CA AuthMinder

Release Notes

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 1: General Release Information

This section contains the following topics:

Operating System Support

The prerequisites for CA AuthMinder are based on the server platform.

For detailed information about platform support and system requirements, see the *CA AuthMinder Installation and Deployment Guide* for your platform.

Documentation

Updated documentation for this product is available at http://ca.com/support.

The documentation, in bookshelf format, includes:

- CA AuthMinder Installation and Deployment Guide for UNIX Platforms
- CA AuthMinder Installation and Deployment Guide for Microsoft Windows
- CA AuthMinder Administration Guide
- CA AuthMinder Java Developer's Guide
- CA AuthMinder Web Services Developer's Guide
- CA AuthMinder Release Notes

Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Chapter 2: New Features

This section contains the following topics:

Support for Oracle RAC

From this release onward, Oracle RAC version 11.2.0.1.0 has been added to the list of databases supported by CA AuthMinder and CA Adapter.

Support for MySQL

From this release onward, MySQL Enterprise Edition 5.1 has been added to the list of databases supported by CA AuthMinder.

Support for Transaction Signing

ArcotID OTP supports the Transaction Signing feature in the Sign mode of passcode generation. This feature conforms to the OATH Challenge-Response Algorithm (OCRA) defined by RFC 6287.

Support for Configuring the Time Step for TOTP-Based ArcotID OTP

From this release onward, you can set the size of the time interval during which the OTP generated by the client is the same as the OTP generated by the server.

Support for Salt-Based Encryption

In the encryption context, salt is random data that is prefixed to a data item during the encryption process. Addition of this random data improves the strength of the encryption. In this release, salt-based encryption is applied to most of the user and credential parameters and configuration parameters that were only encrypted in earlier releases.

Note: For the full list of parameters to which salt-based encryption is applied, see the *CA AuthMinder Administration Guide*.

Key Management Enhancements

The following are the enhancements to the key management feature in this release:

- Support for Creating Domain Key for an Organization (see page 12)
- Support for OATH OTP, ArcotOTP-OATH, and ArcotOTP-EMV Master Key Creation and Rotation (see page 13)

Support for Creating Domain Key for an Organization

A Domain Key is used to protect the public key stored in the ArcotID. When an ArcotID is created, the current default domain key for the organization is used to protect it. With this release of AuthMinder, you can:

- Create multiple key configurations using the Administration Console. The latest key is used as the default key while creating ArcotIDs and authenticating those ArcotIDs. The other active keys will be used for authentication only. You can configure keys at the global level or at the organization level.
- Update the key validity period. You can update the validity of active and expired keys.
- Retire a key, which means the key will no longer be valid after this operation.

During the AuthMinder server bootstrap, a domain key is created at the global level. For more information about Domain Key management, see the CA AuthMinder Administration Guide.

Support for OATH OTP, ArcotOTP-OATH, and ArcotOTP-EMV Master Key Creation and Rotation

Keys are used to protect the shared secret that is used to generate OTPs, which include OATH OTP, ArcotOTP-OATH, and ArcotOTP-EMV.

In this release of AuthMinder, you can:

- Create multiple key configurations using the Administration Console. The latest key is used as the default key for creating OTPs and authenticating those OTPs. The other active keys will be used for authentication only. You can configure keys at the global level or at the organization level.
- Update the key validity period. You can update the validity of active and expired keys.
- Retire a key, which means the key will no longer be valid after this operation, and the OTPs associated with that key will expire.

RADIUS Enhancements

The following are the RADIUS enhancements in this release:

- Support for Wireless LAN Authentication (see page 13)
- Support for Multiple Authentication Mechanisms Over RADIUS (see page 14)
- Support for Handling Multiple Organizations for RADIUS (see page 14)
- Enhancements to RADIUS Client Configurations (see page 15)
- Support for WebFort Server as a RADIUS Proxy (see page 15)

Support for Wireless LAN Authentication

AuthMinder now supports ArcotID authentication for accessing Wireless Local Area Network over RADIUS. To use this feature, you have to select the Authentication Type as EAP when you add RADIUS clients using the Administration Console. EAP uses TLS between client and AuthMinder Server.

Support for Multiple Authentication Mechanisms Over RADIUS

AuthMinder now supports a new authentication type for RADIUS called In-Band Password. This authentication type can be mapped to various password type credentials supported by AuthMinder. The incoming credential is resolved based on the Credential Type Resolution configuration that is configured by using the Administration Console.

In-Band Password authentication type supports the following password type credentials:

- Password
- One-Time Password
- OATH OTP
- ArcotOTP-OATH
- ArcotOTP-EMV
- RADIUS OTP
- Native Token

To support this feature you must configure the credential type resolution for the organization. You can also apply credential type resolution for a user by using the user custom attributes. If the credential type resolution is not configured, then by default the RADIUS OTP credential is used.

Support for Handling Multiple Organizations for RADIUS

You can now specify the organization information in the RADIUS requests. To do so, you need to use the In-Band Password authentication type.

If you are adding RADIUS client at the global level, then you need to select the organizations for which the RADIUS client will be applicable. You can also set the default organization.

If you are adding RADIUS client at the organization level, then the RADIUS client will be configured for that organization.

You can also pass the organization information as part of the Password field by prefixing the organization name to the Password field. The organization name and password must be separated with \n. If the organization name is not specified in the Password field, then the default organization will be used.

Enhancements to RADIUS Client Configurations

The following enhancements have been made to the RADIUS Client Configuration page in the Administration Console:

- Support for returning arbitrary RADIUS attributes to the client.
- Provision to add user and credential custom attributes, which will be included in the response message sent to the RADIUS client.
- Support to drop the RADIUS packets under certain conditions, instead of responding with an error.

  The RADIUS packets are dropped if the user or credential is not found, if the request is not valid, or if there is an internal error. This enables the RADIUS client to correct the request and then send it to the same AuthMinder Server instance or to a different instance.

Support for WebFort Server as a RADIUS Proxy

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

A new screen called, RADIUS Proxy Configuration has been included in the Administration Console to enable AuthMinder Server as a proxy server and to add the details of RADIUS server that processes the proxy requests.

For more information about configuring AuthMinder as a RADIUS Proxy Server, see the CA AuthMinder Administration Guide.

Support for Hardware Security Module

The following are the new Hardware Security Module (HSM) features:

- Support for Hardware Security Module (HSM) (see page 16)
- Support for Configuration of a Different Key Per Organization (see page 16)

Support for Hardware Security Module

In addition to storing keys in the database, AuthMinder now enables you to store the following keys in the HSM:

- Master Keys: AuthMinder uses different keys to protect data stored in the database. These keys can be configured by using the Administration Console and can be stored in an HSM.
- WebFort Server listener SSL key: By default, AuthMinder components use Transmission Control Protocol (TCP) to communicate with each other, and support Secure Socket Layer (SSL) for all TCP-based listeners.

  You can store the WebFort SSL listener key in an HSM

Support for Configuration of a Different Key Per Organization

In addition to the global key that is used to encrypt configuration data at the global-level, you can also configure the keys at the organization-level, which will be used to encrypt organization configuration and user data.

Configuration Management Enhancements

The following are the configuration management enhancements in this release:

- Support for Programmable Configuration Management (see page 17)
- Support for Organization-Level Cache Refresh (see page 17)
- Configuration Names are No Longer Case-Sensitive (see page 17)
- Configuration Name Unique to Each Credential Type (see page 17)
- Provision to Copy Configurations from Any Organization in the Administrator's Scope (see page 18)

Support for Programmable Configuration Management

The following enhancements have been made to the configuration experience:

- Web service interfaces are exposed for all configurations.
- Support for creating multiple configurations per organization.
- Support for updating multiple configurations per organization.
- Support for assigning multiple configurations as default per organization.
- Support for deleting multiple configurations per organization.
- Support for OATH token management.
- Support for key validation by checking if a key for the specified label exists in the HSM device.

Support for Organization-Level Cache Refresh

Administrators can now refresh the cache of all or selected organizations, which are under their purview, without refreshing the global cache. To perform this, the administrator must have the Refresh Organization Cache privilege at the organization level.

Configuration Names are No Longer Case-Sensitive

In this release, configuration names are not case-sensitive.

Configuration Name Unique to Each Credential Type

The configuration names for the credential profiles or authentication policies can be the same across credentials. You can now assign the same name to different policies or profiles that might have similar configurations.

For example, if you want to create ArcotID and password authentication policies with a criteria that the users should not be able to authenticate if they provide an incorrect password three consecutive times, then you can create ArcotID and password authentication policies with the same name, maxthreeattempts, and set the Lockout Credential After parameter to 3.

Provision to Copy Configurations from Any Organization in the Administrator's Scope

This release of AuthMinder extends its support to copy configurations from any organization that is in the Administrator's purview.

OATH OTP Enhancements

The following are the OATH OTP enhancements in this release:

Support for a Token Management Page

You can use the OATH OTP Token Management page to bulk upload the OATH tokens or fetch the OATH tokens that are assigned at the global-level or organization-level in bulk. Using various filters, you can easily view token status, tokens uploaded in the system, and other token-related information.

Support for Bulk Operations Using Web Services

You can now upload and assign the OATH tokens in bulk using the Bulk Upload Web service. In case of a bulk upload request, the AuthMinder Server responds with a Batch ID, and then processes the bulk upload request.

Using the Batch ID status and other details of the token, you can run a query on the upload. The format of the bulk upload request can either be an XML input, or token information passed as individual elements. The seed encryption format supported for methods are AES128-CBC, HEX, and BASE64. For more information, see the chapter about performing bulk operations in the CA AuthMinder Web Services Developer's Guide.

Note: The User Administrator, who manages the user credentials, can also assign tokens individually to users by using the Manage Credentials page of the Administration Console.

Support for Querying Token Information

Once the tokens are uploaded, you can query for information about the upload operation. The following criteria are supported for a query:

- Information related to global organization
- Information related to a specified list of organizations
- Information related to token identifiers (wild cards, such as * or . can be used)
- Information related to Batch ID returned for a given upload operation
- Information related to different token status values, such as free, assigned, abandoned, and failed.

Support for Re-Assigning Abandoned OATH Tokens

User Administrators can now re-assign the unused OATH tokens to different users. This feature helps to reuse the existing tokens, instead of investing in new tokens.

Support for De-Assigning OATH Tokens

Using the Administration Console, administrators can now de-assign the tokens issued to users.

Support for OTP Synchronization

Using the Administration Console, administrators can now perform OTP synchronization for time-based and counter-based OATH OTP and ArcotOTP credentials on behalf of the end user.

Arcot OTP Enhancements

The following are the Arcot OTP Enhancements in this release:

- Support for EMV-Based OTPs (see page 20)
- Support for Arbitrary Custom Card Strings for ArcotOTP-OATH and ArcotOTP-EMV (see page 20)
- Support for ArcotOTP Roaming (see page 20)

Support for EMV-Based OTPs

AuthMinder supports the OTPs that are based on Europay, MasterCard, and VISA (EMV) protocols. This credential is called ArcotOTP-EMV. It supports mode-2 of EMV OTP verification. Similar to other credentials, you can create issuance profile and authentication policy to manage these types of OTPs.

Support for Arbitrary Custom Card Strings for ArcotOTP-OATH and ArcotOTP-EMV

You can customize the ArcotOTP-OATH and ArcotOTP-EMV cards by specifying additional information that you want to add to the cards.

Support for ArcotOTP Roaming

The ArcotOTP card can be downloaded from AuthMinder Server using the downloadCredential API. This API returns the complete card with the current state of the credential. This feature is available for both ArcotOTP-OATH and ArcotOTP-EMV.

Miscellaneous Credential Enhancements

The following are the miscellaneous credential enhancements in this release:

- Support for Password History Check (see page 20)
- Enhancements to AuthMinder Credentials (see page 21)
- Support for Credential Custom Attributes in Profiles (see page 21)
- Enhanced OATH-based OTP Synchronization (see page 21)

Support for Password History Check

AuthMinder now maintains the history of users' ArcotID passwords and Passwords at the organization level. This helps administrators to enforce users not to use the last <N> passwords, or the passwords that were used in the last <X> period. The values of N and X can be configured by using the Administration Console, where N is a numeric value and X is in years, months, days, hours, and minutes.

Enhancements to AuthMinder Credentials

The following enhancements have been made to the AuthMinder credentials:

- Support for Warning Period

  In addition to ArcotID credential, WebFort now supports warning period for all other credentials. This enables your application to send prior notifications to your users about impending credential expiration.

- Support for Grace Period

  In addition to ArcotID credential, WebFort now supports grace period for all other credentials. This enables your application to authenticate users with their expired credentials for a configured period of time.

- Support for Multiple Credentials

  In addition to the support for multiple Password credentials per user, WebFort can now issue multiples of other credential types to a user. The credentials of the user are identified by the Usage Type attribute that defines which credential has to be used for authenticating the user.

  For example, you can issue two ArcotOTPs to a user, with usage types as TOTP and HOTP.

Support for Credential Custom Attributes in Profiles

Administrators can now configure a set of custom attributes for a credential. This enables applications that integrate with AuthMinder to ensure that certain application-related workflows or other such data is pre-set in the credential.

Enhanced OATH-based OTP Synchronization

Using the Administration Console, administrators can now perform OATH OTP synchronization for time-based OATH OTP credentials on behalf of the end user.

Enhancements to Question and Answer (QnA) Credential

The QnA credential has been enhanced to perform one or more of the following operations in one call:

- Deleting an existing QnA pair
- Updating an existing question
- Updating the answer of an existing question
- Resetting the complete question and answer set

Listener Protocol Enhancements

The following are the listener protocol enhancements in this release:

Support for New Configuration Parameters

The following enhancements have been made to all the listener protocols:

- Keep-Alive client connections

  Retains the client connection even after the request is processed. The connection is closed when the connection duration is equal to client idle timeout period.

- Maximum allowed input data packet size

  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. By default, there is no limit on the input request size.

- Client idle timeout

  The interval, in seconds, for which the client waits before closing the connection.

Support for HTTP Connection Header

By default, all connections are kept alive by the server for a configured period of time. This allows for client applications to build connection pools. There may be a situation where connections are created for one-time use and then left open. To close such connections, HTTP connection header can be used for sending notification to AuthMinder server to close the connection immediately.

Support for Proprietary Protocol for Issuance SDK

In addition to the Authentication Java SDK, the Issuance Java SDK also uses the Transaction Native protocol. This removes dependency on Apache Axis for Issuance Java SDK, which in turn makes the SDK considerably thinner.

Support for the Anti-Connection or Thread Hogging Feature

This feature ensures that a certain number of threads are always available on the server to serve requests at all times. A threshold limit is defined per protocol- this is calculated based on the percentage of the maximum number of threads. When the threshold is reached, the AuthMinder Server closes the connection after serving the request to ensure that the thread is available for serving further requests from any of the clients.

Audit Logging Enhancements

The following are the audit logging enhancements in this release:

- Enhanced Audit Logging (see page 23)
- Enhancement in the Credential Management Report (see page 23)

Enhanced Audit Logging

AuthMinder is now equipped to audit HTTP User Agent, HTTP Referrer, Session ID, and IP Address related information. The audited information can be viewed through AuthMinder reports.

Enhancement in the Credential Management Report

This release of AuthMinder provides support for logging disable period in the Credential Management Report.

File Logging Enhancements

The following are the file logging enhancements in this release:

- Support for Setting Logging Parameters Per Transaction (see page 24)
- Support for Mandatory Logging of Certain Parameters Per Transaction (see page 25)
- Java SDK Log Enhancements (see page 27)
- Support for Logging Sensitive Data (see page 28)

Support for Setting Logging Parameters Per Transaction

The following parameters can be set as additional inputs to increase the logging level for a specific transaction. This is useful where test transactions are done for monitoring.

- AR_WF_TXN_FILE_LOG_LEVEL - The values are the same as the log level.
- AR_WF_TXN_FILE_LOG_TRACE - Enables trace logging.
- AR_WF_TXN_DB_LOG_QUERY_DETAILS - Enables database query logging.

These parameters cannot be used to lower the log level that is configured on the server.

Support for Mandatory Logging of Certain Parameters Per Transaction

For every request that the AuthMinder Server processes, the Txn-Begin and Txn-End log lines are logged irrespective of the log level.

The following is an example of a Transaction Begin log line:

```
      TxnID=150057 | ClientTxnID=[_1T8I_31_34] | Protocol=5
(TXN_NATIVE) | ReqSize=936 |
      TST=2011-11-13 15:25:13:0 (DB)
```

The following is an example of a Transaction End log line:

```
      TxnID=150057 | ClientTxnID=[_1T8I_31_34] | Processor=13
(AUTH_ARCOTID) | Operation=1030
      (AUTH_AID_VERIFY_SIGNEDCHAL) | Response=0 (SUCCESS) | Reason=0
(UNDEFINED) | RespSize=245 | Time=97 | DBT=10
      | NQ=9 | ExtEvents={ NONE } | AddInfo=[NONE] | LTB=48631 |
LNL=0402/0402 | LML=196
```

The following are the details of the parameters in the log line:

TxnID

Transaction identifier

ClientTxnID

Client (typically Java SDK) transaction identifier

Protocol

Internal identifier for the input protocol used

ReqSize

Size of the input request in bytes

TST

Timestamp of the request and the source (DB indicates that the time source is the database server)

Processor

Internal identifier for processing module

Operation

Identifier for the operation

Response

Response code, indicates the final status of the transaction

Reason

Further detailed status of the transaction, typically applicable in case of failure

RespSize

Size of the response sent in bytes

Time

Time taken to process the request

DBT

Time spent for database operations

NQ

Number of database queries executed

ExtEvents

Any external events triggered. This is applicable in case of plug-in

AddInfo

Contains operation specific data, if any

LTB

Bytes logged to the file

LNL

Number of lines actually logged or attempted

LML

Longest log line length

Java SDK Log Enhancements

AuthMinder Java SDK logging is enhanced to ensure that there is traceability on the client as well as between the client and the server. All time parameters are in milliseconds.

The following is an example of a Transaction Begin log line:

```
OP=verifySignedChallenge | CTxID=_1T8I_31_34
```

The following is an example of a Transaction End log line:

```
OP=verifySignedChallenge | CTxID=_1T8I_31_34 | STxID=150057 | RC=0 |
REC=0 | TOT=130 | SRT=87 | TGC=10 | TRC=0 | TWR=31 | TRD=2 | TCR=0 |
RTC=1 | NCA=-1 | NCB=-1
```

Following are the details of the parameters in the log line:

OP

Identifier for the operation

CTxID

Java SDK transaction identifier

STxID

WebFort server transaction identifier

RC

Response code that indicates the final status of the transaction

REC

Detailed status of the transaction, typically applicable in case of failure

TOT

Total time taken to process the API call

SRT

Time taken by the server to process and respond to the request

TGC

Time taken to get the connection from the pool

TRC

Time taken to return the connection to the pool

TWR

Time take to write to the socket

TRD

Time take to read from the socket

TCR

Time taken to create a new connection

RTC

Retry count, which specifies the number of attempts made on the pool to get the connection

NCA

Number of connections available in the pool at this point in time

NCB

Number of connections borrowed from the pool at this point in time

Support for Logging Sensitive Data

Typically most of the user and credential data is sensitive. Starting this release such data will not be logged in the server file logs. However, there might be cases where tests have to be performed to verify the user sensitive data. To support such conditions, you have to use the AR_WF_TXN_LOG_SENSITIVE_DATA additional input. When this additional input is passed in the call, AuthMinder Server logs the sensitive data to the log file. This parameter should be used for test transactions only, and must not be used for production transactions.

Installer Enhancements

The following are the installer enhancements in this release:

- Changes in SDK Directory (see page 28)
- Sample XML Files (see page 29)

Changes in SDK Directory

The files in the Install_Directory/sdk/ directory have been classified based on whether they are used by the Java SDK client or AuthMinder Server.

- The Install_Directory/sdk/client directory contains the files that are required for Java SDKs. You will require these files to integrate your application with Java SDK.
- The Install_Directory/sdk/server directory contains C++ SDK that is used by plug-in.

Note: Java SDKs depend on log4j-1.2.16.jar for logging, the JAR itself is expected to be packaged by the application calling the AuthMinder Java SDK.

Sample XML Files

The Install_Directory/samples/xml/webfort/ directory file contains the sample XML files that can be used for uploading and assigning OATH tokens. This file provides predefined tokens and users.

Support for Authentication and Authorization for Web Services

All AuthMinder Web services calls can be protected through authentication and authorization. As a result, all requests to the Web services are authenticated for valid credentials. After which, all requests are then validated for appropriate privileges to access the Web services.

Access Management Enhancements

The following are the access management enhancements in this release:

- Support for Multiple Accounts (see page 30)
- Support for Uploading Users and User Accounts in Bulk (see page 30)
- Support to Recreate a New User With Deleted User's Username (see page 30)
- Support to Recreate a New Administrator With Deleted Administrator's Username (see page 30)
- Support for Deactivating User Account Temporarily (see page 30)
- Support to Add Custom Attributes to Users From an LDAP Based Organization (see page 31)
- Provision to Temporarily Lock Administrator's Password Credential (see page 31)
- Support for New Web Services (see page 31)

Support for Multiple Accounts

From this release, in addition to the UserName attribute, users can also be identified by an alternate ID called Account ID. This ID is also referred to as an Account. The AccountID is further qualified by another attribute, which provides additional context about the usage of the account. This attribute is referred to as Account Type. Users can use UserName or any of the accounts for AuthMinder authentication.

A user can have one or more accounts in AuthMinder. The account ID associated with each user for a different account type can be created by using the Administration Console or User Management Web Services provided by User Data Service (UDS). A default account can be configured for each organization.

See the CA AuthMinder Administration Guide and CA AuthMinder Web Services Guide for more information.

Support for Uploading Users and User Accounts in Bulk

AuthMinder now supports upload of 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.

Support to Recreate a New User With Deleted User's Username

If the user with administrative privileges is deleted, then the same user can be re-created and promoted to administrator in the same organization.

Support to Recreate a New Administrator With Deleted Administrator's Username

After an administrator is deleted, all privileges associated with the administrator are permanently deleted. As a result, the administrator can no longer log in to the Administration Console. However, their information and credentials are not removed from the system. You cannot create a new administrator with the same name as a previously deleted administrator in the same organization, however you can create one in a different organization.

Support for Deactivating User Account Temporarily

In this release, you can temporarily deactivate a user account. When you temporarily deactivate the user account, it is automatically activated when the end of the lock period is reached.

Support to Add Custom Attributes to Users From an LDAP Based Organization

You can now provide additional information about the user while creating LDAP users in the Custom Attributes section on the Create User page.

Provision to Temporarily Lock Administrator's Password Credential

You can choose to lock the administrator's credentials for a specified Credential Lock Period, which you can specify while updating administrators.

Support for New Web Services

AuthMinder now provides Web services for managing organizations, account types, users, and user accounts. See the CA AuthMinder Web Services Guide for more information.

Administration Console Enhancements

The following are the Administration Console enhancements in this release:

- Additional Administrator Profile Settings (see page 31)
- Support for Password History Check (see page 31)
- New Report Download Tool (see page 32)
- Support for Administrator Authentication Using LDAP Password (see page 32)
- Separate Password Policy for Master Administrators (see page 32)

Additional Administrator Profile Settings

Administrators can now set their preferred time zone and locale by using the My Profile page in the Administration Console. By default, the time zone is set to GMT and the locale is set to English - United States (en-US).

Support for Password History Check

The Maximum Password History Count field on the Basic Authentication Policy Page and Master Administrator Authentication Policy Page enables you to specify the maximum number of previously used passwords that cannot be used to log in to the Administration Console.

New 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.

Support for Administrator Authentication Using LDAP Password

The LDAP User Password mechanism is applicable only for LDAP organizations. The authentication policy is defined in the LDAP directory service. If you select this option, then administrators must use the credentials stored in LDAP to log in to the Administration Console.

Separate Password Policy for Master Administrators

By default, the Master Administrator follows the Basic Authentication method that enables them to log in to the Administration Console by using a user ID and the corresponding password. You can use the Master Administrator Authentication Policy page to strengthen the Master Administrator's 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 account.

Enhancements to arwfutil

You can now configure one-way and two-way SSL between arwfutil and the AuthMinder Server. See the CA AuthMinder Administration Guide for more information.

Support for Additional Third-Party Software

AuthMinder now supports the following third-party software:

- JBoss application server 5.1.x
- Oracle Directory Server 11g
- Windows Active Directory 2008

Chapter 3: Changed Features

This section contains the following topics:

Deprecated Features

The following features have been deprecated in this release of the product:

- Callout feature
- The RADIUS ArcotID inband feature has been deprecated.

Chapter 4: Known Issues

This section contains the following topics:

Documentation Not Available for One-Way SSL Communication Between AuthMinder Components and Database Servers

The AuthMinder Administration Guide does not include the steps to configure one-way SSL communication between AuthMinder components (Administration Console and User Data Service) and the database servers.

EAP Authentication Type Not Enabled for RADIUS Configuration

The EAP authentication type is not currently supported although it is displayed as an option on the RADIUS Configuration screen. Do not select this option.

Bulk Upload of User Accounts Does Not Accept a Range of Values for the Account Status

Symptom:

Bulk upload of user accounts does not accept a range of values for the account status. It accepts only the following:

- 0 [for Initial]
- 10 [for Active]

20 [for Inactive]

Solution:

Use the createUserAccount UDS web service, which accepts all values for the status field.

Cannot Use Administration Console to Delete Information About Users Deleted from LDAP Organization

Symptom:

Using the Administration Console, you cannot delete user information, such as accounts, PAM, and custom attributes for users deleted from LDAP organizations.

Solution:

You can delete this information by using Web services, if the user has been deleted from the LDAP organization.

Uninstallation Must Be Performed in Reverse Order

If you have performed Custom installation, then during uninstallation you must follow the reverse sequence in which you performed the installation. For example, if you have installed AuthMinder Authentication Server followed by Administration Console, then you have to first uninstall Administration Console, and then uninstall AuthMinder Authentication Server.

The arwfutil Command Runs Successfully Even with Multiple Options

Running the arwfutil command with multiple options must result in a failure due to invalid options. However, in this release, the arwfutil command runs successfully even when it is run with multiple options.

Global-Level Tokens Fetched on the OATH OTP Token Management Page

Symptom:

On the OATH OTP Token Management page in the Administration Console, clicking the Fetch button fetched all global-level tokens, even when the Fetch Tokens Available at Global Level option was not selected.

Solution:

This issue does not occur if the organization name is specified. Ensure that you specify the organization name when searching for tokens.

Administration Console Not Displayed Correctly in Internet Explorer 9

Symptom:

After you upgrade to Internet Explorer 9, the Administration Console is not displayed correctly.

Solution:

Restore the Internet Explorer 9 settings by navigating to Internet Options, Advanced, and then clicking Restore advanced settings.

After Uninstallation, Registry Entries Are Not Deleted

Symptom:

After uninstallation, some of the registry entries related to the product are not removed.

Solution:

This issue has no functional impact. The registry entries are overwritten during the next installation.

Log File Location is Not Intuitive

Symptom:

At the end of the installation process, the location of the log file displayed on the installer screen is not intuitive.

Solution:

On Windows, ignore the Arcot Systems\..\ part of the directory path that is displayed on the installer screen. Similarly, on UNIX platforms, ignore the arcot/../ part of the directory path.

Null Pointer Exception is Logged When arcotcommon.ini is Missing

Symptom:

If arcotcommon.ini is missing, then a null pointer exception is logged in arcotadmin.log.

Solution:

Ensure that arcotcommon.ini is always present.

When Multiple Parameters are Passed to arwfutil Utility, Only the First Parameter is Used

Symptom:

If you pass multiple parameters to the arwfutil utility, only the first parameter is used by the utility.

Solution:

Do not pass multiple parameters to the arwfutil utility.

Inconsistent Display of the Release Number

Symptom:

When you run the installer for Microsoft Windows, you may see occurrences of “7.1.1” as the release number. You may also see occurrences of “7.1.1” in the registry entries that are created at the end of the installation process.

Solution:

Ignore this inconsistency in the display of the release number. Both “7.1.1” and "7.1.01" refer to the same release.

Chapter 5: Defects Fixed

This section contains the following topics:

UNIX Installation Behavior Inconsistent in GUI Mode

Symptom:

In the earlier releases, GUI mode was enabled as the default mode of installation. As GUI installation is not supported in Linux or Solaris, the UNIX installation experience was not consistent.

Solution:

The GUI mode is not available in the Linux and Solaris installers any more.

No Support for Microsoft SQL Server Replication

Symptom:

Microsoft SQL Server replication was not supported in earlier releases of AuthMinder.

Solution:

In this release, primary keys have been added in all tables to support database replication.

Server Fails to Start if the Backup Folder is Missing in the Logs Folder

Symptom:

The AuthMinder Server failed to start if the backup folder was missing in the *ARCOT_HOME*/logs folder.

Solution:

The server now handles this situation. Log file roll over now happens in the *ARCOT_HOME*/logs folder.

AuthMinder Server Does Not Start in the RHEL 6.2 64 Bit Version

Symptom:

The AuthMinder server did not start in the RHEL 6.2 64 bit version.

Solution:

This release of AuthMinder includes a new version of data direct drivers for RHEL and this issue is resolved.

OTP Length at Issuance Different from What Was Defined in the Profile

Symptom:

When using the ArcotOTP credential, even if the OTP length in the issuance profile was set to 8, during issuance the downloaded credential string always had an OTP length of 6.

Solution:

This issue has been fixed.

Credential Management Screen Not Showing Credential Information

Symptom:

The Credential Management screen did not display credential information, if the usage type was configured in the profile.

Solution:

This issue has now been resolved.

Compilation Errors with wf-common-interface.hpp on RHEL

Symptom:

The wf-common-interface.hpp file, included in the RHEL version of the product, resulted in the following compilation error:

```
memset was not declared in this scope
```

Solution:

This issue has now been resolved.

EAP-TLS Authentication Allowed for Any Certificate/Key Pair

Symptom:

When AuthMinder Server is set up to perform EPA-TLS authentication over RADIUS protocol for ArcotID, authentication should pass if the certificate used by the client contains an Arcot extension. However, authentication was successful even when the client used a certificate that was issued by any CA.

Solution:

This issue has now been resolved.

Deleted Users Not Handled in the AuthMinder Upgrade Tool

Symptom:

In the previous release, the upgrade tool could not retrieve information about deleted users and threw an exception during upgrade.

Solution:

This issue has now been resolved.

Memory Leak in AuthMinder Server While Creating a Profile or Policy

Symptom:

A memory leak was occurring in AuthMinder Server while creating profiles or policies.

Solution:

This issue has been resolved now.

Insufficient Privilege Errors on Some Administration Console Screens

Symptom:

Some screens in the Administration Console, such as the RADIUS client configuration screen and Callout configuration screen, displayed errors unexpectedly informing the user that they have insufficient privileges on that page.

Solution:

This issue has now been resolved.

Configuration Management Report Showed Operation ID After Upgrade

Symptom:

If you had created configurations for different credentials in AuthMinder and then upgraded the AuthMinder instance, the Configuration Management Report on the upgraded instance displayed the operation ID instead of the operation name.

Solution:

This issue has now been resolved.

Authentication Failure When Authenticating LDAP Users

Symptom:

When using RHEL 6.2 (64 bit version), if you created an organization that pointed to an LDAP repository, and set credential resolution to verify LDAP password, then end user authentication failed with an internal error.

Solution:

This issue has now been resolved.

Two-Way SSL Trust Store Details Not Visible When Configuring the Protocol

Symptom:

If you created a trust store to authenticate to the AuthMinder Server during two-way SSL communications, when you selected a protocol on the Protocol Configuration screen and then selected the client store, the screen did not display the details.

Solution:

This issue has now been resolved.

Server Crashing When Authenticating Over RADIUS Protocol

Symptom:

Authentication over RADIUS protocol on RHEL or Solaris resulted in an AuthMinder Server crash.

Solution:

This issue has now been resolved.

Users with View Privilege Able to Enable or Disable Authentication Mechanism

Symptom:

A user who was assigned a role with only View privilege could enable or disable authentication mechanisms in the Administration Console.

Solution:

This issue has now been resolved. Users with View privilege cannot modify any configurations.

Inconsistency in Authentication Error Messages

Symptom:

If authentication failed when using AuthMinder, different error messages were displayed for incorrect user name and incorrect password. This enabled internal users to generate a list of valid contact IDs, thereby speeding up password guessing attacks.

Solution:

This issue has now been resolved. Authentication failure is conveyed using a generic message in case of both incorrect user name and incorrect password.

Server Crashing When Creating Key Configuration with Invalid Input

Symptom:

The AuthMinder Server used to crash when trying to create a key configuration with invalid input, for example, when the key was created with the -genrsa option.

Solution:

This issue has been resolved now.

Some Administration Console Pages Vulnerable to CSS Attacks

Symptom:

The following Administration Console pages, accessible to authenticated users, were vulnerable to CSS attacks:

- Report View
- Change User Credential
- Change My Profile

Solution:

This issue has now been resolved.

JSESSIONID Disclosed in the URL

Symptom:

The JSESSIONID was disclosed in the URL and therefore, the administrator login session was not very secure.

Solution:

To secure the administrator login session, the JSESSIONID is not disclosed in the URL.

UDS Accessible through Axis2 Web Administration Console

Symptom:

Users could earlier upload non-CA applications to UDS by using the Axis2 Web Administration Console.

Solution:

This issue has now been resolved. To prevent malicious access to UDS application, access to Web Administration Module of Axis2 that is shipped with UDS is disabled.

Session IDs Not Generated After User Authentication

Symptom:

Session IDs were not generated after users authenticated to an application successfully. Consequently, in a shared computing environment, or using a cross-site scripting vulnerability, an attacker could record the session ID assigned to a particular computer and use it to access the application as an authenticated user.

Solution:

This issue has now been resolved.

HTTPS Responses Cached

Symptom:

Some browsers, including Internet Explorer, cache content accessed using HTTPS protocol. If sensitive information in application responses is stored in the local cache, then this can be retrieved by other users with access to the same computer at a future time.

Solution:

This issue has now been resolved.

Same Token Used for Cross-Site Request Forgery and the Session ID for Login Session

Symptom:

The token used for Cross-Site Request Forgery and the Session ID for login session were the same and therefore, administrator login session was not very secure.

Solution:

This issue has now been resolved. To secure the administrator login session, the two tokens are not the same anymore.

Cross Frame Scripting Vulnerability

Symptom:

The login page of the Administration Console was vulnerable to cross frame scripting.

Solution:

This issue has now been resolved.

Chapter 6: Product Limitations

The following are the known limitations in this release of the product:

- When using Oracle database and Apache Tomcat application server, if the network cable for the primary database is unplugged, then database failover takes more than 15 minutes.
- The Administration Console and UDS Web services are not supported on 64-bit application servers on Solaris.
- The silent mode of installation is not supported.
- You cannot install multiple instances of AuthMinder on the same system in different folders. If you try to install multiple instances, then the installation is not completed successfully.