# Arcot WebFort® Administration Guide

## Version 5.4.1

ARCOT™

455 West Maude Avenue, Sunnyvale, CA 94085

Arcot WebFort Administration Guide
Version 5.4.1
June 2008
Part Number: AWF01-003DC-05400

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™, the Arcot logo™, WebFort®, ArcotID®, ArcotID Client™, are all trademarks or registered trademarks of Arcot Systems, Inc.

## 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

# Contents

# Preface

Welcome to the Arcot WebFort 5.4 Administration Guide. This guide covers the following topics:

- Description of WebFort Administration Console operations
- WebFort administrator levels
- WebFort configuration for communication with clients
- WebFort reports
- WebFort system administration tools

# About this Guide

This section describes the intended audience for this guide, contents of the guide, publications related to the guide and the conventions used across the guide.

## Intended Audience

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

This guide is intended for users who are experienced with:

- Running operating system-based administration operations, such as creating users and groups, adding users to groups, setting group policies and user rights
- Applicable Oracle and/or MS SQL databases
- Application servers
- Web server administration

## Information Included in this Guide

The chapter covered in this guide include:

- Chapter 1, "Understanding the WebFort Administration Console", provides introduction to Administration Console interface and administrator levels.
- Chapter 2, "Getting Started with Administration Console", describes the basic administrative tasks, such as enrolling administrators, logging in and out of Administration Console, changing the administrator password. It also discusses the procedures for creating, updating, and deleting administrator accounts.
- Chapter 3, "Configuring WebFort", discusses how to configure WebFort for your business needs.
- Chapter 4, "Working with Reports", discusses the various reports offered by WebFort.

- Chapter 5, "Tools for System Administrators", discusses the tools provided by WebFort that system administrators can use to monitor and manage the WebFort setup.
- Appendix A, "Configuring WebFort for Client-based VPN" lists the steps to configure WebFort to provide strong authentication to client-based VPNs.
- Appendix B, "Glossary" lists the key terms related to WebFort.

# Related Publications

Other related publications are as follows:

| | |
|---|---|
| *Arcot WebFort Installation and Deployment Guide* | This guide provides the information to install and configure WebFort and related components. |

# Conventions Used in This Book

The following typographical conventions are used in this guide:

| Type | Usage | Example |
|---|---|---|
| **Bold** | Screen Items | Click the **Register Now** link to enroll a user. |
| *Italic* | Key Words | First time log-in to *Administration Console* must be done using Master Administrator 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 Setting up the Protocol for more information. |
| `Fixed-width` | Command-line input or output | `# cd /opt/arcot` |
|  | Code Samples | `./webfortserver start` |
|  | Text File Content | `[arcot/db/primarydb]`<br>`# The name of the data source as`<br>`# defined in ODBC.`<br>`Datasource.1=ArcotWebFortDatabase` |
|  | File names | `arcotcommon.ini` |

# Chapter 1

# Understanding the WebFort Administration Console

Arcot WebFort Administration Console (referred to as Administration Console later in the guide) is a Web-based, operation and system management tool. It provides administrative functions, such as server configuration, protocol set up, and report generation that enables you to perform the typical administrative tasks relating to provisioning, updating, monitoring performance, and maintenance of WebFort and its components.

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

- Navigating the Administration Console
- Understanding the Administrator Levels

> **NOTE:** The recommended desktop setting for Administration Console screen is: 1024 x 768.

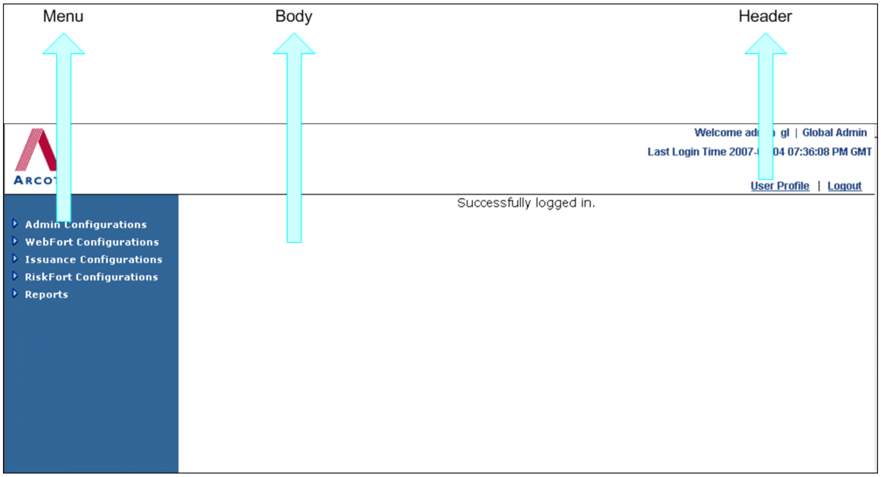
# Navigating the Administration Console

Administration Console provides a uniform user interface for all administrative levels (see "Understanding the Administrator Levels" for more information) supported by WebFort. A typical Administration Console screen can be divided into three frames:

- Header
- Menu
- Body

The following figure depicts the placement of these frames.

**Figure 1-1**



Welcome ad gl | Global Admin
Last Login Time 2007- 04 07:36:08 PM GMT

Successfully logged in.

Table 1-1 discusses the three-framed view of Administration Console user interface.

**Table 1-1** Administration Console User Interface Frames

| Frame | Description |
|---|---|
| **Header** | Displays login information (User Name, the last login date and time). The header displays the following links:<br>• **User Profile:** Displays the logged-in administrator's profile.<br>• **Logout:** Exits the Administration Console, when clicked. |
| **Menu** | Displays the configuration menu available to the current administrator. |

Table 1-1 Administration Console User Interface Frames

| Frame | Description |
|---|---|
| **Body** | Displays the task page for the selected menu. |

# Understanding the Administrator Levels

WebFort Administrative functions are distributed among three levels of administrators:

- Master Administrator
- Global Administrator
- Customer Support Representatives (CSRs)

> **NOTE:** WebFort currently supports two user groups that are available at the end of successful installation. These include, `GROUP2` (user group) and `ADMINISTRATORS` (administrator group).

The following sub-sections describe each administrator role, and the relationship between them.

## Master Administrator

The Master Administrator (MA) is the highest level of administrator. The primary responsibilities of the Master Administrator are to:

- Initialize the system after installation
- Manage Global Administrator accounts

At the end of the successful installation of Administration Console, you must log in for the first time as a Master Administrator using the following credentials:

- **User name:** *master_admin*
- **Password:** *master1234*

> **NOTE:** Arcot strongly recommends that you change the password after the first login. Refer to the section, "Changing the Administrator Password," for more information.

After you log in as Master Administrator for the first time, you must create Global Administrators.

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

As a Master Administrator, you can also view the activity logs of other administrators in the system.

## Global Administrator

Global Administrator (GA) is the second level of administrator. WebFort supports any number of GAs. The primary responsibilities of a Global Administrator include:

- Configuring the system and global settings
- Setting up the protocol
- Managing credential profiles for user group
- Managing administrators and their credentials
- Create Customer Support Representative (CSR) administrator
- Generating activity reports

GAs can view and generate activity reports of CSR Administrators assigned to them.

## Customer Support Representatives (CSRs)

Also known as CSR Administrators, these administrators are responsible for user management operations, such as resetting user credentials. CSRs can *only view* user reports.

CSR accounts are created by Global Administrators.

Chapter 2

# Getting Started with Administration Console

Administrators are the main users of the Administrative console. The primary responsibility of administrators include:

- Creating and updating administrative accounts
- Generating the domain key
- Configuring the authentication mechanisms
- Setting up the protocol

This chapter discusses the following administrative tasks:

- Performing Basic Administrative Tasks
- Managing Administrators

The chapter also provides a summary of administrative privileges available to different administrators in the "Administrators Privileges Summary" section.

Advanced tasks, such as generating domain key, setting up the protocols, and configuring authentication mechanisms are discussed in details in "Configuring WebFort".

# Performing Basic Administrative Tasks

All administrator groups can perform the following administrator-specific tasks:

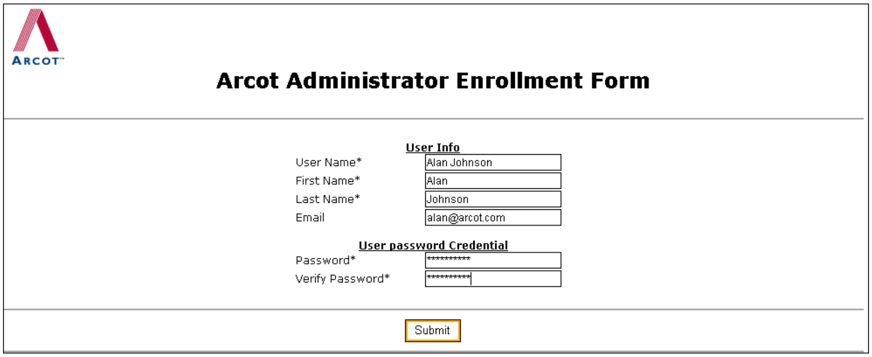
- Enrolling an Administrator
- Logging In and Out of the Administration Console
- Changing the Administrator Password

## Enrolling an Administrator

Administrative users must enroll themselves and obtain credentials to log in and perform the various administrative tasks.

The following figure displays the Enrollment page, used for the purpose of enrolling administrators.

**Figure 2-1**



**Arcot Administrator Enrollment Form**

User Info

| | |
|---|---|
| User Name* | Alan Johnson |
| First Name* | Alan |
| Last Name* | Johnson |
| Email | alan@arcot.com |

User password Credential

| | |
|---|---|
| Password* | ********** |
| Verify Password* | ********** |

**To enroll an administrative user, perform the following steps:**

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

   **`http://<server>:<port>/arcotadmin/adminlogin.htm`**

   The Login page appears.

3. Click the **Register Now** link on the Login page.

   The Arcot Administrator Enrollment Form (Figure 2-1) page appears.

4. Complete the enrollment form by entering the required details and click the **Submit** button.

   > **NOTE:** Fields marked with * are mandatory fields. The field **User Name** is not case sensitive.

After successful enrollment, you will be re-directed to the Administrator login page in 5 seconds.

> **NOTE:** Enrolled users can log in to the Administration Console only if they are promoted to be administrators of the system. See "Creating Administrator Accounts" for more information on promoting the users to administrators.

## Logging In and Out of the Administration Console

For the first time after installation, you can *only* log in to the Administration Console as Master Administrator using the following credentials:

- **User name:** *master_admin*
- **Password:** *master1234*

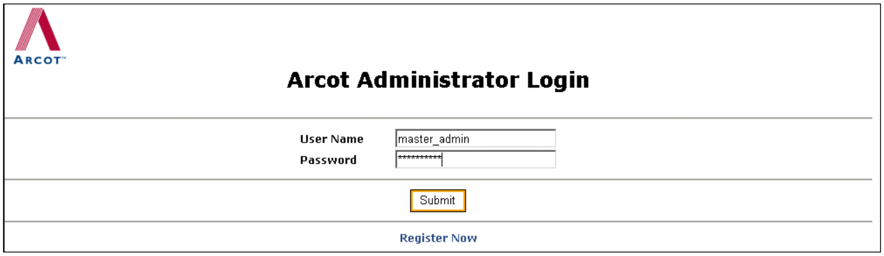
Subsequently to log in as any other administrator, you *must* first enroll the account. See "Enrolling an Administrator" for more information on enrolling an administrative accounts.

**To log in to the Administration Console, perform the following steps:**

1. Open Administration Console in a Web browser window.

   The Arcot Administrator Login page appears, as shown in the following figure.

**Figure 2-2**



Arcot Administrator Login

User Name master_admin

Password **********

2. Enter the **User Name**, **Password** of the Master Administrator, and click **Submit.**

   The "Successfully logged in" message appears.

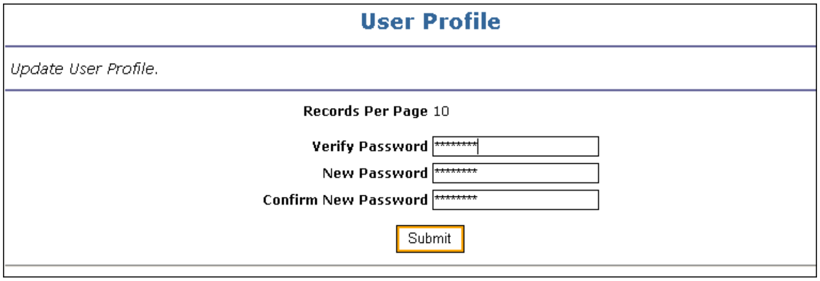
To log out of the Administration Console, click the **Logout** button. The Administration Login page appears.

# Changing the Administrator Password

> **NOTE:**Administrators can change their passwords according to the defined policies, see "Creating Password Profiles" for more information creating the password policies. It is highly recommended that you change the Master Administrator password after logging in to the console for the first time.

Use the User Profile page, shown in the following figure to change the administrator passwords.

**Figure 2-3** Changing the Administrator Password



User Profile

*Update User Profile.*

Records Per Page 10

Verify Password ********

New Password ********

Confirm New Password ********

**To change your administrator password:**

1. In Administration Console, click the **User Profile** link in the Header frame.

   The User Profile (Figure 2-3) page appears.

2. Enter the following information:
   - The current password in the **Verify Password** field.
   - The new password in the **New Password** field.
   - The new password again in the **Confirm New Password** field.
3. Click the **Submit** button.

   A success message appears indicating that the password is changed.

Use this new password to log in to Administration Console.

# Managing Administrators

This section discusses the following tasks related to managing administrators and their accounts:

- Creating Administrator Accounts
- Updating Administrator Accounts
- Enabling or Disabling the Administrator Accounts
- Deleting Administrator Accounts

## Creating Administrator Accounts

An administrator who belongs to one level can create other administrators who belongs to a lower level in the administrator level. For example:

- Master Administrator can create all other types of administrators.
- Global Administrator (GA) accounts can be created by the Master Administrator and, in turn, can create Customer Support Representative (CSR) accounts.

> **NOTE:** For more information on the privileges available to administrators at each level, refer to the "Administrators Privileges Summary" section.

The hierarchical level of an administrator is determined by the administrative policy, which is associated while creating the administrator account.

This section discusses the steps to create the following administrator accounts:

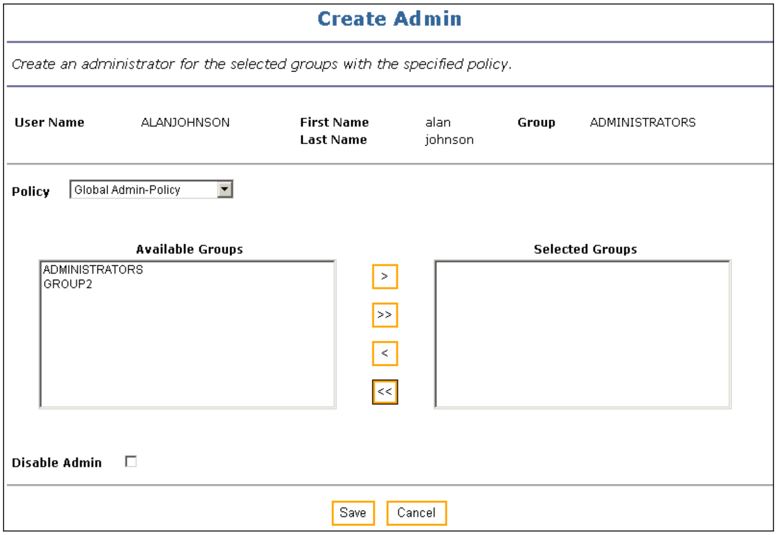
- Creating a Global Administrator Account
- Creating a CSR Account

### Creating a Global Administrator Account

Global Administrator (GA) is the second level of administrator. This section describes the steps to promote a admin user enrolled in the system to a GA.

The following figure shows the screen that you can use to create a GA.

**Figure 2-4**



Create Admin

*Create an administrator for the selected groups with the specified policy.*

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| **User Name** | ALANJOHNSON | **First Name**<br>**Last Name** | alan<br>johnson | **Group** | ADMINISTRATORS |

**Policy** Global Admin-Policy

**Available Groups**: ADMINISTRATORS, GROUP2

**Selected Groups**

**Disable Admin** □

## To create a GA account:

1. Log in to Administration Console with the Master Administrator credentials.
2. In the left pane, under **Admin Configurations**, click the **Create Admin** link.

   The User Search page appears.
3. Enter the partial or complete information of the user who needs to be promoted to GA and click **Search**.

   A list of administrators matching the search criteria appears.
4. Click the **User Name** in the **Create Admin- Search Results** of the user you want to promote as administrator.

   The Create Admin page appears with the user name you have selected.
5. To specify the level of the administrator, select the policy to be associated.

   Select **Global Admin Policy**, from the **Policy** drop-down list to create a GA.
6. Select the group from the **Available Groups** list and click the > button to add the group to the **Selected Groups** list.

   The **Available Groups** list displays all user groups who are under the administrative purview of Global Administrator.

7. The **Selected Groups** represents the groups that the newly created administrator will be managing. Select the group from the **Available Groups** and click the > button to add the group to the selected group.

8. Click the **Save** button, to create the GA.

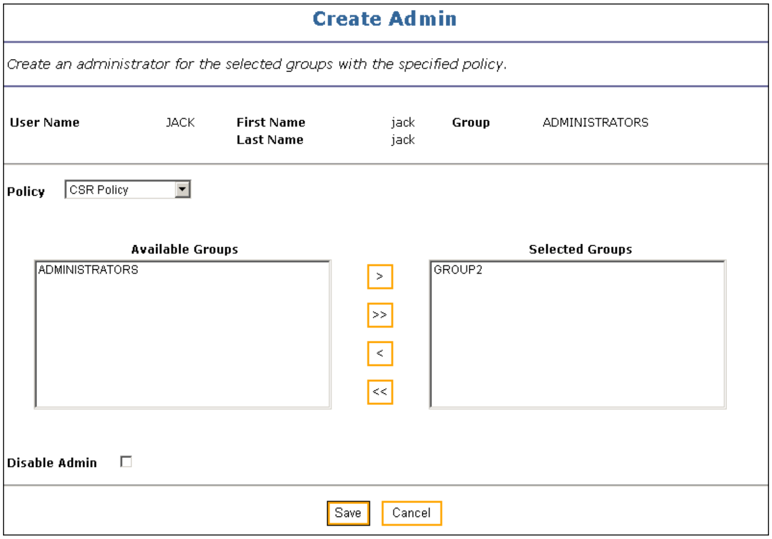
   The "Admin Created Successfully" message appears.

## Creating a CSR Account

Customer Support Representative (CSR)s are responsible for the user management operations in Administration Console. CSR can support only one group at a time.

Use the screen shown in the following figure to create a CSR.

**Figure 2-5**



Create Admin

*Create an administrator for the selected groups with the specified policy.*

| | | | | | |
|---|---|---|---|---|---|
| User Name | JACK | First Name<br>Last Name | jack<br>jack | Group | ADMINISTRATORS |

Policy: CSR Policy

Available Groups: ADMINISTRATORS

Selected Groups: GROUP2

Disable Admin □

**To create a CSR administrator:**

1. Log in to Administration Console using Global Administrator credentials.

2. In the left pane, under **Admin Configurations**, click the **Create Admin** link.

   The User Search page appears.

3. Enter the partial or complete information of the user who needs to be promoted to CSR and click **Search**.

   A list of administrators matching the search criteria appears.

4. Click the **User Name** in the **Create Admin- Search Results** of the user you want to promote as administrator.

   The Create Admin page appears with the user name you have selected.

5. To specify the level of the administrator, select the policy to be associated.

   Select **CSR Policy**, from the **Policy** drop-down list to create a CSR Administrator.

6. Select the group from the **Available Groups** list and click the > button to add the group to the **Selected Groups** list.

   The **Available Groups** list displays all user groups who are under the administrative purview of CSR Administrator.

7. The **Selected Groups** represents the groups that the newly created administrator will be managing. Select the group from the **Available Groups** and click the > button to add the group in the select group.

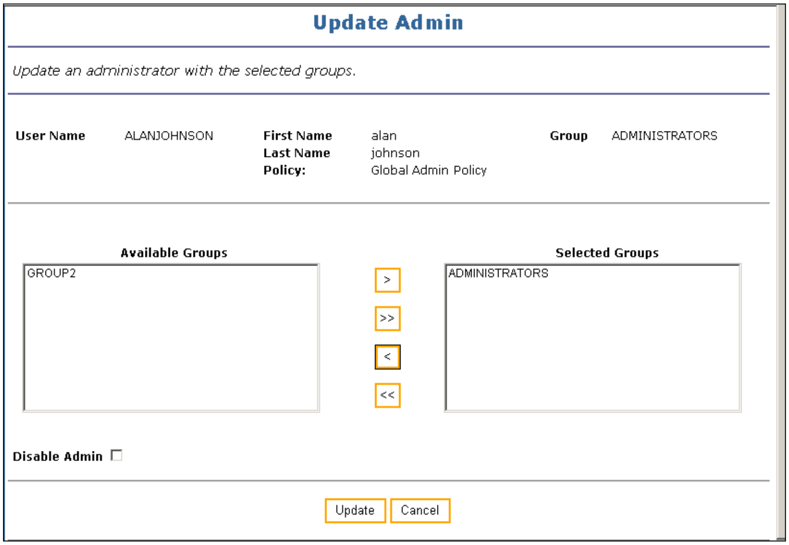
8. Click the **Save** button, to create the CSR.

   The "Admin Created Successfully" message appears.

# Updating Administrator Accounts

When you need to change the group(s) assigned to an administrator, you use the Update Admin page, shown in the following figure.

**Figure 2-6**



Update Admin

*Update an administrator with the selected groups.*

| | | | | | |
|---|---|---|---|---|---|
| **User Name** | ALANJOHNSON | **First Name** | alan | **Group** | ADMINISTRATORS |
| | | **Last Name** | johnson | | |
| | | **Policy:** | Global Admin Policy | | |

**Available Groups**: GROUP2

**Selected Groups**: ADMINISTRATORS

**Disable Admin** ☐

**To update an administrator account:**

1. In the left pane, under **Admin Configurations**, click the **Update Admin** link.

   The User Search page appears.

2. Enter the partial or complete information of the administrator whose account information needs to be updated and click **Search**.

   A list of administrators matching the search criteria appears.

3. Click the **User Name** in the **Update Admin- Search Results** of the administrator you want to update.

   The Update Admin page appears with the user name you have selected.

4. Make the required changes and click the **Update** button to update the selected administrator.

   The "Admin Updated Successfully" message appears.

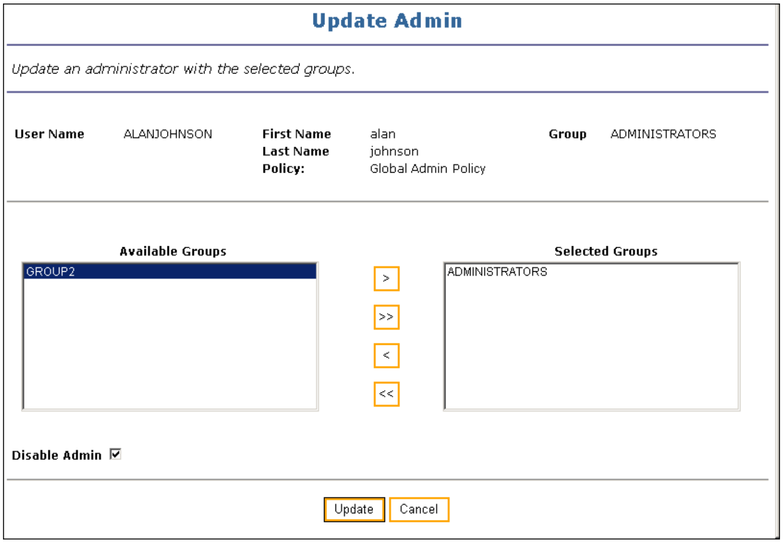
# Enabling or Disabling the Administrator Accounts

There might be situations when you need to disable an existing administrator account. For example, if an administrator might be leaving the organization or going on an extended leave of absence. Disabling an account locks the administrator out of the system.

Alternatively, there might be times when you need to enable a locked account. For example, when an administrator returns from an extended leave of absence.

Use the screen shown in the following figure to enable or disable an administrator account.

**Figure 2-7**



Update Admin

*Update an administrator with the selected groups.*

| | | | | | |
|---|---|---|---|---|---|
| **User Name** | ALANJOHNSON | **First Name** | alan | **Group** | ADMINISTRATORS |
| | | **Last Name** | johnson | | |
| | | **Policy:** | Global Admin Policy | | |

| **Available Groups** | **Selected Groups** |
|---|---|
| GROUP2 | ADMINISTRATORS |

**Disable Admin** ☑

**To enable or disable an administrator account:**

1. In the left pane, under **Admin Configurations**, click the **Update Admin** link.

   The User Search page appears.

2. Enter the partial or complete information of the administrator whose account needs to be enabled or disabled and click the **Search** button.

   A list of administrators matching the search criteria appears.

3. Click the **User Name** in the **Update Admin- Search Results** of the administrator you want to update.

   The Update Admin page appears with the user name you have selected.

4. Enable or disable the selected administrator account.

   **Disabling**

   When an administrator account is created, it is enabled by default. To disable an administrator account, check the **Disable Admin** checkbox.

   **Enabling**

   If the selected administrator account is disabled, then uncheck the **Disable Admin** checkbox to enable the account.

5. Click the **Update** button to reflect the changes.

   > **NOTE:** If an administrator whose account has been disabled tries to login, an error message appears.

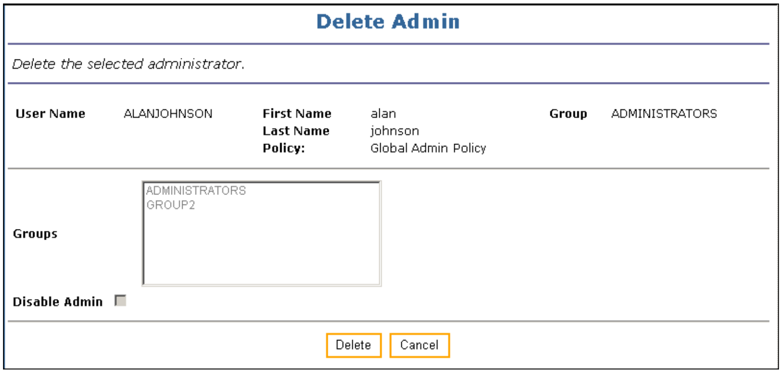
## Deleting Administrator Accounts

Sometime, you might need to delete an existing administrator account. For example, when an administrative user leaves the organization.

> **NOTE:** After an administrator account is deleted, the user can no longer log in to Administration Console. However, the user account and credentials are *not* removed from the system.

You must use the Delete Admin page, as shown in the following figure to delete an administrator account.

**Figure 2-8**



Delete Admin

*Delete the selected administrator.*

| | | | | | |
|---|---|---|---|---|---|
| **User Name** | ALANJOHNSON | **First Name** | alan | **Group** | ADMINISTRATORS |
| | | **Last Name** | johnson | | |
| | | **Policy:** | Global Admin Policy | | |

**Groups** ADMINISTRATORS<br>GROUP2

**Disable Admin** □

**To delete an administrator account:**

1. In the left pane, under **Admin Configurations**, click the **Delete Admin** link.

   The User Search page appears.

2. Enter the partial or complete information of the administrator whose account needs to be deleted and click **Search**.

   A list of administrators matching the search criteria appears.

3. Click the **User Name** in the **Delete Admin- Search Results** of the administrator you want to delete.

   The Delete Admin page appears with the user name you selected.

4. Click the **Delete** button to delete the administrator account.

   A pop-up window appears to confirm the deletion.

5. Click the **OK** button to delete the administrator.

   The "Admin Deleted Successfully" message appears.

   > **NOTE:** After deleting an administrator account, the user name is still present in the list of enrolled users. You can create the administrator again, if required.

# Administrators Privileges Summary

WebFort Administrative functions are distributed among three levels of administrators. Table 2-1 provides a summary of privileges available to different administrator levels.

✓indicates the action that are allowed to be performed by the Administrators. The field name acronyms used in the table are:

- Master Administrator --> MA
- Global Administrator --> GA
- CSR Administrator --> CSR

**Table 2-1** Administrators Privilege Table

| Feature | Action | MA | GA | CSR |
|---|---|---|---|---|
| **Administrator Configurations** | Create GA Account | ✓ | | |
| | Update GA Account | ✓ | | |
| | Delete GA Account | ✓ | | |
| | Create CSR Account | ✓ | ✓ | |
| | Update CSR Account | ✓ | ✓ | |
| | Delete CSR Account | ✓ | ✓ | |
| **WebFort Configurations** | Domain Key Generation | ✓ | | |
| | Protocol Setup | | ✓ | |
| | Authentication Configuration | | ✓ | |
| | RADIUS Configuration | | ✓ | |
| | Disable Credentials | ✓ | ✓ | ✓ |
| | Enable Credentials | ✓ | ✓ | ✓ |
| | Reset Credentials | ✓ | ✓ | ✓ |
| | Revoke Credentials | ✓ | ✓ | ✓ |

**Table 2-1** Administrators Privilege Table

| Feature | Action | MA | GA | CSR |
|---|---|---|---|---|
| **Issuance Configurations** | ArcotID Profiles | | ✓ | |
| | QnA Profiles | | ✓ | |
| | Password Profiles | | ✓ | |
| | OTP Profiles | | ✓ | |
| | Assign Profiles | | ✓ | |
| **Reports** | Administrator Activity Audit Report | ✓ | ✓ | |
| | Credential Management Report | | ✓ | ✓ |
| | Authentication Activity Report | | ✓ | ✓ |
| | User Credential Summary Report | | | ✓ |

# Chapter 3

# Configuring WebFort

This chapter describes tasks for administering WebFort using Administration Console. The administrator can perform the following operations using Administration Console:

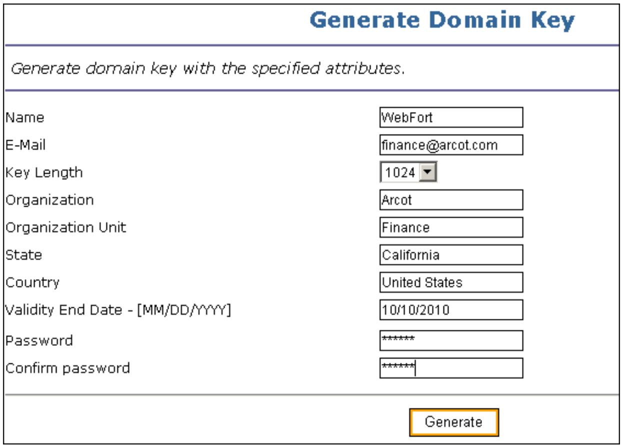
- Generating the Domain Key
- Setting up the Protocol
- Configuring for RADIUS
- Configuring WebFort Authentication Methods
- Configuring the Credentials
- Configuring for Issuance

# Generating the Domain Key

WebFort uses Domain Key to issue ArcotIDs to users and to validate ArcotID-based user authentications. Administration Console supports the secure creation and storage of domain key for use by WebFort server.

Domain key is generated using the Generate Domain Key page, see the following figure.

**Figure 3-1**



Generate Domain Key

*Generate domain key with the specified attributes.*

| | |
|---|---|
| Name | WebFort |
| E-Mail | finance@arcot.com |
| Key Length | 1024 |
| Organization | Arcot |
| Organization Unit | Finance |
| State | California |
| Country | United States |
| Validity End Date - [MM/DD/YYYY] | 10/10/2010 |
| Password | ****** |
| Confirm password | ****** |

**To generate a Domain Key:**

1. Open Administration Console in a Web browser window.
2. In the left pane, under **WebFort Configurations** menu click the **Generate Domain Key** link.

   The Generate Domain Key page appears.
3. Fill the form. See Table 3-1 for more information on form fields. Click the **Generate** button to create the Domain key.

   **NOTE:** Data in all the fields are mandatory.

**Table 3-1** Domain Key Creation Form fields

| Form Fields | Description |
|---|---|
| **Name** | Enter the common name for the subject field of the domain key. |

**Table 3-1** Domain Key Creation Form fields

| Form Fields | Description |
|---|---|
| **E-mail** | It is recommended you leave this field blank as it is visible to end-users who will install the ArcotID Native client.<br>You can optionally enter email address of the support group in your organization.<br>**Example**: support@safebank.com |
| **Key Length** | Select the length of the domain key. The Key can be 512, 1024 or 2048 bits in length. |
| **Organization** | Enter the name of your organization.<br>**Example**: SafeBank |
| **Organization Unit** | It is recommended you leave this field blank as it is visible to end-users who will install the ArcotID Native client.<br>You can optionally enter the name of the business unit that runs Web-Fort Server<br>**Example**: IT Operations |
| **State** | Enter the name of your state. |
| **Country** | Enter the name of your country. |
| **Validity End Date - [mm/dd/yyyy]** | Specify the period for which the Domain Key is valid.<br>Arcot recommends that Domain key be valid for at least for 5 years, this avoids frequent re-issue of ArcotIDs. |
| **Password** | Enter the password is used for secure storage of the domain key created. Provide a strong password to protect your domain key. |
| **Confirm password** | Re-enter the password to confirm it. |

On successful creation of the Domain key, the "Domain-Key successfully generated" message appears.

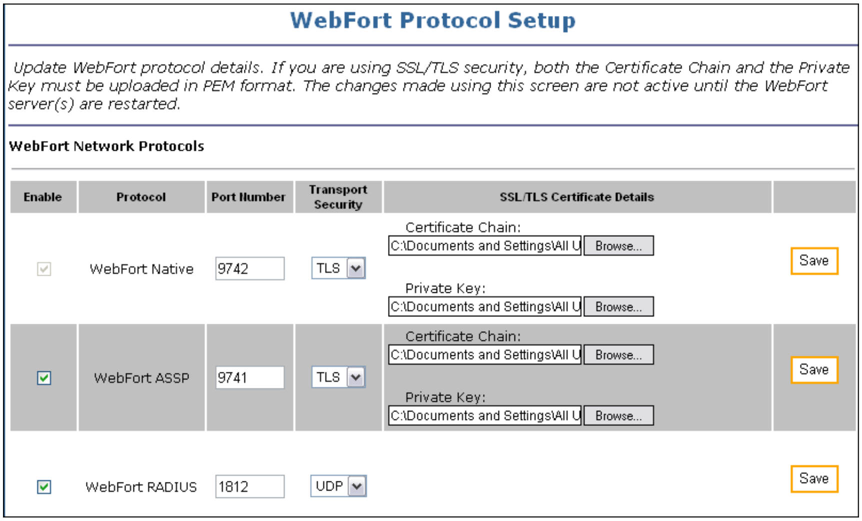
# Setting up the Protocol

WebFort must be configured so that it can communicate with clients. The port on which the server listens for each protocol can be configured using the WebFort Protocol Setup page. These protocols are:

- WebFort Native Protocol Module
- WebFort ASSP Protocol Module
- WebFort RADIUS Protocol Module
- Server Management Protocol Module

WebFort supports protocols that are used by clients to communicate with the server for the purpose of authentication and administration. The port on which WebFort Server listens for each protocol can be configured by using the *WebFort Protocol Setup* page.

**Figure 3-2**



WebFort Protocol Setup

*Update WebFort protocol details. If you are using SSL/TLS security, both the Certificate Chain and the Private Key must be uploaded in PEM format. The changes made using this screen are not active until the WebFort server(s) are restarted.*

**WebFort Network Protocols**

| Enable | Protocol | Port Number | Transport Security | SSL/TLS Certificate Details | |
|---|---|---|---|---|---|
| ☑ | WebFort Native | 9742 | TLS | Certificate Chain: C:\Documents and Settings\All U Browse...<br>Private Key: C:\Documents and Settings\All U Browse... | Save |
| ☑ | WebFort ASSP | 9741 | TLS | Certificate Chain: C:\Documents and Settings\All U Browse...<br>Private Key: C:\Documents and Settings\All U Browse... | Save |
| ☑ | WebFort RADIUS | 1812 | UDP | | Save |

**To configure WebFort network protocols:**

1. Open the Administration Console in a Web browser window.
2. In the left pane, under **WebFort Configurations** menu click the **Protocol Setup** link.

   The WebFort Protocol Setup page appears.

3. Configure the following parameters for a network protocol:

   a. **Protocol enabling**

      Use the check box in the **Enable** column, to enable the protocol.

      **NOTE:** The WebFort Native and Server Management Protocol is enabled by default.

   b. **Protocol**

      The following are the network protocols supported by WebFort:

      - **WebFort Native:** This is a proprietary, binary protocol supported by WebFort for the purpose of authentication. This port is used by SDK and Web Service APIs of Authentication and Issuance
      - **WebFort ASSP:** This protocol is used with Adobe® Reader and Adobe® Acrobat® to authenticate user for server-side digital signing of the PDF documents. Digital signing, in itself, is not in scope of WebFort.
      - **WebFort RADIUS:** This is used to support the Remote Authentication Dial In User Service (RADIUS) protocol. When configured to support RADIUS protocol, WebFort server acts as a RADIUS server.
      - **Server Management:** This protocol is used to manage WebFort server.

   c. **Port Number**

      Enter the port number where the WebFort service is available. The following are the default port numbers for WebFort network protocols:

      - WebFort Native - 9742
      - WebFort ASSP - 9741
      - WebFort RADIUS - 1812
      - Server Management - 9743

   d. **Transport Security**

      The following are the modes supported for data transfer.

      - **TCP** - Transmission Control Protocol (TCP) mode is supported by all WebFort network protocols other than WebFort RADIUS protocol.
      - **TLS** - Transport Layer Security (TLS) uses the PKI to encrypt and decrypt data under transmission. See **“Configuring TLS Communication (Optional)”** for more details.

**NOTE:** WebFort RADIUS protocol does not support TLS transport mode.

- **UDP** - User Datagram Protocol (UDP) is used for WebFort RADIUS protocol.

4. Click the **Save** button for the protocol, after the configurations are completed.

## Configuring TLS Communication (Optional)

By default, Administration Console uses Transmission Control Protocol (TCP) to communicate with WebFort Server. However, TCP is vulnerable to spoofing and man-in-the-middle attacks. To ensure secure communication between Administration Console and WebFort Server, you can configure WebFort Native protocol to TLS (Transport Layer Security).

To configure WebFort Native Protocol:

1. Under **WebFort Configurations** from the left-hand menu, select **Protocol Setup.**

   The WebFort Protocol Setup page appears, as shown in Figure 3-2.

2. Perform the following steps to configure the WebFort Native protocol for TLS:

   a. In the **Enable** column, ensure that the check box for the protocol to be enabled for TLS is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      I. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the SSL certificate chain for the server.

      **NOTE:** The certificates in the chain *must* start from Leaf certificate, Intermediate CA certificates, and then Root certificate.

      II. Click **Browse** against **Private Key** to navigate to the appropriate location and upload the corresponding private key of the certificate.

      **NOTE:** The certificate chain and the private key, both *must* be in `.PEM` format private key uploaded must be not be password protected.

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

3. Configure the `adminserver.ini` file as follows:

   a. Navigate to the following location:

   `<install_location>\Arcot Systems\conf\`

b. Open the `adminserver.ini` file in an editor window.

c. In the `[arcot/admin/authconfig]` section, set the following parameters:

- `transport=TLS` (By default, this parameter is set to TCP.)
- `server.CACert=<`*`absolute_path_of_Root_Certificate`*`>`

**NOTE:** Server CA certificate file name must not contain spaces.

d. Save the changes and close the file.

4. Restart WebFort Server as follows:

a. Click the **Start** button on your desktop window.

b. Navigate to **Settings** -> **Control Panel** -> **Administrative Tools** -> **Services.**

c. Locate and double-click the following services:

i. **Arcot WebFort Authentication Service**

ii. Click the **Stop** button in each service's window to stop the respective service.

iii. Click the **Start** button in each service's window to start the respective service.

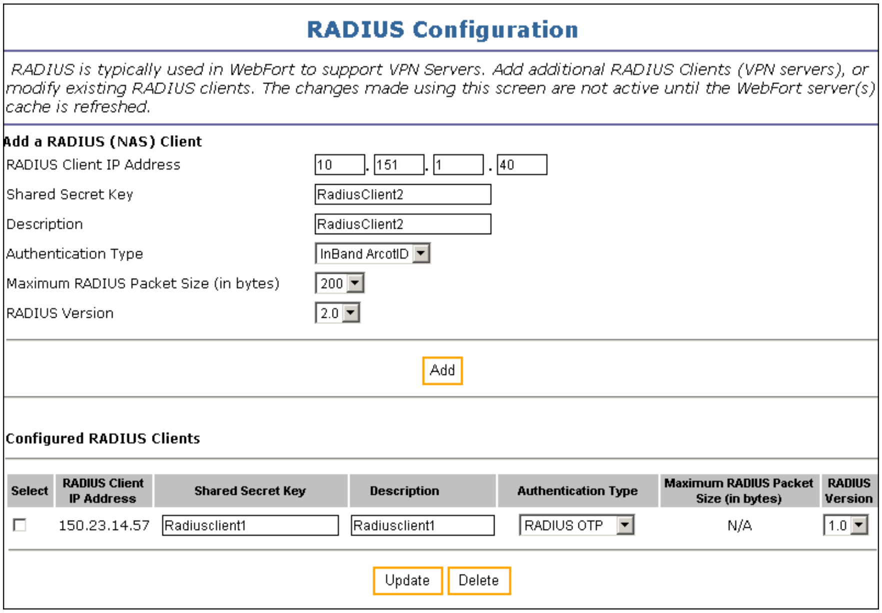
5. Restart Administartion Console.

# Configuring for RADIUS

RADIUS protocol is supported by WebFort to enable integration with different VPN vendors. This screen collects the Network Access Server (NAS)/RADIUS client information. Only the configured RADIUS clients are served by WebFort.

The RADIUS Configuration is done using the screen shown in the following figure.

**Figure 3-3**



RADIUS Configuration

*RADIUS is typically used in WebFort to support VPN Servers. Add additional RADIUS Clients (VPN servers), or modify existing RADIUS clients. The changes made using this screen are not active until the WebFort server(s) cache is refreshed.*

**Add a RADIUS (NAS) Client**

| | |
|---|---|
| RADIUS Client IP Address | 10 . 151 . 1 . 40 |
| Shared Secret Key | RadiusClient2 |
| Description | RadiusClient2 |
| Authentication Type | InBand ArcotID |
| Maximum RADIUS Packet Size (in bytes) | 200 |
| RADIUS Version | 2.0 |

**Configured RADIUS Clients**

| Select | RADIUS Client IP Address | Shared Secret Key | Description | Authentication Type | Maximum RADIUS Packet Size (in bytes) | RADIUS Version |
|---|---|---|---|---|---|---|
| ☐ | 150.23.14.57 | Radiusclient1 | Radiusclient1 | RADIUS OTP | N/A | 1.0 |

**To configure the RADIUS protocol support:**

1. Open Administration Console in a Web browser window.
2. In the left pane, under **WebFort Configurations** menu, click the **RADIUS Configuration** link.

   The RADIUS Configuration page appears.
3. 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 RADIUS server.

- **Shared Secret Key** - The secret that is shared between the RADIUS client and the WebFort server. The same shared secret key must be configured on the RADIUS client in a secure manner.

  **NOTE:** The minimum length of key is *1* and the maximum length 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 type of authentication that is used for Virtual Private Network (VPN) authentication.

  - **RADIUS OTP** is used for client-less VPNs. These are the VPN setups that do not need a client to be installed on the end-user computer. Most SSL VPNs do not require the client to be installed on the end-user computer.

  - **InBand ArcotID** is used for client-based VPNs. These are the VPN setups that need a client to be installed on the end-user computer. Most IPSec VPNs and some SSL VPNs need an installed client on the end-user computer. See Appendix A, “Configuring WebFort for Client-based VPN for more information on configuring WebFort for using with client-based VPN.

  **NOTE:** After performing InBand ArcotID configuration you must re-start the WebFort server for successful configuration.

- **Maximum RADIUS Packet Size** - If the authentication type selected in the preceding step is **InBand ArcotID**, then select the packet size at which the RADIUS messages are transferred. Refer to the VPN vendor manual to check the maximum packet size allowed by the VPN vendor on RADIUS.

- **RADIUS Version** - This is the version of the supported RADIUS protocol. Refer to the VPN vendor manual to check the RADIUS version supported. Select the highest version that is common to both VPN vendor and WebFort.

4. Click the **Add** button to add the IP address of the new RADIUS client.

The RADIUS configuration page also displays the table **Configured RADIUS Clients,** which helps to update or delete the RADIUS client IP addresses.

**To delete the RADIUS client:**

1. Check the **Select** check box of the RADIUS client IP address you want to delete.
2. Click the **Delete** button.

**To update the RADIUS client:**

1. Check the **Select** check box of the RADIUS client IP address you want to update.
2. Update any of the column for the selected IP address and click the **Update** button.

# Configuring WebFort Authentication Methods

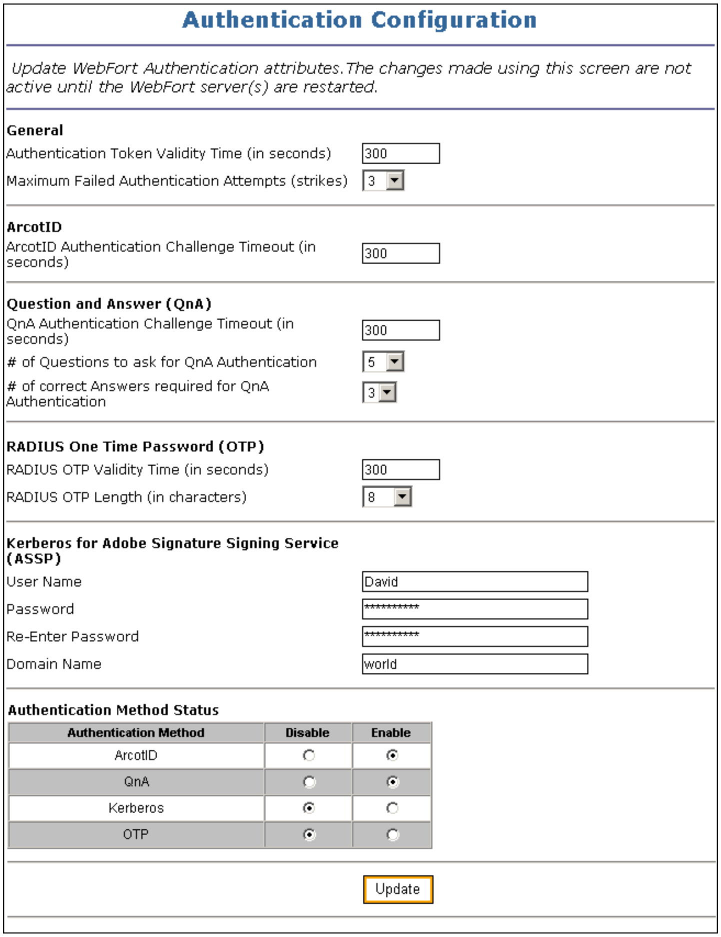
WebFort supports authentication methods, such as ArcotID, QnA, UserName /Password, OTP, and Kerberos authentications. Several aspects of these authentication methods can be configured by using the Authentication Configuration page.

Refer to *Arcot WebFort Installation and Deployment Guide* for more information about the authentication methods supported.

> **NOTE:** It is strongly recommended that the following set of configurations must be done by an advanced user of the system who has sufficient knowledge of general authentication protocols and has a good understanding of the Authentication methods supported by Arcot WebFort.

The following figure shows the Authentication Configuration page.

**Figure 3-4**



## Authentication Configuration

*Update WebFort Authentication attributes.The changes made using this screen are not active until the WebFort server(s) are restarted.*

**General**

| | |
|---|---|
| Authentication Token Validity Time (in seconds) | 300 |
| Maximum Failed Authentication Attempts (strikes) | 3 |

**ArcotID**

| | |
|---|---|
| ArcotID Authentication Challenge Timeout (in seconds) | 300 |

**Question and Answer (QnA)**

| | |
|---|---|
| QnA Authentication Challenge Timeout (in seconds) | 300 |
| # of Questions to ask for QnA Authentication | 5 |
| # of correct Answers required for QnA Authentication | 3 |

**RADIUS One Time Password (OTP)**

| | |
|---|---|
| RADIUS OTP Validity Time (in seconds) | 300 |
| RADIUS OTP Length (in characters) | 8 |

**Kerberos for Adobe Signature Signing Service (ASSP)**

| | |
|---|---|
| User Name | David |
| Password | *********** |
| Re-Enter Password | *********** |
| Domain Name | world |

**Authentication Method Status**

| Authentication Method | Disable | Enable |
|---|---|---|
| ArcotID | ○ | ● |
| QnA | ○ | ● |
| Kerberos | ● | ○ |
| OTP | ● | ○ |

### To configure authentication parameters:

1. Open Administration Console in a Web browser window.

2. In the left pane, under **WebFort Configurations** menu, click the **Authentication Configuration** link.

   The Authentication Configuration page appears.

3. You can perform the following operations using this screen:

   a. **General Configuration**

i. Set the duration for which the Authentication token is valid in the **Authentication Token Validity Time** field.

**NOTE:** The time displayed is in seconds.

ii. Enter the **Maximum Failed Authentication Attempts** that a user can make. Maximum strikes are the number of times the user can fail authentication before their credentials are locked.

The user's access to the system is locked when the number of wrong attempts made during authentication is equal to the Maximum Strikes count.

b. **ArcotID Configuration**

Set the time for ArcotID authentication challenge timeout in the **ArcotID Authentication Challenge Timeout** field.

c. **QnA Configuration**

i. Set the time for QnA authentication challenge timeout in the **QnA Authentication Challenge Timeout** field.

ii. Select the number of questions that should be asked for QnA authentication in the **# of Questions to ask for QnA Authentication** field.

iii. Select the required number of correct answers to authenticate the user in the **# of correct Answers required for QnA Authentication** field.

d. **RADIUS OTP Configuration**

i. Enter the validity period for One Time Password (OTP) for RADIUS Token in **RADIUS OTP Validity Time** field. The OTP is used in SSL VPN authentication. The default validity period is 300 seconds.

ii. Select the length for the OTP in the **RADIUS OTP Length** field. The default length of OTP is 8.

e. **Kerberos Configuration**

Configure the information required for the Kerberos authentication. WebFort can verify Kerberos ticket for the users from the same domain for which the valid credentials of the user from a particular domain are needed:

i. **User Name**: Name of the user with which WebFort will log in to the domain for verifying the Kerberos tickets.

ii. **Password**: Password associated with the user name.

iii. **Re-Enter Password**: Confirm the password in this field.

iv. **Domain Name**: The name of the domain, to which the user belongs to.

f. **Enabling the authentication method**

Enable the type of authentication required using **Authentication Method Status** table.

4. Click the **Update** button to set the new configurations.

**NOTE:** Restart the WebFort server by using the services from control panel.

# Configuring the Credentials

User credentials operations that are supported are:

- Disabling Credentials
- Enabling Credentials
- Resetting Credentials
- Revoking Credentials

> **NOTE:** Few of the above actions might be allowed on a sub-set of credentials. Refer to the description of the action to find these exceptions.

Administrators obtain and use WebFort credentials for logging in to Administration Console. As a result, credentials of administrators can also be managed in the same manner as other user credentials.

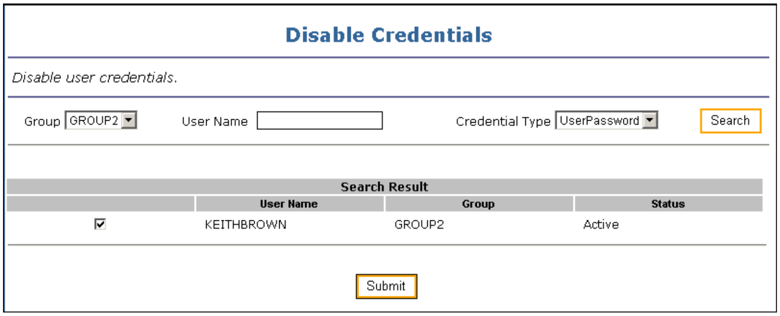
## Disabling Credentials

The credentials of a user can be disabled temporarily in a corporate environment. For example, if an employee goes on an extended leave, the required department should be able to lock their account in order to prevent unintended access.

User credentials are locked, if the user exceeds the number of minimum failed authentication attempts.

The following figure shows the page used for disabling credentials.

**Figure 3-5**



Disable Credentials

*Disable user credentials.*

Group: GROUP2 User Name: Credential Type: UserPassword

Search Result

| | User Name | Group | Status |
|---|---|---|---|
| ☑ | KEITHBROWN | GROUP2 | Active |

**To disable credentials:**

1. Open Administration Console in a Web browser window.
2. In the left pane, under **WebFort Configurations** menu, click the **Disable Credentials** link.

   The Disable Credentials page appears.
3. Select the group name and provide a complete or a partial user name of the user in the **User Name** field.
4. Select the type of the credential to be disabled from the drop-down list in the **Credential Type** field and click the **Search** button.

   A list of users matching the search criteria appears.
5. Check the user whose credential has to be disabled and click the **Submit** button.

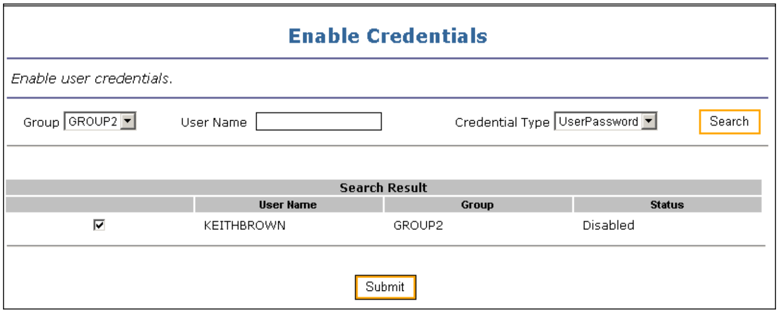
   The credential of the selected user is disabled. Use of a disabled credential will result in failed authentication attempts.

# Enabling Credentials

Administration Console permits administrators to enable credentials that are disabled or locked out. When the credential is enabled, it can be used for normal authentication purposes with WebFort.

The following figure shows the page used for enabling credentials.

**Figure 3-6**



Enable Credentials

*Enable user credentials.*

Group GROUP2 ▾ User Name Credential Type UserPassword ▾ Search

Search Result

| | User Name | Group | Status |
|---|---|---|---|
| ☑ | KEITHBROWN | GROUP2 | Disabled |

Submit

**To enable Credentials:**

1. Open Administration Console in a Web browser window.

2. In the left pane, under **WebFort Configurations** menu, click the **Enable Credentials** link.

   The Enable Credentials page appears.

3. Select the **Group** name and provide a complete or a partial user name in the **User Name** field.

4. Select the type of the credential to be enabled from the drop-down list in the **Credential Type** field and click the **Search** button.

   The list of users matching the search criteria appears.

5. Check the user whose credential has to be enabled and click the **Submit** button.

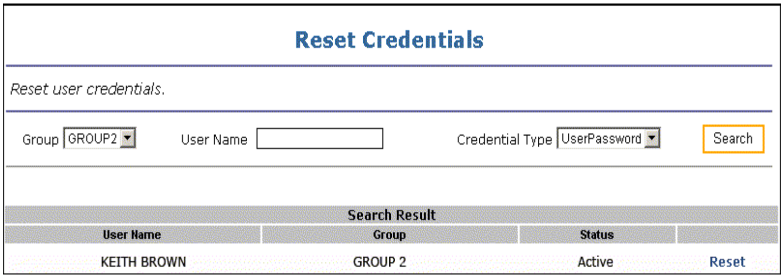
   The selected credential is enabled for the user.

# Resetting Credentials

Administration Console allows you to reset both the user password and the ArcotID password. After resetting the password successfully, the user must login with the new password.

The following figure shows the page used for resetting credentials.

**Figure 3-7**



Reset Credentials

*Reset user credentials.*

Group: GROUP2 User Name: Credential Type: UserPassword

Search Result

| User Name | Group | Status | |
|---|---|---|---|
| KEITH BROWN | GROUP 2 | Active | Reset |

**To reset user password:**

1. Open Administration Console in a Web browser window.

2. In the left pane, under **WebFort Configurations** menu, click the **Reset Credentials** link.

   The Reset Credentials page appears.

3. Select the group name and provide a complete or a partial user name of the user in the **User Name** field.

4. In the **Credential Type** drop-down list, select **UserPassword** and click the **Search** button.

   A list of users matching the search criteria appears.

5. Click the **Reset** button for the user whose password has to be reset.

   The task page for resetting the password appears.

6. Enter the new password for the chosen credential in the **Password** field, re-enter the same password to confirm the new password in the **Confirm password** field and click the **Submit** button.

   The new password for the user is updated and the Reset Credentials page appears.

**To reset ArcotID PIN:**

1. Open Administration Console in a Web browser window.

2. In the left pane, under **WebFort Configurations** menu, click the **Reset Credentials** link.

   The Reset Credentials page appears.

3. Select the group name and provide a complete or a partial user name of the user in the **User Name** field.

4. In the **Credential Type** drop-down list, select **ArcotID** and click the **Search** button.

   A list of users matching the search criteria appears.

5. Click the **Reset** button for the user whose ArcotID PIN has to be reset.

   The task page for resetting the ArcotID PIN appears.

6. Enter the new PIN for the chosen credential in the **PIN** field, re-enter the same PIN to confirm the new PIN in the **Confirm PIN** field and click the **Submit** button.

7. The new PIN for the ArcotID is updated and the Reset Credentials page appears.

# Revoking Credentials

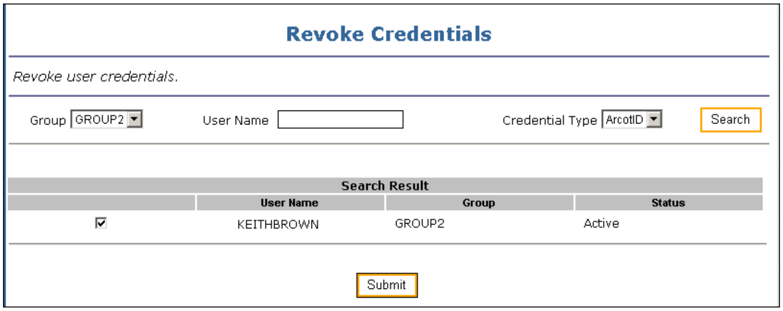
Administration Console permits the administrators to revoke credentials.

> **NOTE:** Only ArcotIDs can be revoked.

Revocation of ArcotID is similar to revocation of user certificates in a PKI system. Any authentication attempts using a revoked ArcotID will be rejected by WebFort server. Therefore, revocations should be done with care and in accordance with policies and procedures of your organizations.

The following figure shows the page used for revoking credentials.

**Figure 3-8**



Revoke Credentials

*Revoke user credentials.*

Group: GROUP2 User Name: Credential Type: ArcotID

Search Result

| | User Name | Group | Status |
|---|---|---|---|
| ☑ | KEITHBROWN | GROUP2 | Active |

**To revoke a credential:**

1. Open Administration Console in a Web browser window.

2. In the left pane, under **WebFort Configurations** menu, click the **Revoke Credentials** link.

   The Revoke Credentials page appears.

3. Select the group name and provide a complete or a partial user name of the user in the **User Name** field and click the **Search** button.

   A list of users matching the search criteria appears.

4. Check the user whose ArcotID has to be revoked and click the **Submit** button.

   The credential for the user is revoked.

# Configuring for Issuance

Issuance configurations enable the creation of profiles for all the credential types supported by Arcot WebFort. Profiles can be associated with user groups. WebFort makes use of the configured profiles at the time of issuing credentials to users.

Credential Profiles specify settings for credential attributes, such as validity period, key strengths, minimum lengths for passwords, etc. This section describes the following profiles:

- Creating ArcotID Profiles
- Creating QnA Profiles
- Creating Password Profiles
- Creating OTP Profiles
- Assigning Profiles

## Creating ArcotID Profiles

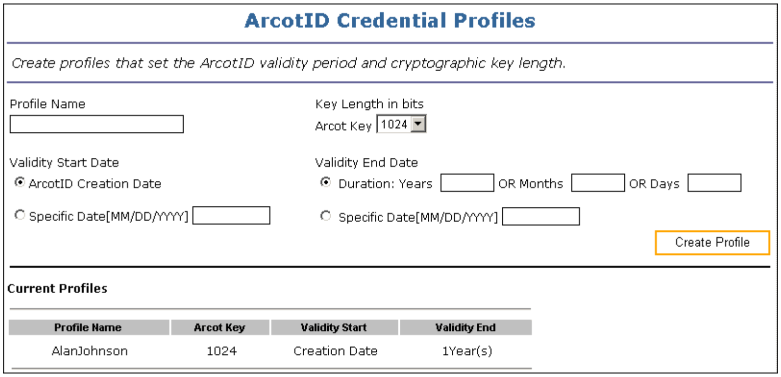
An ArcotID profile can be used to specify the following attributes:

- **Key Strength**- The key strength for the ArcotIDs created.
- **Validity period**- The validity period for the ArcotIDs created.

By assigning an ArcotID profile to a user group, an administrator can control the characteristics of ArcotIDs that are issued to users of the group.

The following figure shows the page used for creating ArcotID profile.

**Figure 3-9**



ArcotID Credential Profiles

*Create profiles that set the ArcotID validity period and cryptographic key length.*

Profile Name

Key Length in bits
Arcot Key 1024

Validity Start Date
● ArcotID Creation Date
○ Specific Date[MM/DD/YYYY]

Validity End Date
● Duration: Years OR Months OR Days
○ Specific Date[MM/DD/YYYY]

Current Profiles

| Profile Name | Arcot Key | Validity Start | Validity End |
|---|---|---|---|
| AlanJohnson | 1024 | Creation Date | 1Year(s) |

**To create an ArcotID profile:**

1. Open Administration Console in a Web browser window.
2. In the left pane, under **Issuance Configurations** menu, click the **ArcotID Profiles** link.

   The ArcotID Credential Profiles page appears.
3. Enter the profile name in the **Profile Name** field.
4. Select the key length for encryption from the **Arcot Key** drop-down list.
5. Set the duration for which the profile is valid in the **Validity Start Date** and **Validity End Date** fields.
6. Click the **Create Profile** button to create a new ArcotID profile.

   The "ArcotID Profile created successfully" message appears and the profile is listed in the **Current Profiles** table.

# Creating QnA Profiles

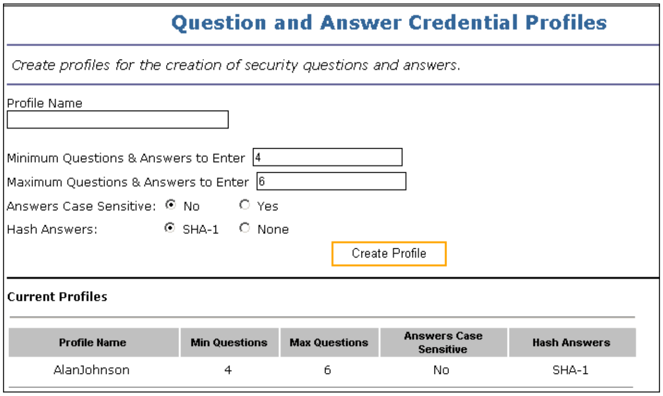
A Question and Answer (QnA) profile can be used to specify the following attributes for QnA credentials:

- Minimum number of questions and answers to be entered by user at the time of enrollment.
- Maximum number of questions and answers to be entered by user at the time of enrollment.

By assigning a QnA profile to a user group, an administrator can control the preceding aspects during the issuance of QnA credentials to users of the group.

The following figure shows the page used for creating QnA profile.

**Figure 3-10**



Question and Answer Credential Profiles

*Create profiles for the creation of security questions and answers.*

Profile Name

Minimum Questions & Answers to Enter 4

Maximum Questions & Answers to Enter 6

Answers Case Sensitive: ● No ○ Yes

Hash Answers: ● SHA-1 ○ None

**Current Profiles**

| Profile Name | Min Questions | Max Questions | Answers Case Sensitive | Hash Answers |
|---|---|---|---|---|
| AlanJohnson | 4 | 6 | No | SHA-1 |

### To create a QnA profile:

1. Open Administration Console in a Web browser window.
2. In the left pane, under **Issuance Configurations** menu, click the **QnA Profiles** link.

   The QnA Credential Profiles page appears.
3. Enter the profile name in the **Profile Name** field.
4. Enter the minimum answers to be answered in the **Minimum Questions & Answers to Enter** field.
5. Enter the maximum questions to be asked in the **Maximum Questions & Answers to Enter** field.
6. Select **No** for the answers not to be stored in case-sensitive format.

   If **Yes** is selected, then the answers supplied by the enrolling user are stored in case sensitive format.
7. Select the option **SHA-1** for the answers to be hashed. (For example: If the answers supplied by enrolling users, should be stored securely by using the hash functions or not.)

   If **None** is selected, the hash function is disabled.

8. Click the **Create Profile** button to create the new QnA profile.

   The "QnA Profile created successfully" message appears and the profile is listed in the **Current Profiles** table.

## Creating Password Profiles

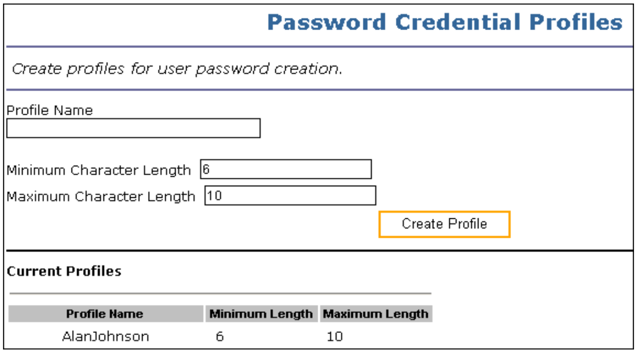
A Password profile can be used to specify the following attributes for Password credentials:

- Minimum length of password
- Maximum length of password

By assigning a Password profile to a user group, an administrator can control the preceding aspects during the issuance of Password credentials to users of the group.

The following figure shows the page used for creating Password profile.

**Figure 3-11** Password Profile



Password Credential Profiles

*Create profiles for user password creation.*

Profile Name

Minimum Character Length 6

Maximum Character Length 10

Current Profiles

| Profile Name | Minimum Length | Maximum Length |
|---|---|---|
| AlanJohnson | 6 | 10 |

**To create a Password profile:**

1. Open Administration Console in a Web browser window.
2. In the left pane, under **Issuance Configurations** menu, click the **Password Profiles** link.

   The Password Credential Profiles page appears.
3. Enter the profile name in the **Profile Name** field.
4. Enter the minimum character length for the password in the **Minimum Character Length** field.

5. Enter the maximum character length for the password in the **Maximum Character Length** field.

6. Click the **Create Profile** button to create a new password profile.

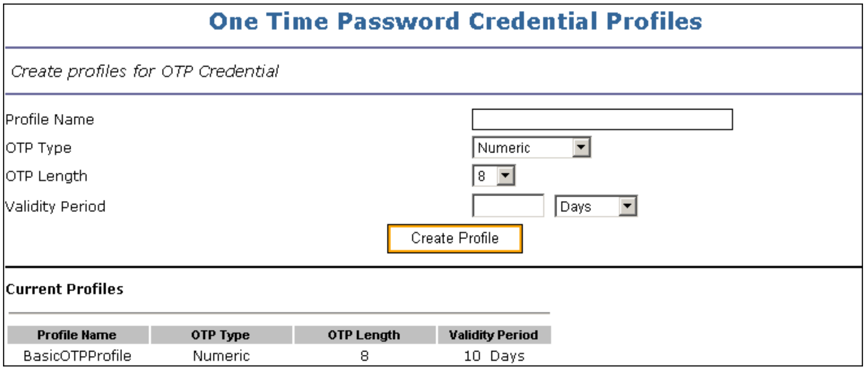
   The "Password Profile created successfully" message appears and the profile is listed in the **Current Profiles** table.

## Creating OTP Profiles

One Time Password (OTP) credentials are used to authenticate to WebFort. The OTP credential is valid for a pre-configured period and can be used only once. The OTPs can be distributed to the user through email, support representative, or any other pre-configured method.

The following figure shows the page used for creating OTP profile.

**Figure 3-12**



One Time Password Credential Profiles

*Create profiles for OTP Credential*

| | |
|---|---|
| Profile Name | |
| OTP Type | Numeric |
| OTP Length | 8 |
| Validity Period | Days |

**Current Profiles**

| Profile Name | OTP Type | OTP Length | Validity Period |
|---|---|---|---|
| BasicOTPProfile | Numeric | 8 | 10 Days |

**To create a OTP profile:**

1. Open Administration Console in a Web browser window.

2. In the left pane, under **Issuance Configurations** menu, click the **OTP Profiles** link.

   The OTP Credential Profiles page appears.

3. Enter the profile name in the **Profile Name** field.

4. Select the type of OTP in the **OTP Type** field. The OTP can either be numeric or alphanumeric.

5. Select the length of OTP using the **OTP Length** drop-down list.

6. Enter the period for which the OTP is valid in **Validity Period** field.
7. Click the **Create Profile** button to create the OTP profile.

   The "OTP Profile created successfully" message appears and the profile is listed in the **Current Profiles** table.

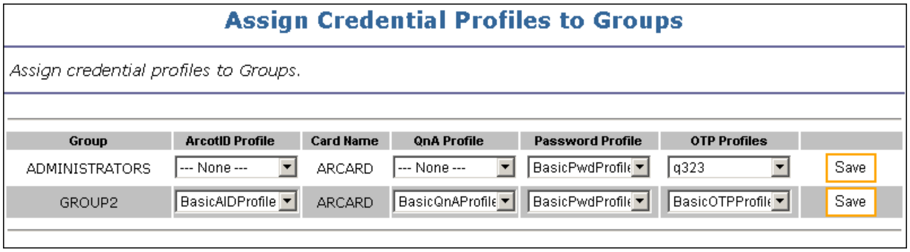
## Assigning Profiles

Credential profiles can be assigned to groups by administrators. In this way, the administrator can control the credentials that a group of users can get.

**NOTE:** A minimum of one profile has to be set for a group.

The following figure shows the page used for assigning the profiles.

**Figure 3-13**



Assign Credential Profiles to Groups

*Assign credential profiles to Groups.*

| Group | ArcotID Profile | Card Name | QnA Profile | Password Profile | OTP Profiles | |
|---|---|---|---|---|---|---|
| ADMINISTRATORS | --- None --- | ARCARD | --- None --- | BasicPwdProfil | q323 | Save |
| GROUP2 | BasicAIDProfile | ARCARD | BasicQnAProfil | BasicPwdProfil | BasicOTPProfil | Save |

**To assign profiles for a group:**

1. Open Administration Console in a Web browser window.
2. In the left pane, under **Issuance Configurations** menu, click the **Assign Profiles** link.

   The Assign Credential Profiles to Groups page appears.
3. Select the respective profile from the drop-down list.
4. Click the **Save** button to save the selected profile.

   The "Profile(s) updated successfully" message appears.

# Chapter 4

# Working with Reports

Reports capture details of transactions performed by users authenticating with WebFort and also record day-to-day operations performed by the administrators.

The following topics are discussed in this chapter:

- WebFort Reports
- Exporting Reports

**NOTE:** The activity timings displayed in all reports are in server time zone.

# WebFort Reports

This section explains the reports provide by WebFort. These reports include:

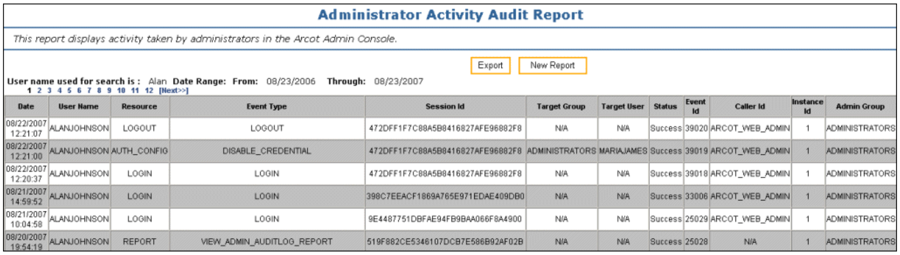
-
- Credential Management Report
- Authentication Activity Report
- User Credential Summary Report

## Administrator Activity Audit Report

This report lists all the activities performed out by the administrator using the Administration Console. This report can be generated by the Master Administrator and GAs.

The following figure shows a sample Administrator Activity Audit Report.

**Figure 4-1**



Administrator Activity Audit Report

*This report displays activity taken by administrators in the Arcot Admin Console.*

**User name used for search is :** Alan **Date Range: From:** 08/23/2006 **Through:** 08/23/2007

| Date | User Name | Resource | Event Type | Session Id | Target Group | Target User | Status | Event Id | Caller Id | Instance Id | Admin Group |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 08/22/2007 12:21:07 | ALANJOHNSON | LOGOUT | LOGOUT | 472DFF1F7C88A5B8416827AFE96882F8 | N/A | N/A | Success | 39020 | ARCOT_WEB_ADMIN | 1 | ADMINISTRATORS |
| 08/22/2007 12:21:00 | ALANJOHNSON | AUTH_CONFIG | DISABLE_CREDENTIAL | 472DFF1F7C88A5B8416827AFE96882F8 | ADMINISTRATORS | MARIAJAMES | Success | 39019 | ARCOT_WEB_ADMIN | 1 | ADMINISTRATORS |
| 08/22/2007 12:20:37 | ALANJOHNSON | LOGIN | LOGIN | 472DFF1F7C88A5B8416827AFE96882F8 | N/A | N/A | Success | 39018 | ARCOT_WEB_ADMIN | 1 | ADMINISTRATORS |
| 08/21/2007 14:59:52 | ALANJOHNSON | LOGIN | LOGIN | 398C7EEACF1869A765E971EDAE409DB0 | N/A | N/A | Success | 33006 | ARCOT_WEB_ADMIN | 1 | ADMINISTRATORS |
| 08/21/2007 10:04:58 | ALANJOHNSON | LOGIN | LOGIN | 9E4487751DBFAE94FB9BAA066F8A4900 | N/A | N/A | Success | 25029 | ARCOT_WEB_ADMIN | 1 | ADMINISTRATORS |
| 08/20/2007 19:54:19 | ALANJOHNSON | REPORT | VIEW_ADMIN_AUDITLOG_REPORT | 519F882CE5346107DCB7E586B92AF02B | N/A | N/A | Success | 25028 | N/A | 1 | ADMINISTRATORS |

Table 4-1 describes the information included in the Administrator Activity Audit Report.

**Table 4-1** Administrator Activity Audit Report Fields

| Report Field | Description |
|---|---|
| Date | The date and time of the activity. |
| User Name | The name of the administrator. |
| Resource | The resource created, modified, deleted, read, or viewed by the administrator. |

**Table 4-1** Administrator Activity Audit Report Fields

| Report Field | Description |
|---|---|
| **Event Type** | The type of activity performed by the administrator, such as, create, read, modify, delete, or view. |
| **Session Id** | The session Id of the Administrator who has logged in. |
| **Target Group** | Group to which the Target User belongs. |
| **Target User** | The name of the user whose attributes were administered by the administrator. |
| **Status** | The status of the action taken. Action status can be:<br>• **Success** - If the action was completed successfully.<br>• **Failure** - If the administrator failed to complete the action. |
| **Event Id** | The unique Id for every activity performed by the administrator. |
| **Caller Id** | The unique identifier set by the calling application. Caller Id can be blank if the calling application does not set the value. |
| **Instance Id** | The unique identifier for the Administration Console application instance, in case multiple instances of the application are running. |
| **Admin Group** | The group to which the administrator belongs. |

**To generate a Administrator Activity Audit Report:**

1. In the left pane, under **Reports** menu, click the **Administrator Activity Audit Report** link.

   The Administrator Activity Audit Report page appears.

2. Select the **Date Range** from the drop-down list or enter a predefined date range in the **From** and **Through** fields

3. Enter the **User Name** of the user whose activity report has to be displayed.

4. Select the **Group** from the drop-down list:

   - **Administrators**: Displays all the administrators of the group.
   - **Group2**: Displays all the normal users of the group.

5. Click the **Display Report** button to view the report generated for the administrator.

6. Click the **Export** button to save the file. Refer to the section "Exporting Reports," for more information on exporting the report.

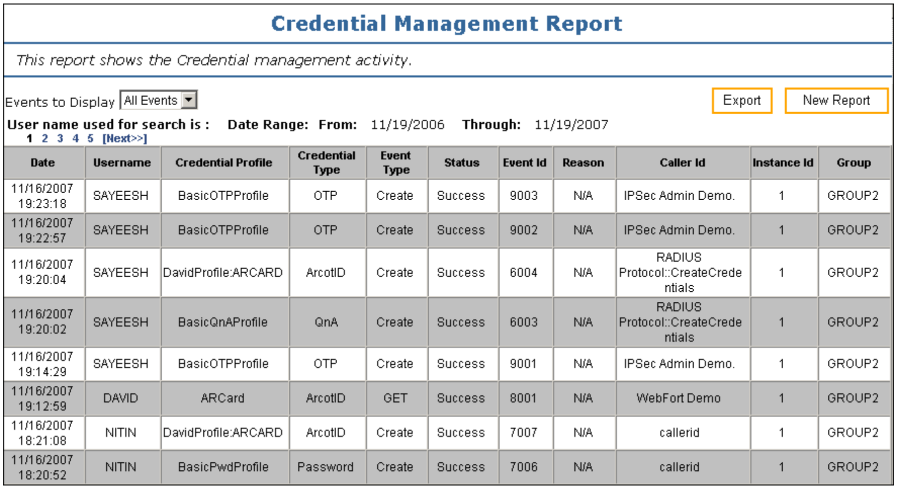
7. Click the **New Report** button to make a new selection.

# Credential Management Report

This report provides details of all operations that were performed on user and administrator credentials. Common operations include, creation of credentials, enabling and disabling of credentials, and resetting or revoking of credentials.

The following figure shows a sample Credential Management Report.

**Figure 4-2**



Credential Management Report

*This report shows the Credential management activity.*

Events to Display All Events ▼

**User name used for search is : Date Range: From:** 11/19/2006 **Through:** 11/19/2007

**1** 2 3 4 5 [Next>>]

| Date | Username | Credential Profile | Credential Type | Event Type | Status | Event Id | Reason | Caller Id | Instance Id | Group |
|---|---|---|---|---|---|---|---|---|---|---|
| 11/16/2007 19:23:18 | SAYEESH | BasicOTPProfile | OTP | Create | Success | 9003 | N/A | IPSec Admin Demo. | 1 | GROUP2 |
| 11/16/2007 19:22:57 | SAYEESH | BasicOTPProfile | OTP | Create | Success | 9002 | N/A | IPSec Admin Demo. | 1 | GROUP2 |
| 11/16/2007 19:20:04 | SAYEESH | DavidProfile:ARCARD | ArcotID | Create | Success | 6004 | N/A | RADIUS Protocol::CreateCredentials | 1 | GROUP2 |
| 11/16/2007 19:20:02 | SAYEESH | BasicQnAProfile | QnA | Create | Success | 6003 | N/A | RADIUS Protocol::CreateCredentials | 1 | GROUP2 |
| 11/16/2007 19:14:29 | SAYEESH | BasicOTPProfile | OTP | Create | Success | 9001 | N/A | IPSec Admin Demo. | 1 | GROUP2 |
| 11/16/2007 19:12:59 | DAVID | ARCard | ArcotID | GET | Success | 8001 | N/A | WebFort Demo | 1 | GROUP2 |
| 11/16/2007 18:21:08 | NITIN | DavidProfile:ARCARD | ArcotID | Create | Success | 7007 | N/A | callerid | 1 | GROUP2 |
| 11/16/2007 18:20:52 | NITIN | BasicPwdProfile | Password | Create | Success | 7006 | N/A | callerid | 1 | GROUP2 |

Table 4-2 describes the information included in the Credential Management Report.

**Table 4-2** Credentials Management Report Fields

| Report Field | Description |
|---|---|
| **Date** | The date and time of login. |
| **User Name** | The name of the user whose credential is being managed. |
| **Credential Profile** | The profile used to create the credential. |
| **Credential Type** | The type of the credential issued to the user. |
| **Event Type** | The type of action performed on the credential. |
| **Status** | The status of the action taken. Action status can be:<br>• **Success** - If the action was completed successfully.<br>• **Failure** - If the administrator failed to complete the action. |
| **Event Id** | The generated event Id. |

**Table 4-2** Credentials Management Report Fields

| Report Field | Description |
|---|---|
| **Reason** | The reason for failure. |
| **Caller Id** | A unique identifier set by the calling application. Caller Id can be blank if the calling application does not set the value. |
| **Instance Id** | The Id to identify the server instance. |
| **Group** | The group to which the administrator belongs. |

**To generate a Credential Management Report:**

1. In the left pane, under **Reports** menu click **Credential Management Report** link.

   The Credential Management Report page appears.

2. Select the **Date Range** from the drop-down list or enter a predefined date range in the **From** and **Through** fields

3. Enter the **User Name** of the user whose credential summary has to be displayed.

4. Select the **Group** from the drop-down list.

5. Click the **Display Report** button to view the report generated for the administrator.

6. Select an event, if required, from the **Events to Display** drop-down list.

   **Events to Display** drop-down list is an additional filter, which helps to query on the specific event. For example, if the administrator selects **Create** from the **Events to Display** drop-down list, the report displays only the activities related to credential creation.

7. Click the **Export** button to save the file. Refer to the section "Exporting Reports," for more information on exporting the report.

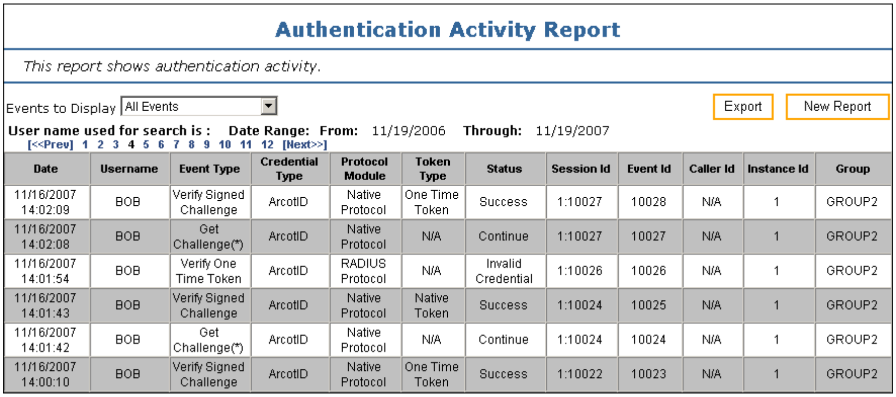
8. Click the **New Report** button to make a new selection.

# Authentication Activity Report

This report provides details of activities that were performed by users authenticating with the WebFort. The credentials issued by WebFort are used for the purpose of authentication. Some of the authentication methods (such as QnA and User Name-Password) are single step process. ArcotID authentication is a multi-step challenge/response process and multiple records are created to mark each step. Multiple steps of an authentication process are tied together by a session ID, which is also available in the report.

The following figure shows a sample Authentication Activity Report.

**Figure 4-3**



Authentication Activity Report

*This report shows authentication activity.*

Events to Display All Events

**User name used for search is : Date Range: From:** 11/19/2006 **Through:** 11/19/2007

[<<Prev] 1 2 3 4 5 6 7 8 9 10 11 12 [Next>>]

| Date | Username | Event Type | Credential Type | Protocol Module | Token Type | Status | Session Id | Event Id | Caller Id | Instance Id | Group |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 11/16/2007 14:02:09 | BOB | Verify Signed Challenge | ArcotID | Native Protocol | One Time Token | Success | 1:10027 | 10028 | N/A | 1 | GROUP2 |
| 11/16/2007 14:02:08 | BOB | Get Challenge(*) | ArcotID | Native Protocol | N/A | Continue | 1:10027 | 10027 | N/A | 1 | GROUP2 |
| 11/16/2007 14:01:54 | BOB | Verify One Time Token | ArcotID | RADIUS Protocol | N/A | Invalid Credential | 1:10026 | 10026 | N/A | 1 | GROUP2 |
| 11/16/2007 14:01:43 | BOB | Verify Signed Challenge | ArcotID | Native Protocol | Native Token | Success | 1:10024 | 10025 | N/A | 1 | GROUP2 |
| 11/16/2007 14:01:42 | BOB | Get Challenge(*) | ArcotID | Native Protocol | N/A | Continue | 1:10024 | 10024 | N/A | 1 | GROUP2 |
| 11/16/2007 14:00:10 | BOB | Verify Signed Challenge | ArcotID | Native Protocol | One Time Token | Success | 1:10022 | 10023 | N/A | 1 | GROUP2 |

Table 4-3 describes the information included in the Authentication Activity Report.

**Table 4-3** Authentication Activity Report Fields

| Report Field | Description |
|---|---|
| **Date** | The date and time of login. |
| **User Name** | The name of the user who has authenticated with the WebFort server. |
| **Event Type** | The type of event that took place for the activity. |
| **Credential Type** | The type of the credential issued to the user. |
| **Protocol Module** | The protocol used for authentication. |
| **Token Type** | The token issued to the user after successful authentication. The token can be any of the type:<br>• **Native** - This is an Arcot proprietary token. The token can be used multiple times for verification during the configured validity period.<br>• **RADIUS OTP** - This token is designed for *one* time use and is valid for a specified period. |
| **Status** | The status of the action taken. Action status can be:<br>• **Success** - If the action was completed successfully.<br>• **Failure** - If the administrator failed to complete the action. |
| **Session Id** | The session Id for the transaction provided by the Web server. |

**Table 4-3** Authentication Activity Report Fields

| Report Field | Description |
|---|---|
| Event Id | The generated event Id. |
| Caller Id | The unique identifier set by the calling application. Caller Id can be blank if the calling application does not set the value. |
| Instance Id | The Id to identify the server instance. |
| Group | The group of the administrator. |

**To generate an Authentication Activity Report:**

1. In the left pane, under **Reports** menu, click the **Authentication Activity Report** link.

   The Authentication Activity Report page appears.

2. Select the **Date Range** from the drop-down list or enter a predefined date range in the **From** and **Through** fields

3. Enter the **User Name** of the user whose authentication activity details has to be displayed.

4. Select the **Group** from the drop-down list.

5. Click the **Display Report** button to view the report generated for the administrator.

6. Select an event, if required, from the **Events to Display** drop-down list.

7. Click the **Export** button to save the file. Refer to the section "Exporting Reports," for more information on exporting the report.

8. Click the **New Report** button to make a new selection.

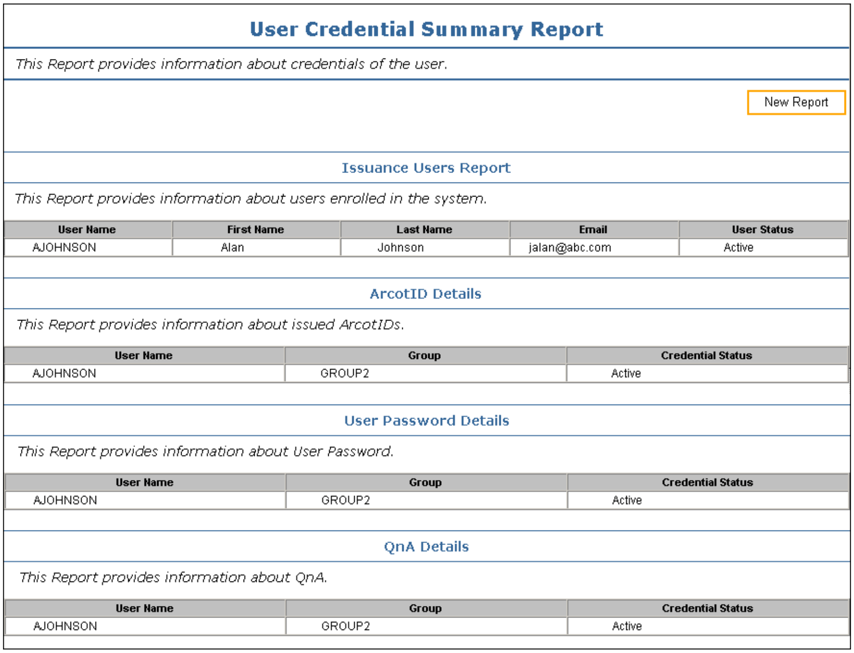
# User Credential Summary Report

This report provides a summary of the credentials that are issued to a specified user. The report contains details such as, types of credentials issued, date of issuance and the current status of the credentials.

**NOTE:** This report can only be generated by CSR Administrators.

The following figure shows a sample User Credential Summary Report.

**Figure 4-4**



User Credential Summary Report

*This Report provides information about credentials of the user.*

Issuance Users Report

*This Report provides information about users enrolled in the system.*

| User Name | First Name | Last Name | Email | User Status |
|---|---|---|---|---|
| AJOHNSON | Alan | Johnson | jalan@abc.com | Active |

ArcotID Details

*This Report provides information about issued ArcotIDs.*

| User Name | Group | Credential Status |
|---|---|---|
| AJOHNSON | GROUP2 | Active |

User Password Details

*This Report provides information about User Password.*

| User Name | Group | Credential Status |
|---|---|---|
| AJOHNSON | GROUP2 | Active |

QnA Details

*This Report provides information about QnA.*

| User Name | Group | Credential Status |
|---|---|---|
| AJOHNSON | GROUP2 | Active |

### To generate a User Credential Summary Report:

1. Log in as a CSR Administrator.
2. In the left pane, under **Reports** menu, click the **User Credential Summary Report** link.
3. Enter the user name in the **User Name** field and click the **Display Report** button.

   The "User Credential Summary Report" page appears.

# Exporting Reports

Reports can be exported to a Comma-Separated Value (CSV) file. The exported report files can be later opened in a spreadsheet, such as Microsoft Excel for any data manipulation. This feature is very useful if any post-processing or sorting of the reports is required.

Figure 4-5 shows the screen to export the report.

**To export a report to a file:**

1. Click the desired report link from the **Reports** menu.

   The Report Criteria page for the selected report appears.

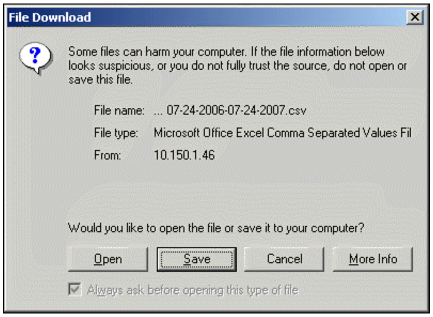
2. Select the **Date Range** option from the drop-down list. You can either select a pre-defined date range in the **From** and **Through** fields or enter a **User Name**.

3. Click the **Display Report** button to view the report generated for the administrator.

4. Click the **Export** button to save the file on your local disk.

   The File Download pop-window appears, as shown below:

**Figure 4-5**



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: ... 07-24-2006-07-24-2007.csv

File type: Microsoft Office Excel Comma Separated Values Fil

From: 10.150.1.46

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

5. Click the **Save** button to save the file. This file can be viewed using a spreadsheet application, such as Microsoft Excel.

# Chapter 5

# Tools for System Administrators

This chapter describes the command-line utilities that are packaged with WebFort:

- dbutil
- arversion
- aradmin

All the tools discussed in this chapter are available in the folder:

**Solaris:** `<install_location>/arcot/sbin/`

**Windows:** `<install_location>\Arcot Systems\bin`

# dbutil

The `dbutil` tools allows the administrator to set the master key and database-related user names and passwords after installation, in `securestore.enc`  file. This information is stored in the encrypted format.

Following operations can be performed using `dbutil` tool:

- Setting up the Master Key
- Using Additional dbutil Options

## Setting up the Master Key

The master key is used to encrypt all the values in the `securestore.enc` file. It also encrypts all of the encryption keys that are stored in the database.

If, for some reason, you need to change the Master Key value in `securestore.enc`, perform the following steps:

> **CAUTION:** THIS PROCEDURE SHOULD ONLY BE DONE IF THE MASTER KEY SETUP FAILED DURING INSTALLATION. CONTACT ARCOT TECHNICAL SUPPORT PRIOR TO PERFORMING THIS PROCEDURE.

1. Take a backup of `securestore.enc` file.
2. Delete the existing `securestore.enc` file.
3. Enter the following command:

   ```
   dbutil -init masterKey
   ```

   In the preceding command, *`masterKey`* is the new key you want to use as Master Key.

   For example:

   ```
   dbutil -init WebFortMasterKey
   ```

   In this example, `dbutil` adds the master key in the `securestore.enc` file.

# Using Additional dbutil Options

Table 5-1 lists additional 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 and user name-password is used by WebFort and Issuance Java APIs.

**Table 5-1** Additional dbutil Options

| Option | Description |
|---|---|
| `-pd` | Deletes the specified key/value pair from `securestore.enc`.<br>Syntax:<br>`dbutil -pd` *`key`*<br>For example:<br>`dbutil -pd WebFortDatabaseDSNOld`<br>`dbutil -pd Jack` |
| `-pi` | Inserts an additional key/value pair into `securestore.enc` file.<br>Each key can only have one value. If you have already inserted a key/value pair, you cannot insert another value for the same key.<br>Syntax:<br>`dbutil -pi` *`key value`*<br>For example:<br>`dbutil -pi WebFortBackupDSN dbapassword`<br>`dbutil -pi Jack userpassword` |
| `-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.<br>Syntax:<br>`dbutil -pu` *`key value`*<br>For example:<br>`dbutil -pu WebFortDatabaseDSN newPassword`<br>`dbutil -pu Jack userPassword` |

# arversion

The `arversion` tool helps the administrators to find the version information of the modules provided by WebFort. Arcot technical support may ask for this information in case of deployment issues.

## Usage

```
arversion <library1_path> [<library2_path> ...]
```

`<libraryN_path>:`

- In the preceding syntax, the string specifies the name of individual module.

  For example:

  `aradminprotocol.dll` for Windows

  `libaradminprotocol.so` for Solaris

You can specify the relative path of the module. In this case, the module is looked up in set of folders specified by the standard environment variable.

For example:

`%PATH%` for Windows

`$LD_LIBRARY_PATH` for Solaris

**Example:** **Windows:**

```
arversion "<install_location>\Arcot
Systems\plugins\protocols\aradminprotocol.dll"
```

**Solaris:**

```
arversion
/<install_location>/arcot/plugins/protocols/libaradminprotoc
ol.so
```

## Sample Output

Following code snippet shows a sample output of `arversion` tool on Windows platform:

**For Windows:**

```
aradminprotocol.dll- [Server Management Protocol 1.0.0_w]
nativeprotocol.dll- [Arcot WebFort 5.4_Native Authentication
Protocol 1.0.0_w]
```

# aradmin

The WebFort server must be refreshed to apply the configurations made by the administrator using Administration Console. The aradmin tool provides the refresh option, to refresh the server and ensures the server is not down during refresh process.

> **NOTE:** Certain configurations made using Administration Console mandates the restart of WebFort server. In such cases, the Administration Console screen instructs the administrator to restart WebFort server.

> **NOTE:** To update the INI file changes, the server must be restarted.

The aradmin tool also provides the option to gracefully shut down the server. In case of graceful shutdown, the server allows all existing requests to complete, while not accepting any new requests.

## Usage

```
aradmin <server ip> <sever management port> <options>
```

Table 5-2 lists the parameters used by aradmin.

**Table 5-2** aradmin Parameters

| Parameters | Description |
|---|---|
| server ip | The IP address or host name on which the WebFort server is available. You can also provide the name of the local host. |
| server management port | Port number where server processes the operations request mentioned below.<br>**NOTE:** The default server management port is 9743. |

Table 5-3 lists the options supported by aradmin.

**Table 5-3** aradmin Options

| Options | Description |
|---|---|
| -d | This option is used to initiate graceful shutdown of the server.<br>Example:<br>aradmin 10.150.1.40 9743 -d |

**Table 5-3** `aradmin` Options

| Options | Description |
|---|---|
| `-r` | This option is used to send a refresh request.<br>Example:<br>`aradmin 10.150.1.40 9743 -r`<br>To refresh a particular log level, the refresh options is used as follows:<br>`aradmin <server ip> <server manager port> -r log:all=<log level>`<br>The possible values for `<log level>` are:<br>• 0 FATAL<br>• 1 WARNING<br>• 2 INFO<br>• 3 DETAIL |

# Configuring aradmin for TLS

To configure aradmin tool for TLS, you must perform the following steps:

1. Editing the arcotcommon.ini File
2. Configuring Server Management Protocol

## Editing the arcotcommon.ini File

Add the following section to `arcotcommon.ini` file:

```
[arcot/aradmin/tlsconfig]
ServerCACert=<absolute_path_of_Root_Certificate>
```

Set the parameter `ServerCACert` to the absolute path of the CA certificate file. The file *must* be in `.PEM` format. For example:

**For Windows:**

```
ServerCACert=<install_location>\Arcot
Systems\certs\webfort_ca.pem
```

**For Solaris:**

```
ServerCACert=<install_location>/arcot/certs/webfort_ca.pem
```

## Configuring Server Management Protocol

**To configure WebFort Server Management protocol for TLS:**

1. Under **WebFort Configurations** from the left-hand menu, select **Protocol Setup.**

   The WebFort Protocol Setup page appears.

2. Perform the following steps to configure the WebFort Server Management protocol for TLS:

   a. In the **Enable** column, ensure that the check box for **Server Management** protocol to be enabled for TLS is selected.

   b. In the **Transport Security** column, select **TLS** from the drop-down list.

   c. In the **SSL/TLS Certificate Details** column:

      i. Click **Browse** against **Certificate Chain** to navigate to the appropriate location and upload the SSL certificate chain for the server.

      **NOTE:** The certificates in the chain *must* start from Leaf certificate, Intermediate CA certificates, and then Root certificate.

      ii. Click **Browse** against **Private Key** to navigate to the appropriate location and upload the corresponding private key of the certificate.

      **NOTE:** The certificate chain and the private key, both *must* be in `.PEM` format private key uploaded must be not be password protected.

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

3. Restart WebFort Server.

4. Restart Administration Console.

Appendix A

# Configuring WebFort for Client-based VPN

This appendix lists the steps for configuring client-based VPNs to communicate with WebFort over RADIUS protocol.

> **NOTE:** On **Windows**, set the `JAVA_HOME` environment variable before proceeding with the VPN configuration. On **Solaris**, if you have installed JDK 1.5.*x* for use by Apache Tomcat 5.5.*x*, then you need to make sure that the path you specify for `JAVA_HOME`  contains Java executable in it.

# Configuring WebFort for Client-Based VPN

**To configure WebFort for client-based VPNs:**

1. Open Administration Console in a Web browser window.
2. Log in using a Global Administrator account.
3. In the left pane, under **WebFort Configurations** menu, click the **Authentication Configuration** link.

   The Authentication Configuration page appears.
4. Set the value of # **of Questions to ask for QnA Authentication** to 2.
5. Set the value of # **of Answers required for QnA Authentication** to **2.**
6. Enable **OTP** authentication method in **Authentication Method Status** table.
7. Click the **Update** button to apply the configurations.
8. In the left pane, under **WebFort Configurations** menu, click the **RADIUS Configuration** link.

   The RADIUS Configuration page appears.
9. Enter the VPN gateway IP Address in the **RADIUS Client IP Address** field and shared secret in **Shared Secret Key** field. See "Configuring for RADIUS" for more information on other field entries.
10. Select the **Authentication Type** as **InBand ArcotID**.

    **NOTE:** Ensure the **Maximum RADIUS Packet Size (in bytes)** and **RADIUS Version** are set according to the specification of the VPN gateway vendor.
11. Click the **Add** button to add the IP Address of the VPN.
12. In the left pane, under **WebFort Configurations** menu, click the **Protocol Setup** link.

    The WebFort Protocol Setup page appears.
13. Enable the **WebFort RADIUS** protocol and click the **Save** button.
14. Restart the WebFort server.

Appendix B

# Glossary

| | |
|---|---|
| **3DES** | 3DES is a block cipher formed from the Data Encryption Standard (DES) by using it three times. There are variations of 3DES which use two different keys and three different keys (3DES) |
| **ArcotID Domain** | A domain is a group of servers to which users may authenticate using the ArcotID. |
| **ArcotID Domain Key** | The domain key is a key issued to a Domain. When an Arcot ID is created, it is enabled for a set of domain keys. The domain key is used during authentication to encrypt/decrypt the public key stored in the certificate. |
| **ArcotID** | Is a secure software credential that allows hardware level authentication in software form. |
| **Authentication** | Is a process by which an entity proves that it is who it claims to be. |
| **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 may be stored on hardware such as smart cards or USB tokens or on the server. They are verified during authentication. |
| **Cryptographic device** | Hardware device used to store the user sensitive keys. |
| **cryptographic hash function** | A cryptographic hash function is a hash function with additional security properties, used in security-related applications such as authentication. |
| **Customer Support Representatives (CSR)** | CSRs are the administrators responsible for the day-to-day operations related to users of the security system. For example, Administrators can assist users with enrollment, reset users passwords, and view a variety of enrollment reports. |
| **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** | An administrator responsible for setting up CSR Administrator accounts and configuring the system. |
| **N-Strikes** | The maximum failed authentication attempts that a user can make before the credentials are locked. |
| **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. |
| **PKCS#15** | Defines a standard allowing users of cryptographic token to identify themselves to applications, independent of the application's cryptoki implementation or other API. |
| **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** | An 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. |
| **Secure Hash Algorithm (SHA)** | Secure Hash Algorithm (SHA) family is a set of cryptographic hash functions. |
| **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. |
| **Transport Layer Security (TLS)** | TLS is a protocol intended to secure and authenticate communications across public networks by using data encryption. |
| **UserID/Password** | One of the credential issued to the user during enrollment. |
| **WebFort** | WebFort server authenticates the end users with the help of user credentials which are issued by Issuance. |
| **Web Services Definition Language (WSDL)** | A standard XML format prescribed by W3C to describe network services as collections of communication end points capable of exchanging messages. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint.<br>A WSDL document describes a Web Service and specifies the location and the methods that the service exposes. |
| **Web Services Security (WS-Security)** | This is a communication protocol providing a means for applying security to Web Services. |

# Index