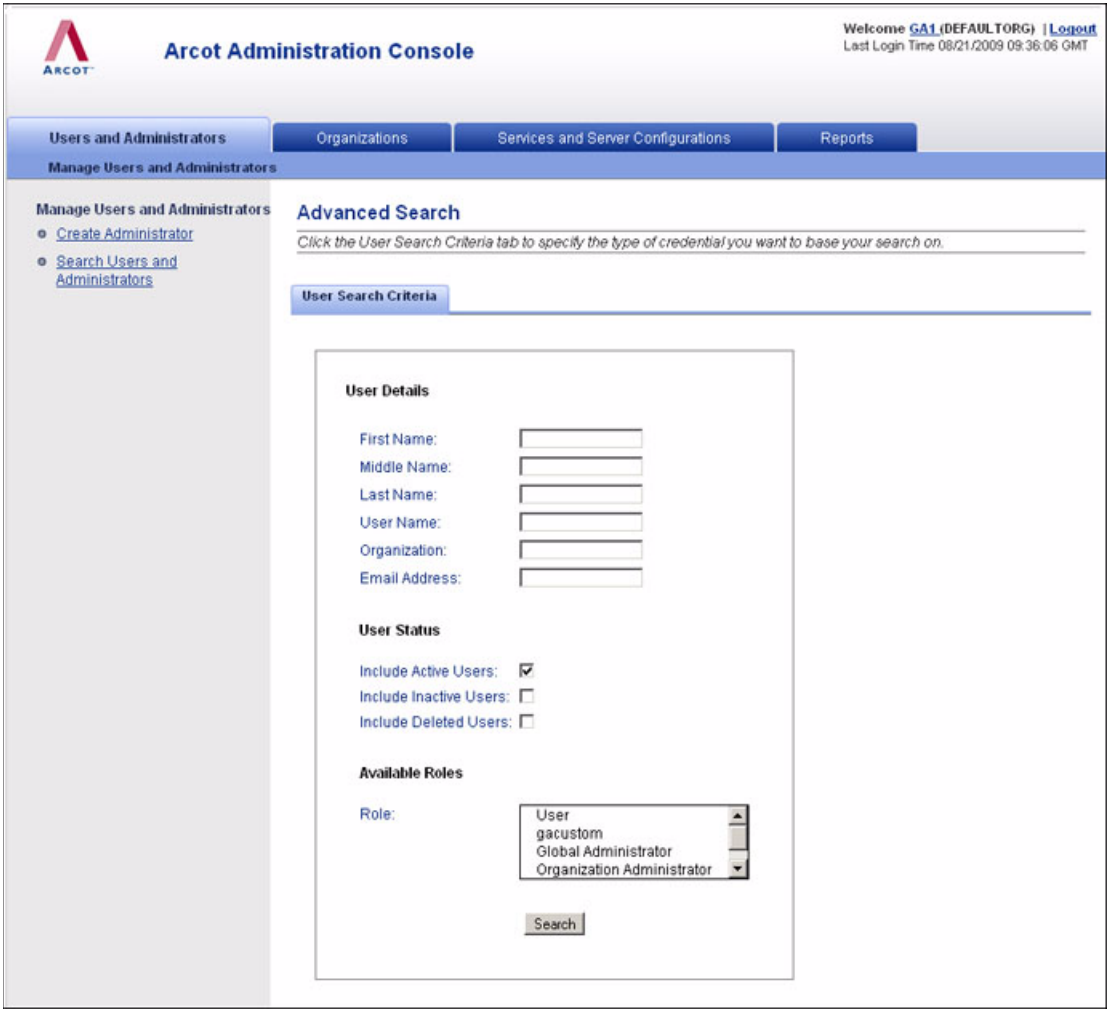
図 7-1［Search Users and Administrators］ページ



4. 検索するユーザの条件を指定します。以下の方法が可能です。
   - 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。

- 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、単に［**Search**］をクリックしてユーザを検索します。
- ［**Advanced Search**］リンクをクリックすると、［Advanced Search］ページ（図 7-2）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。

図 7-2［Advanced Search］ページ



5. ユーザに関する必要な詳細情報を指定し、［**Search**］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

注 : ユーザ アカウント設定を更新するには、更新するための適切な権限とスコープを持っている必要があります。MA は、いずれのユーザ アカウントも更新できます。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。

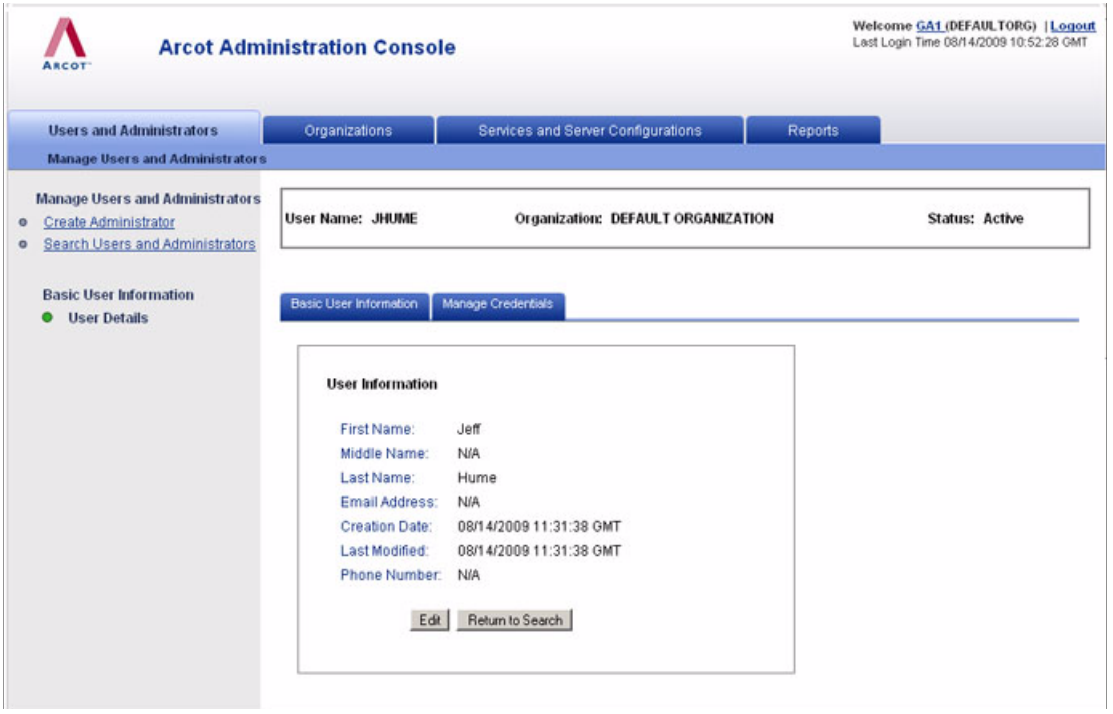
ユーザの基本的な詳細情報（名、ミドル ネーム、および姓、連絡先情報など）を更新するには、以下の手順に従います。

1. ユーザ情報を更新するために必要な権限およびスコープで、ログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションの［**Search Users and Administrators**］リンクをクリックすると、［Search Users and Administrators］ページ（図 7-1）が表示されます。
4. （前のセクションで説明されているように）アカウントを更新するユーザの部分的または完全な情報を入力し、［**Search**］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。
5. 編集するアカウントのユーザの *<user name>* リンクをクリックします。

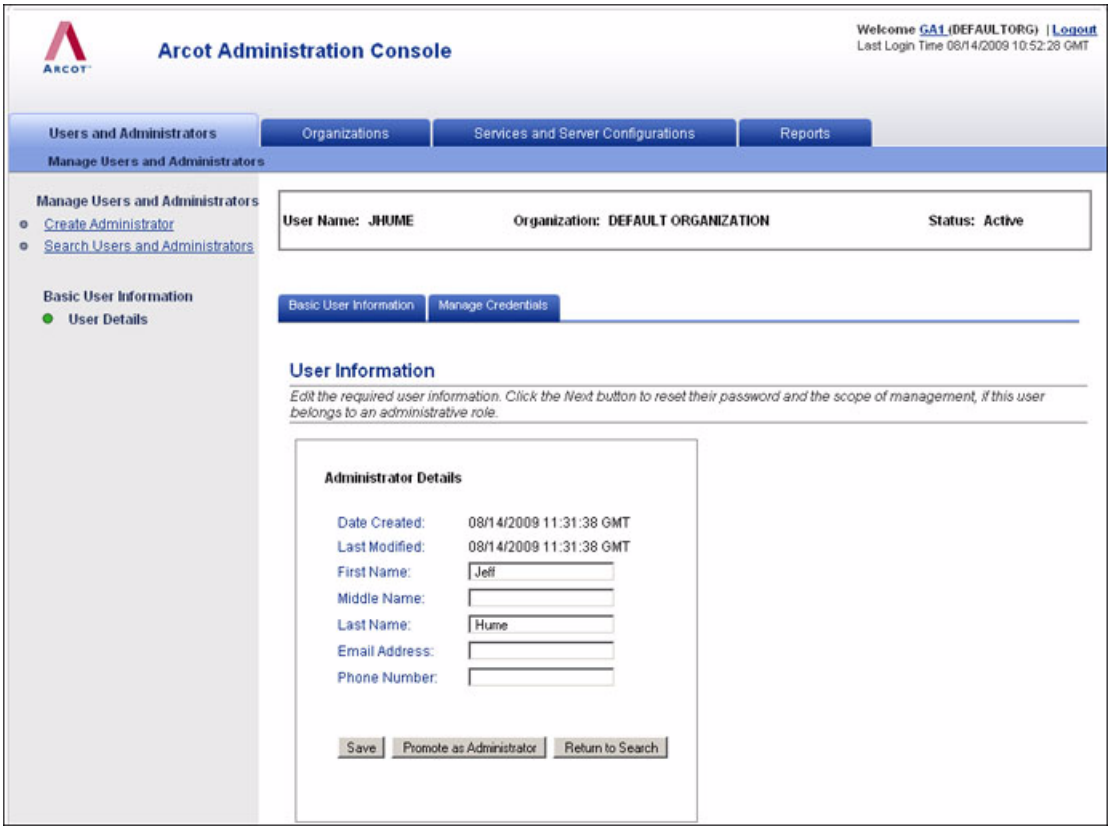
   図 7-3 のような［Basic User Information］ページが表示されます。

図 7-3［Basic User Information］ページ



6. ［**Edit**］をクリックし、図 7-4 に示されているように、このページのユーザ情報を変更します。

図 7-4［User Information］ページ



7. 必要なフィールド（［**First Name**］、［**Middle Name**］、［**Last Name**］、［**Email Address**］、および［**Phone Number**］）を編集します。
8. ［**Save**］をクリックして変更した内容を保存し、［User Information］ページに戻ります。

ユーザを管理者レベルに上げる

	**注：** ユーザ アカウント設定のレベルを上げるには、レベルを上げるための適切な権限とスコープを持っている必要があります。MA はいずれのユーザのレベルも上げることができます。GA、OA、および UA は、スコープ内のユーザのレベルを上げることができます。

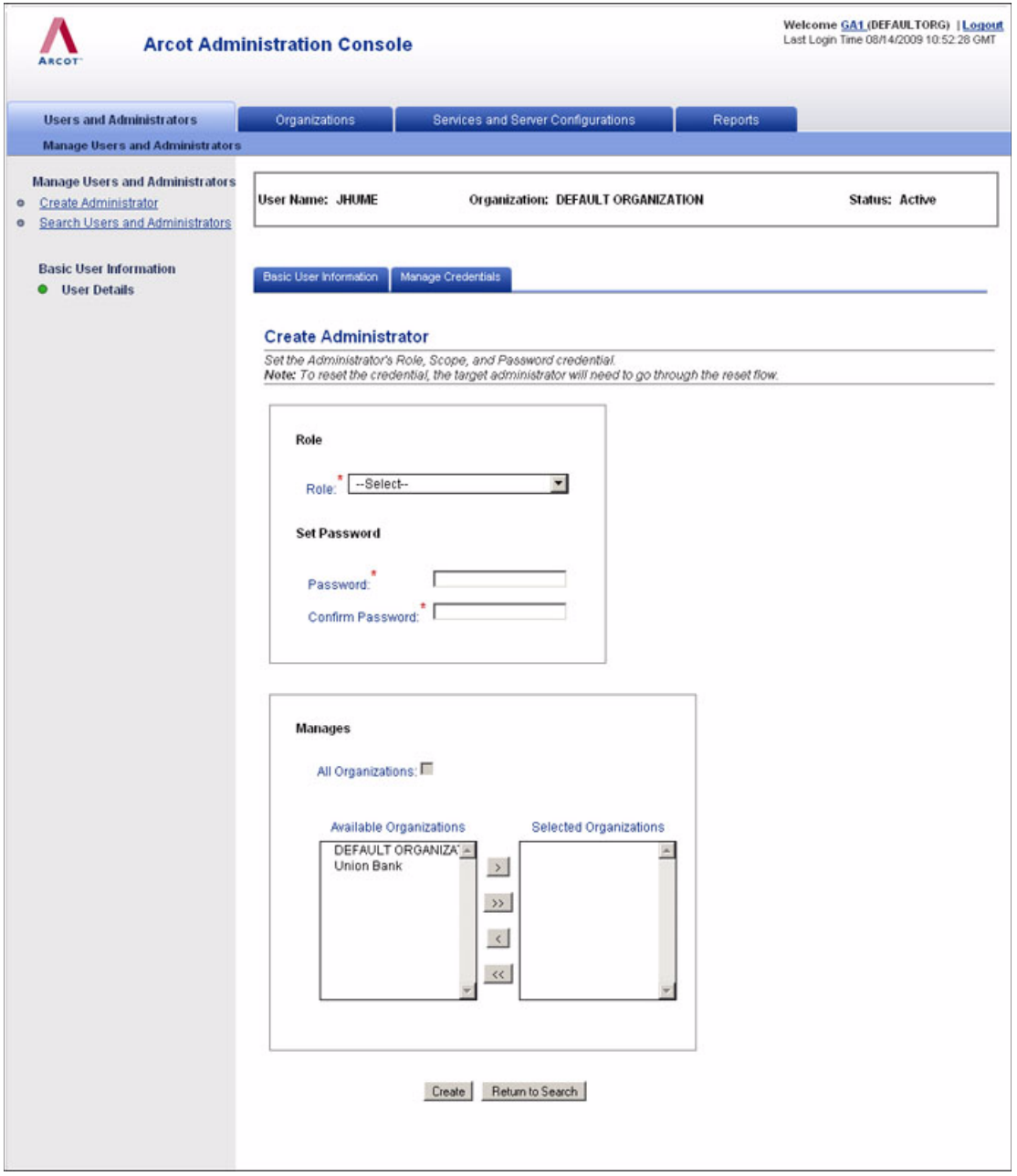
ユーザの管理ロール、パスワード、および管理スコープを更新する方法

1. 管理者を作成しユーザ情報を更新するために必要な権限およびスコープで、ログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションの［**Search Users and Administrators**］リンクをクリックすると、［Search Users and Administrators］ページ（図 7-1）が表示されます。
4. （前のセクションで説明されているように）アカウントを更新するユーザの部分的または完全な情報を入力し、［**Search**］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。
5. 編集するアカウントのユーザの *<user name>* リンクをクリックします。

   図 7-3 のような［Basic User Information］ページが表示されます。
6. ［**Edit**］をクリックすると、（図 7-4 のような）編集可能な［User Information］ページが開きます。
7. ユーザの［**Email Address**］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. ［**Promote as Administrator**］をクリックすると、［Create Administrator］ページ（図 7-5）が表示されます。

図 7-5［Create Administrator］ページ



9. このページ上で、以下の手順に従います。
   - ［**Role**］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。
   - 管理者アカウントのパスワードを［**Password**］および［**Confirm Password**］フィールドに入力します。

注 : 組織が WebFort ユーザ名 - パスワード認証用に設定されていると、これらのフィールドは表示されません。

   - ［**Manages**］セクションで、管理者がスコープを持つ組織を選択します。
     - 作成する管理者がシステム内の現在および将来のすべての組織を管理する場合は、［**All Organizations**］オプションを選択します。

       または

     - ［**Available Organizations**］リストから必要な組織を選択し、［>］ボタンをクリックすると、それらの組織が［**Selected Organizations**］リストに追加されます。

       ［**Available Organizations**］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。［**Selected Organizations**］には、この管理者が管理するように選択した組織のリストが表示されます。

10. ［**Create**］をクリックして、変更の保存、管理者アカウント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 WebFort ユーザ名 - パスワード認証を使用する組織に属している場合は、［**Create**］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、管理者レベルに上がったユーザが、Administration Console にログインするときに使用します。

ユーザ クレデンシャル情報の更新

ユーザは、システムに認証されるためにクレデンシャルを使用する必要があります。WebFort はすぐに使える ArcotID、Q&A、ユーザ名 - パスワード、OTP、OATH OTP および ArcotOTP の各クレデンシャルをサポートします。

ユーザのクレデンシャルを更新するには、［Credential Details］ページ（図 7-6）を使用する必要があります。このページでは、クレデンシャルの有効化または無効化、および有効期限の延長を行うことができます。

	**注：** ユーザのクレデンシャルを更新するには、更新するための適切な権限とスコープを持っている必要があります。MA はいずれのクレデンシャルも管理 *できません*。GA は、スコープ内の他の GA を含むすべてのユーザ アカウントのクレデンシャルを管理できます。OA と UA は、権限の範囲内のすべてのユーザのクレデンシャルを管理できます。

ユーザのクレデンシャルを更新する方法

1. ユーザのクレデンシャルを更新するために必要な権限およびスコープで、ログインしていることを確認します。
2. 7-206 ページの「ユーザ情報の更新」の手順 2 から手順 5 を完了します。
3. ［**Manage Credentials**］タブをアクティブにすると、［Credential Details］ページ（図 7-6）が表示されます。
4. 選択したユーザのすべてのクレデンシャルを同じステータスに設定するには、すべてのセクションで個々に変更しなくても、［**All Credentials**］セクションを使用してこれを行うことができます。これを行うには、以下の手順に従います。
   a. ［**All Credentials**］セクションを展開します。これをするには、左横の［**+**］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。
      - ［**Enable**］：ユーザのすべてのクレデンシャルを有効にします。
      - ［**Disable**］：ユーザのすべてのクレデンシャルを無効にします。
      - ［**Disable for a Period**］：ユーザのすべてのクレデンシャルを、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［**Save**］ボタンをクリックします。
5. クレデンシャル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. 目的のクレデンシャル セクションの左横の［**+**］記号をクリックすると、そのセクションが展開されます。

注 : ユーザが複数のユーザ名 - パスワード クレデンシャルを所有している場合、クレデンシャルごとに異なるセクション（**Username-Password <** ***（使用法）*** **>**）が表示されます。

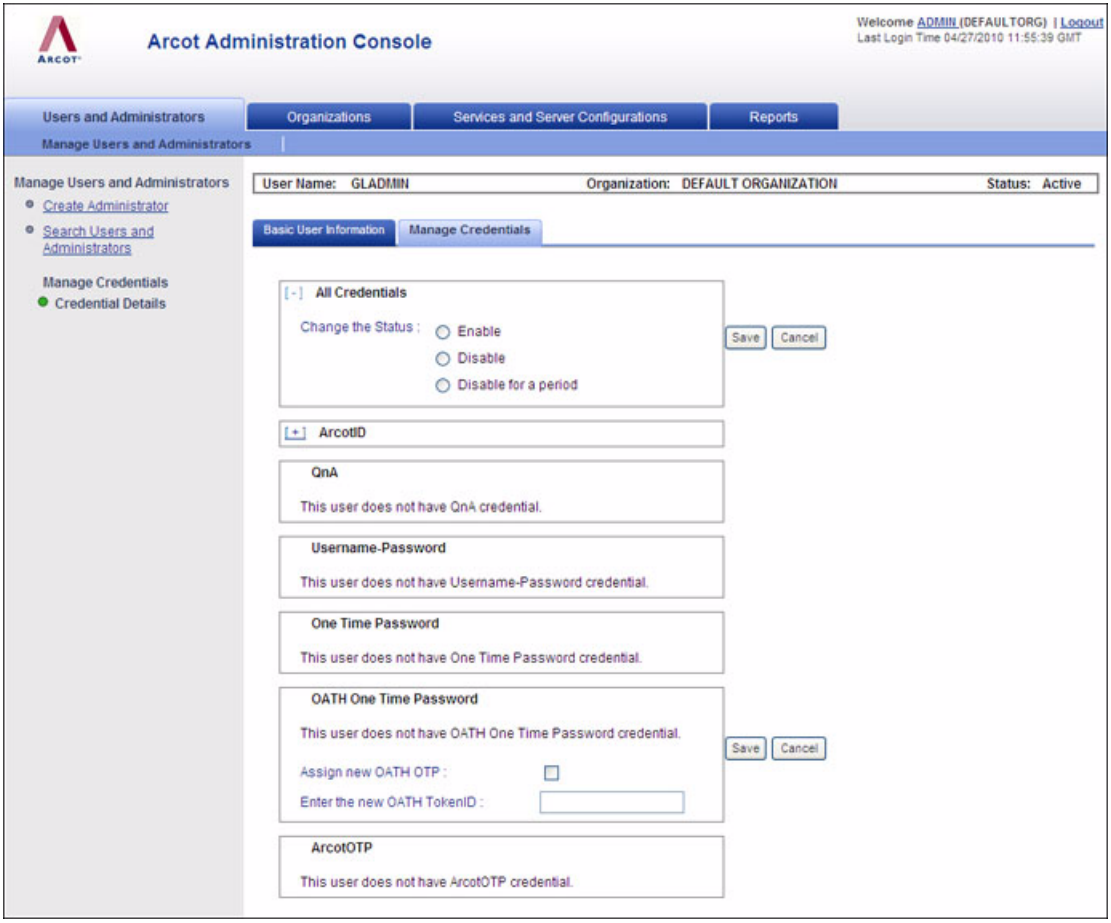
b. 目的のクレデンシャルの設定を変更します。このページを使用して、以下のクレデンシャル設定を変更できます。

- クレデンシャルのステータス
- クレデンシャルの有効期間の延長
- 既存のクレデンシャルのカスタム属性の追加または変更

注 : OATH OTP クレデンシャルについては、WebFort サーバによって生成される OATH OTP とベンダー トークン ID を関連付けることができます。

c. 変更したクレデンシャルに対応する［**Save**］ボタンをクリックします。

図 7-6［Credential Details］ページ



ユーザ アカウントの無効化

セキュリティ上の理由により、ユーザがアカウントにログインできないようにする場合、それらのアカウントを削除する代わりに無効にすることができます。ユーザ アカウントを無効にすると、ユーザはアカウントからロック アウトされ、アカウントが再度有効にされない限り、ログインできなくなります。

注： ユーザ アカウントを無効にするには、無効にするための適切な権限とスコープを持っている必要があります。MA はいずれのユーザ アカウントも無効にできます。GA はスコープ内の他の GA を含むすべてのユーザ アカウントを無効にできます。OA と UA は、権限の範囲内のすべてのユーザ アカウントを無効にできます。

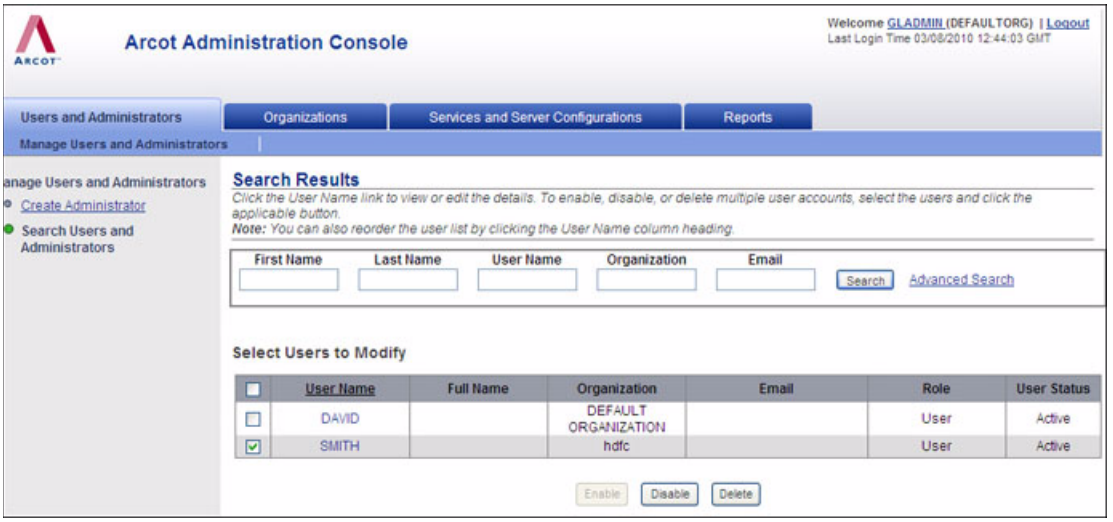
ユーザ アカウントを無効にする方法

1. ユーザ アカウントを無効にするために必要な権限およびスコープで、ログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションの［**Search Users and Administrators**］リンクをクリックすると、［Search Users and Administrators］ページ（図 7-1）が表示されます。
4. アカウントを無効にするユーザの部分的または完全な情報を入力し、［**Search**］をクリックします。

   ［**Advanced Search**］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（GA、OA、または UA）に基づいてユーザを検索できます。

   ［Search Results］ページ（図 7-7）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。

図 7-7 検索結果



5. アカウントを無効にする 1 つ以上のユーザを選択します。
6. ［**Disable**］をクリックすると、選択したユーザ アカウントが無効になります。

ユーザ アカウントの有効化

無効になっているアカウントの再有効化が必要になることがあります。たとえば、管理者が長期間の休暇を取得する場合、管理者のアカウントを無効にすることにより、管理者のアカウントへの不正なアクセスを防ぐことができます。

［Search Users and Administrators ］ページにおいて、検索条件を指定して［**Search**］ボタンをクリックしても、無効になっているアカウントを直接に検索することはできません。このようなユーザの場合には、［**Advanced Search**］を実行し、検索で［**Include Inactive Users**］オプションを使用します。

注 : ユーザ アカウントを有効にするには、有効にするための適切な権限とスコープを持っている必要があります。MA はいずれのアカウントも有効にすることができます。GA は、スコープ内のすべてのアカウントを有効にすることができます。OA と UA は、権限の範囲内のすべてのユーザ アカウントを有効にできます。

ロック アウトされたユーザ アカウントを有効にする方法

1. ユーザ アカウントを有効にするために必要な権限で、ログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションの［**Search Users and Administrators**］リンクをクリックすると、［Search Users and Administrators］ページ（図 7-1）が表示されます。
4. ［**Advanced Search**］をクリックし、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します。

   ［Advanced Search］ページ（図 7-2）が表示されます。
5. ［**User Account**］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。
6. ［**User Status**］セクションで、［**Include Inactive Users**］オプションを選択してすべての非アクティブなユーザ アカウントを検索します。
7. ［**Search**］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。
8. アカウントを有効にするユーザを選択します。
9. ［**Enable**］をクリックすると、ユーザ アカウントが有効になります。

ユーザ アカウントの削除

ユーザ アカウントを削除すると、そのアカウントに関連付けられたすべての権限が完全に削除されます。その結果、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。ただし、アカウント情報とクレデンシャルは、システムから削除されません。

以前に削除したユーザと同じ名前のユーザ アカウントを新しく作成しても、新しいアカウントが、以前に削除したアカウントの権限を自動的に引き継ぐことはありません。削除したアカウントを複製するには、すべての権限を手動で再作成する必要があります。

	**注：** ユーザ アカウントを削除するには、削除するための適切な権限とスコープを持っている必要があります。MA はいずれのアカウントも削除できます。GA は、スコープ内の MA アカウントを*除いて*、他の GA を含むすべてのアカウントを削除できます。OA と UA は、権限の範囲内のすべてのユーザ アカウントを削除できます。

ユーザ アカウントを削除する方法

1. ユーザ アカウントを削除するために必要な権限で、ログインしていることを確認します。
2. ［**Users and Administrators**］タブをアクティブにします。
3. ［**Manage Users and Administrators**］セクションの［**Search Users and Administrators**］リンクをクリックすると、［Search Users and Administrators］ページ（図 7-1）が表示されます。
4. アカウントを削除するユーザの部分的または完全な情報を入力し、［**Search**］をクリックします。

   ［**Advanced Search**］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（User）に基づいてユーザを検索できます。

   図 7-7 のような［Search Results］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. アカウントを削除する 1 つ以上のユーザを選択します。
6. ［**Delete**］をクリックします。

注： ユーザを削除しても、そのアカウント情報はデータベース内に維持されます。

第 8 章
レポートの管理

レポートを使用すると、管理者の階層レベルに応じて、WebFort データベースの情報を簡単に要約および分析できます。たとえば、上位の階層レベルの管理者は、システムにアクセスした下位の管理者に関して、管理者名、アクセス日時、および実行したアクティビティに関する情報を入手できます。以下のセクションは、管理者の階層レベルに応じて利用可能なレポートの簡単な概要を説明します。

- Master Administrator レポート
- Global Administrator レポート
- Organization Administrator レポート
- User Administrator レポート

レポートは Administration Console を通して利用でき、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
- 管理者名
- 組織
- ユーザ名

セクション「レポートの生成」は、管理者のためのアクティビティ レポートおよび WebFort 固有のレポートを生成するための一般的なプロセスについて説明します。

また、生成されたすべてのレポートをファイルにエクスポートできます。詳細については、「レポートをエクスポートする方法」を参照してください。

Master Administrator レポート

MA によって生成されるレポートは、概して次のように分類されます。

- 管理者レポート
- WebFort レポート

管理者レポート

この分類には、以下のレポートが含まれます。

- My Activity Report
- Administrator Activity Report
- Organization Report

My Activity Report

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、Administrator Activity Report 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、個別に提供されています。

- 管理者は、所属している組織をスコープに持たないことがあります。たとえば、管理者 *Alan* が組織「MyOrg」に属しますが、「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、Administrator Activity Report 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。
- Administrator Activity Report 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。My Activity Report 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。

図 8-1 は、My Activity Report のサンプルを示します。

図 8-1 My Activity Report

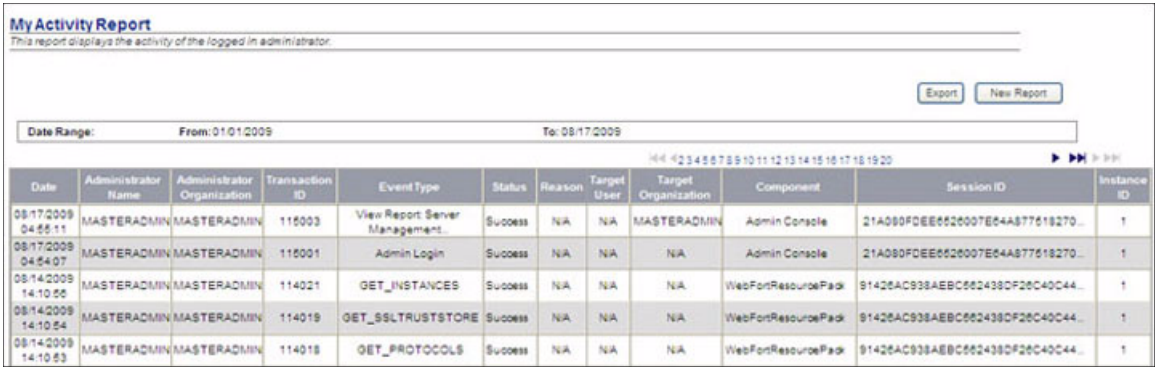


表 8-1 は、このレポートのフィールドについて説明します。

表 8-1. My Activity Report のフィールド

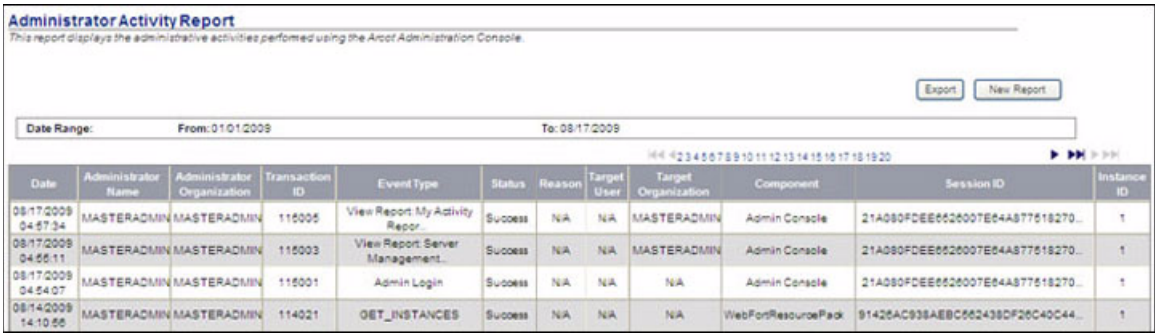
レポート フィールド	説明
[Date]	アクティビティを実行した日時です。
[Administrator Name]	レポートを生成している管理者の名前です。
[Administrator Organization]	管理者が属する組織の名前です。
[Transaction ID]	管理者によって実行されたアクティビティごとに生成された一意の ID です。
[Event Type]	管理者によって実行されたアクティビティのタイプ（作成、読み取り、変更、削除、表示など）です。
[Status]	実行されたアクションのステータスです。 • **Success** - アクションは正常に完了しました。 • **Failure** - アクションは正常に終了しませんでした。
[Reason]	操作が失敗した理由を示します。
[Target User]	属性が管理者によって管理されたユーザの名前です。
[Target Organization]	アクティビティが実行された組織です。
[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。 • Administration Console • WebFort
[Session ID]	管理者がログインした Administration Console のセッション識別子です。
[Instance ID]	複数の Administration Console アプリケーション インスタンスが実行している場合の、インスタンスの一意の識別子です。

Administrator Activity Report

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。

図 8-2 は Administrator Activity Report のサンプルを示します。

図 8-2 Administrator Activity Report



このレポートのフィールドは My Activity Report と同じです。フィールドの詳細については、表 8-1 を参照してください。

Organization Report

8-230 ページの「Organization Administrator レポート」で説明されている「Organization Report」を参照してください。

WebFort レポート

MA が生成できる WebFort 固有のレポートは Server Management Activity Report のみです。

Server Management Activity Report

このレポートは、MA によって実行された WebFort 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、信頼された認証機関の設定、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。

図 8-3 は、Server Management Report のサンプルを示します。

図 8-3 Server Management Report

表 8-2 は、このレポートのフィールドについて説明します。

表 8-2. Server Management Report のフィールド

レポート フィールド	説明
[Activity Time]	アクティビティを実行した日時です。
[Response Time (ms)]	リクエストを処理するために WebFort サーバによって費やされた時間（ミリ秒）です。
[Instance Configuration]	すべての WebFort サーバ インスタンス設定の詳細を示します。 ヒント：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]	WebFort サーバ インスタンスの名前です。
[Instance Status]	WebFort サーバ インスタンスのステータスです。
[Operation]	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。
[Response Code]	実行されたアクションのステータスです。 • **Success** - アクションは正常に完了しました。 • **Failure** - アクションは正常に終了しませんでした。

表 8-2. Server Management Report のフィールド

レポート フィールド	説明
[Transaction ID]	WebFort 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。
[Caller IP]	操作の実行元のシステムの IP アドレスです。
[Caller 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、[Caller ID] はブランクになることがあります。

Global Administrator レポート

GA によって生成されるレポートは、概して次のように分類されます。

- 管理者レポート
- WebFort レポート

管理者レポート

GA は、管理者関連の以下のレポートを生成できます。

- My Activity Report
- Administrator Activity Report
- Organization Report
- ユーザ アクティビティ レポート

My Activity Report

8-219 ページの「Master Administrator レポート」で説明されている「My Activity Report」を参照してください。

Administrator Activity Report

8-219 ページの「Master Administrator レポート」で説明されている「Administrator Activity Report」を参照してください。

Organization Report

8-230 ページの「Organization Administrator レポート」で説明されている「Organization Report」を参照してください。

ユーザ アクティビティ レポート

8-233 ページの「User Administrator レポート」で説明されている「ユーザ アクティビティ レポート」を参照してください。

WebFort レポート

GA は、WebFort 設定に関連する以下のレポートを生成できます。

- Authentication Activity Report
- Credential Management Activity Report
- Configuration Management Report

Authentication Activity Report

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。使用されたクレデンシャルのタイプ、クレデンシャルの有効性、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。

図 8-4 は、Authentication Activity Report のサンプルを示します。

図 8-4 Authentication Activity Report

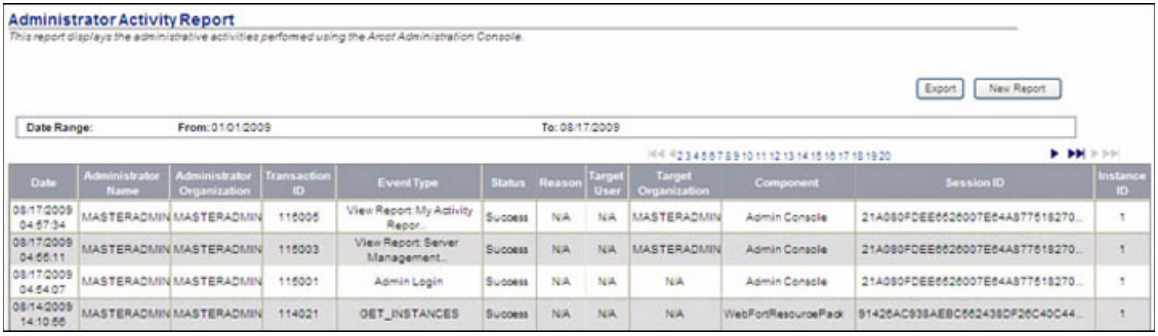


表 8-3 は、このレポートのフィールドについて説明します。

表 8-3. Authentication Activity Report のフィールド

レポート フィールド	説明
[Activity Time]	アクティビティを実行した日時です。
[Response Time (ms)]	リクエストを処理するために WebFort サーバによって費やされた時間（ミリ秒）です。
[Organization]	ユーザが属する組織の名前です。
[User Name]	認証アクティビティを実行したユーザの ID です。
[Credential Type]	認証に使用されたクレデンシャルのタイプです。
[Credential Status]	クレデンシャルのステータスです。
[Validity Start Date]	クレデンシャルの有効期間の開始日時のタイム スタンプです。
[Validity End Date]	クレデンシャルの有効期間の終了日時のタイム スタンプです
[Failed Attempts]	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。
[Remaining Uses]	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、他のクレデンシャルには適用 *されません*。
[Operation]	ユーザを認証するために WebFort サーバによって実行されたタスクです。
[Response Code]	実行されたアクションのステータスです。 • **Success** - アクションは正常に完了しました。 • **Failure** - アクションは正常に終了しませんでした。
[Reason Code]	[Operation] が失敗した理由です。
[Token Type]	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 Administration Console のセッション識別子です。
[Transaction ID]	トランザクションを追跡するために WebFort サーバによって生成された一意の識別子です。
[Protocol 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 WebFort サーバ インスタンスの名前です。
[Caller 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。
[Caller 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、[Caller ID] はブランクになることがあります。

Credential Management Activity Report

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。

図 8-5 は、Credential Management Report のサンプルを示します。

図 8-5 Credential Management Activity Report

表 8-4 は、このレポートのフィールドについて説明します。

表 8-4. Credential Management Report のフィールド

レポート フィールド	説明
[Activity Time]	アクティビティを実行した日時です。
[Response Time (ms)]	認証リクエストを処理するために WebFort サーバによって費やされた時間（ミリ秒）です。
[Organization]	ユーザが属する組織の名前です。
[User Name]	クレデンシャルが更新されたユーザの名前です。
[Credential Type]	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 • Q&A • OTP • パスワード

表 8-4. Credential Management Report のフィールド

レポート フィールド	説明
[Credential Status]	クレデンシャルの現在の状態です。以下のいずれかの値を示します。 • アクティブ • 無効 • 確認済み • ロック済み
[Validity Start Date]	クレデンシャルの有効期間の開始日時のタイム スタンプです。
[Validity End Date]	クレデンシャルの有効期間の終了日時のタイム スタンプです
[Failed Attempts]	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。
[Remaining Uses]	OTP を認証のために使用できる残りの回数です。
[Operation]	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。
[Response Code]	実行されたアクションのステータスです。 • **Success** - アクションは正常に完了しました。 • **Failure** - アクションは正常に終了しませんでした。
[Reason Code]	[Operation] が失敗した理由です。
[Transaction ID]	トランザクションを追跡するために WebFort サーバによって生成された一意の識別子です。
[Protocol 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 WebFort サーバ インスタンスの名前です。
[Caller 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。
[Caller 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、[Caller ID] はブランクになることがあります。
[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。

Configuration Management Report

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 WebFort 設定をリスト表示します。認証ポリシー、クレデンシャル プロファイル、プラグイン、コールアウト、SAML トークン、RADIUS クライアント、および ArcotID と Q&A 用の認証チャレンジの各設定情報を表示します。

図 8-6 は、Configuration Management Report のサンプルを示します。

図 8-6 Configuration Management Report

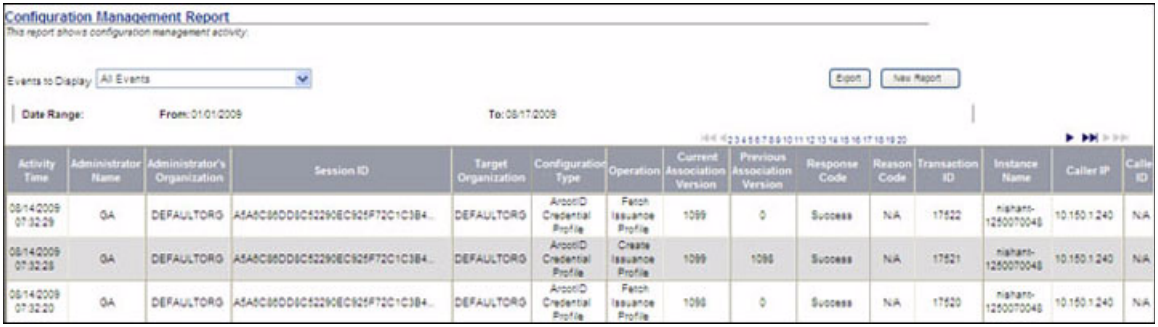


表 8-5 は、このレポートのフィールドについて説明します。

表 8-5. Configuration Management Report のフィールド

レポート フィールド	説明
[Activity Time]	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。
[Administrator's Organization]	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 Administration Console のセッション識別子です。
[Target Organization]	設定作成の対象となる組織です。
[Configuration Type]	影響を受けた（変更された）設定のタイプです。
[Operation]	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。
[Current Association Version]	設定の現バージョンです。
[Previous Association Version]	設定の旧バージョンです。
[Response Code]	実行されたアクションのステータスです。 • **Success** - アクションは正常に完了しました。 • **Failure** - アクションは正常に終了しませんでした。
[Reason Code]	操作が失敗した理由を示します。

表 8-5. Configuration Management Report のフィールド

レポート フィールド	説明
[Transaction ID]	WebFort 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]	WebFort サーバ インスタンスの名前です。
[Caller IP]	操作の実行元のシステムの IP アドレスです。
[Caller 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、[Caller ID] はブランクになることがあります。

Organization Administrator レポート

OA によって生成されるレポートは、概して次のように分類されます。

- 管理者レポート
- WebFort レポート

管理者レポート

OA は以下の管理者レポートを生成できます。

- My Activity Report
- Administrator Activity Report
- Organization Report
- ユーザ アクティビティ レポート

My Activity Report

「Master Administrator レポート」で説明されている「My Activity Report」を参照してください。

Administrator Activity Report

「Master Administrator レポート」で説明されている「Administrator Activity Report」を参照してください。

Organization Report

このレポートは、指定した組織上で実行し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。

図 8-7 は Organization Report のサンプルを示します。

図 8-7 Organization Report

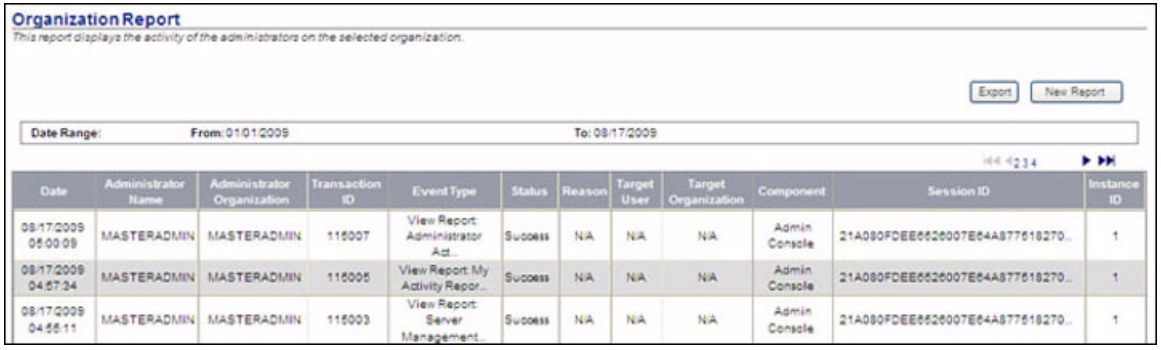


表 8-6 は、このレポートのフィールドについて説明します。

表 8-6. Organization Report のフィールド

レポート フィールド	説明
[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。
[Administrator Organization]	管理者が属する組織の名前です。
[Transaction 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。
[Status]	実行されたアクションのステータスです。 • **Success** - アクションは正常に完了しました。 • **Failure** - アクションは正常に終了しませんでした。
[Reason]	操作が失敗した理由を示します。
[Target User]	属性が管理者によって管理されたユーザの名前です。

表 8-6. Organization Report のフィールド

レポート フィールド	説明
[Target Organization]	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。 • Administration Console • WebFort
[Session ID]	管理者がログインした Administration Console のセッション識別子です。
[Instance ID]	複数の Administration Console アプリケーション インスタンスが実行している場合の、インスタンスの一意の識別子です。

ユーザ アクティビティ レポート

8-233 ページの「User Administrator レポート」で説明されている「ユーザ アクティビティ レポート」を参照してください。

WebFort レポート

OA は、WebFort 設定に関連する以下のレポートを生成できます。

- Authentication Activity Report
- Credential Management Activity Report
- Configuration Management Report

Authentication Activity Report

8-224 ページの「Global Administrator レポート」で説明されている「Authentication Activity Report」を参照してください。

Credential Management Activity Report

8-224 ページの「Global Administrator レポート」で説明されている「Credential Management Activity Report」を参照してください。

Configuration Management Report

8-224 ページの「Global Administrator レポート」で説明されている「Configuration Management Report」を参照してください。

User Administrator レポート

UA によって生成されるレポートは、概して次のように分類されます。

- 管理者レポート
- WebFort レポート

管理者レポート

UA は以下の管理者レポートを生成できます。

- My Activity Report
- Administrator Activity Report
- ユーザ アクティビティ レポート

My Activity Report

8-219 ページの「Master Administrator レポート」で説明されている「My Activity Report」を参照してください。

Administrator Activity Report

8-219 ページの「Master Administrator レポート」で説明されている「Administrator Activity Report」を参照してください。

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。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、ユーザの認証などのアクティビティを表示します。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。

図 8-8 は、ユーザ アクティビティ レポートのサンプルを示します。

図 8-8 ユーザ アクティビティ レポート

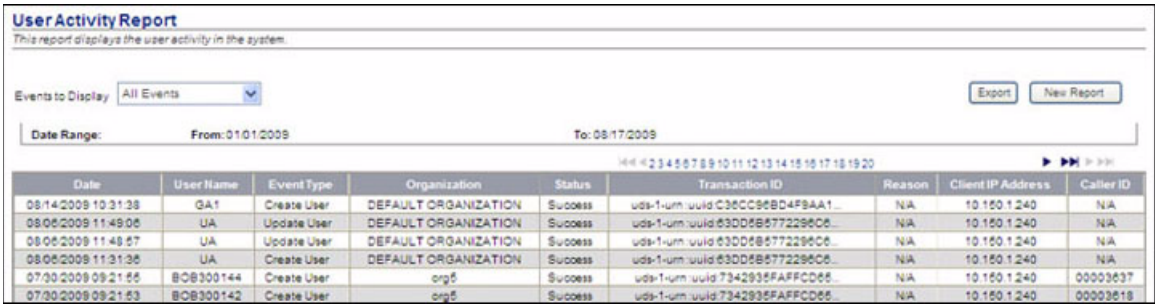


表 8-7 は、このレポートのフィールドについて説明します。

表 8-7. ユーザ アクティビティ レポートのフィールド

レポート フィールド	説明
[Date]	アクティビティを実行した日時です。
[User Name]	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。
[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。
[Organization]	ユーザが属する組織の名前です。
[Status]	操作のステータスです。 • **Success** - 操作は正常に完了しました。 • **Failure** - 操作は正常に終了しませんでした。
[Transaction 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。
[Reason]	操作が失敗した理由を示します。
[Client IP Address]	エンド ユーザのシステムの IP アドレスです。
[Caller 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、[Caller ID] はブランクになることがあります。

WebFort レポート

UA は以下の管理者レポートを生成できます。

- Authentication Activity Report
- Credential Management Report

Authentication Activity Report

8-224 ページの「Global Administrator レポート」で説明されている「Authentication Activity Report」を参照してください。

Credential Management Report

8-224 ページの「Global Administrator レポート」で説明されている「Credential Management Activity Report」を参照してください。

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
- レポートを生成する方法

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、Organization Administrator （OA）は、OA と User Administrator （UA）のレポートを生成できます。
- 管理者がカスタム ロール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、管理者 *MyGlobalAdmin* を GA から派生させて作成した場合、*MyGlobalAdmin は、GA とみなされます。これは、MyGlobalAdmin に、Organization Administrator または User Administrator より少ない権限を割り当てた場合も同じです。*
- 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

これまでの説明しているレポートを生成する方法

1. 適切なクレデンシャル（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［**Reports**］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。
   - Administrator Activity Report を生成する場合は、［**Administrator Reports**］サブメニューを選択します。
   - WebFort 固有のレポートを生成する場合は、［**WebFort Reports**］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 パネルに表示されます。
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. 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［**Date Range**］

        または
      - ［**From**］と ［**To**］のフィールドで事前定義済み日付範囲

   b. ［**Organization Name**］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。
   c. ［**User Name**］フィールドで、生成するレポートに応じて、以下の手順に従います。
      - Authentication Activity Report および Credential Management Report の場合、ユーザ名を入力します。

        または
      - 設定レポートの場合、管理者名を入力します。
6. ［**Display Report**］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。

レポートをエクスポートする方法

Administration Console 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［**Export**］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。詳細については、「レポートを生成する方法」を参照してください。

   レポートが表示されます。

2. ［**Export**］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. ［**Open**］または［**Save**］をクリックします。レポートの保存を選択した場合は、ダウンロードする場所を指定する必要があります。

   このファイルは後ほど適切なアプリケーションを使用して表示できます。

第 9 章
システム管理者用のツール

この章では、システム管理タスクを実行するために提供されている、WebFort のコマンド ライン ツールについて説明します。WebFort 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簡単な概要を説明します。

- DBUtil
- arwfserver
- arwfclient

DBUtil

WebFort のインストール時に、インストーラは、WebFort 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、WebFort サーバがデータベースに接続するための情報は、`securestore.enc` と呼ばれるファイルに暗号化された形式で格納されます。何らかの理由でデータベースのユーザ名またはパスワードを追加または変更することが必要になった場合、`DBUtil` ツールを使用して、これらの操作を実行できます。これを行うには、以下の手順に従います。

1. ツールが利用可能な場所に移動します。

   Windows の場合：

   < インストール ディレクトリ >`\Arcot Systems\bin\`

   UNIX ベースのプラットフォームの場合

   < インストール ディレクトリ >`/arcot/bin/`

2. 以下のコマンドを実行します。

   ```
   dbutil -h
   ```

   ツールでサポートされるコマンドが表示されます。

3. 実行する操作のタイプに応じてオプションを入力します。表 9-1 は、DBUtil で利用できるオプションを示します。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。DSN とパスワードのペアが WebFort サーバで使用され、ユーザ名とパスワードのペアが Administration Console とユーザ データ サービスで使用されます。

表 9-1. その他の DBUtil オプション

オプション	説明
-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 キー 例： dbutil -pd WebFortDatabaseDSNOld dbutil -pd Jack
-pi	追加のキーと値のペアを securestore.enc に挿入します。 構文： dbutil -pi キー 値 例： dbutil -pi WebFortBackupDSN dbapassword dbutil -pi Jack userpassword **重要：**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します。 構文： dbutil -pu キー 値 例： dbutil -pu WebFortDatabaseDSN newPassword dbutil -pu Jack userPassword

arwfserver

arwfserver ツールは中核的な認証サーバで、以下を設定するために対話モードでも実行できます。

- ほとんど使用されないか、特定の展開シナリオでのみ必要な WebFort 設定
- Administration Console で操作できない少数の設定

対話モードでのツールの実行

ツールを対話モードで実行するには、-i オプションを指定します。このモードでは、リスナは起動されませんが、すべてのサーバ設定はサービス モードとほとんど同様の方法で実行されます。

サーバはこのモードで実行されると、自身のコンソール プロンプト（wf>）を使用して開始し、**スタートアップ ログ**を *<インストール ディレクトリ>*/logs/arcotwebfortstartupcmd.log に、**トランザクション ログ**を *<インストール ディレクトリ>*/logs/arcotwebfortcmd.log に生成します。

arwfserver ツールを実行する方法

1. ツールが利用可能な場所に移動します。
   - **Windows の場合**

     <インストール ディレクトリ>\Arcot Systems\bin\
   - **UNIX ベースのプラットフォームの場合**

     <インストール ディレクトリ>/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. 表 9-2 に示されているオプションを指定して、必要なタスクを実行します。

表 9-2. arwfserver オプション

オプション	説明
?	arwfserver でサポートされるすべてのオプションに対するコマンドをリスト表示します。
help	特定のコマンドについてより詳細に説明します。
??	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、「??conf」と入力すると、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。
log2c	ファイルの代わりに、コンソールにログを出力します。 ログをコンソールに出力するには Y を、ファイルに出力するには N を入力します。

表 9-2. arwfserver オプション

オプション	説明
MD5	webfort-md5-<dd>-<mmm>-<yy>.txt と呼ばれるファイルを生成します。このファイルは、WebFort によってインストールされたすべてのファイルの MD5 ダイジェスト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**：< *インストール ディレクトリ* >\Arcot Systems\logs **UNIX ベースのプラットフォーム**：< *インストール ディレクトリ* >/arcot/logs
version	webfort-ver-<dd>-<mmm>-<yy>.txt と呼ばれるファイルを生成します。このファイルは、すべての WebFort ライブラリ ファイルのバージョン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**：< *インストール ディレクトリ* >\Arcot Systems\logs **UNIX ベースのプラットフォーム**：< *インストール ディレクトリ* >/arcot/logs
setsvrmgmtconf	サーバ管理プロトコルのポート番号を変更します。 WebFort 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。
setmiscconf	WebFort サーバ インスタンスが接続されているデータベース間の時間のずれの値を設定します。 **注：** これらの値を設定する必要がある場合は、Arcot のテクニカル サポート チーム（*support@arcot.com*）にお問い合わせください。
setmodconf	プラグインを有効化または無効化します。プラグインを有効化するには「1」を、無効化するには「0」を入力します。
setsaconf	認証と許可を行うために WebFort サーバによって提供されている Web サービス API を設定します。 アクセスを保護する場合は「1」を、通常のアクセスを使用する場合は「0」を入力します。
getmiscconf	setmiscconf の使用により設定される設定を取得します。
getmodconf	現在のモジュールの設定を取得します。たとえば、クレデンシャル モジュールおよびプラグインの設定を取得します。
getsaconf	Web サービスの現在のセキュリティ アクセスの詳細を取得します。API および対応する保護ステータスがリスト表示されます。
getprotoconf	すべてのプロトコルの設定を取得します。

表 9-2. arwfserver オプション

オプション	説明
uoathtok	ファイルから OATH トークン詳細をアップロードします。OATH トークンをアップロードするには、以下の情報を入力する必要があります。 • トークン詳細が含まれる XML ファイルのパス。 • XML ファイル内で機密情報を暗号化するために使用されるキー。たとえば、XML ファイル内の Secret フィールド。 • バッチ ID の番号。この値はアップロードされるトークンを識別するために使用されます。 • トークンが特定の組織向けである場合は、その組織の名前。
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。
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。
ddn	表示名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。
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。
q	対話モードを終了します。

arwfclient

arwfclient ツールを使用して、サーバのリフレッシュおよびサーバのシャットダウンを行うことができます。また、ライブラリ バージョン、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ができます。

対話モードでのツールの実行

ツールを対話モードで実行するには、-i オプションを指定します。ツールはこのモードで実行されると、それ自身のコンソール プロンプト（arwfclient#）を表示して開始します。

arwfclient ツールを実行する方法

1. ツールが利用可能な場所に移動します。
   - Windows の場合

     < インストール ディレクトリ >\Arcot Systems\bin\
   - UNIX ベースのプラットフォームの場合

< インストール ディレクトリ >/arcot/sbin/

2. 以下のコマンドを実行します。

   arwfclient -i

   ツールが対話モードで起動されます。

3. 表 9-3 に示されているオプションを指定して、必要なタスクを実行します。

表 9-3. arwfclient オプション

オプション	説明
?	arwfclient でサポートされる *すべて*のオプションに対するコマンドをリスト表示します。
help	特定のコマンドについてより詳細に説明します。
ssc	サーバ設定を設定します。 **重要 :** 設定対象の WebFort サーバのインスタンス 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。
sso	各プロトコルの統計を設定します。 プロトコルごとの統計を設定するために「1」を入力します。
gss	webfort-stats-<dd>-<mmm>-<yy>.txt と呼ばれる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** : *< インストール ディレクトリ >*\Arcot Systems\logs **UNIX ベースのプラットフォーム** : *< インストール ディレクトリ >*/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 • すべてのリクエストを処理するために総時間 • リクエストを処理するために費やされた平均時間
cr	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、メッセージ「Instance refreshed successfully」とトランザクション ID が返されます。

表 9-3. arwfclient オプション（続き）

オプション	説明
`sd`	WebFort 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、メッセージ「Successfully initiated shutdown operations」とトランザクション ID が返されます。
`q`	対話モードを終了します。

付録 A
WebFort のログ

WebFort サーバとユーザのアプリケーションの間の通信を効率的に管理するために、サーバのアクティビティおよびパフォーマンスならびに発生したあらゆる問題に関する情報を取得する必要があります。

この付録では、WebFort によってサポートされる各種ログ ファイル、これらのファイルで出現する重大度レベル、およびこれらのログ ファイルのフォーマットについて説明します。この章には、以下のトピックがあります。

- ログ ファイルについて
- WebFort ログ ファイルのフォーマット
- UDS ログ ファイルおよび Administration Console ログ ファイルのフォーマット
- サポートされる重大度レベル

ログ ファイルについて

WebFort ログ ファイルは次のように分類できます。

- スタートアップ ログ ファイル
- トランザクション ログ ファイル
- UDS ログ ファイル
- Administration Console ログ ファイル

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、UDS ログ ファイルと Administration Console 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、WebFort ログ ファイルの場合は Administration Console 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典型的なログ記録設定オプションには次のものが含まれます。

- **Specifying log file name and path**：ログ ファイルを書き込み、バックアップ ログ ファイルを格納するため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 ファイルの最大バイト数です。ログ ファイルがこのサイズに達すると、指定された名前の新規ファイルが作成されます。また、古いファイルはバックアップ ディレクトリに移動されます。
- **Using log file archiving**：WebFort コンポーネントが実行され、診断メッセージを生成するにつれて、ログ ファイルのサイズが増加します。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。ログ ファイル データが収集および保存される量を制限する設定オプションを指定できます。WebFort では、診断ログ記録ファイルのサイズを制御する設定オプションを指定できます。これにより、ログ ファイルの最大サイズを決定することができます。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てから、新しいログ情報が保存されます。
- **Setting logging levels**：WebFort では、ロギング レベルを設定することもできます。ロギング レベルを設定することによって、診断ログ ファイルに保存されるメッセージの数を減少できます。たとえば、システムが重要なメッセージのみをレポートし保存するように、ロギング レベルを設定できます。サポートされるログ レベルの詳細については、「サポートされる重大度レベル」を参照してください。
- **Specifying time zone information**：ログ記録された情報のタイム スタンプを記録するために、ローカル タイム ゾーンまたは GMT のいずれかを使用できます。

スタートアップ ログ ファイル

WebFort 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。このファイル内の情報は、WebFort サービス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：

< インストール ディレクトリ >`\Arcot Systems\logs\`

UNIX ベースの場合：

< インストール ディレクトリ >`/arcot/logs/`

トランザクション ログ ファイル

トランザクション ログには以下のタイプがあります。

- WebFort サーバのログ
- WebFort 統計ログ ファイル

WebFort サーバのログ

WebFort では、サーバが処理したリクエストはすべて arcotwebfort.log ファイルに保存されます。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：

< インストール ディレクトリ >\Arcot Systems\logs\

UNIX ベースの場合：

< インストール ディレクトリ >/arcot/logs/

このファイルのログ記録を制御するパラメータは、Administration Console を使用することによって設定できます。パラメータを設定するには、対象のインスタンスを［**Instance Management**］画面でクリックし、インスタンス固有のサブ画面を使用する必要があります。

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 フォーマットの詳細については、A-251 ページの「WebFort ログ ファイルのフォーマット」を参照してください。

WebFort 統計ログ ファイル

WebFort では、統計のログ記録に arcotwebfortstats.log ファイルを使用します。

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：

< インストール ディレクトリ >\Arcot Systems\logs\

UNIX ベースの場合：

< インストール ディレクトリ >/arcot/logs/

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、Administration Console 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：

<インストール ディレクトリ>\Arcot Systems\logs\

UNIX ベースの場合：

<インストール ディレクトリ>/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 フォーマットの詳細については、「UDS ログ ファイルおよび Administration Console ログ ファイルのフォーマット」を参照してください。

Administration Console ログ ファイル

ユーザが Administration Console を展開して開始すると、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、Master Administrator が指定した他の Administration Console 情報

このファイル内の情報は、Administration Console 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：

<インストール ディレクトリ>\Arcot Systems\logs\

UNIX ベースの場合：

< インストール ディレクトリ >/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。

ロギング 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 フォーマットの詳細については、「UDS ログ ファイルおよび Administration Console ログ ファイルのフォーマット」を参照してください。

WebFort ログ ファイルのフォーマット

表 A-1 に、以下の WebFort ロガーのエントリのフォーマットを示します。

- arcotwebfort.log（WebFort サーバのログ）
- arcotwebfortstartup.log （スタートアップ ログ ファイル）
- arcotwebfortstats.log （WebFort 統計ログ ファイル）

表 A-1. WebFort のログ フォーマット

列	説明
タイム スタンプ	エントリがログ記録された時間です。設定したタイム ゾーンに変換されます。この情報のログ記録のフォーマットは、以下のとおりです。 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）	ログ記録されたエントリの重大度レベルです。詳細については、「サポートされる重大度レベル」を参照してください。 **注：** WebFort では、フロー詳細を含むトレース ロギングも用意されています。トレース ログは、arcotwebfort.log ファイルにログ記録されます。トレース メッセージのエントリは TRACE: で始まります。

表 A-1. WebFort のログ フォーマット

列	説明
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です。以下のいずれかの値です。 • AUTH_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、または監視モードである場合、プロトコルは使用されず、以下の値がそれぞれ表示されます。 • STARTUP • SHUTDOWN • MONITOR
スレッド ID (THREADID)	エントリをログ記録したスレッドの ID です。
トランザクション ID (000TXNID)	エントリをログ記録したトランザクションの ID です。
メッセージ	自由なフォーマットでサーバによりログ ファイルにログ記録されたメッセージです。 **注：** メッセージの粒度は、ログ ファイルで設定される**ログ レベル**によって決まります。

UDS ログ ファイルおよび Administration Console ログ ファイルのフォーマット

表 A-2 に、以下のロガーのエントリのフォーマットを示します。

- arcotuds.log （UDS ログ ファイル）
- arcotadmin.log （Administration Console ログ ファイル）

表 A-2. UDS ログ ファイルおよび Administration Console ログ ファイルのフォーマット

列	関連付けられたパターン（ログ ファイル内）	説明
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。この情報のログ記録のフォーマットは、以下のとおりです。 `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] :`	エントリをログ記録したスレッドの ID です。
ログ レベル（または重大度）	`%-5p :`	ログ記録されたエントリの重大度レベルです。 詳細については、サポートされる重大度レベル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 :`	自由なフォーマットでサーバによりログ ファイルにログ記録されたメッセージです。 **注**：メッセージの粒度は、ログ ファイルで設定される**ログ レベル**によって決まります。

UDS ログ ファイルおよび Administration Console 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（または重大度レベル）を使用すると、WebFort ログに格納された情報の詳細のレベルを指定できます。また、ログ ファイルのサイズが増加する速度を制御できます。

表 A-3 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に示します。

表 A-3. WebFort ログ レベル（重大度の降順）

ログ レベル		説明
0	FATAL	このログ レベルは、WebFort サービスの突然な終了を引き起こす場合がある、重大で回復不能なエラーに使用します。
1	WARNING	このログ レベルは、FATAL と分類するほどではないが、望ましくないランタイム例外、潜在的に有害な状況、および回復可能な問題に使用します。
2	INFO	このログ レベルは、ランタイム イベントについての情報を収集するために使用します。 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	このログ レベルは、デバッグ目的で詳細情報のログ記録に使用します。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： WebFort サーバ（arcotwebfort.log）については、これらのレベルのいずれにもログ記録を設定します。また、TRACE ログ記録がフロー詳細を収集することもできます。

注： ログ レベルを指定すると、重要度が*より高い*他のすべてのレベルのメッセージも同様にレポートされます。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。

WebFort ログ ファイル内のいくつかサンプル 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
```

WARNING

```
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
```

（WebFort 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 B
用語集

Administration Console	WebFort サーバとそのコンポーネントの間の通信モードを設定し、管理タスクを実行するための Web ベースのコンソール。
Adobe 署名サービス プロトコル	「ASSP」を参照してください。
ArcotID	ソフトウェアの形でのハードウェア レベルの認証を可能にするセキュアなソフトウェア クレデンシャル。
ASSP	Acrobat と Reader のユーザがデジタル署名のローミング クレデンシャルにアクセスできるようにします。ASSP はハッシュを ASSP 対応サーバに渡して署名をし、その後でハッシュをエンド ユーザのドキュメントに埋め込みます。
Digest-MD5	広く使用される暗号化ハッシュ関数。ハッシュ値は 128 ビットです。
FYP（Forgot Your Password、パスワードを忘れた場合）	ユーザが ArcotID のパスワードを忘れた場合、ユーザと WebFort の間で Q&A セッションが実施されます。ユーザは簡単な質問に答えた後で、新しい ArcotID パスワードの入力を求められ、新しい ArcotID が発行されます。
MA **（Master Administrator、マスタ管理者）**	必要に応じて、WebFort のセットアップおよびそのコンポーネント（Administration Console および UDS を含む）の初期化、ならびに GA、OA および UA の作成を担当するメイン管理者。
OTP	「ワンタイム パスワード」を参照してください。
OTT	「ワンタイム トークン」を参照してください。
PKCS	RSA によって考案され発行された公開キー暗号化標準のグループ。詳細については、「公開キー暗号化法」を参照してください。
PKCS#12	パスワードベースの対称キーで保護された添付の公開キー証明書を使用して秘密キーを保存するために共通で使用されるファイル フォーマットの定義。
PKI（Public Key Infrastructure）	ネットワーク環境における公開キー暗号化法および証明書の使用を促進する標準およびサービス。
Q&A	チャレンジ レスポンス認証メカニズム。Q&A を使用することにより、ユーザ エージェントとサーバの間で情報を交換するダイアログが表示されます。サーバは任意の数の質問をし、ユーザは正しい回答を提供します。

RADIUS **Remote Authentication Dial-In User Service**	一元化された認証、許可、および監査（AAA）用のプロトコル。
SAML	ID プロバイダ（アサーションを提供します）とサービス プロバイダ（アサーションを使用します）の間の認証データの交換のための XML 基準。
Security Assertion Markup Language	「SAML」を参照してください。
SHA（Secure Hash Algorithm）	暗号化ハッシュ関数のセット。
SSL **（Secure Sockets Layer）**	データの暗号化により、公衆ネットワーク間での通信のセキュリティ保護および認証を目的とするプロトコル。
SSO（Single Sign-On）	複数のシステム間で共有される単一の ID。SSO によって、ユーザがコンピュータまたはネットワークに 1 回ログオンすると、単一のクレデンシャルを使用して複数のアプリケーションおよびシステムにアクセスできます。
UDS	「ユーザ データ サービス」を参照してください。
WebFort	エンド ユーザを認証するための強力な認証システム。
WebFort サーバ	WebFort SDK を介してアプリケーションと通信し、発行リクエストと認証リクエストを受理するサーバ コンポーネント。
GA **（Global Administrator、グローバル管理者）**	CSR 管理者アカウントのセットアップおよびシステムの設定を担当する管理者。
OA **（Organization Administrator）**	組織の管理に関連するすべてのタスクを担当する管理者。
UA **（User Administrator）**	セキュリティ システムのユーザに関連する日常業務を担当する管理者。この管理者は、ユーザの登録支援、ユーザ パスワードのリセット、およびさまざまな登録レポートの表示を行います。

アクティベーション コード	組織が WebFort ユーザ名 - パスワード認証メカニズムを使用するように設定されている場合に管理者がログインするための、WebFort サーバによって返される 8 桁の数値コード。
インスタンス	指定されたポートで WebFort サーバが利用可能なシステム。
エラー メッセージ	エラーが発生した場合に、その状況に関してユーザ エージェントに報告するためにアプリケーションによって返されるメッセージ。
カスタム ロール	GA、OA、および UA を含む事前に定義した親ロールの 1 つから権限のサブセットを継承することにより派生するロール。
クレデンシャル	ユーザ ID を証明するもの。デジタル クレデンシャルがスマート カードまたは USB トークンなどのハードウェアまたはサーバ上に保存される場合があります。そのクレデンシャルは認証時に検証されます。
クレデンシャル プロファイル	複数の組織および複数のユーザの間で共有可能な、すぐに使える共通のクレデンシャル設定。
サンプル アプリケーション	WebFort Java API の使用方法と、ユーザのアプリケーションを WebFort に統合する方法を示す例。また、WebFort が正常にインストールされたかどうか、発行操作と認証操作を実行できるかどうかを確認するために使用できます。
デジタル証明書	証明書は、個人、コンピュータ システム、または組織の ID およびキーの所有権の証明となるデジタル ドキュメント。この認証方式は PKI 暗号化法に基づいています。
デフォルトの組織	ユーザが Administration Console を展開するときにデフォルトで作成される組織。
ユーザ データ サービス	WebFort が既存の LDAP ベースのユーザ情報にアクセスできるようにしたり、データベースに LDAP ユーザをマッピングしたりするためのサービス。
ユーザ名 / パスワード	登録時にユーザに発行されるクレデンシャルの 1 つ。
ワンタイム トークン	認証成功後に WebFort サーバによって返されるトークン。
ワンタイム パスワード	単一セッションで有効なパスワード クレデンシャル。WebFort には、複数回使用できる OTP が実装されています。
暗号化	内容を判読できないように情報にスクランブルをかける処理。
暗号化ハッシュ関数	認証などのセキュリティ関連アプリケーションで使用される、セキュリティ プロパティが追加されたハッシュ関数。
公開キー	公開キー暗号化法で使用される 1 対のキーの一方。公開キーは自由に配布され、証明書の一部としてとして発行されます。通常、公開キーの所有者に送信されたデータを暗号化するために使用されます。その後、公開キーの所有者は、対応する秘密キーを使用して、データを復号化します。

公開キー暗号化法	秘密の共有について事前に合意しなくてもユーザが安全に通信することができる最新の暗号化形式。この方法では、対称暗号化法と異なり、全員が知っている公開キーと、公開キーと秘密キーのペアの所有者のみが知っている秘密キーという 2 つのキーを使用します。公開キー暗号化法は、非対称暗号化法とも呼ばれます。
再試行許容回数 N 回	ユーザが認証を失敗できる最大回数。この数を超えると、ユーザはロック アウトされます。
質問と回答	「Q&A」を参照してください。
組織	企業全体（すなわち会社）、特定の部門、または企業内の他のエンティティにマッピングできる WebFort の単位。
認証	エンティティのログイン情報が本人のものであることを証明するプロセス。
認証 SDK	WebFort サーバに認証リクエストを転送するためにアプリケーションによって呼び出し可能な API。
認証トークン	トークンは、コンピュータ サービスの許可ユーザに与えられるオブジェクトで、認証の際に補助的に使用されます。
認証ポリシー	認証プロセスを制御するルールのセット。
発行 SDK	WebFort へのユーザ登録およびユーザのクレデンシャル作成のために WebFort サーバに発行リクエストを転送するためにアプリケーションによって呼び出し可能な API。
秘密キー	公開キー暗号化法で使用される 1 対のキーの一方。このキーは秘密に保持され、データの復号化または暗号化に使用できます。

索引

A

Administration Console 1-1
ASSP 5-155

B

BA 2-32

E

EcA 1-15

L

log
  重大度レベル A-253

S

SAML 5-152

U

UDS 2-23

い

イベント 5-163
インスタンス 1-1

か

管理ユーザ
  Global Administrator 1-9
  Master Administrator 1-8
  Organization Administrator 1-10
  User Administrator 1-10

き

基本認証 2-32

く

クレデンシャル プロファイル 4-74
  ArcotID プロファイル 4-84
  ArcotOTP プロファイル 4-121
  OATH OTP ポリシー 4-114
  OTP プロファイル 4-107
  Q&A プロファイル 4-91
  ユーザ名 - パスワード プロファイル 4-99

こ

コールアウト 5-158

し

システム管理ツール 9-239
  DBUtil 9-239
システム ツール
  arwfclient 9-243
  arwfserver 9-240
信頼されるストア 3-50

す
スコープ 1-7

せ
接続プーリング 3-47

そ
組織 5-135

た
対象読者 A-ix

て
デフォルトの組織 2-28

と
登録 7-203

に
認証ポリシー 4-75
- ArcotID ポリシー 4-88
- ArcotOTP ポリシー 4-124
- OATH OTP ポリシー 4-117
- OTP ポリシー 4-111
- Q&A ポリシー 4-95
- ユーザ名 - パスワード ポリシー 4-104

は
ハンドラ ファイル 3-63

ふ
プラグイン 3-61
プラグイン設定テンプレート ファイル 3-63
プラグイン ライブラリ ファイル 3-63
プロファイル 4-74

ゆ
ユーザ データ サービス 2-23
優先組織 6-182

ろ
ロール 1-1
- 管理ユーザ 1-6
- ユーザ 1-6

ログ レベル A-253