CA AuthMinder

Administration Guide

r7.1.01

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 4: Managing AuthMinder Server Instances 63

Chapter 5: Managing Global AuthMinder Configurations 89

Chapter 1: Overview of the Administration Console

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

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

This guide provides information for setting up and managing CA AuthMinder using the Administration Console. This guide covers information for both Windows and UNIX-based platforms that are supported by CA AuthMinder.

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

Note: The recommended desktop screen resolution is the optimal resolution of the system that is used to access the Administration Console.

Note: CA AuthMinder still contains the terms Arcot and WebFort in some of its code objects and other artifacts. Therefore, you will find occurrences of Arcot and WebFort in all CA AuthMinder documentation. In addition, some of the topics in this guide do not follow the standard formatting guidelines. These inconsistencies will be fixed in a future release.

About the Administration Console

The Administration Console is a browser-based, graphical user interface and is accessible from any supported web browser with network access to the Console. This Console enables you to manage all deployed CA AuthMinder (later referred to as AuthMinder) instances, where an *instance* represents a AuthMinder Server that is installed on a system.

You can use the Administration Console to configure AuthMinder Server, to create users, administrative roles, and perform other administrative operations and configuration tasks, such as:

- Configure and refresh server instances
- Configure communication parameters between the server and other AuthMinder components
- Manage organizations, administrators, organizations that are mapped to LDAP, and users and their credentials
- Configure plug-ins
- Set authentication policies
- Set credential profiles
- Generate administration, transaction, and configuration reports

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

Elements of the Administration Console

A typical Administrative screen can be divided into the following elements:

- Header
- Main Menu
- Submenu
- Tasks
- Body

The following table describes these elements:

Element	Description
Header	Displays login information (administrator name, organization that the administrator belongs to, the last login date, and time). You can use the links in the header to: ■ Change the password, specify the organization that you want to use as a preferred organization for all tasks that you may perform in future, and select your preferred locale and time zone. ■ Log out from the Administration Console.
Main Menu	Displays the high-level options available to the current administrator.
Submenu	Displays the options available for the Main Menu item that you selected.
Tasks	Displays the tasks available for the Submenu item that you selected.
Body	Displays the corresponding page for the selected task.

Console Messages

All the information, warning, and error messages that are generated when you use the Administration Console are displayed at the top of the body page.

While the error messages are displayed in red, the messages indicating success are displayed in blue. Any additional instructions are also a part of these messages.

Supported Roles

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

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

The Administration Console supports the following types of roles:

- Users (see page 14)
- Default Administrative Roles (see page 15)
- Custom Roles (see page 21)

Users

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

If the user already exists in your LDAP system, then map the LDAP attributes to AuthMinder supported attributes. See "Creating Organization in LDAP Repository" (see page 168) for more information.

To enroll the users in the AuthMinder database, select the organization whose repository type is Arcot Database. See "Creating Organization in LDAP Repository" (see page 168) for more information.

Default Administrative Roles

The Administration Console is shipped with an out-of-the-box administrator called the Master Administrator (see page 18) who can perform high-level configurations. Other than this, assign users to administrative roles to administer the AuthMinder system or to access your business data. An administrative role typically comprises a set of permissions that are based on a job function profile and the scope in which these permissions are applicable. The users with administrative permissions are referred to as *administrative user*.

Note: See "Summary of Administrative Permissions" (see page 57) for a comprehensive list of permissions available to each administrative role.

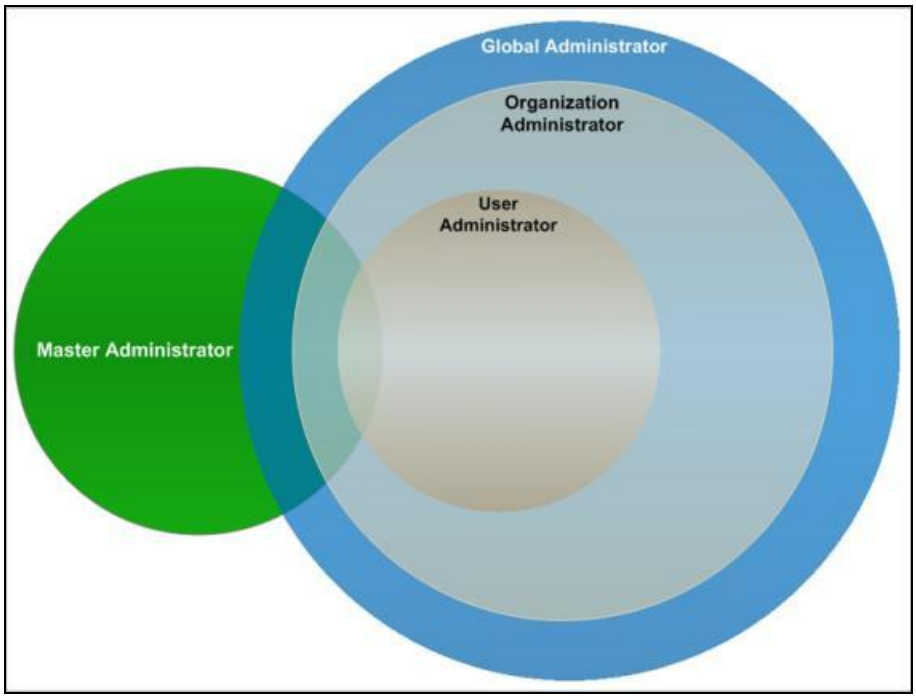
The Administration Console supports the following predefined administrative roles:

- Master Administrator (see page 18)
- Global Administrator (see page 19)
- Organization Administrator (see page 20)
- User Administrator (see page 20)

In addition, you can also create Custom Roles (see page 21).

Note: The administrators are also considered as users of the system.

The following figure depicts these administrative roles and the relationships between the permissions available to these roles. The sections following the figure discuss the supported administrator levels in detail.



Note: The hierarchical distribution of permissions does not allow the administrators to access features beyond their fixed boundaries. Each level has a predefined permission or role.

Scope of an Administrative Role

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

- All the organizations that an administrator with a specific role can manage.
- The permissions that are associated with the role.

Important Notes About Scope

While creating an administrative role, remember that:

- The scope of the Master Administrator (see page 18) is **All Organizations**, and this administrator manages *all* existing and organizations that will be created in the future.
- An administrator (Global Administrator (see page 19), Organization Administrator (see page 20), or User Administrator (see page 20)) can manage their peers and the roles with fewer permissions, provided they have scope on the organization to which the administrators belong.

  For example, a Global Administrator can manage other Global Administrators, Organization Administrators and User Administrators. However, they *cannot* manage Master Administrator.
- The scope of a Global Administrator (see page 19) role *can* be defined as All Organizations, in which case this administrator can manage all existing and future organizations.
- An Organization Administrator (see page 20) or a User Administrator (see page 20) can be limited to manage only specific organizations.
- If the administrator is derived by using Custom Roles (see page 21), then the derived administrator belongs to the same level as that of the parent level.

  For example, if you derive the MyGlobalAdmin administrator from Global Administrator, then MyGlobalAdmin is considered to be a Global Administrator. This is true even though you may have assigned MyGlobalAdmin fewer permissions compared to an Organization Administrator or User Administrator.

  Note: An **Organization Administrator** or a **User Administrator** role *should not* be defined with the scope as All Organizations.

Master Administrator

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

The primary responsibilities of an MA are to:

- Bootstrap (or initialize) the system after installation.
- Configure the UDS connection parameters.
- Configure the global settings for organizations and cache refresh settings for the Administration Console and for User Data Service.
- Configure custom locales.
- Set the Default organization.
- Enable authentication and authorization for Web Services.
- Configure the AuthMinder Server communication parameters.
- Configure and manage AuthMinder Server instances.
- Configure the AuthMinder Server protocol settings.
- Configure the authentication mechanism for the Administration Console and Server components and other miscellaneous settings.
- Register plug-ins, if you want to extend the feature offering from AuthMinder using custom plug-ins.

  Note: See "Registering and Updating Plug-Ins" (see page 84) for more information about how to register a plug-in and "Configuring Plug-Ins" (see page 157) for more information about how to configuring the plug-in.
- Create and manage organizations.
- Create and manage administrators of any role (Global, Organization, or User Administrator), as required.
- Create and Manage Custom Roles (see page 21).
- Generate instance statistics.

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

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

Resetting the Master Administrator Password

If your MA account password is locked because of multiple failed password attempts, you can run the **arcot-masteradmin-password-reset-2.0.sql** script to reset your password. This script is available in the **<INSTALL_HOME>\dbscripts\<database>** folder.

The Master Administrator must now log in to Administration Console using the default password, **master1234!**. After the login, the Master Administrator must reset the password.

Global Administrator

The Global Administrator (GA) is the second level in the administrative hierarchy. These administrators can perform few of the tasks of an MA.

By default, GA has scope on all organizations present in the system. If you want the GA to manage only specific organizations, then specify it while creating the GA accounts.

The main tasks of a GA are to:

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

  Note: This includes editing the organization details.
- Create and manage users, as required.
- Configure Adobe Signature Service Protocol (ASSP) and Secure Assertion Markup Language (SAML).
- Manage user credentials.
- Configure AuthMinder Profiles and Policies for supported authentication mechanisms.
- Assign configurations globally or to an organization.
- Configure registered plug-ins.
- Configure RADIUS clients and RADIUS proxy server.

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

Organization Administrator

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

The main tasks of an OA are to:

- Create and manage other Organization Administrators or User Administrators, as required.
- Create and manage the users that belong to the organizations in their purview.
- Manage organizations in their purview.
- Refresh the cache of organizations in their purview.
- Configure the authentication policy for organizations.
- Manage (update) organization-specific configurations.

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

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

User Administrator

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

- Manage other UAs, as required.
- Create and Manage end users, as required.

  Note: This includes editing the user details.
- Manage user credentials.

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

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

Custom Roles

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

- Global Administrator (see page 19)
- Organization Administrator (see page 20)
- User Administrator (see page 20)

These roles are called *custom roles*, and are derived by **disabling** some of the default permissions that are associated with the parent role. For example, if you want to disable the "Organization Creation Permission" for a GA, then you can create a custom role by disabling this permission.

If you create a custom role, then it becomes available as a role option when you create or update an administrative role. In addition to creating custom roles, you can also update and delete them.

See "Working with Custom Roles" (see page 53) for more information about working with these custom roles.

Next Steps: Quick Administration

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

- For Simple Deployments (see page 22)
- For Complex Deployments (see page 24)

For Simple Deployments

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

Note: See "Planning the Deployment" in the *CA AuthMinder Installation and Deployment Guide* for more information about this type of deployment.

The following table summarizes the typical characteristics of this deployment type:

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

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

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

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

   Note: See "Deploying AuthMinder on a Single System" in the *CA AuthMinder Installation and Deployment Guide* for more information about installing AuthMinder, deploying the WAR files, and performing other post-installation tasks.

2. Log in to the Administration Console as MA (see "Accessing the Administration Console" (see page 28)) and follow the steps in the Bootstrap wizard to initialize the system.

   Note: See "Bootstrapping the System" in the *CA AuthMinder Installation and Deployment Guide* for more information.

3. Create the required GAs and UAs.

   See "Creating Administrators" (see page 196) for more information.

4. Create appropriate Credential Profiles (see page 90) and Authentication Policies (see page 91), and assign these configurations.

   See "Managing Global (see page 89)AuthMinder Configurations" (see page 89) for more information.

5. Enroll users with AuthMinder.

   See "Creating Users" (see page 226) for more information.

With this your system is set for administration. You can now manage the system ("Managing (see page 63)AuthMinder Server Instances" (see page 63)), administrators ("Managing Administrators" (see page 195)), and users ("Managing Users and Their Credentials" (see page 225)).

For Complex Deployments

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

Note: See "Planning the Deployment" in the *CA AuthMinder Installation and Deployment Guide* for more information about this type of deployments.

The following table summarizes the typical characteristics of this deployment type:

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

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

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

   Note: See the *CA AuthMinder Installation and Deployment Guide* for more information about installing AuthMinder, deploying the WAR files, and performing other post-installation tasks.

2. Log in to the Administration Console as MA (see "Accessing the Administration Console" (see page 28)) and follow the steps in the Bootstrap wizard to initialize the system.

   Note: See "Bootstrapping the System" in the *CA AuthMinder Installation and Deployment Guide* for more information.

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

   See "Configuring Administration Console Settings" (see page 31) for more information.

4. Set up AuthMinder Server instances on different systems.

   See "Setting Up Server Instances" (see page 67) for more information.

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

   See "Configuring Communication Protocols" (see page 76) for more information.

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

   See "Creating and Activating Organizations" (see page 164) for more information.

7. Plan and create the administrators (see "Creating Administrators" (see page 196)) and custom roles (see "Working with Custom Roles" (see page 53)), if required.

8. Create appropriate Credential Profiles (see page 90) and Authentication Policies (see page 91), and assign these configurations.

   See "Managing Global (see page 89)AuthMinder Configurations" (see page 89) for more information.

9. Enroll users with AuthMinder.

   See "Creating Users" (see page 226) for more information.

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

    See "Updating Organization Information" (see page 176) for more information.

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

    See "Creating Trust Stores" (see page 76) for more information.

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

    See "Configuring Miscellaneous Settings" (see page 86) for more information.

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

Note: See "Registering and Updating Plug-Ins" (see page 84) for more information about how to register a plug-in, "Configuring Plug-Ins" (see page 157) on how to configure a plug-in.

With this your system is set for administration. You can now manage the system ("Managing (see page 63)AuthMinder Server Instances" (see page 63)), administrators ("Managing Administrators" (see page 195)), and users ("Managing Users and Their Credentials" (see page 225)).

Chapter 2: Getting Started

This chapter walks you through the steps for logging in to the Administration Console as Master Administrator (see page 18) and initializing the system, after you have successfully installed AuthMinder and have deployed the Console. It covers the following tasks:

Note: See the *CA AuthMinder Installation and Deployment Guide* for detailed information about installing AuthMinder, deploying the Administration Console, and bootstrapping it.

- Accessing the Administration Console (see page 28)
- Changing Password and Profile Information (see page 30)
- Configuring Administration Console Settings (see page 31)

Accessing the Administration Console

The default Master Administrator (MA) role is used to log in to the Administration Console for the first time. The out-of-the-box credentials for MA to log in to the Console are:

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

The bootstrap wizard enforces the Master Administrator to reset their password.

Note: See the *CA AuthMinder Installation and Deployment Guide* for more information about the bootstrap flow.

To log in to the Administration Console:

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

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

   In the preceding URL:

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

   The Master Administrator Login page appears.
3. Enter the password that was set in the bootstrap wizard in the **Password** field and click **Log In.**

   The landing page of the Administration Console appears.

Security Recommendations While Using the Administration Console

When you access Administration Console, ensure that you follow the best practices that are listed here:

- Do not share the browser session with other applications.
- Do not open any other site while working with the Administration Console.
- Do not open any other site in other browser tabs.
- Enforce strict password restrictions for the Administration Console.
- Always log out after using the Administration Console.
- Close the browser window after the session is over.

- Assign proper roles to users according to the tasks they need to perform.

Logging Out of the Administration Console

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

Changing Password and Profile Information

Change your password regularly to maintain high security, so that unauthorized persons do not gain access to the Administration Console using administrator's credentials.

Use the My Profile page to change your current password and your preferences that will be reflected by default for all administrator-related tasks that you perform in future.

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

1. Ensure that you are logged in as the MA.
2. Click the **MASTERADMIN** link in the Console header.

   The My Profile page appears.
3. In the **Change Password** section, specify:
   a. The **Current Password**.
   b. The **New Password**.
   c. The new password again in the **Confirm Password** field.
4. In the **Administrator Preferences** section, specify:
   a. Whether you would like to Enable Preferred Organization.

      This organization is selected by default in the "Organization" field for all administrator-related tasks that you perform from now on. For example, when you search the administrators and users, by default they are searched in the preferred organization.
   b. The **Preferred Organization** that is selected by default in the "Organization" field from now on.
   c. The preferred **Date Time Format**.

      This Date Time format is shown from now on in the **Last Login** timestamp and all other timestamps in the Console. In addition, the reports data (such as Transaction Date) uses this Date Time format.
   d. The preferred **Locale** for your login of Administration Console.

      See "Configuring Custom Locales" (see page 41) for more information about how to configure locales. AuthMinder supports English (United States) out-of-the-box.
   e. The preferred **Time Zone**.

      This Time Zone is shown from now on in the **Last Login** timestamp and all other timestamps in the Console. In addition, the reports data (such as Transaction Date) and other dates and timestamps uses this Time Zone.

      The default **Time Zone** is **GMT**.
5. Click **Save**.

Configuring Administration Console Settings

Before you configure the AuthMinder-specific settings, it is recommended that you configure the global configurations for the Administration Console. This includes the following tasks:

Updating UDS Connectivity

User Data Service (UDS) is a user virtualization layer that enables access to the third-party data repositories (such as, LDAP directory servers) deployed by your organization. UDS enables AuthMinder and the Administration Console to seamlessly access your existing data and leverage end-user information, without having to duplicate it in the standard AuthMinder SQL database tables.

AuthMinder can access user data either from a relational database (RDBMS) or directly from an LDAP server:

- **If you are using a relational database**, then seed the database with the AuthMinder schema as a part of the post-installation configurations.
- **If you are using an LDAP directory server** and you want AuthMinder Server and Administration Console to seamlessly access it, then you must have deployed UDS as part of the post-installation configurations

To update the default UDS connectivity settings, use the User Data Service Connectivity Configuration page.

To update the UDS connectivity configuration:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.

   The **UDS Connectivity Configuration** page appears.
4. Specify the parameters that are listed in the following table in the **User Data Service Connectivity Configuration** section. Most of the parameters on this page are mandatory.

Parameter	Default Value	Description
Protocol	TCP	The protocol to connect to the UDS service using the Administration Console. The available options are: ■ TCP ■ One-Way SSL ■ Two-Way SSL
Host	localhost	The IP address or host name of the system where the UDS is available. The default value of localhost will not work.
Port	8080	The port at which the UDS is available.
Application Context Root	arcotuds	Application context that is specified when UDS is deployed in the application server.

Parameter	Default Value	Description
Read Timeout (in milliseconds)	10000	The maximum time in milliseconds to wait for a response from UDS.
Idle Timeout (in milliseconds)	30000	The time (in milliseconds) after which an idle connection not serving requests will be closed.
Server Root Certificate		The path to the CA certificate file of UDS server. The file must be in PEM format.
Client Certificate		The path to the CA certificate file of the Administration Console. The file must be in PEM format.
Client Private Key		The location of file that contains the CA's private key. The path can be an absolute path or relative to ARCOT_HOME.
Minimum Connections	4	The minimum number of connections that will be created between the AuthMinder Server and the UDS server.
Maximum Connections	32	The maximum number of connections that can be created between the AuthMinder Server and the UDS server.
Connection Timeout (in milliseconds)	30000	Maximum time in milliseconds before the UDS service is considered unreachable.

1. Click **Save** to save the configurations.
2. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Updating UDS Parameters

If you want to update the UDS parameters, use the UDS Configuration page.

To update the UDS parameters:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **UDS Configuration** section on the side-bar menu, click the **UDS Configuration** link to display the page.
5. Specify the parameters, explained in the following table, on the page. All the parameters on this page are mandatory.

Parameter	Default Value	Description
Search Configuration		
Maximum Search Return Count	500	The maximum number of records that will be returned for all **Search** operations in the Administration Console.
LDAP Configuration **Note:** These fields cannot be edited using Administration Console. For information about configuring these parameters, see the "Enabling LDAP Connection Pooling" section in *CA AuthMinder Installation and Deployment* Guide.		
LDAP Connection Pool Initial Size	NA	The initial number of connections between UDS and LDAP that will be created in the pool.
LDAP Connection Pool Maximum Size	NA	The maximum number of connections allowed between UDS and LDAP.
LDAP Connection Pool Preferred Size	NA	The preferred number of connections between UDS and LDAP.
LDAP Connection Pool Timeout (in milliseconds)	NA	The period for which UDS waits for a response from the LDAP, when a new connection is requested.
Authentication Token Configuration		
Purge Interval (in seconds)	3600	The maximum interval after which an authentication token is purged from the database, *after* the token expires.
Validity Period (in seconds)	86400	The maximum period (default is one day) after which an issued authentication token expires.

6. Click **Save** to save the changes you made.
7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Refreshing the Cache

Administration Console caches certain data, which serves frequently-accessed Console pages and UDS data faster. Typically, organizations and roles are cached. AuthMinder maintains cached data at the system level and at the organization level.

Data Cached at the System Level

The following data is cached at the system level:

- **All system-level configurations**
  - UDS configuration and UDS connectivity
  - LDAP connection pool details
  - Global Key label
  - Account type details
  - Custom roles
- **Global data**
  - Encryption sets
  - Localization configuration
  - Email and Telephone types
  - Authentication and Authorization configuration
- **Resources applicable to all organizations**
  - Global account types that are applicable to all organizations

Data Cached at the Organization Level

The following data is cached at the organization level:

- **Data that is applicable to individual organizations**
  - Configurations not referring to global data such as encryption set, localization configuration, and email and telephone types
- **Resources applicable to a set of organizations**
  - Organization-specific account types

Important! When you make data configuration changes that involve both system level and organization level changes, the system cache is refreshed first, followed by the organization cache. Any change in this order of cache refresh may result in inconsistent behavior.

Cache Refresh Order Example

Account type details and global account types are cached at the system level. Whenever you create an account type, irrespective of whether it is global or organization-specific, refresh the system cache. In addition, if the account type is organization-specific, refresh the cache of all the organizations that are in the scope. For more information about account types, see "Configuring the Account Type" (see page 43).

Permissions Required

The MA and GA can refresh the cache of the Administration Console and all instances of the AuthMinder Server. The MA, GA, and OA can refresh the cache of the organizations within their scope.

Refreshing the Cache

If you have made any configuration changes, refresh the cache of the affected server instances for the changes to take effect. AuthMinder now provides an *Integrated Cache Refresh* feature that enables administrators to refresh the cache of all server instances from the Administration Console.

To refresh the cache:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.

   Under the **System Configuration** section on the side-bar menu, click the **Refresh Cache** link to display the page.
4. Select one or both of the following:
   - Select **Refresh System Configuration** to refresh the cache configuration of the Administration Console, User Data Service (if deployed), and all AuthMinder Server instances.
   - Select **Refresh Organization Configuration** to refresh the cache configuration of all organizations in your purview.
5. Click **OK**.

   The "Cache refresh request submitted successfully. Request ID: *<n>*" message appears. The return message also provides a unique identifier for the cache refresh request, which can be used later to view the details of the request.

Viewing the Status of Cache Refresh Requests

Using Administration Console, you can view the details of the cache refresh requests. The Check Cache Refresh Status page enables you to view the cache refresh requests based on its unique identifier or on the status of the request.

To view the status of the cache refresh requests:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **System Configuration** section on the side-bar menu, click the **Check Cache Refresh Status** link to display the page.
5. Provide the details of the cache refresh request by using any of the following fields:
   - **Request ID**: Enter the unique identifier of the cache refresh request.
   - **Status**: Select the status based on which you want to view the cache refresh request details. A cache refresh request can be in any of the following states:
     - **All**: Lists all the cache refresh requests received.
     - **In Progress**: Lists the cache refresh requests that are currently being processed.
     - **Failure**: Lists the cache refresh requests that failed.
     - **Successful**: Lists the cache refresh requests that were processed successfully.
6. Click **Search** to view the cache refresh requests.

   The search result lists the following:
   - The unique identifier of the cache refresh request
   - Time when the request was received
   - Organizations that were affected by cache refresh request
   - The event type
   - AuthMinder components that were affected by cache refresh request. Details of these components are given in the following table:

Parameter	Description
Resource	Specifies the AuthMinder resource that was refreshed. Possible values are: ■ **AdminConsole** For Administration Console and User Data Service ■ **WebFort** For AuthMinder Server

Parameter	Description
Server Instance ID	Specifies the unique identifier of the server instance that was refreshed. ■ For Administration Console and User Data Server, this value is fetched from the InstanceID parameter that is set in the arcotcommon.ini file. ■ For AuthMinder Server, it is the instance name of the AuthMinder Server. By default, it is a combination of host name and a unique identifier.
Server Instance Name	Specifies the instance name of the AuthMinder component that was refreshed. Possible values are: ■ Arcot Administration Console ■ User Data Service ■ Instance name of the AuthMinder Server. By default, it is a combination of host name and a unique identifier.
Host Name	Specifies the name of the system on which the refreshed component is installed.
Status	Specifies the status of the cache refresh request.

Configuring Attribute Encryption

By default, AuthMinder stores the user-related data in plain format in the database tables that you seed during installation. To encrypt this data, you use the Attribute Encryption Set Configuration page and select the user attributes that you want to encrypt. See "Multi-Byte Characters and Encrypted Parameters" (see page 287) for the list of attributes that can be stored in an encrypted format.

To store the user attributes in the encrypted format:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.

   Under the **System Configuration** section on the side-bar menu, click the **Attribute Encryption Configuration** link to display the page.

   Note: If you choose to encrypt the User Identifier attribute, all the following attributes that help in uniquely identifying the user are also encrypted:

   - User ID
   - Account ID
   - Account ID attributes
4. In the **Select Attribute(s) for Encryption** section, select the attributes that you want to encrypt from the **Available Attributes for encryption** list to the **Attributes Selected for encryption** list.

   Click the > button to move selected attributes to the desired list. You can also click the >> button to move all attributes to the desired lists.

   Note: Hold the **Ctrl** key to select more than one attribute at a time.

   The **Attributes Selected for encryption** list displays all the attributes that will be stored in an encrypted format.
5. In the **Data Masking Configuration** section, specify the parameters that are described in the following table:

Parameter	Description
Type	Select an option from the drop-down list to **Mask** or **Unmask** the attributes configured for encryption.
Start Length	The number of characters to be masked or unmasked from the start of the actual data string.
End Length	The number of characters to be masked or unmasked from the end of the actual data string.
Masking Character	The character that will be used to mask (hide) the actual data.

For example, if you want to mask a user name that has been configured for encryption, and the **Start Length**, **End Length**, and **Masking Character** are 2, 2, and x, then the user name "mparker" is masked as "xxarkxx", and vice-versa for unmasking.

6. Click **Save** to save the changes that you have made.
7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Configuring Custom Locales

AuthMinder supports *localization*, which is the process of adapting internationalized software for a region or language of your choice, by adding locale-specific components and translating the text. You can configure the supported locales in the Localization Configuration page.

Before you configure custom locales, you can add languages that will appear in the **Available** list for you to choose. See "Preparing for Localization" in the *CA AuthMinder Installation and Deployment Guide*.

To configure custom locales and set the default locale and date time format:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **System Configuration** section on the side-bar menu, click the **Localization Configuration** link to display the page.
5. In the **Configure Supported Locales** section, select the locales that you want to add from the **Available** list to the **Selected** list.

   Click the > button to move selected locales to the desired list. You can also click the >> button to move all locales to the desired lists.

   Note: Hold the **Ctrl** key to select more than one locale at a time.
6. In the **Configure Default Locale** section, select the **Default Locale** from the drop-down list.
7. In the **Configure Default Date Time Format** section, specify the **Date Time Format** you want to use.

   Note: The Administrator can change the Locale and Date Time Format on the My Profile page.
8. Click **Save** to save your changes.
9. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Setting the Default Organization

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

As a single-organization system, the Default Organization is useful because you do not need to create organizations. You can configure the Default Organization settings, change its Display Name (see "Updating the Basic Organization Information" (see page 177)), and then continue to use it for administering purposes. In the case of a multi-organization system, however, you can either rename the Display Name of the Default Organization, configure its settings, and continue to use it as the default, or you can create an organization and set it as the Default Organization.

Note: Typically, when you perform an operation *without* specifying the organization, then that operation is carried on the Default Organization. For example, if you create administrators without specifying the organization, then the administrators are created in the Default Organization.

The Set Default Organization page enables you to select the organization that will be used as the Default Organization.

To specify the Default Organization:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. In the left pane, under the **UDS Configuration** section, click the **Set Default Organization** link to display the Set Default Organization page.
5. Under **Default Organization**, select the organization that you want to set as the Default Organization from the **Organization Name** list.
6. Click **Save** to save the changes you made on this page.

   The "Default organization set successfully" message appears.
7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Configuring the Account Type

All AuthMinder users are identified in the system by a unique user name. AuthMinder supports the concept of an *account* or *account ID*, which is an alternate ID to identify the user in addition to the user name. A user can have none or one or more accounts or account IDs.

For example, consider a banking institution that uses the ID from the Customer Information File (CIF), to identify the customer Robert Laurie. In addition, Robert uses his account number to transact with the bank for his fixed deposits and also a different account ID for online banking. So, Robert has the following account IDs:

- User name: BNG02132457678
- Account ID for fixed deposits: 000203876544
- Account ID for online banking: rlaurie

An *account type* is an attribute that qualifies the account ID and provides additional context about the usage of the account ID. An account ID uniquely identifies a user for the given account type.

For example, you can create an account type called FIXED_DEPOSITS for the 000203876544 account ID, and another account type called ONLINE_BANKING for the account ID rlaurie.

Now, Robert can log in to the system and can be identified using any of the following:

- BNG02132457678
- FIXED_DEPOSITS/000203876544
- ONLINE_BANKING/rlaurie

You first create an account type in the Administration Console before you can create account IDs. You can configure the account type to be available to specific organizations only or to all organizations, including those that will be created in the future. At the organization level, each organization can choose to support a set of account types.

Note: No two users in a given organization can have the same account ID. At any given time, the following combinations are unique:

- Organization name, account type, and account ID
- Organization name and user name

Creating a New Account Type

To create an account type:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.

3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **UDS Configuration** section on the side-bar menu, click the **Configure Account Type** link to display the page.
5. (If this is the first account type you are adding) In the **Add New Account Type** section:
   a. Enter the **Name** of the account type.
   b. Enter a **Display Name** for the account type.
   c. If required, expand the **Custom Attributes** section by clicking the + sign and specify the **Name** and **Value** of any custom attributes that you want to add for this account type.
6. In the **Assign to Organizations** section:
   - Select **Apply to all organizations** if you want to use this account type for all existing organizations and any organizations that may be created in future.

     Note: Such accounts appear under **Global Accounts** on the **Configure Account Type** page at the organization level.

     or
   - Select the organization to which you want to assign the account type from the **Available** list to the **Selected** list.

     Note: Such accounts appear under **Organization Specific Accounts** on the **Configure Account Type** page at the organization level.

     Click the > button to move selected organizations to the desired list. You can also click the >> button to move all organizations to the desired lists.

     Note: Hold the **Ctrl** key to select more than one organization at a time.
7. Click **Create** to create the account type.
8. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Updating an Account Type

To update an existing account type, select the account type that you want to modify from the **Select Account Type** drop-down list, modify the required fields, and click **Update**.

Note: You *cannot* change the **Name** or **Scope** of the account type.

Deleting an Account Type

To delete an existing account type, select the account type that you want to delete from the **Select Account Type** drop-down list and click **Delete**.

Refresh *all* deployed AuthMinder Server instances after modifying or deleting an account type. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Note: You *cannot* delete an account type if you have created user accounts for that type.

Configuring Email and Telephone Types

AuthMinder allows you to specify multiple email addresses and telephone numbers while creating users and administrators. The MA can configure multiple email and telephone types at the global level, which automatically become available to all organizations. The MA can also specify certain email and telephone types as mandatory and others as optional. When you create users and administrators in an organization, you are prompted to enter values for the email and telephone types that the MA has configured. You can choose to override the global configuration by configuring different email and telephone types while creating organizations.

Note: Email and telephone type attributes configured at the organization level override and take precedence over the values that are configured at the global level.

Email and Telephone Type Example

Assume that the MA has configured the following email and telephone types that all organizations must use:

- (Mandatory) Email type: Work Email
- (Optional) Email type: Personal Email
- (Mandatory) Telephone type: Work Phone
- (Optional) Telephone type: Home Phone

Now, when a GA creates an administrator for an organization *Org1* that uses the global configuration, the GA *must* provide values for Work Email and Work Phone. The GA can add additional email and telephone types, if required, but cannot delete the global configurations for email and telephone types.

To configure the email and telephone type attributes:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. In the left pane, under the **UDS Configuration** section, click the **Email/Telephone Type Configuration** link to display the page.
5. In the **Configure Email Type** section, specify:
   - **Priority** of the Email Type if more than one Email Type has been configured. Use the up and down icons to change the priority. Priority defines the order in which Email Types are displayed on the screen when multiple Email Types have been configured.
   - **Type** of email being configured, for example, work or personal.
   - **Display Name** of the Email Type.
   - Whether the Email Type is **Mandatory**.

6. In the **Configure Telephone Type** section, specify:
   - **Priority** of the Telephone Type if more than one Telephone Type has been configured. Use the up and down icons to change the priority. Priority defines the order in which Telephone Types are displayed on the screen when multiple Telephone Types have been configured.
   - **Type** of phone number being configured, for example, home or work.
   - **Display Name** of the Telephone Type.
   - Whether the Telephone Type is **Mandatory**.

   Note: You can add more Email and Telephone types by clicking the **+** icon.
7. Click **Save** to save your changes.
8. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Specifying Basic Authentication Settings

Administrators logging into the Administration Console can be authenticated either by using the **Basic User Password**, **LDAP User-Password**, or **WebFort Password** mechanism. The mechanism to be used is determined by the option that you select while creating the organization:

- If you selected the **Basic User Password** option, then you can either use the default authentication settings, or set new configurations as discussed in the Configuring the Basic Authentication Password Policy (see page 48).
- If you selected the **LDAP User Password** option, the password that is stored in LDAP is used by the administrator to log in. The authentication policy is defined in the LDAP system.
- If you selected the **WebFort Password** option, then you first specify the connection information to the AuthMinder Server (as discussed in "Configuring (see page 64)AuthMinder Connectivity" (see page 64)).

Configuring the Basic Authentication Password Policy

As the name implies, *Basic Authentication* method enables administrators to log in to the Console by using a user ID and the corresponding password.

You can use the Basic Authentication Policy page to strengthen the password policy by enforcing restrictions, such as password length, allowed number of special characters, and the number of failed login attempts allowed before locking the user's access to the system.

To specify the Basic Authentication password policy:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. In the left pane, under the **Authentication** section click the **Basic Authentication Policy** link to display the corresponding page.
5. Specify the parameters that are listed in the following table in the **Password Policy Configuration** section. All the parameters on this page are mandatory.

Parameter	Default Value	Description
Minimum Password Length	6	The least number of characters that the password must contain. You can set a value between 6 and 32 characters.
Maximum Password Length	25	The most number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password must contain. You can set a value between 0 and 32 characters.
Maximum Password History Count	3	The number of previous passwords that cannot be reused.
Validity Period	180 days	The maximum number of days for which a password is valid. If you want the password *not* to expire, then choose the **Never Expires** option.

Parameter	Default Value	Description
Allow Multi-Byte Characters	Disabled	Enable this option if you want to store the parameters in multi-byte character format. **Note:** If you select this option, then the next three fields will be disabled.
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of Allowed Special Characters that the password must contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#$%^&*()_+	The list of special characters that the password can contain.

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

   The "Successfully updated the Password Policy" message appears.

Specifying Master Administrator Authentication Policy Settings

By default, the Master Administrator follows the *Basic Authentication* method that enables them to log in to the Console by using a user ID and the corresponding password.

You can use the Master Administrator Authentication Policy page to strengthen the MA password policy by enforcing restrictions, such as password length, allowed number of special characters, and the number of failed login attempts allowed before locking the MA access to the system.

To configure the Master Administrator Authentication policy:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. In the left pane, under the **Authentication** section, click the **Master Administrator Authentication Policy** link to display the corresponding page.
5. Specify the parameters explained in the following table in the **Password Policy Configuration** section. All the parameters on this page are mandatory.

Parameter	Default Value	Description
Minimum Password Length	6	The least number of characters that the password must contain. You can set a value between 6 and 32 characters.
Maximum Password Length	25	The most number of characters that the password can contain. You can set a value between 6 and 32 characters.
Maximum Failed Attempts	5	The maximum consecutive number of times an administrator can specify the password incorrectly, after which the credential will be locked. You can set a value between 3 and 10.
Minimum Numeric Characters	1	The least number of numeric characters (0 through 9) that the password must contain. You can set a value between 0 and 32 characters.
Maximum Password History Count	3	The maximum number of previously used passwords that cannot be reused.
Validity Period	180 days	The maximum number of days for which a password is valid.

Parameter	Default Value	Description
Allow Multi-Byte Characters	Disabled	Enable this option if you want to store the parameters in multi-byte character format. **Note:** If you select this option, then the next three fields are disabled.
Minimum Alphabetic Characters	4	The least number of alphabetic characters (a-z and A-Z) that the password must contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	1	The least number of Allowed Special Characters that the password must contain. You can set a value between 0 and 32 characters.
Allowed Special Characters (optional)	!@#$%^&*()_+	The list of special characters that the password can contain.

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

Enabling Web Services Authentication and Authorization

AuthMinder provides Web Services to programmatically perform credential issuance, user authentication, and administration operations. You can secure these Web Services calls by enabling authentication and authorization. You can use the Administration Console to select the Web Services for which you want to enable authentication and authorization.

Note: See "Managing Web Services Security" in the *CA AuthMinder Web Services Developer's Guide* for more information about how Web Services authentication and authorization works.

To enable Web Services authentication and authorization:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Click the **Administration Console** option on the submenu of the tab.
4. Under the **Web Services** section on the side-bar menu, click the **Authentication and Authorization** link to display the page.
5. In the **Web Services** section, select the Web Services from the **Disabled** list to the **Enabled** list.

   Click the > button to move selected Web Services to the desired list. You can also click the >> button to move all Web Services to the desired lists.

   Note: Hold the **Ctrl** key to select more than one Web Service at a time.
6. Click **Save** to save your changes.
7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing the Cache" (see page 36) for instructions on how to refresh the system cache.

Chapter 3: Working with Custom Roles

Important! The role management tasks that are discussed in this chapter can only be performed by the Master Administrator.

AuthMinder is shipped with out-of-the-box roles that are associated with predefined permissions. (See "Supported Roles" (see page 14) for more information about this topic.) However, AuthMinder also provides you the capability to manipulate these predefined roles in case:

- The default roles do not meet your organization's requirements.
- You want to manage a role information that is different from the one provided by AuthMinder.

This chapter explores the ability to create and apply custom roles in AuthMinder, which are a major benefit. This chapter guides you through:

Understanding Custom Roles

As an MA, you can create *new administrative roles* that inherit a subset of permissions from one of the following predefined parent roles (as discussed in "Overview of the Administration Console" (see page 11)):

- Global Administrator (see page 19)
- Organization Administrator (see page 20)
- User Administrator (see page 20)

These roles are called *custom roles*, and are derived by **disabling** some of the default permissions associated with the parent role. For example, if you want to disable the permission to create organizations for a GA, you can create a custom role by disabling this permission, and assigning the same to the GA.

When you create a custom role, it becomes available as a role option when you create or update an administrator. In addition to creating custom roles, you can also update and delete them. See the following sections in this chapter for more information about management of custom roles.

Things That You Should Know About Custom Roles

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

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

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

  For example, the "Search Organizations" link will appear if the Update permission is still available, even though the Activate, Deactivate, and Delete permissions are disabled.
- A new custom role is available to other instances of Administration Console *only after* you refresh the server cache (see "Refreshing a Server Instance" (see page 67)).

Creating a Custom Role

To create a custom role:

1. Activate the **Users and Administrators** tab.
2. From the submenu, click the **Manage Roles** link to display the Create Custom Role page.
3. In the **Role Details** section, specify the following information:
   - **Role Name:** The unique name to identify the new role. This name is used internally by AuthMinder for authenticating and authorizing this new role.
   - **Role Display Name:** The descriptive name of the role that appears on all other Administration Console pages and reports.
   - **Role Description**: The useful information that is related to the role for later reference.
   - **Role Based On**: The pre-existing role from which this custom role should be derived.
4. In the **Set Privileges** section:
   a. In the **Available Privileges** list, select all the permissions that you want to *disable* for the custom role.

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

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

   b. Click the **>** button to move the selected permissions to the **Unavailable Privileges** list.
5. Click **Create** to create the custom role.
6. Refresh the cache. See "Refreshing the Cache" (see page 36) for more information.

Updating Custom Role Information

To update an existing custom role definition:

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

   The Update Custom Role page appears.
4. Select the **Role Name** that you want to update.
5. Make the required changes to one or all of the fields in the **Role Details** section.
6. In the **Set Privileges** section, perform one of the following steps:
   a. In the **Available Privileges** list, select all the permissions that you want to *disable* for this role.

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

      Alternatively, in the **Unavailable Privileges** list, select the permissions that you want to *enable* for this role.

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

      Note: You can hold the **Ctrl** key to select more than one permission at a time.
   b. Click the **>** button to move the selected permissions to the **Unavailable Privileges** list.
7. Click **Update** to update the Custom role definition.
8. Refresh the cache. See "Refreshing the Cache" (see page 36) for more information.

Deleting a Custom Role

Important! You *cannot* delete a custom role that is currently assigned to an administrator. If you want to delete such a role, first change the role of all administrators who are assigned this role by using the Update Administrator page and then follow the instructions in this section.

To delete an existing custom role:

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

   The Delete Custom Role page appears.
4. In the **Role Details** section, select the custom role that you want to delete from the **Role Name** list.
5. Click **Delete** to delete the selected custom role.

   Note: A custom role *cannot* be deleted if it is assigned to any of the administrators.
6. Refresh the cache. See "Refreshing the Cache" (see page 36) for more information.

Summary of Administrative Permissions

The following table summarizes the permissions available to the supported three levels of administrators using which you create a custom role.

The column name acronyms that are used in the table are as follows:

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

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

Permission	GA	OA	UA
Organization Management Permissions See "Managing Organizations" (see page 163) for more information about the tasks related to these permissions.			
Create Organization		✓	
Update Organization		✓	✓

Permission	GA	OA	UA
Update Organization Status		✓	✓
List Organizations		✓	✓
Retrieve Default Organization		✓	✓
Delete Organization		✓	✓
Account Type Management Permissions See "Configuring the Account Type" (see page 43) for more information about the tasks related to these permissions.			
Create Account Type		✓	
Update Account Type		✓	✓
Delete Account Type		✓	
Administrator Management Permissions See "Managing Administrators" (see page 195) for more information about the tasks related to these permissions.			
Create Administrator		✓	✓
Update Administrator		✓	✓
Delete Administrator		✓	✓
User Management Permissions See "Managing Users and Their Credentials" (see page 225) for more information about the tasks related to these permissions.			
Create User		✓	✓
Update User		✓	✓
Update User Status		✓	✓
List Users		✓	✓
List Users for Account		✓	✓
Get User Status		✓	✓
Set User Custom Attributes		✓	✓

Permission	GA	OA	UA
Search Users		✓	✓
Get PAM		✓	✓
Set PAM	✓	✓	✓
Delete User	✓	✓	✓
User Account Management Premissions See "Managing Users and Their Credentials" (see page 225) for more information about the tasks related to these permissions.			
Create User Account	✓	✓	✓
Update User Account	✓	✓	✓
List User Accounts	✓	✓	✓
Retrieve User Account	✓	✓	✓
Delete User Account	✓	✓	✓
Cache Management Permissions See "Refreshing the Cache" (see page 36) for more information about the tasks related to these permissions.			
Refresh System Cache	✓		
Refresh Organization Cache	✓	✓	
View Global Cache Refresh Requests	✓		
View Organizational Cache Refresh Requests	✓	✓	
Email and Telephone Type Permissions See "Configuring Email and Telephone Types" (see page 46) for more information about the tasks related to these permissions.			
Add Email/Telephone Types	✓	✓	
Update Email/Telephone Types	✓	✓	
List Email Types	✓	✓	
List Telephone Types	✓	✓	
Basic Authentication Permissions See "Specifying Basic Authentication Settings" (see page 47) for more information about the tasks related to these permissions.			
Update Global Basic Authentication Policy	✓		

Permission	GA	OA	UA
Update Organizational Basic Authentication Policy	✓	✓	
Encryption Permissions See "Configuring Attribute Encryption" (see page 40) for more information about the tasks related to these permissions.			
Configure the Encryption Set Selected at the Organization Level	✓	✓	
List Configured Attributes for Encryption	✓	✓	
Credential Management Permissions See "Updating User Credential Information" (see page 234) for more information about the tasks related to these permissions.			
Add Element to ArcotID keybag	✓	✓	✓
Create Credential	✓	✓	✓
Delete ArcotID Attribute	✓	✓	✓
Delete Credential	✓	✓	✓
Delete Elements From ArcotID Key	✓	✓	✓
Disable Credential	✓	✓	✓
Download Credential	✓	✓	✓
Enable Credential	✓	✓	✓
Fetch Credential	✓	✓	✓
Get ArcotID	✓	✓	✓
Get Element from ArcotID Keybag	✓	✓	✓
Get Questions and Answers	✓	✓	✓
Reissue Credential	✓	✓	✓
Reset Credential	✓	✓	✓
Reset Credential Custom Attribute	✓	✓	✓
Reset Credential Validity	✓	✓	✓
Set ArcotID Attribute	✓	✓	✓
View Credential Details	✓	✓	✓

Permission	GA	OA	UA
Configuration Permissions See "Managing Global (see page 89)AuthMinder Configurations" (see page 89) for more information about the tasks related to these permissions.			
Assign Configurations as Default	✓	✓	
Assign Configurations	✓	✓	
Check key label in HSM	✓	✓	
Configure Plug-In	✓	✓	
Create ArcotID Policy	✓	✓	
Create ArcotOTP-EMV OTP Policy	✓	✓	
Create ArcotOTP-OATH Policy	✓	✓	
Create OATH OTP Policy	✓	✓	
Create OTP Policy	✓	✓	
Create QnA Policy	✓	✓	
Create Password Policy	✓	✓	
Credential Key Management	✓	✓	
Credential Type Resolution Configuration	✓	✓	
Fetch Credential Configuration	✓	✓	✓
Manage ASSP Configuration	✓	✓	
Manage ArcotID Profile	✓	✓	
Manage ArcotOTP Profile	✓	✓	
Manage ArcotOTP-EMV Profile	✓	✓	
Manage OATH OTP Profile	✓	✓	
Manage OTP Profile	✓	✓	
Manage QnA Profile	✓	✓	
Manage RADIUS Configuration	✓	✓	
Manage RADIUS Proxy	✓	✓	
Manage SAML Token Configuration	✓	✓	
Manage Password Profile	✓	✓	
Module Association	✓	✓	
OATH Token Management	✓		

Permission	GA	OA	UA
Other Permissions			
Get QnA Attributes	✓	✓	
Get QnA Values	✓	✓	✓
List Arcot Attributes	✓	✓	
List Repository Attributes	✓	✓	
Perform QnA Verification	✓	✓	✓
Bulk Upload	✓	✓	
View Bulk Upload Requests	✓	✓	
Report Permissions See "Managing Reports" (see page 257) for more information about the tasks related to these permissions.			
View My Activity Report	✓	✓	✓
View User Activity Report	✓	✓	✓
View User Creation Report	✓	✓	✓
View Organization Report	✓	✓	
View Administrator Activity Report	✓	✓	✓
View Authentication Report	✓	✓	✓
View Credential Report	✓	✓	✓
View Configuration Management Report	✓	✓	

Chapter 4: Managing AuthMinder Server Instances

Important! All the configurations and tasks that are discussed in this chapter can *only* be performed by **Master Administrator**.

Each system where AuthMinder Server is installed and is configured to listen to the incoming requests on specified ports is referred to as an *instance*. The uniqueness of each server instance is defined by its *instance name*, which is a combination of host name and a unique number.

As a Master Administrator, you can manage each AuthMinder instance either locally or remotely. However, before you can manage a Server instance, you configure the connectivity parameters to connect to the instance. (See "Configuring (see page 64)AuthMinder Connectivity" (see page 64), for information about how the procedure.)

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

- Configuring (see page 64)AuthMinder Connectivity (see page 64)
- Setting Up Server Instances (see page 67)
- Creating Trust Stores (see page 76)
- Configuring Communication Protocols (see page 76)
- Monitoring Instance Statistics (see page 80)
- Registering and Updating Plug-Ins (see page 84)
- Configuring Miscellaneous Settings (see page 86)

Note: Some of these tasks can be performed by using system tools, as discussed in "Tools for System Administrators" **(see page 241).**

Configuring AuthMinder Connectivity

You can install multiple instances of AuthMinder Server. However, you can use the Administration Console to configure the connection details to only one of these instances. This configured instance obtains the data of other instances for performing multi-instance management and failover from one instance to other for operations such as, configuration creation and credential issuance performed using Administration Console.

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

To specify the AuthMinder connectivity parameters:

1. Ensure that you are logged in as the MA.
2. Activate the **Services and Server Configurations** tab.
3. Ensure that the **WebFort** option on the submenu is selected.
4. If not already displayed, click **WebFort Connectivity** in the tasks pane to display the corresponding page.
5. Use the information in the following table to edit the fields on the WebFort Connectivity page.

Field	Default Value	Description
IP Address of the AuthMinder Server	localhost	Enter the IP address of the system where you installed the required AuthMinder Server instance. **Note:** Ensure that the systems where AuthMinder components are installed are accessible to each other by their host name on the network.
Port	9743	Enter the port on which the Server Management web Service protocol service is exposed. **Note:** This field is valid only for Server Management Web Services protocol because it has to fetch information about other AuthMinder instances.

Field	Default Value	Description
Transport	TCP	Specify the transport mode for the corresponding component (Server Management Web Services, Administration Web Services, Transaction Web Services, and Authentication Native) to connect to the specified AuthMinder Server instance. The supported values are: ■ **SSL(1-Way):** One-way Secure Sockets Layer (SSL) is used to encrypt and decrypt data under transmission. ■ **SSL(2-Way)**: Two-way SSL is used to encrypt and decrypt data under transmission. ■ **TCP**: Transmission Control Protocol (TCP) mode is used to encrypt and decrypt data under transmission.
Server CA Certificate in PEM	NA	Upload the server certificate chain by using the respective **Browse** button in the corresponding field. **Note:** This field is applicable if **SSL(1-Way)** or **SSL(2-Way)** is selected in the Transport field.
Client Certificate-Key Pair in PKCS#12	NA	Upload the public and private key pair of the client certificate by using the respective **Browse** button in the corresponding field. **Note:** This field is applicable if **SSL(2-Way)** is selected in the Transport field.
Client PKCS#12 Password	NA	The password corresponding to the P12 file. **Note:** This field is applicable if **SSL(2-Way)** is selected in the Transport field.
Advanced Configurations Section		
Maximum Active Connections	32	The maximum active connections that can be maintained between the client and the AuthMinder Server.
Maximum Idle Connection	8	The maximum number of idle connections that can be maintained with the AuthMinder Server.

Field	Default Value	Description
Maximum Wait Time (in Milliseconds)	-1	The maximum amount of time (in milliseconds) the client must wait (when there are no available connections) for a connection to become available, before timing out.
Minimum Wait Time for Eviction (in Milliseconds)	300000	The minimum amount of time (in milliseconds) a connection might be idle in the pool before it is evicted by the idle connection evictor (if any).
Time Between Eviction Runs (in Milliseconds)	600000	The amount of time (in milliseconds) to wait before checking the pool to evict the idle connections.
Connection Timeout	10000	The maximum amount of time (in milliseconds) before the AuthMinder Server is considered unreachable.
Read Timeout	30000	The maximum amount of time (in milliseconds) allowed for a response from AuthMinder Server.

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

Note: If you add a new AuthMinder Server instance, then before proceeding with the instance-specific configurations, click **Save** on this page. This ensures that the Administration Console gets the details of the newly added instance and the instance management functions will work smoothly for the newly added instance.

Setting Up Server Instances

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

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

Typical instance management operations include:

- Refreshing a Server Instance (see page 67)
- Changing the Instance Name (see page 69)
- Managing (see page 70)AuthMinder Server Logging Configurations (see page 70)
- Configuring Database Parameters (see page 72)
- Reading Instance Timestamp Details (see page 73)
- Shutting Down a Server Instance (see page 73)
- Restarting a Server Instance (see page 75)

Note: You can also perform most of the operations that are discussed in this section by using the arwfutil command-line tool. See "arwfutil: A Utility Tool" (see page 251) for more information.

Refreshing a Server Instance

You can refresh AuthMinder Server instances either through Administration Console or by using the arwfutil tool.

Using Administration Console

You can refresh a specific AuthMinder Server instance by selecting the instance on the Instance Management page.

To refresh AuthMinder Server instances:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab in the main menu.
3. Under the Instance Configurations section, click the Instance Management link to display the WebFort Instances page.
4. In the Select column, select the server instances whose status you want to change.
5. Click Refresh to refresh the selected instances.

Using arwfutil Tool

To refresh a AuthMinder Server instance using the arwfutil tool:

1. Log in to the system where the arwfutil tool is available.
2. Navigate to the following directory:
   - **On Windows:**
     `<install_location>\Arcot Systems\bin\`
   - **On UNIX-based Platforms:**
     `<install_location>/arcot/sbin/`
3. Run the tool, as follows:
   - **On Windows:**
     `arwfutil cr`
   - **On UNIX-based Platforms:**
     `./arwfutil cr`

Changing the Instance Name

Based on the host on which the instance is running and the timestamp of the first startup, AuthMinder Server generates a unique name for each instance. This name is used in reports and is logged in audit logs. To enable easy identification of an instance, provide an appropriate name for each instance.

To change the instance name of an AuthMinder Server instance:

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

   The Instance name: <selected_instance> page appears.
6. In the Instance Attributes section, enable the Change the Instance Name option.
7. Enter the new name in the New Instance Name field.
8. Click Save to save the changes.
9. Refresh the AuthMinder Server instance for which you made the preceding changes. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Managing AuthMinder Server Logging Configurations

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

- AuthMinder log file (arcotwebfort.log)
- AuthMinder Startup log file (arcotwebfortstartup.log)
- Administration Console log file (arcotadmin.log)
- UDS log file (arcotuds.log)

  Note: See " (see page 275)AuthMinder Logging" (see page 275) for detailed information about the location of these log files, the severity levels that you see in these log files, and the formats of these log files.

By using an instance-specific page, you can control logging configurations for the AuthMinder log file for the instance.

To change the AuthMinder Server log configurations:

Note: See "Reading Instance Timestamp Details" (see page 73) for information about how to control the configurations in the AuthMinder Statistics log file by using the Administration Console.

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

   The Instance name: <*selected_instance*> page appears.
6. Edit the fields in the **Logging Configurations** section, as required. The following table describes the fields of this section.

Field	Description
Transaction Log Directory	Specify the directory where the log files have to be created. You can either enter the absolute path or the path relative to ARCOT_HOME.
Rollover After (in Bytes)	Enter the maximum size for the log file. After the log file reaches this size, the log content is moved to a backup file.

Field	Description
Transaction Log Backup Directory	Specify the directory where the backup files will be stored. You can either enter the absolute path or the path relative to ARCOT_HOME.
Log Level	Specify the level of detail of the information to be logged. The possible values are: ■ FATAL ■ WARNING ■ INFO ■ DETAIL See "Supported Severity Levels" (see page 282) for more information about log levels.
Log Timestamps in GMT	Enable this option if you want the AuthMinder Server instance to log all the messages in GMT time zone format.
Enable Trace Logging	Enable this option if you want the AuthMinder Server instance to generate logs for the functional flow for every transaction. This is useful while debugging any flow issues.

1. Click **Save** to save the changes.
2. Refresh the AuthMinder Server instance for which you made the preceding changes. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring Database Parameters

AuthMinder uses *connection pooling*, which helps avoid the overhead of establishing a new database connection each time the server requires access to the database. By using the instance-specific page, you can configure these connection pooling parameters for the instance. The data that is displayed on the Instance Statistics (see "Monitoring Instance Statistics" (see page 80)) page depends on the parameters that are configured on this page.

To change the database configuration parameters:

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

   The Instance name: <selected_instance> page appears.
6. Edit the fields in the Database Configurations section, as required. The following table describes the fields of this section:

Field	Description
Minimum Connections	Enter the minimum number of connections that will be created between AuthMinder Server and the database when the server starts up.
Maximum Connections	Enter the maximum number of connections that can be created between the AuthMinder Server and the database. **Note:** You set this value depending on the maximum connections that the database supports, because this parameter overrides the MaxConnections parameter. See your database vendor documentation for more information.
Increment Connections by	Enter the number of connections that will be added to the existing connections at a time, when the need arises. **Important!** The total number of connections *cannot* exceed the maximum number of connections.

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

7. Click **Save** to save the changes.
8. Refresh the AuthMinder Server instance for which you made the preceding changes. See "Refreshing a Server Instance" (see page 67) for instructions on how to do this.instructions about how to achieve this.

Reading Instance Timestamp Details

The instance-specific page provides the timestamp details for each server instance in the **Server Timestamp Details** section. The following table explains these details:

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

Shutting Down a Server Instance

You can shut down AuthMinder Server instances either through Administration Console or by using the arwfutil tool.

Using Administration Console

You can shut down a specific AuthMinder Server instance by selecting the instance on the Instance Management page.

To shut down AuthMinder Server instances:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab in the main menu.
3. Under the Instance Configurations section, click the Instance Management link to display the WebFort Instances page.
4. In the Select column, select the server instances whose status you want to change.
5. Click Shut Down to shut down the selected instances.

Using arwfutil Tool

To shut down an AuthMinder Server instance by using the arwfutil tool:

1. Log in to the system where the arwfutil tool is available.
2. Navigate to the following directory:
   - **On Windows:**
     `<install_location>\Arcot Systems\bin\`
   - **On UNIX-based Platforms:**
     `<install_location>/arcot/sbin/`
3. Run the tool, as follows:
   - **On Windows:**
     `arwfutil sd`
   - **On UNIX-based Platforms:**
     `./arwfutil sd`

Restarting a Server Instance

If you shut down a AuthMinder Server instance, then start it by following the procedure that is described in this section.

On Windows

To start a server instance on Windows:

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

On UNIX-Based Platforms

To start a server instance on UNIX-based platforms:

1. Log in to the system where the instance has stopped.
2. Navigate to the following directory:
   `<install_location>/arcot/bin/`
3. Run the following command:
   `./webfortserver start`

Creating Trust Stores

You can create a trust store to authenticate AuthMinder components (that includes Administration Console, Java SDKs, and Web Services) or other clients to an AuthMinder Server instance during SSL-based communications. A *trust store* contains the CA root certificates that are trusted by AuthMinder Server.

Each of your AuthMinder Server instances can be configured for different certificates by using different trust stores. You can use the Trusted Certificate Authorities page to create trust stores and to add new root certificates to your trust stores.

To create a trust store for the current server instance:

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

Configuring Communication Protocols

By using the Protocol Configuration page, you can configure the protocols that Administration Console, SDKs, and Web Services use to communicate with a AuthMinder Server instance for credential management, authentication, and administration purposes. The ports on which the server instance listens for each protocol can also be configured using this page.

The following table explains the protocols that are listed on the Protocol Configuration page and gives their default port numbers:

Protocol	**Default Port Number**	**Description**
Administration Web Services	9745	This protocol is used to manage SAML, ASSP, profile and policy configurations.

Protocol	Default Port Number	Description
ASSP	9741	Adobe Signature Service Protocol (ASSP) is used with Adobe Reader and Adobe Acrobat to authenticate users for server-side digital signing of the PDF documents.
RADIUS	1812	This is a RADIUS listener protocol that is used to extend AuthMinder capability to support the Remote Authentication Dial In User Service (RADIUS) protocol. **Note:** When configured to support RADIUS, AuthMinder Server acts as a RADIUS server.
Server Management Web Services	9743	The Administration Console and the arwfutil tool communicate to the AuthMinder Server instance for server management activities by using this protocol.
Transaction HTTP	9746	This protocol receives HTTP data. It is used for ArcotID OTP provisioning and ArcotID PKI key bag management operations. **Note:** This protocol does not expose other generic AuthMinder operations.
Transaction Native	9742	This is a binary AuthMinder protocol for issuance and authentication. This protocol is used by Issuance and Authentication Java SDKs.
Transaction Web Services	9744	This protocol receives Web services requests that are sent by Authentication and Issuance Web services.

To configure AuthMinder network protocols:

Note: The data that is displayed in the Instance Statistics (see "Monitoring Instance Statistics" (see page 80)) page depends on the parameters that are configured on this page.

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab in the main menu.
3. Ensure that the WebFort tab in the submenu is active.

Under the Instance Configurations section, click the Protocol Management link to display the Protocol Configuration page.

1. Select the Server Instance for which you want to configure the protocols.
2. In the List of Protocols section, click the protocol that you want to configure.

   The page to configure the specific protocol appears.
3. Edit the fields on the page, as required. The following table explains these fields:

Field	Description
Protocol Status	Indicates whether the protocol is Enabled or Disabled.
Change Protocol Status Action	Select the Change the Protocol Status option to enable the Action list and then select the new status from the Action drop-down list. **Note:** The Server Management protocol cannot be disabled. Therefore, these options are not displayed for this protocol.
Port	Enter the port number where the protocol service will be available.
Maximum Allowed Request Size (in KB)	Specify the maximum size of the request that can be sent to the AuthMinder Server. If the input size exceeds this value, then the request is *not* processed by the AuthMinder Server. **Note:** By default, there is no limit on the input request size.
Minimum Threads	Specify the minimum number of threads to be maintained between the client and the AuthMinder Server.
Maximum Threads	Specify the maximum number of threads that can exist between the client and the AuthMinder Server.
Note: The following fields are *not* applicable for RADIUS protocol.	

Field	Description
Thread Threshold	Specify the maximum number of threads in percentage. Any additional requests over the threshold percentage of maximum threads will be closed immediately after serving the request. For example, Maximum Threads by default is 128 and Thread Threshold is 90%, this indicates that the threads that are established beyond 115 will be served and closed immediately.
Client Idle Timeout (in Seconds)	Enter the interval, in seconds, for which the AuthMinder Server waits for a request from the client before closing the connection.
Connection Keep Alive	Enable this option if you want the client to retain the connection even after the request is processed. The connection is closed when the connection duration is equal to Client Idle Timeout (in Seconds) period.
Transport	Specify the mode for data transfer. The supported values are: ■ **SSL(1-Way):** One-way Secure Sockets Layer (SSL) is used to encrypt and decrypt data under transmission. ■ **SSL(2-Way)**: Two-way SSL is used to encrypt and decrypt data under transmission. **Note**: This option is available only if you have configured the trust store, as discussed in "Creating Trust Stores" (see page 76). ■ **TCP**: Transmission Control Protocol (TCP) mode is used to encrypt and decrypt data under transmission.
Key in HSM	Enable this check box if the private key for the SSL communication needs to be in the HSM device. In this case, the AuthMinder Server will find the private key based on the certificate chain provided.
Certificate Chain (in PEM Format)	Upload the server certificate chain by using the respective **Browse** button in the corresponding field. **Note:** This field is available *only* if you select the **Key in HSM** option.
P12 File Containing Key Pair	Upload the public and private key pair of the server certificate by using the respective **Browse** button in the corresponding field.

Field	Description
P12 File Password	The password corresponding to the P12 file.
Select Client Store	Select the trust store that contains the root certificates of the trusted CAs. See "Creating Trust Stores" (see page 76) for more information about how to configure a trust store. **Note:** This field is applicable *only* for two-way SSL communication.

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

   Note: Configure each protocol individually.

2. Restart the AuthMinder Server instance for which you made the preceding changes. See "Restarting a Server Instance" (see page 75) for instructions about the procedure.

Monitoring Instance Statistics

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

To view the statistical details for an instance:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab in the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Instance Configurations section, click the Instance Statistics link to display the WebFort Statistics page.
5. Select the instance whose details you want to monitor from the Select Instance list.

   The following instance details are displayed:

   - Database Connectivity (see page 81)
   - Server Protocols (see page 81)
   - Thread Statistics (see page 82)
   - User Data Service Connectivity (see page 83)

Database Connectivity

The following table lists the database connection information:

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

Server Protocols

The following table lists the request, response, and the processing details for each configured AuthMinder protocol:

Field	Description
Processing Numbers	
Name	The name of the configured protocol.
Requests	The number of requests that are handled by the server instance.
Responses	The number of responses sent by the server instance.
Successful	The number of requests that were successfully processed by the server instance.

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

Thread Statistics

The following table lists the details of threads per protocol. It displays the configured values and the current state per protocol:

Field	Description
Configured Data	
Name	The name of the protocol that is used by the client to communicate with AuthMinder Server.
Minimum	The minimum configured threads for the listed protocol.
Maximum	The maximum threads allowed for the listed protocol.
Threshold	Threshold value of the maximum threads for the listed protocol. By default, this value is 115.

Field	Description
Current Footing	
Current	The current number of active threads established between the listed protocol and the AuthMinder Server.

User Data Service Connectivity

The following table lists the details for the connections between the AuthMinder Server instance and the UDS:

Field	Description
Processing Time (Milliseconds)	
Minimum	The minimum time taken by the UDS to process a request sent by the server instance.
Maximum	The maximum time taken by the UDS to process a request sent by the server instance.
Total (Seconds)	The total time taken by the UDS to process all requests from server instance.
Average	The average time taken by the UDS to process all server instance requests.
Total Calls Made	The total number of requests sent to UDS by AuthMinder Server.
Connection Details This section is applicable for requests sent by AuthMinder Server to the UDS Web service for operations such as, Web service authentication and authorization, and LDAP authentication.	
Minimum Connections	The minimum number of connections that exist between the server instance and the UDS.
Maximum Connections	The maximum number of connections that exist between the server instance and the UDS.
Active Connections	The number of connections that are active between the server instance and the UDS.
Inactive Connections	The number of idle connections between the server instance and the UDS.
Web Service Timeouts	The total number of requests that timed-out before a response from UDS was received.

Registering and Updating Plug-Ins

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

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

Registering Plug-Ins

To register a new plug-in with the system:

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

   For UNIX platforms, if this file is available in the path that is specified by LD_LIBRARY_PATH, then you do not need to provide the absolute path to the handler file. You can simply specify the name of the file without the extension. However, if this handler file is not available in the path that is specified by LD_LIBRARY_PATH, then specify the absolute path to it.
8. Click Browse available next to Configuration Template and navigate to the location of the plug-in configuration template file.

   The configuration template file defines the type of data that is used to configure the plug-in and the default values for the parameters that are used by the plug-in. This information is also used to render the Administration Console screen for plug-in configuration.
9. Select the events that you want to associate with the plug-in from the Available Events list, and click the > button to add these events to the Supported Events list.

   Note: The Available Events list displays all the events that are exposed by AuthMinder, while the Supported Events list displays the events that will be available for the new plug-in that you are registering.
10. Click Register to register the plug-in with *all* instances of AuthMinder.
11. Restart *all* deployed AuthMinder Server instances. See "Restarting a Server Instance" (see page 75) for instructions about how to perform this procedure.

Updating Plug-In Configurations

To update an existing plug-in configuration:

1. Ensure that you are logged in as the MA.
2. Navigate to the Register Plug-In page.
3. Select the Update option.
4. Select the required plug-in from the Name list.
5. Update the Handler Path and Configuration Template configuration for the plug-in.
6. Update the events that are associated with the plug-in.
7. Click Register to update the changes.
8. Restart *all* deployed AuthMinder Server instances. See "Restarting a Server Instance" (see page 75) for instructions about the procedure.

Configuring Miscellaneous Settings

The Miscellaneous Configurations page enables you to change the following settings (applicable to all instances of AuthMinder Server) that you may need to update:

- Length of One-Time Token (OTT) and its validity
- Validity of authentication tokens
- Enable or disable an authentication mechanism

To change the miscellaneous configurations:

1. Ensure that you are logged in as the MA.
2. Activate the Services and Server Configurations tab in the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Miscellaneous Configurations section, click the Miscellaneous Configurations link to display the corresponding page.
5. Edit the fields on the page, as required. The following table describes the fields of this page:

Field	Default Value	Description
General		
One-Time Token Length	6	Specify the length of the One-Time Token (OTT) that is issued to the users after successful authentication.

Field	Default Value	Description
Token Validity (in Seconds)	300	Specify the interval for which an OTT issued by AuthMinder will be valid.
Authentication Token Validity (in Seconds)	300	Specify the interval for which an authentication token issued by AuthMinder will be valid.
Change Authentication Mechanism Status		
ArcotID	Enabled	Specify whether you want AuthMinder to provide the ArcotID PKI authentication capability.
QnA	Enabled	Specify whether you want AuthMinder to provide QnA authentication.
Password	Enabled	Specify whether you want AuthMinder to provide the basic password authentication functionality.
OTP	Enabled	Specify whether you want AuthMinder to support OTP-based authentication.
OATH OTP	Enabled	Specify whether you want AuthMinder to support OATH OTP-based authentication.
Kerberos	Disabled	Specify whether you want AuthMinder to support Kerberos-based authentication. **Note:** Kerberos authentication is supported *only* for Adobe Signature Service Protocol (see "Configuring ASSP" (see page 151)).
ArcotOTP-OATH	Enabled	Specify whether you want AuthMinder to support ArcotOTP credentials that are OATH compliant.
ArcotOTP-EMV	Enabled	Specify whether you want AuthMinder to support ArcotOTP credentials that are EMV compliant.

6. Click **Update** to save the changes.
7. If you have changed the **General** configurations, then refresh *all* deployed AuthMinder Server instances. However, restart the AuthMinder Server if you change the authentication mechanism status. See "Refreshing a Server Instance" (see page 67) and "Restarting a Server Instance" (see page 75) for instructions about the procedure.

Chapter 5: Managing Global AuthMinder Configurations

Important! All the configurations and tasks that are discussed in this chapter can *only* be performed by **Global Administrators**.

You can manage AuthMinder configurations at two levels:

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

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

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

Note: These configurations are applicable for all organizations that are in the purview of the GA setting them. If you want to configure individual organizations, then first log in as the Global Administrator (GA) or as the Organization Administrator (OA) of the target organization. See "Updating Organization Information" (see page 176) for more information.

In addition to these tasks, GAs can also configure the Basic Authentication Policy at the global level. See "Configuring the Basic Authentication Password Policy" (see page 48) for information about the procedure.

Understanding AuthMinder Profiles and Policies

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

Credential Profiles

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

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

AuthMinder ships a default profile for each credential, *except* ArcotOTP-EMV credential. You can also create multiple profiles, each with a unique name, for all credential types. You can then set one profile as default. AuthMinder uses these configured profiles at the time of issuing credentials to users.

Authentication Policies

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

AuthMinder can generate the following types of tokens:

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

As in case of credential profiles, AuthMinder is also shipped with a default policy for each credential. You can also create multiple profiles, each with a unique name, for all credential types. You can then set one profile as the default.

Logging in as a Global Administrator

The first GA *must* be created by the MA. To log in as a GA and proceed with further configurations, obtain your login credential details from the MA. The GA can log in either by Using WebFort Password (see page 92) or by Using Basic User Password (see page 94).

Using WebFort Password

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

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

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

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

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

   Note: It is recommended that you bookmark this URL to access the Administration Console. Any GA, OA, or UA can use this URL to log in to the Administration Console by using their WebFort Password credentials.

   The Administrator Login page appears.
3. Enter the Organization Name that you want to log in to.

   Important! *Do not* enter the Display Name of the organization. Enter the unique ID of the organization (as defined by the Organization Name.) For example, if you want to log in to the Default Organization, whose Display Name is CA, then enter defaultorg, which is the (default) unique ID of this organization. Do not specify CA here.
4. Click Log In.

   The Login page appears.
5. Specify the user ID in User Name field, enter the corresponding activation code that you received in the Password field, and click Log In.
6. If you are logging in for the first time, you aree prompted to change the password.
7. Specify the New Password, Confirm Password, and then click Log In.

   You are redirected to the login page.
8. Specify the Password again and click Log In.

   The landing page of the Administration Console appears.

In Case You Forgot Your Password

If you forget your WebFort Password credential, then follow these steps to regenerate it:

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

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

   The Administrator Login page appears.

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

   The Login page appears.

3. Enter the User Name.

4. Click the Forgot Password? link.

   The Forgot Your Password? page appears.

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

   The page that displays the questions that you set in your Profile Information (See "Changing Administrator Profile Information" (see page 198) for instructions on how to set this QnA information) appears.

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

   The Reset Password page appears.

7. Specify the new password in New Password and Confirm Password fields.

8. Click Log In.

   The Login page appears.

9. Specify the Password again and click Log In.

   The landing page of the Administration Console appears.

Using Basic User Password

To log in to the Administration Console as a GA by using basic user password credentials:

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

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

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

   Note: It is recommended that you bookmark this URL to access the Administration Console. Any GA, OA, or UA can use this URL to log in to the Administration Console by using their credentials.

   The Administrator Login page appears.
3. Enter the Organization Name that you want to log in to.

   Important! Do not enter the Display Name of the organization. Enter the unique ID of the organization (as defined by the Organization Name.) For example, if you want to log in to the Default Organization, whose Display Name is CA, then enter defaultorg, which is the (default) unique ID of this organization. Do not specify CA here.
4. Click Log In.

   The Login page appears.

   Note: This page does *not* show the Forgot Password? link that is available when you log in by using WebFort Password credentials.
5. Specify the user ID in User Name field, enter the corresponding password in the Password field, and click Log In.

   If you are logging in for the first time, you will be prompted to change the password.
6. Specify the New Password, Confirm Password, and then click Log In.

   You are redirected to the login page.
7. Specify the **Password** again and click **Log In**.

   The landing page of the Administration Console appears.

Logging Out of the Administration Console

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

Security Recommendations While Using the Administration Console

When you access Administration Console, ensure that you follow the best practices listed here:

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

Configuring Profiles and Policies

This section walks you through configuring profiles and policies for credentials that are supported by AuthMinder:

Configuring ArcotID PKI Settings

This section walks you through the following procedures:

Configuring ArcotID PKI Credential Profile

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

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

By configuring an ArcotID PKI profile and assigning it to one or more organizations, you can control the characteristics of ArcotID PKIs that are issued to users of those organizations. Use the ArcotID Profiles page for creating an ArcotID PKI credential profile.

To create an ArcotID PKI profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the ArcotID section, click the Issuance link to display the ArcotID Profiles page.
5. Edit the fields in the Profile Configurations section, as required. The following table describes the fields of this section:

Field	Description
Profile Configurations	
Create	If you choose to create a new profile, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Configuration** list.
Copy Configuration	Enable this option if you want to create the profile by copying the configurations from an existing profile. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the profile from which the configurations will be copied.

Field	Description
Key Length (in Bits)	Specify the size of the key (in bits) to be used for encryption. The default value is 1024 bits.
Validity Start Date	Set the date from which the issued ArcotID PKI credential will be valid. The validity can start from either the date when the ArcotID PKI is created or you can specify a specific date.
Validity End Date	Set the date when the ArcotID PKI will expire. You can either specify the duration for the credential's expiration or you can specify the specific date.
Password Strength	
Minimum Characters	Specify the least number of characters that the password can contain. You can set a value between 4 and 64 characters.
Maximum Characters	Specify the most number of characters that the password can contain. You can set a value between 4 and 64 characters.
Minimum Alphabetic Characters	Specify the least number of alphabetic characters (a-z and A-Z) that the password can contain. This value must be lesser than or equal to the value specified in the **Minimum Characters** field.
Minimum Numeric Characters	Specify the least number of numeric characters (0 through 9) that the password can contain.
Minimum Special Characters	Specify the least number of special characters that the password can contain. By default, all the special characters excluding ASCII (0-31) characters are allowed.

1. Expand the **Advanced Configurations** section.
2. In the **Additional Attributes** section, specify any extra information (unsigned attributes) that you pass for the ArcotID PKI credential in the **Name**-**Value** pair format.

   For example, if you want to lock the ArcotID PKI to a specific device, say the end user's system, then you use this section to send this extra information as listed in the following table:

Name	Value
devlock_required	yes
devlock_type	hd

Note: See the *ArcotID Client Reference Guide* for more information about what extra information you can specify here.

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

3. In the **Custom Attributes** section, specify any extra information in the **Name**-**Value** pair format. For example, the organization information that can be used by plug-ins.
4. Set the following in the **User Validations** section:
   - Select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
     - Create credential
     - Re-issue credential
     - Reset credential
     - Reset validity of the credential
   - Select the **User Attribute** option if you want to verify whether the user attribute matches certain values. You can set the value for the following user attributes:
     - Date when the user was created
     - Date when the user details were modified
     - Email address
     - First name
     - Middle name
     - Last name
     - User status
     - Telephone number
     - Unique user identifier

   Note: The User attribute check feature is available *only* if you are performing configurations at the organization-level.
5. In the **Multiple Credential Options** section, enter the description to identify the purpose for which the ArcotID PKI is used in the **Usage Type** field. For example, a user can have a temporary credential to perform a remote login to the network, the usage type for this credential can be *temporary*.
6. The **History Validation** section enables you to enforce users to not reuse the old ArcotID PKI passwords. You can select any of the following options:
   - **Last <N> Passwords**: Select this option, if you want the current ArcotID PKI password to be different from the last *<n>* passwords.

- **Password Created in Last**: Select this option, if you want the current ArcotID PKI password to be different from the passwords that are used in the specified duration.

7. Click **Save** to create or update the ArcotID PKI profile.
8. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring ArcotID PKI Authentication Policy

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

- **User status:** The status of the user, which can be active or inactive.

  Note: If the user status check is enabled, then the authentication for users in inactive state results in failure.

- **Lockout criteria:** The number of failed attempts after which the user's credentials are locked out.
- **Unlocking criteria:** The number of hours after which a locked ArcotID PKI credential can be used to log in again. This feature can drastically reduce the number of requests for resetting the credential.
- **Using expired ArcotID PKI:** The number of days a user is allowed to authenticate successfully with their expired ArcotID PKI credential.
- **Expiry warning settings:** The number of days before the warning is sent to the calling application about the user's impending ArcotID PKI credential expiration.

Note: Exercise caution while using these options.

To configure a global ArcotID PKI authentication policy:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the ArcotID section, click the Authentication link to display the ArcotID Authentication Policy page.
5. Edit the fields in the Policy Configuration section, as required. The following table describes the fields of this section:

Field	Description
Policy Configurations	
Create	If you choose to create a new policy, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new policy in the field that appears.

Field	Description
Update	If you choose to update an existing policy, then select the policy that you want to update from the **Select Configuration** list that appears.
Copy Configuration	Enable this option if you want to create the policy by copying the configurations from an existing policy. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the policy from which the configurations will be copied.
Lockout Credential After	Specify the number of failed attempts after which the user credential will be locked.
Check User Status Before Authentication	Select this option if you want to verify whether the user status is active, before authenticating them.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. Edit the fields in the section, as required. The following table describes the fields of this section:

Field	Description
Advanced Configurations	
Issue Warning	Specify the number of days before the warning is sent to the calling application about the user's impending ArcotID PKI credential expiration.
Allow Successful Authentication	Specify the number of days for which the users can use an expired ArcotID PKI credential to successfully log in.
Enable Automatic Credential Unlock	Select this option if you want a locked credential to be automatically unlocked after the time you specify in the **Unlock After** field. This field is valid only if you specify the corresponding value in the Lockout Credential After field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.
Challenge Validity (in Seconds)	Specify the duration for which the ArcotID PKI challenge has to be valid.
Multiple Credential Options	

Field	Description
Usage Type for Verification	If you want users to authenticate with the particular ArcotID PKI, then enter the name of its usage type in this field. If you do not specify the usage type, then the usage type mentioned in the default ArcotID PKI authentication policy is used.

3. Click **Save** to create or update the ArcotID PKI policy.
4. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring QnA Settings

This section walks you through:

- Configuring QnA Issuance Profile (see page 102)
- Configuring QnA Authentication Policy (see page 105)

Configuring QnA Issuance Profile

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

- **Number of questions:**
  - Minimum number of questions and answers the user must set during issuance.
  - Maximum number of questions and answers the user can set during issuance
- **Validity period:** The period for which a QnA credential is valid.
- **Case-sensitive Answers:** Decides whether the answers entered by the users must be case-sensitive or not.
- **Question Bank:** The users will use these pre-configured questions in the question bank for setting up their QnA credential.

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

To create or update a QnA profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the QnA section, click the Issuance link to display the Questions and Answers Profiles page.
5. Edit the fields in the Profile Configurations section, as required. The following table describes the fields of this section:

Field	Description
Profile Configurations	
Create	If you choose to create a profile, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Configuration** list that appears.
Copy Configuration	Enable this option if you want to create the profile by copying the configurations from an existing profile. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.

Field	Description
Available Configurations	Select the profile from which the configurations will be copied.
Minimum Questions and Answers	Specify the minimum number of questions and answers that have to be set by users. For example, if you set 3 here and 5 in the Maximum Questions and Answers field, then the users will be prompted for *at least* three questions during authentication out of the five they set.
Maximum Questions and Answers	Specify the maximum number of questions and answers that can be set by users.
Answers Case-Sensitive	Specify whether the answers that the users specify must match the case that they used to set the QnA.
Validity Start Date	Set the date from which the issued QnA credential will be valid. The validity can start from either the date when the QnA is created or you can specify a specific date.
Validity End Date	Set the date when the QnA credential will expire. You can either specify the duration for the credential's expiration or you can specify a specific date.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. In the **Custom Attributes** section, specify any extra information in the **Name**-**Value** pair format. For example, the organization information that can be used by plug-ins.
3. Set the following in the **User Validations** section:
   - Select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
     - Create credential
     - Re-issue credential
     - Reset credential
     - Reset validity of the credential
   - Select the **User Attribute** option if you want to verify whether the user attribute matches certain values. You can set the value for the following user attributes:
     - Date when the user was created
     - Date when the user details were modified
     - Email address
     - First name
     - Middle name
     - Last name
     - User status
     - Telephone number
     - Unique user identifier

     Note: The User attribute check feature is available *only* if you are performing configurations at the organization level.
4. Set the following in the Question Bank for QnA Issuance section:
   - In the Question Return Mode, specify how the questions must be selected for the users to set their answers. The supported modes are:
     - Static - A fixed set of questions is selected from the configured set and presented to the users.
     - Random - The questions are selected randomly from the configured set and presented to the users.
   - In the Questions Bank table, enter the questions, which will be configured at the global-level. You can overwrite these questions at the organization-level.
5. In the Multiple Credential Options section, enter the description to identify the purpose for which the QnA is used in the Usage Type field. For example, a user can have a temporary credential to perform a remote login to the network, the usage type for this credential can be temporary.

6. Click Save to create or update the QnA profile.
7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring QnA Authentication Policy

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

- **User status**: The status of the user, which can be active or inactive.

  Note: If the user status check is enabled, then the authentication for users in inactive state results in failure.

- **Number of questions**:
  - AuthMinder must ask the users during authentication process.
  - For which correct answers are required during authentication.
- **Caller Verification**: The answers are verified by a third party and the result is then sent to AuthMinder Server.
- **Lockout criteria**: The number of failed attempts after which the user's credential is locked out.
- **Unlocking criteria:** The number of hours after which a locked QnA credential can be used to log in again.
- **Question Selection Mode**: The questions are selected either randomly or alternately, which means a new set of questions is asked based on the **Change Question Set** option.
- **Change Question Set**: The questions are changed either after every attempt or after successful authentication.

To configure a QnA authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the QnA section, click the Authentication link to display the QnA Authentication Policy page.
5. Edit the fields in the Policy Configuration section, as required. The following table describes the fields of this section:

Field	Description
Policy Configuration	

Field	Description
Create	If you choose to create a new policy, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new policy in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the **Select Configuration** list that appears.
Copy Configuration	Enable this option if you want to create the policy by copying the configurations from an existing policy. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the policy from which the configurations will be copied.
Number of Questions to Challenge	Set the number of questions that users will be prompted to answer during authentication.
Number of Correct Answers Required	Specify the number of correct answers that users must provide to authenticate successfully. For example, if you set 3 here and set 5 in the Number of Questions to Challenge field, then users must answer *at least* three questions correctly out of the five they will be prompted to answer.
Enable Caller Verification	If you enable this option, then during authentication the answers are collected and verified by a Customer Support Representative (CSR) or a similar facility, and the verification result is sent to the AuthMinder Server.
Lockout Credential After	Specify the number of failed attempts after which the user credential will be locked.
Check User Status Before Authentication	Select this option if you want to verify whether the user status is active, before authenticating them.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. Edit the fields in the section, as required. The following table describes the fields of this section:

Field	Description
Advanced Configurations	
Issue Warning	Specify the number of days before the warning is sent to the calling application about the user's impending credential expiration.

Field	Description
Allow Successful Authentication	Specify the number of days for which the users can use an expired credential to successfully log in.
Enable Automatic Credential Unlock	Select this option if you want the locked credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the Lockout Credential After field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.
Question Selection Mode	Specify how the questions are selected for the challenge. The supported values are: ■ **Random** - The questions are selected randomly from the configured set. ■ **Alternate** - A new set of questions is selected from the configured set, which means the questions that were asked in the last authentication prompt are skipped.
Change Question Set	Specify when the AuthMinder Server must select a new set of questions to challenge. The supported options are: ■ **Only on Successful Authentication** - A new set of questions that are based on the Question Selection Mode is selected after the user authenticates successfully. ■ **For Every Attempt** - A new set of questions that are based on the Question Selection Mode is selected after every authentication attempt, irrespective of the authentication result.
Challenge Validity (in Seconds)	Specify the duration for which the QnA challenge has to be valid.
Multiple Credential Options	
Usage Type for Verification	If you want the users to authenticate with the particular QnA credential, then enter the name of its usage type in this field. If you do not specify the usage type, then the usage type mentioned in the default QnA authentication policy is used.

1. Click **Save** to create or update the QnA policy.
2. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring Password Settings

This section walks you through:

- Configuring Password Issuance Profile (see page 108)
- Configuring Password Authentication Policy (see page 113)

Configuring Password Issuance Profile

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

- **Password strength**: The effectiveness of password, which is determined by the length of the password and number of alphabets, numerals, and special characters in it.
- **Validity period**: The period for which the password credential is valid.
- **Auto-generate password**: The password is generated by the AuthMinder Server.
- **Usage count**: Number of times the password can be used.
- **Usage type and password uniqueness**: Based on the usage requirement, a user can have multiple password credentials. For example, a temporary password and a permanent password. These passwords can be same or unique.

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

To create or update a Password profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Password section, click the Issuance link to display the Password Profiles page.
5. Edit the fields in the Profile Configurations section, as required. The following table describes the fields of this section:

Field	Description
Profile Configurations	

Field	Description
Create	If you choose to create a new profile, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Configuration** list.
Copy Configuration	Enable this option if you want to create the profile by copying the configurations from an existing profile. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the profile from which the configurations will be copied.
Validity Start Date	Set the date from when the issued password credential will be valid. The validity can start from either the date when this credential is created or you can specify a custom date.
Validity End Date	Set the date when the password will expire. You can choose any of the following options to set the expiration date: ■ Specify the duration ■ Specify a custom date ■ Choose **Never Expires** option if you want the password to not expire at all.
Password Strength Options	
Minimum Characters	Specify the least number of characters that the password can contain. You can set a value between 4 and 64 characters. The default value is 6.
Maximum Characters	Specify the most number of characters that the password can contain. You can set a value between 4 and 64 characters. The default value is 10.
Minimum Alphabetic Characters	Specify the least number of alphabetic characters (a-z and A-Z) that the password can contain. This value must be lesser than or equal to the value specified in the **Minimum Characters** field.

Field	Description
Minimum Numeric Characters	Specify the least number of numeric characters (0 through 9) that the password can contain. You can set a value between 0 and 32 characters.
Minimum Special Characters	Specify the least number of special characters that the password can contain. By default, all the special characters excluding ASCII (0-31) characters are allowed.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. In the **Custom Attributes** section, specify any extra information in the **Name**-**Value** pair format. For example, the organization information that can be used by plug-ins.
3. Set the following in the **User Validations** section:
   - Select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
     - Create credential
     - Re-issue credential
     - Reset credential
     - Reset validity of the credential
   - Select the **User Attribute** option if you want to verify whether the user attribute matches certain values. You can set the value for the following user attributes:
     - Date when the user was created
     - Date when the user details were modified
     - Email address
     - First name
     - Middle name
     - Last name
     - User status
     - Telephone number
     - Unique user identifier

     Note: The User attribute check feature is available *only* if you are performing configurations at the organization-level.
4. Set the following in the **Additional Password Options** section:
   - Enable **Auto-Generate Password** option if you want the AuthMinder Server to generate the user passwords. This feature can be used in scenarios where a user forgets their password, the Server can auto-generate a new password and the user can use this new password for the next login.
   - In the **Usage Count** option, select **Unlimited** if you want the password to be valid until it expires. If you want to limit the number of times the password has to be used, then enter the number of times in the second option.
5. Set the following in the **Multiple Credential Options** section:
   - Enter the description to identify the purpose for which the password is used in the **Usage Type** field. For example, a user can have a temporary password to perform a remote login to the network, the usage type for this password can be *temporary*.

- Enable **Password Unique Across Usage Types** option if the passwords of different usage types must be unique.

6. The **History Validation** section enables you to enforce the users to not reuse the old passwords. You can select any of the following options:
   - **Last <N> Passwords**: Select this option, if you want the current password to be different from the last *<n>* passwords.
   - **Password Created in Last**: Select this option, if you want the current password to be different from the passwords that are used in the specified duration.
7. Click **Save** to create or update the Password profile.
8. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring Password Authentication Policy

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

- **User status**: The status of the user, which can be active or inactive.

  Note: If the user status check is enabled, then the authentication for users in inactive state results in failure.

- **Lockout criteria**: The number of failed attempts after which the user's credential is locked out.
- **Unlocking criteria:** The number of hours after which a locked user password credential can be used to log in again.
- **Partial password options**: Number of password characters to challenge.

  When AuthMinder Server receives the partial password authentication request, the user will be challenged with the number of characters from their password at various positions. For example, if the password is welcome1 and the **Number of Password Characters to Challenge** field is set to 4. The challenge might look like "Enter the characters at positions 2, 4, and 7". If the user enters ece, then the authentication will be successful.

- **Multi-password options**: Specifies whether the user is allowed to enter any of their passwords or a password with the specific usage type.

To configure a Password authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Password section, click the Authentication link to display the Password Authentication Policy page.
5. Edit the fields in the Policy Configuration section, as required. The following table describes the fields of this section:

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

Field	Description
Copy Configuration	Enable this option if you want to create the policy by copying the configurations from an existing policy. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the policy from which the configurations will be copied.
Lockout Credential After	Specify the number of failed attempts after which the user credential will be locked.
Check User Status Before Authentication	Select this option if you want to verify whether the user is active, before authenticating them.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. Edit the fields in the section, as required. The following table describes the fields of this section:

Field	Description
Additional Password Options	
Issue Warning	Specify the number of days before the warning is sent to the calling application about the user's impending credential expiration.
Allow Successful Authentication	Specify the number of days for which the users can use an expired credential to successfully log in.
Enable Automatic Credential Unlock	Select this option if you want the credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the Lockout Credential After field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.
Challenge Validity (in Seconds)	Specify the duration for which the password challenge has to be valid.
Partial Password Options	
Number of Password Characters to Challenge	Specify the total number of password characters that have to be challenged. The number of random positions challenged by AuthMinder Server is equal to this value.
Alternate Processing Options	

Field	Description
Alternate Processing Options	The AuthMinder Server acts as a proxy and passes the authentication requests to other authentication servers, based on the following conditions: ■ **User Not Found**: If the user trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. ■ **Credential Not Found**: If the credential with which the user is trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. See "Configuring (see page 156)AuthMinder as RADIUS Proxy Server" (see page 156) for more information to enable this feature.
Multiple Credential Options	
Usage Type for Verification	Choose the **Any Usage Type** option if you want to authenticate users with any of their passwords. For example, if the user has two passwords, *welcome123* with usage type as permanent and *hello123* with usage type as temporary, then the user will be authenticated if they provide either of the passwords. If you want the user to authenticate with the particular password, then enter the name of its usage type in the **UsageType** field.

1. Click **Save** to create or update the Password policy.
2. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring OTP Settings

This section walks you through:

- Configuring OTP Issuance Profile (see page 116)
- Configuring OTP Authentication Policy (see page 119)

Configuring OTP Issuance Profile

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

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

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

To create or update an OTP profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the OTP section, click the Issuance link to display the One Time Password Profiles page.
5. Edit the fields in the Profile Configurations section, as required. The following table describes the fields of this section:

Field	Description
Profile Configurations	
Create	If you choose to create a new profile, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Configuration** list that appears.
Copy Configuration	Enable this option if you want to create the profile by copying the configurations from an existing profile. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the profile from which the configurations will be copied.
Type	Specify whether you want to issue numeric or alphanumeric OTPs to users. The default value is Numeric.

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

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. In the **Custom Attributes** section, specify any extra information in the **Name**-**Value** pair format. For example, the organization information that can be used by plug-ins.
3. Set the following in the **User Validations** section:
   - Select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
     - Create credential
     - Re-issue credential
     - Reset credential
     - Reset validity of the credential
   - Select the **User Attribute** option if you want to verify whether the user attribute matches certain values. You can set the value for the following user attributes:
     - Date when the user was created
     - Date when the user details were modified
     - Email address
     - First name
     - Middle name
     - Last name
     - User status
     - Telephone number
     - Unique user identifier

     Note: User attribute check feature is available *only* if you are performing configurations at the organization-level.
4. In the **Multiple Credential Options** section, enter the description to identify the purpose for which the OTP is used in the **Usage Type** field. For example, a user can have a temporary credential to perform a remote login to the network, the usage type for this credential can be *temporary*.
5. Click **Save** to create or update the OTP profile.
6. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring OTP Authentication Policy

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

- **User status**: The status of the user, which can be active or inactive.

  Note: If the user status check is enabled, then the authentication for users in inactive state will result in a failure.

- **Lockout criteria**: The number of failed attempts after which the user's credential will be locked.

To configure an OTP authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the OTP section, click the Authentication link to display the OTP Authentication Policy page.
5. Edit the fields in the Policy Configuration section, as required. The following table describes the fields of this section:

Field	Description
Policy Configurations	
Create	If you choose to create a new policy, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new policy in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the **Select Configuration** list that appears.
Copy Configuration	Enable this option if you want to create the policy by copying the configurations from an existing policy. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the policy from which the configurations will be copied.
Lockout Credential After	Specify the number of failed attempts after which the OTP will be locked.
Check User Status Before Authentication	Select this option if you want to verify whether the user status is active, before authenticating them.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. Edit the fields in the section, as required. The following table describes the fields of this section:

Field	Description
Advanced Configurations	
Issue Warning	Specify the number of days before the warning is sent to the calling application about the user's impending credential expiration.
Allow Successful Authentication	Specify the number of days for which the users can use an expired credential to successfully log in.
Enable Automatic Credential Unlock	Select this option if you want the credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the Lockout Credential After (see page 141) field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.
Alternate Processing Options	
Alternate Processing Options	The AuthMinder Server acts as a proxy and passes the authentication requests to other authentication servers, based on the following conditions: ■ **User Not Found**: If the user trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. ■ **Credential Not Found**: If the credential with which the user is trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. See "Configuring (see page 156)AuthMinder as RADIUS Proxy Server" (see page 156) for more information to enable this feature.
Multiple Credential Options	
Usage Type for Verification	If you want users to authenticate with the particular OTP credential, then enter the name of its usage type in this field. If you do not specify the usage type, then the usage type mentioned in the default OTP authentication policy is used.

1. Click **Save** to create or update the OTP policy.
2. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring OATH OTP Settings

This section walks you through:

- Configuring OATH OTP Issuance Profile (see page 121)
- Configuring OATH OTP Authentication Policy (see page 124)
- Managing OATH OTP Tokens (see page 128)

Configuring OATH OTP Issuance Profile

An OATH OTP profile can be used to specify the following attribute related to an OATH One-Time Password (OATH OTP) credential:

- **Validity period**: The period for which an OATH OTP is valid.

By configuring an OATH OTP profile and assigning it to one or more organizations, you can control the characteristics of OATH OTP credentials that are issued to users of those organizations. Use the OATH OTP Profiles page to create OATH OTP credential profiles.

To create or update an OATH OTP profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the **Services and Server Configurations** tab on the main menu.
3. Ensure that the **WebFort** tab in the submenu is active.
4. Under the **OATH OTP** section, click the **Issuance** link to display the OATH One Time Password Profiles page.
5. Edit the fields in the **Profile Configurations** section, as required. The following table describes the fields of this section:

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

Field	Description
Copy Configuration	Enable this option if you want to create the profile by copying the configurations from an existing profile. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the profile from which the configurations will be copied.
Validity Start Date	Set the date from when the issued OATH OTP credential will be valid. The validity can start from either the date when this credential is created or you can specify a custom date.
Validity End Date	Set the date when the OATH OTP will expire. You can choose any of the following options to set the expiration date: ■ Specify the duration ■ Specify a custom date ■ Choose **Never Expires** option if you want the OATH OTP to not expire at all.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. In the **Custom Attributes** section, specify any extra information in the **Name**-**Value** pair format. For example, the organization information that can be used by plug-ins.
3. Set the following in the **User Validations** section:
   - Select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
     - Create credential
     - Re-issue credential
     - Reset credential
     - Reset validity of the credential
   - Select the **User Attribute** option if you want to verify whether the user attribute matches certain values. You can set the value for the following user attributes:
     - Date when the user was created
     - Date when the user details were modified
     - Email address
     - First name
     - Middle name
     - Last name
     - User status
     - Telephone number
     - Unique user identifier

     Note: User attribute check feature is available *only* if you are performing configurations at the organization-level.
4. In the **Multiple Credential Options** section, enter the description to identify the purpose for which the OATH OTP is used in the **Usage Type** field. For example, a user can have a temporary credential to perform a remote login to the network, the usage type for this credential can be *temporary*.
5. Click **Save** to create or update the OATH OTP profile.
6. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring OATH OTP Authentication Policy

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

- **User status**: The status of the user, which can be active or inactive.

  Note: If the user status check is enabled, then the authentication for users in inactive state results in failure.

- **Lockout criteria**: The number of failed attempts after which the user's credential are locked.
- **Unlocking criteria:** The number of hours after which a locked credential can be used again.

To configure an OATH OTP authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the OATH OTP section, click the Authentication link to display the OATH OTP Authentication Policy page.
5. Edit the fields in the Policy Configuration section, as required. The following table describes the fields of this section:

Field	Description
Policy Configurations	
Create	If you choose to create a new policy, then: ■ Select the Create option. ■ Specify the Configuration Name of the new policy in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the Select Configuration list that appears.
Copy Configuration	Enable this option if you want to create the policy by copying the configurations from an existing policy. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the policy from which the configurations will be copied.

Field	Description
Authentication Look Ahead Count	Enter the number of times the OATH OTP counter on the AuthMinder Server is increased to verify the OATH OTP entered by the user. The OATH OTP entered by the user is compared with all the OATH OTPs that are generated from current count - Authentication Look Back Count to current count + Authentication Look Ahead Count on the server, and if the OATH OTP entered by the user matches, then the user is authenticated. **Note:** If the client and server OATH OTP matches, then that count is set as the current count on the server.
Authentication Look Back Count	Enter the number of times the OATH OTP counter on the AuthMinder Server is decreased to verify the OATH OTP entered by the user. The OATH OTP entered by the user is compared with all the OATH OTPs that are generated from current count - Authentication Look Back Count to current count + Authentication Look Ahead Count on the server, and if the OATH OTP entered by the user matches, then the user is authenticated. **Note:** If the client and server OATH OTP matches, then that count is set as the current count on the server.
Synchronization Look Ahead Count	Enter the number of times the OATH OTP counter on the AuthMinder Server is increased to synchronize with the OATH OTP counter on the client device. To synchronize the client and the server OATH OTPs, the user has to provide two consecutive OATH OTPs and if these OATH OTPs match with the consecutive server OATH OTPs in the lookup range (count - Synchronization Look Back Count to current count + Synchronization Look Ahead Count), then the server counter is synchronized with the count corresponding to the second OATH OTP entered by the user.

Field	Description
Synchronization Look Back Count	Enter the number of times the OATH OTP counter on the AuthMinder Server is decreased to synchronize with the OATH OTP counter on the client device. To synchronize the client and the server OATH OTPs, the user has to provide two consecutive OATH OTPs and if these OATH OTPs match with the consecutive server OATH OTPs in the lookup range (count - Synchronization Look Back Count to current count + Synchronization Look Ahead Count), then the server counter is synchronized with the count corresponding to the second OATH OTP entered by the user.
Lockout Credential After	Specify the number of failed attempts after which the OATH OTP will be locked.
Check User Status Before Authentication	Select this option if you want to verify whether the user status is active, before authenticating them.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. Edit the fields in the section, as required. The following table describes the fields of this section:

Field	Description
Advanced Configurations	
Issue Warning	Specify the number of days before the warning is sent to the calling application about the user's impending credential expiration.
Allow Successful Authentication	Specify the number of days for which the users can use an expired credential to successfully log in.
Enable Automatic Credential Unlock	Select this option if you want the credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the Lockout Credential After field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.
Alternate Processing Options	

Field	Description
Alternate Processing Options	The AuthMinder Server acts as a proxy and passes the authentication requests to other authentication servers, based on the following conditions: ■ **User Not Found**: If the user trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. ■ **Credential Not Found**: If the credential with which the user is trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. See "Configuring (see page 156)AuthMinder as RADIUS Proxy Server" (see page 156) for more information to enable this feature.
Multiple Credential Options	
Usage Type for Verification	If you want the users to authenticate with the particular OATH OTP credential, then enter the name of its usage type in this field. If you do not specify the usage type, then the usage type mentioned in the default OATH OTP authentication policy is used.

1. Click **Save** to create or update the OATH OTP policy.
2. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Managing OATH OTP Tokens

You can use the Administration Console to bulk-upload OATH tokens or to bulk-fetch OATH tokens that are assigned at the global- or organization-level.

This section walks you through:

- Fetching OATH OTP Tokens
- Uploading OATH OTP Tokens

Fetching OATH OTP Tokens

To fetch the OATH OTP tokens that are assigned at the global level:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the OATH OTP section, click the Token Management link to display the OATH OTP Token Management page.
5. Edit the fields in the Fetch Tokens section, as required. The following table describes the fields of this section:

Field	Description
Token Status	Select the status to fetch the tokens. The possible statuses are: ■ **Free**: Indicates that the token is not assigned to a user. ■ **Assigned**: Indicates that the token is assigned to a user. ■ **Abandoned**: Indicates that the user for whom the token was assigned is no longer associated with the token. For example, an employee who has obtained a new token or an employee who has left the organization. Abandoned tokens can be assigned to other users. ■ **Failed**: Indicates the tokens that failed during the upload operation.
Batch ID	The identifier that denotes the batch in which the OATH token is manufactured.

Field	Description
Token ID	Specify the unique identifier of the token. You can also include wild characters such as, * (asterisk), . (period), and \ (backslash) in your search criteria. You can use these characters as explained in the following example. If you have the following tokens in the database: ■ 12 ■ 123 ■ 1234 ■ 123*4 If you enter the token ID as 12*, then all the tokens listed above will be fetched. If you enter the token ID as 12., then the token 123 will be fetched. If you enter 123*4, then the token 123*4 will be fetched.
Fetch Tokens Available at Global Level	Select this option if you want to fetch the tokens that are assigned at the global level.
Fetch Tokens Assigned to Organizations	Select the organizations for which the tokens have been assigned. The tokens that are assigned to the selected organizations will be fetched.

1. Click **Fetch** to fetch the tokens.

Uploading OATH OTP Tokens

To upload OATH tokens to the database:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the OATH OTP section, click the Token Management link to display the OATH OTP Token Management page.
5. Click the Browse button corresponding to the XML File Containing OATH OTP Tokens to upload the XML file that defines the key container for OTPs that have to be issued by the AuthMinder Server.

   Note: AuthMinder provides a sample XML file oath-token-upload.xml to upload OATH tokens to the users. This file creates OATH tokens for predefined users. It is available at the following location:

   On Windows: *<install_location>*\Arcot Systems\samples\xml\webfort

   On UNIX Platforms: *<install_location>*/arcot/samples/xml/webfort
6. Click **Upload** to upload the tokens.

Configuring ArcotID OTP (OATH-Compliant) Settings

This section walks you through:

- Configuring ArcotID OTP (OATH-Compliant) Issuance Profile (see page 131)
- Configuring ArcotID OTP (OATH-Compliant) Authentication Policy (see page 134)

Configuring ArcotID OTP (OATH-Compliant) Issuance Profile

An ArcotID OTP-OATH profile can be used to specify the following attributes related to ArcotID OTPs that are complaint to OATH standards.

- **Length**: The length of the ArcotID OTP.
- **Validity period**: The period for which an ArcotID OTP is valid.

By configuring an ArcotID OTP-OATH profile and assigning it to one or more organizations, you can control the characteristics of ArcotID OTP credentials that are issued to users of those organizations. Use the ArcotOTP Profiles page to create ArcotOTP credential profiles.

To create or update an ArcotID OTP-OATH profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the ArcotOTP-OATH section, click the Issuance link to display the ArcotOTP-OATH Profiles page.
5. Edit the fields in the Profile Configurations section, as required. The following table describes the fields of this section:

Field	Description
Profile Configurations	
Create	If you choose to create a new profile, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Configuration** list that appears.
Copy Configuration	Enable this option if you want to create the profile by copying the configurations from an existing profile. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the profile from which the configurations will be copied.
Token Type	Select the type of ArcotID OTP that must be created for the user. **HOTP** represents counter-based tokens and **TOTP** represents time-based tokens.

Field	Description
Length	Set the length of an ArcotID OTP. The minimum length of the ArcotID OTP can be 6 (which is also the default value) and the maximum length can be up to 8 characters.
Time Step	The time interval, in seconds, during which the OTP generated by the client is the same as the OTP generated by the server. A larger time step allows the two OTPs to match for a longer period. In other words, a larger time step can accommodate a longer delay in receipt of the OTP from the client. You can enter any value from 1 to 300. The default is 30. **Note:** This option is applicable only for TOTP-based ArcotID OTPs.
Logo URL	Enter the URL that contains the logo, which will be displayed on your client device that uses ArcotID OTP for authenticating to AuthMinder-protected applications.
Display Name	Enter the name that is used to display the ArcotID OTP on the client device. You can either enter a fixed string or pass the following user variables as $$(*<variable>*)$$: ■ user name (userName) ■ organization name (orgName) ■ credential custom attributes ■ user custom attributes
Validity Start Date	Set the date from when the issued ArcotID OTP credential will be valid. The validity can start from either the date when this credential is created or you can specify a custom date.
Validity End Date	Set the date when the ArcotID OTP will expire. You can choose any of the following options to set the expiration date: ■ Specify the duration ■ Specify a custom date ■ Choose **Never Expires** option if you want the ArcotID OTP to not expire at all.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. In the **Custom Attributes** section, specify any extra information in the **Name**-**Value** pair format. For example, the organization information that can be used by plug-ins.
3. In the **Custom Card Attributes** section, specify the additional information that you want to add to the ArcotID OTP-OATH card. These custom attributes will be available as part of the card string.
4. Set the following in the **User Validations** section:
   - Select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
     - Create credential
     - Re-issue credential
     - Reset credential
     - Reset validity of the credential
   - Select the **User Attribute** option if you want to verify whether the user attribute matches certain values. You can set the value for the following user attributes:
     - Date when the user was created
     - Date when the user details were modified
     - Email address
     - First name
     - Middle name
     - Last name
     - User status
     - Telephone number
     - Unique user identifier

     Note: User attribute check feature is available *only* if you are performing configurations at the organization-level.
5. In the **Multiple Credential Options** section, enter the description to identify the purpose for which the ArcotID OTP is used in the **Usage Type** field. For example, a user can have a temporary credential to perform a remote login to the network, the usage type for this credential can be *temporary*.
6. Click **Save** to create or update the ArcotID OTP profile.
7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about how to perform this procedure.

Configuring ArcotID OTP (OATH-Compliant) Authentication Policy

An ArcotID OTP-OATH policy can be used to specify the following authentication-related attributes for ArcotID OTPs that are OATH-compliant:

- **User status**: The status of the user, which can be active or inactive.

  Note: If the user status check is enabled, then the authentication for users in inactive state results in failure.

- **Lockout criteria**: The number of failed attempts after which the user's credential is locked.
- **Unlocking criteria:** The number of hours after which a locked credential can be used again.

To configure an ArcotID OTP-OATH authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the ArcotOTP-OATH section, click the Authentication link to display the ArcotOTP-OATH Authentication Policy page.
5. Edit the fields in the Policy Configuration section, as required. The following table describes the fields of this section:

Field	Description
Policy Configurations	
Create	If you choose to create a new policy, then: ■ Select the Create option. ■ Specify the Configuration Name of the new policy in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the Select Configuration list that appears.
Copy Configuration	Enable this option if you want to create the policy by copying the configurations from an existing policy. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the policy from which the configurations will be copied.

Field	Description
Authentication Look Ahead Count	Enter the number of times the ArcotID OTP counter on the AuthMinder Server is increased to verify the ArcotID OTP entered by the user. The ArcotID OTP entered by the user is compared with all the ArcotID OTPs that are generated from current count - Authentication Look Back Count to current count + Authentication Look Ahead Count on the server, and if the ArcotID OTP entered by the user matches, then the user is authenticated. **Note:** If the client and server ArcotID OTP matches, then that count is set as the current count on the server.
Authentication Look Back Count	Enter the number of times the ArcotID OTP counter on the AuthMinder Server is decreased to verify the ArcotID OTP entered by the user. The ArcotID OTP entered by the user is compared with all the ArcotID OTPs that are generated from current count - Authentication Look Back Count to current count + Authentication Look Ahead Count on the server, and if the ArcotID OTP entered by the user matches, then the user is authenticated. **Note:** If the client and server ArcotID OTP matches, then that count is set as the current count on the server.
Synchronization Look Ahead Count	Enter the number of times the ArcotID OTP counter on the AuthMinder Server is increased to synchronize with the ArcotID OTP counter on the client device. To synchronize the client and the server ArcotID OTPs, the user has to provide two consecutive ArcotID OTPs and if these ArcotID OTPs match with the consecutive server ArcotID OTPs in the lookup range (count - Synchronization Look Back Count to current count + Synchronization Look Ahead Count), then the server counter is synchronized with the count corresponding to the second ArcotID OTP entered by the user.

Field	Description
Synchronization Look Back Count	Enter the number of times the ArcotID OTP counter on the AuthMinder Server is decreased to synchronize with the ArcotID OTP counter on the client device. To synchronize the client and the server ArcotID OTPs, the user has to provide two consecutive ArcotID OTPs and if these ArcotID OTPs match with the consecutive server ArcotID OTPs in the lookup range (count - Synchronization Look Back Count to current count + Synchronization Look Ahead Count), then the server counter is synchronized with the count corresponding to the second ArcotID OTP entered by the user.
Lockout Credential After	Specify the number of failed attempts after which the ArcotID OTP will be locked.
Check User Status Before Authentication	Select this option if you want to verify whether the user status is active, before authenticating them.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. Edit the fields in the section, as required. The following table describes the fields of this section:

Field	Description
Advanced Configurations	
Issue Warning	Specify the number of days before the warning is sent to the calling application about the user's impending credential expiration.
Allow Successful Authentication	Specify the number of days for which the users can use an expired credential to successfully log in.
Enable Automatic Credential Unlock	Select this option if you want the credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the Lockout Credential After field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.
Alternate Processing Options	

Field	Description
Alternate Processing Options	The AuthMinder Server acts as a proxy and passes the authentication requests to other authentication servers, based on the following conditions: ■ **User Not Found**: If the user trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. ■ **Credential Not Found**: If the credential with which the user is trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. See "Configuring (see page 156)AuthMinder as RADIUS Proxy Server" (see page 156) for more information to enable this feature.
Multiple Credential Options	
Usage Type for Verification	If you want the users to authenticate with the particular ArcotID OTP credential, then enter the name of its usage type in this field. If you do not specify the usage type, then the usage type mentioned in the default ArcotID OTP authentication policy is used.

1. Click **Save** to create or update the ArcotID OTP policy.
2. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring ArcotID OTP (EMV-Compliant) Settings

This section walks you through:

- Configuring ArcotID OTP (EMV-Compliant) Issuance Profile (see page 138)
- Configuring ArcotID OTP (EMV-Compliant) Authentication Policy (see page 141)

Configuring ArcotID OTP (EMV-Compliant) Issuance Profile

An ArcotID OTP-EMV profile can be used to specify the following attribute related to ArcotID OTPs that are complaint with Europay, MasterCard, and VISA (EMV) protocol.

- **Validity period**: The period for which an ArcotID OTP-EMV is valid.

By configuring an ArcotID OTP-EMV profile and assigning it to one or more organizations, you can control the characteristics of ArcotID OTP-EMV credentials that are issued to users of those organizations. Use the ArcotOTP-EMV Profiles page to create ArcotID OTP-EMV credential profiles.

Note: To configure an ArcotID OTP-EMV profile, you first create account types. See "Configuring the Account Type" in Chapter 3 (see page 43) for more information about the procedurer.

To create or update an ArcotID OTP-EMV profile:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the ArcotOTP-EMV section, click the Issuance link to display the ArcotOTP-EMV Profiles page.
5. Edit the fields in the Profile Configurations section, as required. The following table describes the fields of this section:

Field	Description
Profile Configurations	
Create	If you choose to create a new profile, then: ■ Select the **Create** option. ■ Specify the **Configuration Name** of the new profile in the field that appears.
Update	If you choose to update an existing profile, then select the profile that you want to update from the **Select Configuration** list that appears.
Copy Configuration	Enable this option if you want to create the profile by copying the configurations from an existing profile. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the profile from which the configurations will be copied.
Account Type	Specify the account type that has to used for creating ArcotID OTP-EMV credential.

Field	Description
Attribute For PAN Sequence	Specify the Primary Account Number (PAN) sequence that helps to differentiate two cards with the same PAN. For example, a card that is reissued after the expiry might have the same PAN but a different sequence number. To add PAN sequence, you need to add custom attributes while configuring account types. See "Configuring the Account Type" (see page 43). To assign PAN sequence to a user in the organization, you need to edit the user account to add values for custom attribute. See "Creating Account IDs" (see page 207). This value will be included in the card string. The custom attribute value is not mandatory, if not provided, then 00 is used by default.
Logo URL	Enter the URL that contains the logo, which will be displayed on the client device that uses EMV OTP for authenticating to AuthMinder-protected applications.
Display Name	Enter the name that is used to display the EMV OTP on the client device. You can either enter a fixed string or pass the following user variables as $$(<*variable*>)$$: ■ user name (userName) ■ organization name (orgName) ■ credential custom attributes ■ user custom attributes
Validity Start Date	Set the date from when the issued ArcotID OTP credential will be valid. The validity can start from either the date when this credential is created or you can specify a custom date.
Validity End Date	Set the date when the ArcotID OTP will expire. You can choose any of the following options to set the expiration date: ■ Specify the duration ■ Specify a custom date ■ Choose **Never Expires** option if you want the ArcotID OTP to not expire at all.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. In the **Custom Attributes** section, specify any extra information in the **Name**-**Value** pair format. For example, the organization information that can be used by plug-ins.
3. In the **Custom Card Attributes** section, specify the additional information that you want to add to the ArcotID OTP-EMV card.
4. Set the following in the **User Validations** section:
   - Select the **User Active** option if you want to verify the user status for the following operations involving the current credential:
     - Create credential
     - Re-issue credential
     - Reset credential
     - Reset validity of the credential
   - Select the **User Attribute** option if you want to verify whether the user attribute matches certain values. You can set the value for the following user attributes:
     - Date when the user was created
     - Date when the user details were modified
     - Email address
     - First name
     - Middle name
     - Last name
     - User status
     - Telephone number
     - Unique user identifier

     Note: User attribute check feature is available *only* if you are performing configurations at the organization-level.
5. In the **Multiple Credential Options** section, enter the description to identify the purpose for which the EMV OTP is used in the **Usage Type** field. For example, a user can have a temporary credential to perform a remote login to the network, the usage type for this credential can be *temporary*.
6. Click **Save** to create or update the EMV OTP profile.
7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring ArcotID OTP (EMV-Compliant) Authentication Policy

An ArcotID OTP-EMV policy can be used to specify the following authentication-related attributes for ArcotID OTPs that are EMV-compliant:

- **User status**: The status of the user, which can be active or inactive.

  Note: If the user status check is enabled, then the authentication for users in inactive state results in failure.

- **Lockout criteria**: The number of failed attempts after which the user's credential is locked.
- **Unlocking criteria:** The number of hours after which a locked credential can be used again.

To configure an ArcotID OTP-EMV authentication policy for organizations:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the ArcotOTP-EMV section, click the Authentication link to display the ArcotOTP-EMV Authentication Policy page.
5. Edit the fields in the Policy Configuration section, as required. The following table describes the fields of this section:

Field	Description
Policy Configurations	
Create	If you choose to create a new policy, then: ■ Select the Create option. ■ Specify the Configuration Name of the new policy in the field that appears.
Update	If you choose to update an existing policy, then select the policy that you want to update from the Select Configuration list that appears.
Copy Configuration	Enable this option if you want to create the policy by copying the configurations from an existing policy. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the policy from which the configurations will be copied.

Field	Description
Authentication Look Ahead Count	Enter the number of times the ArcotID OTP-EMV counter on the AuthMinder Server is increased to verify the ArcotID OTP-EMV entered by the user. The ArcotID OTP-EMV entered by the user is compared with all the ArcotID OTPs that are generated from current count - Authentication Look Back Count to current count + Authentication Look Ahead Count on the server, and if the ArcotID OTP-EMV entered by the user matches, then the user is authenticated. **Note:** If the client and server ArcotID OTP-EMV matches, then that count is set as the current count on the server.
Authentication Look Back Count	Enter the number of times the ArcotID OTP-EMV counter on the AuthMinder Server is decreased to verify the ArcotID OTP-EMV entered by the user. The ArcotID OTP-EMV entered by the user is compared with all the ArcotID OTPs that are generated from current count - Authentication Look Back Count to current count + Authentication Look Ahead Count on the server, and if the ArcotID OTP-EMV entered by the user matches, then the user is authenticated. **Note:** If the client and server ArcotID OTP-EMV matches, then that count is set as the current count on the server.
Synchronization Look Ahead Count	Enter the number of times the ArcotID OTP-EMV counter on the AuthMinder Server is increased to synchronize with the ArcotID OTP-EMV counter on the client device. To synchronize the client and the server ArcotID OTPs, the user has to provide two consecutive ArcotID OTPs and if these ArcotID OTPs match with the consecutive server ArcotID OTPs in the lookup range (count - Synchronization Look Back Count to current count + Synchronization Look Ahead Count), then the server counter is synchronized with the count corresponding to the second ArcotID OTP-EMV entered by the user.

Field	Description
Synchronization Look Back Count	Enter the number of times the ArcotID OTP-EMV counter on the AuthMinder Server is decreased to synchronize with the ArcotID OTP-EMV counter on the client device. To synchronize the client and the server ArcotID OTPs, the user has to provide two consecutive ArcotID OTPs and if these ArcotID OTPs match with the consecutive server ArcotID OTPs in the lookup range (count - Synchronization Look Back Count to current count + Synchronization Look Ahead Count), then the server counter is synchronized with the count corresponding to the second ArcotID OTP-EMV entered by the user.
Lockout Credential After	Specify the number of failed attempts after which the ArcotID OTP-EMV will be locked.
Check User Status Before Authentication	Select this option if you want to verify whether the user status is active, before authenticating them.

1. Expand the **Advanced Configurations** section by clicking the **[+]** sign.
2. Edit the fields in the section, as required. The following table describes the fields of this section:

Field	Description
Advanced Configurations	
Issue Warning	Specify the number of days before the warning is sent to the calling application about the user's impending credential expiration.
Allow Successful Authentication	Specify the number of days for which the users can use an expired credential to successfully log in.
Enable Automatic Credential Unlock	Select this option if you want the credential to be automatically unlocked after the time you specify in the following field. This field is valid only if you specify the corresponding value in the Lockout Credential After field.
Unlock After	Specify the number of hours after which a locked credential can be used again for authentication.
Alternate Processing Options	

Field	Description
Alternate Processing Options	The AuthMinder Server acts as a proxy and passes the authentication requests to other authentication servers, based on the following conditions: ■ **User Not Found**: If the user trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. ■ **Credential Not Found**: If the credential with which the user is trying to authenticate is not present in the AuthMinder database, then the request is passed to the other server. See "Configuring (see page 156)AuthMinder as RADIUS Proxy Server" (see page 156) for more information to enable this feature.
Multiple Credential Options	
Usage Type for Verification	If you want the users to authenticate with the particular ArcotID OTP-EMV credential, then enter the name of its usage type in this field. If you do not specify the usage type, then the usage type mentioned in the default ArcotID OTP-EMV authentication policy is used.

1. Click **Save** to create or update the ArcotID OTP-EMV policy.

   Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring Credential Management Keys

Keys are used to protect the shared secret that is used to generate and authenticate credentials, which include ArcotID PKI, OATH OTP, ArcotID OTP-OATH, and ArcotID OTP-EMV. The key that are used to create and manage the ArcotID PKI is called the *Domain Key.* The keys that are used to create and manage other credentials are called *Master Keys.*

When the user tries to authenticate using their credential, AuthMinder first checks whether the right key is used to protect the credential. If the key is valid, then the user will be authenticated on providing the correct credential. Else, the user authentication fails.

By default, a key configuration is created when the AuthMinder Server is started for the first time. You can either use this default configuration or create your own configuration by using the Credential Key Management page. You can create multiple key configurations, but only the configuration that is assigned to the credential type is used for creating credentials and authenticating those configurations. The other active configurations are used for authentication *only*.

This section walks you through:

- Creating Keys (see page 146)
- Updating Key Validity (see page 147)
- Retiring Keys (see page 148)

Creating Keys

To create a key:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Key Management section, click the Credential Key Management link to display the Credential Key Management Configuration page.
5. Click the Create button to display the Setup Key page.
6. Enter the name for the key configuration in the Configuration Name field.
7. Enter the label that is to be used to store the key in the Key Label field.
8. If you want to store the key in the Hardware Security Module (HSM), then select the Key in HSM option.

   Note: You can use the Check button to verify that the key label exists in the HSM. This button is enabled only when you select the Key in HSM check box.
9. Set the expiry date for the key in the Validity End Date field. You can either specify the duration for which the key must be valid or you can specify a specific date.
10. Click Create to generate the key.

Note: After you create a key configuration, assign this configuration to the credential by using the Assign Default Configuration page. See "Configuring (see page 152)AuthMinder for RADIUS" (see page 152) for more information.

Updating Key Validity

Administration Console also enables you to update the key validity period. When the key expires, the credentials issued with that key are no longer valid. You have to create new credentials and issue them to the users. Extending the validity of the key avoids creating the credentials again with the new key and distributing them to the users.

If the key has already expired, you can also extend the validity of the expired key, and therefore continue to use the existing credentials.

Perform the following steps to extend the key validity:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Key Management section, click the Credential Key Management link to display the Credential Key Management Configuration page.
5. You can update an active or expired key.
   - To update an active key:

     In the Active Configurations section, click the <Configuration Name> link of the key, whose validity you want to extend.
   - To update an expired key:

     In the Retired and Expired Configurations section, click the <Configuration Name> link of the expired key, whose validity you want to extend.

     The Credential Key Management Configuration page appears.
6. Choose the Update option.
7. Set the new expiry date for the key in the Validity End Date field. You can either specify the duration for the key expiration or you can specify a specific date.
8. Click **Update** to update the key validity.

Retiring Keys

Retiring or revoking a key means the key will no longer be valid after this operation, and the credentials that are associated with that key will expire.

Perform the following steps to retire or revoke a key:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Key Management section, click the Credential Key Management link to display the Credential Key Management Configuration page.
5. You can retire an active or expired key.
   - To retire an active key:

     In the Active Configurations section, click the <Configuration Name> link of the key, whose validity you want to extend.
   - To retire an expired key:

     In the Retired and Expired Configurations section, click the <Configuration Name> link of the expired key, whose validity you want to extend.

   The Credential Key Management Configuration page appears.
6. Choose the Retire option.
7. Click the Retire button to retire the key.

Configuring SAML Tokens

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

If you want to issue SAML as authentication tokens, then configure the SAML token properties:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.

   Ensure that the WebFort tab in the submenu is active.
3. Under SAML, click the SAML Token Configuration link to display the SAML Token Configuration page.
4. Depending on whether you want to create a SAML configuration or update an existing SAML configuration, select one of the following options:
   - If you want to create a configuration, then enter the configuration name in the Configuration Name field.
   - If you want to update an existing configuration, then select the configuration that you want to update from the Select Configuration list.
5. Select the SAML Signing Key in HSM option if you want to store the keys that are used for signing SAML assertions in Hardware Security Module (HSM). Otherwise, the keys are stored in the database.
6. (Only if SAML Signing Key in HSM is enabled) Click Browse against the SAML Signing Certificate Chain (in PEM Format) field to upload the certificate that is used by the AuthMinder Server to issue the SAML token.
7. Click Browse against the P12 File Containing SAML Signing Key Pair field to upload the PKCS#12 file containing the certificate that is used by the AuthMinder Server to issue the SAML token.
8. Enter the password for the PKCS#12 file in the P12 File Password field.
9. In the Digest Method field, specify the algorithm (such as SHA1, SHA256, SHA384, SHA512, or RIPEMD 160) that is to be used for hashing the SAML tokens.
10. Enter the name of the Issuer who will provide the SAML token generated by AuthMinder.

    For example, if company XYZ is using AuthMinder to generate SAML tokens, then you can enter XYZ in this field.
11. In the Subject Format Specifier (SAML 1.1) field, specify the format of the SAML subject for SAML 1.1.
12. In the Subject Format Specifier (SAML 2.0) field, specify the format of the SAML subject for SAML 2.0.

13. Enable the Single-Use Token option, if you want the SAML token to be used only once for authentication.
14. In the Token Validity (in Seconds) field, enter the duration after which the SAML token cannot be used.
15. If required, set the additional attributes for SAML token generation in the Additional Token Attributes section.

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

    Click Add More if you want to add more audiences.
17. Click Save to save the SAML token configuration.
18. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring ASSP

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

To configure ASSP:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.

   Ensure that the WebFort tab in the submenu is active.
3. Under ASSP, click the ASSP Configuration link to display the ASSP Configuration page.
4. Depending on whether you want to create an ASSP configuration or update an existing ASSP configuration, select one of the following options:
   - If you want to create a configuration, then enter the configuration name in the Configuration Name field.
   - If you want to update an existing configuration, then select the configuration that you want to update from the Select Configuration list.
5. Enter the ArcotID Roaming URL that will be used to download ArcotID PKIs in case of ArcotID PKI Roaming Download.

   In the case of ArcotID PKI authentication, if the user does not have their ArcotID PKI present on their current system, then the ArcotID Roaming URL is used to authenticate to the AuthMinder Server and download the user's ArcotID PKI.
6. From Authentication Mechanism(s) to Enable, select the authentication method that will be used to authenticate the user before signing.

   If you enable ArcotID authentication method, then select QnA because the QnA authentication method is used for roaming download of ArcotID PKI.
7. If you enable Kerberos authentication method in the preceding step, then set the parameters required for Kerberos authentication in Kerberos Configurations section. Perform one of the following steps:
   - Select the Use Windows Logon Credential option, if you want to use the Kerberos token of the AuthMinder Server process.
   - Specify new credentials in the User Name, Password, and Domain Name fields for Kerberos authentication.
8. In the SAML section:
   a. Select the SAML Signing Key in HSM option if you want to store the keys that are used for signing SAML assertions in Hardware Security Module (HSM). Else, the keys will be stored in the database.

b. (Only if SAML Signing Key in HSM is enabled) Click Browse against the SAML Signing Certificate Chain (in PEM Format) field to upload the certificate that is used by the AuthMinder Server to issue the SAML token.

c. Click Browse against the P12 File Containing SAML Signing Key Pair field to upload the PKCS#12 file containing the key and the certificate that is used by the AuthMinder Server to issue the SAML token.

d. Enter the password for the PKCS#12 file in the P12 File Password field.

e. Enter the URL of the AuthMinder Server in the Issuer field.

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

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

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

   Click Add More to add more audiences.

9. Click Save to save the ASSP configuration.

10. Refresh *all* deployed AuthMinder Server instances.

    See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Configuring AuthMinder for RADIUS

This section walks you through:

- Configuring RADIUS Clients (see page 152)
- Configuring (see page 156)AuthMinder as RADIUS Proxy Server (see page 156)

Configuring RADIUS Clients

If configured, AuthMinder can serve as a RADIUS Server to the configured Network Access Server (NAS) or the RADIUS clients.

Adding RADIUS Clients

To configure RADIUS clients for an organization:

1. Ensure that you are logged in with the required permissions and scope.
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the RADIUS section, click the RADIUS Client link to display the corresponding page.
5. Click Add to set up a RADIUS client configuration.
6. Provide the following information in the respective fields:
   - **RADIUS Client IP Address:** The IP Address of the RADIUS client through which users authenticate to AuthMinder Server.
   - **Shared Secret Key:** The secret key that is shared between the RADIUS client and the AuthMinder Server.

     Note: The minimum length of key is *1* and the maximum is *512* characters.
   - **Description**: Enter a string to describe the RADIUS client. The description helps to identify the RADIUS client, if multiple clients are configured.
   - **Authentication Type**: Select the authentication mechanism that will be used for VPN authentication:
     - **RADIUS OTP:** The default authentication mechanism that is used to authenticate RADIUS requests.
     - **In-Band Password:** Use this option in the following scenarios:

       To resolve credential type
       If you want to authenticate users with the credential that is configured using credential type resolution (see "Resolving Credential Types" (see page 158)). By default, password authentication mechanism is used.

       (Optional, applicable for Global Configurations Only) To specify the organization name
       In a RADIUS request, organization information can be sent with a password in the <orgname>\n<password> format. AuthMinder can extract the organization name from a password that is specified in this format. To enable the use of this feature, associate organizations with the RADIUS client as follows:

       a. Use the > button to move the required organizations from the Available Organizations list to the Supported Organizations list.

       b. Specify the Default Organization for the RADIUS client. If organization information is not presented in a RADIUS request, then this default organization is considered in the authentication to resolve user details.
     - **EAP:** This option is not currently supported. Do not select it.

7. In the **RADIUS Retry Handling** section, specify the following:
   - Select the Enable Retry option if you want the RADIUS client to try sending the request to AuthMinder Server if it does not receive any response.
   - In the Retry Window field, enter the duration in seconds within which the client can retry to connect to the AuthMinder Server if it does not receive any response. After this period, the retry is considered invalid. Ensure that the retry window period is greater than the client timeout period.
8. In the Additional RADIUS Response Attributes section, specify the attributes that you want the AuthMinder Server to include in the response sent to the RADIUS client.
   - **Attribute ID**: Enter a unique attribute identifier in this column. For example, 26.
   - **Attribute Value**: Enter the value corresponding to the attribute ID. You can pass static values or variables such as, user attributes or custom attributes, or a combination of static values and variables. For example, for the user JSmith, if the custom user attribute key-value pair is Employee ID=150, then you can include the employee ID in the RADIUS response, as follows:

   JSmith = $$Employee ID$$

   This returns JSmith = 150.
9. Click Add More to add more attributes.
10. In the RADIUS Packet Drop Options section, select the options when the AuthMinder Server must not process RADIUS packets.

    Following are the supported options to drop the RADIUS packets:
    - User not Found
    - Credential not Found
    - Invalid Request
    - Internal Error
11. Click Add to add the new RADIUS client.
12. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about the procedure.

Updating or Deleting RADIUS Clients

If a RADIUS client is configured, then the RADIUS Configuration page displays the configured clients in the **Configured RADIUS Clients** table**,** which helps you update or delete the RADIUS client IP addresses.

Updating RADIUS Clients

To update the RADIUS client:

1. In the Configured RADIUS Clients section, click the IP address of the client you want to update.
2. Update any of the columns for the selected client (see "Configuring RADIUS Clients" (see page 152) for details) and click Update.
3. Refresh *all* deployed AuthMinder Server instances.

   See "Refreshing a Server Instance" (see page 67) for instructions on how to do this.

Deleting RADIUS Clients

To delete a RADIUS client:

1. In the Configured RADIUS Clients section, click the IP address of the client you want to delete.
2. Click Delete.
3. Refresh *all* deployed AuthMinder Server instances.

   See "Refreshing a Server Instance" (see page 67) for instructions about how to perform this procedure.

Configuring AuthMinder as RADIUS Proxy Server

AuthMinder can now be used as a proxy server to pass any password-based authentication requests to other servers that work on RADIUS protocol.

Note: Ensure that the policy that is being used for authentication has either User Not Found or Credential Not Found selected in the Alternate Processing Options section.

To enable AuthMinder Server as a proxy, and add the RADIUS server to which AuthMinder will proxy the requests to:

1. Ensure that you are logged in with the required permissions and scope.
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the RADIUS section, click the RADIUS Proxy link to display the corresponding page.
5. Select the Enable Proxy option to enable AuthMinder Server to pass the RADIUS requests to RADIUS server.
6. Select the Use Global Configuration option if you want to use the configurations available at the global level.

   Note: This option is available *only* if you are performing organization-specific configuration.
7. Enter the details of the RADIUS server that processes the request in the Primary Proxy Server Details section, as follows:
   - **IP Address**: The IP Address of the RADIUS server.
   - **RADIUS Port**: The port number on which the RADIUS server is listening.
   - **Shared Secret Key**: The secret key shared between the RADIUS client and the RADIUS server.

     Note: The minimum length of the key is *1* and the maximum is *512* characters.
   - **Description**: Enter a string to describe the RADIUS server. The description helps to identify the RADIUS server, if multiple servers are configured.
   - **Read Timeout**: Enter the maximum time in milliseconds to wait for a response from the RADIUS server.
   - **Retry Count**: Enter the number of times the AuthMinder Server should attempt to send the request to RADIUS server, if it does not receive the response.
8. In the Additional RADIUS Response Attributes section, specify the attributes that you want the AuthMinder Server to include in the request that it sends to the RADIUS server.

   Attribute ID: Enter a unique attribute identifier in this column. For example, 26.

   Attribute Value: Enter the value corresponding to the attribute ID. For example, value corresponding to attribute identifier 26.

9. Click Add More to add more attributes.
10. If you want to configure an additional RADIUS server, then provide the details of that server in the Backup Proxy Server Details section.
11. Click Update to save the configurations made.

Configuring Plug-Ins

A plug-in registered by a Master Administrator (see "Registering and Updating Plug-Ins" (see page 84)) must be configured (*only* by a GA) to work with the AuthMinder Server.

To configure a registered plug-in as a GA:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.

   Ensure that the WebFort tab in the submenu is active.
3. Under Extensible Configurations, click the Plug-In Configurations link to display the Configure Plug-in page.
4. From the Name drop-down list, select the plug-in that you want to configure.

   The configuration information displayed on this screen is rendered by the Handler file that the MA has uploaded while registering the plug-in.
5. Enter the plug-in configuration details.
6. Select the events that you want the plug-in to support.
7. Click Submit to configure the plug-in and save the changes.
8. Refresh *all* deployed AuthMinder Server instances.

   See "Refreshing a Server Instance" (see page 67) for instructions about how to perform this procedure.

Resolving Credential Types

The authentication requests that are presented to the AuthMinder Server must specify the type of credential that has to be used to process the request. In case of RADIUS and ASSP authentication requests, the input requests do not have the provision to specify the credential type, and therefore RADIUS uses One-Time Password and ASSP uses password as a default credential for authentication.

To support any password-based authentication mechanisms for RADIUS and ASSP, or to use the verifyPlain authentication function, you must create the *Credential Type Resolution* configuration. You can map the input request to any of the following password type credentials that AuthMinder supports:

- Password
- One-Time Password
- OATH OTP
- ArcotID OTP-OATH
- ArcotID OTP-EMV
- RADIUS OTP
- LDAP Password
- Native Token

To resolve the credential type:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Miscellaneous Configurations section, click the Credential Type Resolution link to display the corresponding page.
5. Edit the fields in the section, as required. The following table describes the fields of this section:

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

Field	Description
Copy Configuration	Enable this option if you want to create or update the configuration by copying the existing configurations. **Note:** You can also copy from configurations that belong to other organizations that you have scope on.
Available Configurations	Select the configuration from which the settings will be copied.
Resolve Plain to	Choose the authentication mechanism that you want to map the incoming password type credential to.
User Custom Attribute for Credential Type	The custom attribute of the user that defines the credential type to be used to authenticate the user. **Note:** The user attributes that you provide here must match the attributes that you have specified for the user during user creation. FirstName, LastName, and TelNumber are examples of the user attribute that you can use.

1. Click **Save** to create or update the credential type resolution configuration.

Note: After you create the configuration, you must apply it using the Assign Default Configurations page, as discussed in "Assigning Default Configurations" (see page 160).

Assigning Default Configurations

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

This section explains how to apply configurations at the global level. For assigning the configurations to the organization, see "Managing Organization-Specific (see page 191)AuthMinder Configurations" (see page 191).

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

To assign default configurations as global:

1. Ensure that you are logged in as a Global Administrator (GA).
2. Activate the Services and Server Configurations tab on the main menu.
3. Ensure that the WebFort tab in the submenu is active.
4. Under the Assign Configurations section, click the Assign Default Configurations link to display the corresponding page.
5. Select the configurations that you want to use from the corresponding drop-down lists.

   You can assign the following using this page:

   - Profiles and policies for all supported credentials
   - Domain key configuration for ArcotID
   - Master key configuration for OATH-OTP, ArcotID OTP-OATH, and ArcotID OTP-EMV
   - SAML token configuration
   - ASSP configuration
   - The configuration to resolve authentication requests, if the credential type is unknown
   - The configuration to identify the credential type that has to be used to process ASSP authentication requests
   - The configuration to identify the credential type that has to be used to process RADIUS authentication requests
6. Click **Save** to assign the default profiles and policies.

   Note: These configurations can be overridden at organization-level.

7. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about how to perform this procedure.

Chapter 6: Managing Organizations

Note: Most of the tasks in this chapter can be performed by a Global Administrator (GA) or an Organization Administrator (OA), if they have the required scope to the organization.

In the Administration Console, an *organization* can either map to a complete enterprise (or a company) or a specific division, department, or other entities within the enterprise. The organization structure that is provided by the Administration Console is flat. In other words, organizational hierarchy (in the form of parent and child organizations) is *not* supported, and all organizations are created at the same level as the Default Organization. (See "Setting the Default Organization" (see page 42) for more information about Default Organization.)

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

Creating and Activating Organizations

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

Note: In the case of a small deployment, you can rename the Default Organization, instead of creating an organization.

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

- Creating Organizations in AuthMinder Repository (see page 164)
- Creating Organization in LDAP Repository (see page 168)

Permissions Required

To be able to create and activate an organization, ensure that you have the appropriate permissions and scope to do so. MA and GAs can create and activate all organizations.

Creating Organizations in AuthMinder Repository

To create an organization in the AuthMinder repository:

1. Ensure that you are logged in with the required permissions and scope to create the organization.
2. Activate the Organizations tab.
3. Under the Manage Organizations section, click the Create Organization link to display the Create Organization page.
4. Enter the details of the organization, as discussed in the following table:

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

Field	Description
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators belonging to this organization. Administration Console supports the following three types of authentication mechanisms: ■ **Basic User Password** This is the built-in authentication mechanism that is provided by Administration Console. If you select this option, then administrators log in to the Console by specifying their ID and password. ■ **WebFort Password** This is the WebFort password authentication method. If you select this option, then the administrator credentials are issued and authenticated by AuthMinder Server. To use this mechanism, the Administration Console must be connected to AuthMinder Server. You can set the connection details in the WebFort Connectivity page, see "Configuring (see page 64)AuthMinder Connectivity" (see page 64) for more information.
Key Label Configuration AuthMinder enables you to use hardware- or software-based encryption of your sensitive data. You can choose the encryption mode by using the arcotcommon.ini configuration file. For more information, see the appendix, "Configuration Files and Options" in the *CA AuthMinder Installation and Deployment Guide*. Irrespective of hardware or software encryption, all Arcot products use the Global Key Label or the organization-specific key label for encrypting user and organization data. If you are using hardware encryption, then this label serves only as a reference (or pointer) to the actual 3DES key stored in the HSM device, and therefore must match the HSM key label. However, in the case of software-based encryption, this label acts as the key.	
Use Global Key	This option is selected by default. Deselect this option if you want to override the Global Key Label you specified in the bootstrap process and specify a new label for software-based encryption or hardware-based encryption.
Key Label	If you deselected the Use Global Key option, then specify the new key label that you want to use for the organization.
Storage Type	Indicates whether the encryption key is stored in the database (Software) or the HSM (Hardware).
Localization Configuration	
Use Global Configuration	Select this option to use the localization parameters that are configured at the global level.

Field	Description
Date Time Format	If you deselected the Use Global Configuration option, then specify the Date Time format that you want to use.
Preferred Locale	If you deselected the Use Global Configuration option, then select a preferred locale.
User Data Location	
Repository Type	Select Arcot Database. By specifying this option, the user and administrator details for the new organization will be stored in the RDBMS repository supported by AuthMinder.
Custom Attributes Use this section to provide additional information specific to the organization you are creating.	
Name	Name of the custom attribute.
Value	Value of the custom attribute.

1. Click Next.

   The Select Attribute(s) for Encryption page appears.

2. In the Attribute(s) for Encryption section, perform one of the following steps:

   - Select Use Global Configuration if you want to use the global settings for your attribute encryption set configuration.
   - Select the attributes that you want to encrypt from the Available Attributes for Encryption list and add them to the Attributes Selected for Encryption list.

     Click the > button to move selected attributes to the desired list. You can also click the >> button to move all attributes to the required lists.

     Note: Hold the Ctrl key to select more than one attribute at a time.

3. Click Next.

   The Add Administrators page appears.

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

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

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

   Note: If some administrators have scope to manage all organizations in the system, then the corresponding entries for those administrators do not appear in this list.

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

4. Click the Next to proceed.

   The Configure Account Type page appears only if the logged-in administrator has account types to manage. If the logged-in administrator does not have any account types to manage, then the Configure Email/Telephone Type page appears.

   a. In the Assign Account Types section, select account types from the Available list and click the > button to move them to the Selected list.

      The Configure Account Custom Attributes page appears.

   b. Specify one or more attributes for the account.

5. Click Next to proceed.

   The Configure Email/Telephone Type page appears.

6. Specify the mandatory and optional email address and telephone number types the user must provide.

7. Click Skip to use the email and telephone types that are configured at the system level and move to the Activate Organization page, or click Save to save your changes.

8. In the Activate Organization page, click Enable to activate the new organization.

   A message appears.

9. Click OK to complete the process.

   Note: Even if you do not choose to activate the organization, the organization is created in Initial state. You can activate the organization later. For instructions, see "Activating Organizations in Initial State" (see page 188).

10. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about how to perform this procedure.

Information! If you have configured the attribute encryption set, account types, and email and telephone types while creating the organization, ensure that you refresh *both* the system configuration and organization cache. If you do not refresh the organization-level cache, the system gets into an unrecoverable state.

Creating Organization in LDAP Repository

To support LDAP user directories, create an organization in AuthMinder repository and then map the AuthMinder attributes with the LDAP attributes.

Perform the following steps:

1. Ensure that you are logged in with the required permissions and scope to create the organization.
2. Activate the Organizations tab.
3. Under the Manage Organizations section, click the Create Organization link to display the Create Organization page.
4. Enter the details of the organization, as discussed in the following table:

Field	Description
Organization Information	
Organization Name	Enter the unique ID for the organization that you want to create. **Note:** You can use the Administration Console to log in to this organization, by specifying this value, *not* the Display Name of the organization.
Display Name	Enter a unique descriptive name for the organization. **Note:** This name appears on all other Administration Console pages and reports.

Field	Description
Description	Provide a description for the administrators who will manage this organization. **Note:** You can provide additional details for later reference for the organization by using this field.
Administrator Authentication Mechanism	Select the mechanism that will be used to authenticate administrators belonging to this organization. Administration Console supports the following three types of authentication mechanisms: ■ **Basic User Password** This is the in-built authentication mechanism that is provided by Administration Console. If you select this option, then administrators log in to the Console by specifying their ID and plain text password. ■ **LDAP User Password** The authentication policy is defined in the LDAP directory service. If you select this option, then administrators must use the credentials that are stored in LDAP to log in to the Console. ■ **WebFort Password** This is the WebFort password authentication method. If you select this option, then the administrator credentials are issued and authenticated by AuthMinder Server.
Key Label Configuration	
Use Global Key	This option is selected by default. Deselect this option if you want to override the Global Key Label you specified in the bootstrap process and specify a new label for software-based encryption.
Key Label	If you deselected the Use Global Key option, then specify the new key label that you want to use for the organization.
Storage Type	Indicates whether the encryption key is stored in the database (Software) or the HSM (Hardware).
Localization Configuration	
Use Global Configuration	Select this option to use the localization parameters that are configured at the global level.
Date Time Format	If you deselected the Use Global Configuration option, then specify the Date Time format that you want to use.
Preferred Locale	If you deselected the Use Global Configuration option, then select a preferred locale.
User Data Location	

Field	Description
Repository Type	Select Enterprise LDAP. By specifying this option, the user and administrator details for the new organization will be stored in the AuthMinder repository.
Custom Attributes	
Name	Name of the custom attribute.
Value	Value of the custom attribute.

1. Click Next.

   The Create Organization page to collect the LDAP repository details appears.

2. Enter the details, described in the following table, to connect to the LDAP repository.

Field	Description
Host Name	Enter the host name of the system where the LDAP repository is available.
Port Number	Enter the port number on which the LDAP repository service is listening.
Schema Name	Specify the LDAP schema used by the LDAP repository. This schema specifies the types of objects that an LDAP repository can contain, and specifies the mandatory and optional attributes of each object type. Typically, the schema name for Active Directory is user and for SunOne Directory it is user and inetorgperson.
Base Distinguished Name	Enter the base Distinguished Name of the LDAP repository. This value indicates the starting node in the LDAP hierarchy to search in the LDAP repository. For example, to search or retrieve a user with a DN of cn=rob laurie, ou=sunnyvale, o=arcot, c=us, you must specify the base DN as the following: ■ ou=sunnyvale, o=arcot, c=us **Note:** Typically, this field is case-sensitive and searches all sub-nodes under the provided base DN.

Field	Description
Redirect Schema Name	Specify the name of the schema that provides the definition of the "*member*" attribute. This is an optional field. You can search for users in the LDAP repository using the Base DN defined for an organization. But this search only returns users belonging to the specific Organization Unit (OU). An LDAP administrator might want to create a group of users belonging to different Organization Units for controlling access to an entire group, and might want to search for users from different groups. When the administrator creates groups, user node DNs are stored in a "member" attribute within the group node. By default, UDS does not allow search and DN resolution based on attribute values. Redirection enables you to search for users belonging to different groups within LDAP, based on specific attribute values for a particular node. Typically, the redirect schema name for Active Directory is group and for SunOne directory it is groupofuniquenames.
Connection Type	Select the type of connection that you want to use between the Administration Console and the LDAP repository. Supported types are: ■ TCP ■ One-way SSL ■ Two-way SSL
Login Name	Enter the complete distinguished name of the LDAP repository user who has the permission to log in to the repository server and manage the Base Distinguished Name. For example, uid=gt,dc=arcot,dc=com
Login Password	Enter the password of the user provided in the Login Name.
Server Trusted Root Certificate	Enter the path for the trusted root certificate who issued the SSL certificate to the LDAP server, by using the Browse button. This field is applicable if you selected One-way SSL or Two-way SSL in the Connection Type field.
Client Key Store Path	Enter the path for the key store that contains the client certificate and the corresponding key by using the Browse button. This field is applicable only if you selected Two-way SSL in the Connection Type field. **Note:** Upload either PKCS#12 or JKS key store type.

Field	Description
Client Key Store Password	Enter the password for the client key store, if the required SSL option is selected. This field is applicable *only* if you selected **Two-way SSL** in the **Connection Type** field.

1. Click Next to proceed.

   The page to map the repository attributes appears.

2. On this page:

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

      Important! Mapping of the UserName attribute is compulsory. If you are using Active Directory, then map UserName to sAMAccountName. If you are using SunOne Directory, then map UserName to uid.
      For Active Directory, you must map STATUS to userAccountControl.

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

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

      The attributes that you have mapped are moved to the Mapped Attributes list.

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

   c. If you specified the Redirect Schema Name in the previous page, select the search attribute from the Redirect Search Attribute list.

      Typically, the attribute for Active Directory is member and for SunOne directory, it is uniquemember.

3. Click Next to proceed.

   The Select Attribute(s) for Encryption page appears.

4. In the Attribute(s) for Encryption section, perform one of the following:

   - Select Use Global Configuration if you want to use the global settings for your attribute encryption set configuration.
   - Select the attributes that you want to encrypt from the Available Attributes for encryption list to add them to the Attributes Selected for encryption list.

     Click the > button to move selected attributes to the desired list. You can also click the >> button to move all attributes to the desired lists.

     Note: Hold the Ctrl key to select more than one attribute at a time.

5. Click Next.

   The Add Administrators page appears.

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

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

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

Note: If some administrators have scope to manage all organizations in the system, then the corresponding entries for those administrators are not displayed in this list.

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

6. Click Next to proceed.

   The Configure Account Type page appears only if the logged-in administrator has account types to manage. If the logged-in administrator does not have any account types to manage, then the Configure Email/Telephone Type page appears.

   a. In the Assign Account Types section, select account types from the Available list and click the > button to move them to the Selected list.

      The Configure Account Custom Attributes page appears.

   b. Specify one or more attributes for the account.

7. Click Next to proceed.

   The Activate Organization page appears.

8. Click Enable to activate the new organization.

   A warning message appears.

9. Click OK to complete the process.

10. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about how to perform this procedure.

Information! If you have configured the attribute encryption set, account types, and email and telephone types while creating the organization, ensure that you refresh *both* the system configuration and organization cache. If you do not refresh the organization-level cache, the system gets into an unrecoverable state.

Searching for Organizations

Permissions Required

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

Searching Organization

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

1. Ensure that you are logged in with the required permissions and scope to create the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the partial or complete information of the required organization. You can select the following options to broaden your search:

   Note: In the **Organization** field, enter the partial or complete display name of the organization and *not* the actual organization name.

   - **Initial** (to display the organizations that have been created but have not been activated yet.)
   - **Active** (to display the organizations that have been created and have been activated.)
   - **Inactive** (to display the organizations that have been disabled.)
   - **Deleted** (to display the organizations that have been deleted.)
5. Click **Search** to display the page, with all the matches for the specified criteria.

Updating Organization Information

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

- **Organization information** that includes organization display name, description, status, email types, telephone types, encryption type, account types and its custom attributes, and the administrators that manage the organization ("Updating the Basic Organization Information" (see page 177)).
- **AuthMinder-specific configurations** for the organizations that include credential profiles, authentication policies, extensible configurations, and the assigned default configurations ("Updating (see page 179)AuthMinder-Specific Configurations" (see page 179)).

Permissions Required

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

Updating the Basic Organization Information

To update the basic organization information:

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

   A list of organizations matching the search criteria appears.
5. Under the Organization column, click the <ORGANIZATION_NAME> link for the required organization.

   The Organization Information page appears.
6. In the Organization Details section, edit the required fields (Display Name and Description).

   You can change the Administrator Authentication Mechanism if there are no administrators in the organization.
7. In the Localization Configuration section, perform one of the following steps:
   - Select the Use Global Configuration.
   - Edit the Date Time Format and Preferred Locale.
8. In the Custom Attributes section, edit the Name and Value fields, if required.
9. Click Next to proceed with additional configurations:
   - If the organization was created in the AuthMinder Repository and if the administrators in the organization have scope to manage organizations in the system, then do the following:
     a. On the Select Attribute(s) for Encryption page, Use Global Configuration if you want to use the global settings for your attribute encryption set configuration or select the attributes that you want to encrypt from the Available Attributes for encryption list and add them to the Attributes Selected for encryption list, and click Next.
     You cannot update the attributes if users have already been created in the organization.

     b. On the Update Administrators page, update the administrators who will manage the organization and click Next.

     c. On the Configure Account Type page, configure the account types by moving them from the Available list to the Selected list and click Next. This page is displayed only if there are account types applicable to the organization that you are updating.

d. You cannot clear global account types.

e. On the Configure Account Custom Attributes page, configure one or more custom attributes for the accounts in your organization and click Next. This page is displayed only if there are account types applicable to the organization that you are updating.

f. On the Configure Email/Telephone Type page, configure the mandatory and optional Email address and Telephone Type for the users, and click Save to complete the process.

- If the organization was created in the LDAP repository, then the Edit Organization page appears:

  a. Use the information in the table in the "Creating Organization in LDAP Repository (see page 168)" section to update the fields, as required, and click Next to display the page to edit the Repository Attribute Mappings.

  b. You cannot update the user name mapping. You can map unmapped attributes, if any, in this flow. Click Next to display the Select Attribute(s) for Encryption page.

  c. On the Select Attribute(s) for Encryption page, Use Global Configuration if you want to use the global settings for your attribute encryption set configuration or select the attributes that you want to encrypt from the Available Attributes for encryption list to add them to the Chosen Attributes for encryption list, and click Next.

  Note: You cannot update the attributes if users have already been created in the organization. In the case of LDAP, even a simple search operation for users in the LDAP repository registers the users in the database. So, you cannot update the attributes if you have searched for users in the LDAP repository.

  d. On the Update Administrators page, update the administrators who will manage the organization and click Next.

  e. On the Configure Account Type page, configure the account types by moving them from the Available list to the Selected list and click Next.

  f. You cannot clear global account types.

  g. On the Configure Account Custom Attributes page, configure one or more custom attributes for the accounts in your organization and click Update to save your changes and complete the process.

10. Refresh *all* deployed AuthMinder Server instances. See "Refreshing a Server Instance" (see page 67) for instructions about how to perform this procedure.

Updating AuthMinder-Specific Configurations

To update the AuthMinder configurations of an organization:

1. Ensure that you are logged in with the required permissions and scope to create the organization.
2. Activate the Organizations tab.
3. Under the Manage Organizations section, click the Search Organization link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search for and click the Search button to display a list of organizations matching the search criteria.
5. Under the Organization column, click the <ORGANIZATION_NAME> link for the required organization to display the Organization Information page.
6. Activate the WebFort Configuration tab to display the links for AuthMinder configurations in the task pane.

   See "Managing Organization-Specific (see page 191)AuthMinder Configurations" (see page 191) for detailed information about these configurations.

Uploading Users and User Accounts in Bulk

AuthMinder now allows you to upload users and user accounts in bulk through the Administration Console. You need a comma-separated value (CSV) input file to upload information for multiple users and user accounts.

Uploading Users in Bulk

The first line in the CSV input file to upload users must be as follows:
`#UserID,fName,lName,status,EmailAddr,telephoneNumber,INFOLIST,mName#`

Caution: The preceding first (template) line is *always* required. If you do not specify this line, then the bulk user upload operation will fail.

Note the following when you create the CSV input file to upload users:

- The CSV file should have one header starting and ending with # and all the other field names should be provided between these # symbols.
- Only the UserID entry is mandatory. The other entries are optional. If a particular user already exists, then their record gets updated. If a user does not exist, a new user is created.
- You can provide up to five email addresses and five telephone numbers. In this case, specify the header, as follows:

`#UserID,fName,lName,status,EmailAddr,EMAIL.2,EMAIL.3,EMAIL.4,EMAIL.5,telephoneNumber,PHONE.2,PHONE.3,PHONE.4,PHONE.5,INFOLIST,mName#`

The entries in the file are described in the following table:

Entry	Description
UserID	The unique ID of the user.
fName	The first name of the user.
mName	The middle name of the user.
lName	The last name of the user.
status	The status of the user. Possible values are: ■ INITIAL ■ ACTIVE
pam	The personal authentication message.
pamURL	The URL where the user's personal authentication message image is available.
EmailAddr	The contact email ID of the user.

Entry	Description
telephoneNumber	The complete phone number of the user with the international code. For example, US phone numbers should start with 1.
PHONE.2	The optional phone number of the user.

A sample file, for example, can contain:

```
#UserID,fName,lName,status,EmailAddr,telephoneNumber,PHONE.2,INFOLIST#
mparker,martin,parker,ACTIVE,mparker@ca.com,12345,9999,age=29;favsport=cricket
jhume,john,hume,ACTIVE,jhume@ca.com,3939292,203939393,age=32;favbook=fiction
fantony,francis,antony,ACTIVE,fantony@ca.com,130203,29888,age=25;favfood=pizza
```

Uploading User Accounts in Bulk

The first line in the CSV input file to upload user accounts must be as follows:

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,acco
untIDAttribute3,customAttr1,customAttr2,customAttr3,customAttr4,customAttr5,custo
mAttr6,customAttr7,customAttr8,customAttr9,customAttr10#
```

Important! The preceding first (template) line is *always* required. If you do not specify this line, then the bulk user account upload operation fails.

Note the following when you create the csv input file to upload user accounts:

- Only the UserID, accountType, and accountID entries are mandatory. The other entries are optional.
- You must have created the user in the system.
- You must have created the account type and assigned it to the organization.
- You must have created custom attributes for the account type. This is optional and needs to be done only if you want to add custom attributes to the account type for a particular user.
- You can provide up to three account ID attributes for an account type.
- You can provide up to 10 custom attributes for an account type.

The entries in the file are described in the following table:

Entry	Description
UserID	The unique ID of the user.
accountType	The account type.
accountID	The alternate ID of the user.

Entry	Description
status	The status of the account ID. Possible values are: ■ [0-9]: INITIAL ■ [10-19]: ACTIVE ■ [20-29]: INACTIVE
accountIDAttribute1	Attribute of the accountID. *Only* three account ID attributes are supported.
customAttr1	Custom attribute for the user.

A sample file, for example, can contain:

```
#UserID,accountType,accountID,status,accountIDAttribute1,accountIDAttribute2,acco
untIDAttribute3,customAttr1,customAttr2#
prush,ONLINE_BANKING,OB_ID1,10,login,password,image,chicago,music
jhume,SAVINGS,SA_ID1,10,interest,deposit,check,florida,soccer
```

To create multiple users and user accounts in the AuthMinder database:

1. Ensure that you are logged in with the required permissions and scope to update the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search for and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select the organization to which you want to upload users and user accounts in bulk.
6. Under the **Basic Organization Information** section, click the **Bulk Upload** link to display the Bulk Data Upload page.
7. In the **Bulk Upload** section:
   a. Select **Upload User Accounts** or **Upload Users** from the **Bulk Upload Operation** drop-down list.
   b. Click **Browse** to navigate to the required csv file containing the user account or user entries.
   c. Provide a **Description** for the operation.
8. Click **Upload** to upload user accounts or users in bulk.

   After the operation completes, you will see a Request ID in the message.

   Important! Note down the Request ID. You use it to view the status of the bulk data upload operation. Typically, bulk upload operations are not triggered immediately and may take up to 10 minutes to start. The RequestID for each operation is displayed as a link. You can click the link to view the status result page.

Viewing the Status of the Bulk Data Upload Request

To view the status of the bulk data upload request:

1. Ensure that you are logged in with the required permissions and scope to perform this operation.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select the organization for which you want to view the status of the bulk upload request.
6. Under the **Basic Organization Information** section, click the **View Bulk Requests** link to display the Search Bulk Requests page.
7. In the Search Bulk Requests page:
   a. Enter the Request ID that you noted down earlier (Step 11 in "Uploading Users and User Accounts in Bulk" (see page 180)).

      or

   b. Select a **Status** based on which you want to view the bulk request.

      or

   c. Select an **Operation**, depending on whether you want to view **Upload Users** or **Upload User Accounts** requests.
8. Click **Search** to display the search results.
9. Click the **Request ID** link to get more information about the bulk request.
10. Click the **No. of failed operations** link to view the reason why the operation failed.

In the case of failed operations for a request, the **Export Failures** button is enabled. You can click **Export Failures** to export all the failed operations to a csv file. You can then correct the errors in the exported file, and resubmit the file for bulk upload.

Refreshing Organization Cache

Organization configurations that do not refer to the global configuration, such as attribute encryption set, localization configuration, and email and telephone types are cached at the organization level. When you make changes to these configurations at the organization level, refresh the organization cache for the changes to take effect.

Permissions Required

The MA can refresh the cache of all organizations. The GA and OA can refresh the cache of all organizations within their scope.

Refreshing Organization Cache

To refresh the organization cache:

1. Ensure that you are logged in with the required permissions and scope to refresh the organization cache.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search for and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select the organizations whose cache you want to refresh.
6. Click **Refresh Cache**.
7. Click **OK** in the dialog to confirm your cache refresh request.

A message with a Request ID for the current cache refresh request is displayed. You can check the status of your cache refresh request by clicking the **Check Cache Refresh Status** link and selecting this **Request ID**.

Note: Refreshing the cache of one organization does not affect the response time of transactions going on at that time for other organizations.

Deactivating Organizations

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

Permission Required

To be able to disable an organization, ensure that you have the appropriate permissions and scope to do so. The MA can disable all organizations. GAs and OAs can disable all organizations in their scope.

Deactivating Organizations

To deactivate one or more organizations:

1. Ensure that you are logged in with the required permissions and scope to deactivate the organization.
2. Activate the Organizations tab.
3. Under the Manage Organizations section, click the Search Organization link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search for and click Search.

   A list of organizations matching the search criteria appears.
5. Select one or more organizations that you want to deactivate.
6. Click Deactivate to disable the selected organizations.

   A message box asking you to confirm that you want to deactivate the organization appears.
7. Click OK to confirm the deactivation.

Activating Organizations

You may need to activate a deactivated organization. In this case, select the **Inactive** option while specifying the search criteria on the Search Organization page.

Permission Required

To be able to enable an organization, ensure that you have the appropriate permissions and scope to do so. The MA can enable all organizations. GAs and OAs can enable all organizations in their scope.

Activating Organizations

To activate a deactivated organization:

1. Ensure that you are logged in with the required permissions and scope to activate the organization.
2. Activate the **Organizations** tab.
3. Under the **Manage Organizations** section, click the **Search Organization** link to display the Search Organization page.
4. Enter the complete or partial information of the organization you want to search for and click **Search**.

   A list of organizations matching the search criteria appears.
5. Select one or more organizations that you want to enable again.
6. Click **Activate** to activate the selected organizations.

   A message asking you to confirm activation of the organization appears.
7. Click **OK** to confirm the activation.

Activating Organizations in Initial State

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

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

Permissions Required

To be able to activate an organization that is in the Initial state, ensure that you have the appropriate permissions and scope. The MA can activate all organizations. GAs and OAs can activate all organizations in their scope.

Activating Organizations in Initial State

To activate an organization that is in the **Initial** state:

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

Deleting Organizations

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

Permissions Required

To be able to delete an organization, ensure that you have the appropriate permissions and scope to do so. The MA can delete all organizations. GAs and OAs can delete all organizations in their scope.

Deleting Organizations

To delete an organization:

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

   A list of organizations matching the search criteria appears.
5. Select one or more organizations that you want to delete.
6. Click **Delete** to delete the selected organizations.

   A message box appears asking you to confirm that you want to delete the organization.
7. Click **OK** to confirm the activation.

Chapter 7: Managing Organization-Specific AuthMinder Configurations

Note: To be able to manage the configurations of an organization, you (Organization Administrator) must ensure that you have the appropriate permissions and scope to do so.
A Master Administrator cannot manage any organization-specific configurations. GAs and OAs can manage the configurations for all organizations in their scope.

Although you can use the "templatized" profiles, policies, and other configurations that are set by the Global Administrators (GAs) (as discussed in "Managing Global (see page 89)AuthMinder Configurations" (see page 89)), you may want to modify them or create new ones to meet the specific business requirements of the organizations in your purview.

When you set configurations at the organization-level, the changes are restricted to the specific organization where they were set. Also, the changes you make to the configurations are *not* applied automatically. You refresh all server instances to apply these configuration changes.

As an OA or GA, if you have the scope on the given organizations, then you can perform the following tasks:

- Assigning Organization-Specific (see page 192)AuthMinder Configurations (see page 192)
- Setting Other (see page 193)AuthMinder Configurations for An Organization (see page 193)

Assigning Organization-Specific AuthMinder Configurations

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

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

   A list of organizations matching the search criteria appears.
5. Under the Organization column, click the link for the required organization.

   The Organization Information page appears.
6. Activate the WebFort Configuration tab.

   The organization-specific configuration links are displayed in the tasks pane.
7. Configure and assign the credential profiles and authentication policies.

   See "Managing Global (see page 89)AuthMinder Configurations" (see page 89) for detailed information about how to configure the required profiles and policies and assign them, as needed. The operations that are discussed in "Managing Global (see page 89)AuthMinder Configurations" (see page 89) are for the global level. However, the configurations discussed in this chapter are for the organization level. Although the approach to access the task page is different, the configurations for both levels are the same.

Setting Other AuthMinder Configurations for An Organization

As a Global Administrator (GA) or as an Organization Administrator (OA), you can set the following configurations for an organization:

- Configuring the profiles and policies for the organizations in your scope.

  See "Configuring Profiles and Policies" (see page 95) for detailed steps.

- Configuring the OATH Token.

  See "Managing OATH OTP Tokens" (see page 128) for detailed steps.

  Note: This configuration is *not* available for an OA.

- Creating and managing Keys that are used to issue and authenticate credentials.

  See "Configuring Credential Management Keys" (see page 145) for detailed steps.

  Note: This configuration is *not* available for an OA.

- Configuring SAML tokens that are returned to the user after successful authentication.

  See "Configuring SAML Tokens" (see page 149) for detailed steps.

- Configuring Adobe Signature Service Protocol (ASSP) that is used for signing PDF documents.

  See "Configuring ASSP" (see page 151) for detailed steps.

- Configuring RADIUS clients for the AuthMinder Server and AuthMinder Server as a proxy for RADIUS requests.

  See "Configuring AuthMinder for RADIUS" (see page 152) for detailed steps.

- Assigning configurations. You can assign the default configurations that are available out-of-the-box or your custom configurations.

  See "Assigning Default Configurations" (see page 160) for detailed steps.

- Configuring plug-ins to extend the functionality of AuthMinder Server.

  See "Configuring Plug-Ins" (see page 157) for detailed steps.

- Resolving unknown password type credentials.

  See "Resolving Credential Types" (see page 158) for detailed steps.

Chapter 8: Managing Administrators

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

See "Supported Roles" (see page 14) for information about supported administrative roles. The Summary of Administrative Privileges (see page 57) section provides a quick summary of the tasks that each of these administrators can perform. This chapter covers the following administrator management operations:

Note: In addition to all the operations discussed in this chapter, the MA has the permission to create custom roles that are derived from the existing default roles supported by AuthMinder. See "Working with Custom Roles" (see page 53) for more information.

Creating Administrators

Privileges Required to Create Administrators

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

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

Creating Administrators with WebFort Password Credential

To create an administrator with WebFort Password credential:

1. Ensure that you are logged in with the required permissions and scope to create the administrative user.
2. Activate the Users and Administrators tab.
3. Under the Manage Users and Administrators section, click the Create Administrator link to display the Create Administrator page.
4. In the Administrator Details section, enter the details of the administrator. The following table explains the fields on this page:

Input	Description
User Name	The unique user name for the administrator.
Organization	The display name of the organization to which the administrator will belong. You have to select the organization that is configured for the WebFort User Password authentication mechanism. See "Creating and Activating Organizations" (see page 164) for more information. **Note:** This is *not* the organization that this administrator will manage.
First Name	The first name of the administrator.

Input	Description
Middle Name (optional)	The middle name, if any, of the administrator.
Last Name	The last name of the administrator.

5. In the Email Address(es) section, enter the email address of the administrator for the email types that are configured for the organization.
6. In the Telephone Number(s) section, enter the phone number to contact the administrator.

   If multiple telephone types are configured, enter values for all the mandatory telephone types.
7. In the Custom Attributes section, enter the Name and Value of any attributes you want to add, such as personal email address or home phone number.
8. Click Next to proceed.

   The next page to Create Administrator appears.
9. On this page:
   - Specify the role of the new administrator from the Role drop-down list.
   - In the Manages section, select the organizations that fall within the scope of the administrator by performing one of the following steps:
     - Select the All Organizations option, if you want the administrator to manage all current and future organizations in the system.
     - Select the required organizations from the Available Organizations list and click the > button to add these organizations to the Selected Organizations list.

       The Available Organizations list displays all the organizations that are available in the scope of the administrator creating this administrator. The Selected Organizations displays the list of organizations that you have selected for the administrator to manage.
10. Click Create to save the changes, create the administrator.

    A success message appears indicating that the administrator was created successfully. This message also includes the activation code that the new administrator can use to log in for the first time. The following is a sample message: `"Successfully created the administrator. The activation code for first login for this administrator is 03768672."`
11. Note down the numeric activation code that you see as a part of the success message and communicate it to the administrator.

Creating Administrators with Basic User Password Credential

If you are creating administrators in an organization that is configured for basic user password credential, then:

1. Complete Step 1 through Step 8, as discussed in "Creating Administrators with WebFort Password Credential" (see page 196) to display the Create Administrator page.
2. On this page:
   - Specify the role of the new administrator from the Role drop-down list.
   - In the Set Password section, set and confirm the password for the administrator.
   - In the Manages section, select the organizations that fall within the scope of the administrator. Perform one of the following steps:
     - Select the All Organizations option, if you want the administrator to manage all current and future organizations in the system.
     - Select the required organizations from the Available Organizations list and click the > button to add these organizations to the Selected Organizations list.

     The Available Organizations list displays all the organizations that are available in the scope of the administrator creating this administrator. The Selected Organizations displays the list of organizations that you have selected for the administrator to manage.
3. Click Create to save the changes, create the administrator.
4. Communicate the new password to the administrator.

Changing Administrator Profile Information

The profile information for an administrator includes:

- Personal information (first, middle, and last names and contact information)
- Password for the administrator
- Administrator preferences, such as Preferred Organization (the organization that will be selected by default in the **Organization** fields for all administrator-related tasks that you may perform in future), date time format, locale, and time zone information

Note: An administrator can change their profile information at any time. To change the information for any other administrator, see "Updating Administrator Information" (see page 202).

For Administrators Using WebFort Password Credential

To change your profile information, if it was created with WebFort Password credential:

1. Log in to the Administration Console.
2. In the Header frame, click the <ADMINISTRATORNAME> link to display the My Profile page.
3. Edit the required settings in the sections on this page:
   a. Edit the fields in the Personal Information section, as needed.
   b. If you want to change the current password, then in the Change Password section enter the Current Password and specify a new password in the New Password and Confirm Password fields.
   c. In the Configure Questions and Answers section, set the questions that you are prompted to answer for resetting your password, for example, In Case You Forgot Your Password (see page 93). Specify a distinct Question and its corresponding Answer.

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

   d. In the Administrator Preferences section:
      - Select the Enable Preferred Organization option, and select an organization from the Preferred Organization list. This organization is selected for all administrator-related tasks that you perform from now on.
      - Specify the preferred Date Time Format.
      - Select the preferred Locale for your instance of Administration Console
      - Select the required option from the Time Zone list. This timestamp is shown in the Last Login information in the Console header and all reports from now on.
4. Click Save to change the profile information.

For Administrators Using Basic User Password Credential

To change your profile information, if it was created with basic user password credential:

1. Log in to Administration Console.
2. In the **Header** frame, click the *<ADMINISTRATORNAME>* link to display the My Profile page.
3. Edit the required settings in the sections on this page:
   a. Edit the fields in the **Personal Information** section, as needed.
   b. If you want to change the current password, then in the **Change Password** section enter the **Current Password** and specify a new password in the **New Password** and **Confirm Password** fields.
   c. In the **Administrator Preferences** section:
      - Select the **Enable Preferred Organization** option, and select an organization from the **Preferred Organization** list. This organization is selected for all administrator-related tasks that you perform from now on.
      - Specify the preferred **Date Time Format**.
      - Select the preferred **Locale** for your instance of Administration Console.
   d. Select the required option from the **Time Zone** list. This timestamp is shown in the time-related fields. For example, **Last Login** information in the Console header and all reports.
4. Click **Save** to change the profile information.

Searching Administrators

Note: As long as you do not need to update, activate, or deactivate administrators, you do not need permissions to search. However, you *must* have the scope over the organizations that the administrator belongs to. For example, a UA can search for administrators in the target organization *if* that organization is in their purview. The partial search feature is not supported if the Administrator information is stored in the encrypted format.

To search for administrators with the specified criteria:

1. Ensure that you are logged in with the required permissions and scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Specify the search criteria to display the list of administrators. You can:
   - Search for administrators by specifying the partial or complete information of the administrator in the fields on this page.
   - Search for administrators by specifying the organization's Display Name.
   - Search for administrators by not specifying any criteria and just clicking **Search**.
   - Click the **Advanced Search** link to display the Advanced Search page to search for the required administrators by specifying their Status or Role.

   Note: In the **User Status** section, you can search for **Current Users** based on the user status (Active, Inactive, or Initial) or you can search for **Deleted Users**.
5. Select **Enable search by Accounts** if you want to search for administrators based on account IDs.
6. Specify the required details of the administrators and click **Search**.

   A list of administrators matching the search criteria appears.

Updating Administrator Information

Permissions Required

To be able to update administrators, ensure that you have the appropriate permissions and scope to do so. The MA can update any administrator. GAs can update all administrators (including other GAs), *except* for MA, in their scope. The OAs can update all other OAs and the UAs in their purview, while UAs can only update their peers within their scope.

Updating Administrator Information

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

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

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

   The Basic User Information page appears.

   Note: This page also displays the User Account Information (Account Type, AccountID, and Status) if any account type was configured.
6. Click Edit to change the administrator information about this page, as shown in the following figure.
7. In the User Details section, edit the required fields (First Name, Middle Name, and Last Name).
8. In the Email Address(es) section, edit the email addresses for the email types that are configured for the organization**.**
9. In the **Telephone Number(s)** section, edit the telephone numbers for the telephone types that are configured for the organization.
10. In the **Custom Attributes** section, edit the **Name** and **Value** of the custom attributes.
11. You can click **Save** to save the changes and return to the User Information page. Alternatively, click **Next** to proceed with additional configurations.

    Note: If you do not see the **Next** button, it means that no account type has been configured for the organization. In this case, click **Update Administrator Details** and go to Step 14.

If you click **Next**, then the User Account page appears.

12. In the **User Account** section:
    - Edit the **Account Type** and **Status** fields.
    - Expand **Advanced Attributes** to add **AccountID Attributes** for the account ID.
13. Click **Update Administrator Details**.

    The Update Administrator page appears.
14. In the **Role** section on this page, change the role of the administrator using the **Role** drop-down list.
15. In the **Set Password** section:
    - Set the **Password** and **Confirm Password** for the administrator.
    - Select **Lock** to lock the administrator's credentials for a specific period, which you can specify in the **From** and **To** fields of the **Credential Lock Period** section.
16. In the **Manages** section:
    - Select the organizations that the administrator will manage. You can also remove the organization from the administrator's scope by moving the specific organization from **Selected Organizations** to **Available Organizations**.
17. Click **Save** to save the updates.

Regenerating Activation Code

Note: This information is applicable for the WebFort Password mechanism *only*.

If your organization is using WebFort Password as the authentication mechanism, and if any of the administrators forget the activation code that they need to log in, they will contact you for a new activation code. In these cases, you generate a new activation code.

Permissions Required

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

Regenerating Activation Code

To regenerate an activation code for an administrator:

1. Ensure that you are logged in with the required permissions to update the administrative user.
2. Complete Step 2 through Step 13 in "Updating Administrator Information" (see page 202) to display the Update Administrator page.
3. In the Activation Code section, select the Regenerate Activation Code option.
4. Click Save to generate the activation code.

   The success message includes the new activation code.

   Send the new activation code to the administrator.

Updating Administrator Credentials

Administrators, like end users, must use credentials to authenticate to the system. AuthMinder supports QnA, Password, and OTP credentials out-of-the-box for administrators. You use the Credential Details page to update the credentials of an administrator. Through this page, you can enable or disable the credential, or extend its validity.

Permissions Required

To be able to update administrators, ensure that you have the appropriate permissions and scope to do so. MA *cannot* manage any credentials. GAs can manage the credentials for all administrators (including other GAs), *except* for MA, in their scope. The OAs can manage the credentials of all other OAs and UAs in their purview. UAs can manage only the credentials of the peers within their scope.

Updating Administrator Credential

To update the credential information of an administrator:

1. Ensure that you are logged in with the required permissions to update the administrative user credentials.
2. Complete Step 2 through Step 5 in "Updating Administrator Information" (see page 202).
3. Activate the **Manage Authentication Credentials** tab to display the Credential Details page.
4. Expand the required credential section by clicking the arrow sign preceding it.
5. Change the settings of the required credentials. You can change the following credential settings by using this page:
   - Status of the credential
   - Extend the credential validity
6. Click the **Save** button corresponding to the credential you have changed.

Changing Administrator Role to User

You can change the role of an administrator to a user. For example, an administrator in the IT department may have moved to the Engineering department. In this case, we would want to retain the user details, but remove the administrative permissions for the user.

To change the role of an administrator to a user:

1. Log in to Administration Console with appropriate permissions.
2. Complete Step 2 through Step 13 in "Updating Administrator Information" (see page 202) to display the Update Administrator page.
3. On the Update Administrator page, click **Change role to User**.
4. Click **OK** in the confirmation dialog that appears.

   The following message appears:

   Successfully demoted the administrator to user.

Configuring Account IDs for Administrators

An account ID is an alternate ID to identify the user, in addition to the user name. After you have configured the account types that your organization will use, you can associate one account ID per user for any of these account types. For more information about account types, see "Configuring the Account Type" (see page 43).

Permissions Required

To be able to configure an account ID for an account type, ensure that you have the permissions and scope that is required to update the user account. The MA can update any user account. GAs can update all user accounts in their scope. The OAs and UAs can update the user accounts in their purview.

Creating Account IDs

To create an account ID:

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

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

   The Basic User Information page appears.
6. Click **Edit** to open the Update Administrator page.
7. Click **Next** to display the User Account page.
8. Select the **Account Type** for which you want to add the account ID.
9. Specify the unique **AccountID** in the text box.

   This combination of account type and account ID is used to identify the user in addition to the user name.
10. Select the **Status** of the user account from the drop-down list.
11. (Optional) Expand the **Advanced Attributes** section, and provide account ID attributes and custom attributes for the account ID you are creating.

    Note: You can specify up to a maximum of three attributes for any account ID.
12. Click **Add** to add the account ID.

Updating Account IDs

Note: You cannot change the account ID once it is created. You can only change the status of the user account and add account ID attributes.

To update an account ID:

1. Complete Step 1 through Step 7 in "Creating Account IDs" (see page 207) to display the User Account page.
2. Select the **Account Type** for which you want to update the account ID information.
3. (Optional) Change the **Status** of the user account from the drop-down list.
4. (Optional) Expand the **Advanced Attributes** section, and provide attributes for the account ID you are creating.
5. Click **Update** to save your changes.

Deleting Account IDs

To delete an account ID:

1. Complete Step 1 through Step 7 in "Creating Account IDs" (see page 207) to display the User Account page.
2. Select the **Account Type** for which you want to delete the account ID.
3. Click **Delete** to delete the account ID.

Deactivating Administrators

To prevent an administrator from logging in to the system for security reasons, you can deactivate them instead of deleting it. If you deactivate an administrator permanently, the administrator is locked out, and cannot log in unless you manually activate the administrator.

Permissions Required

To be able to deactivate administrators, ensure that you have the appropriate permissions and scope to do so. The MA can deactivate any administrators, while GAs can deactivate all administrators (including other GAs), *except* MA, in their scope. The OAs can deactivate all other OAs and UAs in their purview, while UAs can only deactivate their peers within their scope.

Deactivating Administrators Permanently

To deactivate administrators permanently:

1. Ensure that you are logged in with the required permissions to deactivate administrators.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator whom you want to deactivate and click **Search**.

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

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators who you want to deactivate.
6. Click **Deactivate** to deactivate the selected administrators.

Deactivating Administrators Temporarily

Temporarily deactivating the administrator differs from *deactivating* the administrator (see "Deactivating Administrators" (see page 209)) in that you manually activate it again whenever you want to provide access to the administrators.

In temporary deactivation, the administrator is automatically activated when the end of the lock period is reached.

To temporarily deactivate an administrator, specify the **Start Lock Date** and **End Lock Date** for which you want the administrator's access to be locked. When the **End Lock Date** is reached, the administrator access is automatically activated.

To temporarily deactivate an administrator:

1. Ensure that you are logged in with the required permissions to deactivate administrators.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator who you want to deactivate and click **Search**.

   You can also click the **Advanced Search** link to search for **Current Users** based on their status (active or inactive) or their roles (GA, OA, or UA).
5. The Search Results page appears, with all the matches for the specified criteria.
6. Select one or more administrators who you want to deactivate temporarily.
7. Click **Deactivate Temporarily**. The Deactivate User Temporarily dialog appears.
8. In the **Starting From** section, select the start lock **Date** and the **Time**.
9. In the **To** section, select the end lock **Date** and the **Time**.
10. Click **Save** to save your changes.

    Note: If you do not specify any value for the **Start Lock Date**, the administrator's access is locked from the current time. If you do not specify an **End Lock Date**, the administrator's access is locked forever.

Activating Administrators

You may need to activate a deactivated administrator. For example, you may deactivate an administrator in case the administrator is on long vacation. This helps prevent unauthorized access to that administrator's login.

You cannot search directly for deactivated administrators by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. Perform an **Advanced Search** for such users, and use the **Inactive** option in the **Current Users** section to search.

Permissions Required

To be able to activate administrators, ensure that you have the appropriate permissions and scope to do so. The MA can activate any administrators, while GAs can activate all administrators (including other GAs), *except* MA, in their scope. The OAs can activate all other OAs and UAs in their purview, while UAs can only activate their peers within their scope.

Activating Administrators

To activate a deactivated administrator:

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

   The Advanced Search page appears.
5. Enter the partial or complete information of the administrator in **User Details** section.
6. In the **User Status** section, for **Current Users**, select the **Inactive** and **Initial** options to search for all inactive or initial administrators.
7. Click **Search** to display the list of all administrators matching the search criteria.
8. Select the administrators who you want to activate.
9. Click **Activate** to activate the administrators.

Deleting Administrators

Administrator information in AuthMinder includes personal information (first name, middle name, last name, email address, and telephone number), credentials, and accounts. After you delete an administrator from the Administration Console, their credentials and account information is still maintained in the database. You use the AuthMinder Software Development Kit to delete this information from the database.

If you create an administrator with the same name as a previously deleted administrator, then the new administrator does not automatically assume the permissions of the previously deleted administrator. If you want to duplicate a deleted administrator, then you manually re-create all permissions.

Permissions Required

To be able to delete administrators, ensure that you have the appropriate permissions and scope to do so. The MA can delete any administrators, while GAs can delete all administrators (including other GAs), *except* MA, in their scope. The OAs can delete all other OAs and UAs in their purview. However, UAs *cannot* delete other UAs.

Deleting Administrators

To delete an administrator:

1. Ensure that you are logged in with the required permissions to delete administrators.
2. Activate the Users and Administrators tab.
3. Under the Manage Users and Administrators section, click the Search Users and Administrators link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the administrator who you want to delete and click Search.

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

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more administrators who you want to delete.
6. Click Delete.

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

Chapter 9: How to Configure CA AuthMinder for RADIUS

You can configure AuthMinder for one of the following roles:

- As a RADIUS server that processes authentication requests from RADIUS clients

  The following steps summarize the process that takes place when AuthMinder is configured as a RADIUS server:

  1. A RADIUS client sends an authentication request to AuthMinder.

  2. AuthMinder authenticates the user and sends the authentication response.

- As a proxy server that passes authentication requests to an existing RADIUS server

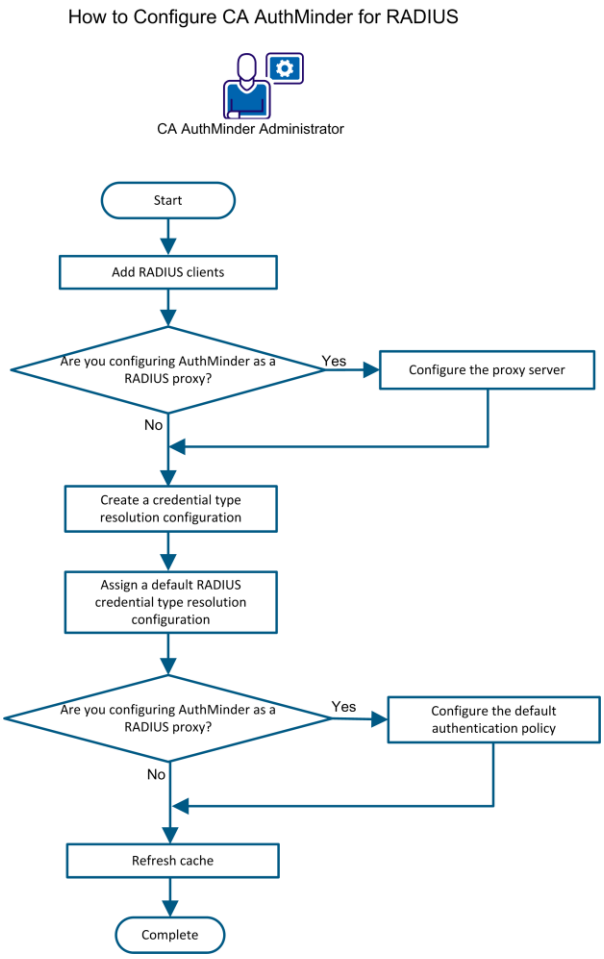
  The following steps summarize the process that takes place when AuthMinder is configured as a proxy server for a RADIUS server:

  1. A RADIUS client sends an authentication request to AuthMinder.

  2. Based on the authentication policy configured in AuthMinder, the request may be forwarded to the RADIUS server. For example, you can configure AuthMinder to forward authentication requests to the RADIUS server when the user or user's credential is not found in the AuthMinder database.

In some scenarios, you may want to configure AuthMinder as both a RADIUS server and as a proxy to a RADIUS server. For example, suppose you have recently installed AuthMinder. Some users have been migrated to AuthMinder, and the remaining users are still on the existing RADIUS solution. In this case, you configure AuthMinder as both a RADIUS server and as a proxy to a RADIUS server. Now, RADIUS authentication requests from users that have been migrated to AuthMinder are handled by AuthMinder. For all other users, AuthMinder forwards the RADIUS authentication requests to the existing RADIUS server because the users or users' credentials are not found in the AuthMinder database.

This scenario explains the procedure to configure AuthMinder for RADIUS. The following diagram outlines the steps of this procedure:



Perform the following tasks to configure AuthMinder as a RADIUS server or as a proxy server for a RADIUS server:

1. Add RADIUS clients (see page 215).
2. If you are configuring AuthMinder as a proxy for a RADIUS server, then configure AuthMinder as the proxy server (see page 218).
3. (Optional) Create a credential type resolution configuration (see page 220).
4. Assign a default RADIUS credential type resolution configuration (see page 222).
5. If you are configuring AuthMinder as a proxy for a RADIUS server, then configure the default authentication policy (see page 223).
6. Refresh cache (see page 224).

Add RADIUS Clients

A single RADIUS client can be configured in AuthMnder. If you want to configure multiple organizations in AuthMinder to use the same RADIUS client, then add the RADIUS client at the global level. Otherwise, for a single organization, add the RADIUS client for that organization.

Follow these steps:

1. Log in to the Administration Console.
2. Perform the following steps if you want to add RADIUS clients at the global level:
   a. Click the Services and Server Configurations tab on the main menu.
   b. Ensure that the WebFort tab is selected.
3. Perform the following steps if you want to add RADIUS clients at the organization level:
   a. Click the Organizations tab.
   b. Search for the organization.
   c. Select the organization from the search results.
   d. Click the Webfort Configuration tab.
4. Click RADIUS Client in the left pane.
5. Click Add.
6. Enter the following information:

   RADIUS Client IP Address

   Specifies the IP Address of the RADIUS client through which users authenticate to AuthMinder Server.

   Shared Secret Key

   Specifies the secret key shared between the RADIUS client and the AuthMinder Server.

   Note: The minimum length of the key is 1 character, and the maximum length is 512 characters.

   Description

   Specifies a short description of the RADIUS client. If you configure multiple clients, the description of each client helps distinguish between clients.

   Authentication Type

   Indicates the authentication mechanism that will be used for RADIUS-based access. Select one of the following authentication mechanisms:

   - **RADIUS OTP**

Specifies the default authentication mechanism that is used to authenticate RADIUS requests. A One-Time Token (OTT) is used as the password for authentication.

- **In-Band Password**

  Specifies that any password or OTP can be used for authentication. Typically, the In-Band Password option is used in the following scenarios:

  To resolve the credential type

  Use the In-Band Password option if you want to authenticate users with credentials that are set using credential type resolution.

  Note: You configure credential type resolution to map an input request that has an unknown credential type with a particular password-based authentication mechanism or to support any password-based authentication mechanism for RADIUS.

  (Optional, applicable for global configurations only) To specify the organization name

  In a RADIUS request, organization information can be sent with a password in the <orgname>\n<password> format. AuthMinder can extract the organization name from a password specified in this format. To enable the use of this feature, associate organizations with the RADIUS client as follows:

  a. Use the > button to move the required organizations from the Available Organizations list to the Supported Organizations list.

  b. Specify the default organization for the RADIUS client. If organization information is not sent with the password, then this default organization is considered in the authentication to resolve user details.

- **EAP:** This option is not currently supported. Do not select it.

7. In the RADIUS Retry Handling section, specify the following:
   - Select the Enable Retry option if you want the RADIUS client to retry sending the request to AuthMinder Server if it does not receive a response.
   - In the Retry Window field, enter the duration in seconds within which the client can retry connecting to the AuthMinder Server if it does not receive a response. After this period, the retry is considered invalid. Ensure that the retry window period is greater than the client timeout period.
8. In the Additional RADIUS Response Attributes section, specify the attributes that you want the AuthMinder Server to include in the response sent to the RADIUS client after successful authentication:

   Attribute ID

   Specifies a unique attribute identifier.

   Example: 26

   Attribute Value

Specifies the value corresponding to the attribute ID. You can pass static values, variables such as user attributes or custom attributes, or a combination of static values and variables. For example, for the user JSmith, if the custom user attribute key-value pair is Employee ID=150, then you can include the employee ID in the RADIUS response as follows:

```
JSmith = $$Employee ID$$
```

This setting returns JSmith = 150.

9. In the RADIUS Packet Drop Options section, select the events for which the AuthMinder Server must drop RADIUS packets. You can select any combination of the following events:
   - User not Found
   - Credential not Found
   - Invalid Request
   - Internal Error
10. Click Add.

    The RADIUS client is added. This configuration will take effect after you refresh the cache.

Configure AuthMinder as the Proxy Server

Configure AuthMinder as the proxy server for a RADIUS server.

Note: Perform the procedure described in this section only if you want to configure AuthMinder as a RADIUS proxy. Do not perform this procedure if you want to configure AuthMinder as a RADIUS server.

Follow these steps:

1. Log in to the Administration Console.
2. Perform the following steps if you want to add RADIUS clients at the global level:
   a. Click the Services and Server Configurations tab on the main menu.
   b. Ensure that the WebFort tab is selected.
3. Perform the following steps if you want to add RADIUS clients at the organization level:
   a. Click the Organizations tab.
   b. Search for the organization.
   c. Select the organization from the search results.
   d. Click the Webfort Configuration tab.
4. Click RADIUS Proxy in the left pane.
5. Select Enable Proxy.
6. If you want multiple organizations to use AuthMinder as the proxy server for RADIUS, then select the Use Global Configuration check box.
7. Enter the following details of the RADIUS server in the Primary Proxy Server Details section:

   IP Address

   Specifies the IP address of the RADIUS server.

   RADIUS Port

   Specifies the port number on which the RADIUS server is listening.

   Shared Secret Key

   Specifies the secret key shared between the AuthMinder Server and the RADIUS server.

   Note: The minimum length of the key is 1, and the maximum is 512 characters.

   Description

   Specifies a string to describe the RADIUS server. The description helps to identify the RADIUS server, if multiple servers are configured.

   Read Timeout

Specifies the maximum time in milliseconds for which the AuthMinder must wait for a response from the RADIUS server.

Retry Count

Specifies the number of times the AuthMinder Server must attempt to send the request to RADIUS server, if it does not receive a response.

8. In the Additional RADIUS Response Attributes section, specify the attributes that you want the AuthMinder Server to include in the request that it sends to the RADIUS server after successful authentication.

   Attribute ID

   Specifies a unique attribute identifier in this column. For example, 26.

   Attribute Value

   Specifies the value corresponding to the attribute ID. For example, a value corresponding to attribute identifier 26.

9. (Optional) Click Add More if you want to add more attributes.
10. (Optional) If you have configured an additional RADIUS server, then provide the details of that RADIUS server in the Backup Proxy Server Details section.

    AuthMinder forwards RADIUS authentication requests to this backup RADIUS server after the retry count (configured earlier) is exhausted.

11. Click Update to save the configuration.

    AuthMinder is configured as a proxy server for a RADIUS server.

Create or Update a Credential Type Resolution Configuration

Note: Perform the procedure described in this section only if you set the In-Band Password option as the authentication type while adding a RADIUS client.

You can configure credential type resolution for mapping an in-band password to any one of the following authentication types:

- Password
- ArcotOTP-OATH
- OATH OTP
- OTP
- ArcotOTP-EMV
- RADIUS OTP
- LDAP Password
- Native Token

The following predefined credential type resolutions are available in AuthMinder:

- VerifyArcotOTP-EMV
- VerifyArcotOTP-OATH
- VerifyLDAPPassword
- VerifyNativeToken
- VerifyOATH
- VerifyOTP
- VerifyOTT
- VerifyPassword

If any of these predefined credential type resolution configurations meet your requirements for processing in-band passwords, then you need not perform the procedure described in this section. Perform the procedure only if none of these predefined configurations meet your requirements.

You assign credential type resolution as the default for the organization. You can also configure credential type resolution per user by configuring a custom user attribute that specifies the mechanism to be used for each user. This custom user attribute is part of the credential type resolution configuration.

Follow these steps:

1. Log in to the Administration Console.
2. Perform the following steps if you want to add RADIUS clients at the global level:

a. Click the Services and Server Configurations tab on the main menu.

b. Ensure that the WebFort tab is selected.

3. Perform the following steps if you want to add RADIUS clients at the organization level:

   a. Click the Organizations tab.

   b. Search for the organization.

   c. Select the organization from the search results.

   d. Click the Webfort Configuration tab.

4. Click Credential Type Resolution in the left pane.

   The Credential Type Resolution Configuration screen opens.

5. Click Create.

6. Enter a name for the configuration.

7. If you want to copy an existing configuration, then:

   a. Select the Copy Configuration check box.

   b. From the Available Configurations drop-down list, select the configuration that you want to copy.

8. From the Resolve plain to drop-down list, select the credential type to which you want to map the incoming password type credential.

9. (Optional) If you have created a custom user attribute for specifying the credential type, then specify the name of that custom attribute in the User Custom Attribute For Credential Type field.

   When a RADIUS authentication request is received, the credential type specified in this custom user attribute overrides the credential type that you configure in the preceding step. If the credential type is not specified in the custom user attribute, then the credential type that you configure in the preceding step is used as the default credential type.

   While a user is being created, ensure that the value for the custom user attribute is set to one of the following integer values:

   - Password: 1
   - ArcotOTP-OATH: 8
   - OATH OTP: 7
   - OTP: 4
   - ArcotOTP-EMV: 8
   - RADIUS OTP: 5
   - LDAP Password: 10
   - Native Token: 11

For example, if you want the custom user attribute to specify OATH OTP as the credential type, then ensure that 7 is set as the value of the custom user attribute.

10. Click Save.

    The credential type resolution configuration is saved.

Assign a Default RADIUS Credential Type Resolution Configuration

Note: Perform the procedure described in this section only if you set the In-Band Password option as the authentication type while adding a RADIUS client.

Set the credential type resolution configuration as the default configuration for authentication requests sent by RADIUS clients.

Follow these steps:

1. Log in to the Administration Console.
2. Perform the following steps if you want to add RADIUS clients at the global level:
   a. Click the Services and Server Configurations tab on the main menu.
   b. Ensure that the WebFort tab is selected.
3. Perform the following steps if you want to add RADIUS clients at the organization level:
   a. Click the Organizations tab.
   b. Search for the organization.
   c. Select the organization from the search results.
   d. Click the Webfort Configuration tab.
4. Click Assign Default Configurations in the left pane.
5. From the RADIUS Credential Type Resolution Configuration drop-down list, select the credential type resolution configuration that you want to use for processing in-band passwords.
6. Click Save.

   The default RADIUS credential type resolution configuration is assigned.

Configure the Default Authentication Policy

If you are configuring AuthMinder as a RADIUS proxy, then create or update an authentication policy for the credential type for which you are configuring AuthMinder as a RADIUS proxy. Set this policy as the default authentication policy for that credential type. In the authentication policy, specify the conditions under which authentication requests must be forwarded by AuthMinder to the RADIUS server.

Note: Perform the procedure described in this section only if you want to configure AuthMinder as a RADIUS proxy. Do not perform this procedure if you want to configure AuthMinder as a RADIUS server.

Follow these steps:

1. Log in to the Administration Console.
2. Perform the following steps if you want to add RADIUS clients at the global level:
   a. Click the Services and Server Configurations tab on the main menu.
   b. Ensure that the WebFort tab is selected.
3. Perform the following steps if you want to add RADIUS clients at the organization level:
   a. Click the Organizations tab.
   b. Search for the organization.
   c. Select the organization from the search results.
   d. Click the Webfort Configuration tab.
4. In the left pane, click the Authentication link for the credential type for which you are configuring AuthMinder as a RADIUS proxy server.

   The Password Authentication Policy screen opens.
5. Click Create if you want to create a policy configuration. Alternatively, click Update if you want to update an existing policy configuration.
6. Enter the required data in the remaining fields of the Policy Configuration section.

   Note: For detailed information about the fields of the Policy Configuration section, see the *CA AuthMinder Administration Guide*.
7. Expand Advanced Configurations.
8. Select one or both of the following options:

   User not Found

   Specifies that the authentication request must be forwarded to the RADIUS server if the user does not exist in the AuthMinder database.

   Credential not Found

Specifies that the authentication request must be forwarded to the RADIUS server if the credential with which the user is trying to authenticate does not exist in the AuthMinder database.

9. Enter the required data in the remaining fields of the Advanced Configurations section.

   Note: For detailed information about the fields of the Advanced Configurations section, see the *CA AuthMinder Administration Guide*.

10. Click Save.

    The authentication policy is configured.

Refresh Cache

Refresh the cache for all the configurations to take effect.

Follow these steps:

1. Log in to the Administration Console.
2. Select Services and Server Configurations, Administration Console, Refresh Cache in the System Configuration section.

   The Refresh Cache screen opens.
3. Select any one or both of the following options depending on whether you have configured AuthMinder as a RADIUS server for a single organization or multiple organizations:

   - Refresh System Configuration
   - Refresh Organization Configuration
4. Click OK.

   A message stating that the request was submitted successfully appears.
5. Select Services and Server Configurations, Administration Console, Check Cache Refresh Status.

   The Search Cache Refresh Request screen opens.
6. Select the request ID of the refresh request, and then click Search.

   The status of the refresh request is displayed. The SUCCESS message in the Status column indicates that the configuration has taken effect.

Chapter 10: Managing Users and Their Credentials

AuthMinder works with your application to manage strong authentication for administrators and end users. AuthMinder allows you to create the end users directly through the Administration Console. For the purpose of migrating existing users and creating new users in the AuthMinder database as bulk operations, AuthMinder provides extensive Web Services. This process of creating users in AuthMinder is known as *migration*.

Note: See "Enrollment Workflows" in the *CA AuthMinder Web Services Developer's Guide* to understand the workflows for user enrollment.

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

Creating Users

Global Administrators (GAs), Organization Administrators (OAs), and User Administrators (UAs) can create users for organizations within their scope.

To creates users, it is not mandatory to specify the first name and last name of the users.

To create a user:

1. Ensure that you are logged in with the required permissions and scope to create the user.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Create User** link to display the Create User page.
4. In the **User Details** section, enter the details of the user. The following table explains the fields on this page:

Input	Description
User Name	The unique user name.
Organization	The display name of the organization to which the user will belong.
First Name	The first name of the user.
Middle Name	The middle name, if any, of the user.
Last Name	The last name of the user.

5. In the **Email Address(es)** section, enter the **Email** address of the user.
6. In the **Telephone Number(s)** section, enter the **Phone Number** to contact the user.
7. Select whether you want the user to be in the **Initial** state or in the **Active** state.
8. In the **Custom Attributes** section, enter the **Name** and **Value** of any attributes you want to add, such as personal email address or home phone number.
9. Click **Create User** to create the user.

Searching for Users

Permissions Required

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

Searching For Users

To search for users with the specified criteria:

1. Ensure that you are logged in with the appropriate scope.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Specify the search criteria to display the list of users. You can:
   - Search for users by specifying the partial or complete information of the user in the fields on this page.

     Note: Specifying partial information in the fields works only if the fields are not marked for encryption. If any of the fields on this page have been marked for encryption, then specify the complete value for the search to function correctly.
   - Search for users by specifying the organization's display Name.
   - Search for users by not specifying any criteria and just clicking **Search**.
   - Click the **Advanced Search** link to display the Advanced Search page to search for users by specifying their Status or Role.
5. Specify the required details of the users and click **Search**.

   A list of users matching the search criteria appears.

Updating User Information

Note: To be able to update a user's information, ensure that you have the appropriate permissions and scope to do so. The MA can update any user. GAs can update all users in their scope. The OAs and UAs can update the users in their purview.

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

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

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

   The Basic User Information page appears.

   Note: This page also displays the **User Account Information** (**Account Type**, **AccountID**, and **Status**) if any account type was configured.
6. Click **Edit** to change the user information about this page.
7. In the **User Details** section, edit the required fields (**First Name**, **Middle Name**, **Last Name**).
8. In the **Email Address(es)** section, edit the email addresses for the email types that are configured for the organization**.**
9. In the **Telephone Number(s)** section, edit the telephone numbers for the telephone types that are configured for the organization.
10. (Optional) Update the **User Status**.
11. (Optional) Edit the **Name** and **Value** of **Custom Attributes**.
12. Click **Save** to save the changes and return to the User Information page. Alternatively, click **Next** to proceed with additional configurations.

    If you click **Next**, then the User Account page appears.
13. In the **User Account** section:
    - (Optional) Select the **Account Type,** and edit the **Status**.
    - Expand **Advanced Attributes** to add **AccountID Attributes** and **Custom Attributes** for the account ID.

Note: If this is the first account ID you are creating, click **Add** to add an account ID before you can update it. For more information about adding an account ID, see "Creating Accounts" (see page 232).

14. Click **Update** to save your changes.

Promoting Users to Administrators

Permissions Required

To be able to promote a user to an administrator, ensure that you have the appropriate permissions and scope to do so. The MA can promote any user. GAs can promote users to OA, UA, or GA for organizations within their administrative purview. OAs can promote users to OA or UA for organizations within their administrative purview. UAs *cannot* promote users to administrators.

Promoting Users to Administrator

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

1. Ensure that you are logged in with the required permissions and scope to create administrators and update the user information.
2. Activate the Users and Administrators tab.
3. Under the Manage Users and Administrators section, click the Search Users and Administrators link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user who you want to promote (as discussed in the preceding section) and click Search.

   A list of administrators and users matching the search criteria appears.
5. Click the <user name> link of the user who you want to promote.

   The Basic User Information page appears.
6. Click Edit to open the User Information page.
7. If the user's First Name, Last Name, Email address(es), Telephone Number(s) are not specified, enter the same. These attributes are mandatory for administrators.
8. If the user's Email is not specified, enter the same. This attribute is mandatory for administrators.
9. Click Next to display the User Account page.

   Note: If no account type is configured for the user's organization, then the Change Role to Administrator button is displayed on the Update User page itself.
10. On the User Account page, click Change Role to Administrator to display the Create Administrator page.
11. On this page:
    - Specify the role of the new administrator from the Role drop-down list.
    - Enter the password for the administrator in the Password and Confirm Password fields.

    Note: If the organization is configured for AuthMinder User Password authentication, these fields are not displayed.

- In the Manages section, select the organizations that fall within the scope of the administrator. Perform one of the following steps:
  - Select the All Organizations option, if you want the administrator to manage all current and future organizations in the system.
  - Select the required organizations from the Available Organizations list and click the > button to add these organizations to the Selected Organizations list.

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

12. Click Create to save the changes and create and activate the administrator.

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

Configuring Account IDs for Users

An account ID (also known as *account*) is an alternate ID to identify the user, in addition to the user name. After you have configured the account types that your organization will use, you can associate one account ID per user for any of these account types. For more information about account types, see "Configuring the Account Type" (see page 43).

Permissions Required

To be able to configure an account ID for an account type, ensure that you have the appropriate permissions and scope to update the user information. MA can update any user. GAs can update all users in their scope. The OAs and UAs can update users in their purview.

Creating Accounts

To create an account:

1. Ensure that you are logged in with the permissions and scope that is required to update the user information.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user for whom you want to create the account ID, and click **Search**.

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

   The Search Results page appears, with all the matches for the specified criteria.
5. Click the <*user name*> link of the user whose account you want to edit.

   The Basic User Information page appears.

   Note: This page also displays the **User Account Information** (**Account Type**, **AccountID**, and **Status**) for the account types configured.
6. Click **Edit** to open the Update User page.
7. Click **Next** to display the User Account page.
8. Select the **Account Type** for which you want to add the account ID.
9. Specify the unique **AccountID** in the text box.

   This combination of account type and account ID is used to identify the user in addition to the user name. Ensure that the account type and account ID combination is unique for a particular organization.
10. Select the **Status** of the user account from the drop-down list.
11. (Optional) Expand the **Advanced Attributes** section, and perform the following steps:
    a. Enter attribute values for the account ID that you are creating.

       Note: You can specify up to a maximum of three attributes for any account ID.

    b. Enter values for any **Custom Attributes** that are configured for the account type.
12. Click **Add** to add the account ID.

Updating Accounts

Note: You cannot change the account ID after the account has been created. You can only change the status of the user account and add or delete account ID and custom attributes.

To update an account:

1. Complete Step 1 through Step 7 in "Creating Accounts" (see page 232) to display the User Account page.
2. Select the **Account Type** for which you want to update the account ID.
3. (Optional) Change the **Status** of the user account from the drop-down list.
4. (Optional) Expand the **Advanced Attributes** section, and provide **AccountID Attributes** and **Custom Attributes** for the account ID you are updating.
5. Click **Update** to save your changes.

Deleting Accounts

To delete an account:

1. Complete Step 1 through Step 7 in "Creating Accounts" (see page 232) to display the User Account page.
2. Select the **Account Type** for which you want to delete the account ID.
3. Click **Delete** to delete the account ID.

Updating User Credential Information

Users, must use credentials to authenticate to the system. AuthMinder supports ArcotID PKI, QnA, Password, OTP, OATH OTP, ArcotID OTP-OATH, and ArcotID OTP-EMV credentials out-of-the-box.

You use the Credential Details page under Manage Authentication Credentials to update the credentials of the user. Through this page, you can enable or disable the credential, or extend its validity.

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

To update the credential information of user:

1. Ensure that you are logged in with the required permissions and scope to update the user credentials.
2. Complete Step 2 through Step 5 in "Updating User Information" (see page 228).
3. Activate the Manage Authentication Credentials tab to display the Credential Details page.
4. If you want to set all the credentials of the selected user to the same status, then instead of changing it in every section corresponding to the credential, you can use the All Credentials section to achieve this. Perform the following steps:
    a. Expand the All Credentials section by clicking the arrow sign preceding it.
    b. Choose any of the following options:

        Note: These statuses are not applicable for an OTP if the credential is in the Verified state.

        - **Enable**: To enable all the credentials of the user. For example, if the credentials of the user are locked, then you can enable them with this option.
        - **Enable and Reset Disable Period**: To enable the disabled credentials and reset the disable period. For example, the user is on a vacation and their account is disabled, if you want to enable this user's credential before the disable end date, then you can use this option to enable the credential and reset their disable period.
        - **Disable**: To disable all the credentials of the user.
        - **Disable for a Period**: To disable all the credentials of the user for the period that you specify.

    c. Click the Save button corresponding to this section.
5. If you want to apply different configurations for different credentials, then perform the following steps:

a. Expand the required credential section by clicking the arrow sign preceding it.

   Note: If the user has multiple credentials of the same type, then a separate section (<*Credential Type*> <(Usage Type)>) is shown for each of these credentials.

b. Change the settings of the required credentials. You can change the following credential settings by using this page:

   - Status of the credential
   - Extend the credential validity
   - Add or change the existing credential custom attributes

   Note: For OATH OTP credentials, you can reuse abandoned tokens, assign new tokens, deassign tokens, associate the vendor token ID with the OATH OTP that is generated by the AuthMinder Server, and synchronize the OATH OTP.

c. Click the Save button corresponding to the credential you have changed.

Deactivating Users

To prevent a user from logging in to the system for security reasons, you can deactivate their access instead of deleting it. If you deactivate the user, then they are locked out of the system, and cannot log in unless they are activated again.

Permissions Required

To be able to deactivate users, ensure that you have the appropriate permissions and scope to do so. MA can deactivate any user, while GAs can deactivate all users (including other GAs) within their scope. The OAs and UAs can deactivate all users in their purview.

Deactivating Users

To deactivate users:

1. Ensure that you are logged in with the required permissions and scope to deactivate users.
2. Activate the Users and Administrators tab.
3. Under the Manage Users and Administrators section, click the Search Users and Administrators link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user who you want to deactivate and click Search.

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

   The Search Results page appears with all the matches for the specified criteria.
5. Select one or more users who you want to deactivate.
6. Click Deactivate to deactivate the selected user.

Deactivating Users Temporarily

Temporarily deactivating the users differs from *deactivating* the users (see "Deactivating Users" (see page 236)) in that you manually activate it again whenever you want to provide access to the system.

In temporary deactivation, the user is automatically activated when the end of the lock period is reached.

To temporarily deactivate users, specify the **Start Lock Date** and **End Lock Date** for which you want the user's access to the system to be deactivated. When the **End Lock Date** is reached, the user is automatically activated.

To temporarily deactivate a user:

1. Ensure that you are logged in with the required permissions and scope to temporarily deactivate users.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user who you want to temporarily deactivate and click **Search**.

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

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users who you want to deactivate temporarily.
6. Click **Deactivate Temporarily**. The Deactivate User Temporarily dialog appears.
7. In the **Starting From** section, select the start lock **Date** and the **Time**.
8. In the **To** section, select the end lock **Date** and the **Time**.
9. Click **Save** to save your changes.

   Note: If you do not specify any value for the **Start Lock Date**, the access is locked from the Current Time. If you do not specify an **End Lock Date**, the access is locked forever.

Activating Users

You may need to activate a deactivated user. For example, you may deactivate a user in case the user is on long a vacation. This helps to prevent unauthorized access to that user's login.

You cannot search directly for deactivated users by specifying the search criteria and clicking the **Search** button on the Search Users and Administrators page. You perform an **Advanced Search** for such users and use the **Inactive** option in the **Current Users** section to search.

Permissions Required

To be able to activate users, ensure that you have the appropriate permissions and scope to do so. The MA can activate any user, while GAs can activate all users within their scope. The OAs and UAs can activate all users in their purview.

Activating Users

To activate locked-out users:

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

   The Advanced Search page appears.
5. Enter the partial or complete information of the user in **User Account** section.
6. In the **User Status** section, for **Current Users**, select the **Inactive** and **Initial** options to search for all inactive or initial users.
7. Click **Search** to display the list of all users matching the search criteria.
8. Select the users who you want to activate.
9. Click **Activate** to activate the user.

Deleting Users

After a user is deleted, all the permissions that are associated with the user are permanently deleted. As a result, the user can no longer log in to your application. Their information and credentials are also deleted from the system.

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

Permissions Required

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

Deleting Users

To delete users:

1. Ensure that you are logged in with the required permissions to delete the users.
2. Activate the **Users and Administrators** tab.
3. Under the **Manage Users and Administrators** section, click the **Search Users and Administrators** link to display the Search Users and Administrators page.
4. Enter the partial or complete information of the user who you want to delete and click **Search**.

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

   The Search Results page appears, with all the matches for the specified criteria.
5. Select one or more users who you want to delete.
6. Click **Delete**.

   Note: After you have deleted the user, their information is deleted from the database. The user history is archived for billing purposes.

Chapter 11: Tools for System Administrators

This chapter discusses the command-line tools that are shipped with AuthMinder that you can use to perform system management tasks. It provides a quick overview of functions and useful options for the tools that are available with AuthMinder and can be useful to administrators:

- DBUtil: (see page 241)AuthMinder Database Tool (see page 241)
- arwfserver: Server Management Tool (see page 247)
- arwfutil: A Utility Tool (see page 251)

DBUtil: AuthMinder Database Tool

During AuthMinder installation, the installer collects information to connect to the AuthMinder database. After the installation is completed, this information is stored in encrypted format in the securestore.enc file.

This file stores the following encrypted information that is required to connect to the AuthMinder database:

- Database user name and password (Used by the AuthMinder Server to connect to the database.)
- Master key (Used for encrypting the database user name and password that is stored in securestore.enc.)

AuthMinder supports both software and hardware modes to protect the data. The DBUtil tool can be used to perform database operations for both the modes.

If you want to add a new database user name, password, or DSN or change the master key value at any time *after* installation, then use DBUtil.

This section covers the following topics:

- Using DBUtil Options (see page 242)
- Updating the Master Key (see page 245)

Note: Because the master key is used for encrypting sensitive information, for security reasons, the DBUtil tool *does not* provide any option to view the key value.

Using DBUtil Options

The following table lists the options for DBUtil. In this table, *key-value* pair refers to either DSN, password, or database user name/password pair. The DSN/password is used by AuthMinder Server, while user name/password is used by Administration Console and User Data Service.

Option	Description
-h	Displays the Help for the tool. Syntax: dbutil -h
-init	Creates a new securestore.enc with the new master key that you specify, as discussed in "Updating the Master Key" (see page 245). Syntax: dbutil -init key For example: dbutil -init MasterKeyNew dbutil -init WebFortDatabaseMKNew **Important!** This command succeeds only if there is no securestore.enc in the conf directory.
-pi	Inserts an additional key-value pair into securestore.enc, as discussed in "Updating the Master Key" (see page 245). Syntax: dbutil -pi <key> <value> [-h HSMPin [-d HSMModule]] -h HSMPin is required if securestore.enc is protected by HSM cryptography. -d HSMModule is optional when -h is present. It defaults to "nfast" (NCipher). For example: dbutil -pi WebFortBackupDSN dbapassword dbutil -pi Jack userpassword dbutil -pi Jack userpassword -h hsmpassword -d chrysalis **Important!** Each key can only have one value. If you have already inserted a key-value pair, then you cannot insert another value for the same key.

Option	Description
-pu	Updates the value for an existing key-value pair in securestore.enc. This feature can be used when you need to update the database password. Syntax: dbutil -pu <key> <value> [-h HSMPin [-d HSMModule]] For example: dbutil -pu WebFortDatabaseDSN newPassword dbutil -pu Jack userPassword dbutil -pu Jack userpassword -h hsmpassword -d chrysalis
-pd	Deletes the specified key-value pair from securestore.enc. Syntax: dbutil -pd <key> [-h HSMPin [-d HSMModule]] For example: dbutil -pd WebFortDatabaseDSNOld dbutil -pd Jack
-i	Inserts the specified primary name-value pair in the securestore.enc file, if hardware-based encryption is used to secure the data in this file. This is used during server startup to provide HSM initialization information. Syntax: dbutil -i <primeKey> <HSMPin> where primeKey is the name of the HSM module For example: dbutil -i chrysalis pin
-u	Updates the specified primary name-value pair in the securestore.enc file, if hardware-based encryption is used to secure the data in this file. Syntax: dbutil -u <primeKey> <HSMPin> where primeKey is the name of the HSM module For example: dbutil -u chrysalis newHSMpin

Option	Description
-d	Deletes the specified primary name-value pair, if hardware-based encryption is used to secure the data in this file. Syntax: dbutil -d <primeKey> where primeKey is the name of the HSM module For example: dbutil -d chrysalis

Updating the Master Key

The *master key* is used to encrypt the values in the securestore.enc file. It also encrypts all encryption keys that are used by the product and are stored in the AuthMinder database.

If you want to change the master key value in the securestore.enc file, then:

1. Back up the current securestore.enc file.

   The current securestore.enc is available at:

   - **On Windows**
     `<install_location>\Arcot Systems\conf\`
   - **On UNIX-Based Platforms**
     `<install_location>/arcot/conf/`

2. Delete the securestore.enc file that is available in the directory that is mentioned in the preceding step.
3. Open the Command Prompt Window.
4. Change the working directory to the following location where DBUtil is available:

   - **For Windows**:
     `<install_location>\Arcot Systems\tools\win`
   - **For UNIX-Based Platforms**:
     `<install_location>/arcot/tools/<platform_name>`

5. Run the following command:

   (For software mode) dbutil -init *<master_key>*

   (For hardware mode) dbutil -init *<master_Key_Label>*

   The tool re-creates securestore.enc with the master key name that you specify.

   Important! If the master key setup fails, then contact CA Support for help.

6. Update the database information in the securestore.enc file.

   The AuthMinder installer automatically configures the database username/password and database DSN/password information in securestore.enc. However, after creating a securestore.enc file, manually insert this information in the new file by using the dbutil -pi option.

   To insert the supplied database values in securestore.enc, enter the following command:

   - (For software mode) dbutil -pi *<dbUser> <dbPassword>*
   - (For hardware mode) dbutil -pi *<dbUser> <dbPassword> [*-h *HSMPin [*-d *HSMModule]]*

     In the preceding command, dbUser is the database user name and dbPassword is the password that is associated with the specified user name. For example:
     `dbutil -pi arcotuser welcome123`

Note: The user name that you specify in this command is case-sensitive.

- (For software mode) dbutil -pi <*dsn*> <*dbPassword*>

  Note: <*dbPassword*> is the password of the database user.

- (For hardware mode) dbutil -pi <*dsn*> <*dbPassword*> *[*-h *HSMPin [*-d *HSMModule]]*

  In the preceding command, dsn is the data source name and dbPassword is the database password. For example:
  `dbutil -pi arcotdsn welcome123`

  Note: The DSN name that you specify in this command is case-sensitive.

7. If you have performed distributed deployment of AuthMinder, then copy the new securestore.enc file to all the systems where AuthMinder components are installed.

arwfserver: Server Management Tool

The arwfserver tool is an interactive utility that you can use to manage AuthMinder Server configurations and troubleshoot connection errors. For example, Administration Console uses the Server Management protocol for managing AuthMinder Server instance, and the default port number of this protocol is 9743. If this port is already in use by some other application, then you can use arwfserver tool to set the protocol on a different port.

In addition to server configuration management, the arwfserver tool also enables you to configure AuthMinder settings that are either used rarely (authentication and authorization for Web Service APIs) or are needed only in certain deployment scenarios (enable or disable plug-ins).

Running the Tool in Interactive Mode

The tool provides the -i option to run it in the interactive mode. In this mode, all server configurations are performed in a manner that is similar to how it is done in service mode, except that the listeners are not started.

When run in this mode, the arwfserver tool starts its own console prompt (wf>) and generates the startup logs in *<install_location>*/logs/arcotwebfortstartupcmd.log and the transaction logs in *<install_location>*/logs/arcotwebfortcmd.log.

To run the arwfserver tool:

1. Navigate to the location where the tool is available:
   - **On Windows**
     `<install_location>\Arcot Systems\bin\`
   - **On UNIX-based Platforms**
     `<install_location>/arcot/bin/`
2. Run the following command:
   - **On Windows**
     `arwfserver -i`
   - **On UNIX-based Platforms**
     `./webfortserver -i`

   The tool starts in interactive mode.
3. Specify the options that are listed in the following table to perform the required task:

Option	Description
Display Message Operations	

Option	Description
ddn	Enables you to download display names to a file. You must enter the context name of the application whose display names you want to download, and the path where the file must be downloaded. **Syntax**: ddn *<application_context> <file_location>* **Example**: ddn Admin ARCOT_HOME>/logs
dmsg	Enables you to download the display messages to a file. You must enter the application context and path where the file must be downloaded. **Syntax**: dmsg *<application_context> <file_location>* **Example**: dmsg Admin ARCOT_HOME>/logs
udn	Enables you to upload the file containing the customized display names to the database. **Syntax**: udn *<file_path>*
umsg	Enables you to upload the file containing the customized display messages to the database. **Syntax**: umsg *<file_path>*
Plug-In Configurations	
getmodconf	Fetches the configuration for the current modules. For example, credential modules and plug-ins. **Syntax**: getmodconf
upluginstatus	Updates the status of the plug-in. Following are the supported states: ■ 0: Indicates that the plug-in is DISABLED. ■ 1: Indicates that the plug-in is ACTIVE. ■ 2: Indicates that the plug-in is NOT_LOADED. **Syntax**: upluginstatus
Protocol Operations	

Option	Description
getprotoconf	Fetches the configurations for all protocols. **Syntax**: getprotoconf
setsvrmgmtport	Allows you to change the port number of the Server Management protocol. If you have enabled AuthMinder Server for SSL, then this tool also provides you an option to change the transport mode from SSL to TCP. **Syntax**: setsvrmgmtconf <*Server Management port*> TCP **Example**: setsvrmgmtconf 9743 TCP
Server Management Operations	
version	Generates a file called arcotwebfort-ver-<*dd*>-<*mmm*>-<*yy*>.txt, which lists the version of all AuthMinder library files. This file is available in the following directory: **Windows**: <*install_location*>\Arcot Systems\logs **UNIX-Based Platforms**: <*install_location*>/arcot/logs **Syntax**: version
Utility Operations	
??	Searches the commands based on the pattern you provide. Syntax: ?? *<search text>* Example: ?? conf All the options that set or get configurations are displayed. For example: ■ getmodconf ■ getprotoconf

Option	Description
?	Lists the commands supported by arwfserver. If you provide the command name along with this option, then the tool provides help on command usage. **Syntax**: ■ ? Lists all the supported commands ■ ? <*command_option*> Provides help on the command usage. **Example**: ? setsvrmgmtport Explains the usage of set server management port command.
help	Provides the help on the command usage. **Syntax**: help <*command_option*> Provides help on the command usage. **Example**: help setsvrmgmtport Explains the usage of set server management port command.
log2c	Allows you to write the logs to the Console. Enter Y to write the logs to the Console or N to write the logs to the file. **Syntax**: log2c <*option*> **Example**: log2c n
q	Closes the interactive mode.

arwfutil: A Utility Tool

You can use the arwfutil tool to manage server cache, refresh the server, shut down the server, and read server configuration information, such as protocol configurations and server statistics.

You can run the tool in interactive mode or directly access the commands.

To run the arwfutil tool:

1. Navigate to the location where the tool is available:
   - **On Windows**
     `<install_location>\Arcot Systems\bin\`
   - **On UNIX-based Platforms**
     `<install_location>/arcot/sbin/`
2. You can run the tool in one of the following modes:
   - In the interactive mode, as follows:
     - **On Windows**
       `arwfutil -i`
     - **On UNIX-based Platforms**
       `./arwfutil -i`

     The tool starts in interactive mode. Now, run the commands that are listed in the following table.
   - By entering the commands directly, as follows:
     - **On Windows**
       `arwfutil <command_option>`
     - **On UNIX-based Platforms**
       `./arwfutil <command_option>`

   The following table lists the command options that are provided by the arwfutil tool:

Option	Description
Server Management Operations	

Option	Description
cr	Refreshes the cache of the AuthMinder Server instance. You *must* enter the instance IP and the server management port number. After successful operation, the message "The operation was successful" is displayed and a transaction ID is returned. **Syntax**: arwfutil cr *<AuthMinder Server IP> <Server Management port>* **Example**: arwfutil cr localhost 9743
dc	Downloads the server configuration cache to a file called arcotwebfortcache-<*transaction ID*>.log. This file is available in the following directory: **For Windows**: <*install_location*>\Arcot Systems\logs **For UNIX-Based Platforms**: <*install_location*>/arcot/logs Every time you download the server configuration cache, a new file will be created with the unique transaction identifier. **Syntax**: ■ arwfutil dc Prompts whether to download the complete or partial cache. Enter 1 for complete cache or 0 for partial cache. ■ arwfutil dc <AuthMinder *Server IP> <Server Management port>* Downloads the complete cache. **Example**: arwfutil dc localhost 9743

Option	Description
gss	Generates a file called wf-server-stats-<*dd*>-<*mmm*>-<*yy*>.xml, which lists the server statistics. This file is available in the following directory: **For Windows**: <*install_location*>\Arcot Systems\logs **For UNIX-Based Platforms**: <*install_location*>/arcot/logs The statistics file includes the following information for each protocol: ■ Number of requests received ■ Number of successful transactions ■ Number of failed transactions ■ Minimum time that is taken to process requests ■ Maximum time that is taken to process requests ■ Total time that is taken to process all requests ■ Average time that is required to process a request After successful operation, the message "The operation was successful" is displayed and the transaction details are returned. **Syntax**: arwfutil gss
sd	Shuts down the AuthMinder Server instance. You *must* enter the instance IP and the server management port number. After successful operation, the message "The operation was successful" is displayed and the transaction details are returned. **Syntax**: ■ arwfutil sd ■ arwfutil sd *<AuthMinder Server IP> <Server Management port>* **Example**: arwfutil sd localhost 9743

Option	Description
ssc	Sets the AuthMinder Server configuration. You need to provide the IP address of the AuthMinder Server and port number of the Server Management protocol. **Syntax**: arwfutil -i ssc *<AuthMinder Server IP> <Server Management port>* **Example**: arwfutil -i ssc localhost 9743 **Note:** It is recommended that you run this command in interactive mode. Otherwise, the server configurations that are set using this command cannot be used by the other commands.
Setup Validator Operations	
vah	Validates the ARCOT_HOME by computing hex-encoded MD5 of AuthMinder Server files. This command generates a file called arcotwebfort-vah-*<dd>-<mmm>-<yy>*.txt, which lists the MD5 of AuthMinder files. This file is available in the following directory: **For Windows**: <*install_location*>\Arcot Systems\logs **For UNIX-Based Platforms**: <*install_location*>/arcot/logs **Syntax**: arwfutil vah
vdb	Validates the AuthMinder database tables. This command generates a file called arcotwebfort-vdb-*<dd>-<mmm>-<yy>*.txt, which lists the AuthMinder database tables. This file is available in the following directory: **For Windows**: <*install_location*>\Arcot Systems\logs **For UNIX-Based Platforms**: <*install_location*>/arcot/logs **Syntax**: arwfutil vdb

Option	Description
vsetup	Validates the ARCOT_HOME by computing hex-encoded MD5 of AuthMinder Server files and the AuthMinder database tables. This command generates a file called arcotwebfort-setup-<*dd*>-<*mmm*>-<*yy*>.txt, which lists the MD5 of AuthMinder files and the database tables. This file is available in the following directory: **For Windows**: <*install_location*>\Arcot Systems\logs **For UNIX-Based Platforms**: <*install_location*>/arcot/logs **Syntax**: arwfutil vdb
Utility Operations	
??	Searches the commands based on the pattern you provide. For example, if you enter ?? ss, then all the commands that contain ss in their names are displayed. **Syntax**: arwfutil ?? <*seach text*> **Example**: arwfutil ?? SS The preceding command fetches the following options: ■ gss ■ ssc
?	Lists the commands supported by arwfserver. If you provide the command name along with this option, then the tool provides the help on command usage. **Syntax**: ■ arwfutil ? Lists all the supported commands ■ arwfutil ? <*command_option*> Provides help on the command usage. **Example**: arwfutil ? ssc Explains the usage of Set Server Configuration (SSC) command.

Option	Description
help	Provides the help on the command usage. **Syntax**: help <*command_option*> Provides help on the command usage. **Example**: arwfutil help ssc Explains the usage of Set Server Configuration (SSC) command.
q	Closes the interactive mode.
rai	Reads the additional input that you want to include when you invoke other commands. Before you run this command, you must add the additional input name-value pairs as follows: ■ 1. Navigate to the following location: **On Windows**: <*install_location*>\Arcot Systems\conf **On UNIX Platforms**: <*install_location*>/conf ■ 2. Open the arcotcommon.ini file in a text editor. ■ 3. Add a section called [arcot/webfort/tool/additionalInputs]. ■ 4. Include the name-value pairs in the section that you added in the preceding step. ■ 5. Save and close the arcotcommon.ini file. **Syntax**: rai

Chapter 12: Managing Reports

Based on your administrator level, reports enable you to summarize and analyze information in the AuthMinder database. For example, a report can tell a higher-level administrator which of their administrators accessed the system, at what times, and what activities were performed. Summary of Reports Available to All Administrators (see page 257) provides a summary of all reports that are available to the different administrators in a tabular format. The sections following Summary of Reports Available to All Administrators (see page 257) explain these reports:

- Administrator Reports (see page 258)
- AuthMinder Reports (see page 263)

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

- Date Range
- Administrator Name
- Organizations
- User Name

Generating Reports (see page 268) walks you through the generic process to generate activity reports for administrators and AuthMinder-specific reports.

You can also export all generated reports to a file. See Exporting Reports (see page 270) for information about the procedure.

Summary of Reports Available to All Administrators

The following table summarizes the reports in all categories (Administrator Reports and AuthMinder Reports) that are available to all administrators in the system. These reports are then covered in detail in the following sections.

Reports	Master Administrator	Global Administrator	Organization Administrator	User Administrator
Administrator Reports				
My Activity Report		✓	✓	✓
Administrator Activity Report		✓	✓	✓

Reports	Master Administrator	Global Administrator	Organization Administrator	User Administrator
User Activity Report			✓	✓
User Creation Report			✓	✓
Organization Report		✓	✓	✓
AuthMinder Reports				
Server Management Activity Report		✓		
Authentication Activity Report			✓	✓
Credential Management Activity Report			✓	✓
Configuration Management Report			✓	✓

Administrator Reports

All administrator reports available in the system include:

- My Activity Report (see page 259)
- Administrator Activity Report (see page 260)
- User Activity Report (see page 260)
- User Creation Report (see page 261)
- Organization Report (see page 262)

My Activity Report

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

Even though the logged-in administrator can view their activities by using the Administrator Activity Report (see page 260), this report is provided separately because:

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

The following table explains the fields of this report:

Report Field	Description
Date	The date and time of the activity.
Administrator ID	The name of the administrator who is generating the report.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	The unique ID generated for each activity performed by the administrator.
Event Type	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Status	The status of the action taken: ■ **Success** - If the action was completed successfully. ■ **Failure** - If the administrator failed to complete the action.
Reason	The reason why the operation failed.
User ID	The name of the user whose attributes were administered by the administrator.
Target Organization	The organization on which the activity was performed.
Component	The resource that was used to perform the task. The column values can be: ■ Administration Console ■ AuthMinder

Report Field	Description
Session ID	The session identifier of the Administration Console to which the administrator logged in.
Instance ID	The unique identifier for the Administration Console application instance, in case multiple instances of the application are running.

Administrator Activity Report

This report lists all activities that are performed by administrators belonging to the organizations that are in the scope of the administrator generating this report. By using this report, you can filter the activities of a specific administrator or view the activities for all the administrators of a single organization or multiple organizations. This report includes information such as, administrator login and logout timestamps, organization search, administrator account updates, and related details.

The fields of this report are same as My Activity Report. See My Activity Report (see page 259) for more information about the field details.

User Activity Report

This report lists all activities that are performed on user attributes, which include creating users, updating users, setting PAM, deleting users, update user status, and authenticating users. The report contains details such as, user name, status of the user, type of operations performed, and also the IP address of the user system.

The following table explains the fields of this report:

Report Field	Description
Date	The date and time of the activity.
User ID	The name of the user for whom the activity was performed.
Account Type	The account type associated with the organization to which the user belongs.
Account ID	The account ID of the user.
Event Type	The type of activity (such as, create, update, and delete user) performed by the administrator.
Organization	The organization name to which the user belongs.

Report Field	Description
Status	The status of the operation: ■ **Success** - If the operation was completed successfully. ■ **Failure** - If the user failed to complete the operation.
Transaction ID	The unique ID generated for every activity performed by the user.
Reason	The reason why the Operation failed.
Client IP Address	The IP address of the end user's system.
Caller ID	The unique identifier set by the calling application. **Note:** The Caller ID can be blank, if the calling application did not set the value.

User Creation Report

The User Creation Report displays details of the users that are created in the AuthMinder system.

The following table explains the fields of this report:

Report Field	Description
Date Created	The date and time when the user was created.
User ID	The name of the user who was created.
Organization	The organization name to which the user belongs.
User Status	The status of the user: ■ **Active** - If the user is an active user. ■ **Inactive** - If the user is deactivated. ■ **Initial** - If the user has been created, but not yet activated.
First Name	First name of the user.
Middle Name	Middle name of the user.
Last Name	Last name of the user.
Email Address	Email address of the user.
Telephone Number	Phone number of the user.

Organization Report

This report provides the details of all operations that are performed on the specified organization. Irrespective of any policies, this report displays *all* the activities in the organization under the administrator's purview.

The following table explains the fields of this report:

Report Field	Description
Date	The date and time of the activity.
Administrator Name	The name of the administrator who performed the activity.
Administrator Organization	The name of the organization to which the administrator belongs.
Transaction ID	The unique identifier generated for every activity performed by the administrator.
Event Type	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Status	The status of the action taken: ■ **Success** - If the action was completed successfully. ■ **Failure** - If the administrator failed to complete the action.
Reason	The reason why the operation failed.
Target User	The name of the user whose attributes were administered by the administrator.
Target Organization	The organization to which the user belongs.
Component	The resource that was used to perform the task. The column values can be: ■ Administration Console ■ AuthMinder
Session ID	The session identifier for the Administration Console to which the administrator logged in.
Instance ID	The unique identifier for the Administration Console application instance, in case multiple instances of the application are running.

AuthMinder Reports

Server Management Activity Report

This report lists the AuthMinder Server configurations made by the MA, and includes information about the activities that are related to log settings, database settings, protocol configurations, plug-in configurations, trusted certificate authority configurations, and server startup, shutdown, and refresh.

The following table explains the fields of this report:

Report Field	Description
Activity Time	The date and time of the activity.
Response Time (ms)	The time taken (in milliseconds) by the AuthMinder Server to process the request.
Instance Configuration	The details for all AuthMinder Server instance configurations. **Note:** To see the complete configuration details for an instance, hover the mouse on the column entry.
Instance Name	The name of the AuthMinder Server instance.
Instance Status	The status of the AuthMinder Server instance.
Operation	The type of activity performed (such as, create, read, modify, delete, or view) by the administrator.
Response Code	The status of the action taken: ■ **Success** - If the action was completed successfully. ■ **Failure** - If the administrator failed to complete the action.
Transaction ID	The unique identifier generated by the AuthMinder Server for the transaction.
Application IP	The IP address of the system where the calling application is hosted.
Caller ID	The unique identifier set by the calling application. **Note:** The Caller ID can be blank, if the calling application did not set the value.

Authentication Activity Report

This report provides a detailed list of the authentication activity of all users. It lists the authentication details, such as the type of credential used, validity of the credential, the number of times the OTP can be used, and number of times the user failed to authenticate.

The following table explains the fields of this report:

Report Field	Description
Activity Time	The date and time of the activity.
Response Time (ms)	The time taken (in milliseconds) by the AuthMinder Server to process the request.
Organization	The name of the organization to which the user belongs.
Input User ID	The unique identifier that is assigned for the user to track the operations performed by the user.
User Name	The ID of the user who performed the authentication activity.
Account ID	The account ID of the user.
Account Type	The account type associated with the organization to which the user belongs.
Credential Type	The type of credential that was used for authentication.
Credential Status	The status of the credential.
Validity Start Date	The timestamp from when the credential is considered to be valid.
Validity End Date	The timestamp when the credential expires.
Failed Attempts	The number of times the user failed to authenticate by using the credential.
Remaining Uses	The number of times for which the OTP can still be used for authentication. **Note:** This field is *not* applicable for other credentials.
Operation	The task that was performed by the AuthMinder Server to authenticate the user.
Response Code	The status of the action taken: ■ **Success** - If the action was completed successfully. ■ **Failure** - If the administrator failed to complete the action.
Reason Code	The reason why the Operation failed.
Token Type	The type of token that was returned after the authentication was successful.

Report Field	Description
Session ID	The session identifier for the Administration Console to which the current administrator is logged in.
Transaction ID	The unique identifier generated by the AuthMinder Server to track the transaction.
Protocol ID	The name of the protocol that was used to perform the activity.
Instance Name	The name of the AuthMinder Server instance that processed the request.
Application IP	The IP address of the system where the calling application is hosted.
Caller ID	The unique identifier set by the calling application in the AR_WF_CALLER_ID additional input.
User Agent	The user agent value as passed by calling application in the AR_WF_USER_AGENT additional input.
Referrer	The referrer value as passed by calling application in the AR_WF_REFERRER additional input.
Client Session ID	The identifier of the client session as passed in the AR_WF_CLIENT_SESSION_ID additional input.
Caller IP	The unique IP that is passed by calling application in the AR_WF_IP_ADDRESS additional input.

Credential Management Activity Report

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

The following table explains the fields of this report:

Report Field	Description
Activity Time	The date and time of the activity.
Response Time (ms)	The time taken (in milliseconds) by the AuthMinder Server to process the authentication request.
Organization	The name of the organization to which the user belongs.
Input UserID	The unique identifier that is assigned for the user to track the operations performed by the user.
User Name	The name of the user whose credential was updated.
Account ID	The account ID of the user.

Report Field	Description
Account Type	The account type associated with the organization to which the user belongs.
Credential Type	The type of credential that was affected (changed.) Possible values are: ■ ArcotID PKI ■ QnA ■ OTP ■ Password ■ OATH ■ ArcotID OTP-OATH ■ ArcotID OTP-EMV
Credential Status	The current state of the credential. Possible values are: ■ Active ■ Disabled ■ Verified ■ Locked
Validity Start Date	The timestamp from when the credential is considered to be valid.
Validity End Date	The timestamp when the credential expires.
Failed Attempts	The number of times the user failed to authenticate using the credential.
Remaining Uses	The number of times the OTP can still be used for authentication.
Operation	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.
Response Code	The status of the action taken: ■ **Success** - If the action was completed successfully. ■ **Failure** - If the administrator failed to complete the action.
Reason Code	The reason why the operation failed.
Transaction ID	The unique identifier generated by the AuthMinder Server to track the transaction.
Protocol ID	The name of the protocol that was used to perform the activity.
Instance Name	The name of the AuthMinder Server instance that processed the request.

Report Field	Description
Application IP	The IP address of the system where the calling application is hosted.
Caller ID	The unique identifier set by the calling application in the AR_WF_CALLER_ID additional input.
User Agent	The user agent value as passed by calling application in the AR_WF_USER_AGENT additional input.
Referrer	The referrer value as passed by calling application in the AR_WF_REFERRER additional input.
Client Session ID	The identifier of the client session as passed in the AR_WF_CLIENT_SESSION_ID additional input.
Caller IP	The IP address of the system from where the request originated.
Profile Name	The profile name associated with the credential using which the activity was performed.

Configuration Management Report

This report lists all the AuthMinder configurations that are made by the GA (or the OA.) It provides the configuration information of authentication policies, credential profiles, plug-in, SAML token, RADIUS client, and authentication challenge for ArcotID PKI and QnA.

The following table explains the fields of this report:

Report Field	Description
Activity Time	The date and time of the activity.
Administrator Name	The administrator who performed the configuration.
Administrator's Organization	The name of the organization to which the administrator belongs.
Session ID	The session identifier of the Administration Console to which the administrator logged in.
Target Organization	The organization for which the configurations are made.
Configuration Name	The name of the configuration.
Configuration Type	The type of configuration that was affected (changed.)
Operation	The type of activity (such as, create, read, modify, delete, or view) performed by the administrator.

Report Field	Description
Current Association Version	The current version of the configuration.
Previous Association Version	The previous version of the configuration.
Response Code	The status of the action taken: ■ **Success** - If the action was completed successfully. ■ **Failure** - If the administrator failed to complete the action.
Reason Code	The reason why the operation failed.
Transaction ID	The unique identifier generated by the AuthMinder Server for the transaction.
Instance Name	The instance name of the AuthMinder Server.
Application IP	The IP address of the system where the calling application is hosted.
Caller ID	The unique identifier set by the calling application in the AR_WF_CALLER_ID additional input.
User Agent	The user agent value as passed by calling application in the AR_WF_USER_AGENT additional input.
Referrer	The referrer value as passed by calling application in the AR_WF_REFERRER additional input.
Client Session ID	The identifier of the client session as passed in the AR_WF_CLIENT_SESSION_ID additional input.
Caller IP	The unique IP that is passed by calling application in the AR_WF_IP_ADDRESS additional input.

Generating Reports

This section covers:

- Notes for Generating Reports (see page 269)
- Generating the Report (see page 269)

Notes for Generating Reports

While generating reports, remember that:

- The administrator can *only* generate the reports of the organizations on which they have the scope.
- The administrator can generate the reports of their subordinates or peers. For example, an Organization Administrator (OA) can generate the reports of an OA and User Administrator (UA).
- If you are using Oracle Database, then ensure that you have enabled the UNLIMITED TABLESPACE permission.

Generating the Report

To generate any of the reports that are discussed earlier in the chapter:

1. Ensure that you are logged in with proper credentials (MA, GA, OA, or UA.)
2. Activate the Reports tab in the main menu.
3. If you want to generate:
   - Administrator activity report, then select the Administrator Reports submenu.
   - AuthMinder-specific report, then select the WebFort Reports submenu.

   The corresponding links for the report type appear in the left-handle task pane.
4. Based on the report you want to generate, click the required report link.
5. Specify the criteria to view the report:
   a. Enable the Decrypt Sensitive Information option if you want to view encrypted data in clear text.
   b. Specify one of the following:
      - The Date Range from the drop-down list.
      - A predefined date range in the From and To fields.
   c. From the Organization Name list, select the required organizations whose data you want to include in the report.
   d. In the User Name field, based on the report you want to generate, perform one of the following steps:
      - Enter a user name (for Authentication Activity and Credential Management reports.)
      - Enter the administrator name (for configuration reports.)
6. Click **Display Report** to generate the report based on the criteria you specified.

Exporting Reports

The Administration Console provides the ability to export reports to a file. By exporting a report, you can save a local copy of a report, which enables you to track trends. You can also work with the saved report data in another application.

The exported reports are generated in the comma-separated value (CSV) format that can be viewed by using text editors and spreadsheet applications, such as Microsoft Excel. The export option is available through the **Export** button, which appears at the top-right of every rendered report.

To export a report to a local file:

1. Generate the required report. See "Generating the Report" (see page 269) for detailed instructions.

   The report opens.

2. Click **Export**.

   You are prompted to save or open the report.

3. Click **Open** or **Save**. If you click Save, then specify the download location.

   The file can be viewed by using the appropriate application.

arreporttool: Report Download Tool

The arreporttool enables you to export reports in the comma-separated value (CSV) format from the command line. You can then view these reports by using text editors and spreadsheet applications, such as Microsoft Excel.

Using the Tool

The arreporttool.jar file is available at the following location:

On Windows:

`<install_location>\Arcot Systems\tools\common\arreporttool`

On UNIX Platforms:

`<install_location>/arcot/tools/common/arreporttool`

Syntax:

Run the following command to use the tool:

```
java -jar arreporttool.jar –-protocol <protocol> --host <host>
--port <app_server_port> --admin-orgid <admin-organization>
--admin-id <admin-user-id> --admin-password <password>
[--report-type hour | day | month [duration] | range]
--report-id <Report ID> --reporturl <Url of the report>
--is-filter-req <true | false> --data-type <Data Type>
--reportdata [Report Data] --start-date-time <date-and-time> [--end-date-time
<date-andtime>] [--logfile <logfile>]
[--log-level <loglevel>][log-file-max-size] <logfilesize>] [--organizations <target
orgNames>] [--userName <User/Admin Name>] [--output-file <output-file>.CSV]
[--is-url-encoded [true|false]]
```

The following table lists the options that are supported by the tool:

Option	Description
protocol	The protocol being used for communication. The possible values are http and https. The default protocol is http.
host	The host name or the IP address of the system where you have deployed the Administration Console.
app_server_port	The port at which the Console is listening.
admin-orgid	The organization to which the administrator belongs.
admin-id	The unique administrator ID.
admin-password	The administrator password
report-type	Specify hour, day, month, or range. ■ Hour, day, month can be followed by a numeric number. For example, --report-type day 2 indicates two days of records from the start-date-time specified. ■ Range: If range is specified, enter an end-date-time.
report-id	Identifier of the report to be fetched. See "List of Report Identifiers" (see page 273) for the list of report identifiers that you can use.
reporturl	Administrator URL of the report. See "List of Report URLs" (see page 273) for the list of report URLs that you can use.
is-filter-req	This is true by default. Set this value to false for reports that do not have a filter page, for example, AuthMinder reports.
data-type	This is applicable only for AuthMinder reports to specify ACTIVE or STAGING.

Option	Description
reportdata	In addition to start and end dates, certain reports need additional filters. These additional filters can be specified as report data. The report data must be in the 'key=value' format. You can use a semicolon to separate multiple key-value pairs. The report data must be URL-encoded if it contains ; or =. Ensure that you set the is-url-encoded parameter to true if URL-encoded value is passed.
start-date-time	Specify the date or time after which report content must be fetched. **Format**: MM/dd/yyyy HH:mm:ss Hour (HH) and Minutes (mm) are optional and are used only for hourly reports. For daily and monthly reports, only the date part is used. By default, the TimeZone is in GMT. **Example**: 03/21/2010 09:10:20
end-date-time	[Optional] Specify the end date and time till which the report content should be selected.
logfile	[Optional] Specify the location of the log file. If no log file is specified, the **arreporttool.log** file is automatically created in the current directory.
log-level	[Optional] Specify the log level. Default log level is INFO.
log-file-max-size	[Optional] Specify the maximum size of the log file. The default value is 10MB.
organizations	[Optional] Specify semicolon-separated target organization names for the report. You *must* specify this value for reports that have organizations as a mandatory parameter. The value must be URL-encoded if the organization name contains a semicolon(;). Ensure that you set the is-url-encoded parameter to true if a URL-encoded value is passed.
userName	[Optional] Specify the user or administrator name.
output-file	[Optional] Specify the output file where the report content must be written. If no file name is specified, **<reporttype>-timestamp.CSV** is used.
is-url-encoded	[Optional] Set this value to true or false depending on whether your report data and organizations contain URL-encoded information. The default value is false.

List of Report Identifiers

The following table shows the various report identifiers that you can use for the report-id argument:

Report	Report ID
My Activity Report	AAC.ViewMyActivityReport
Administrator Activity Report	AAC.ViewActivityReport
User Activity Report	AAC.ViewUserActivityReport
Organization Report	AAC.ViewOrgActivityReport

List of Report URLs

The following table shows the various report URLs that you can use for the reporturl argument:

Report	Report URL
My Activity Report	/Ac_AdminMyActivity/view.htm
Administrator Activity Report	/Ac_Adminreport/view.htm
User Activity Report	/Ac_AdminUserActivity/view.htm
Organization Report	/Ac_AdminOrgActivity/view.htm

Examples of Using the Tool

The following is the code snippet for downloading the User Activity Report:

```
java –jar arreporttool.jar --protocol http --host localhost --port
8080
-- admin-org-id arcot --admin-id ga --admin-password ga123
--report-id AAC.ViewUserActivityReport --report-url
/Ac_AdminUserActivity/view.htm --startdate-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log -- organizations
ARCOT –-userName ua
```

The following is the code snippet for downloading the Organization Report:

```
java -jar arreporttool.jar --protocol http --host localhost --port
8080 -- admin-org-id arcot --admin-id ga --admin-password ga123
--report-id AAC.ViewOrgActivityReport –report-url
/Ac_AdminOrgActivity/view.htm --start-date-time "01/01/2012"
--end-date-time "01/30/2012" --log-file C:/tool.log --organizations
ARCOT;TEST
```

Appendix A: AuthMinder Logging

To effectively manage communication between the AuthMinder Server and your application, you need information about the activity and performance of the Server and also about any problems that may have occurred.

This appendix covers the following topics:

About the Log Files

The AuthMinder log files can be categorized as:

- Installation Log File (see page 277)
- AuthMinder Server Startup Log File (see page 277)
- AuthMinder Server Log File (see page 278)
- UDS Log File (see page 279)
- Administration Console Log File (see page 280)

The parameters that control logging in these files can be configured either by using the relevant INI files (as is the case with Administration Console, UDS, and AuthMinder Server startup log files) or by using the Administration Console itself (as is the case with AuthMinder log file.) The typical logging configuration options that you can change in these files include:

- **Specifying log file name and path:** AuthMinder enables you to specify the directory for writing the log files and storing the backup log files. Specifying the diagnostic logging directory allows administrators to manage system and network resources.
- **Log file size:** The maximum number of bytes the log file can contain. When the log files reach this size, a new file is created and the old file is moved to the backup directory.
- **Using log file archiving:** As AuthMinder components run and generate diagnostic messages, the size of the log files increases. If you allow the log files to keep increasing in size, then the administrator must monitor and clean up the log files manually. AuthMinder enables you to specify configuration options that limit how much log file data is collected and saved. AuthMinder lets you specify the configuration option to control the size of diagnostic logging files. This lets you determine a maximum size for the log files. When the maximum size is reached, older log information is moved to the backup file before the newer log information is saved.
- **Setting logging levels:** AuthMinder also allows you to configure logging levels. By configuring logging levels, the number of messages that are saved to diagnostic log files can be reduced or increased. For example, you can set the logging level so that the system only reports and saves critical messages. See "Supported Severity Levels" (see page 282) for more information about the supported log levels.
- **Specifying time zone information:** AuthMinder enables you to either use the local time zone for time stamping the logged information or use GMT for the same.

Installation Log File

When you install AuthMinder, the installer records all the information that you supply during the installation and the actions (such as creating the AuthMinder directory structure and making registry entries) that it performs in the Arcot_WebFort_Install_*[assign the value for mm in your book]*_<dd>_<yyyy>_<hh>_*[assign the value for mm in your book]*_*SpectroSERVER*.log file. The information in this file is very useful in identifying the source of the issue if the AuthMinder installation was not completed successfully.

The default location of this file is:

Windows:

<install_location>\

UNIX-Based Platforms:

<install_location>/

AuthMinder Server Startup Log File

When you start the AuthMinder Server, it records all start-up (or boot) actions in the arcotwebfortstartup.log file. The information in this file is useful in identifying the source of the issue if the AuthMinder service does not start up.

The default location of this file is:

Windows:

<install_location>\Arcot Systems\logs\

UNIX-Based:

<install_location>/arcot/logs/

AuthMinder Server Log File

When you perform AuthMinder Server configurations, for example, protocol configurations and profile configurations, such configurations are written to the arcotwebfort.log file. The default location of this file is:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

The parameters that control logging in this file can be configured by using the Administration Console. To do so, use the instance-specific configuration sub-screen that you can access by clicking the required instance in the **Instance Management** screen.

In addition to the log file path, the maximum log file size (in bytes), backup directory, logging level, and timestamp information, you can also control whether you want to enable trace logging. See Format of the AuthMinder Log Files (see page 281) for information about the default format that is used in the file.

UDS Log File

All User Data Service (UDS) information and actions are recorded in the arcotuds.log file. This information includes:

- UDS database connectivity information
- UDS database configuration information
- UDS instance information and the actions that are performed by this instance

The information in this file is useful in identifying the source of the problems if the Administration Console could not connect to the UDS instance. The default location of this file is:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

The parameters that control logging in this file can be configured by using the udsserver.ini file, which is available in the conf folder in ARCOT_HOME.

In addition to the logging level, log file name and path, the maximum file size (in bytes), and archiving information, you can also control the layout of the logging pattern for UDS by specifying the appropriate values for log4j.appender.debuglog.layout.ConversionPattern. See Format of UDS and Administration Console Log Files (see page 282) for information about the default format used in the file.

Administration Console Log File

When you deploy the Administration Console and then start it, the details of all its actions and processed requests are recorded in the arcotadmin.log file. This information includes:

- Database connectivity information
- Database configuration information
- Instance information and the actions that are performed by this instance
- UDS configuration information
- Other Administration Console information that is specified by the Master Administrator, such as cache refresh

The information in this file is very useful in identifying the source of the problems if the Administration Console does not start up. The default location of this file is:

Windows:

`<install_location>\Arcot Systems\logs\`

UNIX-Based:

`<install_location>/arcot/logs/`

The parameters that control logging in this file can be configured by using the adminserver.ini file, which is available in the conf folder in ARCOT_HOME.

In addition to the logging level, log file name and path, the maximum log file size (in bytes), and log file archiving information, you can also control the layout of the logging pattern for the Console by specifying the appropriate values for log4j.appender.debuglog.layout.ConversionPattern. See "Format of UDS and Administration Console Log Files" (see page 282) for information about the default format used in the file.

Format of the AuthMinder Log Files

The following table describes the format of the entries in the following AuthMinder loggers:

- arcotwebfort.log (AuthMinder Server Log File (see page 278))
- arcotwebfortstartup.log (AuthMinder Server Startup Log File (see page 277))

Column	Description
Time Stamp	The time when the entry was logged, translated to the time zone you configured. The format of logging this information is: mm/dd/yy HH:MM:SS.mis Here, mis represents milliseconds.
Log Level (LEVEL) (or Severity)	The severity level of the logged entry. See "Supported Severity Levels" (see page 282) for more information. **Note:** AuthMinder also provides trace logging, which contains the flow details. The trace logs are logged in the arcotwebfort.log file. The entries for the trace messages start with TRACE.
Protocol Name (PROTOCOLNAME)	The protocol used for the transaction. Possible values are: ■ TXN_NATIVE ■ ADMIN_WS ■ ASSP_WS ■ RADIUS ■ SVRMGMT_WS ■ TXN_WS In case the server is starting up, shutting down, or is in the monitoring mode, then no protocol is used and the following values are displayed, respectively: ■ STARTUP ■ SHUTDOWN ■ MONITOR
Thread ID (THREADID)	The ID of the thread that logged the entry.
Transaction ID (000TXNID)	The ID of the transaction that logged the entry.
Message	The message logged by the Server in the log file in the free-flowing format. **Note:** The granularity of the message depends on the **Log Level** that you set in the log file.

Format of UDS and Administration Console Log Files

The following table describes the format of the entries in the following loggers:

- arcotuds.log (UDS Log File (see page 279))
- arcotadmin.log (Administration Console Log File (see page 280))

Column	Associated Pattern (In the Log File)	Description
Time Stamp	%d{yyyy-MM-dd hh:mm:ss,SSS z} :	The time when the entry was logged. This entry uses the application server time zone. The format of logging this information is: yyyy-MM-dd hh:mm:ss,SSS z Here, SSS represents milliseconds.
Thread ID	[%t] :	The ID of the thread that logged the entry.
Log Level (or Severity)	%-5p :	The severity level of the logged entry. See Supported Severity Levels (see page 282) for more information.
Logger Class	%-5c{3}(%L) :	The name of the logger that made the log request.
Message	%m%n :	The message logged by the Server in the log file in the free-flowing format. **NOTE:** The granularity of the message depends on the **Log Level** that you set in the log file.

See the following URL for customizing the **PatternLayout** parameter in the UDS and Administration Console log files:

http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html

Supported Severity Levels

A *log level* (or *severity level*) enables you to specify the level of detail of the information that is stored in the AuthMinder logs. This also enables you to control the rate at which the log file grows.

Server Log File Security Levels

The following table describes the log levels that you see in all log files, in *decreasing* order of severity:

Log Level		Description
0	FATAL	Use this log level for serious, non-recoverable errors that can cause the abrupt termination of the AuthMinder service.
1	WARNING	Use this log level for undesirable run-time exceptions, potentially harmful situations, and recoverable problems that are not yet FATAL.
2	INFO	Use this log level for capturing information about run-time events. In other words, this information highlights the progress of the application, which might include changes in: ■ Server state, such as start, stop, and restart. ■ Server properties. ■ State of services. ■ State of processes on the Server.
3	DEBUG	Use this log level for logging detailed information for debugging purposes. This might include process tracing and changes in Server states.

Note: For AuthMinder Server (arcotwebfort.log), you can set logging to any of these levels and also enable TRACE logging to capture flow details.

Note: When you specify a log level, messages from all other levels of *higher* significance are also reported. For example, if the LogLevel is specified as 3, then messages with log levels of FATAL, WARNING, and INFO level are also captured.

Administration Console and UDS Log File Severity Levels

The following table describes the log levels that you see in Administration Console and UDS log files, in *decreasing* order of severity.

Log Level		Description
0	OFF	Use this level to disable all logging.
1	FATAL	Use this log level for serious, non-recoverable errors that can cause the abrupt termination of Administration Console or UDS.

Log Level		Description
2	WARNING	Use this log level for undesirable run-time exceptions, potentially harmful situations, and recoverable problems that are not yet FATAL.
3	ERROR	Use this log level for recording error events that might still allow the application to continue running.
4	INFO	Use this log level for capturing information about run-time events. In other words, this information highlights the progress of the application, which might include changes in: ■ Server state, such as start, stop, and restart. ■ Server properties. ■ State of services. ■ State of processes on the Server.
5	TRACE	Use this log level for capturing finer-grained informational events than DEBUG.
6	DEBUG	Use this log level for logging detailed information for debugging purposes. This might include process tracing and changes in Server states.
7	ALL	Use this log level to enable all logging.

Note: When you specify a log level, messages from all other levels of *higher* significance are also reported. For example, if the LogLevel is specified as 4, then messages with log levels of FATAL, WARNING, ERROR, and INFO are also captured.

Sample Entries for Each Log Level

The following subsections show a few sample entries (based on the Log Level) in the AuthMinder log file.

FATAL

```
07/17/09 11:49:20.404  FATAL  STARTUP  00002872  00WFMAIN - Unable to
initialize the database

07/17/09 11:49:20.405  FATAL  STARTUP  00002872  00WFMAIN - Failed to
load the ini parameters

07/17/09 11:49:20.406  FATAL  STARTUP  00002872  00WFMAIN - Cannot
continue due to setConfigData failure, SHUTTING DOWN
```

WARNING

```
07/17/09 12:50:05.848  INFO  AUTH_NATIVE  00002780  00022508 - Fail
to connect to Database prdsn for 1 time(s). DbUsername system

07/17/09 12:50:05.848  INFO  AUTH_NATIVE  00002780  00022508 -
ReportError: SQL Error State:08001, Native Error Code: FFFFFFFF, ODBC
Error: [Arcot Systems][ODBC Oracle Wire Protocol
driver][Oracle]TNS-12505: TNS:listener could not resolve SID given in
connect descriptor
```

INFO

```
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mMinConnections [4]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mMaxConnections [128]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mCurrPoolSize   [4]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mNumDBFailure     [0]
07/17/09 11:51:20.166 INFO MONITOR 00000424 STATSMON - mCurrNumUsed
[0]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON -
mCurrNumAvailable [4]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [0]
mNumTimesConnIdxLocked   [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [0]
mNumTimesConnIdxReleased [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [1]
mNumTimesConnIdxLocked   [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [1]
mNumTimesConnIdxReleased [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [2]
mNumTimesConnIdxLocked   [24]
```

```
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [2]
mNumTimesConnIdxReleased [24]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [3]
mNumTimesConnIdxLocked   [23]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - idx [3]
mNumTimesConnIdxReleased [23]
07/17/09 11:51:20.166  INFO  MONITOR  00000424  STATSMON - ----------
logging stats for databse [wf-test-p] : [primary] [ACTIVE] end
----------
```

DEBUG

```
03/25/10 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBPoolManagerImpl::getLockedDBConnection: [primary] DSN [webfort]
is active. Will get the connection from this
03/25/10 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBPoolManagerImpl::getLockedDBConnection: Returning DBPool
[0112FD80]
03/25/10 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBM::Number of queries being executed [1]
03/25/10 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBM::Found query string for query-id : [SSL_TRUST_STORE_FETCH_ALL].
03/25/10 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 -
ArDBM::Executing Query[ArWFSSLTrustStoreQuery_FetchAll]
03/25/10 15:29:30.921 DEBUG SVRMGMT_WS   00000536 00000620 - Number
of rows fetched : 0
```

(For AuthMinder Server *Only*) Trace Logs

```
03/25/10 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
Released Cache read lock on [01129D98]
03/25/10 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
CallTrace::Leaving : [ArDBPoolManagerImpl::selectAnActivePool].
time : 0
03/25/10 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
CallTrace::Entering : [ArDBPool::getLockedDBConnectionConst]
03/25/10 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
ArDBPool::getLockedDBConnection [(primary)] : GotContext [1], [3]
more connections available
03/25/10 15:23:38.515 DEBUG SVRMGMT_WS   00004396 00000596 - TRACE:
CallTrace::Leaving : [ArDBPool::getLockedDBConnectionConst]. time :
0
```

Appendix B: Multi-Byte Characters and Encrypted Parameters

AuthMinder now supports UTF-8, which is the variable width 8-bit encoding format of the universal Unicode encoding scheme.

Note: For information about configuring UTF-8, see "Configure UTF-8 Support on Client Systems" in the *CA AuthMinder Installation and Deployment Guide*.

AuthMinder also enables you to use hardware- or software-based encryption of sensitive data. You can choose to encrypt sensitive parameters and also decide whether you want to display clear text data or encrypted data in Reports.

The following table lists the user and credential parameters that can be selected for encryption and multi-byte character encoding. It also lists the keys that are used for the parameter and the level at which the key is applicable.

Note: Any of the keys that are listed in the Key Type column of this table can be stored in the HSM.

Parameter	Multi-byte	Encrypted	Salt Added	Key Level	Key Type	Case-Sensitive
User Name	Yes	Optional	No	Organization level	Organization key	Yes
User Attributes	Yes	Optional	No	Organization level	Organization key	Yes
Password	Yes	Yes	Yes	Organization level	Organization key	No
One-Time Password	No	Yes	Yes	Organization level	Organization key	No
OATH Seed	No	Yes	Yes	Organization level	OATH Master Key	No
OATH OTP	No	No	No	NA	NA	No
ArcotOTP OATH Seed	No	Yes	Yes	Organization level	ArcotOTP OATH Master Key	No
ArcotOTP OATH OTP	No	No	No	NA	NA	No

Parameter	Multi-byte	Encrypted	Salt Added	Key Level	Key Type	Case-Sensitive
ArcotOTP EMV Seed	No	Yes	Yes	Organization level	ArcotOTP EMV Master Key	No
ArcotOTP EMV OTP	No	No	No	NA	NA	No
QnA Questions	Yes	Yes	Yes	Organization level	Organization key	Yes
QnA Answers	Yes	Yes	Yes	Organization level	Organization key	Yes
ArcotID Key Secret	No	Yes	Yes	Organization level	Organization key	No
ArcotID Primary Key	No	Yes	Yes	Organization level	ArcotID Master key	No
One-Time Token	No	Yes	Yes	Organization level	Global Key	No
Account ID for EMV	Yes	Yes	Yes	Organization level	Organization key	Yes
Transient Data Encryption Key	No	Yes	No	Global level	Global key	No
Native Token	No	Yes	No	Global level	Transient data encryption key	No
Password Challenge	No	Yes	Yes	Global level	Transient data encryption key	No
ArcotID Challenge	No	Yes	No	Global level	Transient data encryption key	No

Parameter	Multi-byte	Encrypted	Salt Added	Key Level	Key Type	Case-Sensitive
QnA Question ID	No	Yes	No	Global level	Transient data encryption key	No
Credential Custom Attributes	Yes	Yes	No	Organization level	Organization key	Yes

The following table lists the configuration parameters that can be selected for encryption and multi-byte character encoding. It also lists the keys that are used for the parameter and the level at which the key is applicable.

Note: Any of the keys that are listed in the Key Type column of this table can be stored in the HSM.

Parameter	Multi-byte	Encrypted	Salt Added	Key Level	Key Type	Case-Sensitive
OATH Seed in the Uploaded Token	No	Yes	Yes	Global level	Global key	No
	No	Yes	Yes	Organization level	Organization key	No
RADIUS Shared Secret	No	Yes	Yes	Global level	Global key	No
	No	Yes	Yes	Organization level	Organization key	No
SAML Signing Key	No	Yes	Yes	Global level	Global key	No
	No	Yes	Yes	Organization level	Organization key	No
ASSP SAML Signing Key	No	Yes	Yes	Global level	Global key	No
	No	Yes	Yes	Organization level	Organization key	No
ASSP Kerberos Credentials	Yes	Yes	Yes	Global level	Global key	No
	Yes	Yes	Yes	Organization level	Organization key	No
ArcotID CA Key	No	Yes	No	Global level	Global key	No
ArcotID Master	No	Yes	Yes	Global level	Global key	No

Parameter	Multi-byte	Encrypted	Salt Added	Key Level	Key Type	Case-Sensitive
Key	No	Yes	Yes	Organization level	Organization key	No
OATH OTP Master Key	No	Yes	Yes	Global level	Global key	No
	No	Yes	Yes	Organization level	Organization key	No
ArcotOTP OATH OTP Master Key	No	Yes	Yes	Global level	Global key	No
	No	Yes	Yes	Organization level	Organization key	No
ArcotOTP EMV OTP Master Key	No	Yes	Yes	Global level	Global key	No
	No	Yes	Yes	Organization level	Organization key	No
SSL Signing Key	No	Yes	Yes	Global level	Global key	No
Messages	Yes	No	No	NA	NA	Yes
Display Name	Yes	No	No	NA	NA	Yes
Audit - Reason	Yes	No	No	NA	NA	No
Audit - Event Message	Yes	No	No	NA	NA	No
Audit - Internal Additional Information	Yes	No	No	NA	NA	No
Audit - External Additional Information	Yes	No	No	NA	NA	No
User Attribute Check	Yes	No	No	NA	NA	No

Appendix C: Summary of Server Refresh and Restart Tasks

Many configuration changes that you make may need the server to be restarted. For example, all .ini file changes need the server to be restarted. Also, some changes that are made by using Administration Console also require the server to be either restarted or refreshed. In such cases, the Administration Console prompts you to refresh or restart, as applicable.

Note: The refresh option ensures that the server does not require any downtime.

The following table lists various server tasks that either need to be refreshed or restarted after you have made any configuration changes:

Task	Refresh	Restart
Configure UDS Connectivity	✓	
Configure UDS	✓	
Configure Attribute Encryption	✓	
Configure Custom Locales	✓	
Set Default Organization	✓	
Add Account Type	✓	
Update Account Type	✓	
Delete Account Type	✓	
Add Custom Attributes for Account Type	✓	
Configure Email/Telephone Type	✓	
Configure Basic Authentication Policy	✓	
Enable Authentication and Authorization For Web Services	✓	
AuthMinder Connectivity		✓
Updates to following operations using Instance Management page: ■ Log Level ■ Enable Trace Logging ■ Log Query Details	✓	

Task	Refresh	Restart
Updates to following operations using Instance Management page: ■ Instance Attributes ■ Transaction Log Directory ■ Rollover After ■ Transaction Log Backup Directory ■ Log Timestamps in GMT ■ Database Configurations		✓
Trusted Certificate Authorities	✓	
Protocol Management	✓	✓
Updates to **General** configurations using Miscellaneous Configurations page	✓	
Updates to **Change Authentication Mechanism Status** using Miscellaneous Configurations page		✓
Profile Configurations	✓	
Policy Configurations	✓	
Credential Key Management	✓	
SAML Token Configurations	✓	
ASSP Configurations	✓	
Credential Type Resolution	✓	
Plug-In Registration	✓	✓
Plug-In Configurations	✓	
Assign Default Configurations	✓	
RADIUS Client	✓	
RADIUS Proxy	✓	

Appendix D: Configuring SSL

By default, AuthMinder components use Transmission Control Protocol (TCP) to communicate with each other. To ensure secure communication between Administration Console and AuthMinder Server and between SDKs and AuthMinder Server, you can configure Server Management and Transaction Native protocols to support SSL (Secure Sockets Layer), which ensures secure communication between applications across insecure media.

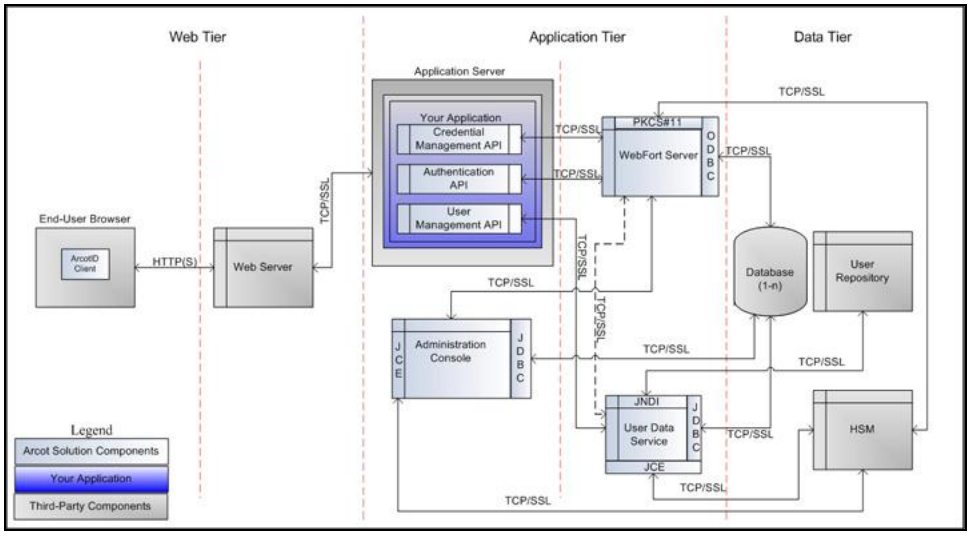
The following sections list how to set up SSL between different AuthMinder components:

Note: After you set up SSL between the components, test whether the connection has been set successfully.

- AuthMinder Components and Their Communication Modes (see page 294)
- Prepare for SSL Communication (see page 295)
- Enable SSL Between AuthMinder Server and User Data Service (see page 301)
- Enable SSL Between Administration Console and AuthMinder Server (see page 304)
- Enable SSL Between Java SDKs and AuthMinder Server (see page 309)
- Enable SSL Between Transaction Web Services and AuthMinder Server (see page 315)
- Enable SSL Between arwfutil and AuthMinder Server (see page 319)
- Enable One-Way SSL Between AuthMinder Components and Database (see page 325)

AuthMinder Components and Their Communication Modes

The following figure illustrates the possible communication modes that are supported between AuthMinder and its components.



As shown in this figure, the default mode of communication between components is TCP, AuthMinder Server supports SSL communication (two-way and one-way) with the following components to ensure integrity and confidentiality of the data being exchanged during a transaction:

- Administration Console
- User Data Service
- AuthMinder Database (One-way *only*)
- AuthMinder Java SDKs (Authentication and Issuance)
- AuthMinder Web Services (Authentication and Issuance)

Prepare for SSL Communication

To enable SSL communication between the AuthMinder components, you must first obtain server and client certificates. You can obtain these certificates by using one of the following methods:

- Directly Through a Certificate Authority (CA) (see page 296)
- Using a Utility to Generate Certificate Request (see page 300)

When a CA generates a certificate for you (as discussed in the section, "Directly Through a Certificate Authority (CA)" (see page 296)), they also generate the private key that is associated with the certificate. As a result, the private key may not be as secure as when it is generated at your site. If you do not want the key to be generated "off site", then follow the steps that are described in Using a Utility to Generate Certificate Request (see page 300).

Directly Through a Certificate Authority (CA)

The steps that are explained in this section are specific to **Microsoft CA 2008**. If you are using any other CA to generate the certificate and the private key, then see the vendor documentation.

To generate a CA-issued certificate:

1. Access the link to the CA of your choice. For Microsoft CA, it is as follows:

   http://<IP_Address_of_the_CA>/certsrv/

2. Navigate to the link to create and submit the certificate request.

   For example, if you are using **MSCA**, then under **Select a task** section, click the **Request a certificate** option, then **advanced certificate request** option, and then finally the **Create and submit a request to this CA** option.

3. Specify the details on the certificate request form that appears.

   - The identification information for the certificate, as discussed in the following table:

Certificate Attribute	Required Information
Common Name (Name)	The fully qualified domain name (FQDN) of your server. When prompted for Common Name, you *must* specify the Fully Qualified Domain Name (FQDN) of the server to be protected by SSL. For example, an SSL certificate issued for login.my-bank.com will *not* be valid for online.my-partner.com. If the URL to be used for SSL is login.my-bank.com, then ensure that the common name submitted in the CSR is login.my-bank.com.
Email Address	The email ID of the contact person in your organization. Typically, this is the email address of the certificate administrator or an administrator in the IT department.
Organization (Company)	The name of your organization. Ensure that this entry is *not* abbreviated. You must also ensure that you do not specify any suffixes, such as Inc., Corp., or LLC.
Organizational Unit (Department)	The division (for example, IT) of your Organization handling the certificate.

Certificate Attribute	Required Information
City (Locality)	The city (for example, Brisbane) where your Organizational Unit is located.
State	The state or region (for example, Queensland) where your Organizational Unit is located. Ensure that this entry is not abbreviated.
Country (Region)	The ISO code (for example, AU) for the country where your organization is headquartered.

- The details of the certificate. Consider the details that are specified in the following table while specifying these certificate details.

Certificate Attribute	Required Information
Certificate Type	**Server Authentication Certificate**, if you are generating a server certificate. **Client Authentication Certificate**, if you are generating a client certificate.
CSP	CSP of your choice.
Key Usage	Choose the key usage type as **Exchange**.
Key Size	The key size in bytes.
Key Exportability	Select **Mark keys as exportable**.
Request Format	Specify the format in which you want to download the certificate.

4. Click **Submit** to request the certificate.
5. Click **Install the Certificate** link to install the certificate in the browser store.

Download Certificates

The certificates that you have requested using MS CA 2008 are installed in the browser store from where you have to download them. The format in which you have to download the certificate depends on the encryption mode. If software encryption is used, then certificates must be in PKCS#12 format. If hardware encryption is used, then certificates must be PEM format.

In PKCS#12 Format

Perform the following steps to download the certificate and private key to a PKCS#12 file using Microsoft CA 2008:

1. Open an Internet Explorer window.
2. Navigate to **Tools** and then **Internet Options**.

   The Internet Options dialog appears.
3. Activate the **Content** tab, in the Certificates section click **Certificates**.

   The Certificates dialog appears.
4. Select the certificate that you want to download and click **Export**.

   The Certificate Export Wizard appears.
5. Click **Next** on the Welcome screen.
6. Choose **Yes, export the private key** option and then **Next**.
7. Ensure that the **Personal Information Exchange - PKCS # 12 (.PFX)** option is selected.
8. Select **Enable Strong Protection,** and click **Next**.
9. Enter the password for the PKCS#12 (.PFX) file in **Password** and **Confirm password** fields and click **Next**.
10. Enter the **File name** with which you want to download the PKCS#12 (.PFX) file and click **Next**.
11. Click **Finish** to complete the wizard.

    The certificate and private key is now available on your system in the specified location.

In PEM Format

You cannot directly export the certificate in PEM format from the browser certificate store, therefore you must first download it in DER format and then convert to PEM.

Preform the following steps to download certificate in DER format using Microsoft CA 2008, and then convert it to PEM:

1. Open an Internet Explorer window.
2. Navigate to **Tools** and then **Internet Options**.

   The Internet Options dialog appears.
3. Activate the **Content** tab, in the Certificates section click **Certificates**.

   The Certificates dialog appears.
4. Select the certificate that you want to download and click **Export**.

   The Certificate Export Wizard appears.
5. Click **Next** on the Welcome screen.
6. Choose **No, do not export the private key** option and then **Next**.
7. Ensure that the **DER encoded binary X.509 (.CER)** option is selected.
8. Click **Next**.
9. Enter the **File name** with which you want to download the certificate and click **Next**.
10. Click **Finish** to complete the wizard.

    The certificate is now available on your system in the specified location.
11. Convert the certificate from DER to PEM format. You can use open source tools such as OpenSSL. Use the following command to convert using OpenSSL tool:

    openssl x509 -inform der -in <*certificate*>.cer -out <*certificate*>.pem

Using a Utility to Generate Certificate Request

You can also generate a certificate request by using any utility or tool of your choice, and then submit it to CA for obtaining the certificate. The keytool utility (which is available with JDK) has been used for the following operations:

1. Generate the keystore.

   keytool stores the keys and certificates in a file termed as *keystore*, which is a repository of certificates used for identifying a client or a server. Typically, a keystore is specific to one client or one server. The default keystore implementation implements the keystore as a file. It protects private keys by using a password. The keystores are created in the directory from which you run keytool.

   Use the following command to generate the keystore:
   `%JAVA_HOME%/bin/keytool -genkey -keyalg RSA -alias <server/or/client> -keystore <keystore_name>.jks -storetype JKS -storepass <password> -keysize 1024 -validity <validity_period_in_days>`

2. Generate the Certificate Signing Request (CSR).

   CSR is encrypted identification text, and must be generated on the system where the certificate will be used. A private key is usually created at the same time that you create the CSR.

   Use the following command to generate the CSR:
   `%JAVA_HOME%/bin/keytool -certreq -v -alias <server/or/client> -keystore <keystore_name>.jks -storepass <password> -file <server/or/client>certreq.csr`

3. Generate the certificate by submitting the CSR generated in the preceding step to a CA.

   a. Access the link to the CA of your choice.

      For example, if you are using **MSCA**, then the link will be similar to:

      http://<IP_Address_of_the_CA>/certsrv/

   b. Navigate to the link to create and submit the certificate request.

      For example, if you are using **MSCA**, then under **Select a task** section, click the **Request a certificate** option, then **advanced certificate request** option, and then the **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file** option (or if you are renewing the certificate, then submit a renewal request by using a base-64-encoded PKCS #7 file). Finally, copy and paste the contents of *<server/or/client>*certreq.csr in the **Base-64-encoded certificate request** field and click **Submit**.

   c. Download the following files in the DER-encoded format:

      - Signed certificate as *<server/or/client>*cert.cer
      - Complete certficate chain as *<server/or/client>*cert.p7b
      - CA certficate as *<server/or/client>*cacert.cer

4. Import the certificate chain into the keystore.

   Use the following command to do so:
   `%JAVA_HOME%/bin/keytool -import -keystore <server/or/client>keystore.jks -storepass <password> -file <server/or/client>certchain.p7b -alias <server/or/client>`

5. Convert the certificates or keystore to the required formats using open source tools such as OpenSSL.

   - From DER Format

     - To convert DER format to PEM, use the following command:

     `openssl x509 -inform der -in <server/or/client>cert.cer -out <server/or/client>cert.pem`

     - To convert DER format to PKCS#12, first convert DER to PEM using the preceding command, and then convert PEM to PKCS#12 use the following command:

     `openssl pkcs12 -export -out <server/or/client>cert.pfx -inkey privateKey.key -in <server/or/client>cert.cer -certfile <server/or/client>cacert.cer`

   - From P7B Format

     - To convert P7B format to PEM, use the following command:

     `openssl pkcs7 -print_certs -in <server/or/client>cert.p7b -out <server/or/client>cert.cer`

     - To convert P7B format to PKCS#12, first convert P7B to PEM using the preceding command, and then convert PEM to PKCS#12 use the following command:

     `openssl pkcs12 -export -in <server/or/client>cert.cer -inkey privateKey.key -out <server/or/client>cert.pfx -certfile <server/or/client>cacert.cer`

Enable SSL Between AuthMinder Server and User Data Service

To set up one-way SSL between AuthMinder Server and User Data Service (UDS), you must upload the UDS Server certificates required for SSL communication by using the User Data Service Connectivity Configuration page of the Administration Console. In case of two-way SSL, you must also upload the AuthMinder Server client certificate by using the User Data Service Connectivity Configuration page. The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 302)
- Two-Way SSL (see page 303)

Note: In this communication, AuthMinder Server is the client and UDS is the server.

One-Way SSL

To enable one-way SSL communication between AuthMinder Server and UDS:

1. Enable the application server where UDS is deployed for SSL communication.

   See your application server vendor documentation for more information about how to do this.

2. Access the Administration Console in a Web browser window.
3. Log in to Administration Console as the Master Administrator (MA).
4. Activate the Services and Server Configurations tab in the main menu.
5. Ensure that the Administration Console tab in the submenu is active.
6. Under System Configuration, click the UDS Connectivity Configuration link to display the corresponding page.
7. In the Protocol field, select One-Way SSL.
8. Set the Port value to default SSL port.
9. Click the Browse button adjacent to the Server Root Certificate field to select the UDS root certificate.
10. Click Save.
11. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.

Two-Way SSL

To set up two-way SSL between AuthMinder Server and User Data Service (UDS):

1. Enable the application server where User Data Service (UDS) is deployed for SSL communication.

   See your application server vendor documentation for more information about how to do this.

2. Access the Administration Console in a Web browser window.
3. Log in to Administration Console as the MA.
4. Activate the Services and Server Configurations tab in the main menu.
5. Ensure that the Administration Console tab in the submenu is active.
6. Under Administration Console, click the UDS Connectivity Configuration link to display the corresponding page.
7. In the Protocol field, select Two-Way SSL.
8. Set the Port value to default SSL port.
9. Click the Browse button adjacent to the Server Root CA field to select the UDS root certificate.
10. Click the Browse button adjacent to the Client Certificate field to select the AuthMinder root certificate.
11. Click the Browse button adjacent to the Client Private Key field to select the AuthMinder private key.
12. Click Save.
13. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.

Enable SSL Between Administration Console and AuthMinder Server

To set up one-way SSL between Administration Console and AuthMinder Server, you must upload the AuthMinder Server root certificate using the Protocol Management (Server Management Web Services) and WebFort Connectivity (Server Management Web Services) pages of the Administration Console.

In case of two-way SSL, you must create the client store using the Trusted Certificates Authorities page, configure the client store using the Protocol Management (Server Management Web Services) page, and configure the client certificates using the WebFort Connectivity (Server Management Web Services) page of the Administration Console.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 305)
- Two-Way SSL (see page 307)

Note: In this communication, Administration Console is the client and AuthMinder Server is the server.

One-Way SSL

To set up one-way SSL between Administration Console and AuthMinder Server:

1. Access the Administration Console in a Web browser.
2. Log in to Administration Console as the MA.
3. Activate the Services and Server Configurations tab in the main menu.
4. Activate the WebFort tab in the submenu.
5. Under Instance Configurations, click the Protocol Management link to display the corresponding page.

   The Protocol Configuration page appears.
6. Select the Server Instance for which you want to configure the protocols.
7. In the List of Protocols section, click the Server Management Web Services link.

   The page to configure the protocol appears.
8. Configure the following fields:
   - Ensure that the protocol is enabled.
   - In the Transport field, select SSL (1-Way).
   - Select Key in HSM if you want to store the SSL key in HSM.
   - (Only if you selected Key in HSM in the preceding step) Click the Browse button adjacent to the Certificate Chain (in PEM Format) field to select the AuthMinder root certificate.
   - Click the Browse button adjacent to the P12 File Containing Key Pair field to select the AuthMinder root certificate.
   - Enter the password for the PKCS#12 store in the P12 File Password field.
9. Click the Save button.
10. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
11. Activate the Services and Server Configurations tab in the main menu.
12. Activate the WebFort tab in the submenu.
13. Under System Configuration, click the WebFort Connectivity link to display the corresponding page.

    The WebFort Connectivity page appears.
14. Set the following for the Server Management Web Services protocol:
    - Ensure that the IP Address and Port number of the AuthMinder Server is set appropriately.
    - In the Transport field, select SSL(1-Way).

- Click the Browse button adjacent to the Server CA Certificate in PEM field to select the AuthMinder root certificate.

15. Click the **Save** button.
16. Restart the AuthMinder Server.
17. Verify that the AuthMinder Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
    b. Open the arcotwebfortstartup.log file in a text editor.
    c. Check for the following line in the [ArWFProtocolConfiguration] section of the Server Management Web Services protocol ([ServerManagement-WS]):
    `P0RTTYPE : [SSL]`
    d. Close the file.

Two-Way SSL

To set up two-way SSL between Administration Console and AuthMinder Server:

1. Enable the application server where Administration Console is deployed for SSL communication. See your application server vendor documentation for more information about how to do this.
2. Log in to Administration Console using a Master Administrator account.
3. Activate the Services and Server Configurations tab in the main menu.
4. Activate the WebFort tab in the submenu.
5. Under Instance Configurations, click the Trusted Certificate Authorities link to display the corresponding page.

   The Trusted Certificate Authorities page appears.
6. Set the following information:
   - In the Name field, enter the name for the SSL trust store.
   - Click the Browse button to select the root certificate of the application server where Administration Console is deployed.
7. Click the Save button.
8. Under Instance Configurations, click the Protocol Management link to display the corresponding page.

   The Protocol Configuration page appears.
9. Select the Server Instance for which you want to configure the protocols.
10. In the List of Protocols section, click the Server Management Web Services link.

    The page to configure the protocol appears.
11. Configure the following fields:
    - Ensure that the protocol is enabled.
    - In the Transport field, select SSL (2-Way).
    - Select Key in HSM if you want to store the SSL key in HSM.
    - (Only if you selected Key in HSM in the preceding step) Click the Browse button adjacent to the Certificate Chain (in PEM Format) field to select the AuthMinder root certificate.
    - Click the Browse button adjacent to the P12 File Containing Key Pair field to select the AuthMinder root certificate.
    - Enter the password for the PKCS#12 store in the P12 File Password field.
    - Select the Client Store that you created in Step 6.
12. Click the Save button.

13. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
14. Activate the Services and Server Configurations tab in the main menu.
15. Activate the WebFort tab in the submenu.
16. Under System Configuration, click the WebFort Connectivity link to display the corresponding page.

    The WebFort Connectivity page appears.
17. Set the following for the Server Management Web Services protocol:
    - Ensure that the IP Address and Port number of the AuthMinder Server is set appropriately.
    - In the Transport field, select SSL(2-Way).
    - Click the Browse button adjacent to the Server CA Certificate in PEM field to select the AuthMinder root certificate.
    - Click the Browse button adjacent to the Client Certificate-Key Pair in PKCS#12 field to select the PKCS#12 file that contains the root certificate of the application server where Administration Console is deployed.
    - Enter the PKCS#12 file password in the Client PKCS#12 Password field.
18. Click the Save button.
19. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
20. Verify that the AuthMinder Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
       - **On Windows**:
         `<install_location>\Arcot Systems\logs`
       - **On UNIX-Based Platforms**:
         `<install_location>/arcot/logs`
    b. Open the arcotwebfortstartup.log file in a text editor.
    c. Search for the following section:

       Listing : [Successful listeners(Type-Port-FD)]
    d. In this section, you must find the following line:
       `ServerManagement-WS..... : [SSL-9743-<Internal_listener_identifier>-[subject [<cert_subject>] issuer [<cert_issuer>] sn [<cert_serial_number>] device [<device_name>]]]`
    e. Close the file.

Enable SSL Between Java SDKs and AuthMinder Server

To set up one-way SSL between Java SDKs (Authentication and Issuance) and AuthMinder Server, you must first configure the Transaction Native protocol by using the Protocol Management page of the Administration Console and then configure the webfort.authentication.properties and webfort.issuance.properties files.

In case of two-way SSL, you must create the client store using the Trusted Certificates Authorities page, configure the client store using the Protocol Management (Transaction Native) page, configure the client certificates using the WebFort Connectivity (Transaction Native) page of the Administration Console, and then configure the webfort.authentication.properties and webfort.issuance.properties files.

Note: If you want to enable SSL between Administration Web Service and AuthMinder Server, then you need to follow the steps mentioned in this section.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 310)
- Two-Way SSL (see page 312)

Note: In this communication, your application integrated with the Java SDKs is the client and AuthMinder Server is the server.

One-Way SSL

To enable SSL communication mode between Java SDKs and AuthMinder Server:

1. Access the Administration Console in a Web browser.
2. Ensure that you are logged in as the MA.
3. Activate the Services and Server Configurations tab in the main menu.
4. Ensure that the WebFort tab in the submenu is active.
5. Under the Instance Configurations section, click the Protocol Management link to display the Protocol Configuration page.
6. Select the Server Instance for which you want to configure the protocols.
7. In the List of Protocols section, click the Transaction Native protocol link

   The page to configure the protocol appears.
8. Configure the following fields:
   - Ensure that the Protocol Status is Enabled.
   - In the Transport field, select SSL (1-Way).
   - Select Key in HSM if you want to store the SSL key in HSM.
   - (Only if you selected Key in HSM in the preceding step) Click the Browse button adjacent to the Certificate Chain (in PEM Format) field to select the AuthMinder root certificate.
   - Click the Browse button adjacent to the P12 File Containing Key Pair field to select the AuthMinder root certificate.
   - Enter the password for the PKCS#12 store in the P12 File Password field.
9. Click the Save button.
10. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
11. Navigate to the following location:
    - **On Windows:**
      `<install_location>\Arcot Systems\sdk\client\java\properties`
    - **On UNIX-Based Platforms:**
      `<install_location>/arcot/sdk/client/java/properties`
12. Open the webfort.authentication.properties file in an editor window.
    a. Set the following parameters:
       - authentication.transport = 1SSL (By default, this parameter is set to TCP.)
       - authentication.serverCACertPEMPath = *<absolute_path_of_Root_Certificate_in_PEM_FORMAT>*

For example, you can specify authentication.serverCACertPEMPath = <install_location>/certs/<ca_cert>.pem.

Note: See "Configuration Files and Options" the in *CA AuthMinder Installation and Deployment Guide* for more information about the webfort.authentication.properties file.

b. Save the changes and close the file.

13. Open the webfort.issuance.properties file in an editor window.

a. Set the following parameters:

- issuance.transport = SSL (By default, this parameter is set to TCP.)
- issaunce.serverCACertPEMPath = <*absolute_path_of_Root_Certificate_in_PEM_FORMAT*>

For example, you can specify issuance.serverCACertPEMPath = <install_location>/certs/<ca_cert>.pem.

Note: See "Configuration Files and Options" in the *CA AuthMinder Installation and Deployment Guide* for more information about the webfort.issuance.properties file.

b. Save the changes and close the file.

14. Restart the application server where Java SDKs are deployed.

Two-Way SSL

To enable SSL communication mode between Java SDKs and AuthMinder Server:

1. Enable the application server where Java SDKs are deployed for SSL communication. See your application server vendor documentation for more information about how to do this.
2. Access the Administration Console in a Web browser.
3. Log in to Administration Console as the MA.
4. Activate the Services and Server Configurations tab in the main menu.
5. Activate the WebFort tab in the submenu.
6. Under Instance Configurations, click the Trusted Certificate Authorities link to display the corresponding page.

   The Trusted Certificate Authorities page appears.
7. Set the following information:
   - In the Name field, enter the name for the SSL trust store.
   - Click the Browse button to select the root certificate of the application server where Java SDKs are deployed.
8. Click the Save button.
9. Under Instance Configurations, click the Protocol Management link to display the corresponding page.

   The Protocol Configuration page appears.
10. Select the Server Instance for which you want to configure the protocols.
11. In the List of Protocols section, click the Transaction Native link.

    The page to configure the protocol appears.
12. Configure the following fields:
    - Ensure that the protocol is enabled.
    - In the Transport field, select SSL (2-Way).
    - Select Key in HSM if you want to store the SSL key in HSM.
    - (Only if you selected Key in HSM in the preceding step) Click the Browse button adjacent to the Certificate Chain (in PEM Format) field to select the AuthMinder root certificate.
    - Click the Browse button adjacent to the P12 File Containing Key Pair field to select the AuthMinder root certificate.
    - Enter the password for the PKCS#12 store in the P12 File Password field.
    - Select the Client Store that you created in Step 7.
13. Click the Save button.

14. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
15. Activate the Services and Server Configurations tab in the main menu.
16. Activate the WebFort tab in the submenu.
17. Under System Configuration, click the WebFort Connectivity link to display the corresponding page.

    The WebFort Connectivity page appears.
18. Set the following for the Transaction Native protocol:
    - Ensure that the IP Address and Port number of the AuthMinder Server is set appropriately.
    - In the Transport field, select SSL(2-Way).
    - Click the Browse button adjacent to the Server CA Certificate in PEM field to select the AuthMinder root certificate.
    - Click the Browse button adjacent to the Client Certificate-Key Pair in PKCS#12 field to select the PKCS#12 file that contains the root certificate of the application server where Java SDKs are deployed.
    - Enter the PKCS#12 file password in the Client PKCS#12 Password field.
19. Click the Save button.
20. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
21. Navigate to the following location:
    - **On Windows:**
      `<install_location>\Arcot Systems\sdk\client\java\properties`
    - **On UNIX-Based Platforms:**
      `<install_location>/arcot/sdk/client/java/properties`
22. Open the webfort.authentication.properties file in an editor window.
    a. Set the following parameters:
       - authentication.transport = 2SSL (By default, this parameter is set to TCP.)
       - authentication.serverCACertPEMPath = *<absolute_path_of_Root_Certificate_in_PEM_FORMAT>*

       For example, you can specify authentication.serverCACertPEMPath = <install_location>/certs/<ca_cert>.pem.
       - authentication.clientCertKeyP12Path = *<absolute_path_of_Client_Certificate_in_P12_FORMAT>*
       - authentication.clientCertKeyPassword = Password for the client PKCS#12 file.

Note: See "Configuration Files and Options" in the *CA AuthMinder Installation and Deployment Guide* for more information about the webfort.authentication.properties file.

b. Save the changes and close the file.

23. Open the webfort.issuance.properties file in an editor window.

a. Set the following parameters:

- issuance.transport = SSL (By default, this parameter is set to TCP.)
- issaunce.serverCACertPEMPath = <*absolute_path_of_Root_Certificate_in_PEM_FORMAT*>

For example, you can specify issuance.serverCACertPEMPath = <install_location>/certs/<ca_cert>.pem.

- issuance.clientCertKeyP12Path = <*absolute_path_of_Client_Certificate_in_P12_FORMAT*>
- issuance.clientCertKeyPassword = Password for the client PKCS#12 file.

Note: See "Configuration Files and Options" in the *CA AuthMinder Installation and Deployment Guide* for more information about the webfort.issuance.properties file.

b. Save the changes and close the file.

24. Restart the application server where your Java SDKs are deployed.

25. Verify that the AuthMinder Server is enabled for SSL communication by performing the following steps:

a. Navigate to the following location:

- **On Windows**:

<*install_location*>\Arcot Systems\logs

- **On UNIX-Based Platforms**:

<*install_location*>/arcot/logs

b. Open the arcotwebfortstartup.log file in a text editor.

c. Search for the following section:

Listing : [Successful listeners(Type-Port-FD)]

d. In this section, you must find the following line:

```
Transaction-Native.............................. :
[SSL-9742-<Internal_listener_identifier>-[subject
[<cert_subject>] issuer [<cert_issuer>] sn
[<cert_serial_number>] device [<device_name>]]]
```

e. Close the file.

Enable SSL Between Transaction Web Services and AuthMinder Server

To set up one-way SSL between Transaction Web services (used for credential issuance and authentication) and AuthMinder Server, you must first configure the Transaction Web Services protocol by using the Protocol Management page of the Administration Console.

In case of two-way SSL, you must create the client store using the Trusted Certificates Authorities page, configure the client store using the Protocol Management (Transaction Web Services) page, and configure the client certificates using the WebFort Connectivity (Transaction Web Services) page of the Administration Console.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 316)
- Two-Way SSL (see page 317)

Note: In this communication, your application integrated with Web services is the client and AuthMinder Server is the server.

One-Way SSL

Perform the following steps to set up SSL between Web services and AuthMinder Server:

1. Access the Administration Console in a Web browser.
2. Log in to Administration Console as the Master Administrator (MA).
3. Activate the Services and Server Configurations tab in the main menu.
4. Ensure that the WebFort tab in the submenu is active.
5. Under the Instance Configurations section, click the Protocol Management link to display the Protocol Configuration page.
6. Select the Server Instance for which you want to configure the protocols.
7. In the List of Protocols section, click the Transaction Web Services protocol link

   The page to configure the protocol appears.
8. Configure the following fields:
   - Ensure that the Protocol Status is Enabled.
   - In the Transport field, select SSL (1-Way).
   - Select Key in HSM if you want to store the SSL key in HSM.
   - (Only if you selected Key in HSM in the preceding step) Click the Browse button adjacent to the Certificate Chain (in PEM Format) field to select the AuthMinder root certificate.
   - Click the Browse button adjacent to the P12 File Containing Key Pair field to select the AuthMinder root certificate.
   - Enter the password for the PKCS#12 store in the P12 File Password field.
9. Click the Save button.
10. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.

Two-Way SSL

To enable SSL communication mode between Web services and AuthMinder Server:

1. Enable the application server where your client integrated with Web services is deployed for SSL communication. See your application server vendor documentation for more information about how to do this.
2. Log in to Administration Console as the MA.
3. Activate the Services and Server Configurations tab in the main menu.
4. Activate the WebFort tab in the submenu.
5. Under Instance Configurations, click the Trusted Certificate Authorities link to display the corresponding page.

   The Trusted Certificate Authorities page appears.
6. Set the following information:
   - In the Name field, enter the name for the SSL trust store.
   - Click the Browse button to select the root certificate of the application server where Web services client is deployed.
7. Click the Save button.
8. Under Instance Configurations, click the Protocol Management link to display the corresponding page.

   The Protocol Configuration page appears.
9. Select the Server Instance for which you want to configure the protocols.
10. In the List of Protocols section, click the Transaction Web Services link.

    The page to configure the protocol appears.
11. Configure the following fields:
    - Ensure that the protocol is enabled.
    - In the Transport field, select SSL (2-Way).
    - Select Key in HSM if you want to store the SSL key in HSM.
    - (Only if you selected Key in HSM in the preceding step) Click the Browse button adjacent to the Certificate Chain (in PEM Format) field to select the AuthMinder root certificate.
    - Click the Browse button adjacent to the P12 File Containing Key Pair field to select the AuthMinder root certificate.
    - Enter the password for the PKCS#12 store in the P12 File Password field.
    - Select the Client Store that you created in Step 6.
12. Click the Save button.

13. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
14. Activate the Services and Server Configurations tab in the main menu.
15. Activate the WebFort tab in the submenu.
16. Under System Configuration, click the WebFort Connectivity link to display the corresponding page.

    The WebFort Connectivity page appears.
17. Set the following for the Transaction Web Services protocol:
    - Ensure that the IP Address and Port number of the AuthMinder Server is set appropriately.
    - In the Transport field, select SSL(2-Way).
    - Click the Browse button adjacent to the Server CA Certificate in PEM field to select the AuthMinder root certificate.
    - Click the Browse button adjacent to the Client Certificate-Key Pair in PKCS#12 field to select the PKCS#12 file that contains the root certificate of the application server where Java SDKs are deployed.
    - Enter the PKCS#12 file password in the Client PKCS#12 Password field.
18. Click the Save button.
19. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
20. Verify that the AuthMinder Server is enabled for SSL communication by performing the following steps:
    a. Navigate to the following location:
       - **On Windows**:
         `<install_location>\Arcot Systems\logs`
       - **On UNIX-Based Platforms**:
         `<install_location>/arcot/logs`
    b. Open the arcotwebfortstartup.log file in a text editor.
    c. Search for the following section:

       Listing : [Successful listeners(Type-Port-FD)]
    d. In this section, you must find the following line:
       ```
       Transaction-WS.............................. :
       [SSL-9744-<Internal_listener_identifier>-[subject
       [<cert_subject>] issuer [<cert_issuer>] sn
       [<cert_serial_number>] device [<device_name>]]]
       ```
    e. Close the file.

Enable SSL Between arwfutil and AuthMinder Server

To set up one-way SSL between arwfutil: A Utility Tool (see page 251) and AuthMinder Server, you must first upload the AuthMinder Server root certificate using the Protocol Management (Server Management Web Services) page of the Administration Console, and then edit the arcotcommon.ini file to set the transport mode and server certificate.

In case of two-way SSL, create the client store using the Trusted Certificates Authorities page, configure the client store using the Protocol Management (Server Management Web Services) page of the Administration Console, and edit the arcotcommon.ini file to set the transport mode, server and client certificates.

The following subsections walk you through the detailed steps for configuring:

- One-Way SSL (see page 320)
- Two-Way SSL (see page 323)

One-Way SSL

Perform the following steps to enable one-way SSL between arwfutil and the AuthMinder Server:

1. Access the Administration Console in a Web browser.
2. Log in to Administration Console as the MA.
3. Activate the **Services and Server Configurations** tab in the main menu.
4. Activate the **WebFort** tab in the submenu.
5. Under **Instance Configurations**, click the **Protocol Management** link to display the corresponding page.

   The Protocol Configuration page appears.
6. Select the **Server Instance** for which you want to configure the protocols.
7. In the **List of Protocols** section, click the **Server Management Web Services** link.

   The page to configure the protocol appears.
8. Configure the following fields:
   - Ensure that the protocol is enabled.
   - In the **Transport** field, select **SSL (1-Way)**.
   - Select **Key in HSM** if you want to store the SSL key in HSM.
   - (*Only* if you selected **Key in HSM** in the preceding step) Click the **Browse** button adjacent to the **Certificate Chain (in PEM Format)** field to select the AuthMinder root certificate.
   - Click the **Browse** button adjacent to the **P12 File Containing Key Pair** field to select the AuthMinder root certificate.
   - Enter the password for the PKCS#12 store in the **P12 File Password** field.
9. Click the **Save** button.
10. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
11. Navigate to the following location:
    - **On Windows:**
      `<install_location>\Arcot Systems\conf`
    - **On UNIX-Based Platforms:**
      `<install_location>/arcot/conf`
12. Open the arcotcommon.ini file in an editor window to add the SSL configuration parameters.
    a. Add the following section at the end of the file:
    ```
    [arcot/webfort/wfutil]
    Transport=
    ```

```
ReadTimeOut=
ServerRootPEM=
ClientP12=
ClientP12PwdKey=
ClientPEM=
```

The following table explains these parameters:

Parameter	Default Value	Description
Transport	TCP	The communication mode between the arwfutil utility and the AuthMinder Server. Following are the supported values: ■ TCP ■ 1SSL ■ 2SSL
ReadTimeout	No Default	The maximum time in milliseconds allowed for a response from AuthMinder Server.
ServerRootPEM	No Default	Provide the complete path for the CA certificate file of the server. The file *must* be in PEM format. For example: server.CACertPEMPath=<*%SystemDrive%*>/certs/webfort_ca.pem
(For software encryption) ClientP12	No Default	Provide the path for the client certificate, which is in p12 format.
(For software encryption) ClientP12PwdKey	No Default	Enter the key label that is used to access the client P12 password stored in the securestore.enc file.
(For hardware encryption) ClientPEM	No Default	Provide the complete path for the CA certificate file of the client. The file *must* be in PEM format.

a. Save the changes and close the file.

1. Verify that the AuthMinder Server is enabled for SSL communication by performing the following steps:

   a. Navigate to the following location:

   b. Open the arcotwebfortstartup.log file in a text editor.

   c. Check for the following line in the [ArWFProtocolConfiguration] section of the Server Management Web Services protocol ([ServerManagement-WS]):
   `P0RTTYPE : [SSL]`

   d. Close the file.

Two-Way SSL

Perform the following steps to enable two-way SSL between arwfutil and the AuthMinder Server:

1. Log in to Administration Console using a Master Administrator account.
2. Activate the Services and Server Configurations tab in the main menu.
3. Activate the WebFort tab in the submenu.
4. Under Instance Configurations, click the Trusted Certificate Authorities link to display the corresponding page.

   The Trusted Certificate Authorities page appears.
5. Set the following information:
   - In the Name field, enter the name for the SSL trust store.
   - Click the Browse button to select the root certificate used by arwfutil.
6. Click the Save button.
7. Under Instance Configurations, click the Protocol Management link to display the corresponding page.

   The Protocol Configuration page appears.
8. Select the Server Instance for which you want to configure the protocols.
9. In the List of Protocols section, click the Server Management Web Services link.

   The page to configure the protocol appears.
10. Configure the following fields:
    - Ensure that the protocol is enabled.
    - In the Transport field, select SSL (2-Way).
    - Select Key in HSM if you want to store the SSL key in HSM.
    - (Only if you selected Key in HSM in the preceding step) Click the Browse button adjacent to the Certificate Chain (in PEM Format) field to select the AuthMinder root certificate.
    - Click the Browse button adjacent to the P12 File Containing Key Pair field to select the AuthMinder root certificate.
    - Enter the password for the PKCS#12 store in the P12 File Password field.
    - Select the Client Store that you created in Step 6.
11. Click the Save button.
12. Restart the AuthMinder Server instance. See "Restarting a Server Instance" (see page 75) for instructions on how to restart the AuthMinder Server.
13. Navigate to the following location:
    - **On Windows:**

`<install_location>\Arcot Systems\conf`

- **On UNIX-Based Platforms:**
  `<install_location>/arcot/conf`

14. Open the arcotcommon.ini file in an editor window to add the SSL configuration parameters.

    a. Add the following section at the end of the file:

```
[arcot/webfort/wfutil]
Transport=
ReadTimeOut=
ServerRootPEM=
ClientP12=
ClientP12PwdKey=
ClientPEM=
```

    The following table explains these parameters:

Parameter	Default Value	Description
Transport	TCP	The communication mode between the arwfutil utility and the AuthMinder Server. Following are the supported values: ■ TCP ■ 1SSL ■ 2SSL
ReadTimeout	No Default	The maximum time in milliseconds allowed for a response from AuthMinder Server.
ServerRootPEM	No Default	Provide the complete path for the CA certificate file of the server. The file *must* be in PEM format. For example: server.CACertPEMPath=*<%SystemDrive%>*/certs/webfort_ca.pem
(For software encryption) ClientP12	No Default	Provide the path for the client certificate, which is in p12 format.
(For software encryption) ClientP12PwdKey	No Default	Enter the key label that is used to access the client P12 password stored in the securestore.enc file.
(For hardware encryption) ClientPEM	No Default	Provide the complete path for the CA certificate file of the client. The file *must* be in PEM format.

a. Save the changes and close the file.

1. Verify that the AuthMinder Server is enabled for SSL communication by performing the following steps:

   a. Navigate to the following location:

      - **On Windows**:
        `<install_location>\Arcot Systems\logs`
      - **On UNIX-Based Platforms**:
        `<install_location>/arcot/logs`

   b. Open the arcotwebfortstartup.log file in a text editor.

   c. Search for the following section:

      Listing : [Successful listeners(Type-Port-FD)]

   d. In this section, you must find the following line:
      `ServerManagement-WS..... : [SSL-9743-<Internal_listener_identifier>-[subject [<cert_subject>] issuer [<cert_issuer>] sn [<cert_serial_number>] device [<device_name>]]]`

   e. Close the file.

Enable One-Way SSL Between AuthMinder Components and Database

This section walks you through the steps to set up one-way SSL communication between AuthMinder components and AuthMinder database. The section covers the following topics:

Note: Before proceeding with the configurations explained in this section, ensure that you have enabled the database server for SSL communication. See your database vendor documentation for more information about how to do this.

AuthMinder Server and Database

AuthMinder uses DataDirect driver to connect to the database. This section walks you through the configurations that you must perform on the system where you have installed the AuthMinder Server.

On Windows

Perform the following steps to enable one-way SSL between AuthMinder Server and Oracle database:

1. Log in to the system where you have installed the AuthMinder Server.
2. Open the ODBC Data Source Manager.
3. Activate the System DSN tab.
4. Select the data source that is used by AuthMinder to configure for SSL.
5. Click Configure.

   The ODBC Oracle Wire Protocol Driver Setup dialog appears.
6. In the Encryption section, select 1-SSL Auto in the Encryption Method drop down list.
7. Set Truststore to the location where the trust store file containing a list of the valid Certificate Authorities (CAs) that are trusted by the AuthMinder is available.
8. Specify the password for the trust store in the Truststore Password field.
9. Set the Host Name in Certificate fields to the host name of the system where the database server is installed. See your database vendor documentation for this parameter.
10. Click OK to save the configurations.

On UNIX-Based Platforms

If you want to enable SSL between AuthMinder and the database on UNIX platforms, then you need to edit the odbc.ini file to configure the DataDirect driver.

Perform the following steps to configure the odbc.ini file:

1. Navigate to the following location:
   `<install_location>/arcot/odbc32v70wf`
2. Open the odbc.ini file in a file editor.
3. In the [*<Database_name>* Wire Protocol] section that corresponds to the database you are using, you must edit the parameters required for SSL connection as listed in the following table:

Parameter	Description
EncryptionMethod	Specifies the method the driver uses to encrypt data sent between the driver and the database server. Set this parameter to 1 to encrypt the data using SSL.

Parameter	Description
Truststore	Specifies the location of the trust store file, which contains a list of the valid Certificate Authorities (CAs) that are trusted by the client machine for SSL server authentication.
TrustStorePassword	Specifies the password required to access the trust store.
ValidateServerCertificate	Validates the security certificate of the server as part of the SSL authentication handshake. Set this parameter to 1 to validate the certificate sent by the database server.

4. Save and close the odbc.ini file.

Administration Console and Database

Administration Console uses Java Database Connectivity (JDBC) to connect to the database. To enable SSL between Administration Console and database:

1. Configure the application server where the Administration Console is deployed for SSL.
2. Configure the TrustStorePath.*<N>* and HostNameInCertificate.*<N>* parameters in the arcotcommon.ini file.

Note: See "Configuration Files and Options" in the *CA AuthMinder Installation and Deployment Guide* for more information about the arcotcommon.ini parameters.

User Data Service and Database

UDS uses JDBC to connect to the database. To enable SSL between User Data Service and database:

1. Configure the application server where UDS is deployed for SSL.
2. Configure the TrustStorePath.*<N>* and HostNameInCertificate.*<N>* parameters in the arcotcommon.ini file.

Note: See "Configuration Files and Options" in the *CA AuthMinder Installation and Deployment Guide* for more information about the arcotcommon.ini parameters.

Appendix E: Troubleshooting Administration Console Errors

This appendix describes the troubleshooting steps, which will help you resolve the errors that you might face while using Administration Console.

Before you perform any troubleshooting tasks, check the Administration Console log file (arcotadmin.log) to see if there were any errors. By default, the arcotadmin.log file is saved in the following location:

On Windows:

`<install_location>\Arcot Systems\logs\`

On Unix-Based Platforms:

`<install_location>/arcot/logs/`

Note: See "AuthMinder Logging" (see page 275) for detailed information about the AuthMinder log files.

Problem:

I am not able to log in to Administration Console by using the Master Administrator (MA) account. I see the "Administrator Account is locked" message.

Cause:

You might have tried to authenticate with the wrong password for more than the allowed authentication attempts.

Solution:

Reset the authentication attempt count, also known as *strike count* to 0, by using the following script:

For MS SQL

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN';
GO
```

For Oracle

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN'; commit;
```

For DB2

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN'; commit;
```

For MySQL

```
update ARADMINBASICAUTHUSER set STRIKECOUNT=0 where
USERID='MASTERADMIN';
```

Problem:

When I try to log in to the Administration Console as the Master Administrator, I see the following error message:

```
There was an internal server error while processing the database query.
Please contact your database administrator.
```

Cause:

The possible cause for this issue might be that all active datasources in the database pool have been exhausted.

Solution:

To resolve this issue, do the following:

1. Ensure that the database server is reachable.

2. Restart the database or the database listener
3. If the Administration Console and the AuthMinder Server are using the same database, then:
   a. Restart the AuthMinder service.
   b. Restart the browser.

Problem:

I do not remember the MA password, how do I reset the password?

Solution:

To reset the MA password:

1. Locate the folder with the scripts for your database type. The default location is:

   (for Windows-MS SQL) <*install_location*>\Arcot Systems\dbscripts\mssql

   (for Windows-Oracle) <*install_location*>\Arcot Systems\dbscripts\oracle

   (for Windows- IBM DB2 UDB) <*install_location*>\Arcot Systems\dbscripts\db2

   (for Windows-MySQL) <*install_location*>\Arcot Systems\dbscripts\mysql

   (for UNIX-MS SQL) <*install_location*>/arcot/dbscripts/mssql

   (for UNIX-Oracle) <*install_location*>/arcot/dbscripts/oracle

   (for UNIX-IBM DB2 UDB) <*install_location*>/arcot/dbscripts/db2

   (for UNIX-MySQL) <*install_location*>/arcot/dbscripts/mysql
2. Run the arcot-masteradmin-password-reset-2.0.sql script by using the database vendor tools.

   The MA password in now reset to the default password, which is master1234!.

Problem:

I cannot access the AuthMinder pages from the Services and Server Configuration tab. I see the following error message.
`Unable to contact the servers at this point of time. Please try later.`

Solution:

Ensure the following:

- WebFort Server is running.
- The WebFort Server connectivity details are correct.

Log in to the Administration Console as MA. Navigate to the Services and Server Configurations -> WebFort -> Connectivity Details page, and check whether the AuthMinder host and port information for the Server Management Web Services is set correctly.

Problem

When I try to log in to the Administration Console, I see the following message.
`ErrorCode 500: Internal server error.`

Cause:

- Your browser cache might be full.
- Your application server time-out settings might need to be reset.

Solution:

Do the following:

- Empty the browser cache of the browser you are trying to open the Console in and try again.
- If the message persists, then try opening the Console by using a different browser.
- Check the time-out settings for the application server container.
- If the problem still persists, then open the arcotadmin.log file and search for the "Administration Console configured successfully." string.
- If you do not find the "Administration Console configured successfully." string, then look for the error description, and act accordingly.

Problem:

The Administration Console did not correctly deploy. I see the java.lang.ClassNotFoundException exception in the arcotadmin.log file:

Cause:

This issue occurs only if the WAR or EAR was not properly deployed or was corrupted.

Solution:

To resolve this, do the following:

1. Clean up the working directory of your application server.

   For example, on Apache Tomcat, this directory is called work.

2. Deploy the WAR or EAR file again.

Problem:

I have created and activated an Organization, but when I try to perform any AuthMinder configurations, I see the following error:
`Organization not Found`

Cause:

The possible causes might be you are trying to perform the task for a new organization that you created, but did not refresh the AuthMinder Server cache.

Solution:

Refresh the AuthMinder Server Cache.

When you create a new organization by using the Administration Console, always restart the AuthMinder Server cache.

Note: See "Refreshing a Server Instance" (see page 67) in the *CA AuthMinder Administration Guide* for more information.

Problem

While searching for users and administrators, I see the following error message:
`There was an internal server error while communicating with User Data Service. Please contact your Administrator.`

Cause:

There might be too many users to be searched in the given organization(s). As a result, the operation timed out.

Solution:

Do the following:

1. Log in to the Administration Console as MA.
2. Navigate to the **Services and Server Configurations** -> **Administration Console** -> **UDS Connectivity Configuration** page.
   - Increase the value of the **Connection Timeout** field.
   - Increase the value for the **Read Timeout** field.

3. Change the search criteria to narrow down the expected search results.