Arcot WebFort™ Administration Guide

Version 6.0

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot WebFort Administration Guide
Version 6.0
August 2009
Part Number: AWF01-002DC-60000

Copyright © 2009 Arcot Systems, Inc. All rights reserved.

This guide, as well as the software described herein, is furnished under license and may be used or copied only in accordance with the terms of the license. The content of this guide is furnished for informational purposes only. It is subject to change without notice and should not be construed as a commitment by Arcot Systems.

Arcot Systems makes no warranty of any kind with regard to this guide. This includes, but is not limited to the implied warranties of merchantability, fitness for a particular purpose or non-infringement. Arcot Systems shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Except as permitted by the software license, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior written permission of Arcot Systems, Inc.

Trademarks

Arcot®, ArcotID®, and WebFort VAS® are registered trademarks of Arcot Systems, Inc. The Arcot logo™, the Authentication Authority tagline, ArcotID Client™, RegFort™, RiskFort™, SignFort™, and TransFort™ are all trademarks of Arcot Systems, Inc.

All other product or company names may be trademarks of their respective owners.

Patents

This software is protected by United States Patent No. 6,170,058, 6,209,102 and other patents pending.

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

Third Party Software

All third-party software used by Arcot WebFort and related components are listed in the appendix “Third-Party Software Licenses” in the *Arcot WebFort 6.0 Installation and Deployment Guide*.

Contents

Preface . . . . . **ix**
Intended Audience ix
Information Included in this Guide ix
Related Publication x
Conventions Used in This Book xi
Contacting Support xi

Chapter 1 Overview of the Administration Console **1**
About the Administration Console 2
Elements of the Administration Console 3
Supported Roles 6
Users 6
Default Administrative Roles 6
Scope of an Administrative Role 7
Master Administrator 8
Global Administrator 9
Organization Administrator 10
User Administrator 10
Summary of Administrative Privileges 11
Custom Roles 14
Next Steps 16
For Simple Deployments 16
For Custom Deployments 17

Chapter 2 Getting Started **21**
Accessing the Administration Console 22
Configuring Administration Console Settings 24

Specifying UDS Configurations 24
Specifying Global Settings for Organizations 28
Specifying Cache Refresh Settings 30
Specifying Basic Authentication Policy Settings 31
Specifying the Basic Authentication Password Policy 31
Changing Profile Information 34

Chapter 3 Managing WebFort Server Instances 37
Configuring WebFort Connectivity 38
Setting Up Server Instances 40
Refreshing or Shutting Down Instances 42
Restarting a Server Instance 42
Changing the Instance Name 43
Managing WebFort Server Logging Configurations 44
Configuring Database Parameters 46
Enabling Connectivity Statistics Logging 47
Reading Instance Timestamp Details 48
Creating Trust Stores 49
Configuring Communication Protocols 50
Monitoring Instance Statistics 54
Database Connectivity 55
Server Protocols 56
User Data Service Connectivity 56
Registering and Updating Plug-Ins 58
Registering Plug-Ins 59
Updating Plug-In Configurations 60
Configuring Miscellaneous Settings 61
Working with Custom Roles 63
Creating a Custom Role 63
Updating a Custom Role Information 64
Deleting a Custom Role 66

Chapter 4 Managing Global WebFort Configurations 69
Understanding WebFort Profiles and Policies 71
Credential Profiles 71
Authentication Policies 71
Logging in as a Global Administrator 72
Using WebFort Username-Password 72
In Case You Forgot Your Password 74
Using Basic Username-Password 76
Logging Out of the Administration Console 77
Security Recommendations While Using the Administration Console 77

Configuring ArcotID Settings 78
Configuring ArcotID Credential Profile 78
Configuring ArcotID Authentication Policy 82
Configuring QnA Settings 85
Configuring QnA Issuance Profile 85
Configuring QnA Authentication Policy 88
Configuring Username-Password Settings 91
Configuring Username-Password Issuance Profile 91
Configuring Username-Password Authentication Policy 94
Configuring OTP Settings 97
Configuring OTP Issuance Profile 97
Configuring OTP Authentication Policy 100
Assigning Default Configurations 103

Chapter 5 Managing Organizations 105
Creating and Activating Organizations 106
Creating Organizations in Arcot Repository 106
Creating Organization in LDAP Repository 110
Searching for Organizations 116
Managing Organization-Specific Configurations 118
Configuring SAML Tokens 121
Configuring RADIUS Clients 124
Configuring RADIUS Clients 124
Deleting and Updating RADIUS Clients 126
Configuring ASSP 127
Configuring Callouts 130
Configuring Plug-Ins 133
Associating Events 135
Updating Organization Information 137
Updating the Organization Information 137
Updating WebFort-Specific Configurations 139
Disabling Organizations 140
Enabling Organizations 141
Activating Organizations in Initial State 142
Deleting Organizations 143

Chapter 6 Managing Administrators 145
Creating Administrators 146
Creating an Account with WebFort Username-Password Credential 146
Creating an Account with Basic Username-Password Credential 149
Changing Profile Information for Administrator Accounts 151
For Accounts with WebFort Username-Password Credential 151

For Accounts with Basic Username-Password Credential 153
Searching Administrators 155
Updating Administrator Account Information 157
Regenerating Activation Code 161
Updating Administrator Credentials 163
Disabling Administrator Accounts 165
Enabling Administrator Accounts 167
Deleting Administrator Accounts 168

Chapter 7 Managing Users 169
Searching Users 170
Updating User Information 172
Promoting Users to Administrators 175
Updating User Credential Information 178
Disabling User Accounts 180
Enabling User Accounts 182
Deleting User Accounts 183

Chapter 8 Managing Reports 185
Master Administrator Reports 186
Administrator Reports 186
My Activity Report 186
Administrator Activity Report 188
Organization Report 188
WebFort Reports 188
Server Management Activity Report 189
Global Administrator Reports 191
Administrator Reports 191
My Activity Report 191
Administrator Activity Report 191
Organization Report 191
User Activity Report 191
WebFort Reports 192
Authentication Activity Report 192
Credential Management Activity Report 193
Configuration Management Report 195
Organization Administrator Reports 197
Administrator Reports 197
My Activity Report 197
Administrator Activity Report 197
Organization Report 197
User Activity Report 199

WebFort Reports . . . 199
Authentication Activity Report . . . 199
Credential Management Activity Report . . . 199
Configuration Management Report . . . 199
User Administrator Reports . . . 200
Administrator Reports . . . 200
My Activity Report . . . 200
Administrator Activity Report . . . 200
User Activity Report . . . 200
WebFort Reports . . . 201
Authentication Activity Report . . . 202
Credential Management Report . . . 202
Generating Reports . . . 203
Notes for Generating Reports . . . 203
Generating the Report . . . 203
Exporting Reports . . . 205

Chapter 9 Tools for System Administrators . . . 207
dbutil . . . 208
webfortserver . . . 210
arwfclient . . . 212

Appendix A WebFort Logging . . . 215
About the Log Files . . . 216
Startup Log File . . . 217
Transaction Log Files . . . 217
WebFort Server Log . . . 217
WebFort Statistics Log File . . . 217
UDS Log File . . . 218
Administration Console Log File . . . 218
Format of the WebFort Log Files . . . 220
Format of UDS and Administration Console Log Files . . . 222
Supported Severity Levels . . . 223

Appendix B Glossary . . . 225

Index . . . 229

Preface

The Arcot WebFort 6.0 Administration Guide provides information for setting up and managing Arcot WebFort 6.0 using the Arcot Administration Console. This guide covers information for both Windows and UNIX-based platforms (Solaris SPARC® and Red Hat Enterprise Linux 4.0.)

Intended Audience

This guide is intended for administrators of Arcot WebFort. It describes how to use the Administration Console to perform the typical administrative tasks relating to maintenance, provisioning, updating, monitoring performance, and modifications of WebFort configurations.

This guide is intended for users who are experienced with:

- Operating system-based administration
- Applicable Oracle and/or MS SQL databases
- Application server and Web server administration

Information Included in this Guide

This guide is organized as follows:

- **Chapter 1, "Overview of the Administration Console"**, introduces you to the WebFort Administration Console interface and management hierarchy.

- **Chapter 2, "Getting Started"**, describes the basic administrative tasks, such as creating administrators, logging in and out of the Administration Console, changing the administrator password. It also discusses the procedures for creating, updating, and deleting administrator accounts.
- **Chapter 3, "Managing WebFort Server Instances"**, describes how to set up and manage WebFort Server instances.
- **Chapter 4, "Managing Global WebFort Configurations"**, describes the configurations that you can set at the global level, and that can be inherited by individual organizations configured in the system.
- **Chapter 5, "Managing Organizations"**, describes how to create, search, activate, enable, disable, or delete organizations in WebFort. The chapter also walks you through the tasks to manage organization-specific configurations that cannot be set at global level.
- **Chapter 6, "Managing Administrators"**, describes how to create, search, activate, enable, disable, or delete various administrators in the system.
- **Chapter 7, "Managing Users"**, describes how to search, activate, enable, disable, or delete end users by using the Administration Console.
- **Chapter 8, "Managing Reports"**, discusses the reports available to each administrative level and explains the use of these reports.
- **Chapter 9, "Tools for System Administrators"**, discusses the tools provided by WebFort that system administrators can use to monitor and manage the system.
- **Appendix A, "WebFort Logging"**, covers information about all WebFort log files, the severity levels recorded in the files, and the format of the entries in these files.
- **Appendix B, "Glossary"**, lists the key terms used in the guide.

Related Publication

Other related publications are as follows:

Arcot WebFort 6.0 Installation and Deployment Guide	This guide provides information for installing and configuring WebFort and its components.
Arcot WebFort 6.0 Java Developer's Guide	This guide describes the Java APIs provided by WebFort and also explains how to use them.
Arcot WebFort 6.0 Business Logic Extension Guide	This guide provides information about how to write a plug-in or callout to extend the existing authentication and issuance processes.

ArcotID Client 6.0 Reference Guide	This guide describes ArcotID Client types and the APIs provided by the client.
ArcotID Flash Client 6.0 API Guide	This guide explains the ArcotID Flash client APIs provided by the client.

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Click the **Install** button to install the product.
Italic	Key Words	First time log in to the *Administration Console* must be done using Master Admin credentials.
	Names of Publications	For more information, see the *Arcot WebFort Installation and Deployment Guide*.
	Emphasis	*Never* give anyone your password.
Cross reference	Links in the guide	Refer to the section Searching Users for more information.
`Fixed-width`	Command-line input or output	`# cd /opt/oracle/`
	Code Samples	`./webfortserver start`

	Text File Content	`[arcot/db/primarydb]`
		`# The name of the data source as`
		`# defined in ODBC.`
		`Datasource.1=ArcotWebFortDatabase`

	File and folder names	`arcotcommon.ini`

Contacting Support

If you need help, contact Arcot Support as follows:

Email	`support@arcot.com`
Web site	`http://support.arcot.com`

Chapter 1

Overview of the Administration Console

Arcot Administration Console (referred to as "Administration Console" later in the guide) is a Web-based, operation and system management tool, which provides a consistent, unified interface for managing all Arcot products.

This console offers true *multi-tenant* architecture, which enables you to use a single instance of the console to administer multiple organizations or business units within an enterprise. In this model, each organization or business unit can be set up individually with its own configuration. On the other hand, the Administration Console also provides you with the ability to inherit configuration data from the system level and build only specific configurations for each organization.

This chapter introduces you to the Administration Console interface and the supported administrator hierarchy. It covers the following topics:

- About the Administration Console
- Elements of the Administration Console
- Supported Roles
- Next Steps

NOTE: The recommended desktop screen resolution for Administration Console is 1024 x 768.

About the Administration Console

The Administration Console is a Web browser-based, graphical user interface and is accessible from any supported Web browser with network access to the Administration Server. This console enables you to manage all deployed WebFort instances, where an *instance* represents a WebFort Server that is available on a specified port.

You can use the Administration Console to configure WebFort, to set up users and administrative roles, and complete other administrative operations and configuration tasks, such as:

- Configure and refresh server instances
- Configure communication parameters between the server and other WebFort components
- Manage organizations, administrators, users and their credentials
- Set authentication policies
- Set credential profiles
- Generate administration, transaction, and configuration reports

The tasks that you are authorized to perform display on the Administration Console through various tabs. These tasks are based on the user group or role that you belong to and the administrative privileges that this role has.

Elements of the Administration Console

A typical Administrative screen can be divided in to the following elements:

- Header
- Main Menu
- Sub Menu
- Tasks
- Body

Figure 1-1 illustrates the placement of these elements in the Administration Console.

Figure 1-1 General Layout of the Administration Console

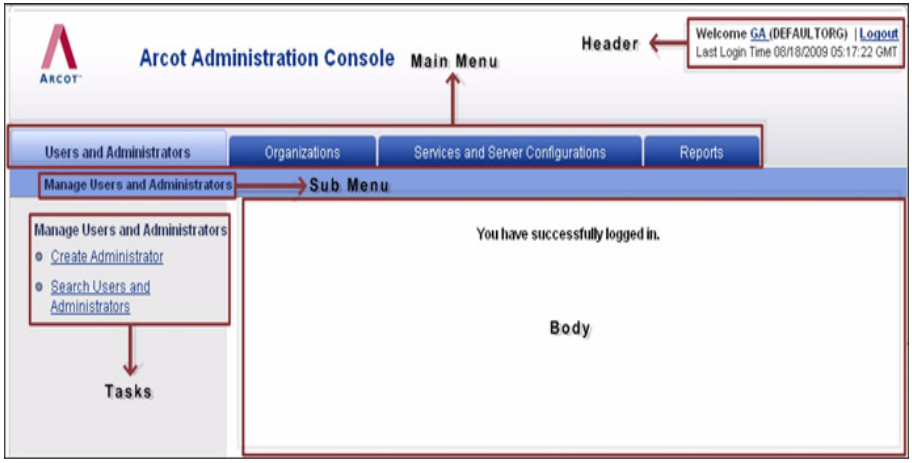


Table 1-1 describes these elements.

Table 1-1 Elements of the Administration Console

Element	Description
Header	Displays login information (administrator name, current organization, the last login date, and time). You can use the links in the header to: • Change the profile information (name, phone number, email ID) and current password. You can also specify the organization that will be selected by default in the Organization field for all tasks that you might perform in future. • Log out from the Administration Console.
Main Menu	Displays the main configuration and management options available to the current administrator.
Sub Menu	Displays the options available for the Main Menu item that you selected.
Tasks	Displays the tasks available for the Sub Menu item that you selected.
Body	Displays the corresponding page for the selected task.

Console Messages

As shown in Figure 1-2, all the information, warning, and error messages that are generated in the course of using the Administration Console are displayed at the top of the body page.

While the error messages are displayed in red, as shown in Figure 1-2, the messages indicating success are displayed in blue. Any additional instructions are also a part of these messages, as shown in Figure 1-3.

Figure 1-2 Console Message: Error

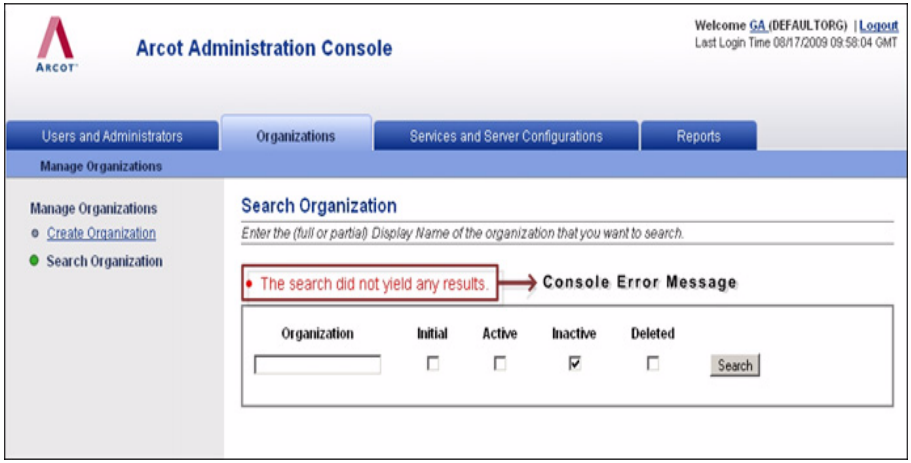
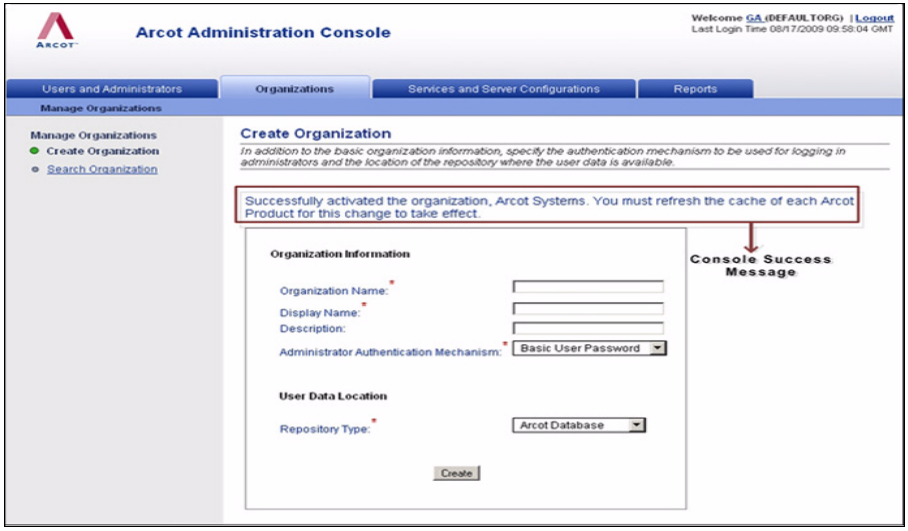


Figure 1-3 Console Message: Success



Supported Roles

Roles enable you to specify which operations and privileges are assigned to a user or a set of users who share similar responsibilities. When a user is assigned to a specific role, the set of functions called tasks that are associated to that role become available to the user. As a result, administrators can exercise fine-grain control on the tasks assigned to each user in the system.

The Arcot Administration Console provides you flexibility to set up your administration hierarchy and assign rights to the administrators. You can create different levels of administrators, each with varying degrees of access. You can also create administrators that can, in turn, delegate administration tasks to other users.

The Administration Console supports the following types of roles:

- **Users**
- **Default Administrative Roles**
- **Custom Roles**

Users

Every end user of your online application system is referred to as a *user* in Arcot Administration Console. This user can either exist in your Lightweight Directory Access Protocol (LDAP) repository or in WebFort database.

If the user already exists in your LDAP system, then you need to map the organization LDAP attributes to Arcot supported attributes. See **"Creating Organization in LDAP Repository"** for more information on how to do this.

To create the users in WebFort database, select the organization whose repository type is Arcot Database. See **"Creating Organizations in Arcot Repository"** for more information on how to do this.

Default Administrative Roles

The Administration Console is shipped with an out-of-the-box administrative user called the **Master Administrator**. Other than this, you must assign users to administrative roles to administer the WebFort system or to access business data.

Any user who you "promote" to an administrative role is referred to as an *administrative user*. An administrative role typically comprises a set of privileges based on a job function profile and the scope in which these permissions are applicable.

> **NOTE:** See "Summary of Administrative Privileges" on page 11 for a comprehensive list of privileges available to the each administrative role.

The Administration Console supports the following pre-defined administrative roles:

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

In addition, you can also create Custom Roles.

Scope of an Administrative Role

The *scope* of an administrative role in the Arcot Administration Console consists of:

- All the organizations that the role can manage.
- The privileges the role has on the organizations.
- The tasks assigned to the role.

Important Notes About Scope

While creating an administrative role, you must remember that:

- The scope of the Master Administrator is **All Organizations** by default, and this administrator manages *all* existing and future organizations. This cannot be changed.
- A role (Global Administrator, Organization Administrator, or User Administrator) can only manage down the administrative hierarchy, never up. In other words, a role that manages a child role is defined so that it does not manage the child's parent.

  For example, a GA can manage OAs and UAs. However, they *cannot* manage an MA.
- A Global Administrator role scope can be defined as All Organizations, in which case the role can manage all existing as well as future organizations.
- An **Organization Administrator** or a **User Administrator** role *should not* be defined with the scope as All Organizations.

- An **Organization Administrator** or a **User Administrator** role can be limited to manage only specific organizations.
- If the administrator is derived by using **Custom Roles**, then the derived administrator belongs to the same level as that of the parent level.

  For example, if you derive an administrator MyGlobalAdmin from GA, then MyGlobalAdmin is considered to be a GA, even though you might have assigned MyGlobalAdmin less number of privileges compared to an OA or UA.

Master Administrator

The MA is the super user of the system, who has unrestricted access to the whole system. The default scope of an MA is All Organizations, as a result of which they can manage all the existing organizations as well as those organizations that will be created by them or any other administrator in the future.

The primary responsibilities of an MA are to:

- Bootstrap (or initialize) the system after installation.
- Configure the User Data Service (UDS) connection parameters.
- Configure the global organizations settings and cache refresh settings for the Administration Console.
- Configure the WebFort Server communication parameters.
- Configure the WebFort Server instance settings, trust store settings, and protocol settings.
- Configure the authentication mechanism for the Administration Console and Server components and other miscellaneous settings.
- Register plug-ins, if you are using any, for supported events.

  NOTE: See the *Arcot WebFort 6.0 Business Logic Extension Guide* for more information on how to write callouts and plug-ins. Also see **"Registering and Updating Plug-Ins"** for more information on how to register a plug-in, **"Configuring Callouts" on page 130** on how to configure a callout, and **"Configuring Plug-Ins" on page 133** on how to configure a plug-in.

- Create and manage organizations, as required.
- Create and manage administrators of any role (Global, Organization, or User Administrator), as required.
- Manage **Custom Roles**.
- Generate instance statistics.

At the end of a successful deployment of Administration Console, you must log in for the first time as a Master Administrator (MA). The MA account (**masteradmin**) is shipped with a default password (**master1234!**). Because the actions of an MA can affect the security of the entire system, Arcot strongly recommends that you change this password after you log in to the console for the first time. Arcot also recommends that you safeguard this password and change it regularly.

> **NOTE:** In case if the account is locked, then you must contact Arcot Technical Support at support@arcot.com.

To track and analyze data, an MA can not only generate a comprehensive report of all their activities, but also generate a report for the activities of other administrators in the system. In addition, they can also generate reports for all organizations and reports for all server configurations.

Global Administrator

The Global Administrator (GA) is the second level in the WebFort administrative hierarchy. These administrators can perform most of the tasks of an MA, except for bootsrapping the system, performing initial Administration Console configurations, specifying server configurations, and creating custom roles.

Typically when you create a GA, you need to specify the scope of their administration. Unless you do so, they cannot manage any organization.

The main tasks of a GA are to:

- Create and manage other Global, Organization, or User Administrators, as required.
- Configure the authentication policy for the Administration Console.
- Create and manage organizations, as required.

  > **NOTE:** This includes editing the organization details.

- Manage user credentials.
- Configure WebFort Profiles and Policies for supported authentication mechanisms.
- Assign configurations.
- Configure callouts and registered plug-ins.

To track and analyze available information, GAs can generate and view all administrative activity, configuration, and credential management reports for the organizations under their administrative purview. They can also view the reports for all the Organization and User Administrators assigned to them.

Organization Administrator

The Organization Administrator (OA) is the third level in the administrative hierarchy. These administrators can perform all tasks related to management of the organizations assigned to them either by the MA or a GA and the users that belong to the organizations. These tasks include:

- Managing organizations in their purview.
- Managing (updating) organization-specific configurations.
- Managing the users that belong to the organizations they manage.
- Managing the User Administrators assigned to them.

When you create an OA, you need to specify the scope of their administration. Unless you do so, they cannot manage any organization.

OAs can generate and view administrative activity, configuration, and transaction reports for the organizations under their administrative purview. They can also view the reports for all the User Administrators assigned to them.

User Administrator

The User Administrator (UA) role is the final level in the administrative hierarchy. These administrators can perform all tasks related to user management for the organizations assigned to them either by the MA or a GA. These include:

- Creating and managing users, as required, for the organizations under their purview.

  NOTE: This includes editing the user details.

- Manage user credentials.
- Promoting users to UAs.

When you create a UA, you need to specify the scope of their administration. Unless you do so, they cannot manage any organization.

UAs can generate and view user and UA activity reports for the organizations under their administrative purview.

Summary of Administrative Privileges

Table 1-2 summarizes the privileges available to the supported three levels of administrators.

The column name acronyms used in the table are:

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

NOTE: The ✓ sign indicates the actions (or privileges) that are available to the specified level of administrator.

Table 1-2 Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
Authentication Policy Management	Update the Basic Authentication Policy	✓	✓	✓	
	Update WebFort Authentication Configuration	✓			
Cache Management	Update Cache Refresh Configuration	✓			
Global Administrator Account Management	Create Global Administrator Accounts	✓	✓		
	Search or View Global Administrator Details	✓	✓		
	Update Global Administrator Account Information	✓	✓		
	Delete Global Administrator Accounts	✓	✓		

Table 1-2 Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
Organization Administrator Account Management	Create Organization Administrator Accounts	✓	✓	✓	
	Search or View Organization Administrator Details	✓	✓	✓	
	Update Organization Administrator Account Information	✓	✓	✓	
	Delete Organization Administrator Accounts	✓	✓	✓	
User Administrator Account Management	Create User Administrator Accounts	✓	✓	✓	✓
	Search or View User Administrator Details	✓	✓	✓	✓
	Update User Administrator Account Information	✓	✓	✓	✓
	Delete User Administrator Accounts	✓	✓	✓	✓
User Data Service (UDS) Management	Update Global User Data Service (UDS) Configuration	✓			
Custom Role Management	Create Custom Roles	✓			
	Update Custom Roles	✓			
	Delete Custom Roles	✓			
Default Organization Management	Configure Default Organization	✓			
Organization Management	Create Organizations	✓	✓		
	Search and View Organization Details	✓	✓	✓	✓
	Update Organization Information	✓	✓	✓	
	Activate Organizations	✓	✓	✓	✓
	Deactivate Organizations	✓	✓	✓	✓
	Delete Organizations	✓	✓		

Table 1-2 Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
User Management	Search and View User Details	✓	✓	✓	✓
	Update User Information	✓	✓	✓	✓
	Activate Users	✓	✓	✓	✓
	Deactivate Users	✓	✓	✓	✓
	Delete Users	✓	✓	✓	✓
WebFort Configurations	Create ArcotID Policy		✓	✓	
	Assign Configurations		✓	✓	
	Register Callouts		✓	✓	
	Configure Plug-ins		✓	✓	
	Manage ArcotID Profiles		✓	✓	
	Manage ASSP Configuration		✓	✓	
	Manage OTP Profiles		✓	✓	
	Manage Username-Password Profiles		✓	✓	
	Manage QnA Profiles		✓	✓	
	Manage RADIUS Configurations		✓	✓	
	Manage SAML Tokens		✓	✓	
	Create OTP Policies		✓	✓	
	Create Password Policies		✓	✓	
	Associate Events		✓	✓	
	Create QnA Policies		✓	✓	
	Update System Configurations		✓		
	View Credential Details		✓	✓	✓

Table 1-2 Administrative Privileges Summary

Feature	Task	MA	GA	OA	UA
Instance Management	WebFort Connectivity	✓			
	Instance Management	✓			
	Protocol Management	✓			
	Plug-in Registration	✓			
	Miscellaneous Configuration	✓			
	Generate Instance Statistics	✓			
	Set Trusted CA	✓			
Reports Management	View Administrator Activity Report	✓	✓	✓	✓
	View My Activity Report	✓	✓	✓	✓
	Organization Report	✓	✓	✓	
	View User Activity Report		✓	✓	✓
	View Authentication Report		✓	✓	
	View Credential Report		✓	✓	
	Server Management Report	✓			
	Configuration Report		✓	✓	

Custom Roles

As MA, you can also create new administrative roles that inherit a subset of privileges from one of the following predefined parent roles:

- **Global Administrator**
- **Organization Administrator**
- **User Administrator**

These roles are called *custom roles*, and are derived by **disabling** some of the default privileges associated with the parent role. For example if you need to disable the "Organization Creation Privilege" for a GA, then you can create a Custom role for the purpose.

If you create a Custom role, then it becomes available as a role option when you create a new administrative account.

Notes About Custom Roles

- Only an MA can create custom roles.
- A custom role can only inherit the subset of privileges from a single role. In other words, a custom role *cannot* inherit privileges from two different roles.

  For example, you *cannot* create a custom UA role that has privileges to manage users (UA privilege) and create organizations (OA privilege.)
- You cannot assign new privileges to a custom role, if the parent role does not have these privileges.

  For example, if the predefined OA roles does not have the privilege to Create an Organization, then the custom role based on this OA role cannot have that privilege either.
- When you create a custom role, a task representing one or more privileges will continue to be visible, as long as at least one of the privileges is *still* available.

  For example, the "Search Organizations" link will appear if the Update privilege is still available, even though the Activate, Deactivate, and Delete privileges are disabled.
- A new custom role is available to other instances of Administration Console *only after* you refresh the Administration Console server cache.

Next Steps

Now that you are familiar with the WebFort Administration Console concepts, this section quickly walks you through the steps for getting ready for administering your deployment. For this purpose, it provide a quick overview for:

- For Simple Deployments
- For Custom Deployments

For Simple Deployments

The simplest implementation of WebFort typically provides strong authentication internally for a small user base. It consists of all the WebFort components and Web applications installed on a single system. The database can be on the same system where WebFort is installed, or on a different system.

See Chapter 2, "Planning the Deployment" in the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on this type of deployments.

Table 1-3 summarizes the typical characteristics of this deployment type.

Table 1-3 Characteristics of Simple Deployments

Characteristic	Details
Deployment Type	• Development, proof of concept, initial testing, or initial pilot • Small to medium businesses (SMBs) • Regional deployment within an enterprise
Geographic Expanse	Typically restricted to a single location
Deployment Requirements	Ease of implementation and management

In case of small deployments, most of the default settings will work out of the box. Because this is a single-organization system, you can use the Default Organization that is created automatically when you initialize the system instead of setting up a new organization. As a result, you might not need OA accounts either. You, then, only need to create the required GA and UA accounts.

You can create the end users in WebFort by using the SDKs that are shipped with the system. (See *Arcot WebFort 6.0 Developer's Guide* for more information on how to use the SDKs for creating users.)

The quick overview of the steps to set up and start managing strong authentication for your users is:

1. Ensure that WebFort is installed and configured properly and that you have deployed the WAR files for the Administration Console and User Data Service.

   See Chapter 4, "Deploying WebFort on a Single System" in the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on installing WebFort, deploying the WAR files, and performing other post-installation tasks.

2. Log into the Administration Console as MA (see **"Accessing the Administration Console" on page 22**) and follow the steps in the Bootstrap wizard to initialize the system.

   See section, "Bootstrapping the System" in Chapter 4 of the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information.

3. Create the required GA and UA accounts.

   See **"Creating Administrators" on page 146** for more information.

4. Enroll users with WebFort.

   Use Java SDKs shipped with WebFort for this purpose. See *Arcot WebFort 6.0 Developer's Guide* for detailed information on how to integrate with these SDKs.

With this your system is set for administration. You can now manage the system (**Chapter 3, "Managing WebFort Server Instances"**), administrators (**Chapter 6, "Managing Administrators"**), and users (**Chapter 7, "Managing Users"**).

For Custom Deployments

In larger enterprises, where the deployments are complex and high availability is a must, WebFort can be implemented to provide strong authentication for the large user base, as well as administrators who manage the system. In these deployments, WebFort components are installed on different servers. This is done for security, performance, high availability, and/or to enable multiple applications to use the strong-authentication functionality.

See Chapter 2, "Planning the Deployment" in the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on this type of deployments.

Table 1-4 summarizes the typical characteristics of this deployment type.

Table 1-4 Characteristics of Distributed Deployments

Characteristic	Details
Deployment Type	• Complex medium to large businesses • Enterprise deployments • Staging deployments
Geographic Expanse	Distributed across the globe
Deployment Requirements	• Ease of implementation and management • Global availability • High availability

The quick overview of the steps to set up and start managing strong authentication for your users is:

1. Ensure that WebFort is installed and configured properly and that you have deployed the WAR files for the Administration Console and User Data Service.

   See Chapter 4, "Deploying WebFort on a Single System" in the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information on installing WebFort, deploying the WAR files, and performing other post-installation tasks.

2. Log into the Administration Console as MA (see **"Accessing the Administration Console" on page 22**) and follow the steps in the Bootstrap wizard to initialize the system.

   See section, "Bootstrapping the System" in Chapter 4 of the *Arcot WebFort 6.0 Installation and Deployment Guide* for more information.

3. Configure the Administration Console settings, which include UDS settings, global organization settings, Administration Console cache settings, and the basic username-password authentication policy for logging in to the console.

   See **"Configuring Administration Console Settings" on page 24** for more information.

4. Set up WebFort Server instances on different systems.

   See **"Setting Up Server Instances" on page 40** for more information.

5. Configure the protocols that Administration Console, SDKs, and Web Services use to communicate to WebFort Server.

   See **"Configuring Communication Protocols" on page 50** for more information.

6. Plan and create organizations. The organization architecture is flat and each organization that you create can map to a business unit in your enterprise.

   See **"Creating and Activating Organizations" on page 106** for more information.

7. Plan and create the administrators (see **"Creating Administrators" on page 146**) and custom roles (see **"Working with Custom Roles" on page 63**), if required.

8. Create appropriate **Credential Profiles** and **Authentication Policies**, and assign these configurations.

   See **Chapter 4, "Managing Global WebFort Configurations"** for more information.

9. Enroll users with WebFort.

   Use Java SDKs shipped with WebFort for this purpose. See *Arcot WebFort 6.0 Developer's Guide* for detailed information on how to integrate with these SDKs.

10. If required, configure the SAML token settings, RADIUS clients, and ASSP settings.

    See **"Managing Organization-Specific Configurations" on page 118** for more information.

11. If required, configure SSL-based communication between WebFort Server and its clients.

    See **"Creating Trust Stores" on page 49** for more information.

12. If required, configure the miscellaneous settings (such as token validity and challenge validity settings.)

    See **"Configuring Miscellaneous Settings" on page 61** for more information.

13. If you are planning to extend the WebFort functionality by the use of callouts and plug-ins, then register and configure these.

    See the *Arcot WebFort 6.0 Business Logic Extension Guide* for more information on how to write callouts and plug-ins. Also see **"Registering and Updating Plug-Ins"** for more information on how to register a plug-in, **"Configuring Callouts" on page 130** on how to configure a callout, and **"Configuring Plug-Ins" on page 133** on how to configure a plug-in.

With this your system is set for administration. You can now manage the system (**Chapter 3, "Managing WebFort Server Instances"**), administrators (**Chapter 6, "Managing Administrators"**), and users (**Chapter 7, "Managing Users"**).

Chapter 2

Getting Started

This chapter walks you through the steps for logging in to the Administration Console as **Master Administrator** and initializing the system, after you have successfully installed WebFort and have deployed the console. It covers the following tasks:

- **Accessing the Administration Console**
- **Configuring Administration Console Settings**
- **Changing Profile Information**

Accessing the Administration Console

The default Master Administrator (MA) account is used to log into the Administration Console for the first time. Use the following out-of-the-box credentials to log in to the console:

- User name: **masteradmin**
- Password: **master1234!**

To log in to the Administration Console:

1. Open a Web browser window.
2. Enter the URL to access Administration Console. The default Administration Console address is:

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

   In the preceding URL:

   - Replace *hostname* and *port* respectively with the host name or the IP address of the system where you have deployed the Administration Console and the port at which the console is listening.
   - If you change the default application context (`arcotadmin`), then you must replace it with the new value.

     NOTE: Arcot recommends that you bookmark this URL to access the Administration Console as a MA.

   The Master Administrator Login page appears, as shown in Figure 2-1.

Figure 2-1 Master Administrator Login Page

3. Enter **master1234!** in the **Password** field and click **Log In.**

   The landing page of the Administration Console appears, as shown in Figure 2-2.

Figure 2-2 Master Administrator: Successfully Logged In

Security Recommendations While Using the Administration Console

To protect WebFort from malicious attacks through the browser session, while using Administration Console, ensure that you:

- Do not share browser session with other applications.
- Do not open any other site while working with the Console.
- Enforce strict password restrictions for the Administration Console.
- Always log out after using the Administration Console.
- Close the browser window after the session is over.
- Assign proper roles to users according to the tasks they need to perform.

Logging Out of the Administration Console

To log out of the Administration Console, click the **Logout** link in the console Header area, which is located at the top-right corner.

Configuring Administration Console Settings

Before you configure the WebFort-specific settings, it is recommended that you configure the global configurations for the Administration Console, which include:

- UDS configurations
- Organization global configurations
- Cache refresh configurations
- Basic authentication policy configurations

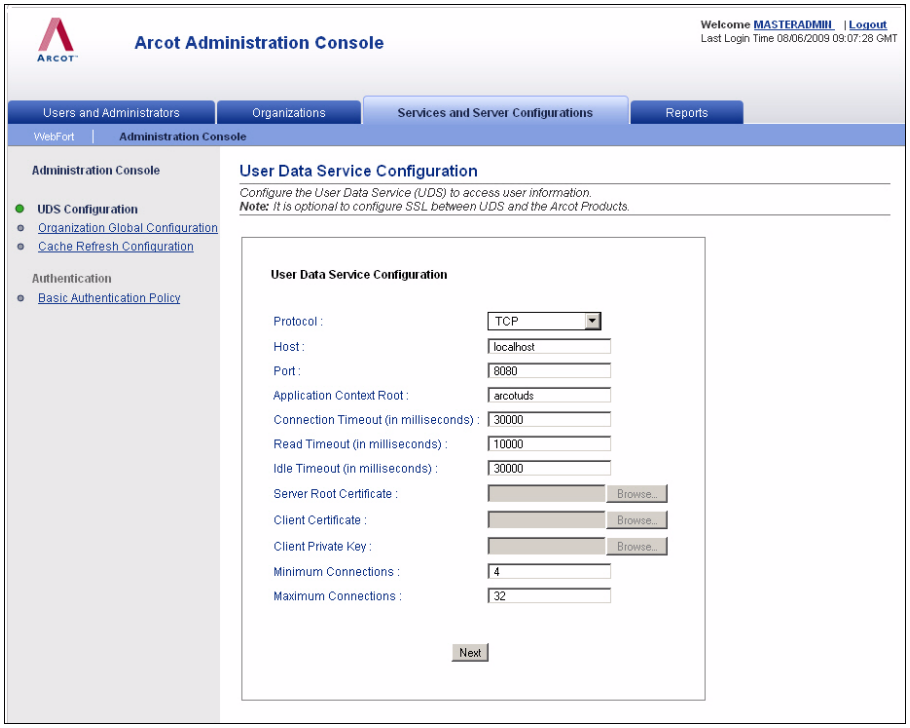
The following sub-sections walk you through the steps for configuring these global settings.

Specifying UDS Configurations

User Data Service (UDS) is an Administration Console module for enabling access to the third-party data repositories (such as, LDAP directory servers) deployed by your organization. UDS enables WebFort and the Administration Console seamless access to your existing data and leverage end-user information, without having to duplicate it in the standard Arcot SQL database tables.

Typically, you specify the UDS parameters while bootstrapping the system. (See section, "Bootstrapping the System" in *Arcot WebFort 6.0 Installation and Deployment Guide* for more information related to this.) However if you would like to update the UDS parameter settings, then use the User Data Service Configuration page (**Figure 2-3**) to do so.

Figure 2-3 User Data Service Configuration: Page 1



To update the UDS configuration:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the tab's sub-menu.
4. If the User Data Service Configuration page is not already displayed, then click the **UDS Configuration** link to display the page (Figure 2-3.)

5. Specify the parameters listed in Table 2-1 in the **User Data Service Configuration** section. Most of the parameters on this page are mandatory.

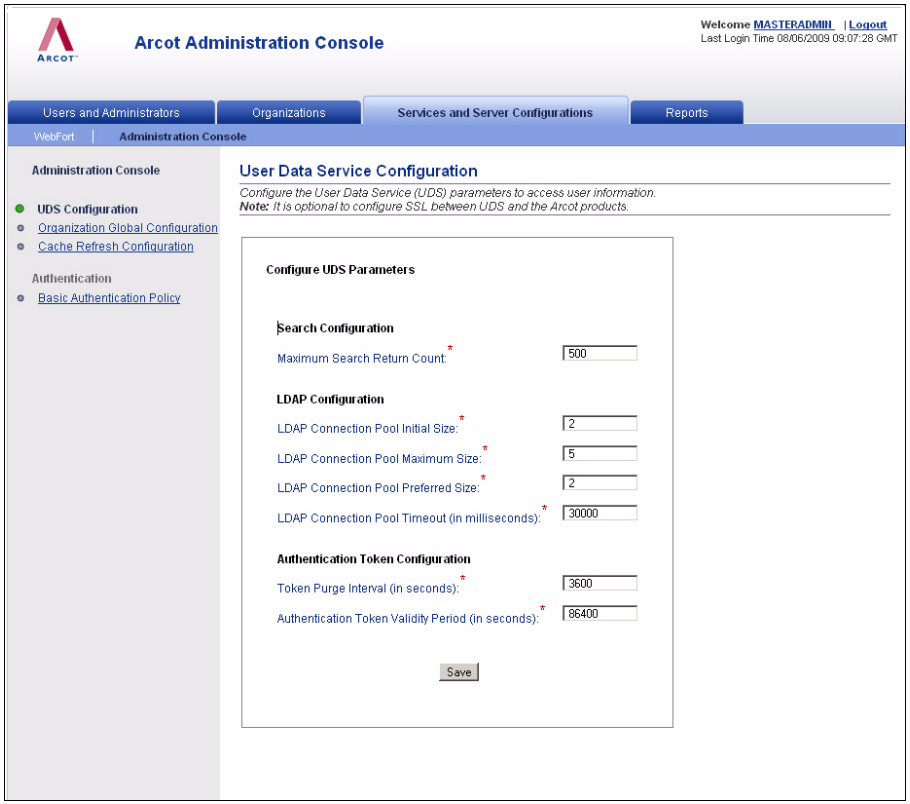
Table 2-1 UDS Configuration Parameters

Parameter	Default Value	Description
Protocol	TCP	The protocol to connect to the UDS service using the Administration Console. The available options are: • **TCP** • **One-Way SSL** • **Two-Way SSL**
Host	**localhost**	The IP address where the UDS is available.
Port	**8080**	The port at which the UDS service is available.
Application Context Root	**arcotuds**	The unique base URL at which UDS is accessible in an application server instance (of the multiple Administration Console applications that are currently running.)
Connection Timeout (in milliseconds)	**30000**	Maximum time in milliseconds before the UDS service is considered unreachable.
Read Timeout (in milliseconds)	**10000**	The maximum time in milliseconds to wait for a response from UDS.
Idle Timeout (in milliseconds)	**30000**	The time (in milliseconds) after which an idle connection not serving requests will be closed.
Server Root Certificate		The path to the CA certificate file of UDS server. The file must be in PEM format.
Client Root Certificate		The path to the CA certificate file of the Administration Console. The file must be in PEM format.
Client Private Key		The location of file that contains the CA's private key. The path can be an absolute path or relative to `ARCOT_HOME`.
Minimum Connections	4	The minimum number of connections that will be created between the Administration Console and the UDS server.
Maximum Connections	32	The maximum number of connections that can be created between the Administration Console and the UDS server.

6. Click **Next** to continue with the configuration.

   The next page, as shown in Figure 2-4, appears.

Figure 2-4 User Data Service Configuration: Page 2



7. Specify the parameters listed in Table 2-2 in the **User Data Service Configuration** section. Most of the parameters on this page are mandatory.

Table 2-2 UDS Search, LDAP, and Authentication Configuration Parameters

Parameter	Default Value	Description
Search Configuration		
Maximum Search Return Count	500	The maximum number of records that will be returned for all **Search** operations in the Administration Console.
LDAP Configuration		

Table 2-2 UDS Search, LDAP, and Authentication Configuration Parameters

Parameter	Default Value	Description
LDAP Connection Pool Initial Size	2	The initial number of connections between UDS and LDAP that will be created in the pool.
LDAP Connection Pool Maximum Size	5	The maximum number of connections allowed between UDS and LDAP.
LDAP Connection Pool Preferred Size	2	The preferred number of connections between UDS and LDAP.
LDAP Connection Pool Timeout (in milliseconds)	30000	The period for which UDS waits for a response from the LDAP, when a new connection is requested.
Authentication Token Configuration		
Token Purge Interval (in seconds)	3600	The maximum interval after which an authentication token is purged from the database, *after* the token expires.
Authentication Token Validity Period (in seconds)	86400	The maximum period (default is one day) after which an issued authentication token expires.

8. Click **Save** to save the changes you made.
9. Refresh *all* deployed WebFort Server instances. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Specifying Global Settings for Organizations

When you deploy the Administration Console, an organization is created by default along with the MA account. This out-of-the-box organization is referred to as *Default Organization* (`DEFAULTORG`).

As a single-organization system, the Default Organization is useful because you do not need to create any new organizations. You can configure the Default Organization settings, change its Display Name, and then continue to use it for administering purposes. In the case of a multi-organization system, however, you can either rename the Display Name of the Default Organization, configure its settings, and continue to use it as the default, or you can create a new organization and set it as the Default Organization.

NOTE: Typically when you create administrators or enroll users *without* specifying their organization, then they are created in the Default Organization.

The Organization Global Configuration page (Figure 2-5) enables you select the organization that will be used as the Default Organization and to control whether all future organizations in the system will inherit the settings of the Default Organization or can be edited individually to override these settings.

Figure 2-5 Organization Global Configuration Page

To specify the Default Organization and whether configurations can be set at the organization-level:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the tab's sub-menu.
4. In the tasks pane, click the **Organization Global Configuration** link to display the corresponding page (Figure 2-5.)
5. Under **Organization Configuration**, deselect the **Allow Configuration at Organization Level** option, if you do not want to set organization-specific configurations.

   By default this option is enabled.
6. Under **Default Organization**, select the organization that you want to set as the Default Organization from the **Organization Name** list.

7. Click **Save** to save the changes you made on this page.

   The "Successfully updated the global organization configuration" message appears.

Specifying Cache Refresh Settings

WebFort Administration Console caches certain data, which serves frequently-accessed console pages and UDS data faster. Typically organizations and roles are cached. The configuration for this can be updated by using the Cache Refresh Configuration page (Figure 2-6.)

Figure 2-6 Cache Refresh Configuration Page

To update the UDS and/or Administration Console cache settings:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the tab's sub-menu.
4. In the tasks pane, click the **Cache Refresh Configuration** link to display the corresponding page (Figure 2-6.)

5. Under **User Data Service** and/or **Administration Console** sections:
   a. Deselect or select the **Enable Automatic Refresh** option.
   b. Edit the **Cache Refresh Interval** value.

      The cache will be refreshed at the interval that you specify. For example, if you enter **60**, then it is automatically refreshed every hour. The default value is 30 minutes.
6. Click **Save** to save the changes that you have made.

Specifying Basic Authentication Policy Settings

Administrators logging into the Administration Console can be authenticated either by using the Basic Authentication (BA) Policy or WebFort User-Password mechanism. The mechanism that will be used is determined by the option that you selected while creating the organization:

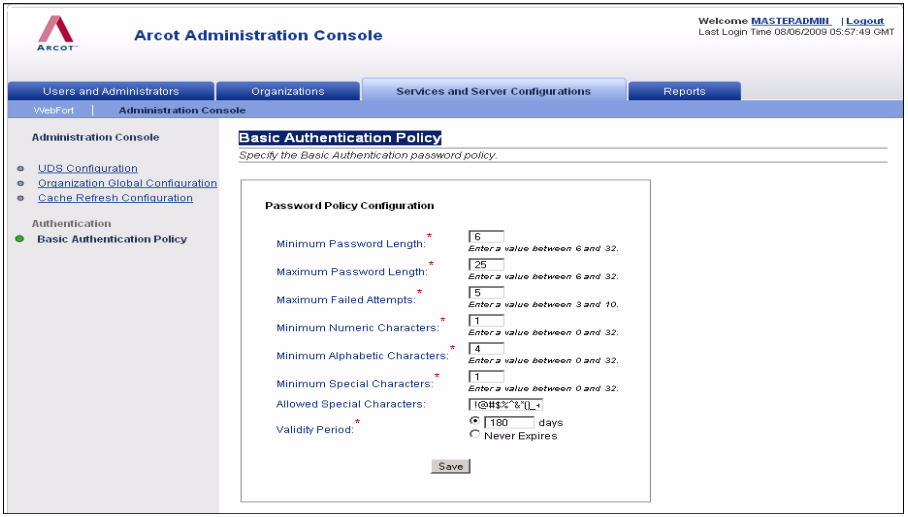
- If you selected the BA policy while creating an organization, then you can either use the default authentication policy, or set new policy as discussed in the **Specifying the Basic Authentication Password Policy** (for global level) or **Configuring Username-Password Authentication Policy** (for organization level).
- If you selected the WebFort User Password option, then you must first specify the connection information to the WebFort Server (as discussed in the **"Configuring WebFort Connectivity" on page 38** section).

Specifying the Basic Authentication Password Policy

As the name implies, *Basic Authentication* is the authentication method that involves administrators to log into the console by using a user ID and a password.

Use the Basic Authentication Policy page (**Figure 2-7**) to update information, such as password length, allowed number of special characters, and the number of failed login attempts allowed before locking the account.

Figure 2-7 Basic Authentication Policy Page



To specify the Basic Authentication policy:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the tab's sub-menu.
4. In the tasks pane, click the **Basic Authentication Policy** link to display the corresponding page (Figure 2-7.)
5. Specify the parameters listed in Table 2-3 in the **Password Policy Configuration** section. Most of the parameters on this page are mandatory.

Table 2-3 Basic Authentication Policy Parameters

Parameter	Default Value	Description
Minimum Password Length	6	The least number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Password Length	25	The most number of characters that the password can contain. You can set a value of between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.

Table 2-3 Basic Authentication Policy Parameters

Parameter	Default Value	Description
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password can contain. You can set a value between 0 and 32 characters.
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password can contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of **Allowed Special Characters** that the password can contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#$%^&*()_+	The list of special characters that the password can contain.
Validity Period	**180 days**	The maximum number of days for which a password is valid.

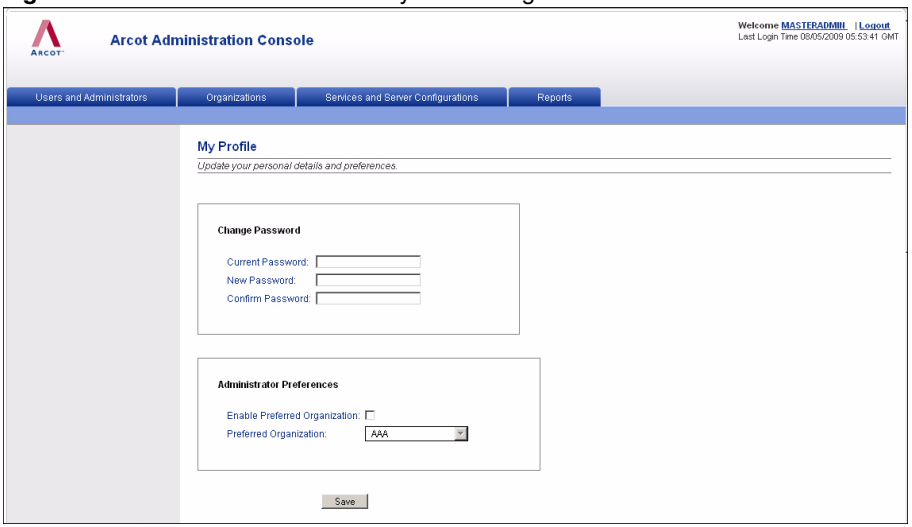
6. Click **Save** to save the changes you made on this page.

Changing Profile Information

Arcot strongly recommends that you change your Master Administrator password regularly to maintain high security, so that unauthorized persons do not gain access to the Administration Console using MA credentials.

Use the My Profile page, as shown in Figure 2-8, to change your current password and the organization that will be selected by default in the Organization field for all administrator-related tasks that you might perform in future.

Figure 2-8 Master Administrator: My Profile Page



To change your current password and/or to set your organization preference:

1. Click the **MASTERADMIN** link in the console header.

   The My Profile page, as shown in Figure 2-8, appears.

2. In the **Change Password** section, specify:

   - The **Current Password**.
   - The **New Password**.
   - The new password again in the **Confirm Password** field.

3. In the **Administrator Preferences** section, specify:

   - If you would like to **Enable Preferred Organization** option.

- The **Preferred Organization** that will be selected by default in the "Organization" field for all administrator-related tasks that you will perform from now on.

4. Click **Save**.

Chapter 3

Managing WebFort Server Instances

IMPORTANT: All the configurations and tasks discussed in this chapter can *only* be performed by **Master Administrator**.

Each system where WebFort Server is installed and is configured to listen at a specified port is referred to as an *instance*. The uniqueness of each server instance is defined by its *instance name*, which is a combination of host name and a unique number.

As a Master Administrator, you can manage each WebFort instance either locally or remotely. However, before you can manage a Server instance, you must configure the connectivity parameters to connect to the instance. (See section, "Configuring WebFort Connectivity", for information on how to do this.)

Only after you have configured one instance's connectivity parameters, can you manage the other WebFort Server instances. The tasks for managing an instance include:

- Configuring WebFort Connectivity
- Setting Up Server Instances
- Creating Trust Stores
- Configuring Communication Protocols
- Monitoring Instance Statistics
- Registering and Updating Plug-Ins
- Configuring Miscellaneous Settings
- Working with Custom Roles

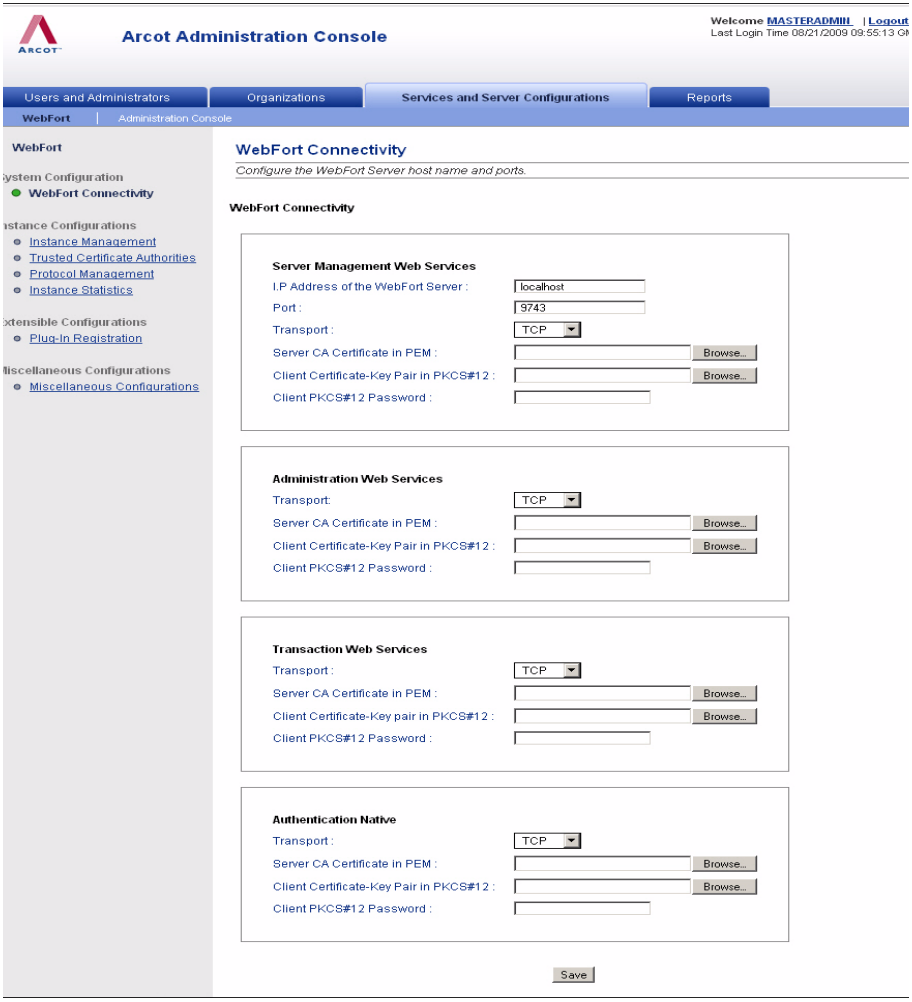
NOTE: Some of these tasks can be performed by using system tools, as discussed in Chapter 9, "Tools for System Administrators".

Configuring WebFort Connectivity

You can install multiple instances of WebFort Server. However, you can use the Administration Console (Figure 3-5) to configure the connection details to only one of these instances. This configured instance then polls other instances in the system for any information required for all instance management tasks.

NOTE: In most cases of single-system deployments, you do not need to configure the instance. The default values will work out of the box.

Figure 3-1 WebFort Connectivity Page



To specify the WebFort connectivity parameters:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Ensure that the **WebFort** option on the tab's sub-menu is selected.
4. If not already displayed, click **WebFort Connectivity** in the tasks pane to display the corresponding page (Figure 3-5.)
5. Use the information in Table 3-1 to edit the fields on the WebFort Connectivity page.

Table 3-1 Generic WebFort Connection Parameters

Field	Description
IP Address of the WebFort Server	Enter the host name of the system where you installed the required WebFort Server instance. **IMPORTANT:** You must specify the host name of the instance, and not the IP Address.
Port	Enter the port on which service for the protocol is exposed.
Transport	Specify the transport mode (**TCP** or **SSL**) for the corresponding component (Server Management Web Services, Administration Web Services, Transaction Web Services, and Authentication Native) to connect to the specified WebFort Server instance.
Server CA Certificate in PEM	Browse to and upload the PKCS#12 Store path that contains the server certificate.
Client Certificate-Key Pair in PKCS#12	Browse to and upload the PKCS#12 Store path that contains the client certificate and the private key.
Password for Client PKCS#12	Enter the password for the PKCS#12 Store.

6. Click **Save** to save the configurations that you have set.

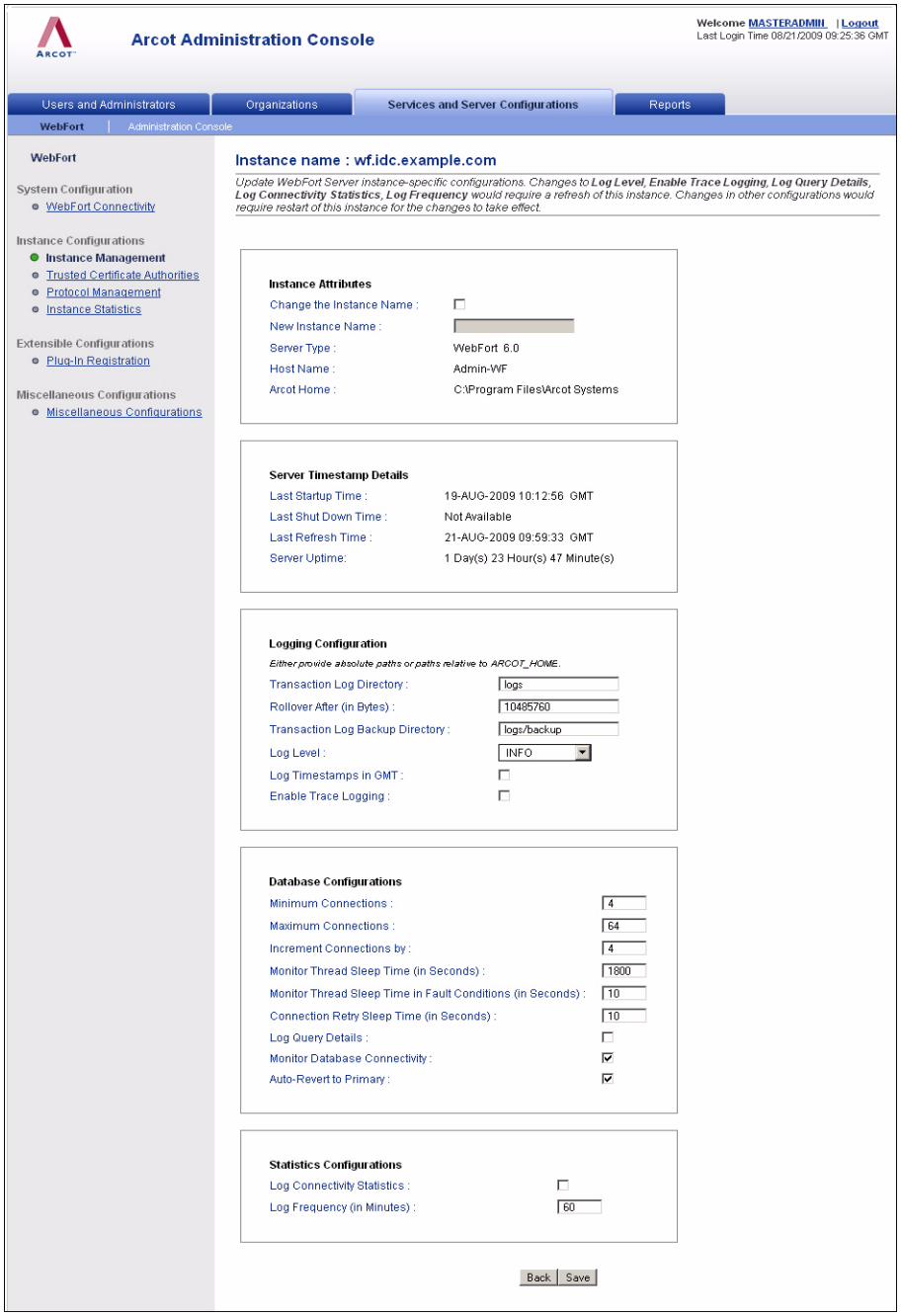
Setting Up Server Instances

The WebFort Instances page (Figure 3-2) lists *all* the configured WebFort Server instances that share the same WebFort database as the Administration Console. The server instance you configured earlier by using the WebFort Connectivity page polls the required information related to all other instances and passes it to the Administration Console, which in turn displays it on this page.

Figure 3-2 WebFort Instances Page

After you deploy an instance of WebFort Server, you might need to update the instance details. The WebFort Instances page enables you to refresh the server cache or shut down the specified instance. However to change instance-specific attributes, database connection parameters, log file details, or statistical data log parameters, you must click the instance name and then make the required changes on the instance's page. Figure 3-3 depicts one such instance-specific page.

Figure 3-3 Instance-Specific Page



Typical instance management operations include:

- Refreshing or Shutting Down Instances
- Changing the Instance Name
- Configuring Database Parameters
- Managing WebFort Server Logging Configurations
- Enabling Connectivity Statistics Logging
- Reading Instance Timestamp Details

NOTE: You can also perform most of the operations discussed in this section by using the `arwfclient` command-line tool. See "arwfclient" on page 212 for more information.

Refreshing or Shutting Down Instances

To refresh or shut down WebFort Server instances:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Under the **Instance Configurations** section, click the **Instance Management** link to display the WebFort Instances page (Figure 3-2.)
4. In the **Select** column, select the server instances whose status you want to change.
5. Do the required action:
   - Click **Refresh** to refresh the selected instances.
   - Click **Shut Down** to stop the selected instance.

Restarting a Server Instance

On Windows

To start a server instance on Windows:

1. Log in to the computer where the instance has stopped.
2. Click the **Start** button on the desktop.
3. Navigate to **Settings**, **Control Panel**, **Administrative Tools**, and **Services**.
4. Double-click **Arcot WebFort Authentication Service** from the listed services.
5. Click **Start** to start the service.

On UNIX-Based Platforms

To start a server instance on UNIX-based platforms:

1. Log in to the computer where the instance has stopped.
2. Navigate to the following directory:

   `<install_location>/arcot/bin/`

3. Run the following command:

   `./webfortserver start`

Changing the Instance Name

Based on the host on which the instance is running and the timestamp of the first startup, WebFort Server generates a unique name for each instance. This name is used in reports and is logged in audit logs. To easily identify an instance, Arcot recommends that you provide an appropriate name to each instance.

To change the instance name of a WebFort Server instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Instance Configurations** section, click the **Instance Management** link to display the WebFort Instances page (Figure 3-2.)
5. Click the required instance link in the **Instance Name** column.

   The Instance name: <*selected_instance*> page (Figure 3-3) appears.

6. In the **Instance Attributes** section, enable the **Change the Instance Name** option.
7. Enter the new name in the **New Instance Name** field.
8. Click **Save** to save the changes.
9. Refresh the WebFort Server instance for which you made the preceding changes. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Managing WebFort Server Logging Configurations

WebFort provides extensive logging capability and provides the following log files:

- WebFort log file (`arcotwebfort.log`)
- WebFort Startup log file (`arcotwebfortstartup.log`)
- WebFort Statistics log file (`arcotwebfortstats.log`)
- Administration Console log file (`arcotadmin.log`)
- UDS log file (`arcotuds.log`)

> **NOTE:** See Appendix A, "WebFort Logging" for detailed information on the location of these log files, the severity levels that you will see in these files, and the formats of these log files.

By using an instance-specific page (Figure 3-3), you can control logging configurations for WebFort log file and WebFort Statistics log file for the instance. To change the WebFort Server log configurations:

> **NOTE:** See "Enabling Connectivity Statistics Logging" on page 47 for information on how to control the configurations in the WebFort Statistics log file by using the Administration Console.

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Instance Configurations** section, click the **Instance Management** link to display the WebFort Instances page (Figure 3-2.)
5. Click the required instance link in the **Instance Name** column.

   The Instance name: <*selected_instance*> page (similar to Figure 3-3) appears.

6. Edit the fields in the **Logging Configurations** section, as required. Table 3-2 describes the fields of this section.

Table 3-2 Log Configuration Fields

Field	Description
Transaction Log Directory	Specify the directory where the log files have to be created. You can either enter the absolute path or the path relative to `ARCOT_HOME`.
Rollover After (in Bytes)	Enter the maximum size for the log file. After the log file reaches this size, the log content is moved to a backup file.
Transaction Log Backup Directory	Specify the directory where the backup files will be stored. You can either enter the absolute path or the path relative to `ARCOT_HOME`.
Log Level	Specify the level of detail of the information to be logged. The possible values are: • `FATAL` • `WARNING` • `INFO` • `DEBUG` See "Supported Severity Levels" on page 223 for more information on log levels.
Log the Timestamps in GMT	Enable this option if you want the WebFort Server instance to log all the messages in GMT time zone format.
Enable Trace Logging	Enable this option if you want the WebFort Server instance to generate logs for the functional flow for every transaction. This is useful while debugging any flow issues.

7. Click **Save** to save the changes.

8. Refresh the WebFort Server instance for which you made the preceding changes. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Configuring Database Parameters

WebFort uses *connection pooling*, which avoids the overhead of establishing a new database connection every time the server requires access to the database. By using the instance-specific page (Figure 3-3), you can configure these connection pooling parameters for the instance. The changes that you make in this section affect the Database Connectivity details displayed in the **Instance Statistics** page discussed in section, "Monitoring Instance Statistics" on page 54.

To change the database configuration parameters:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Instance Configurations** section, click the **Instance Management** link to display the WebFort Instances page (Figure 3-2.)
5. Click the required instance link in the **Instance Name** column.

   The Instance name: <*selected_instance*> page (similar to Figure 3-3) appears.
6. Edit the fields in the **Database Configurations** section, as required. Table 3-3 describes the fields of this section.

Table 3-3 Connection Pooling Parameters Between WebFort Server and Database

Field	Description
Minimum Connections	Enter the minimum number of connections that will be created between WebFort Server and the database when the server starts up.
Maximum Connections	Enter the maximum number of connections that can be created between the WebFort Server and the database. **NOTE**: There is a limit to how many connections a database allows and this limit overrides this parameter. See your database vendor documentation for more information.
Increment Connections By	Enter the number of connections that will be added to the existing connections at a time, when the need arises. **IMPORTANT:** The total number of connections *cannot* exceed the maximum number of connections.
Monitor Thread Sleep Time (in Seconds)	Enter the time for which the monitoring thread will sleep between successive heartbeat checks for all databases.

Table 3-3 Connection Pooling Parameters Between WebFort Server and Database

Field	Description
Monitor Thread Sleep Time in Fault Condition (in Seconds)	Enter the interval at which the database monitor thread will check the health of the connection pool in case of faulty database connections.
Connection Retry Sleep Time (in Seconds)	Enter the time WebFort Server will sleep between consecutive connection retry attempts to the database.
Log Query Details	Enable this option if you want to log the details for all database queries.
Monitor Database Connectivity	Enable checking of the pools proactively in the database monitor thread.
Auto-Revert to Primary	Enable this option if you want WebFort Server to switch from the backup database to the primary database when the primary database becomes available again after a failover condition.

7. Click **Save** to save the changes.
8. Refresh the WebFort Server instance for which you made the preceding changes. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Enabling Connectivity Statistics Logging

By using the options provided in the **Statistics Configurations** section, you can control the logging of connectivity statistics for the specified instance in the `arcotwebfortstats.log` file. The changes that you make in this section affect the details displayed in the **Instance Statistics** page discussed in section, "Monitoring Instance Statistics" on page 54.

To enable WebFort Server to log the statistical data:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Instance Configurations** section, click the **Instance Management** link to display the WebFort Instances page (Figure 3-2.)
5. Click the required instance link in the **Instance Name** column.

   The Instance name: <*selected_instance*> page (similar to Figure 3-3) appears.

6. In the **Statistics Configurations** section:
   - Select the **Log Connectivity Statistics** option for WebFort Server to log all the connectivity statistics.
   - In the **Log Frequency (in Minutes)** field, enter the duration after which the statistics must be logged. For example, if you enter 30, then the statistics will be logged after every 30 minutes.
7. Click **Save** to save the changes.
8. Refresh the WebFort Server instance for which you made the preceding changes. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Reading Instance Timestamp Details

The instance-specific page provides the timestamp details for each server instance in the **Server Timestamp Details** section. Table 3-4 explains these details.

Table 3-4 Server Timestamp Details

Field	Description
Last Startup Time	The timestamp when the server instance was restarted last time.
Last Shutdown Time	The timestamp when the server instance was shut down last time.
Last Refresh Time	The timestamp when the server instance was refreshed last time.
Server Uptime	The duration for which the server instance has been running.

Creating Trust Stores

You can create a trust store to authenticate a WebFort Server instance to its clients during SSL-based communications. A *trust store* is key file that contains the CA root certificates trusted by the WebFort clients that include Administration Console and Java SDKs.

Each of your WebFort Server instances can be configured to present different certificates by using different trust stores. You can use the Trusted Certificate Authorities page (Figure 3-4) to create trust stores and to add new root certificates to your trust stores.

Figure 3-4 Trusted Certificate Authorities Page

To create a trust store for the current server instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Instance Configurations** section, click the **Trusted Certificate Authorities** link to display the Trusted Certificate Authorities page (Figure 3-4.)
5. Enter the name for the trust store that you want to create in the **Name** field.
6. Click the corresponding **Browse** buttons to upload the root certificate of the trusted CAs. You can click **Add More** to display additional fields for uploading certificates.
7. Click **Save** when you finish uploading all required certificates.

Configuring Communication Protocols

By using the Protocol Configuration page (Figure 3-5), you can configure the protocols that Administration Console, SDKs, and Web Services uses to communicate with a WebFort Server instance for authentication and administration purposes. The ports on which the server instance listens for each protocol can also be configured by using this page.

Figure 3-5 Protocol Configuration Page

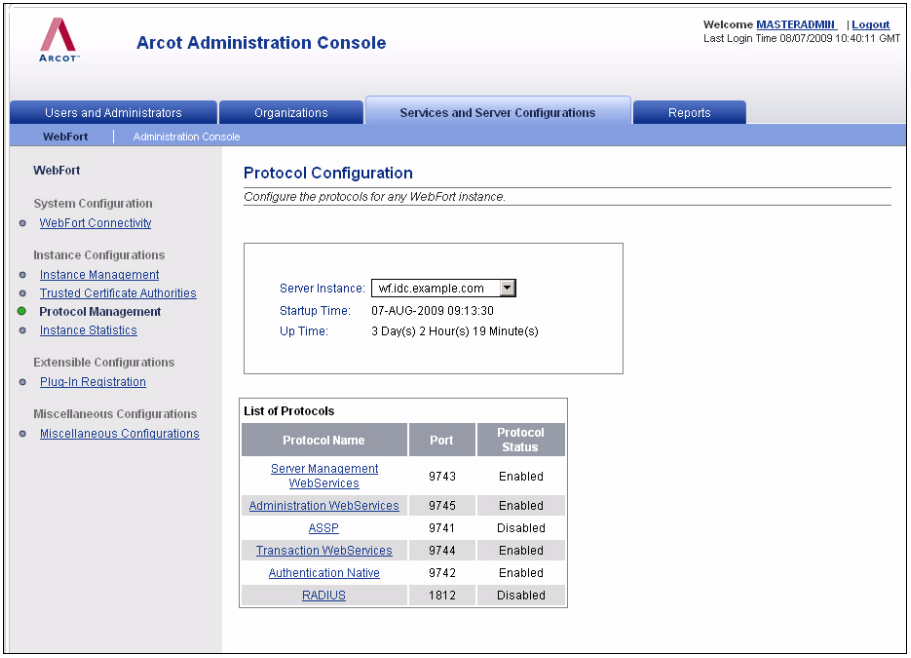


Table 3-5 explains the protocols you see on the Protocol Configuration page and lists their default port numbers.

Table 3-5 WebFort Protocols

Protocol	Default Port Number	Description
Server Management Web Services	9743	The Administration Console and the `arwfclient` tool communicate to the WebFort Server instance for server management activities by using this protocol.

Table 3-5 WebFort Protocols

Protocol	Default Port Number	Description
Administration Web Services	9745	This protocol is used to manage SAML, ASSP, profile, and policy configurations.
ASSP	9741	Adobe Signature Service Protocol (ASSP) is used with Adobe® Reader and Adobe® Acrobat® to authenticate users for server-side digital signing of the PDF documents.
Transaction Web Services	9744	This protocol is used by the Authentication and the Issuance Web services to connect to the WebFort Server instance.
Authentication Native	9742	This is a proprietary, binary WebFort protocol for authentication. This protocol is used by the Authentication Java SDK.
RADIUS	1812	This protocol is used to extend WebFort's capability to support the Remote Authentication Dial In User Service (RADIUS) protocol. **NOTE:** When configured to support RADIUS, WebFort Server acts as a RADIUS server.

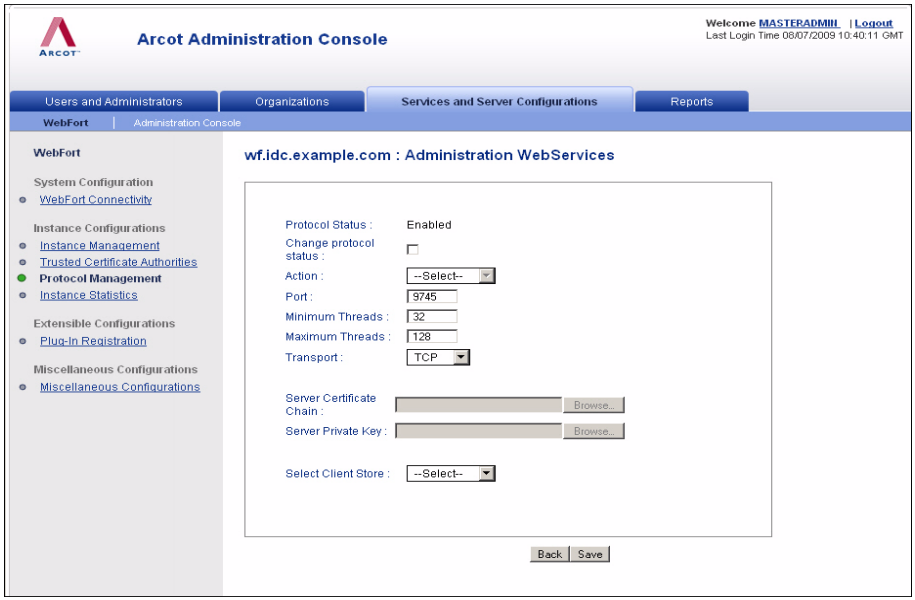
To configure WebFort network protocols:

> **NOTE:** The changes that you make in this page and the subsequent protocol-specific page affect the Server Protocols details displayed in the **Instance Statistics** page discussed in section, "Monitoring Instance Statistics" on page 54.

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Instance Configurations** section, click the **Protocol Management** link to display the Protocol Configuration page (Figure 3-5.)
5. Select the **Server Instance** for which you want to configure the protocols.
6. In the **List of Protocols** section, click the protocol you want to configure.

   The page to configure the specific protocol appears. (For example, Figure 3-6 shows the protocol configuration page for Administration Web Services.)

Figure 3-6 Protocol Configuration Page: Administration Web Services



7. Edit the fields on the page, as required. Table 3-6 explains these fields.

Table 3-6 Fields for Configuring WebFort Protocols

Field	Description
Protocol Status	Indicates whether the protocol is **Enabled** or **Disabled**.
Change the Protocol Status **Action**	Select the **Change the Protocol Status** option to enable the **Action** list and then select the new status from the **Action** drop-down list. **NOTE:** The Server Management protocol cannot be disabled. Therefore, you will not see these options for this protocol.
Port	Enter the port number where the protocol service will be available.
Minimum Threads	Specify the minimum number of threads to be maintained between the client and the WebFort Server.
Maximum Threads	Specify the maximum number of threads that can exist between the client and the WebFort Server.

Table 3-6 Fields for Configuring WebFort Protocols

Field	Description
Transport	Specify the mode for data transfer. **NOTE:** If you are configuring RADIUS, then the value for this field is User Datagram Protocol (UDP). This is the standard transport protocol supported by RADIUS. The supported values are: • **SSL**: Secure Sockets Layer (SSL) uses PKI to encrypt and decrypt data under transmission. • **TCP**: Transmission Control Protocol (TCP) mode is supported for all WebFort protocols, other than the WebFort RADIUS protocol.
Server Certificate Chain	Upload the Certificate Chain by using the respective **Browse** button in the corresponding field. This server certificate chain is used by the SSL transport security mode.
Server Private Key	Upload the Certificate Chain by using the respective **Browse** button in the corresponding field. This server private key is used by the TLS transport security mode.
Select Client Store	Select the trust store that contains the root certificates of the trusted CAs. See "Creating Trust Stores" on page 49 for more information on how to configure a trust store.

8. Click **Save** after you complete the configurations on the page.

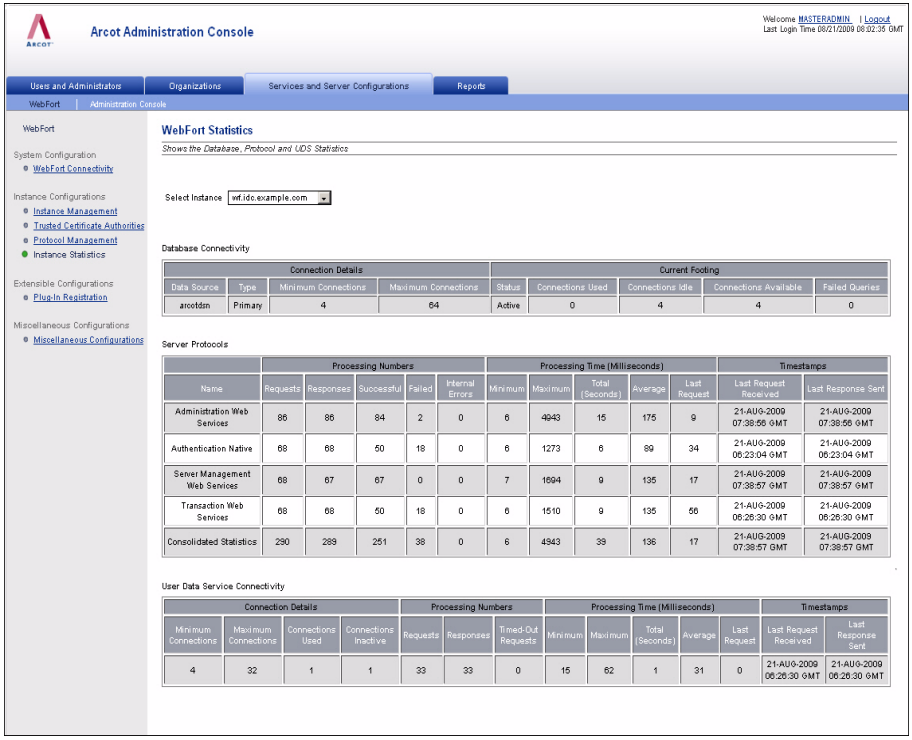
   NOTE: You must configure each protocol individually.

9. Refresh the WebFort Server instance for which you made the preceding changes. See "Restarting a Server Instance" on page 42 for instructions on how to do this.

Monitoring Instance Statistics

The WebFort Statistics page (Figure 3-7) of the Administration Console enables you to monitor the connectivity status and details for WebFort database, UDS, and the configured WebFort protocols for each server instance. By using these statistics, you can tweak your various configuration parameters (as discussed in the preceding sections) for better performance.

Figure 3-7 WebFort Statistics Page



To view the statistical details for an instance:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Instance Configurations** section, click the **Instance Statistics** link to display the WebFort Statistics page (Figure 3-7.)

5. Select the instance whose details you want to monitor from the **Select Instance** list.

   You will see the instance details, which are categorized as:

   - Database Connectivity
   - Server Protocols
   - User Data Service Connectivity

Database Connectivity

Table 3-7 lists the database connection information.

Table 3-7 Database Connectivity Details for an Instance

Field	Description
Connection Details	
Data Source	The data source name (DSN) configured for the selected WebFort Server instance.
Type	Indicates whether the database that the server instance is using is primary or backup.
Minimum Connections	Indicates the minimum number of database connections that are configured for the WebFort Server instance.
Maximum Connections	Indicates the maximum number of database connections that are configured for the WebFort Server instance.
Current Footing	
Status	Indicates whether the pool is active or not.
Connections Used	Indicates the number of database connections that are currently used by the server instance.
Connections Idle	Indicates the number of database connections that are unused by the server instance.
Connections Available	Indicates the total number of database connections that are currently available in the connection pool.
Failed Queries	Indicates the number of queries that failed to return records that matched the specified criteria.

Server Protocols

Table 3-8 lists the request, response, and the processing details for each configured WebFort protocol.

Table 3-8 Protocol Information for an Instance

Field	Description
Processing Numbers	
Name	The name of the configured protocol.
Requests	The number of requests that are handled by the server instance.
Responses	The number of responses sent by the server instance.
Successful	The number of requests that were successfully processed by the server instance.
Failed	The number of requests that the server instance failed to process.
Internal Errors	The number of errors that occurred because of some internal error. Internal errors can happen because of several reasons, for example, database is unreachable, token is not generated, transaction ID is not generated, or the module is not loaded properly.
Processing Time (Milliseconds)	
Minimum	The minimum time taken by the server instance to process a request.
Maximum	The maximum time taken by the server instance to process a request.
Total (Seconds)	The total time taken by the server instance to process requests.
Average	The average time taken by the server instance to process requests.
Last Request	The time taken by the server instance to process the latest request.
Timestamps	
Last Request Received	The timestamp when the last request was received by the server instance.
Last Response Sent	The timestamp when the last response was sent by the server instance.

User Data Service Connectivity

Table 3-9 lists the details for the connections between the WebFort Server instance and the UDS.

Table 3-9 UDS Connectivity Details for an Instance

Field	Description
Connection Details	

Table 3-9 UDS Connectivity Details for an Instance

Field	Description
Minimum Connections	The minimum number of connections that must exist between the server instance and the UDS.
Maximum Connections	The maximum number of connections that can exist between the server instance and the UDS.
Connections Used	The number of connections that are established between the server instance and the UDS.
Connections Inactive	The number of idle connections between the server instance and the UDS.
Processing Numbers	
Requests	The total number of requests from the server instance to the UDS.
Responses	The total number of responses received by the server instance from the UDS.
Timed-Out Requests	The total number of requests that timed out before a response from UDS was received.
Processing Time (Milliseconds)	
Minimum	The minimum time taken by UDS to process a request sent by the server instance.
Maximum	The maximum time taken by the UDS to process a request from the server instance.
Total (Seconds)	The total time taken by the UDS to process all requests from server instance.
Average	The average time taken by the UDS to process all server instance requests.
Last Request	The time required to process the latest request received by the UDS.
Timestamps	
Last Request Received	The timestamp when the latest request was received by the UDS.
Last Response Sent	The timestamp when the last response was sent by the UDS.

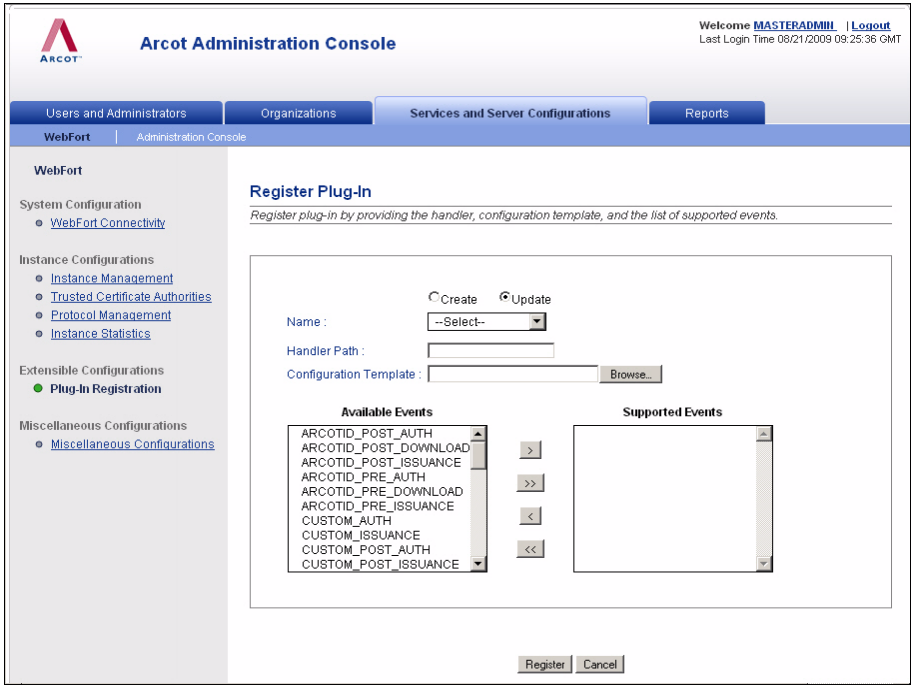
Registering and Updating Plug-Ins

Plug-ins are custom server-side component, written in C or C++, that enables you to extend the functionality of WebFort Server. Plug-ins are loaded by WebFort Server process and are implemented as a custom event handler library.

> **NOTE:** See *Arcot WebFort 6.0 Business Logic Extension Guide* for information on how to write plug-ins.

After you write a plug-in, you must register it to a published set of events, so that the plug-in is invoked when the specified event occurs. You use the Register Plug-In page (Figure 3-8) to do so. You can also use this page to update an existing plug-in. Plug-in-related configurations that you set by using this screen are available to *all* organizations configured in the system, and *cannot* be restricted to a specific instance.

Figure 3-8 Register Plug-In Page



Registering Plug-Ins

To register a new plug-in with the system:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Extensible Configurations** section, click the **Plug-In Registration** link to display the Register Plug-In page (**Figure 3-8**.)
5. Select the **Create** option.
6. Specify the plug-in **Name**.
7. Specify the **Handler Path** to the library file of the plug-in. The Handler file contains the plug-in library that you wrote and that must be exposed to WebFort.

   For *Unix* platforms, if this file is available in the path specified by `LD_LIBRARY_PATH`, then you do not need to provide the absolute path to the Handler file. You can simply specify the name of the file without the extension (`.dll` or `.so`). However, if this Handler file is not available in the path specified by the `LD_LIBRARY_PATH` variable, then you must specify the absolute path to it.
8. Click **Browse** against **Configuration Template** and navigate to the location of the plug-in configuration template file.

   The configuration template file defines the type of data that is used to configure the plug-in and the default values for the parameters used by the plug-in. This information is also used to render the Administration Console screen for plug-in configuration.

   NOTE: Arcot provides a sample plug-in template file, refer to *Arcot WebFort 6.0 Business Logic Extension Guide* for more information on this.
9. Select the events that you want to associate with the plug-in from the **Available Events** list, and click the > button to add these events to the **Supported Events** list.

   NOTE: The **Available Events** list displays all the events that are exposed by WebFort, while the **Supported Events** list displays the events that will be available for the new plug-in that you are registering.
10. Click **Register** to register the plug-in with *all* instances of WebFort.
11. Restart *all* deployed WebFort Server instances. See **"Restarting a Server Instance" on page 42** for instructions on how to do this.

Updating Plug-In Configurations

To update an existing plug-in configuration:

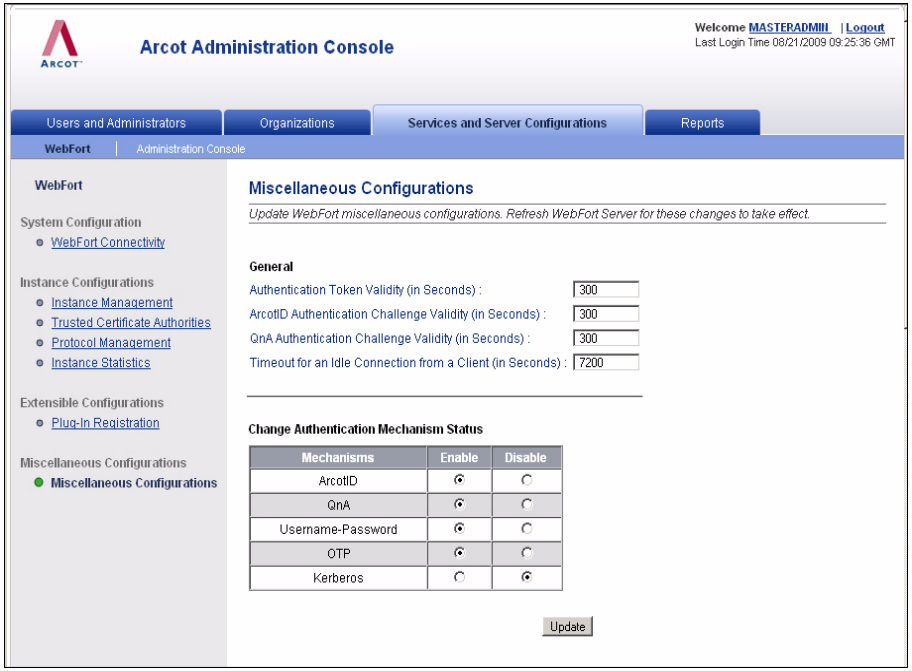
1. Ensure that you are logged in as the MA.
2. Navigate to the Register Plug-In page (Figure 3-8.)
3. Select the **Update** option.
4. Select the required plug-in from the **Name** list.
5. Update the **Handler Path** and/or the **Configuration Template** configuration for the plug-in.
6. Update the events associated with the plug-in.
7. Click **Register** to update the changes.
8. Restart *all* deployed WebFort Server instances. See "Restarting a Server Instance" on page 42 for instructions on how to do this.

Configuring Miscellaneous Settings

The Miscellaneous Configurations page (Figure 3-9) enables you to change the following settings (applicable to all instances of WebFort Server) that you might need to update:

- Validity of authentication tokens
- Validity of ArcotID authentication challenges
- Validity of QnA challenges
- Timeouts for idle client connections
- Enabling the auditing of Instance statistics and Thread statistics
- Enable or disable an authentication mechanism (such as, ArcotID, Questions and Answers (QnA), User-Password, One-Time Password (OTP), and Kerberos)

Figure 3-9 Miscellaneous Configurations Page



To change the miscellaneous configurations:

1. Ensure that you are logged in as the MA.

2. Activate the **Services and Server Configurations** tab in the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Miscellaneous Configurations** section, click the **Miscellaneous Configurations** link to display the corresponding page (Figure 3-9.)
5. Edit the fields on the page, as required. Table 3-10 describes the fields of this page.

Table 3-10 Miscellaneous WebFort Settings

Field	Default Value	Description
General		
Authentication Token Validity (in Seconds)	300	Specify the interval for which an authentication token issued by WebFort will be valid.
ArcotID Authentication Challenge Validity (in Seconds)	300	Specify the interval for which an ArcotID authentication challenge issued by WebFort will be valid.
QnA Authentication Challenge Validity (in Seconds)	300	Specify the interval for which an QnA authentication challenge issued by WebFort will be valid.
Timeout for an Idle Connection from a Client (in Seconds)	7200	Specify the interval after which an idle client connection will be closed.
Change Authentication Mechanism Status		
ArcotID	Enabled	Specify whether you want WebFort to provide the ArcotID authentication capability.
QnA	Enabled	Specify whether you want WebFort to provide QnA authentication.
Username-Password	Enabled	Specify whether you want WebFort to provide the basic username-password authentication functionality.
OTP	Enabled	Specify whether you want WebFort to support OTP-based authentication.
Kerberos	Disabled	Specify whether you want WebFort to support Kerberos-based authentication.

6. Click **Update** to save the changes.
7. If you have changed the **General** configurations, then refresh *all* deployed WebFort Server instances. However, you must restart the WebFort Server if you change the authentication mechanism status. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Working with Custom Roles

See "Custom Roles" on page 14 for more conceptual information. This section guides you through the steps for:

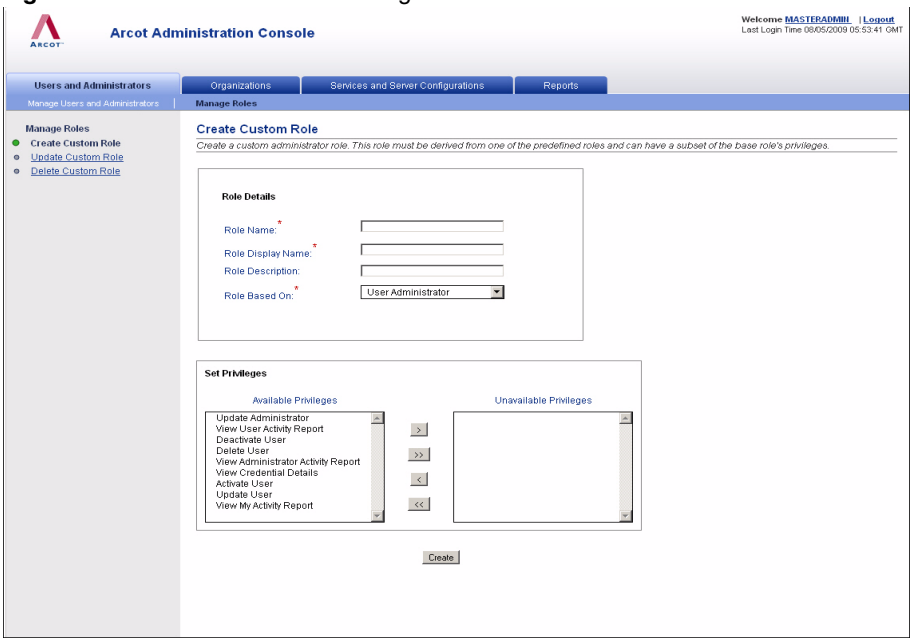
- Creating a Custom Role
- Updating a Custom Role Information
- Deleting a Custom Role

Creating a Custom Role

To create a custom role:

1. Activate the **Users and Administrators** tab.
2. From the sub-menu, click the **Manage Roles** link to display the Create Custom Role page (Figure 3-10.)

Figure 3-10 Create Custom Role Page



3. In the **Role Details** section, specify the following information:
   - **Role Name:** The unique name to identify the new role. This name is used internally by WebFort by authenticating and authorizing this new role.
   - **Role Display Name:** The descriptive name of the role that appears on all other Administration Console pages and reports.
   - **Role Description:** The useful information related to the role for later reference.
   - **Role Based On:** The pre-existing role from which this custom role should be derived.
4. In the **Set Privileges** section:
   a. In the **Available Privileges** list, select all the privileges that you need to *disable* for the new role.

      This list displays all the privileges available to the administrative role that you selected in the **Role Based On** field.

      NOTE: You can hold the **Ctrl** key to select more than one privileges at a time.

   b. Click the > button to move the selected privileges to the **Unavailable Privileges** list.
5. Click **Create** to create the custom role.

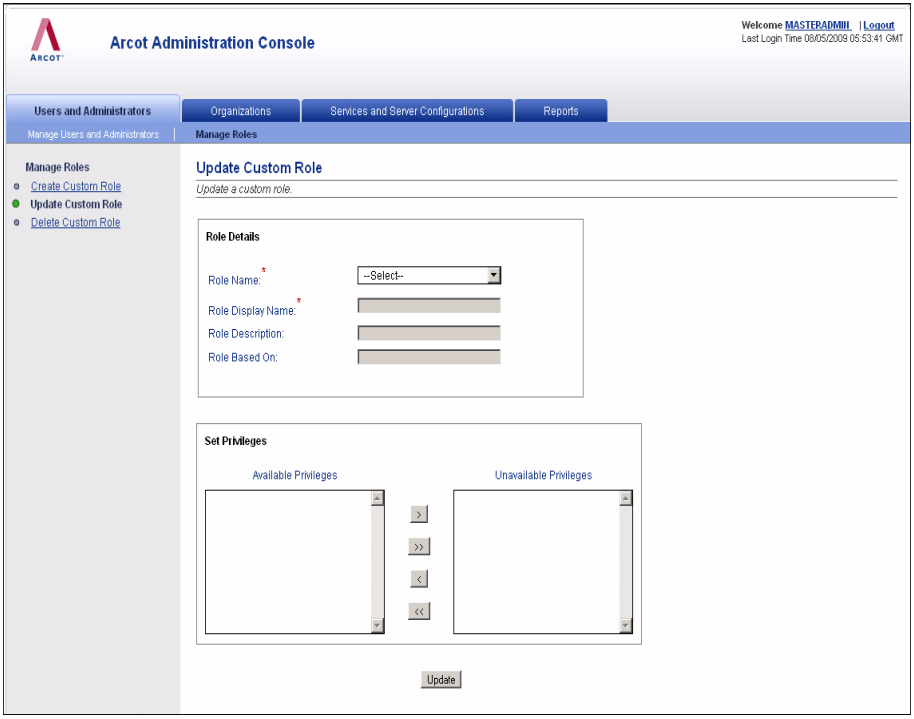
Updating a Custom Role Information

To update an existing custom role definition:

1. Activate the **Users and Administrators** tab.
2. From the sub-menu, click the **Manage Roles** link.
3. From the Tasks menu, click the **Update Custom Role** link.

   The Update Custom Role page, as shown in Figure 3-11, appears.

Figure 3-11 Update Custom Role Page



4. Select the **Role Name** that you want to update.
5. Make the required changes to one or all of the fields in the **Role Details** section.
6. In the **Set Privileges** section:
   a. In the **Available Privileges** list, select all the privileges that you need to *disable* for the new role.

      This list displays all the privileges available to the administrative role that you selected in the **Role Based On** field.

      or

   b. In the **Unavailable Privileges** list, select the privileges that you want to *enable* for the new role.

      This list displays all the privileges that are not available to the administrative role that you selected in the **Role Based On** field.

      NOTE: You can hold the **Ctrl** key to select more than one privileges at a time.

c. Click the > button to move the selected privileges to the **Unavailable Privileges** list.

7. Click **Update** to update the Custom role definition.

Deleting a Custom Role

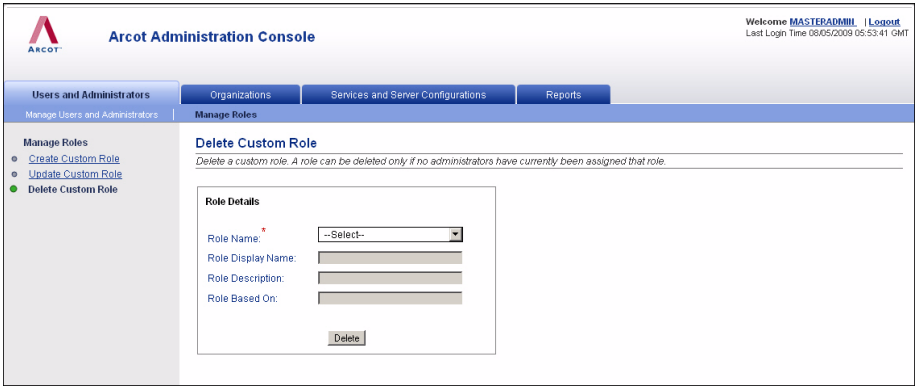
IMPORTANT: You *cannot* delete a custom role that is currently assigned to an administrator. If you need to delete such a role, then you must first change the role of all administrators who are assigned this role by using the Update Administrator page.

To delete an existing custom role:

1. Activate the **Users and Administrators** tab.
2. From the sub-menu, click the **Manage Roles** link.
3. From the Tasks menu, click the **Delete Custom Role** link.

   The Delete Custom Role page, as shown in Figure 3-12, appears.

Figure 3-12 Delete Custom Role Page



4. In the **Role Details** section, select the custom role that you need to delete from the **Role Name** list.
5. Click **Delete** to delete the selected custom role.

Chapter 4

Managing Global WebFort Configurations

IMPORTANT: All the configurations and tasks discussed in this chapter can *only* be performed by **Global Administrators**.

You can manage WebFort configurations at two levels:

- Global, applicable to all organizations
- Organization-level, applicable to individual organization

When you set global configurations at the system level, all organizations in the system can inherit them. You can also override these global settings at the organization level, and they apply only to the specific organization where they were set. The changes you make to the configuration globally or at organization-level are *not* applied automatically. You need to refresh all server instances to apply these configuration changes.

Managing global configurations is a key part of WebFort management and optimization, and a key responsibility of Global Administrators. This chapter discusses global configurations that GAs can set for *all* current and future organizations in the system. These configurations include:

- Configuring ArcotID Settings
- Configuring QnA Settings
- Configuring Username-Password Settings
- Configuring OTP Settings
- Assigning Default Configurations

NOTE: These configurations are applicable for all organizations that are in the purview of the GA setting them. If you want to configure individual organizations, then you must log in as the Global Administrator (GA) or as Organization Administrator (OA) of the target organization to do so. Refer to **"Managing Organization-Specific Configurations" on page 118** for more information.

In addition to these tasks, GAs can also configure the Basic Authentication Policy. See section, **"Specifying the Basic Authentication Password Policy" on page 31** for information on how to do this.

Understanding WebFort Profiles and Policies

Each end user in WebFort is associated with at least one credential (such as ArcotID, QnA, Username-Password, or OTP) that they must use to log in to the system. Every time they log in using their credential, their authentication is controlled by a corresponding policy.

Credential Profiles

With a large number of end users enrolled with WebFort, you might find that the same credential template can be applied as-is to many users. In such cases, WebFort provides you the flexibility to create common ready-to-use credential configurations, known as *credential profiles* that can be shared among multiple organizations and, thereby, applied to multiple users. As a result, credential profiles simplify the management of credential issuance.

Credential Profiles specify issuance configuration properties, and credential attributes, such as validity period, key strengths, and details related to password strength.

WebFort is shipped with a default profile for each credential. You can also create multiple profiles, each with a unique name, for all credential types. You can then assign one or more profiles to an organization, one of which can also be set as default. WebFort makes use of these configured profiles at the time of issuing credentials to users.

Authentication Policies

WebFort supports multiple authentication mechanisms. Every time an end user attempts authentication against WebFort, the authentication process is controlled by a set of rules (or checks) referred to as *authentication policies*. For example, these rules can be configured to track the number of failed authentication attempts allowed before credential lockout and user status before authentication.

WebFort can generate following type of tokens:

- **Native Tokens:** Arcot-proprietary tokens, can be used multiple times before they expire.
- **One-Time Tokens:** Can be used *only* one time before they expire.
- **SAML Tokens:** Can be interpreted by any other authentication system. WebFort supports 1.1 and 2.0 versions of Secure Assertion Markup Language (SAML.)

As in case of credential profiles, WebFort is also shipped with a default policy for each token type. You can also create multiple policies, each with a unique name, for all authentication mechanisms. You can then assign one or more policies to an organization.

Logging in as a Global Administrator

The first GA account *must* be created by MA. To log in as a GA and proceed with further configurations, you must obtain the account details from MA. The GA can log in either by **Using WebFort Username-Password** or by **Using Basic Username-Password**.

Using WebFort Username-Password

If the MA created your account with WebFort Username-Password credentials, then ensure you have been communicated with your ID and the activation code (one-time password), which will be used as your password when you log in to your account for the first time. If for some reason you lose this activation code, then you must contact your administrator to regenerate it and send it to you again.

To log in to the Administration Console as a GA by using WebFort Username-Password credentials:

1. Open a Web browser window.
2. Enter the URL to access Administration Console. The default Administration Console URL is:

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

   Replace *hostname* and *port* in the preceding URL respectively with the host name or the IP address of the system where you have deployed the Administration Console and the port at which the console is listening.

   NOTE: Arcot recommends that you bookmark this URL to access the Administration Console. Any GA, OA, or UA can use this URL to log in to the Administration Console by using their WebFort Username-Password credentials.

   The Administrator Login page appears, as shown in **Figure 4-1**.

Figure 4-1 Administrator Login: Page 1

3. Enter the **Organization Name** that you want to log in to.

   IMPORTANT: *Do not* enter the **Display Name** of the organization. You must enter the unique ID of the organization (as defined by the Organization Name.) For example, if you want to log into the Default Organization, whose Display Name is Arcot Systems, then you must enter **defaultorg**, which is the (default) unique ID of this organization. You must *not* specify **Arcot Systems** here.

4. Click **Log In**.

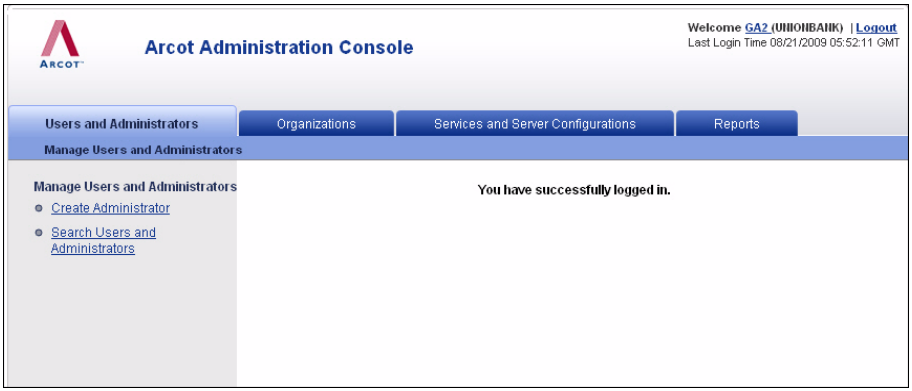
   The Login page shown in Figure 4-2 appears.

Figure 4-2 Administrator Login: Page 2

5. Specify the user ID in **User Name** field, enter the corresponding activation code that you were communicated in the **Password** field, and click **Log In.**

   The landing page of the Administration Console appears, as shown in Figure 4-3.

Figure 4-3 Master Administrator: Successfully Logged In



In Case You Forgot Your Password

In case you forgot your activation code or your WebFort Password credential, then follow these steps to regenerate it:

1. In a browser window, enter the URL to access Administration Console. The default Administration Console URL is:

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

   The Administrator Login page appears, as shown in Figure 4-1.

2. Enter the **Organization Name** that you want to log in to, and clock **Log In**.

   The Login page shown in Figure 4-2 appears.

3. Click the **Forgot Password?** link.

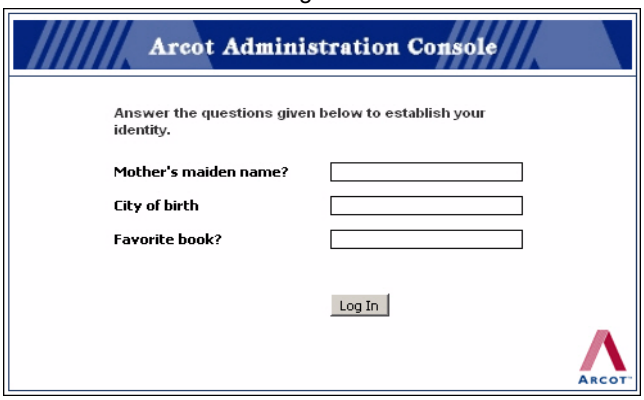
   The Forgot Your Password? page, as shown in Figure 4-4 appears.

Figure 4-4 Forgot Your Password? Page

4. In the **User Name** field, specify your user ID, and click **Log In**.

   The page (Figure 4-5) that displays the questions that you set in your Profile Information (See "Changing Profile Information for Administrator Accounts" on page 151 for instructions on how to set this QnA information) appears.

Figure 4-5 Questions and Answers Page



5. Specify the corresponding answers to the questions that you see and click **Log In**.

   The Reset Password page (Figure 4-6) appears.

Figure 4-6 Reset Password Page

6. Specify the new password in **New Password** and **Confirm Password** fields.
7. Click **Log In**. The Login page (Figure 4-7) appears.
8. Specify the **Password** and click **Log In** to log into the Administration Console.

Using Basic Username-Password

To log in to the Administration Console as a GA by using basic Username-Password credentials:

1. Open a Web browser window.
2. Enter the URL to access Administration Console. The default Administration Console URL is:

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

   Replace *hostname* and *port* in the preceding URL respectively with the host name or the IP address of the system where you have deployed the Administration Console and the port at which the console is listening.

   NOTE: Arcot recommends that you bookmark this URL to access the Administration Console. Any GA, OA, or UA can use this URL to log in to the Administration Console by using their credentials.

   The Administrator Login page appears, as shown in Figure 4-1.

3. Enter the **Organization Name** that you want to log in to.

   IMPORTANT: *Do not* enter the **Display Name** of the organization. You must enter the unique ID of the organization (as defined by the Organization Name.) For example, if you want to log into the Default Organization, whose Display Name is Arcot Systems, then you must enter **defaultorg**, which is the (default) unique ID of this organization. You must *not* specify **Arcot Systems** here.

4. Click **Log In**.

   The Login page shown in Figure 4-7 appears.

   NOTE: This page will *not* show the **Forgot Password?** link that is available when you log in by using WebFort Username-Password credentials.

Figure 4-7 Administrator Login: Page 2

5. Specify the user ID in **User Name** field, enter the corresponding password in the **Password** field, and click **Log In.**

   The landing page of the Administration Console similar to Figure 4-3 appears.

Logging Out of the Administration Console

To log out of the Administration Console, click the **Logout** link in the console Header area, which is located at the top-right corner.

Security Recommendations While Using the Administration Console

To protect WebFort from malicious attacks through the browser session, while using Administration Console, ensure that you:

- Do not share browser session with other applications.
- Do not open any other site while working with the Console.
- Enforce strict password restrictions for the Administration Console.
- Always log out after using the Administration Console.
- Close the browser window after the session is over.
- Assign proper roles to users according to the tasks they need to perform.

Configuring ArcotID Settings

This section walks you through:

- Configuring ArcotID Credential Profile
- Configuring ArcotID Authentication Policy

Configuring ArcotID Credential Profile

An ArcotID profile can be used to define the following attributes related to an ArcotID credential:

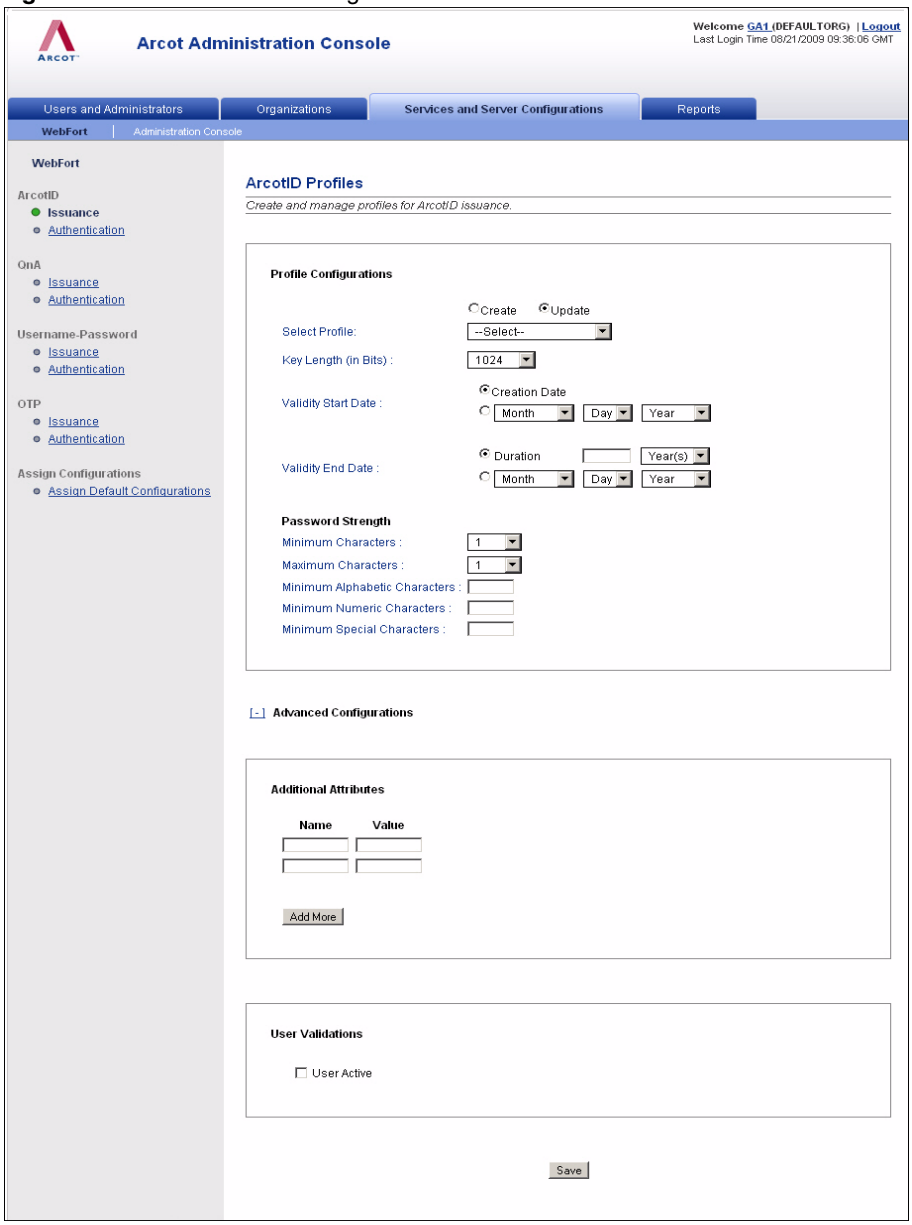
- **Key strength**: The size (in bits) of the key to be used in ArcotID's Cryptographic Camouflage algorithm.
- **Validity period**: The period for which an ArcotID credential is valid.
- **Password strength**: The effectiveness of password, which is determined by a combination of the length of the password and number of alphabets, numerals, and special characters in it.

By configuring an ArcotID profile and assigning it to one or more organizations, you can control the characteristics of ArcotIDs that are issued to users of those organizations. Use the ArcotID Profiles page (Figure 4-8) for creating an ArcotID credential profile.

To create an ArcotID profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **ArcotID** section, click the **Issuance** link to display the ArcotID Profiles page (Figure 4-8.)

Figure 4-8 ArcotID Profiles Page



5. Edit the fields in the **Profile Configurations** section, as required. Table 4-1 describes the fields of this section.

Table 4-1 ArcotID Profile Configuration Fields

Field	Description
Profile Configurations	
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Profile** list.
Key Length (in Bits)	Specify the size of the key (in bits) to be used for encryption. The default value is `1024` bits. **IMPORTANT:** This value is critical in determining the ArcotID strength. Arcot suggests you to choose a higher value to increase the ArcotID strength.
Validity Start Date	Set the date from which the issued ArcotID credential will be valid. The validity can start from either the date when the ArcotID is created or you can specify a specific date.
Validity End Date	Set the date when the ArcotID will expire. You can either specify the duration for the credential's expiration or you can specify the specific date.
Password Strength	
Minimum Characters	Specify the least number of characters that the password can contain. You can set a value between 4 and 64 characters.
Maximum Characters	Specify the most number of characters that the password can contain. You can set a value between 4 and 64 characters.
Minimum Alphabetic Characters	Specify the least number of alphabetic characters (a-z and A-Z) that the password can contain. This value must be lesser than or equal to the value specified in **Minimum Characters** field.
Minimum Numeric Characters	Specify the least number of numeric characters (0 through 9) that the password can contain.

Table 4-1 ArcotID Profile Configuration Fields

Field	Description
Minimum Special Characters	Specify the least number of special characters that the password can contain. By default, all the special characters excluding ASCII (0-31) characters are allowed.

6. Expand the **Advanced Configurations** section by clicking the **[+]** sign.

7. In the **Additional Attributes** section, specify any extra information (unsigned attributes) that you need to pass for the ArcotID credential in the **Name-Value** pair format.

   For example, if you want to lock the ArcotID to a specific device, say the end user's hard disk, then you need to use this section to send this extra information as follows:

   Table 4-2 Providing Additional Attributes for ArcotID

Name	Value
devlock_required	yes
devlock_type	hd

   NOTE: See *ArcotID Client 6.0 Reference Guide* for more information on what extra information you can specify here.

   If you need to specify more attributes, click **Add More** to display extra fields, one at a time.

8. In the **User Validations** section, select the **User Active** option if you want to verify the user status for the following operations involving the current credential:

   - Create credential
   - Re-issue credential
   - Reset credential
   - Reset validity of the credential

9. Click **Save** to create or update the ArcotID profile.

10. Refresh *all* deployed WebFort Server instances. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Configuring ArcotID Authentication Policy

An ArcotID policy can be used to specify the following attributes related to an ArcotID-based authentication:

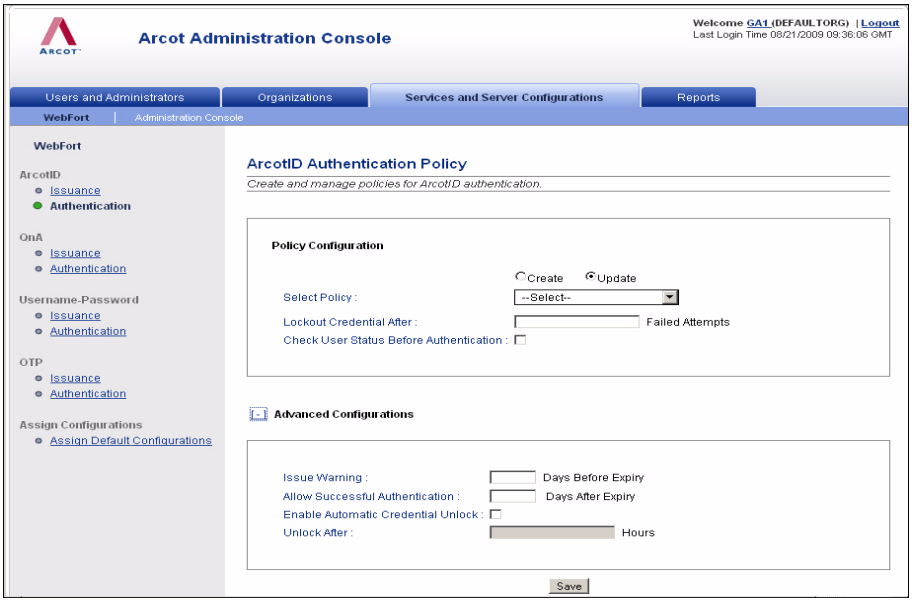
- **User status:** The status of the user, which can be active or inactive.
- **Lockout criteria**: The number of failed attempts after which the user's credentials will be locked out.
- **Unlocking criteria:** The number of hours after which a locked ArcotID credential can be used to log in again. This feature can drastically reduce the number of requests for resetting the credential.
- **Credential expiration settings**: The period before which a user will be warned about their ArcotID expiration.
- **Grace period:** The period for which an expired ArcotID credential is valid.

  NOTE: This option must be used very judiciously.

To configure a Global ArcotID authentication policy:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **ArcotID** section, click the **Authentication** link to display the ArcotID Authentication Policy page (Figure 4-9.)

Figure 4-9 ArcotID Authentication Policy Page



5. Edit the fields in the **Policy Configuration** section, as required. Table 4-3 describes the fields of this section.

Table 4-3 ArcotID Authentication Policy Configuration Fields

Field	Description
Policy Configurations	
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the **Select Policy** list that appears.
Lockout Credential After	Specify the number of failed attempts after which the user credential will be locked.

Table 4-3 ArcotID Authentication Policy Configuration Fields

Field	Description
Check User Status Before Authentication	Select this option if you want to verify the user status for the following operations involving the current credential: • Create credential • Re-issue credential • Reset credential • Reset validity of the credential

6. Expand the **Advanced Configurations** section by clicking the `[+]` sign.
7. Edit the fields in the section, as required. Table 4-4 describes the fields of this section.

Table 4-4 Advanced ArcotID Authentication Policy Configuration Fields

Field	Description
Advanced Configurations	
Issue Warning	Specify the number of days before the users will be warned about their impending ArcotID credential expiration.
Allow Successful Authentication	Specify the number of days for which the users can use an expired ArcotID credential to successfully log in to their accounts.
Enable Automatic Credential Unlock	Select this option if you want a locked credential to be automatically unlocked after the time you specify in the **Unlock After** field. This field is valid only if you specify the corresponding value in the **Lockout Credential After** field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.

8. Click **Save** to create or update the ArcotID policy.
9. Refresh *all* deployed WebFort Server instances. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Configuring QnA Settings

This section walks you through:

- Configuring QnA Issuance Profile
- Configuring QnA Authentication Policy

Configuring QnA Issuance Profile

A QnA profile can be used to specify the following attributes related to a QnA credential:

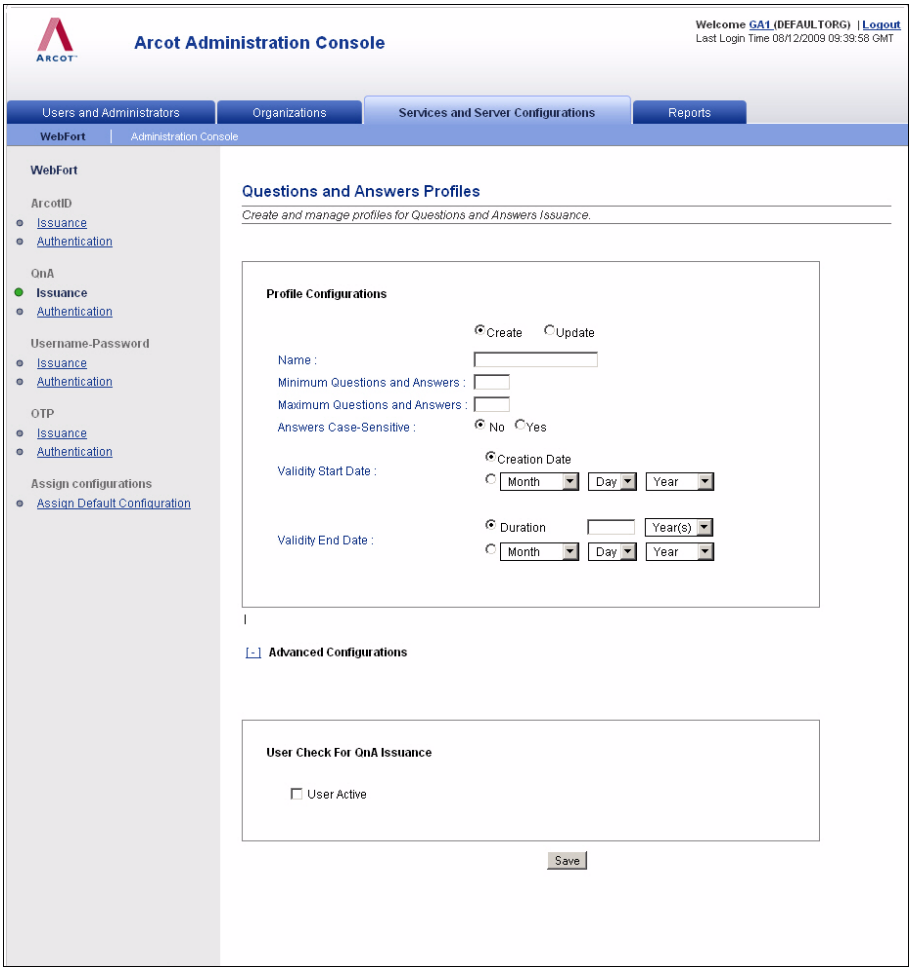
- **Number of questions:**
  - To be set by users (along with their answers) at the time of enrollment.
  - WebFort must ask the users during authentication process.
  - For which correct answers are required during authentication.
- **Validity period**: The period for which a QnA credential is valid.

By configuring a QnA profile and assigning it to one or more organizations, you can control the characteristics of QnA credentials that are issued to users of those organizations. Use the Questions and Answers Profiles page (Figure 4-9) for creating QnA credential profiles.

To create or update a QnA profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **QnA** section, click the **Issuance** link to display the Questions and Answers Profiles page (Figure 4-9.)

Figure 4-10 Questions and Answers Profiles Page



5. Edit the fields in the **Profile Configurations** section, as required. Table 4-5 describes the fields of this section.

Table 4-5 QnA Profile Configuration Fields

Field	Description
Profile Configurations	

Table 4-5 QnA Profile Configuration Fields

Field	Description
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Profile** list that appears.
Minimum Questions and Answers	Specify the minimum number of questions and answers that have to be set by users. For example, if you set 3 here and 5 in the **Maximum Questions and Answers** field, then the users will be prompted for *at least* three questions during the authentication out of the five they set.
Maximum Questions and Answers	Specify the maximum number of questions and answers that can be set by users.
Answers Case-Sensitive	Specify whether the answers that the users specify must match the case that they used to set the QnA.
Validity Start Date	Set the date from which the issued QnA credential will be valid. The validity can start from either the date when the QnA is created or you can specify a specific date.
Validity End Date	Set the date when the QnA credential will expire. You can either specify the duration for the credential's expiration or you can specify a specific date.

6. Expand the **Advanced Configurations** section by clicking the `[+]` sign.
7. In the **User Check For QnA Issuance** section, select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
   - Create credential
   - Re-issue credential
   - Reset credential
   - Reset validity of the credential
8. Click **Save** to create or update the QnA profile.

9. Refresh *all* deployed WebFort Server instances. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Configuring QnA Authentication Policy

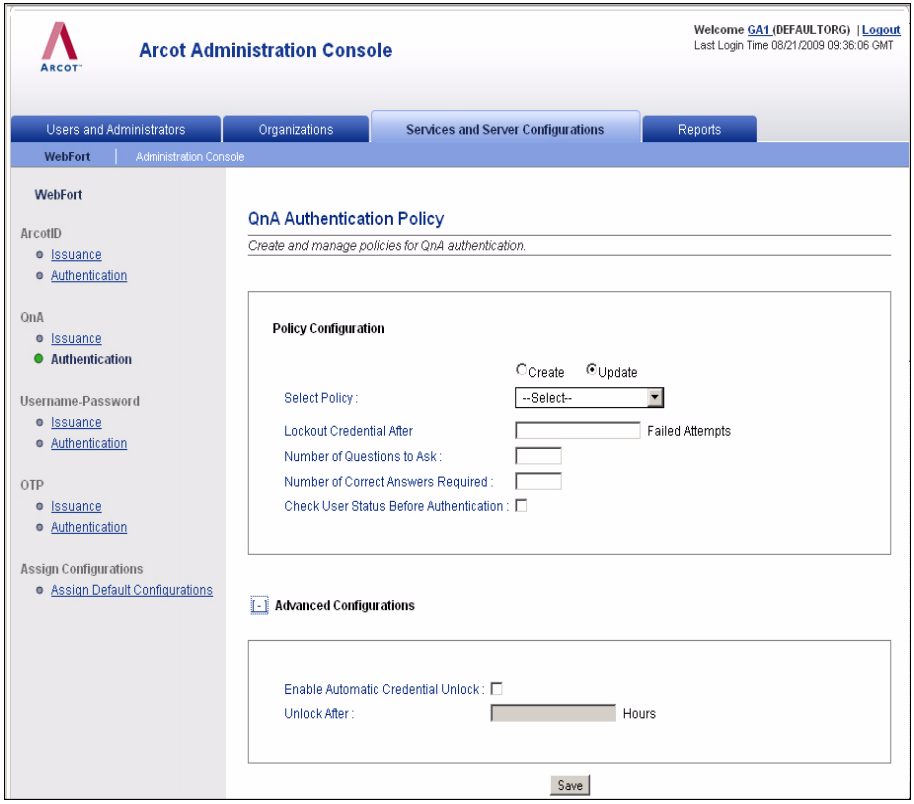
A QnA policy can be used to specify the following attributes related to a QnA-based authentication:

- **User status:** The status of the user, which can be active or inactive.
- **Number of questions:**
  - WebFort must ask the users during authentication process.
  - For which correct answers are required during authentication.
- **Lockout criteria**: The number of failed attempts after which the user's credential will be locked out.
- **Unlocking criteria:** The number of hours after which a locked QnA credential can be used to log in again.

To configure a QnA authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **QnA** section, click the **Authentication** link to display the QnA Authentication Policy page (Figure 4-11.)

Figure 4-11 QnA Authentication Policy Page



5. Edit the fields in the **Policy Configuration** section, as required. Table 4-6 describes the fields of this section.

Table 4-6 QnA Authentication Policy Configuration Fields

Field	Description
Policy Configuration	
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the **Select Policy** list that appears.

Table 4-6 QnA Authentication Policy Configuration Fields

Field	Description
Lockout Credential After	Specify the number of failed attempts after which the user credential will be locked.
Number of Questions to Ask	Set the number of questions that users will be prompted to answer during authentication.
Number of Correct Answers Required	Specify the number of correct answers that users must provide to authenticate successfully. For example, if you set 3 here and set 5 in the **Number of Questions to Ask** field, then users must answer *at least* three questions correctly out of the five they will be prompted to answer.
Check User Status Before Authentication	Select this option if you want to verify the user status for the following operations involving the current credential: • Create credential • Re-issue credential • Reset credential • Reset validity of the credential

6. Expand the **Advanced Configurations** section by clicking the `[+]` sign.
7. Edit the fields in the section, as required. Table 4-7 describes the fields of this section.

Table 4-7 Advanced QnA Authentication Policy Configuration Fields

Field	Description
Advanced Configurations	
Enable Automatic Credential Unlock	Select this option if you want the locked credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the **Lockout Credential After** field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.

8. Click **Save** to create or update the QnA policy.
9. Refresh *all* deployed WebFort Server instances. See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Configuring Username-Password Settings

This section walks you through:

- Configuring Username-Password Issuance Profile
- Configuring Username-Password Authentication Policy

Configuring Username-Password Issuance Profile

A Username-Password profile can be used to specify the following attributes related to a password credential:

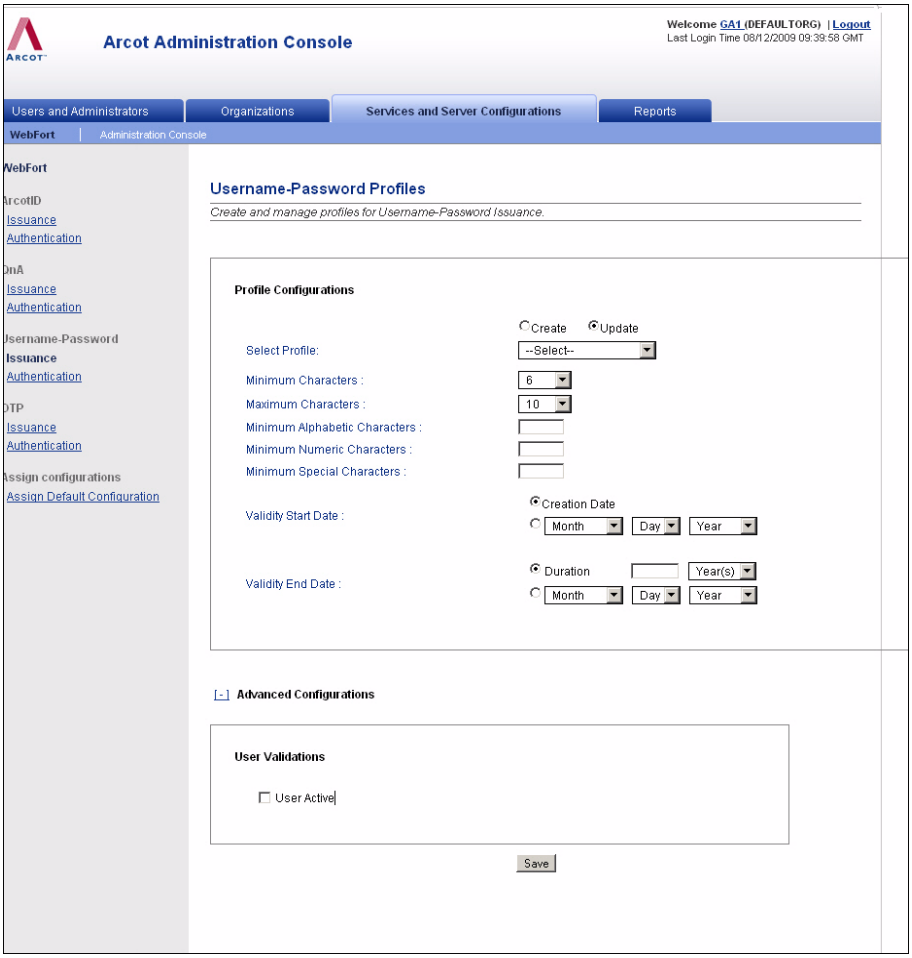
- **Password strength**: The effectiveness of password, which is determined by the length of the password and number of alphabets, numerals, and special characters in it.
- **Validity period**: The period for which the username-password credential is valid.

By configuring a Username-Password profile and assigning it to one or more organizations, you can control the characteristics of password credentials that are issued to users of those organizations. Use the Username-Password Profiles page (Figure 4-12) for creating password credential profiles.

To create or update a Username-Password profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Username-Password** section, click the **Issuance** link to display the Username-Password Profiles page (Figure 4-12.)

Figure 4-12 Username-Password Profiles Page



5. Edit the fields in the **Profile Configurations** section, as required. Table 4-8 describes the fields of this section.

Table 4-8 Username-Password Profile Configuration Fields

Field	Description
Profile Configurations	

Table 4-8 Username-Password Profile Configuration Fields

Field	Description
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Profile** list.
Minimum Characters	Specify the least number of characters that the password can contain. You can set a value between 4 and 64 characters. The default value is `6`.
Maximum Characters	Specify the most number of characters that the password can contain. You can set a value between 4 and 64 characters. The default value is `10`.
Minimum Alphabetic Characters	Specify the least number of alphabetic characters (a-z and A-Z) that the password can contain. This value must be lesser than or equal to the value specified in **Minimum Characters** field.
Minimum Numeric Characters	Specify the least number of numeric characters (0 through 9) that the password can contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	Specify the least number of special characters that the password can contain. By default, all the special characters excluding ASCII (0-31) characters are allowed.
Validity Start Date	Set the date from which the issued password credential will be valid. The validity can start from either the date when this credential is created or you can specify a custom date.
Validity End Date	Set the date when the password will expire. You can either specify the duration for the credential's expiration or you can specify a custom date.

6. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
7. In the **User Validations** section, select the **User Active** option if you want to verify the user status for the following operations involving the current credential:

- Create credential
- Re-issue credential
- Reset credential
- Reset validity of the credential

8. Click **Save** to create or update the Username-Password profile.
9. Refresh *all* deployed WebFort Server instances. See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Configuring Username-Password Authentication Policy

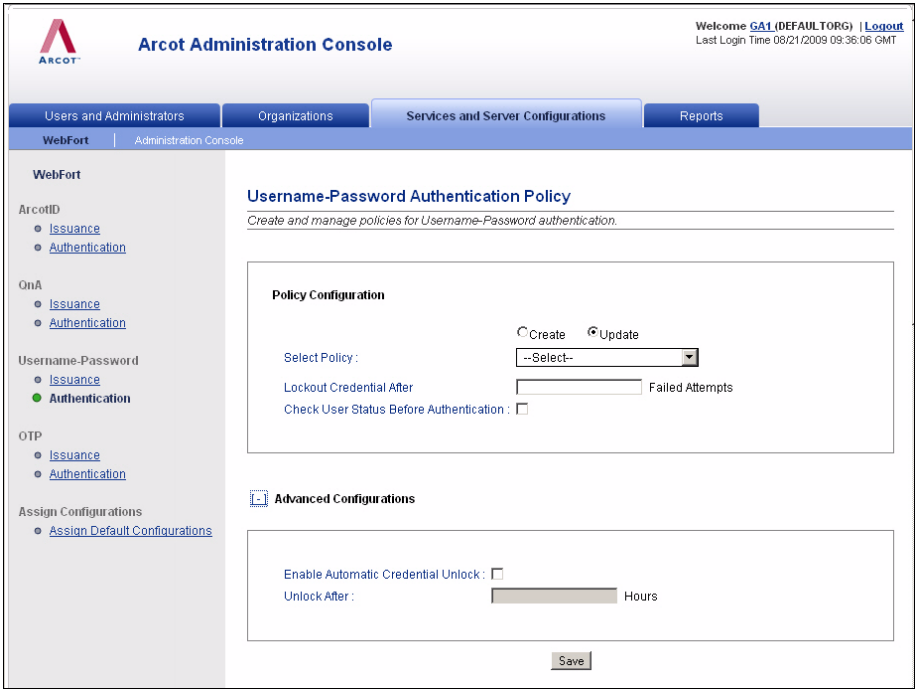
A Username-Password policy can be used to specify the following attributes related to password-based authentication:

- **User status:** The status of the user, which can be active or inactive.
- **Lockout criteria**: The number of failed attempts after which the user's credential will be locked out.
- **Unlocking criteria:** The number of hours after which a locked user password credential can be used to log in again.

To configure a Username-Password authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Username-Password** section, click the **Authentication** link to display the Username-Password Authentication Policy page (**Figure 4-9**.)

Figure 4-13 Username-Password Authentication Policy Page



5. Edit the fields in the **Policy Configuration** section, as required. Table 4-9 describes the fields of this section.

Table 4-9 Username-Password Authentication Policy Configuration Fields

Field	Description
Policy Configuration	
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the **Select Policy** list that appears.
Lockout Credential After	Specify the number of failed attempts after which the user credential will be locked.

Table 4-9 Username-Password Authentication Policy Configuration Fields

Field	Description
Check User Status Before Authentication	Select this option if you want to verify the user status for the following operations involving the current credential: • Create credential • Re-issue credential • Reset credential • Reset validity of the credential

6. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
7. Edit the fields in the section, as required. Table 4-10 describes the fields of this section.

Table 4-10 Advanced Username-Password Authentication Policy Configurations

Field	Description
Advanced Configurations	
Enable Automatic Credential Unlock	Select this option if you want the credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the **Lockout Credential After** field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.

8. Click **Save** to create or update the Username-Password policy.
9. Refresh *all* deployed WebFort Server instances. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Configuring OTP Settings

This section walks you through:

- Configuring OTP Issuance Profile
- Configuring OTP Authentication Policy

Configuring OTP Issuance Profile

An OTP profile can be used to specify the following attributes related to a One-Time Password credential:

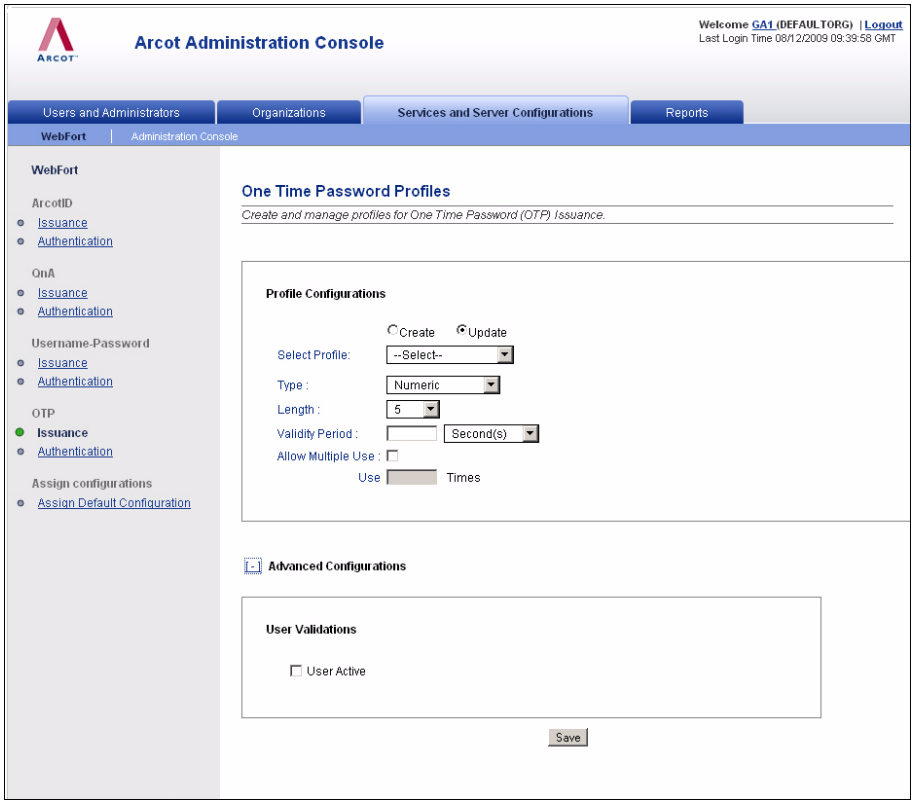
- **OTP strength:** The type (numeric or alphanumeric) and length of the OTP.
- **Validity period**: The period for which an OTP is valid.
- **Usage:** The number of times an OTP can be reused for authentication.

By configuring an OTP profile and assigning it to one or more organizations, you can control the characteristics of OTP credentials that are issued to users of those organizations. Use the One-Time Password Profiles page (Figure 4-14) for creating OTP credential profiles.

To create or update an OTP profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **OTP** section, click the **Issuance** link to display the One Time Password Profiles page (Figure 4-14.)

Figure 4-14 One-Time Password Profiles Page



5. Edit the fields in the **Profile Configurations** section, as required. Table 4-5 describes the fields of this section.

Table 4-11 OTP Profile Configuration Fields

Field	Description
Profile Configurations	
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Profile** list that appears.

Table 4-11 OTP Profile Configuration Fields

Field	Description
Type	Specify whether you want to issue numeric or an alphanumeric OTPs to users. The default value is `Numeric`.
Length	Set the length of an OTP. The minimum length of the OTP can be `5` (which is also the default value) and the maximum length can be up to 32 characters.
Validity Period	Set the interval from which the issued OTP credential will be valid. You can specify this time in seconds, minutes, hours, and days, and even in months and years.
Allow Multiple Use	Select this option if you would like the OTP to be used more than once.
Use	Specify the total number of times an OTP can be used if you selected the **Allow Multiple Use** option.

6. Expand the **Advanced Configurations** section by clicking the **`[+]`** sign.
7. In the **User Validation** section, select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
   - Create credential
   - Re-issue credential
   - Reset credential
   - Reset validity of the credential
8. Click **Save** to create or update the OTP profile.
9. Refresh *all* deployed WebFort Server instances. See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Configuring OTP Authentication Policy

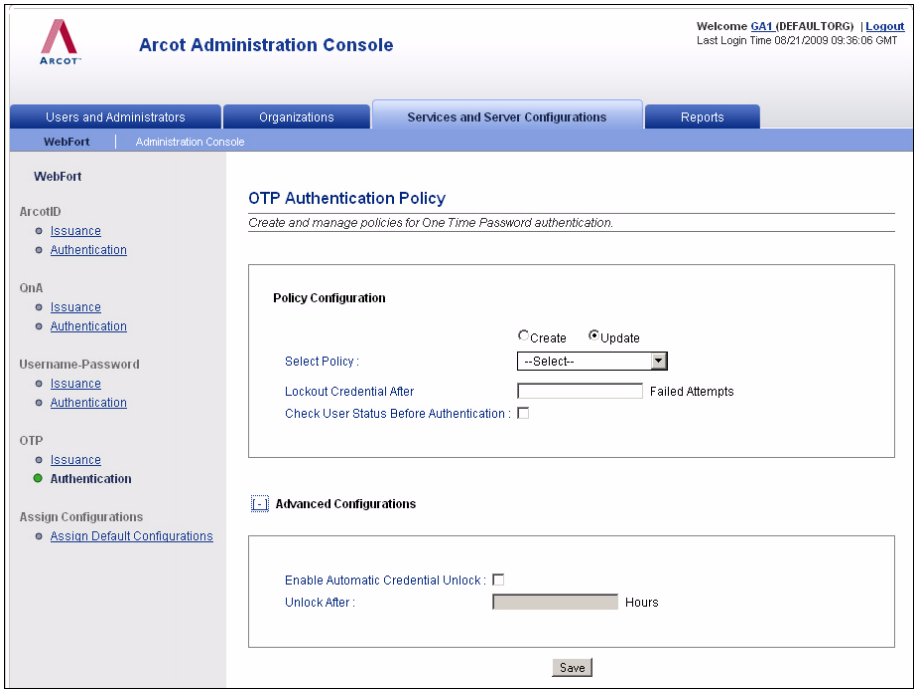
An OTP policy can be used to specify the following attributes related to OTP-based authentication:

- **User status:** The status of the user account, which can be active or inactive.
- **Lockout criteria**: The number of failed attempts after which the user's credential will be locked.
- **Unlocking criteria:** The number of hours after which a locked credential can be used to log in again.

To configure an OTP authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **OTP** section, click the **Authentication** link to display the OTP Authentication Policy page (Figure 4-15.)

Figure 4-15 OTP Authentication Policy Page



5. Edit the fields in the **Policy Configuration** section, as required. Table 4-12 describes the fields of this section.

Table 4-12 OTP Authentication Policy Configuration Fields

Field	Description
Policy Configuration	
Create	If you choose to create a new profile, then: 1. Select the **Create** option. 2. Specify the **Name** of the new profile in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the **Select Policy** list that appears.
Lockout Credential After	Specify the number of failed attempts after which the OTP will be locked.
Check User Status Before Authentication	Select this option if you want to verify the user status for the following operations involving the current credential: • Create credential • Re-issue credential • Reset credential • Reset validity of the credential

6. Expand the **Advanced Configurations** section by clicking the `[+]` sign.

7. Edit the fields in the section, as required. Table 4-13 describes the fields of this section.

Table 4-13 Advanced OTP Authentication Policy Configurations

Field	Description
Advanced Configurations	
Enable Automatic Credential Unlock	Select this option if you want the credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the Lockout Credential After field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.

8. Click **Save** to create or update the OTP policy.

9. Refresh *all* deployed WebFort Server instances. See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

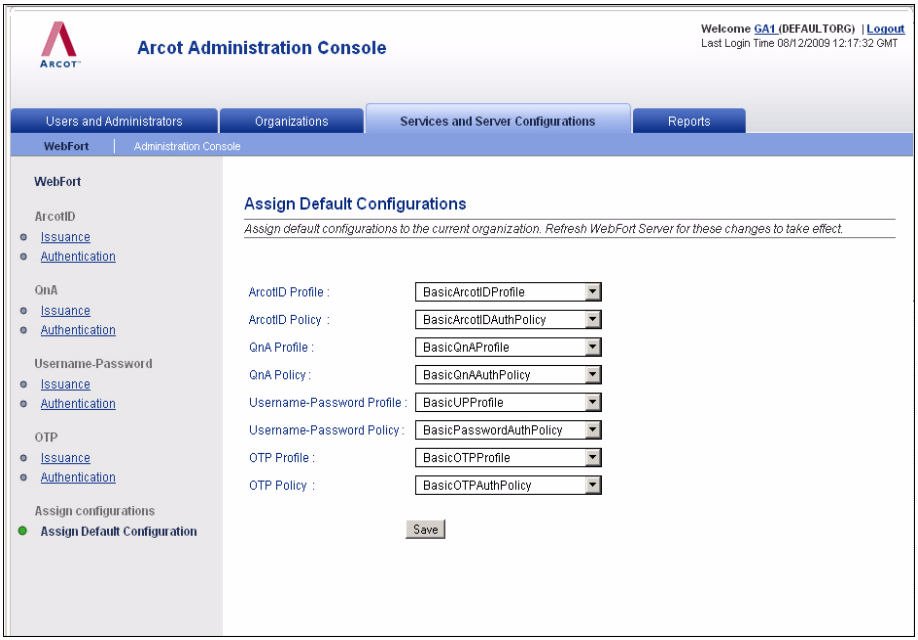
Assigning Default Configurations

After you have created the required credential profiles and authentication policies, you need to assign them globally (as a GA) or to a specific organization (as a Organization Administrator) by using Assign Default Configurations page. You need to use the same page for assigning configurations at both the levels, however the approach to the task page is different.

This section explains how to apply configurations at global level. For assigning the configurations to the organization, see "Managing Organization-Specific Configurations".

> **NOTE:** If the Organization Administrator (OA) does not specify profiles and policies at their organization level, then these profiles and policies are used by default. On the other hand, if a GA or an OA overwrites these configurations at their individual organization level, then those configurations are applicable for the organization.

Figure 4-16 Assign Default Configurations Page



To assign default configurations:

1. Ensure that you are logged in as a Global Administrator (GA).

2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the sub menu is active.
4. Under the **Assign Configurations** section, click the **Assign Default Configuration** link to display the corresponding page (Figure 4-16.)
5. Select the credential profiles or authentication policies from the corresponding drop-down lists.

   The default profiles (**Basic<*Profile_Name*>Profile**) and policies (**Basic<*Profile_Name*>AuthPolicy**) for each credential type is also available in these lists.
6. Click **Save** to assign the default profiles and policies.

   NOTE: These profiles and policies can be overridden at organization-level.
7. Refresh *all* deployed WebFort Server instances. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Chapter 5

Managing Organizations

In Arcot Administration Console, an *organization* can either map to a complete enterprise (or a company) or a specific division, department, or other entities within the enterprise. The organization structure provided by the Administration Console is flat. In other words, organizational hierarchy (in form of parent and child organizations) is *not* supported, and all organizations are created at the same level as the Default Organization. (See **"Specifying Global Settings for Organizations" on page 28** for more information on Default Organization.)

The larger the enterprise, the more complex its organization structure. As a result, management of organizations is a critical part of administration. The organization management operations supported by WebFort include:

- **Creating and Activating Organizations**
- **Searching for Organizations**
- **Managing Organization-Specific Configurations**
- **Updating Organization Information**
- **Disabling Organizations**
- **Enabling Organizations**
- **Activating Organizations in Initial State**
- **Deleting Organizations**

Creating and Activating Organizations

You can create an organization and store its data either in the WebFort repository or in your existing LDAP-based directory server implementations, such as Microsoft Active Directory and Sun ONE Directory Server.

> **NOTE:** In case of a small deployment, you can rename the Default Organization, instead of creating a new organization.

Based on your implementation, this section guides you through the steps for:

- **Creating Organizations in Arcot Repository**
- **Creating Organization in LDAP Repository**

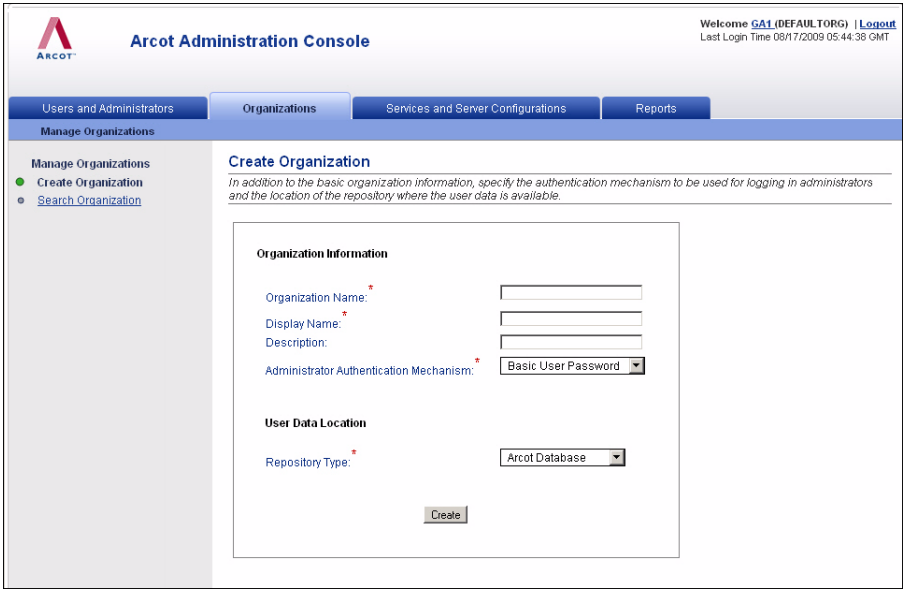
Privileges Required: To be able to create and activate an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can create and activate all organizations. GAs and OAs can create and activate all organizations in their scope.

Creating Organizations in Arcot Repository

To create an organization in the Arcot repository:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Create Organization** link to display the Create Organization page (Figure 5-1.)

Figure 5-1 Create Organization Page



4. Enter the details of the organization, as discussed in Table 5-1.

Table 5-1 Create Organization Fields

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. **NOTE:** You have to specify this value to log in to this organization, *not* the Display Name of the organization.
Display Name	Enter the descriptive name for the organization. **NOTE:** This name appears on all other Administration Console pages and reports.
Description	Provide a description for the administrators who will manage this organization. **NOTE:** You can provide additional details for later reference for the organization by using this field.

Table 5-1 Create Organization Fields

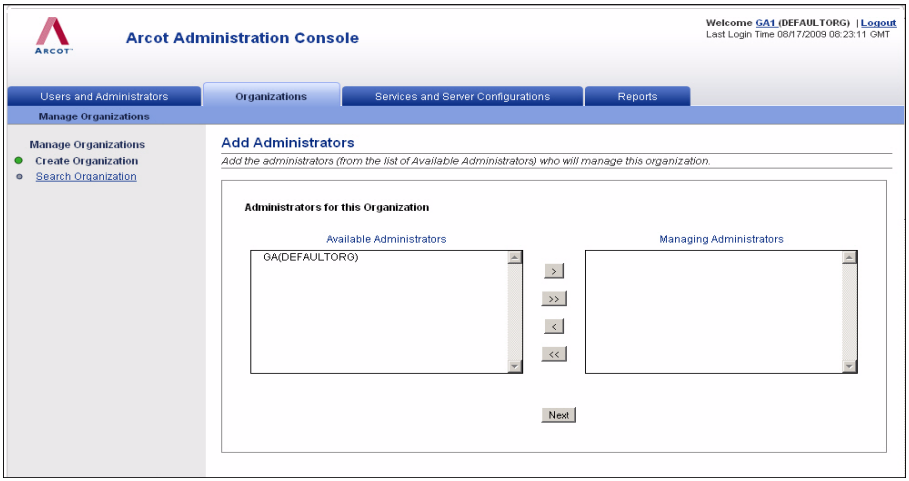
Field	Description
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators belonging to this organization. Administration Console supports the following two types of authentication mechanisms: • **Basic User Password** This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators log in to the console by specifying their ID and password. • **WebFort User Password** This is the WebFort user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by WebFort Server. • To use this mechanism, the Administration Console must be connected to WebFort Server by using WebFort Connectivity page, see "Configuring WebFort Connectivity" for more information.
User Data Location	
Repository Type	Select **Arcot Database**. By specifying this option, the user and administrator details for the new organization will be stored in the RDBMS repository supported by WebFort.

5. Click **Create** to create the new organization.

   The Add Administrators page (Figure 5-2) appears.

   NOTE: This page is *not* displayed, if all the administrators currently present in the system have scope to manage all organizations.

Figure 5-2 Add Administrators



6. From the **Available Administrators** list, select the administrators who will manage the organization and click the > button to add the administrator to the **Managing Administrators** list.

   The **Available Administrators** list displays all the administrators who can manage the new organization.

   > **NOTE:** If some administrators have scope to manage all organizations in the system, then you will not see the corresponding entries for those administrators in this list.

   The **Managing Administrators** list displays the administrators that you have selected to manage this organization.

7. Click the **Next** to proceed.

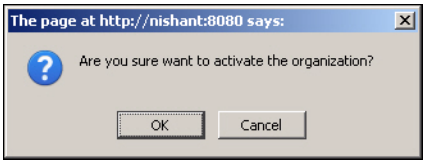
   The Activate Organization page (Figure 5-3) appears.

Figure 5-3 Activate Organization

8. Click **Enable** to activate the new organization.

   The message box shown in Figure 5-3 appears.

Figure 5-4 Activate Organization: Message



9. Click **OK** to complete the process.

10. Refresh *all* deployed WebFort Server instances. See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Creating Organization in LDAP Repository

To support LDAP user directories, you must create an organization in Arcot repository and then map the Arcot attributes with the LDAP attributes. To do so:

1. Ensure that you are logged in with the required privileges and scope to create the organization.

2. Activate the **Organizations** tab.

3. Under the **Manage Organizations** section, click the **Create Organization** link to display the Create Organization page (Figure 5-1.)

4. Enter the details of the organization, as discussed in Table 5-2.

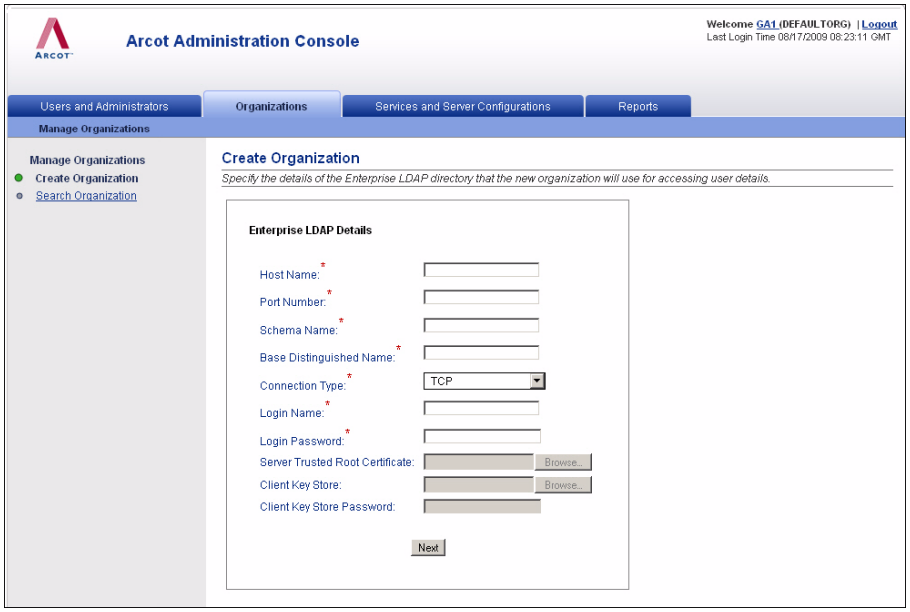
Table 5-2 Create Organization Fields in LDAP Repository

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. **NOTE:** You can use the Administration Console to log in to this organization, by specifying this value, *not* the Display Name of the organization.
Display Name	Enter the descriptive name for the organization. **NOTE:** This name appears on all other Administration Console pages and reports.
Description	Provide a description for the administrators who will manage this organization. **NOTE:** You can provide additional details for later reference for the organization by using this field.
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators belonging to this organization. Administration Console supports the following two types of authentication mechanisms: • **Basic User Password** This is the in-built authentication mechanism provided by Administration Console. If you select this option, then administrators log in to the console by specifying their ID and plain text password. • **WebFort User Password** This is the WebFort user name-password authentication method. If you select this option, then the administrator credentials are issued and authenticated by WebFort Server.
User Data Location	
Repository Type	Select **Enterprise LDAP**. By specifying this option, the user and administrator details for the new organization will be stored in the LDAP repository that you will specify on the next page.

5. Click **Create** to create the new organization.

   The Create Organization page (Figure 5-5) to collect the LDAP repository details appears.

Figure 5-5 Create Organization: Enterprise LDAP Details



6. Enter the details, discussed in Table 5-3, to connect to the LDAP repository.

Table 5-3 LDAP Repository Details

Field	Description
Host Name	Enter the host name of the system where the LDAP repository is available.
Port Number	Enter the port number on which the LDAP repository service is listening.
Schema Name	Specify the LDAP schema used by the LDAP repository. This schema specifies the types of objects that an LDAP repository can contain, and specifies the mandatory and optional attributes of each object type. Typically, the schema name for Active Directory is `user` and for SunOne Directory it is `inteorgperson`.

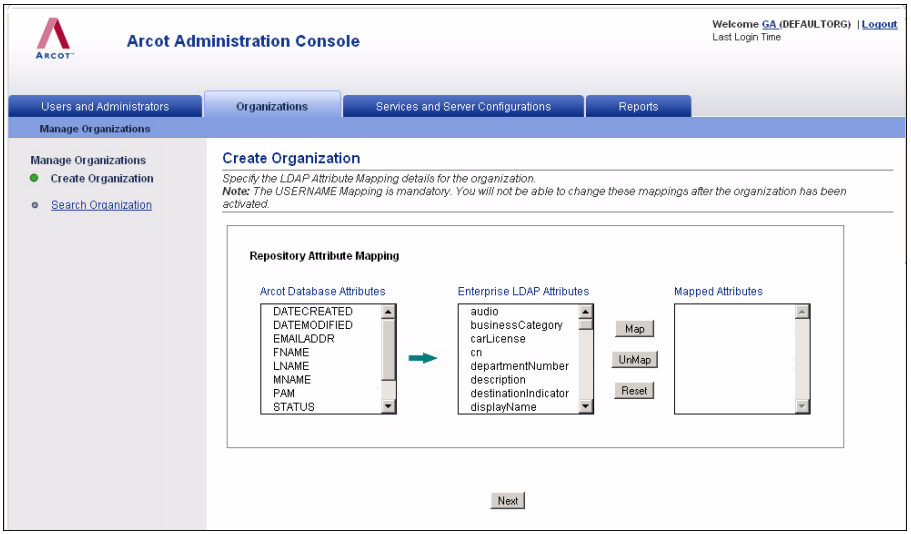
Table 5-3 LDAP Repository Details

Field	Description
Base Distinguished Name	Enter the base Distinguished Name of the LDAP repository. This value indicates the starting node in the LDAP hierarchy to search in the LDAP repository. For example, to search or retrieve a user with a DN of `cn=rob laurie, ou=sunnyvale, o=arcot, c=us`, you must specify the base DN as the following: • `ou=sunnyvale, o=arcot, c=us` **NOTE:** Typically, this field is case sensitive and searches all sub-nodes under the provided base DN.
Connection Type	Select the type of connection that you want to use between the Administration Console and the LDAP repository. Supported types are: • **TCP** • **One-way SSL** • **Two-way SSL**
Login Name	Enter the complete distinguished name of the LDAP repository user who has the privilege to log into repository sever and manage the Base Distinguished Name. For example, `uid=gt,dc=arcot,dc=com`
Login Password	Enter the password of the user provided in the Login Name.
Server Trusted Root Certificate	Enter the path for the trusted root certificate who issued the SSL certificate to the **LDAP** server by using the **Browse** button, if the required SSL option is selected.
Client Key Store Path	Enter the path for the key store that contains the client certificate and the corresponding key by using the **Browse** button, if the required SSL option is selected. **NOTE:** You must upload either PKCS#12 or JKS key store type.
Client Key Store Password	Enter the password for the client key store, if the required SSL option is selected.

7. Click **Next** to proceed.

   The page (Figure 5-6) to map the repository attributes appears.

Figure 5-6 Create Organization: Repository Attribute Mapping



8. On this page:

   a. Select an attribute from the **Arcot Database Attributes** list, then select the appropriate attribute from the **Enterprise LDAP Attributes** list that needs to be mapped with the Arcot attribute, and click **Map**.

   IMPORTANT: Mapping of the **`UserName`** attribute is compulsory. If you do not map this attribute, then the mapping will not be successful. If you are using Active Directory, then map **`UserName`** to **`cn`**. If you are using SunOne Directory, then map **`UserName`** to **`uid.`**

   b. Repeat the process to map multiple attributes, until you finish mapping all the required attributes.

   NOTE: You do not need to map all the attributes in the **Arcot Database Attributes** list. You only need to map the attributes that you will use.

   The attributes that you have mapped will be moved to the **Mapped Attributes** list.

   If required, you can unmap the attributes. If you want to unmap a single attribute at a time, then select the attribute and click **Unmap**. However, if you want to clear the **Mapped Attribute** list, then click **Reset** to unmap all the mapped attributes.

9. Click **Next** to proceed.

   The Add Administrators page (Figure 5-2) appears.

NOTE: This page is *not* displayed, if all the administrators currently present in the system have scope to manage all organizations.

10. From the **Available Administrators** list, select the administrators who will manage the organization and click the > button to add the administrator to the **Managing Administrators** list.

    NOTE: Assigning organization to administrators can be done at any time by updating the scope of existing administrators or by creating new administrators to manage the organization.

    The **Available Administrators** list displays all the administrators who can manage the new organization.

    NOTE: If some administrators have scope to manage all organizations in the system, then you will not see the corresponding entries for those administrators in this list.

    The **Managing Administrators** list displays the administrators that you have selected to manage this organization.

11. Click the **Next** to proceed.

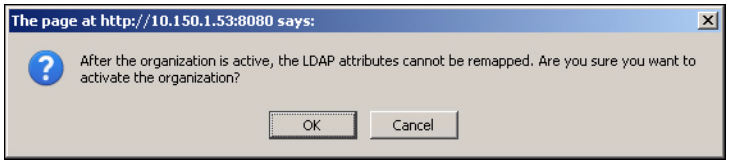
    The Activate Organization page (Figure 5-3) appears.

    NOTE: Mapping details *cannot* be changed or updated after the organization is activated.

12. Click **Enable** to activate the new organization.

    The warning message shown in Figure 5-7 appears.

Figure 5-7 Activate LDAP-Based Organization



13. Click **OK** to complete the process.

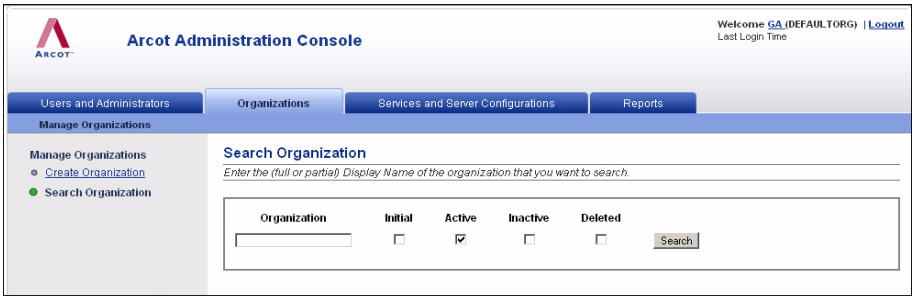
Searching for Organizations

Privileges Required: As long as you do not need to update, activate, or deactivate an organization, you do not need privileges to search. However, you *must* have the scope over the organizations that you are searching. For example, an OA can search for a target organization *if* that organization is in their purview.

You can search for organizations by their name and status. To search for one or more organizations:

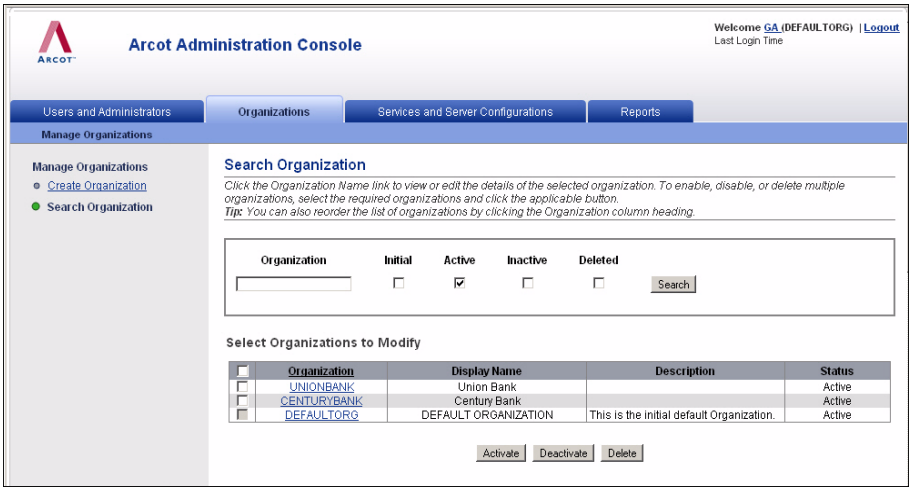
1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-1.)

Figure 5-8 Search Organization Page



4. Enter the partial or complete information of the required organization. You can select the following options to broaden your search:
   - **Initial** (to display the organizations that have been created but have not been activated yet.)
   - **Active** (to display the organizations that have been created and have been activated.)
   - **Inactive** (to display the organizations that have been disabled.)
   - **Deleted** (to display the organizations that have been deleted.)
5. Click **Search** to display the page (similar to Figure 5-9), with all the matches for the specified criteria.

Figure 5-9 Search Organization Page: Result



Managing Organization-Specific Configurations

The GAs or the OAs who have the scope to manage the organization can set the configurations for individual organizations. If the organization-specific configurations are set, then these configurations overwrite the global configurations, discussed in **Chapter 4, "Managing Global WebFort Configurations"**.

Privileges Required:

To be able to manage the configurations of an organization, you must ensure that you have the appropriate privileges and scope to do so. MA *cannot* manage any organization-specific configurations. GAs and OAs can manage the configurations for all organizations in their scope.

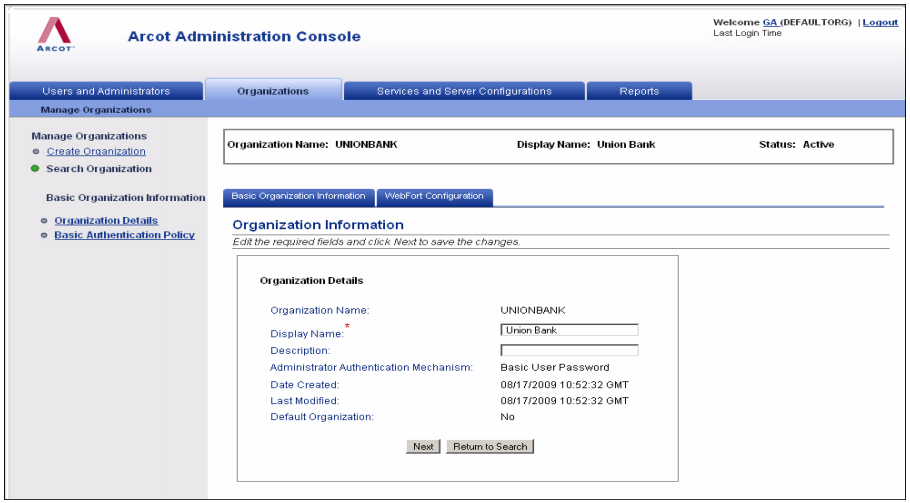
The organization-specific configurations are similar to the global configurations, but navigation paths to their task page is different. To access the task page for performing the organization-specific configurations:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (**Figure 5-8**.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to **Figure 5-9**) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to **Figure 5-10**) appears.

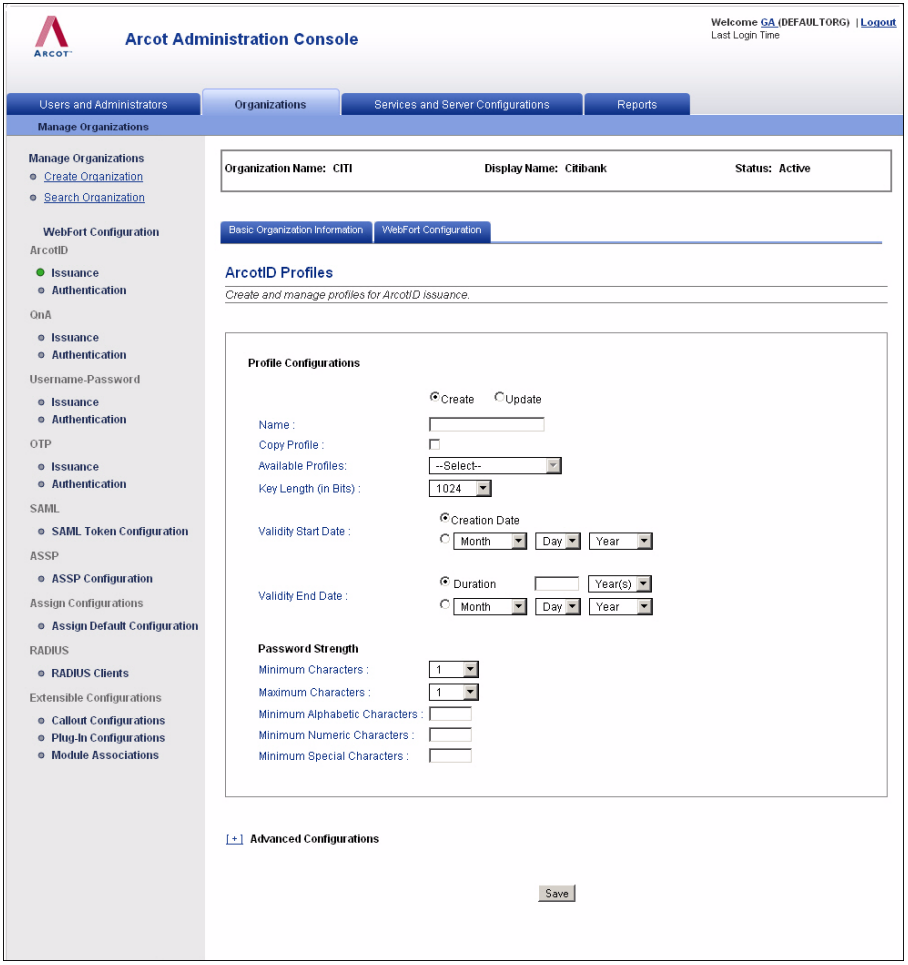
Figure 5-10 Organization Information Page



6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane (Figure 5-11).

Figure 5-11 Organization-Specific WebFort Configurations



7. Configure and assign the credential profiles and authentication policies.

   See Chapter 4, "Managing Global WebFort Configurations" for detailed information on how to configure the required profiles and policies and assign them, as needed. The operations discussed in Chapter 4, "Managing Global WebFort Configurations" are for global level, however the configurations discussed in this chapter are for organization level, the configurations for both are same only the approach to access the task page is different as explained at the beginning of this section.

In addition to configuring ArcotID, QnA, Username-Password, and OTP profiles and policies for an organization, you can also configure the following organization-specific settings:

- Configuring SAML Tokens
- Configuring RADIUS Clients
- Configuring ASSP
- Configuring Callouts
- Configuring Plug-Ins
- Associating Events

Configuring SAML Tokens

On successful authentication, WebFort can return a token. WebFort supports different types of authentication tokens, and Secure Assertion Markup Language (*SAML*) tokens are one among them (in addition to Native and OTT token types.)

If you want to issue SAML as authentication tokens, then you must configure the SAML token properties. To do so:

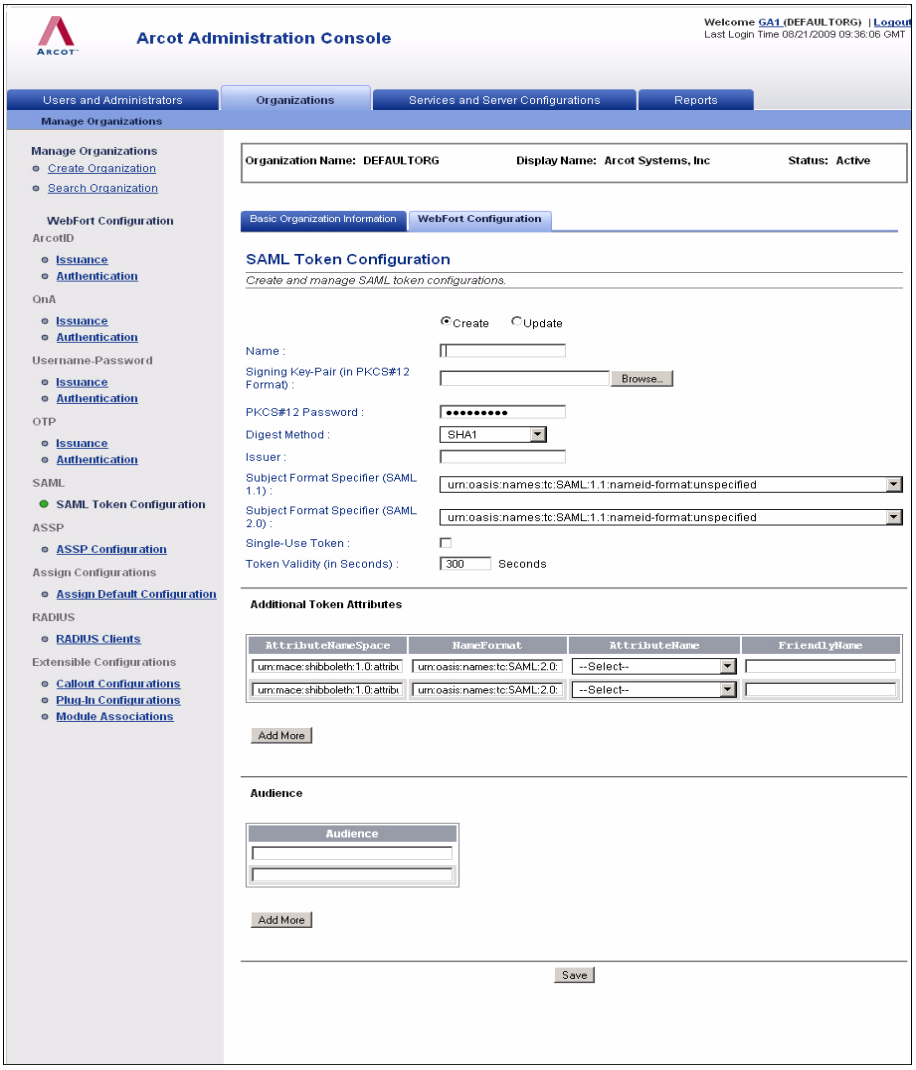
1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to Figure 5-10) appears.
6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane (Figure 5-11).
7. Under **SAML**, click the **SAML Token Configuration** link to display the SAML Token Configuration page (Figure 5-12.)

Figure 5-12 SAML Token Configuration Page



8. Depending on whether you want to create a new SAML configuration or update an existing SAML configuration, choose the respective option:

   - If you choose to **Create** a new configuration, then enter the configuration name in the **Name** field.

     or

- If you choose to **Update** an existing configuration, then select the configuration that you want to update from the **Name** list.

9. Navigate to the location for the PKCS#12 Store, where the SAML certificate and the private key for the **Signing Key-Pair (in PKCS#12 Format)** are available.
10. Enter the corresponding **PKCS#12 Password**.
11. In the **Digest Method** field, specify the algorithm (such as SHA1, SHA256, SHA384, SHA512, or RIPEMD 160) that will be used for hashing the SAML tokens.
12. Enter the name of the **Issuer** who will provide the SAML token generated by WebFort.

    For example, if company XYZ is using WebFort to generate SAML tokens, then you can enter XYZ in this field.
13. In the **Subject Format Specifier (SAML 1.1)** field, specify the format of the SAML subject for SAML 1.1.
14. In the **Subject Format Specifier (SAML 2.0)** field, specify the format of the SAML subject for SAML 2.0.
15. Enable the **Single-Use Token** option, if you want the SAML token to be used only once for authentication.
16. In the **Token Validity (in Seconds)** field, enter the duration after which the SAML token *cannot* be used.
17. In the **Additional Token Attributes** section, set the additional attributes, if required for the SAML token generation.

    Click **Add More** to add more attributes, if needed.
18. In the **Audience** section and table, enter the details of the audience who can use the SAML token.

    Click **Add More** to add more audiences, if needed.
19. Click **Save** to save the SAML token configuration.
20. Refresh *all* deployed WebFort Server instances. See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Configuring RADIUS Clients

If configured, WebFort can serve as a RADIUS Server to the configured Network Access Server (NAS) or the RADIUS clients. RADIUS clients can be categorized as SSL Virtual Private Networks (VPN) and Internet Protocol Security (IPSec) VPNs.

SSL VPN Workflow

The authentication workflow for client-less or SSL VPNs will typically be as follows:

1. User tries to access a secured Web site by providing credentials.
2. Your application, which is integrated with the WebFort Server, performs user authentication and responds back with One-Time Token (OTT) generated by WebFort Server.
3. The OTT is sent through the VPN gateway to WebFort Server for verification.
4. WebFort Server verifies the token
5. After successful verification of the authentication token, the user is granted access to the secured Web site.

IPSec VPN Workflow

The authentication workflow for IPSec VPNs will typically be as follows:

1. User tries to access a secured Web site by providing credentials.
2. The user signs up by creating QnA and ArcotID.
3. The user downloads the ArcotID.
4. On the login page of the VPN client, user specifies their user name and ArcotID password to authenticate to WebFort Server through the VPN Gateway.
5. WebFort Server verifies the token
6. After successful verification of the authentication token, the user is granted access to the secured Web site.

Configuring RADIUS Clients

To configure RADIUS clients for the an organization:

1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)

4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.

5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

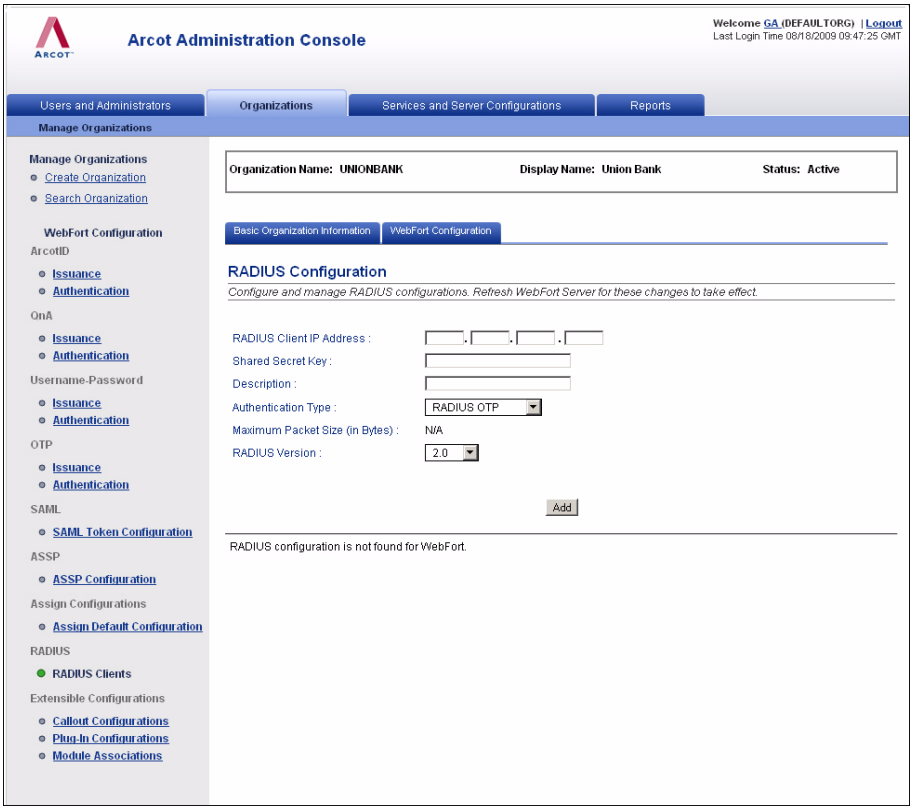
   The Organization Information page (similar to Figure 5-10) appears.

6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane (Figure 5-11).

7. Under **RADIUS**, click the **RADIUS Clients** link to display the RADIUS Configuration page (Figure 5-13.)

Figure 5-13 RADIUS Configuration Page



8. Provide the following information in the respective fields:

- **RADIUS Client IP Address**: The IP Address of the RADIUS client through which users authenticate to WebFort Server.
- **Shared Secret Key**: The secret key shared between the RADIUS client and the WebFort Server.

  NOTE: The minimum length of key is *1* and the maximum is *512* characters.

- **Description**: Enter a string to describe the RADIUS client. The description helps to identify the RADIUS client, if multiple clients are configured.
- **Authentication Type**: Select the authentication mechanism that will be used for VPN authentications:
  - **RADIUS OTP:** Is used for SSL VPN clients.
  - **In-Band ArcotID:** Is used for IPSec VPN clients.
- **Maximum Packet Size (in Bytes):** Select the appropriate packet size for RADIUS messages.

  NOTE: Refer to the *RFC 2865* for more information on the packet format.

- **RADIUS Version:** Specify the RADIUS version supported for the client you are adding.

9. Click **Add** to add the IP address of the new RADIUS client.
10. Refresh *all* deployed WebFort Server instances.See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Deleting and Updating RADIUS Clients

If the configuration is detected, the RADIUS Configuration page also displays the **Configured RADIUS Clients** table, which helps you to update or delete the RADIUS client IP addresses.

Deleting RADIUS Clients

To delete a RADIUS client:

1. Select the IP address you want to delete.
2. Click **Delete**.
3. Refresh *all* deployed WebFort Server instances.

   See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Updating RADIUS Clients

To update the RADIUS client:

1. Select the IP address you want to update.
2. Update any of the column for the selected IP address and click **Update**.
3. Refresh *all* deployed WebFort Server instances.

   See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Configuring ASSP

Adobe Signature Service Protocol (*ASSP*) is used for signing PDF documents by using the Arcot SignFort. Before signing, the users are authenticated either by using WebFort authentication methods. A SAML token is returned to the user after successful authentication. This token is then verified by the SignFort Server.

To configure ASSP:

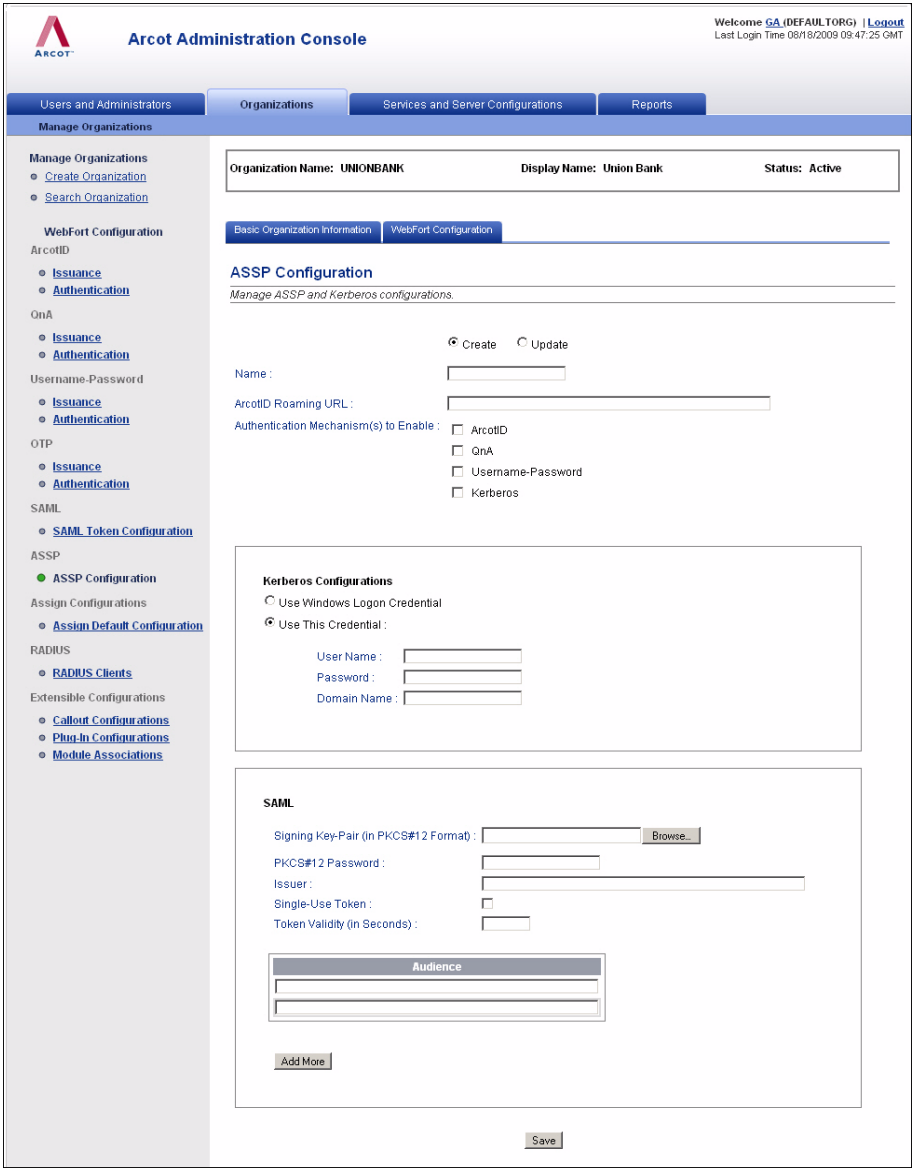
1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (**Figure 5-8**.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to **Figure 5-9**) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to **Figure 5-10**) appears.
6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane (**Figure 5-11**).
7. Under **ASSP**, click the **ASSP Configuration** link to display the ASSP Configuration page (**Figure 5-14**.)

Figure 5-14 ASSP Configuration Page



8. Depending on whether you want to create a new ASSP configuration or update an existing ASSP configuration, choose the respective option:

   - If you choose to **Create** a new configuration, then enter the configuration name in the **Name** field.

or

- If you choose to **Update** an existing configuration, then select the configuration that you want to update from the **Name** list.

9. Enter the **ArcotID Roaming URL** that will be used to download ArcotIDs in case of ArcotID Roaming Download.

   If case of ArcotID Roaming Download, if the user does not have their ArcotID present on their current system, then the **ArcotID Roaming URL** is used to authenticate to the WebFort Server and download the user's ArcotID.

10. From **Authentication Mechanism(s) to Enable**, select the authentication method that will be used to authenticate the user before signing.

    If you enable **ArcotID** authentication method, then you must also select **QnA** because QnA authentication method is used for roaming download of ArcotID.

11. If you enable **Kerberos** authentication method in the preceding step, then you must set the parameters required for Kerberos authentication in **Kerberos Configurations** section, either:

    - Select the **Use Windows Logon Credential** option, if you want to use the Kerberos token of the WebFort Server process.

      or

    - Specify new credentials in the **User Name**, **Password**, and **Domain Name** fields for Kerberos authentication.

12. In the **SAML** section:

    a. Specify the location of the PKCS#12 Store in the **Signing Key-Pair** (**in PKCS#12 Format**) field. It contains the certificate and the private key that will be used by the WebFort Server to issue the SAML token.

    b. Enter the corresponding **PKCS#12 Password**.

    c. Enter the URL of the WebFort Server in the **Issuer** field.

    d. Enable the **Single-Use Token** option, if you want the SAML token to be used only once for authentication.

    e. In the **Token Validity** (**in Seconds**) field, enter the duration after which the SAML token *cannot* be used.

    f. In the **Audience** table, enter the details of the audience who can use the SAML token.

       Click **Add More** to add more audiences.

13. Click **Save** to save the ASSP configuration.
14. Refresh *all* deployed WebFort Server instances.

    See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Configuring Callouts

A *callout* is an external HTTP-based process that serves events exposed by the WebFort Server. The data that WebFort Server sends includes the HTTP name-value pair POST data, along with the encoded URL.

> **NOTE:** See *Arcot WebFort 6.0 Business Logic Extension Guide* for detailed information on callouts.

To configure a callout:

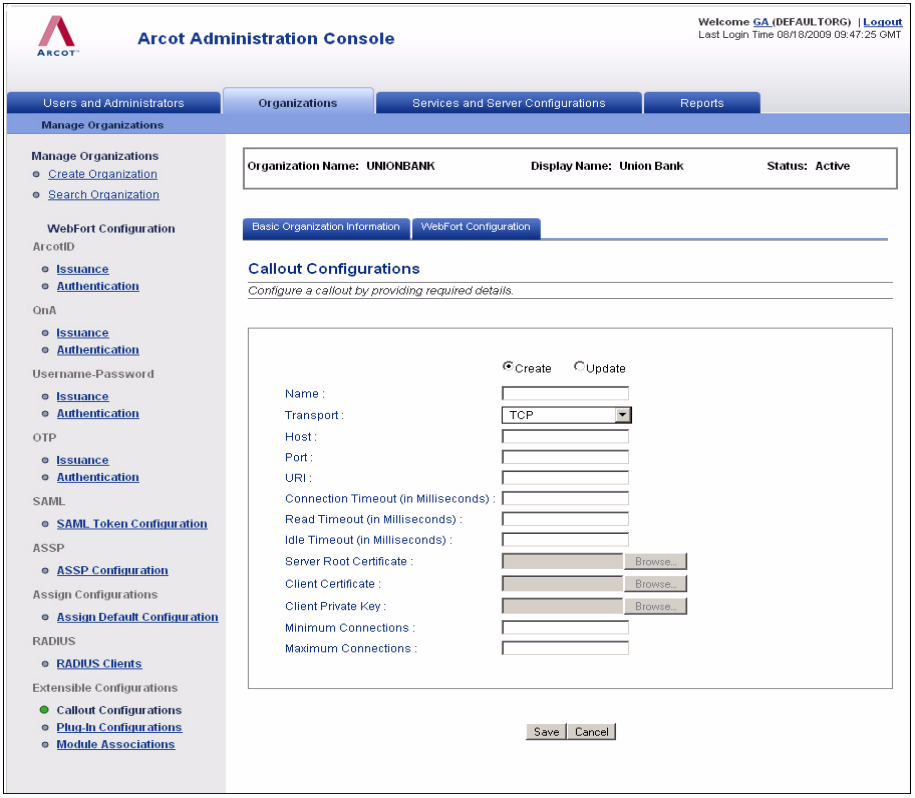
1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (**Figure 5-8**.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to **Figure 5-9**) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to **Figure 5-10**) appears.
6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane (**Figure 5-11**).
7. Under **Extensible Configurations**, click the **Callout Configurations** link to display the Callout Configurations page (**Figure 5-15**.)

Figure 5-15 Callout Configurations Page



8. Edit the fields in the page, as required. Table 5-4 describes the fields of this section.

Table 5-4 Callout Registration

Page Field	Description
Create	If you choose to create a new callout, then: 1. Select the **Create** option. 2. Specify the **Name** of the new callout in the field.
Update	If you choose to update an existing callout, then select the callout that you want to update from the **Name** list.

Table 5-4 Callout Registration

Page Field	Description
Transport	Specify one of the following modes that are supported for data transfer: • **TCP**: This is the default mode between the Callout Server and WebFort Server. It sends data in the clear. • **One-Way SSL**: One-Way Secure Sockets Layer (SSL) provides higher security for transactions, because in addition to encrypting and decrypting the data, it ensures that the Callout Server authenticates to WebFort Server for each session. • **Two-Way SSL**: Two-Way SSL provides higher security for transactions, because in addition to encrypting and decrypting the data, it ensures that both Callout Server and WebFort Server authenticate to each other for each session. **NOTE:** If you select SSL, then add the fields in the XML file for private key and the certificate chain.
Host	Enter the host name of the Callout Server.
Port	Enter the port number where the Callout Server is available.
URI	Enter the Uniform Resource Identifier (URI) at which the Callout Server can be accessed by the WebFort Server.
Connection Timeout (in Milliseconds)	Enter the interval, in milliseconds, for which a request for a connection waits when no connections are available in the connection pool and no new connections can be created.
Read Timeout (in Milliseconds)	Enter the time that the WebFort Server will wait for a response to a request from the callout.
Idle Timeout (in Milliseconds)	Enter the interval, in milliseconds, for which the WebFort Server waits before closing the connection.
Server Root Certificate	Browse to and upload the PKCS#12 Store path that contains the root certificate of the Callout Server.
Client Certificate	Browse to and upload the PKCS#12 Store path that contains the WebFort Server certificate.
Client Private Key	Browse to and upload the private key of the WebFort Server certificate.
Minimum Connections	Enter the maximum number of connections that can be maintained between WebFort Server and the Callout Server.
Maximum Connections	Enter the minimum number of connections that must be maintained between WebFort Server and the Callout Server.

9. Click **Save** to create a new callout or update an existing callout definition.
10. Refresh *all* deployed WebFort Server instances.

    See **"Refreshing or Shutting Down Instances" on page 42** for instructions on how to do this.

Configuring Plug-Ins

A plug-in registered by a Master Administrator (see **"Registering and Updating Plug-Ins" on page 58**) must be configured (*only* by a GA) to work with the WebFort Server.

To configure a registered plug-in as a GA:

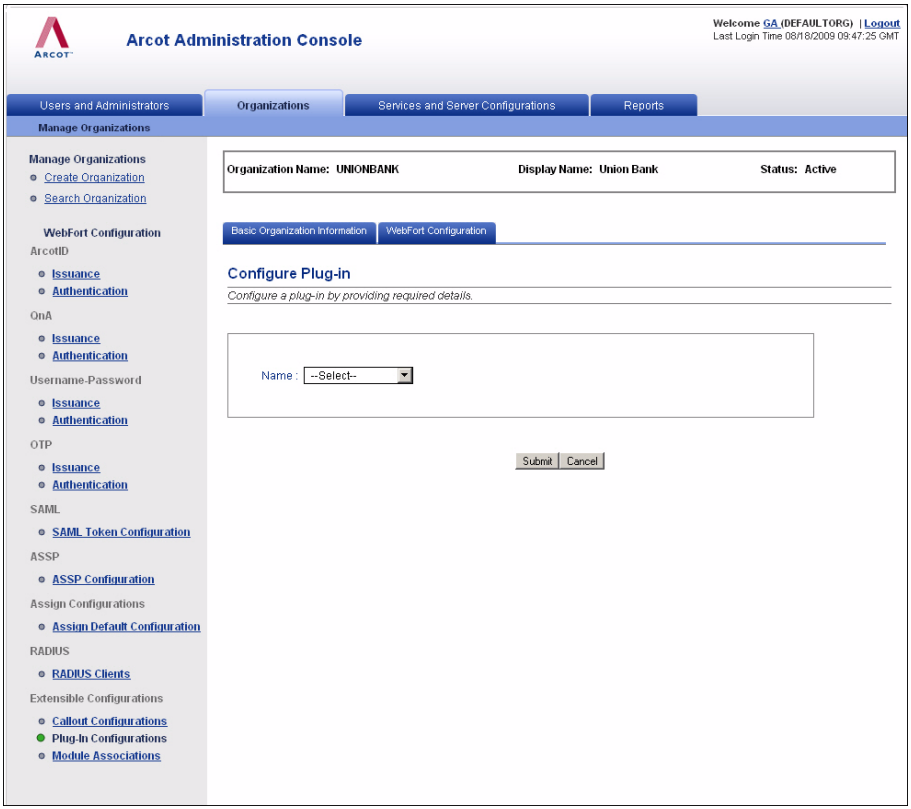
1. Ensure that you are logged in with the required GA privileges and scope.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (**Figure 5-8**.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to **Figure 5-9**) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to **Figure 5-10**) appears.
6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane (**Figure 5-11**).
7. Under **Extensible Configurations**, click the **Plug-In Configurations** link to display the Configure Plug-in page (**Figure 5-16**.)

Figure 5-16 Configure Plug-In Page



8. From the **Name** drop-down list, select the plug-in that you want to configure.

   The configuration information displayed on this screen is rendered by the Handler file that the MA uploaded while registering the plug-in.

9. Enter the plug-in configuration details.

10. Click **Submit** to configure the plug-in and save the changes.

11. Refresh *all* deployed WebFort Server instances.

    See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Associating Events

An *event* is a pre-defined operation in the WebFort system. You must define the events that will invoke a configured callout or a plug-in. Only GAs can perform this task.

To associate events (as a GA) with a configured callout or a plug-in:

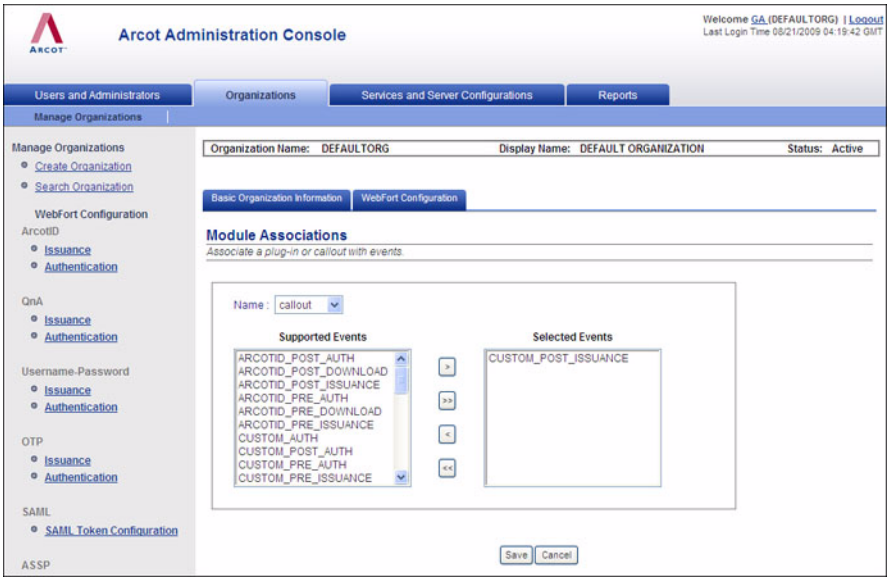
1. Ensure that you are logged in with the required GA privileges and scope.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to Figure 5-10) appears.
6. Activate the **WebFort Configuration** tab.

   The organization-specific configuration links are displayed in the tasks pane (Figure 5-11).
7. Under **Extensible Configurations**, click the **Module Associations** link to display the Module Associations page (Figure 5-16.)

Figure 5-17 Module Associations Page



8. From the **Name** drop-down list, select the module (callout or plug-in) that you want to associate with events.

9. Select the events that you want to associate from the **Supported Events** list and click the > button to add the group to the **Selected Events** list.

   The **Supported Events** list displays *all* events configured for the module, while the **Selected Events** list displays the events that you have selected for the module.

10. Click **Save** to complete the association and to save the changes.

11. Refresh *all* deployed WebFort Server instances.

    See "Refreshing or Shutting Down Instances" on page 42 for instructions on how to do this.

Updating Organization Information

By using the Administration Console, you can update the following information for an organization:

- **Organization information** that includes organization display name, description, and status, and the administrators that manage the organization (“Updating the Organization Information”)
- **WebFort-specific configurations** for the organization that include credential profiles, authentication policies, extensible configurations, and the assigned default configurations (“Updating WebFort-Specific Configurations”)

Privileges Required: To be able to update an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can update all organizations. GAs and OAs can update the information for all organizations in their scope.

Updating the Organization Information

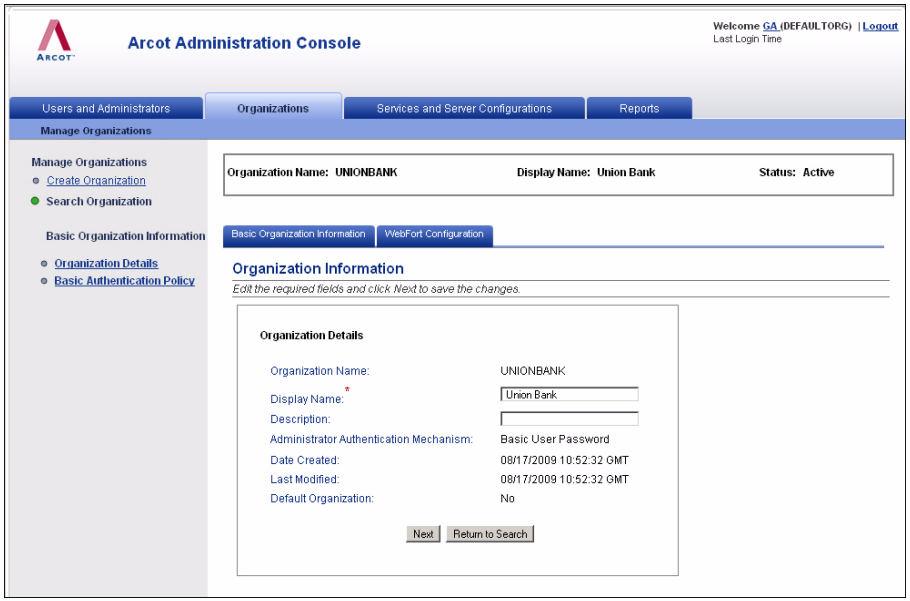
To update the basic organization information:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to Figure 5-18) appears.

Figure 5-18 Organization Information Page



6. Edit the required fields (**Display Name** and **Description**) in the **Organization Details** section.

7. Click **Next** to proceed with additional configurations:

   - If the organization was created **in the Arcot Repository** *and if* the administrators in the organization have scope to manage all organizations in the system, then the Update Administrators page (similar to Figure 5-2) appears.

     On this page, update the administrators who will manage the organization and click **Update** to save the changes and complete the process.

   - If the organization was created **in the LDAP repository**, then Edit Organization page (Figure 5-5) appears:

     I. Use the information in Table 5-3 to update the fields, as required, and click **Next** to display the page to edit the Repository Attribute Mappings (Figure 5-6).

     II. You *cannot* edit the mappings that are created when you created the organization. Click **Update** to display the Update Administrators page (Figure 5-6).

III. On the Update Administrators page, update the administrators who will manage the organization and click **Update** to save the changes and complete the process.

Updating WebFort-Specific Configurations

To update the WebFort configurations of an organization:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)
4. Enter the complete or partial information of the organization you want to search and click the **Search** button.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.
5. Under the **Organization** column, click the <*ORGANIZATION_NAME*> link for the required organization.

   The Organization Information page (similar to Figure 5-18) appears.
6. Activate the **WebFort Configuration** tab.

   The links for WebFort configurations are displayed in the task panel.
7. Refer to "Managing Organization-Specific Configurations" on page 118 for detailed information on these configurations.

Disabling Organizations

When you want to prevent all administrators of an organization from logging in to the Administration Console and end users of the organization from authenticating to your application by using WebFort mechanisms, you disable the organization.

Privileges Required: To be able to disable an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can disable all organizations. GAs and OAs can disable all organizations in their scope.

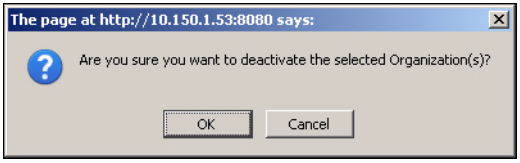
To disable one or more organizations:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.
5. Select one or more organizations that you want to disable.
6. Click **Deactivate** to disable the selected organizations.

   The message box shown in Figure 5-19 appears.

Figure 5-19 Deactivate Organization: Message



7. Click **OK** to confirm the deactivation.

Enabling Organizations

You might need to re-enable a deactivated organization. In this case, you must select the **Inactive** option while specifying the search criteria on the Search Organization page.

Privileges Required: To be able to enable an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can enable all organizations. GAs and OAs can enable all organizations in their scope.

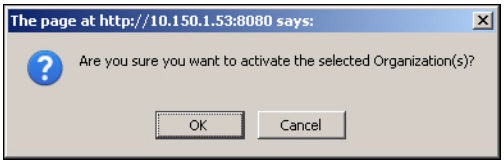
To enable a deactivated organization:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.
5. Select one or more organizations that you want to enable again.
6. Click **Activate** to enable the selected organizations.

   The message box shown in Figure 5-20 appears.

Figure 5-20 Activate Organization: Message



7. Click **OK** to confirm the activation.

Activating Organizations in Initial State

Sometimes you might start creating an organization, but not activate it. For example, you might specify the **Organization Information** and **User Data Location** on the Create Organization page, but not specify the details of the LDAP repository or the administrators who will manage the organization. In such cases, the organization is created, but is not active and is not typically visible in searches (unless you search by selecting the **Initial** option).

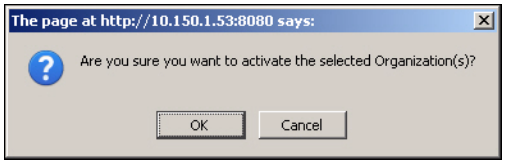
Such organizations remain in the Initial state in the system, unless you activate them. If later, you try to create a new organization with same details as an organization in Initial state, the system does not allow you to, because the organization exists.

Privileges Required: To be able to activate an organization in Initial state, you must ensure that you have the appropriate privileges and scope to do so. MA can activate all organizations. GAs and OAs can activate all organizations in their scope.

To activate an organization that is in Initial state:

1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-1.)
4. Enter the partial or complete information of the required organization and select the **Initial** option.
5. Click **Search** to display the page (similar to Figure 5-9), with all the matches for the specified criteria.
6. Select the organizations that you want to activate.
7. Click **Activate** to enable the selected organizations. The message box shown in Figure 5-21 appears.

Figure 5-21 Activate Organization: Message



8. Click **OK** to confirm the activation.

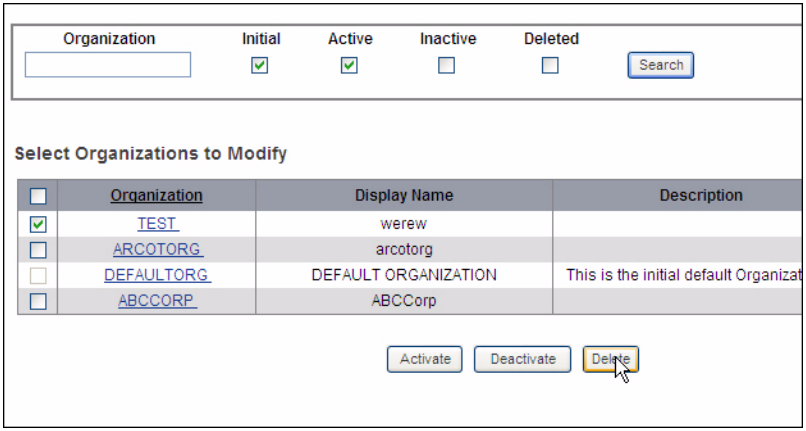
Deleting Organizations

After an organization is deleted, the administrators associated with the organization can no longer log into it by using the Administration Console and the end users who belong to this organization cannot authenticate. However, the information related to the organization is still maintained in the system. The administrator who has scope on the deleted organization can read the organization details.

Privileges Required: To be able to delete an organization, you must ensure that you have the appropriate privileges and scope to do so. MA can delete all organizations. GAs and OAs can delete all organizations in their scope.

To delete an administrator account:

Figure 5-22 Deleting Organization



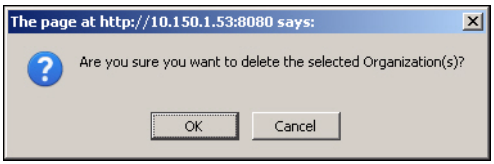
1. Ensure that you are logged in with the required privileges and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page (Figure 5-8.)
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria (similar to Figure 5-9) appears.
5. Select one or more organizations that you want to delete.

6. Click **Delete** to delete the selected organizations.

   The message box shown in Figure 5-23 appears.

Figure 5-23 Delete Organization: Message



7. Click **OK** to confirm the activation.

Chapter 6

Managing Administrators

The types of administrators and their roles and responsibilities depend on the size of your deployment. A small, single-organization deployment can have just one Master Administrator (MA) and a Global Administrator (GA) who administers the organization for end users. On the other hand, a very large multi-organization deployment can find it necessary to have multiple GAs who, based on the complexity of the deployment and the number of end users, can further delegate their organization and user management duties among several Organization Administrators (OAs) and User Administrators (UAs).

See "Supported Roles" on page 6 for information on supported administrative roles. Table 1-2 on page 11 provides a quick summary of tasks each of these administrators can perform. This chapter covers the following administrator management operations:

- Creating Administrators
- Changing Profile Information for Administrator Accounts
- Searching Administrators
- Updating Administrator Account Information
- Regenerating Activation Code
- Updating Administrator Credentials
- Disabling Administrator Accounts
- Enabling Administrator Accounts
- Deleting Administrator Accounts

> **NOTE:** In addition to all the operations discussed in this chapter, the Master Administrator has a privilege to create Custom Roles that are derived from the existing default roles supported by WebFort.

Creating Administrators

Privileges Required: An administrator can create other administrators who belong to the same level or to the lower levels in the administrative hierarchy *and* have the same scope. For example:

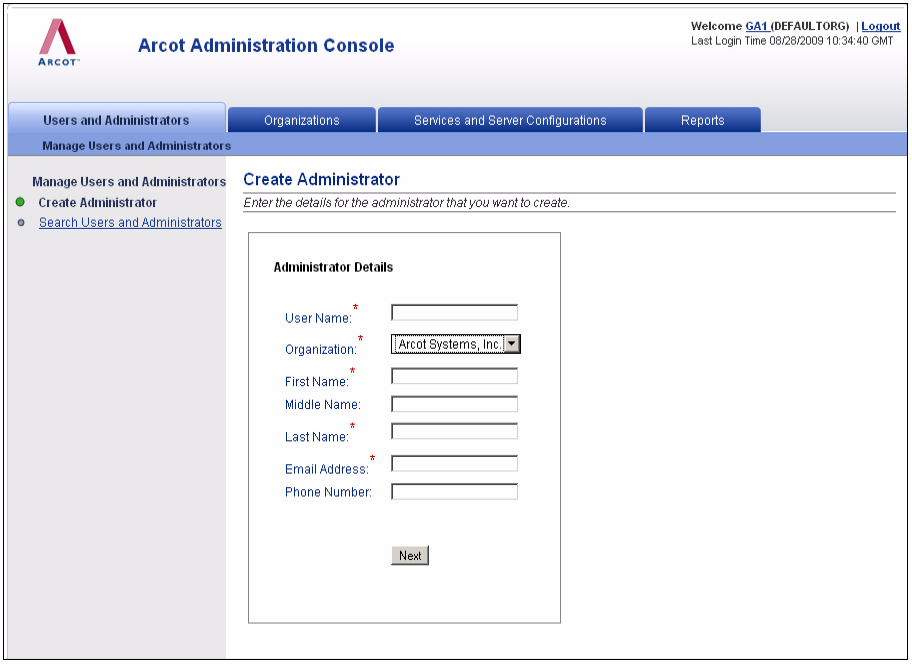
- Master Administrator can create all other types of administrators.
- Global Administrators (GAs) can create the following *within* their scope:
  - Other GAs
  - Organization Administrators (OAs)
  - User Administrators (UAs)
- OAs can create the following *within* their scope:
  - Other OAs
  - UAs
- UAs can create other UAs *within* their scope.

Creating an Account with WebFort Username-Password Credential

To create an administrator account with WebFort Username-Password credential:

1. Ensure that you are logged in with the required privileges and scope to create the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Create Administrator** link to display the Create Administrator page (Figure 6-1.)

Figure 6-1 Create Administrator: Page 1



4. In the **Administrator Details** section, enter the details of the administrator. Table 6-1 explains the fields on this page.

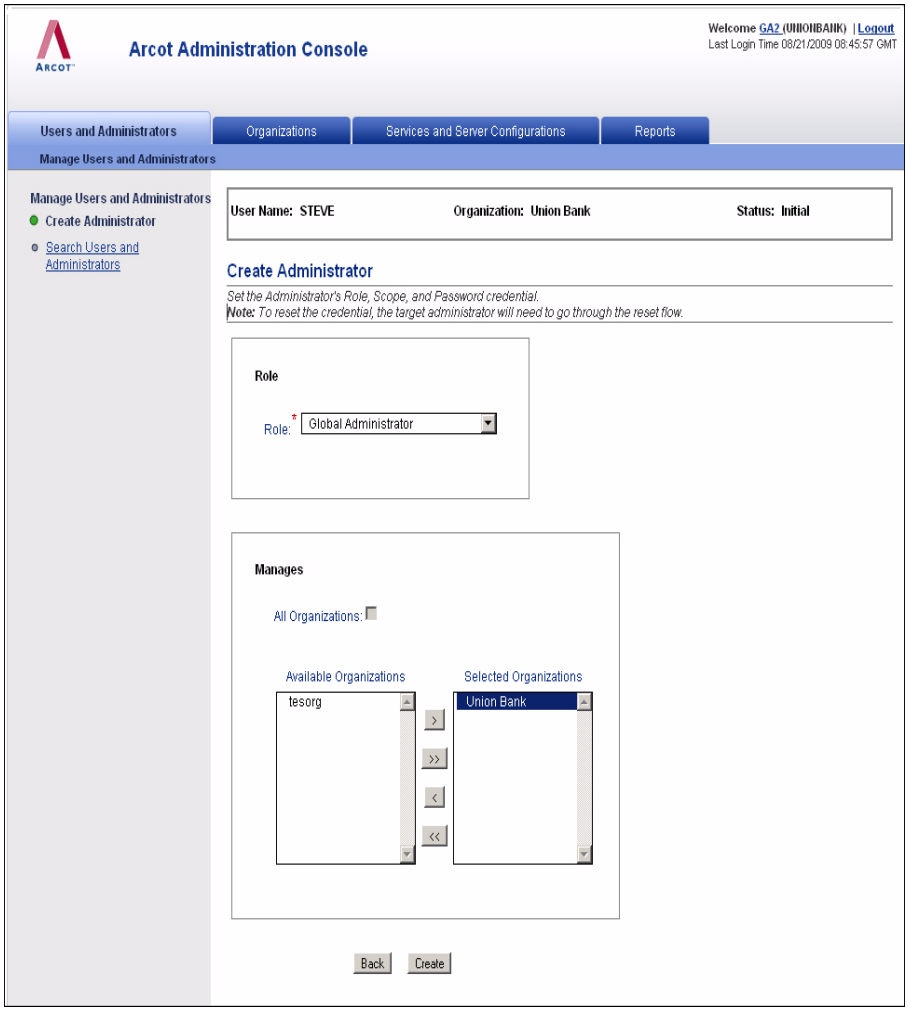
Table 6-1 Inputs for Creating Administrators

Input	Description
User Name	The unique user name for the administrator.
Organization	The display name of the organization to which the administrator will belong. **NOTE:** This is *not* the organization that this administrator will manage.
First Name	The first name of the administrator.
Middle Name (optional)	The middle name, if any, of the administrator.
Last Name	The last name of the administrator.
Email Address	The email address of the administrator.
Phone Number (optional)	The phone number to contact the administrator.

5. Click **Next** to proceed.

   The next page (Figure 6-2) to Create Administrator appears.

Figure 6-2 Create Administrator: Page 2



6. On this page:

   - Specify the role of the new administrator from the **Role** drop-down list.
   - In the **Manages** section, select the organizations that the administrator will have scope on:

- Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.

  or

- Select the required organizations from the **Available Organizations** list and click the > button to add these organization to the **Selected Organizations** list.

  The **Available Organizations** list displays *all* the organizations that are available in the scope of the administrator creating this new account. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.

7. Click **Create** to save the changes, create the account, and activate it.

   You will see a success message that indicates that the administrator was created successfully. As a part of this message, you will also see the activation code that the new administrator must use to log in for the first time. For example, you will see the message similar to the following:

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

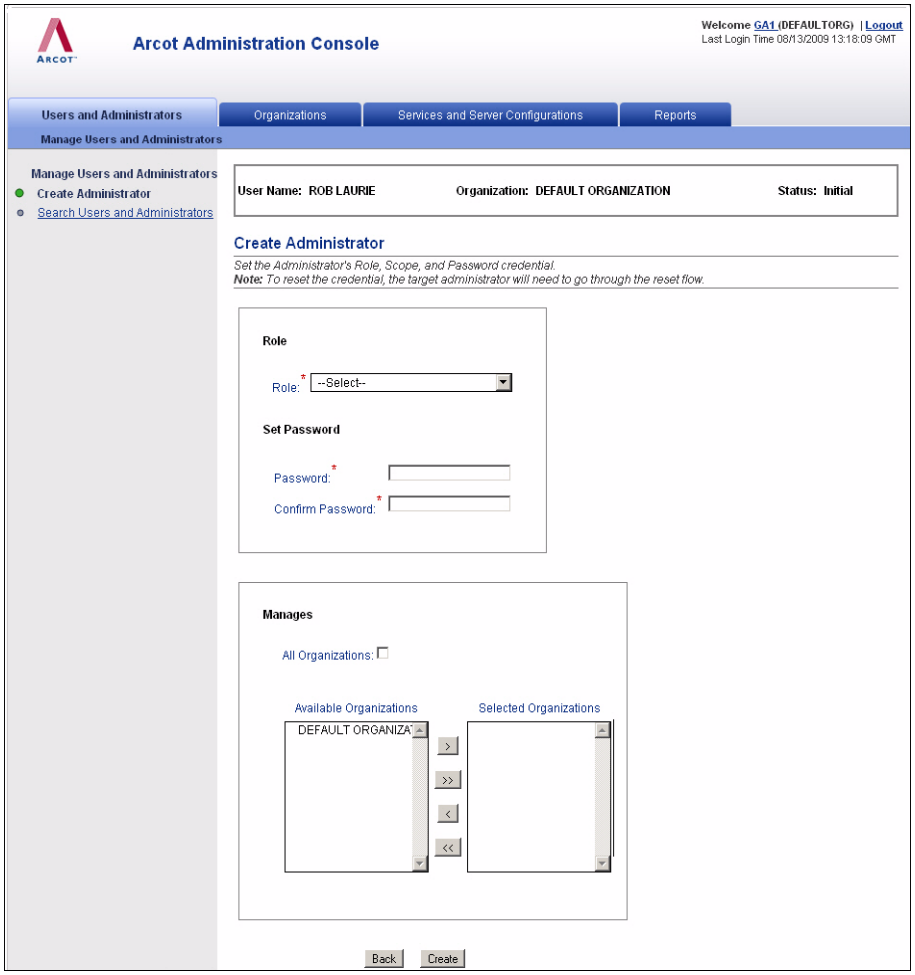
8. Note down the numeric activation code that you see as a part of the success message and communicate it to the administrator.

Creating an Account with Basic Username-Password Credential

If you are creating an administrative account with basic Username-Password credential, then:

1. Complete **Step 1** through **Step 5**, as discussed in section, **"Creating an Account with WebFort Username-Password Credential" on page 146** to display the page (**Figure 6-3**) to Create Administrator appears.

Figure 6-3 Create Administrator: Page 2



2. On this page:
   - Specify the role of the new administrator from the **Role** drop-down list.
   - Enter the password for the administrator account in the **Password** and **Confirm Password** fields.
   - In the **Manages** section, select the organizations that the administrator will have scope on:
3. Click **Create** to save the changes, create the account and activate it.
4. Communicate the new password to the administrator.

Changing Profile Information for Administrator Accounts

The profile information for an account includes:

- Personal information (first, middle, and last names and contact information)
- Password for the account
- Preferred organization (the organization that will be selected by default in the **Organization** fields for all administrator-related tasks that you might perform in future.)

Privileges Required: An administrator can change their account's profile information at any time. However, they do not have any privileges to change this information for any other administrative account.

For Accounts with WebFort Username-Password Credential

To change the administrator profile information for your account, if it was created with WebFort Username-Password credential:

1. Ensure that you are logged in to your account.
2. In the **Header** frame, click the <*ADMINISTRATORNAME*> link to display the My Profile page (Figure 6-5.)
3. This page contains the following three sections:
   - **Personal Information**

     This section enables you to change the first name, last name, middle name, email ID, and the phone number.
   - **Change Password**

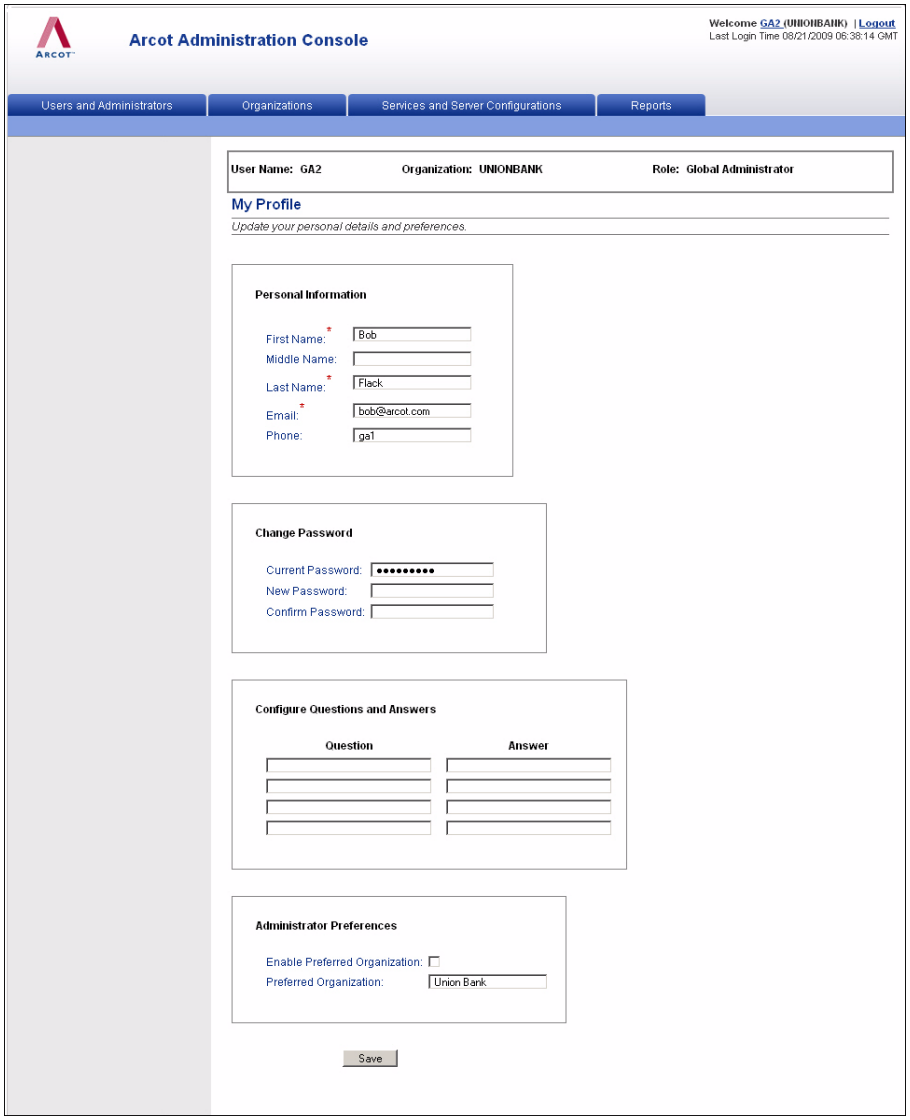
     This section enables you to set a new password.
   - **Questions and Answers**

     In this section you can set the questions that you will be prompted to answer for resetting your password, for example, **In Case You Forgot Your Password**.

- **Administrator Preferences**

  In this section you can set the default organization that the administrator will handle.

Figure 6-4 My Profile Page



4. Edit the required settings in the sections on this page:

   a. Edit the fields in the **Personal Information** section, as needed.

b. In the **Configure Questions and Answers** section, specify distinct **Question** and its corresponding **Answer**.

IMPORTANT: All the questions in this section *must* be set. You *cannot* repeat a question or any of the answers. Also, any question in the section *must not* match with any of the answers that you set in this section.

c. If you want to change the current password, then in the **Change Password** section enter the **Current Password** and specify new password in the **New Password** and **Confirm Password** fields.

d. In the **Administrator Preferences** section, select the **Enable Preferred Organization** option, and select an organization from the **Preferred Organization** list. This organization will be selected for all administrator-related tasks that you perform from now on.

5. Click **Save** to change the profile information.

For Accounts with Basic Username-Password Credential

To change the administrator profile information for your account, if it was created with basic Username-Password credential:

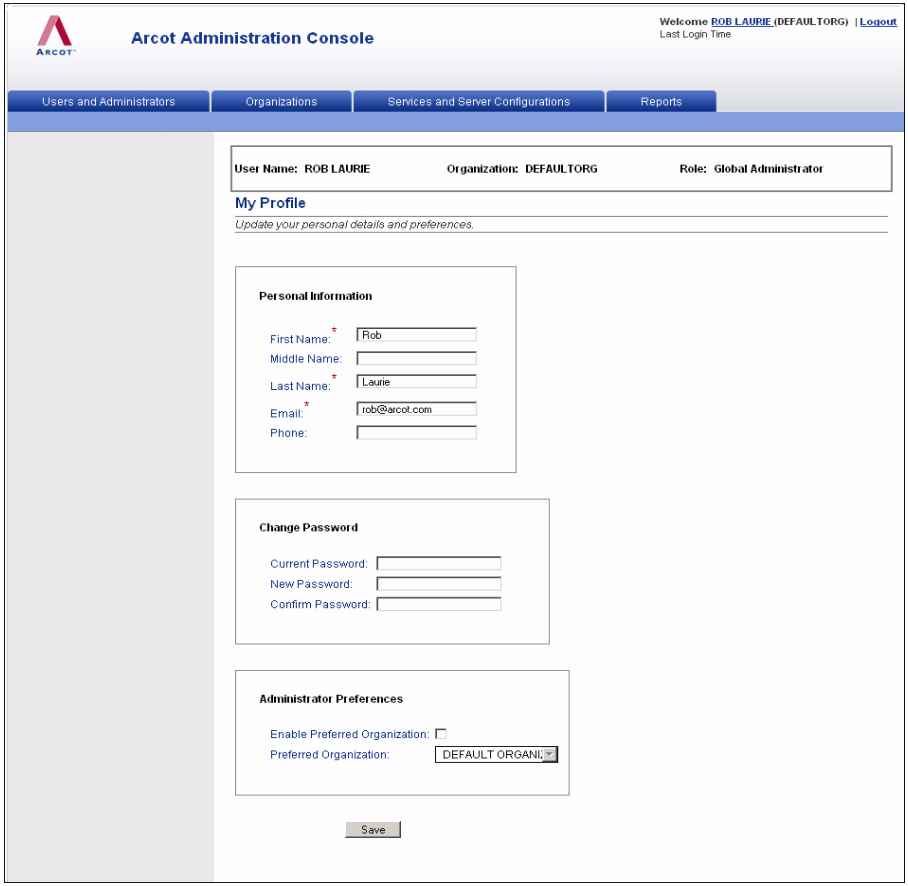
1. Ensure that you are logged in to your account.
2. In the **Header** frame, click the <*ADMINISTRATORNAME*> link to display the My Profile page (Figure 6-5.)
3. This page contains the following three sections:
   - **Personal Information**

     This section enables you to change the first name, last name, middle name, email ID, and the phone number.
   - **Change Password**

     This section enables you to set a new password.
   - **Administrator Preferences**

     In this section you can set the default organization that the administrator will handle.

Figure 6-5 My Profile Page



4. Edit the required settings in the sections on this page:

   a. Edit the fields in the **Personal Information** section, as needed.

   b. If you want to change the current password, then in the **Change Password** section enter the **Current Password** and specify new password in the **New Password** and **Confirm Password** fields.

   c. In the **Administrator Preferences** section, select the **Enable Preferred Organization** option, and select an organization from the **Preferred Organization** list. This organization will be selected for all administrator-related tasks that you perform from now on.

5. Click **Save** to change the profile information.

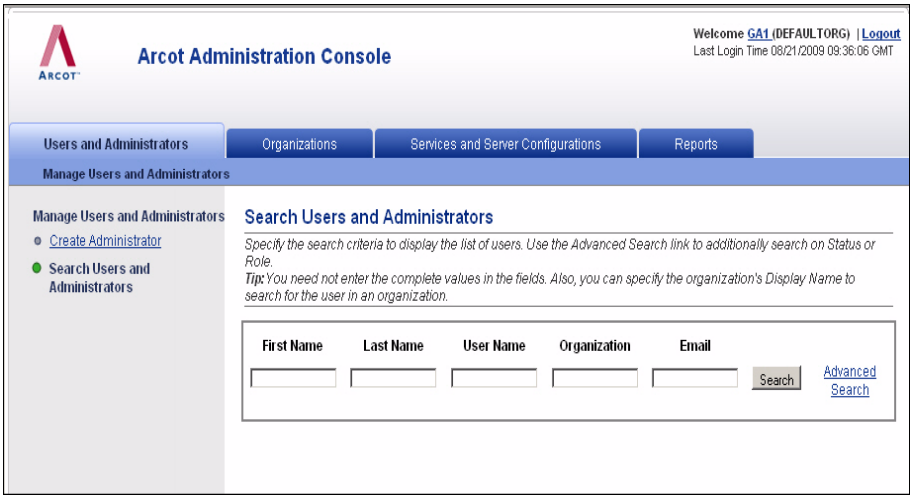
Searching Administrators

Privileges Required: As long as you do not need to update, activate, or deactivate an administrative account, you do not need privileges to search. However, you *must* have the scope over the organizations that the administrator belongs to. For example, a UA can search for administrators in the target organization *if* that organization is in their purview.

To search for administrators with the specified criteria:

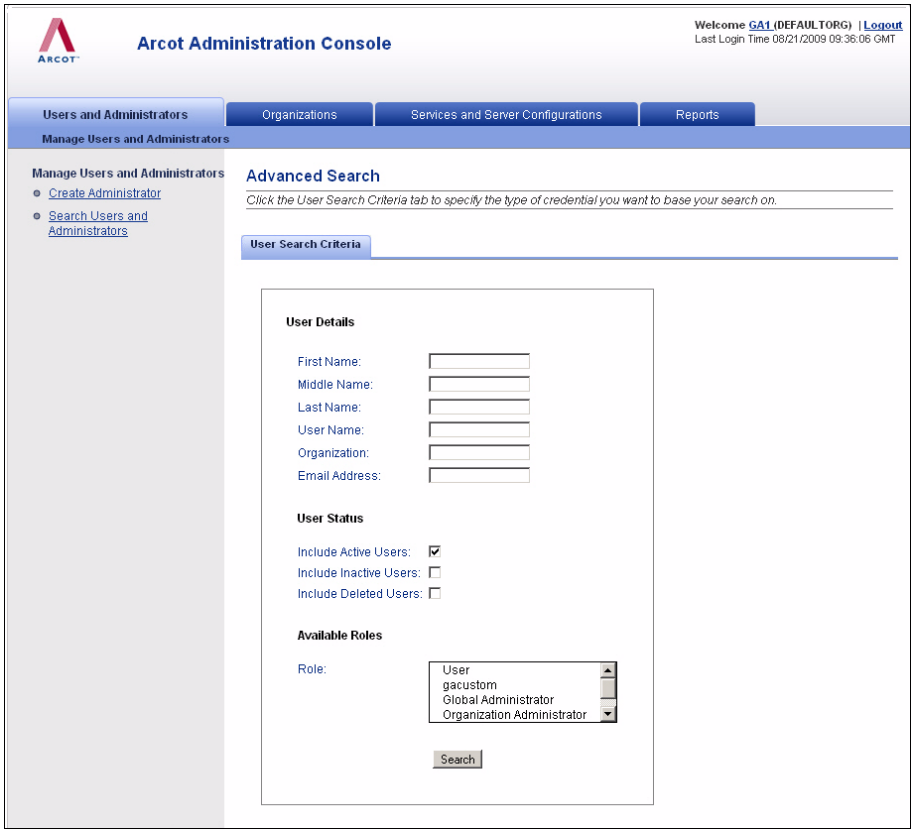
1. Ensure that you are logged in with the required privileges and scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 6-6.)

Figure 6-6 Search Users and Administrators Page



4. Specify the search criteria to display the list of administrators. You can:
   - Search for administrators by specifying the partial or complete information of the administrator in the fields on this page.
   - Search for administrators by specifying the organization's Display Name.
   - Search for administrators by not specifying any criteria and just clicking **Search**.
   - Click the **Advanced Search** link to display the Advanced Search page (Figure 6-7) to search for the required administrators by specifying their Status or Role.

Figure 6-7 Advanced Search Page



5. Specify the required details of the administrators and click **Search**.

   A list of administrators matching the search criteria appears.

Updating Administrator Account Information

Privileges Required:

To be able to update an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can update any account. GAs can update all the accounts (including other GAs), *except* for the MA account, in their scope. The OAs can update all other OA accounts and the UA accounts in their purview, while UAs can only update the accounts of their peers within their scope.

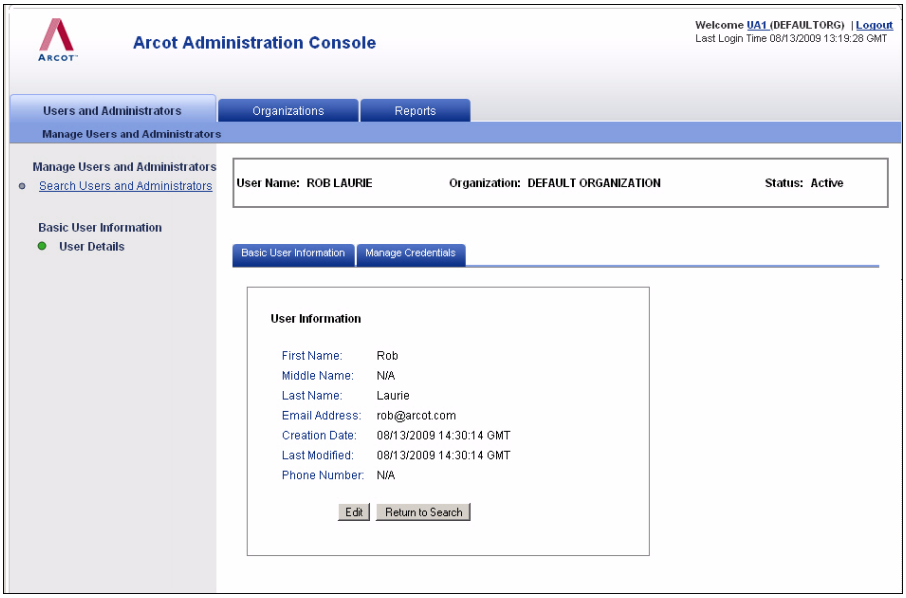
To update an administrator's basic details (such as first, middle, and last names, contact information) and their administrative role, password, and management scope:

1. Ensure that you are logged in with the required privileges to update the administrative user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the corresponding page (Figure 6-6.)
4. Enter the partial or complete information of the administrator whose account you want to update (as discussed in the preceding section) and click **Search**.

   A list of administrators matching the search criteria appears.
5. Click the <*user name*> link of the administrator whose account you want to edit.

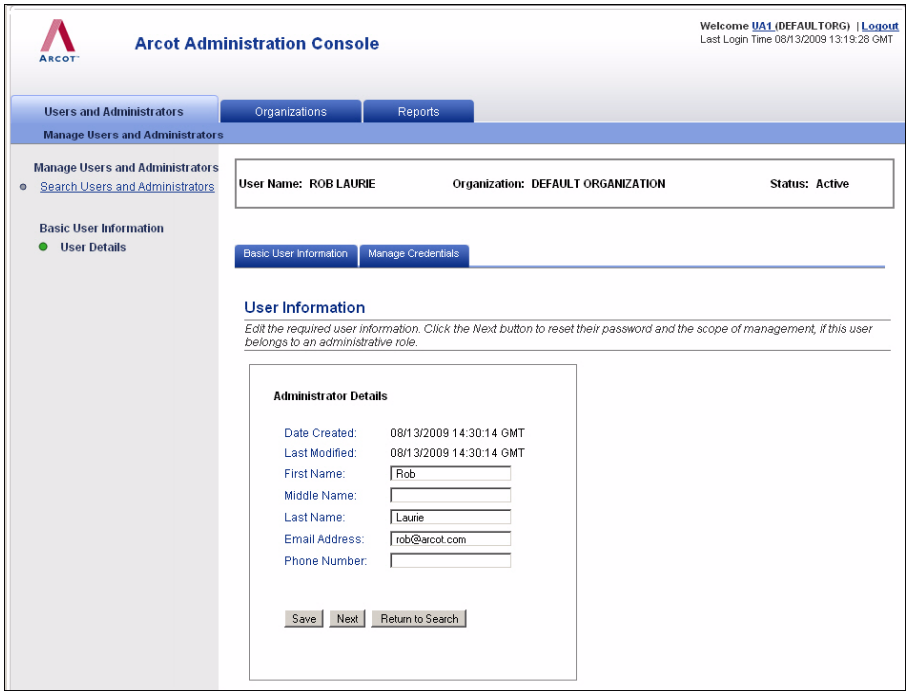
   The Basic User Information page similar to Figure 6-8 appears.

Figure 6-8 Basic Administrator Information Page



6. Click **Edit** to change the administrator information on this page, as shown in the following figure (Figure 6-9.)

Figure 6-9 User Information Page

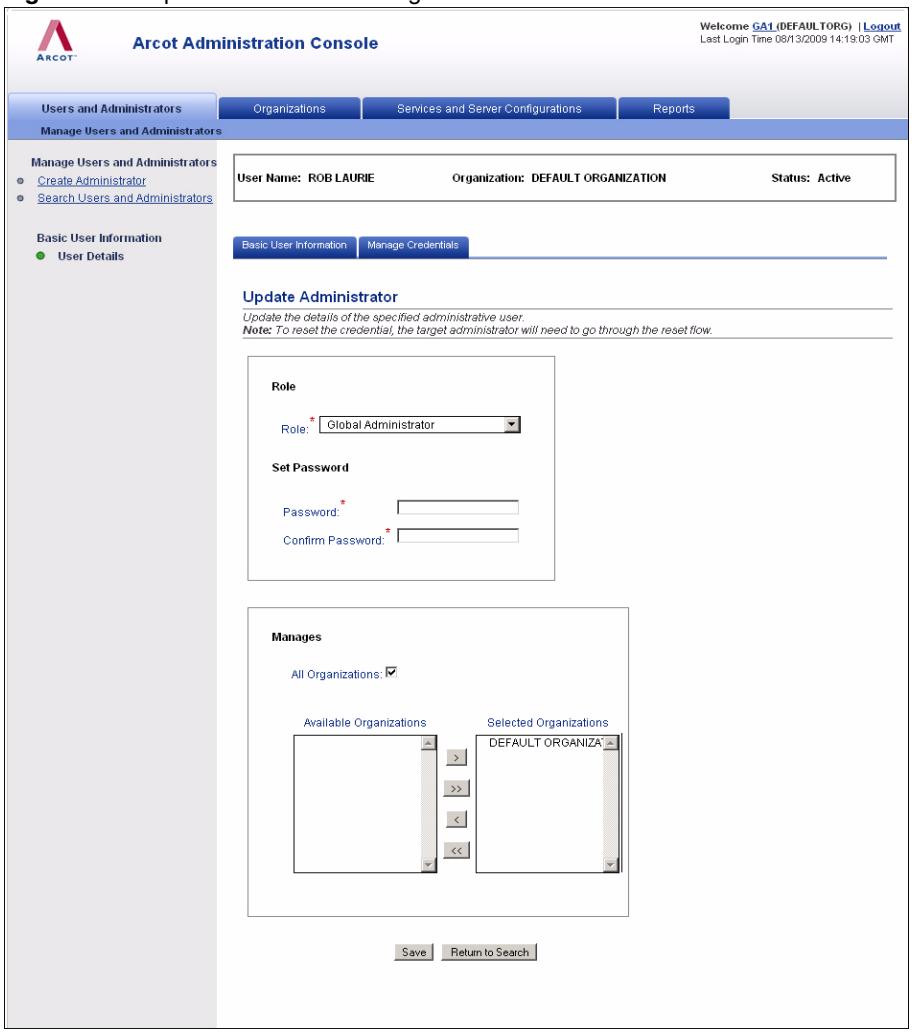


7. In the **Administrator Details** section, edit the required fields (**First Name**, **Middle Name**, **Last Name**, **Email Address**, and **Phone Number**.)

8. You can either click **Save** to save the changes made and return to the User Information page, *or* you can click **Next** to proceed with additional configurations.

   If you click **Next**, then the Update Administrator page (Figure 6-10) appears.

Figure 6-10 Update Administrator Page



9. Edit the required fields on this page:
   - Change the role of the administrator using the **Role** drop-down list.
   - **Set Password** for the administrator.
   - Select the organizations that administrator will manage. You can also remove the organization from the scope by moving the specific organization from **Selected Organizations** to **Available Organizations**.
10. Click **Save** to save the updates.

Regenerating Activation Code

NOTE: This information is applicable for WebFort Username-Password mechanism only.

If your organization is using WebFort Username-Password as the authentication mechanism, and if any of the administrators forget their activation code that they need to log in to their account, they will contact you for new activation code. In this case, you must regenerate the new activation code and communicate the same to them.

Privileges Required:

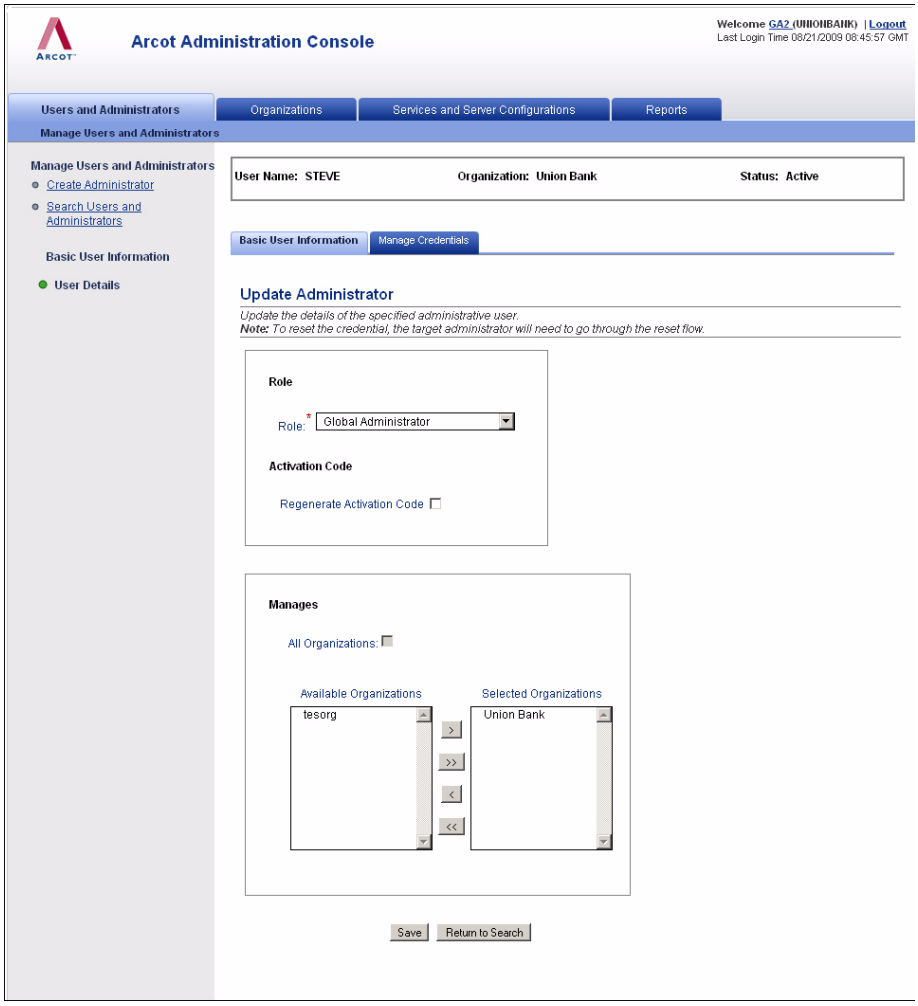
To be able to regenerate an activation code, you must ensure that you have the appropriate privileges and scope to do so. MA can regenerate the activation code for any administrator. GAs can update all the accounts (including other GAs), *except* for the MA account, in their scope. The OAs can update all other OA accounts and the UA accounts in their purview, while UAs can only update the accounts of their peers within their scope.

To do so:

1. Ensure that you are logged in with the required privileges to update the administrative user.
2. Complete **Step 2** through **Step 8** in section, **"Updating Administrator Account Information" on page 157** to display the Update Administrator page (**Figure 6-11**.)
3. In the **Activation Code** section, select the **Regenerate Activation Code** option.
4. Click **Save** to generate the activation code.

   The success message will notify you the new activation code.
5. Communicate the new OTP to the administrator.

Figure 6-11 Update Administrator Page



Updating Administrator Credentials

Administrators, like end users, must use credentials to authenticate to the system. WebFort supports QnA, Username-Password, and OTP credentials out of the box for administrators. You will need to use the Credential Details page (**Figure 6-12**) to update the credentials of an administrator. Through this page, you can enable or disable the credential, or extend its validity.

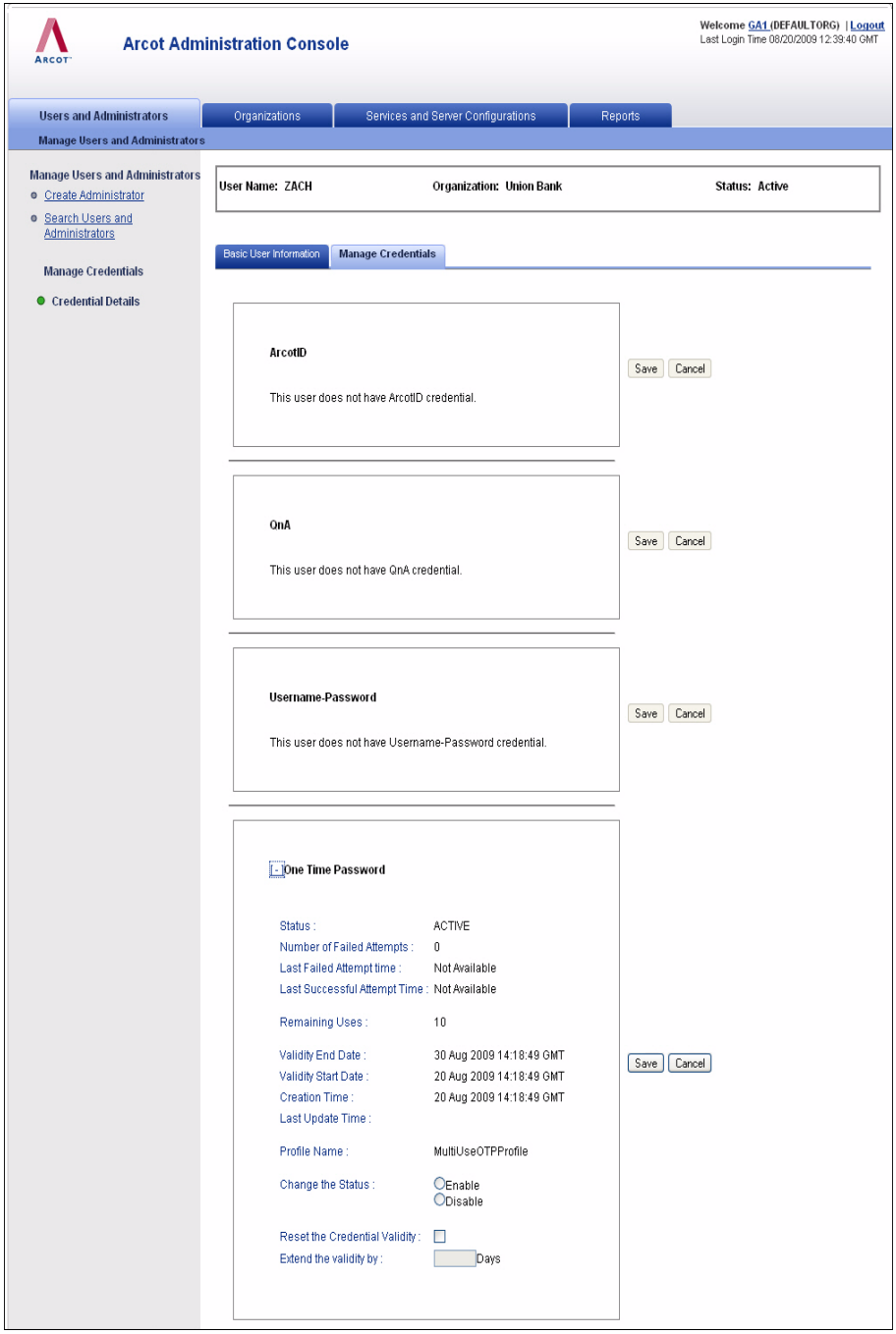
Privileges Required:

To be able to update an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA *cannot* manage any credentials. GAs can manage the credentials for all accounts (including other GAs), *except* for the MA account, in their scope. The OAs can manage all other OA account credentials and the UA accounts in their purview, while UAs can only manage the credentials for their peers within their scope.

To update the credential information of an administrator:

1. Ensure that you are logged in with the required privileges to update the administrative user credentials.
2. Complete **Step 2 on page 157** through **Step 5 on page 157** in section, **"Updating Administrator Account Information" on page 157**.
3. Activate the **Manage Credentials** tab to display the Credential Details page (**Figure 6-12**.)
4. Expand the required credential section by clicking the **[+]** sign preceding it.
5. Change the settings of the required credentials. You can change the following credential settings by using this page:
   - Status of the credential
   - Extend the credential validity
6. Click the **Save** button corresponding to the credential you have changed.

Figure 6-12 Credential Details Page



Disabling Administrator Accounts

To prevent an administrator from logging in to their account for security reasons, you can disable their account instead of deleting it. If you disable an administrator account, the administrator is locked out of their account, and cannot log in unless the account is re-enabled again.

Privileges Required:

To be able to disable an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can disable any account, while GAs can disable all accounts (including other GAs), *except* the MA account, in their scope. The OAs can disable all other OA accounts and the UA accounts in their purview, while UAs can only disable the accounts of their peers within their scope.

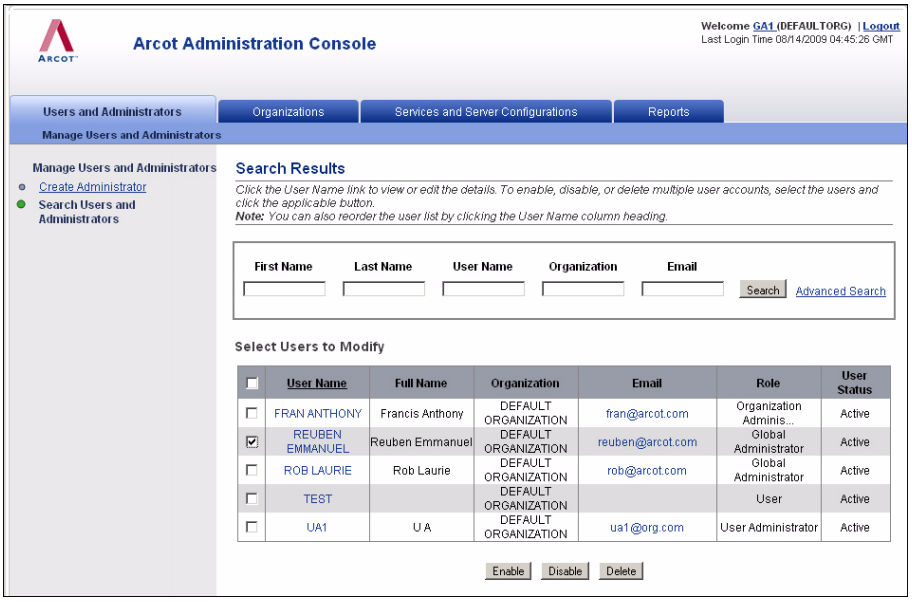
To disable an administrator account:

1. Ensure that you are logged in with the required privileges to disable the administrative user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 6-6.)
4. Enter the partial or complete information of the administrator whose account you want to disable and click **Search**.

   You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (GA, OA, or UA).

   The Search Results page (Figure 6-13) appears, with all the matches for the specified criteria.

Figure 6-13 Search Results



5. Select one or more administrators whose accounts you want to disable.
6. Click **Disable** to disable the selected administrator account.

Enabling Administrator Accounts

You might need to enable a disabled account. For example, you might disable an administrator account in case the administrator is on long vacation. This helps to prevent unauthorized access to that administrator's account.

You cannot search directly for disabled accounts by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You *must* perform an **Advanced Search** for such users and use the **Include Inactive Users** option to search.

Privileges Required:

To be able to enable an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can enable any account, while GAs can enable all accounts (including other GAs), *except* the MA account, in their scope. The OAs can enable all other OA accounts and the UA accounts in their purview, while UAs can only enable the accounts for their peers within their scope.

To enable a disabled administrator account:

1. Ensure that you are logged in with the required privileges to enable the administrative user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 6-6.)
4. Click the **Advanced Search** link to search for users based on their status (active or inactive).

   The Advanced Search page (Figure 6-7) appears.
5. Enter the partial or complete information of the administrator in **User Account** section.
6. In the **User Status** section, select the **Include Inactive Users** option to search for all inactive administrator accounts.
7. Click **Search** to display the list of all administrators matching the search criteria.
8. Select the administrators whose account you want to enable.
9. Click **Enable** to enable the administrator accounts.

Deleting Administrator Accounts

After an administrator account is deleted, all privileges associated with the administrator account are permanently deleted. As a result, the administrator can no longer log in to Administration Console. However, their account information and credentials *are not* removed from the system.

You cannot create a new administrator account with the same name as a previously deleted administrator account in the same organization, however you can create in different organization.

Privileges Required: To be able to delete an administrative user account, you must ensure that you have the appropriate privileges and scope to do so. MA can delete any account, while GAs can delete all accounts (including other GAs), *except* the MA account, in their scope. The OAs can delete all other OA accounts and the UA accounts in their purview, while UAs can only delete their peers within their scope.

To delete an administrator account:

1. Ensure that you are logged in with the required privileges to delete the administrative user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 6-6.)
4. Enter the partial or complete information of the administrator whose account you want to delete and click **Search**.

   You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (GA, OA, or UA).

   The Search Results page (similar to Figure 6-13) appears, with all the matches for the specified criteria.
5. Select one or more administrators whose accounts you want to delete.
6. Click **Delete**.

   NOTE: Even though you have deleted the administrator, their account information is still maintained in the database.

Chapter 7

Managing Users

WebFort works with your application to manage strong authentication for administrators and end users. However, WebFort *does not* allow you to create the end users directly through the Administration Console. For the purpose of migrating existing users and creating new users in WebFort database as bulk operations, WebFort provides extensive SDKs and Web Services. This process of creating users in WebFort is known as *migration*.

> **NOTE:** See section, "Enrollment Workflows" in Chapter 2 of the *Arcot WebFort 6.0 Developer's Guide* to understand the workflows for user enrollment.

Managing user information is a critical part of maintaining a secure system. The end user management operations supported by WebFort for this purpose include:

- Searching Users
- Updating User Information
- Promoting Users to Administrators
- Updating User Credential Information
- Disabling User Accounts
- Enabling User Accounts
- Deleting User Accounts

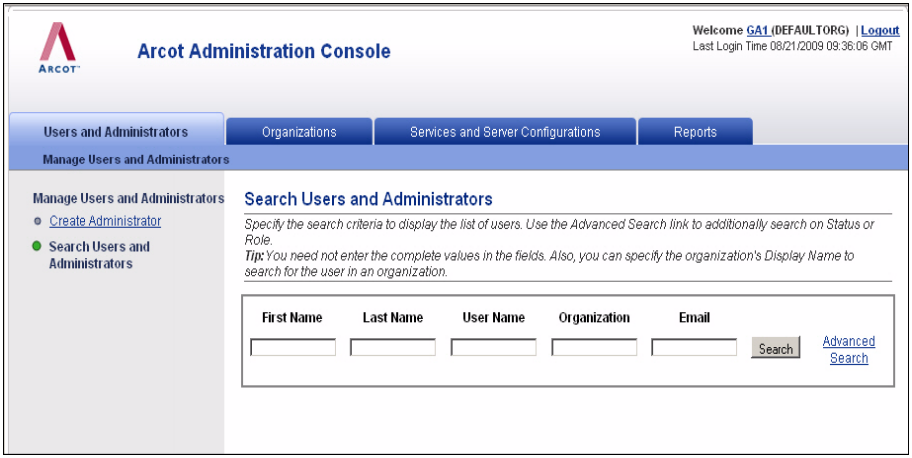
Searching Users

Privileges Required: As long as you do not need to update, activate, or deactivate a user account, you do not need privileges to search. However, you *must* have the scope over the organization that the target user belongs to. For example, a GA from one organization can search for users in another organization, *if* that organization is in their purview.

To search for users with the specified criteria:

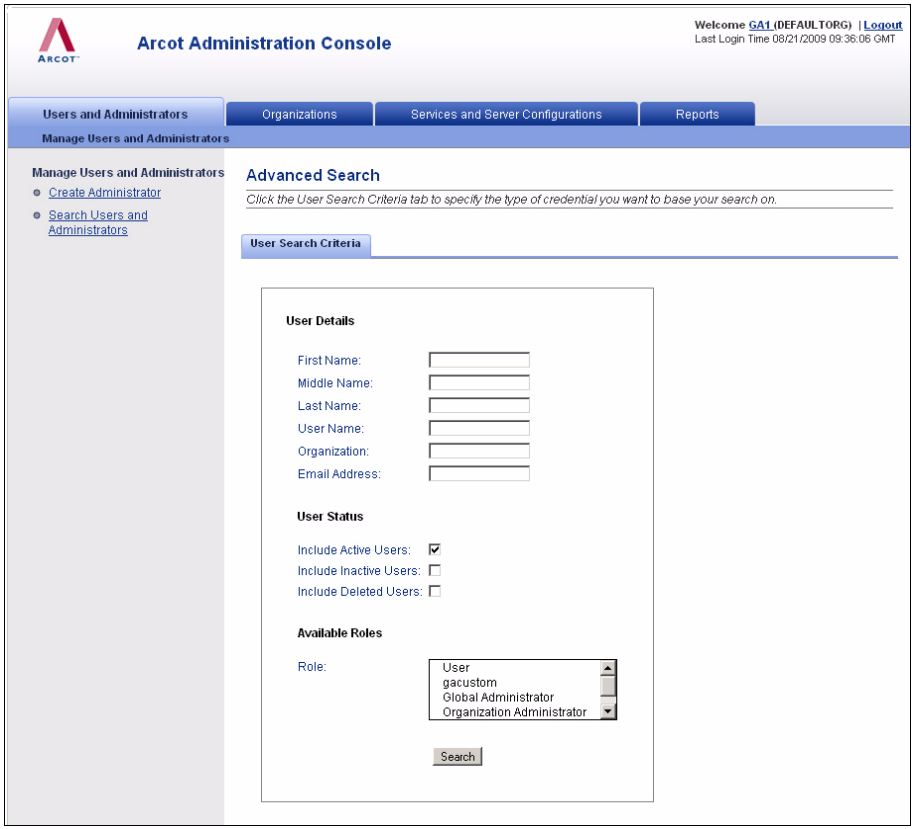
1. Ensure that you are logged in with the appropriate scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 7-1.)

Figure 7-1 Search Users and Administrators Page



4. Specify the search criteria to display the list of users. You can:
   - Search for users by specifying the partial or complete information of the user in the fields on this page.
   - Search for users by specifying the organization's Display Name.
   - Search for users by not specifying any criteria and just clicking **Search**.
   - Click the **Advanced Search** link to display the Advanced Search page (Figure 7-2) to search for users by specifying their Status or Role.

Figure 7-2 Advanced Search Page



5. Specify the required details of the users and click **Search**.

   A list of users matching the search criteria appears.

Updating User Information

Privileges Required: To be able to update a user account's settings, you must ensure that you have the appropriate privileges and scope to do so. MA can update any user account. GAs can update all user accounts in their scope. The OAs and UAs can update the user accounts in their purview.

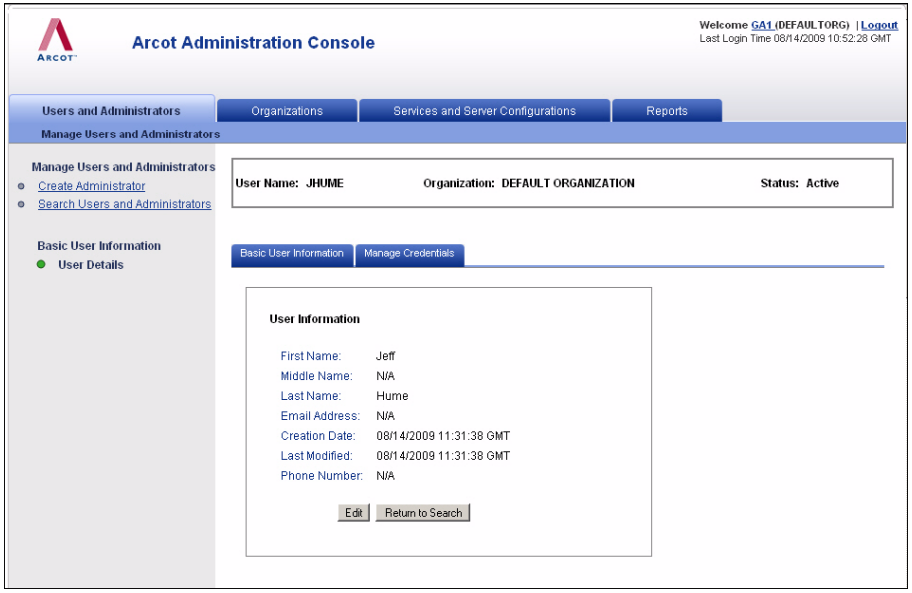
To update a user's basic details (such as first, middle, and last names, contact information):

1. Ensure that you are logged in with the required privileges and scope to update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 7-1.)
4. Enter the partial or complete information of the user whose account you want to update (as discussed in the preceding section) and click **Search**.

   A list of administrators matching the search criteria appears.
5. Click the <*user name*> link of the user whose account you want to edit.

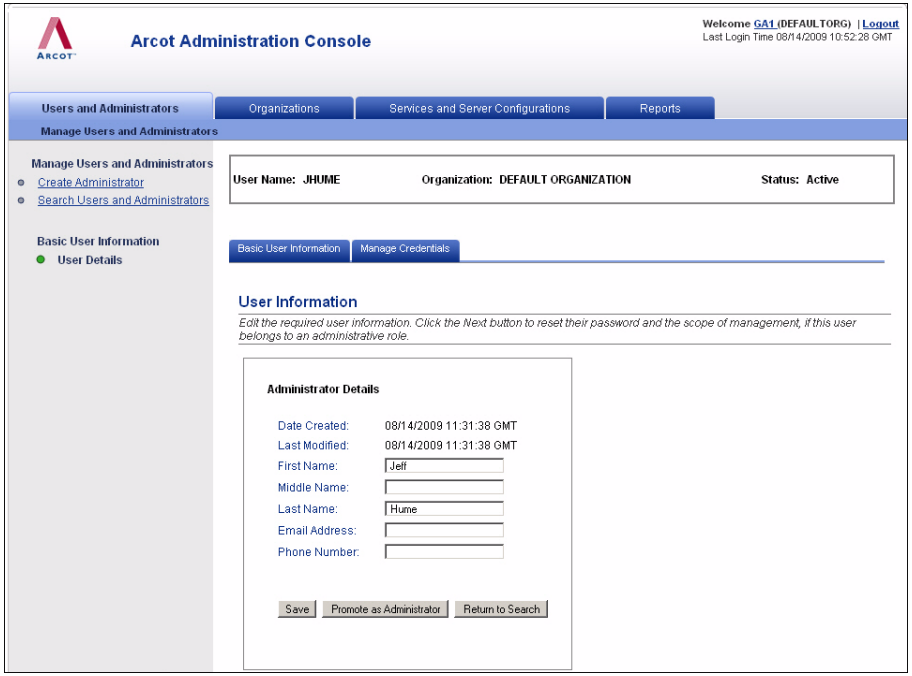
   The Basic User Information page similar to Figure 7-3 appears.

Figure 7-3 Basic User Information Page



6. Click **Edit** to change the user information on this page, as shown in Figure 7-4.

Figure 7-4 User Information Page



7. Edit the required fields (**First Name**, **Middle Name**, **Last Name**, **Email Address**, and **Phone Number**.)

8. Click **Save** to save the changes made and return to the User Information page.

Promoting Users to Administrators

Privileges Required: To be able to promote a user to an administrator, you must ensure that you have the appropriate privileges and scope to do so. MA can promote any user. GAs, OAs, and UAs can promote the users in their scope.

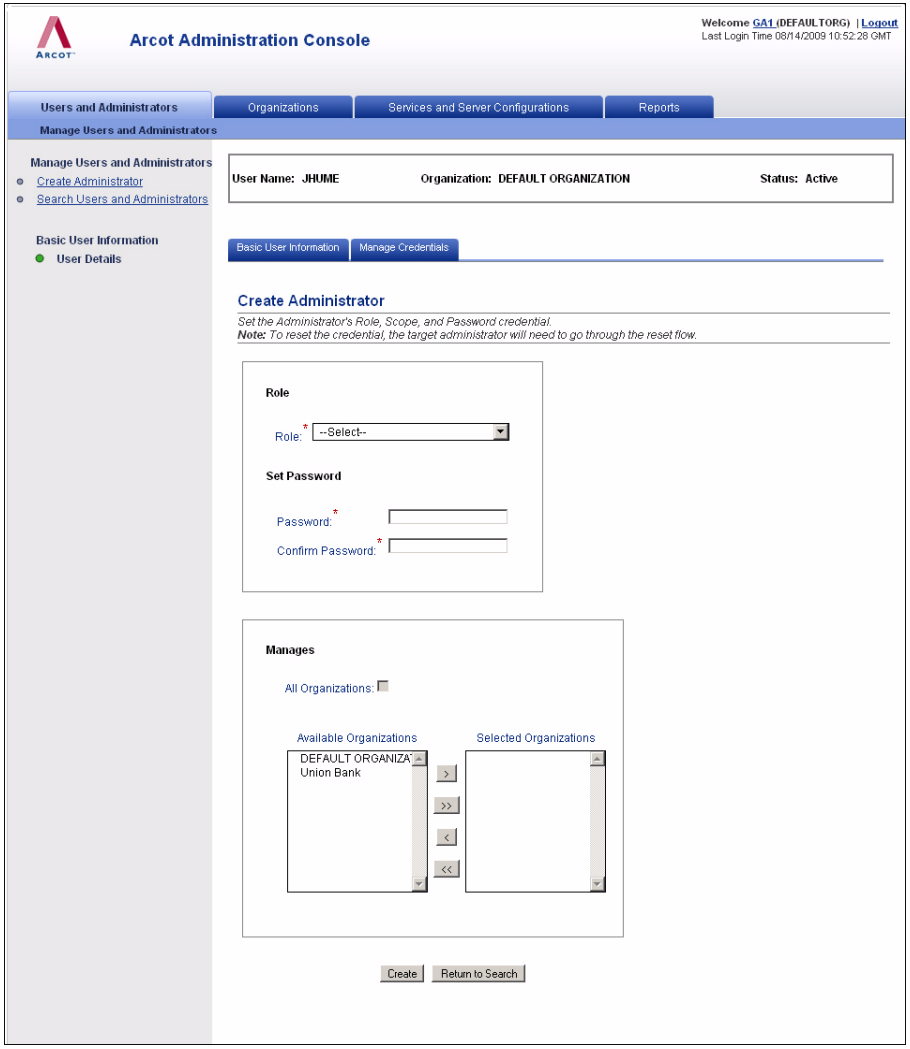
To update a user's administrative role, password, and management scope:

1. Ensure that you are logged in with the required privileges and scope to update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 7-1.)
4. Enter the partial or complete information of the user whose account you want to update (as discussed in the preceding section) and click **Search**.

   A list of users matching the search criteria appears.
5. Click the <*user name*> link of the user whose account you want to edit.

   The Basic User Information page similar to Figure 7-3 appears.
6. Click **Edit** to open the editable User Information page (similar to Figure 7-4.)
7. If the user's **Email Address** is not specified, enter the same. This attribute is mandatory for administrators.
8. Click **Promote as Administrator** to display the Create Administrator page (Figure 7-5.)

Figure 7-5 Create Administrator Page



9. On this page:
   - Specify the role of the new administrator from the **Role** drop-down list.
   - Enter the password for the administrator account in the **Password** and **Confirm Password** fields.
   - In the **Manages** section, select the organizations that the administrator will have scope on:

- Select the **All Organizations** option, if you want the administrator to manage all current and future organizations in the system.

  or

- Select the required organizations from the **Available Organizations** list and click the > button to add these organization to the **Selected Organizations** list.

  The **Available Organizations** list displays *all* the organizations that are available in the scope of the logged in administrator. The **Selected Organizations** displays the list of organizations that you have selected for the administrator to manage.

10. Click **Create** to save the changes and create and activate the administrator account.

NOTE: If the user being promoted is in the organization that uses WebFort User Password authentication, then an Activation Code is generated after you click **Create**. This will be used by the promoted administrator to log in to the Administration Console.

Updating User Credential Information

Users, must use credentials to authenticate to the system. WebFort supports ArcotID, QnA, Username-Password, and OTP credentials out of the box.

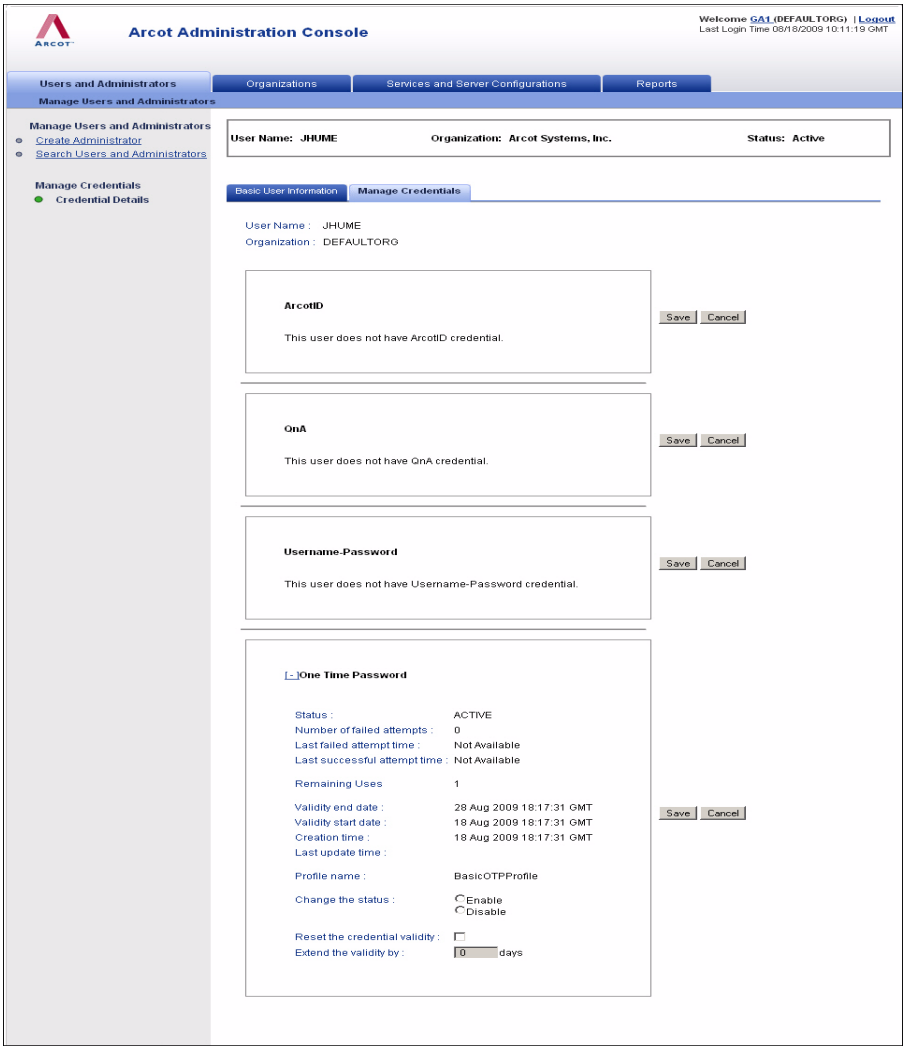
You will need to use the Credential Details page (Figure 7-6) to update the credentials of user. Through this page, you can enable or disable the credential, or extend its validity.

Privileges Required: To be able to update the credentials of a user, you must ensure that you have the appropriate privileges and scope to do so. MA *cannot* manage any credentials. GAs can manage the credentials for all user accounts (including other GAs) within their scope. The OAs and UAs can manage credentials for all users in their purview.

To update the credential information of user:

1. Ensure that you are logged in with the required privileges and scope to update the user credentials.
2. Complete Step 2 on page 172 through Step 5 on page 172 in section, "Updating User Information" on page 172.
3. Activate the **Manage Credentials** tab to display the Credential Details page (Figure 7-6.)
4. Expand the required credential section by clicking the `[+]` sign preceding it.
5. Change the settings of the required credentials. You can change the following credential settings by using this page:
   - Status of the credential
   - Extend the credential validity
6. Click the **Save** button corresponding to the credential you have changed.

Figure 7-6 Credential Details Page



Disabling User Accounts

To prevent a user from logging in to their account for security reasons, you can disable their account instead of deleting it. If you disable user account, then they are locked out of their account, and cannot log in unless the account is re-enabled again.

Privileges Required:

To be able to disable a user account, you must ensure that you have the appropriate privileges and scope to do so. MA can disable any user account, while GAs can disable all user accounts (including other GAs) within their scope. The OAs and UAs can disable all user accounts in their purview.

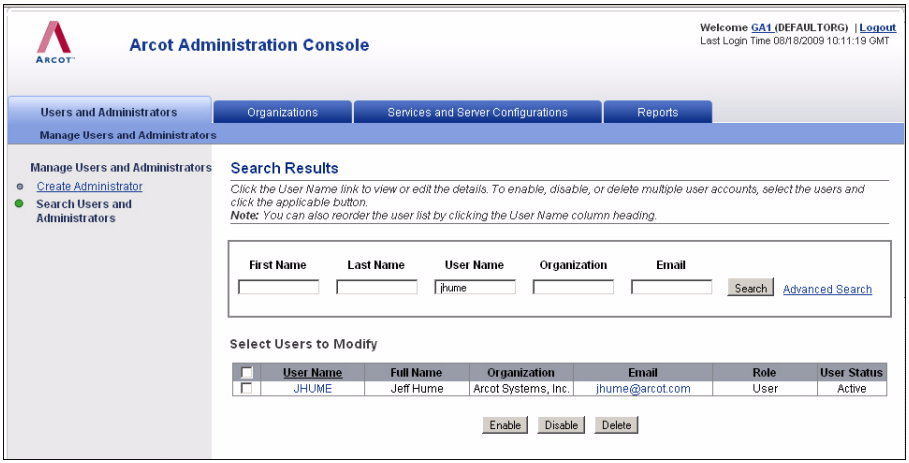
To disable a user account:

1. Ensure that you are logged in with the required privileges and scope to disable the user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 7-1.)
4. Enter the partial or complete information of the user whose account you want to disable and click **Search**.

   You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (GA, OA, or UA).

   The Search Results page (Figure 7-7) appears, with all the matches for the specified criteria.

Figure 7-7 Search Results



5. Select one or more users whose accounts you want to disable.
6. Click **Disable** to disable the selected user account.

Enabling User Accounts

You might need to enable a disabled account.For example, you might disable an administrator account in case the administrator is on long vacation. This helps to prevent unauthorized access to that administrator's account.

You cannot search directly for disabled accounts by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You must perform an **Advanced Search** for such users and use the **Include Inactive Users** option to search.

Privileges Required:

To be able to enable a user account, you must ensure that you have the appropriate privileges and scope to do so. MA can enable any account, while GAs can enable all accounts within their scope. The OAs and UAs can enable all user accounts in their purview.

To enable a locked-out user account:

1. Ensure that you are logged in with the required privileges to enable the user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 7-1.)
4. Click the **Advanced Search** link to search for users based on their status (active or inactive).

   The Advanced Search page (Figure 7-2) appears.
5. Enter the partial or complete information of the user in **User Account** section.
6. In the **User Status** section, select the **Include Inactive Users** option to search for all inactive user accounts.
7. Click **Search** to display the list of all users matching the search criteria.
8. Select the users whose account you want to enable.
9. Click **Enable** to enable the user accounts.

Deleting User Accounts

After a user account is deleted, all privileges associated with the account are permanently deleted. As a result, the user can no longer log in to your application. However, their account information and credentials *are not* removed from the system.

If you create a new user account with the same name as a previously deleted user, then the new account *does not* automatically assume the privileges of the previously deleted account. If you need to duplicate a deleted account, then you must manually re-create all privileges.

Privileges Required: To be able to delete a user account, you must ensure that you have the appropriate privileges and scope to do so. MA can delete any account, while GAs can delete all accounts (including other GAs), *except* the MA account, within their scope. The OAs and UAs can delete all user accounts in their purview.

To delete a user account:

1. Ensure that you are logged in with the required privileges to delete the user account.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page (Figure 7-1.)
4. Enter the partial or complete information of the user whose account you want to delete and click **Search**.

   You can also click the **Advanced Search** link to search for users based on their status (active or inactive) or their roles (User).

   The Search Results page (similar to Figure 7-7) appears, with all the matches for the specified criteria.
5. Select one or more users whose accounts you want to delete.
6. Click **Delete**.

   NOTE: Even though you have deleted the user, their account information is still maintained in the database.

Chapter 8

Managing Reports

Based on your administrator level, reports enable you to instantly summarize and analyze the information in WebFort database. For example, a report can tell a higher-level administrator which of their administrators accessed the system, at what time, and what activities did they perform. The following sections provide a quick overview of the reports that are available to different administrators:

- **Master Administrator Reports**
- **Global Administrator Reports**
- **Organization Administrator Reports**
- **User Administrator Reports**

Reports available through the Administration Console are generated based on the parameters (or filters) that you specify. As a result, you can control the output of a report based on values that you set when you run the reports. The parameters that you can use to filter data include:

- Date Range
- Administrator Name
- Organizations
- User Name

Section, **"Generating Reports"** walks you through the generic process to generate activity reports for administrators and WebFort-specific reports.

You can also export all generated reports to a file. See section, **"Exporting Reports"** for instructions to do so.

Master Administrator Reports

Reports generated by an MA can be broadly categorized as:

- **Administrator Reports**
- **WebFort Reports**

Administrator Reports

These reports include:

- **My Activity Report**
- **Administrator Activity Report**
- **Organization Report**

My Activity Report

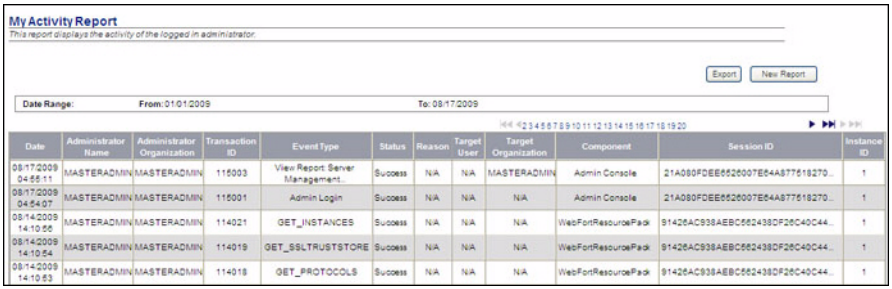
This report lists all operations performed by the administrator generating the report and the details related to these operations.

Even though the logged in administrator can view their activities by using the **Administrator Activity Report**, this report is provided separately because:

- An administrator might not have scope over the organization to which they belong. For example, administrator *Alan* belongs to organization *MyOrg* but has scope over *ScopeOrg*. In this case, Alan cannot view his activities by using Administrator Activity Report because he does not have the required scope.
- Administrator Activity Report lists the activities of all the administrators whose user name completely or partially matches to that of the specified user name. Therefore, the administrator has to search all pages of the report to get their activity report. My Activity report solves this problem, because the report shows the activities of only the logged-in administrator.

Figure 8-1 shows a sample of My Activity Report.

Figure 8-1 My Activity Report



My Activity Report

This report displays the activity of the logged in administrator.

Export New Report

Date Range: From: 01/01/2009 To: 08/17/2009

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID
08/17/2009 04:55:11	MASTERADMIN	MASTERADMIN	115003	View Report Server Management...	Success	N/A	N/A	MASTERADMIN	Admin Console	21A080FDEE6526007E64A877518270...	1
08/17/2009 04:54:07	MASTERADMIN	MASTERADMIN	115001	Admin Login	Success	N/A	N/A	N/A	Admin Console	21A080FDEE6526007E64A877518270...	1
08/14/2009 14:10:56	MASTERADMIN	MASTERADMIN	114021	GET_INSTANCES	Success	N/A	N/A	N/A	WebFortResourcePack	91426AC938AEBC562438DF26C40C44...	1
08/14/2009 14:10:54	MASTERADMIN	MASTERADMIN	114019	GET_SSLTRUSTSTORE	Success	N/A	N/A	N/A	WebFortResourcePack	91426AC938AEBC562438DF26C40C44...	1
08/14/2009 14:10:53	MASTERADMIN	MASTERADMIN	114018	GET_PROTOCOLS	Success	N/A	N/A	N/A	WebFortResourcePack	91426AC938AEBC562438DF26C40C44...	1

Table 8-1 explains the fields of this report.

Table 8-1 My Activity Report Fields

Report Field	Description
Date	The date and time of the activity.
Administrator Name	The name of the administrator who is generating the report.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	The unique ID generated for each activity performed by the administrator.
Event Type	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Status	The status of the action taken: • **Success** - If the action was completed successfully. • **Failure** - If the administrator failed to complete the action.
Reason	The reason why the operation failed.
Target User	The name of the user whose attributes were administered by the administrator.
Target Organization	The organization on which the activity was performed.
Component	The resource that was used to perform the task. The column values can be: • Administration Console • WebFort
Session ID	The session identifier of the Administration Console to which the administrator logged in.

Table 8-1 My Activity Report Fields

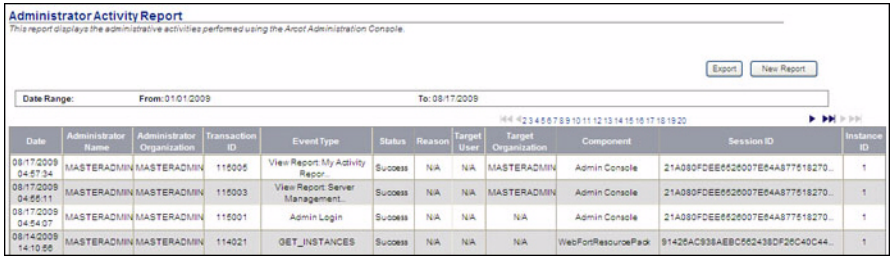
Report Field	Description
Instance ID	The unique identifier for the Administration Console application instance, in case multiple instances of the application are running.

Administrator Activity Report

This report lists all activities performed by administrators belonging to the organizations that are in scope of administrator generating this report. By using this report, you can filter the activities of a specific administrator or view the activities for all the administrators of a single organization or multiple organizations. This report includes information such as, administrator login and logout timestamps, organization search, administrator account updates, and related details.

Figure 8-2 shows a sample Administrator Activity Audit Report.

Figure 8-2 Administrator Activity Report



Administrator Activity Report

This report displays the administrative activities performed using the Arcot Administration Console.

Export New Report

Date Range: From: 01/01/2009 To: 08/17/2009

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID
08/17/2009 04:57:34	MASTERADMIN	MASTERADMIN	115005	View Report: My Activity Repor...	Success	N/A	N/A	MASTERADMIN	Admin Console	21A080FDEE6526007E64A877518270...	1
08/17/2009 04:56:11	MASTERADMIN	MASTERADMIN	115003	View Report: Server Management...	Success	N/A	N/A	MASTERADMIN	Admin Console	21A080FDEE6526007E64A877518270...	1
08/17/2009 04:54:07	MASTERADMIN	MASTERADMIN	115001	Admin Login	Success	N/A	N/A	N/A	Admin Console	21A080FDEE6526007E64A877518270...	1
08/14/2009 14:10:56	MASTERADMIN	MASTERADMIN	114021	GET_INSTANCES	Success	N/A	N/A	N/A	WebFortResourcePack	91426AC938AEBC562438DF26C40C44...	1

The fields of this report are same as My Activity Report. See Table 8-1 for more information on the field details.

Organization Report

Refer to the "Organization Report" discussed in "Organization Administrator Reports" on page 197.

WebFort Reports

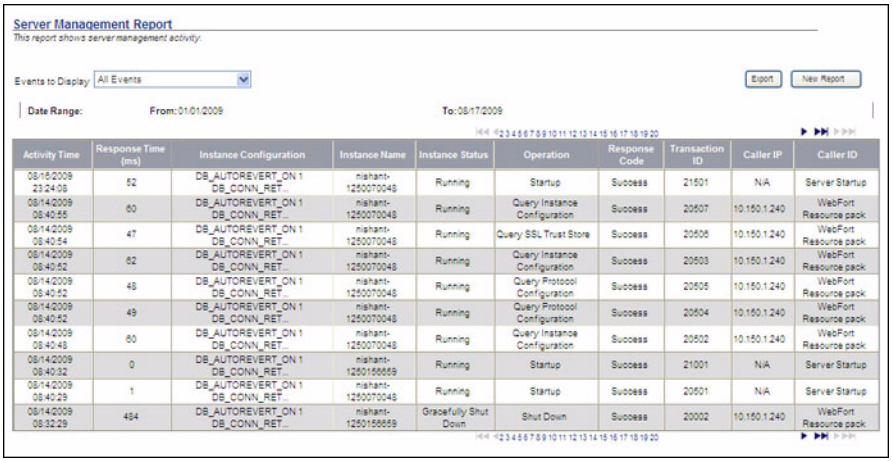
The only WebFort-specific report that an MA can generate is the Server Management Activity Report.

Server Management Activity Report

This reports lists the WebFort Server configurations made by the MA, and includes information about the activities related to log settings, database settings, protocol configurations, plug-in configurations, trusted certificate authority configurations, and server startup, shutdown, and refresh.

Figure 8-3 shows a sample Server Management Report.

Figure 8-3 Server Management Report



Server Management Report

This report shows server management activity.

Events to Display: All Events

Export New Report

Date Range: From: 01/01/2009 To: 08/17/2009

Activity Time	Response Time (ms)	Instance Configuration	Instance Name	Instance Status	Operation	Response Code	Transaction ID	Caller IP	Caller ID
08/18/2009 23:24:08	52	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Startup	Success	21501	N/A	Server Startup
08/14/2009 08:40:55	60	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Query Instance Configuration	Success	20507	10.150.1.240	WebFort Resource pack
08/14/2009 08:40:54	47	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Query SSL Trust Store	Success	20506	10.150.1.240	WebFort Resource pack
08/14/2009 08:40:52	62	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Query Instance Configuration	Success	20503	10.150.1.240	WebFort Resource pack
08/14/2009 08:40:52	48	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Query Protocol Configuration	Success	20505	10.150.1.240	WebFort Resource pack
08/14/2009 08:40:52	49	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Query Protocol Configuration	Success	20504	10.150.1.240	WebFort Resource pack
08/14/2009 08:40:48	60	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Query Instance Configuration	Success	20502	10.150.1.240	WebFort Resource pack
08/14/2009 08:40:32	0	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250156659	Running	Startup	Success	21001	N/A	Server Startup
08/14/2009 08:40:29	1	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250070048	Running	Startup	Success	20501	N/A	Server Startup
08/14/2009 08:32:29	484	DB_AUTOREVERT_ON 1 DB_CONN_RET...	nishant-1250156659	Gracefully Shut Down	Shut Down	Success	20002	10.150.1.240	WebFort Resource pack

Table 8-2 explains the fields of this report.

Table 8-2 Server Management Report Fields

Report Field	Description
Activity Time	The date and time of the activity.
Response Time (ms)	The time taken (in milliseconds) by the WebFort Server to process the request.
Instance Configuration	The details for all WebFort Server instance configurations. **TIP:** To see the complete configuration details for an instance, hover the mouse on the column entry.
Instance Name	The name of the WebFort Server instance.
Instance Status	The status of the WebFort Server instance.
Operation	The type of activity performed (such as, create, read, modify, delete, or view) by the administrator.

Table 8-2 Server Management Report Fields

Report Field	Description
Response Code	The status of the action taken: • **Success** - If the action was completed successfully. • **Failure** - If the administrator failed to complete the action.
Transaction ID	The unique identifier generated by the WebFort Server for the transaction.
Caller IP	The IP address of the system from where the operation was performed.
Caller ID	The unique identifier set by the calling application. **NOTE:** The Caller ID can be blank, if the calling application did not set the value.

Global Administrator Reports

Reports generated by an MA can be broadly categorized as:

- Administrator Reports
- WebFort Reports

Administrator Reports

GAs can generate the following administrator-related reports:

- My Activity Report
- Administrator Activity Report
- Organization Report
- User Activity Report

My Activity Report

Refer to "Server Management Activity Report" discussed in "Master Administrator Reports" on page 186.

Administrator Activity Report

Refer to the "Administrator Activity Report" discussed in "Master Administrator Reports" on page 186.

Organization Report

Refer to the "Organization Report" discussed in "Organization Administrator Reports" on page 197.

User Activity Report

Refer to the "User Activity Report" discussed in "User Administrator Reports" on page 200.

WebFort Reports

GAs can generate the following WebFort configuration-related reports:

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

Authentication Activity Report

This report provides a detailed lists of authentication activity of all users. It lists the authentication details, such as the type of credential used, validity of the credential, the number of times the OTP can be used, and number of times the user failed to authenticate.

Figure 8-4 shows a sample Authentication Activity Report.

Figure 8-4 Authentication Activity Report

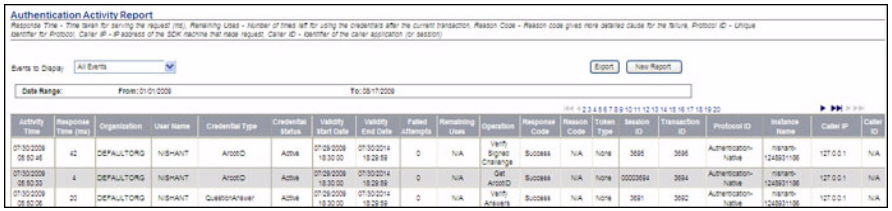


Table 8-3 explains the fields of this report.

Table 8-3 Authentication Activity Report Fields

Report Field	Description
Activity Time	The date and time of the activity.
Response Time (ms)	The time taken (in milliseconds) by the WebFort Server to process the request.
Organization	The name of the organization to which the user belongs.
User Name	The ID of the user who performed the authentication activity.
Credential Type	The type of credential that was used for authentication.
Credential Status	The status of the credential.
Validity Start Date	The timestamp from when the credential is considered to be valid.

Table 8-3 Authentication Activity Report Fields

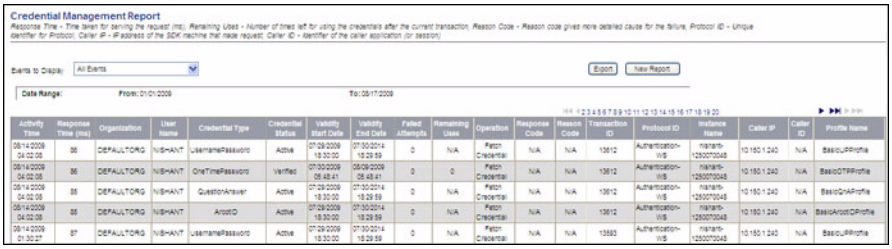
Report Field	Description
Validity End Date	The timestamp when the credential expires.
Failed Attempts	The number of times the user failed to authenticate by using the credential.
Remaining Uses	The number of times for which the OTP can still be used for authentication. **NOTE:** This field is *not* applicable for other credentials.
Operation	The task that was performed by the WebFort Server to authenticate the user.
Response Code	The status of the action taken: • **Success** - If the action was completed successfully. • **Failure** - If the administrator failed to complete the action.
Reason Code	The reason why the **Operation** failed.
Token Type	The type of token that was returned after the authentication was successful.
Session ID	The session identifier for the Administration Console to which the current administrator is logged in.
Transaction ID	The unique identifier generated by the WebFort Server to track the transaction.
Protocol ID	The name of the protocol that was used to perform the activity.
Instance Name	The name of the WebFort Server instance that processed the request.
Caller IP	The IP address of the system from where the request originated.
Caller ID	The unique identifier set by the calling application. **NOTE:** The Caller ID can be blank, if the calling application did not set the value.

Credential Management Activity Report

This report provides a summary of the credentials that are issued to users. The report contains details such as, types of credentials issued, operations on the credential, date of issuance and the current status of the credentials.

Figure 8-5 shows a sample Credential Management Report.

Figure 8-5 Credential Management Activity Report



Credential Management Report

Response Time - Time taken for serving the request (ms), Remaining Uses - Number of times left for using the credentials after the current transaction, Reason Code - Reason code gives more detailed cause for the failure, Protocol ID - Unique identifier for Protocol, Caller IP - IP address of the SDK machine that made request, Caller ID - Identifier of the caller application (or session)

Events to Display: All Events | Export | New Report

Date Range: From: 01/01/2009 To: 08/17/2009

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Activity Time	Response Time (ms)	Organization	User Name	Credential Type	Credential Status	Validity Start Date	Validity End Date	Failed Attempts	Remaining Uses	Operation	Response Code	Reason Code	Transaction ID	Protocol ID	Instance Name	Caller IP	Caller ID	Profile Name
08/14/2009 04:02:06	86	DEFAULTORG	NISHANT	UsernamePassword	Active	07/29/2009 18:30:00	07/30/2014 18:29:59	0	N/A	Fetch Credential	N/A	N/A	13612	Authentication-WS	nishant-1250070048	10.150.1.240	N/A	BasicUPProfile
08/14/2009 04:02:06	86	DEFAULTORG	NISHANT	OneTimePassword	Verified	07/30/2009 06:48:41	08/09/2009 06:48:41	0	0	Fetch Credential	N/A	N/A	13612	Authentication-WS	nishant-1250070048	10.150.1.240	N/A	BasicOTPProfile
08/14/2009 04:02:06	86	DEFAULTORG	NISHANT	QuestionAnswer	Active	07/29/2009 18:30:00	07/30/2014 18:29:59	0	N/A	Fetch Credential	N/A	N/A	13612	Authentication-WS	nishant-1250070048	10.150.1.240	N/A	BasicQnAProfile
08/14/2009 04:02:06	86	DEFAULTORG	NISHANT	ArcotID	Active	07/29/2009 18:30:00	07/30/2014 18:29:59	0	N/A	Fetch Credential	N/A	N/A	13612	Authentication-WS	nishant-1250070048	10.150.1.240	N/A	BasicArcotIDProfile
08/14/2009 01:30:27	87	DEFAULTORG	NISHANT	UsernamePassword	Active	07/29/2009 18:30:00	07/30/2014 18:29:59	0	N/A	Fetch Credential	N/A	N/A	13593	Authentication-WS	nishant-1250070048	10.150.1.240	N/A	BasicUPProfile

Table 8-4 explains the fields of this report.

Table 8-4 Credential Management Report Fields

Report Field	Description
Activity Time	The date and time of the activity.
Response Time (ms)	The time taken (in milliseconds) by the WebFort Server to process the authentication request.
Organization	The name of the organization to which the user belongs.
User Name	The name of the user whose credential was updated.
Credential Type	The type of credential that was affected (changed.) Possible values are: • ArcotID • QnA • OTP • Password
Credential Status	The current state of the credential. Possible values are: • Active • Disabled • Verified • Locked
Validity Start Date	The timestamp from when the credential is considered to be valid.
Validity End Date	The time when the credential expires.
Failed Attempts	The number of times the user failed to authenticate using the credential.
Remaining Uses	The number of times the OTP can still be used for authentication.

Table 8-4 Credential Management Report Fields

Report Field	Description
Operation	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Response Code	The status of the action taken: • **Success** - If the action was completed successfully. • **Failure** - If the administrator failed to complete the action.
Reason Code	The reason why the **Operation** failed.
Transaction ID	The unique identifier generated by the WebFort Server to track the transaction.
Protocol ID	The name of the protocol that was used to perform the activity.
Instance Name	The name of the WebFort Server instance that processed the request.
Caller IP	The IP address of the system from where the request originated.
Caller ID	The unique identifier set by the calling application. **NOTE:** The Caller ID can be blank, if the calling application did not set the value.
Profile Name	The profile name associated with the credential using which the activity was performed.

Configuration Management Report

This report lists all the WebFort configurations that are made by the GA (or the OA.) It provides the configuration information of authentication policies, credential profiles, plug-in, callout, SAML token, RADIUS client, and authentication challenge for ArcotID and QnA.

Figure 8-6 shows a sample Configuration Management Report.

Figure 8-6 Configuration Management Report

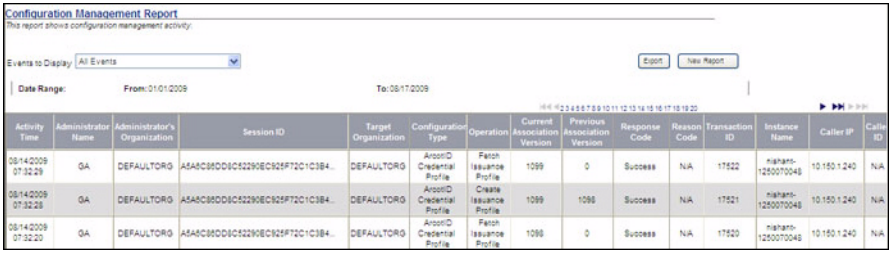


Table 8-5 explains the fields of this report.

Table 8-5 Configuration Management Report Fields

Report Field	Description
Activity Time	The date and time of the activity.
Administrator Name	The administrator who performed the configuration.
Administrator's Organization	The name of the organization to which the administrator belongs.
Session ID	The session identifier of the Administration Console to which the administrator logged in.
Target Organization	The organization for which the configurations are made.
Configuration Type	The type of configuration that was affected (changed.)
Operation	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Current Association Version	The current version of the configuration.
Previous Association Version	The previous version of the configuration.
Response Code	The status of the action taken: • **Success** - If the action was completed successfully. • **Failure** - If the administrator failed to complete the action.
Reason Code	The reason why the Operation failed.
Transaction ID	The unique identifier generated by the WebFort Server for the transaction.
Instance Name	The instance name of the WebFort Server.
Caller IP	The IP address of the system from where the operation was performed.
Caller ID	The unique identifier set by the calling application. **NOTE:** The Caller ID can be blank, if the calling application did not set the value.

Organization Administrator Reports

Reports available to an OA can be broadly categorized as:

- **Administrator Reports**
- **WebFort Reports**

Administrator Reports

An OA can generate the following administrator reports:

- **My Activity Report**
- **Administrator Activity Report**
- **Organization Report**
- **User Activity Report**

My Activity Report

Refer to **"Server Management Activity Report"** discussed in **"Master Administrator Reports" on page 186**.

Administrator Activity Report

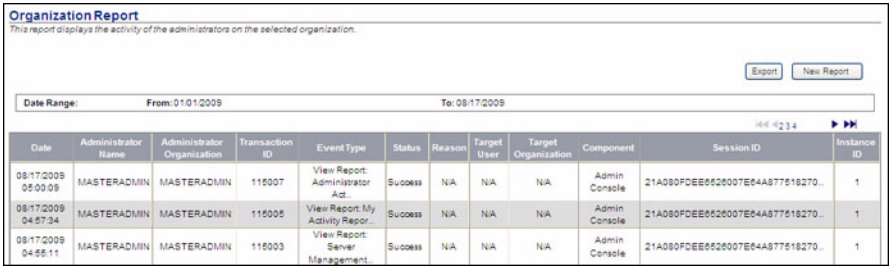
Refer to the **"Administrator Activity Report"** discussed in **"Master Administrator Reports" on page 186**.

Organization Report

This report provides the details of all operations performed on a specified organization. Irrespective of any policies, this report displays *all* the activities in the organization under the administrator's purview.

Figure 8-7 shows a sample Organization Report.

Figure 8-7 Organization Report



Organization Report

This report displays the activity of the administrators on the selected organization.

Export New Report

Date Range: From: 01/01/2009 To: 08/17/2009

1 2 3 4

Date	Administrator Name	Administrator Organization	Transaction ID	Event Type	Status	Reason	Target User	Target Organization	Component	Session ID	Instance ID
08/17/2009 05:00:09	MASTERADMIN	MASTERADMIN	115007	View Report: Administrator Act...	Success	N/A	N/A	N/A	Admin Console	21A090FDEE6526007E64A877518270...	1
08/17/2009 04:57:34	MASTERADMIN	MASTERADMIN	115006	View Report: My Activity Repor...	Success	N/A	N/A	N/A	Admin Console	21A090FDEE6526007E64A877518270...	1
08/17/2009 04:55:11	MASTERADMIN	MASTERADMIN	115003	View Report: Server Management...	Success	N/A	N/A	N/A	Admin Console	21A090FDEE6526007E64A877518270...	1

Table 8-6 explains the fields of this report.

Table 8-6 Organization Report Fields

Report Field	Description
Date	The date and time of the activity.
Administrator Name	The name of the administrator who performed the activity.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	The unique identifier generated for every activity performed by the administrator.
Event Type	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Status	The status of the action taken: • **Success** - If the action was completed successfully. • **Failure** - If the administrator failed to complete the action.
Reason	The reason why the Operation failed.
Target User	The name of the user whose attributes were administered by the administrator.
Target Organization	The organization to which the user belongs.
Component	The resource that was used to perform the task. The column values can be: • Administration Console • WebFort
Session ID	The session identifier for the Administration Console to which the administrator logged in.

Table 8-6 Organization Report Fields

Report Field	Description
Instance ID	The unique identifier for the Administration Console application instance, in case multiple instances of the application are running.

User Activity Report

Refer to the "User Activity Report" discussed in "User Administrator Reports" on page 200.

WebFort Reports

OAs can generate the following WebFort configuration-related reports:

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

Authentication Activity Report

Refer to the "Authentication Activity Report" discussed in "Global Administrator Reports" on page 191.

Credential Management Activity Report

Refer to the "Credential Management Activity Report" discussed in "Global Administrator Reports" on page 191.

Configuration Management Report

Refer to the "Configuration Management Report" discussed in "Global Administrator Reports" on page 191.

User Administrator Reports

Reports available to an OA can be broadly categorized as:

- Administrator Reports
- WebFort Reports

Administrator Reports

UAs can generate the following administrator reports:

- My Activity Report
- Administrator Activity Report
- User Activity Report

My Activity Report

Refer to "Server Management Activity Report" discussed in "Master Administrator Reports" on page 186.

Administrator Activity Report

Refer to the "Administrator Activity Report" discussed in "Master Administrator Reports" on page 186.

User Activity Report

This report lists all activities performed on user attributes, which include creating users, updating users, setting PAM, deleting users, update user status, and authenticating users. The report contains details such as, user name, status of the user, type of operations performed, and also the IP address of the user system.

Figure 8-8 shows a sample User Activity Report.

Figure 8-8 User Activity Report

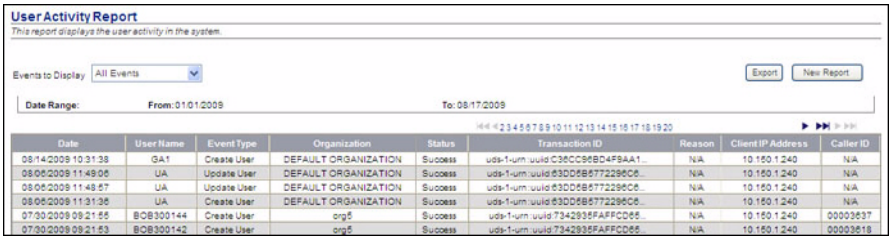


Table 8-7 explains the fields of this report.

Table 8-7 User Activity Report Fields

Report Field	Description
Date	The date and time of the activity.
User Name	The name of the user for whom the activity was performed.
Event Type	The type of activity (such as, create, update, and delete user) performed by the administrator.
Organization	The organization name to which the user belongs.
Status	The status of the operation: • **Success** - If the operation was completed successfully. • **Failure** - If the user failed to complete the operation.
Transaction ID	The unique ID generated for every activity performed by the user.
Reason	The reason why the Operation failed.
Client IP Address	The IP address of the end user's system.
Caller ID	The unique identifier set by the calling application. **NOTE:** The Caller ID can be blank, if the calling application did not set the value.

WebFort Reports

UAs can generate the following administrator reports:

- Authentication Activity Report
- Credential Management Report

Authentication Activity Report

Refer to "Authentication Activity Report" discussed in "Global Administrator Reports" on page 191.

Credential Management Report

Refer to "Credential Management Activity Report" discussed in "Global Administrator Reports" on page 191.

Generating Reports

This section covers:

- Notes for Generating Reports
- Generating the Report

Notes for Generating Reports

While generating reports, remember that:

- The administrator can *only* generate the reports of the organizations on which they have the scope.
- The administrator can generate the report of their subordinate or peers. For example, an Organization Administrator (OA) can generate the reports of an OA and User Administrator (UA).
- If the administrator is derived by using custom role, then the derived administrator belongs to the same level as that of the parent level. For example, if you derive an administrator *MyGlobalAdmin* from GA, then *MyGlobalAdmin* is considered to be a GA even though you might have assigned *MyGlobalAdmin* less number of privileges compared to an OA or UA.

Generating the Report

To generate any of the reports discussed earlier in the chapter:

1. Ensure that you are logged in with proper credentials (MA, GA, OA, or UA.)
2. Activate the **Reports** tab in the main menu.
3. If you want to generate:
   - Administrator activity report, then select the **Administrator Reports** sub-menu.
   - WebFort-specific report, then select the **WebFort Reports** sub-menu.

   The corresponding links for the report type appear in the left-handle task panel.
4. Based on the report you want to generate, click the required report link.
5. Specify the criteria to view the report:

a. Specify one of the following:

- The **Date Range** from the drop-down list.

  or

- A pre-defined date range in the **From** and **To** fields.

b. From the **Organization Name** list, select the required organizations whose data you want to include in the report.

c. In the **User Name** field, based on the report you want to generate:

- Enter a user name (for Authentication Activity and Credential Management reports.)

  or

- Enter the administrator name (for configuration reports.)

6. Click **Display Report** to generate the report based on the criteria you specified.

Exporting Reports

The Administration Console provides the ability to export reports to a file. By exporting a report, you can save a local copy of a report, which enables you to track trends. You can also work with the saved report data in another application.

The exported reports are generated in the comma-separated value (CSV) format that can be viewed by using text editors and spreadsheet applications, such as Microsoft Excel. The export option is available through the **Export** button, which appears at the top-right of every rendered report.

To export a report to a local file:

1. Generate the required report. See section, **"Generating Reports" on page 203** for detailed instructions to do so.

   The report opens.

2. Click **Export**.

   You are prompted to save or open the report.

3. Click **Open** or **Save**. If you choose to save the report, then you must specify the download location.

   This file can later be viewed by using the appropriate application.

Chapter 9

Tools for System Administrators

This chapter discusses the command-line tools shipped along with WebFort that you can use to perform system management tasks. It provides a quick overview of functions and useful options for the tools that are available with WebFort and can be useful to administrators:

- **dbutil**
- **webfortserver**
- **arwfclient**

dbutil

During WebFort installation, the installer collects the information to connect to the WebFort database. After the installation is completed, the information for the WebFort Server to connect to the database is stored in the encrypted format in a file called **`securestore.enc`**. If for some reason, you want to change the database user name or password, then you can use **`dbutil`** tool. This file stores the following encrypted information:

- Database user name
- Database password

1. The **`dbutil`** tool enables you to either change or add new database user name or password. To perform these operations:Navigate to the location where the tool is available:

   - **On Windows**

     `<install_location>\Arcot Systems\bin\`

   - **On UNIX-based Platforms**

     `<install_location>/arcot/bin/`

2. Run the following command:

   `dbutil -h`

   The commands supported by the tool are displayed.

3. Enter the option depending on the type of operation you want to perform. Table 9-1 lists the options for `dbutil`. In this table, *`key-value`* pair refers to either DSN, password, or database user name/password pair. The DSN-password is used by WebFort Server, while the user name-password is used by Administration Console and User Data Service.

Table 9-1 Additional dbutil Options

Option	Description

-pd	Deletes the specified key-value pair from `securestore.enc`.
	Syntax:
	`dbutil -pd key`
	For example:
	`dbutil -pd WebFortDatabaseDSNOld`
	`dbutil -pd Jack`

-pi	Inserts an additional key-value pair into `securestore.enc`.
	Syntax:
	`dbutil -pi key value`
	For example:
	`dbutil -pi WebFortBackupDSN dbapassword`
	`dbutil -pi Jack userpassword`
	IMPORTANT: Each key can only have one value. If you have already inserted a key-value pair, then you cannot insert another value for the same key.

-pu	Updates the value for an existing key-value pair in `securestore.enc`. This feature is used when you need to update the database password.
	Syntax:
	`dbutil -pu key value`
	For example:
	`dbutil -pu WebFortDatabaseDSN newPassword`
	`dbutil -pu Jack userPassword`

webfortserver

The **webfortserver** tool is the core authentication server that can also be run in interactive mode to enable you to configure:

- WebFort settings that are either used rarely or are needed only under certain deployment scenarios
- Few configurations that are not exposed by Administration Console

Running the Tool in Interactive Mode

The tool provides the **-i** option to run it in the interactive mode. In this mode all the server configurations are done in a similar fashion as that in the service mode, except that the listeners are not started.

When run in this mode, the server starts its own console prompt (**wf>**) and generates the **startup logs** in `<install_location>/logs/`**arcotwebfortstartupcmd.log** and the **transaction logs** in `<install_location>/logs/`**arcotwebfortcmd.log**.

To run the **arwfserver** tool:

1. Navigate to the location where the tool is available:
   - **On Windows**

     `<install_location>\Arcot Systems\`**bin**`\`
   - **On UNIX-based Platforms**

     `<install_location>/arcot/`**bin**`/`
2. Run the following command:

Windows:

```
arwfserver -i
```

Unix Platforms:

```
webfortserver -i
```

The tool starts in interactive mode.

3. Specify the options listed in Table 9-2 to perform the required task.

Table 9-2 arwfserver Options

Option	Description
?	Lists the commands for the *all* options supported by `arwfserver`.
help	Explains specific command in more detail.

Table 9-2 arwfserver Options

Option	Description
??	Searches the commands based on the pattern you provide. For example, if you enter **?? conf**, then all the options that set or get the configurations are displayed.
log2c	Allows you to write the logs to the console, instead of file. Enter **1** to write the logs to console or **0** to write the logs to file.
setsvrmgmtconf	Allows you to change the port number of the Server Management protocol. **NOTE:** If you have enabled WebFort Server for SSL, then this tool also provides you an option to change the transport mode from SSL to TCP.
setmiscconf	Allows you to set the time-drift values between the databases that the WebFort Server instance is connected to. **NOTE:** Arcot recommends that you contact the technical support team at support@arcot.com to set these values.
sermodconf	Allows you to enable or disable the plug-ins. Enter **1** to enable the plug-in or **0** to disable.
setsaconf	Enables you to configure the Web Services APIs that are provided by WebFort Server for authentication and authorization. Enter **1** for securing the access or **0** for regular access.
getmiscconf	Fetches the configurations that are set by using **setmiscconf**.
getmodconf	Fetches the configuration for the current modules. For example credential modules and plug-ins.
getsaconf	Fetches the current Web services security access details. It retrieves the list of APIs and their corresponding protection status.
getprotoconf	Fetches the configurations for all protocols.
q	Closes the interactive mode.

arwfclient

You can use the **arwfclient** tool to refresh the server, shutdown the server, and read the server configuration information, such as library versions, protocol configurations, and server statistics.

Running the Tool in Interactive Mode

The tool provides the **-i** option to run it in the interactive mode. When run in this mode, the tool starts its own console prompt (**arwfclient#**).

To run the **arwfclient** tool:

1. Navigate to the location where the tool is available:
   - **On Windows**

     `<install_location>\Arcot Systems\bin\`
   - **On UNIX-based Platforms**

     `<install_location>/arcot/sbin/`
2. Run the following command:

   arwfclient -i

   The tool starts in interactive mode.
3. Specify the options listed in Table 9-3 to perform the required task.

Table 9-3 arwfclient Options

Option	Description
?	Lists the commands for the *all* options supported by `arwfclient`.
help	Explains the command in more detail.
md5	Generates a file called **webfort-md5-<*dd*>-<*mmm*>-<*yy*>.txt**, which lists the MD5 digest for all the files installed by WebFort. This file is available in the following directory: **Windows**: `<install_location>\Arcot Systems\logs` **Solaris Platforms**: `<install_location>/arcot/logs`

Table 9-3 arwfclient Options

Option	Description
ver	Generates a file called **webfort-ver-<*dd*>-<*mmm*>-<*yy*>.txt**, which lists the version of all WebFort library files. This file is available in the following directory: **Windows**: `<install_location>\Arcot Systems\`**logs** **Solaris Platforms**: `<install_location>/arcot/`**logs**
ssc	Sets the server configurations. **IMPORTANT:** You must enter the instance IP and port number of the WebFort Server whose configuration you want to set.
sso	Generates the statistics for each protocol. Enter **1** to set the statistics per protocol.
gss	Generates a file called **webfort-stats-<*dd*>-<*mmm*>-<*yy*>.txt**, which lists the server statistics. This file is available in the following directory: **For Windows**: `<install_location>\Arcot Systems\`**logs** **For UNIX-Based Platforms**: `<install_location>/arcot/`**logs** The statistics file includes the following information for each protocol: • Number of requests received • Number of successful transactions • Number of failed transactions • Minimum time taken to process the requests • Maximum time taken to process the requests • Total time taken to process all the requests • Average time required to process a request
cr	Refreshes the cache of the server instance. You *must* enter the instance IP and the server management port number. After successful operation, the message "Instance refreshed successfully" and a transaction ID is returned.

Table 9-3 arwfclient Options

Option	Description
sd	Shuts down the WebFort Server instance. You *must* enter the instance IP and the server management port number. After successful operation, the message "Successfully initiated shutdown operations" and a transaction ID is returned.
q	Closes the interactive mode.

Appendix A

WebFort Logging

To effectively manage the communication between WebFort Server and your application, it is necessary to get information about the activity and performance of the Server as well as any problems that have occurred.

This appendix describes the various log files supported by WebFort, the severity levels that you will see in these files, and the formats of these log files. It covers the following topics:

- About the Log Files
- Format of the WebFort Log Files
- Format of UDS and Administration Console Log Files
- Supported Severity Levels

About the Log Files

The WebFort log files can be categorized as:

- Startup Log File
- Transaction Log Files
- UDS Log File
- Administration Console Log File

The parameters that control logging in these files can be configured either by using the relevant INI files (as is the case with UDS and Administration Console log files) or by using the Administration Console itself (as is the case with WebFort log file.) The typical logging configuration options that you can change in these files include:

- **Specifying log file name and path:** WebFort enables you to specify the directory for writing the log files and storing the backup log files. Specifying the diagnostic logging directory allows administrators to manage system and network resources.
- **Log file size:** The maximum number of bytes the log file can contain. When the log files reach this size, a new file with the specified name is created and the old file is moved to the backup directory.
- **Using log file archiving:** As WebFort components run and generate diagnostic messages, the size of the log files increases. If you allow the log files to keep increasing in size, then the administrator must monitor and clean up the log files manually. WebFort enables you to specify configuration options that limit how much log file data is collected and saved. WebFort lets you specify the configuration option to control the size of diagnostic logging files. This lets you determine a maximum size for the log files. When the maximum size is reached, older log information is moved to the backup file before the newer log information is saved.
- **Setting logging levels:** WebFort also allows you to configure logging levels. By configuring logging levels, the number of messages saved to diagnostic log files can be reduced. For example, you can set the logging level so that the system only reports and saves critical messages. See "Supported Severity Levels" for more information on the supported log levels.
- **Specifying time zone information:** WebFort enables you to either use the local time zone for time stamping the logged information or use GMT for the same.

Startup Log File

When you start the WebFort Server, it records all start-up (or boot) actions in the **arcotwebfortstartup.log** file. The information in this file is very useful in identifying the source of the problems if the WebFort service does not start up.

The default location of this file is:

Windows: `<install_location>\Arcot Systems\logs\`

UNIX-Based: `<install_location>/arcot/logs/`

Transaction Log Files

The transaction logs consists of the following types:

- WebFort Server Log
- WebFort Statistics Log File

WebFort Server Log

WebFort records all requests processed by the server in the **arcotwebfort.log** file. The default location of this file is:

Windows: `<install_location>\Arcot Systems\logs\`

UNIX-Based: `<install_location>/arcot/logs/`

The parameters that control logging in this file can be configured by using the Administration Console. To do so, you must use the instance-specific configuration sub-screen that you can access by clicking the required instance in the **Instance Management** screen.

In addition to the log file path, the maximum log file size (in bytes), backup directory, logging level, and timestamp information, you can also control whether you want to enable trace logging. See section, "Format of the WebFort Log Files" on page 220 for the details of the default format used in the file.

WebFort Statistics Log File

WebFort uses the **arcotwebfortstats.log** file for logging statistics.

The default location of this file is:

Windows: `<install_location>\Arcot Systems\logs\`

UNIX-Based: `<install_location>/arcot/logs/`

UDS Log File

All User Data Service (UDS) information and actions are recorded in the **`arcotuds.log`** file. This information includes:

- UDS database connectivity information
- UDS database configuration information
- UDS instance information and the actions performed by this instance

The information in this file is very useful in identifying the source of the problems if the Administration Console could not connect to the UDS instance. The default location of this file is:

Windows: `<install_location>\Arcot Systems\logs\`

UNIX-Based: `<install_location>/arcot/logs/`

The parameters that control logging in this files can be configured by using the **`udsserver.ini`** file, which is available in the **`conf`** folder in `ARCOT_HOME`.

In addition to the logging level, log file name and path, the maximum file size (in bytes), and archiving information, you can also control the layout of the logging pattern for UDS by specifying the appropriate values for `log4j.appender.debuglog.layout.`**`ConversionPattern`**. See section, **"Format of UDS and Administration Console Log Files" on page 222** for the details of the default format used in the file.

Administration Console Log File

When you deploy the Administration Console and subsequently start it, the details of all its actions and processed requests are recorded in the **`arcotadmin.log`** file. This information includes:

- Database connectivity information
- Database configuration information
- Instance information and the actions performed by this instance

- UDS configuration information
- Other Administration Console information specified by the Master Administrator, such as cache refresh

The information in this file is very useful in identifying the source of the problems if the Administration Console does not start up. The default location of this file is:

Windows: `<install_location>\Arcot Systems\logs\`

UNIX-Based: `<install_location>/arcot/logs/`

The parameters that control logging in this files can be configured by using the **`adminserver.ini`** file, which is available in the **`conf`** folder in `ARCOT_HOME`.

In addition to the logging level, log file name and path, the maximum log file size (in bytes), log file archiving information, you can also control the layout of the logging pattern for the console by specifying the appropriate values for `log4j.appender.debuglog.layout.`**`ConversionPattern`**. See section, **"Format of UDS and Administration Console Log Files" on page 222** for the details of the default format used in the file.

Format of the WebFort Log Files

Table A-1 describes the format of the entries in the following WebFort loggers:

- `arcotwebfort.log` (**WebFort Server Log**)
- `arcotwebfortstartup.log` (**Startup Log File**)
- `arcotwebfortstats.log` (**WebFort Statistics Log File**)

Table A-1 WebFort Logging Format

Column	Description
Time Stamp	The time when the entry was logged, translated to the time zone you configured. The format of logging this information is: *mm/dd/yy HH:MM:SS.mis* Here, *mis* represents milliseconds.
Log Level (LEVEL) **(or Severity)**	The severity level of the logged entry. See "Supported Severity Levels" on page 223 for more information.
Protocol Name **(PROTOCOLNAME)**	The protocol used for the transaction. Possible values are: • AUTH_NATIVE • ADMIN_WS • ASSP_WS • RADIUS • SVRMGMT_WS • TXN_WS In case the server is starting up, shutting down, or is in the monitoring mode, then no protocol is used and the following values are displayed, respectively: • STARTUP • SHUTDOWN • MONITOR
Thread ID (THREADID)	The ID of the thread that logged the entry.

Table A-1 WebFort Logging Format

Column	Description
Transaction ID (**`000TXNID`**)	The ID of the transaction that logged the entry.
Message	The message logged by the Server in the log file in the free-flowing format. **NOTE:** The granularity of the message depends on the **Log Level** that you set in the log file.

Format of UDS and Administration Console Log Files

Table A-2 describes the format of the entries in the following loggers:

- `arcotuds.log` (UDS Log File)
- `arcotadmin.log` (Administration Console Log File)

Table A-2 UDS and Administration Console Logging Format

Column	Associated Pattern (In the Log File)	Description
Time Stamp	`%d{yyyy-MM-dd hh:mm:ss,SSS z} :`	The time when the entry was logged. This entry uses the application server time zone. The format of logging this information is: *yyyy-MM-dd hh:mm:ss,SSS z* Here, *SSS* represents milliseconds.
Thread ID	`[%t] :`	The ID of the thread that logged the entry.
Log Level (or Severity)	`%-5p :`	The severity level of the logged entry. See "Supported Severity Levels" on page 223 for more information.
Logger Class	`%-5c{3}(%L) :`	The name of the logger that made the log request.
Message	`%m%n :`	The message logged by the Server in the log file in the free-flowing format. **NOTE:** The granularity of the message depends on the **Log Level** that you set in the log file.

Refer to the following URL for customizing the **`PatternLayout`** parameter in the UDS and Administration Console log files:

http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html

Supported Severity Levels

A *log level* (or *severity level*) enables you to specify the level of detail of the information stored in the WebFort logs. This also enables you to control the rate at which the log file will grow.

Table A-3 describes the log levels that you see in all log files, in the *decreasing* order of severity.

Table A-3 WebFort Log Levels (in Decreasing Order of Severity)

Log Level		Description
0	**FATAL**	Use this log level for serious, non-recoverable errors that can cause the abrupt termination of the WebFort service.
1	**WARNING**	Use this log level for undesirable run-time exceptions, potentially harmful situations, and recoverable problems that are not yet FATAL.
2	**INFO**	Use this log level for capturing information on run-time events. In other words, this information highlights the progress of the application, which might include changes in: • Server state, such as start, stop, and restart. • Server properties. • State of services. • State of a processes on the Server.
3	**DEBUG**	Use this log level for logging detailed information for debugging purposes. This might include process tracing and changes in Server states.

NOTE: When you specify a log level, messages from all other levels of *higher* significance are reported as well. For example if the `LogLevel` is specified as `3`, then messages with log levels of `FATAL`, `WARNING`, and `INFO` level are also captured.

The following subsections show a few sample entries (based on the Log Level) in the **WebFort log file.**

FATAL

```
07/17/09 11:49:20.404  FATAL  STARTUP  00002872  00WFMAIN - Unable to initialize
the database

07/17/09 11:49:20.405  FATAL  STARTUP  00002872  00WFMAIN - Failed to load the ini
parameters

07/17/09 11:49:20.406  FATAL  STARTUP  00002872  00WFMAIN - Cannot continue due to
setConfigData failure, SHUTTING DOWN
```

WARNING

```
07/17/09 12:50:05.848  INFO  AUTH_NATIVE  00002780  00022508 - Fail to connect to
Database prdsn for 1 time(s). DbUsername system

07/17/09 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

```
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - mMinConnections [4]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - mMaxConnections [128]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - mCurrPoolSize   [4]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - mNumDBFailure     [0]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - mCurrNumUsed      [0]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - mCurrNumAvailable [4]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [0]
mNumTimesConnIdxLocked   [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [0]
mNumTimesConnIdxReleased [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [1]
mNumTimesConnIdxLocked   [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [1]
mNumTimesConnIdxReleased [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [2]
mNumTimesConnIdxLocked   [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [2]
mNumTimesConnIdxReleased [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [3]
mNumTimesConnIdxLocked   [23]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [3]
mNumTimesConnIdxReleased [23]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - ---------- logging
stats for databse [wf-test-p] : [primary] [ACTIVE] end   ----------
```

DEBUG

```
07/17/09 11:50:20.136  DEBUG  MONITOR  00000424  STATSMON - Acquiring Cache read
lock on [06834624]
07/17/09 11:50:20.136  DEBUG  MONITOR  00000424  STATSMON - Acquired Cache read
lock on [06834624]
07/17/09 11:50:20.136  DEBUG  MONITOR  00000424  STATSMON - Releasing Cache read
lock on [06834624]
07/17/09 11:50:20.136  DEBUG  MONITOR  00000424  STATSMON - Released Cache read
lock on [06834624]
07/17/09 11:50:20.136  INFO  MONITOR  00000424  STATSMON - op
[AUTH_AID_GET_CHAL:1032] rcvd [1] sent [1] success [1] failed [0] intError [0]
minTimeMS [177] maxTimeMS [177] totTimMS [177] avgTimeMs [177]
07/17/09 11:50:20.136  DEBUG  MONITOR  00000424  STATSMON - Acquiring Cache read
lock on [0684D7BC]
```

Appendix B

Glossary

Activation Code	8-digit numeric code returned by WebFort Server in for administrators to log in if their organization is set for WebFort Username-Password mechanism.
Adobe Signature Service Protocol	See ASSP.
Administration Console	Web-based console for configuring communication mode between WebFort Server and its components and for performing administrative tasks.
ArcotID	Is a secure software credential that allows hardware level authentication in software form.
ASSP	Allows Acrobat and Reader users to access their roaming credentials for digital signatures. ASSP passes the hash to an ASSP-enabled server for signature and then after signing, embeds it into the end user's document.
Authentication	Is a process by which an entity proves that it is who it claims to be.
Authentication Policy	Set of rules that control the authentication process.
Authentication SDK	APIs that can be invoked by your application to forward authentication requests to WebFort Server.
Authentication Token	A token is an object that an authorized user of computer services is given to aid in authentication.
Credential	A proof of user identity. Digital credentials might be stored on hardware such as smart cards or USB tokens or on the server. They are verified during authentication.
Credential Profile	Common, ready-to-use credential configuration that can be shared among multiple organizations and multiple users.
Cryptographic Hash Function	A cryptographic hash function is a hash function with additional security properties, used in security-related applications such as authentication.

Custom Role	A role derived by inheriting a subset of privileges from one of the predefined parent roles that include Global Administrator, Organization Administrator, and User Administrator.
Default Organization	The Organization created by default when you deploy the Administration Console.
Digest-MD5	Is a widely used cryptographic hash function with a 128-bit hash value.
Digital Certificates	A certificate is a digital document that vouches for the identity and key ownership of an individual, a computer system, or an organization. This authentication method is based on the PKI cryptography method.
Encryption	The process of scrambling information in a way that disguises its meaning.
Error Message	Message returned by application to report to the user agent regarding any erroneous situations.
Forgot Your Password (FYP)	If the user forgets his ArcotID password, then a QnA session is carried out between the User and WebFort. On answering a minimal set of questions, the user is asked for a new ArcotID password and a new ArcotID is issued.
Global Administrator (GA)	An administrator responsible for setting up CSR Administrator accounts and configuring the system.
Instance	A system where WebFort Server is available at a specified port.
Issuance SDK	APIs that can be invoked by your application to forward issuance requests to WebFort Server for enrolling users and for creating their credentials in WebFort.
Master Administrator (MA)	The main administrator responsible for initializing the WebFort setup and its components (including Administration Console and UDS), creating GAs, and OAs and UAs, if required.
N-Strikes	The maximum number of failed authentication attempts that can be made by the user before locking out.
One-Time Password	Password credential valid for a single session. WebFort provides multi-use OTPs.
One-Time Token	Token returned by WebFort Server after successful authentications.
Organization	A WebFort unit that can either map to a complete enterprise (or a company) or a specific division, department, or other entities within the enterprise.

Organization Administrator **(OA)**	An administrator responsible for all tasks related to management of the organizations.
OTP	See **One-Time Password**.
OTT	See **One-Time Token**.
PKCS	PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA. See **Public-key Cryptography** for more details.
PKCS#12	Defines a file format commonly used to store private keys with accompanying Public key certificates protected with a password-based symmetric key.
Private Key	One of a pair of keys used in public-key cryptography. The private key is kept secret and can be used to decrypt/encrypt data.
Public Key	One of a pair of keys used in public-key cryptography. The public key is distributed freely and published as part of a certificate. It is typically used to encrypt data sent to the public key's owner, who then decrypts the data using the corresponding private key.
Public Key Infrastructure (PKI)	The standards and services that facilitate the use of public-key cryptography and certificates in a networked environment.
Public-key Cryptography	Public-key cryptography is a form of modern cryptography which allows users to communicate securely without previously agreeing on a shared secret. Unlike symmetric cryptography, it uses two keys -- a public key known to everyone and a private or secret key known only to the owner of the public and private key pair. Public key cryptography is also called asymmetric cryptography.
QnA	A challenge-response authentication mechanism, QnA allows for a back and forth dialog between the user agent and server, where the server asks arbitrary number of questions, and the user supplies correct answers.
Questions and Answers	See **QnA**.
RADIUS **Remote Authentication Dial In User Service**	Protocol for centralized Authentication, Authorization, and Accounting (AAA).
SAML	XML standard for exchanging authentication data between an identity provider (provides assertions) and a service provider (uses assertions).

Sample Application	Demonstrates the usage of WebFort Java APIs and how your application can be integrated with WebFort. It can also be used to verify if WebFort was installed successfully, and if is able to perform issuance and authentication operations.
Secure Hash Algorithm (SHA)	Secure Hash Algorithm (SHA) family is a set of cryptographic hash functions.
Security Assertion Markup Language	See SAML
Single Sign-On (SSO)	SSO refers to a single identity that is shared across multiple systems. SSO lets a user logon once to a computer or network and access multiple applications and systems using a single credential.
Secure Sockets Layer (SSL)	SSL is a protocol intended to secure and authenticate communications across public networks by using data encryption.
UDS	See User Data Service.
User Administrator (UA)	An administrator responsible for the day-to-day operations related to users of the security system. These administrators can assist users with enrollment, reset users passwords, and view a variety of enrollment reports.
User Data Service	Service that enables WebFort to access the existing LDAP-based user information or for mapping the LDAP users to the WebFort database.
User Name-Password	One of the credentials issued to the user during enrollment.
WebFort	Strong authentication system for authenticating end users.
WebFort Server	Server component that communicates with and accepts issuance and authentication requests from your application through WebFort SDKs.

Index

A

Administration Console 1
administrative user
    Global Administrator 9
    Master Administrator 8
    Organization Administrator 10
    User Administrator 10
ASSP 127
authentication policy 71
    ArcotID policy 82
    OTP policy 100
    QnA policy 88
    Username-Password policy 94

B

BA 31
Basic Authentication 31

C

callout 130
connection pooling 46
credential profile 71
    ArcotID profile 78
    OTP profile 97
    QnA profile 85
    Username-Password profile 91

D

Default Organization 28

E

enrollment 169
event 135

H

Handler file 59

I

instance 2
intended audience ix

L

log
    severity level 223
log level 223

O

organization 105

P

Plug-in 58
plug-in configuration template file 59
plug-in library file 59
preferred organization 151
profile 71

R

Roles 6
    administrative user 7
    Custom roles 14
    user 6

S

SAML 121
scope 7
system adminsitration tools 207

dbutil 208
system tool
arwfclient 212
arwfserver 210
dbutil 208

T

trust store 49

U

UDS 24
User Data Service 24